A Study on Empirical Evaluation of Mutation Testing for Improving the Test Quality of Safety-Critical Software

S.Saranya[1], M.Manikandan[2],

1-Student, 2-Assistant professor

M.E(Software Engineering)

Mount Zion College of Engineering Technology

Email: abisaranya@rediffmail.com

***Abstract*— Testing** provides a primary means for assuring software in safety-critical systems. To demonstrate, particularly to a certification authority, that sufficient testing has been performed, it is necessary to achieve the test coverage levels recommended or mandated by safety standards and industry guidelines. Mutation testing provides an alternative or complementary method of measuring test sufficiency, but has not been widely adopted in the safety-critical industry. In this study, we provide an empirical evaluation of the application of mutation testing to airborne software systems which have already satisfied the coverage requirements for certification. Specifically, we apply mutation testing to safety-critical software developed using high-integrity subsets ,to identify the most effective mutant types, and analyze the root causes of failures in test cases. Our findings show how mutation testing could be effective where traditional structural coverage analysis and manual peer review have failed. They also show that several testing issues have origins beyond the test activity, and this suggests improvements to the requirements definition and coding process. Our study also examines the relationship between program characteristics and mutation survival and considers how program size can provide a means for targeting test areas most likely to have dormant faults. Industry feedback is also provided, particularly on how mutation testing can be integrated into a typical verification life cycle of airborne software.

***Index Terms*— Mutation** Testing, airborne software, safety-critical systems.

I. INTRODUCTION

Software testing and software fault tolerance are two major techniques for developing reliable software systems, yet limited empirical data are available in the literature to evaluate their effectiveness. We conducted a major experiment to engage 34 programming teams to independently develop multiple software versions for an industry-scale critical flight application, and collected faults detected in these program versions. To evaluate the effectiveness of software testing and software fault tolerance, mutants were created by injecting real faults occurred in the development stage. The nature, manifestation, detection, and correlation of these faults were carefully investigated. The results show that coverage testing is generally an effective mean to detecting software faults, but the effectiveness of testing coverage is not equivalent to that of mutation coverage, which is a more truthful indicator of testing quality. We also found that exact faults found among versions are very limited. This result supports software fault tolerance by design diversity as a creditable approach for software reliability engineering. Finally we conducted domain analysis approach for test case generation, and concluded that it is a promising technique for software testing purpose

II. MUTANT CREATION

RCS was required for source control for each team. Every code change of each program file at each check-in can therefore be identified. Software faults found during each stage are also identified. These faults were then injected into the final program versions to create mutants, each contain one programming fault. We elected 21 program versions for detailed investigation, and created 426 mutants. We disqualified the other 13 versions as their developers did not follow the development and coding standards which were necessary for generating meaningful mutants from their projects.

The following rules are applied in the mutant creation process:

1. Low-grade errors, for example compilation error and core dump exception, are not created.
2. Some changes were only available in middle versions. For example, the changes between 1.1 and 1.2 may not be completely identified in the final version. These changes are then ignored.
3. Code changes for debugging purposes are not included.
4. Modifications of the function prototypes are excluded.
5. As the specification does not mention about memory leaks, mutants are not created for any faults leading to memory leaks
6. The same programming error may span in many blocks of code. For example: a vector missed the division by 1000.0 may occur everywhere in a source file. It is counted as a single fault.

III. MUTATION TESTING

Mutation Testing is a fault-based testing technique which provides a testing criterion called the "mutation adequacy score". The mutation adequacy score can be used to measure the effectiveness of a test set in terms of its ability to detect faults. The general principle underlying Mutation Testing work is that the faults used by Mutation Testing represent the mistakes that programmers often make. By carefully choosing the location and type of mutant, we can also simulate any test adequacy criteria. Such faults are deliberately seeded into the original program, by simple syntactic changes, to create a set of faulty programs called mutants, each containing a different syntactic change. To assess the quality of a given test set, these mutants are executed against the input test set. If the result of running a mutant is different from the result of running the original program for any test cases in the input test set, the seeded fault denoted by the mutant is detected. One outcome of the Mutation Testing process is the mutation score, which indicates the quality of the input test set. The mutation score is the ratio of the number of detected faults over the total number of the seeded faults.

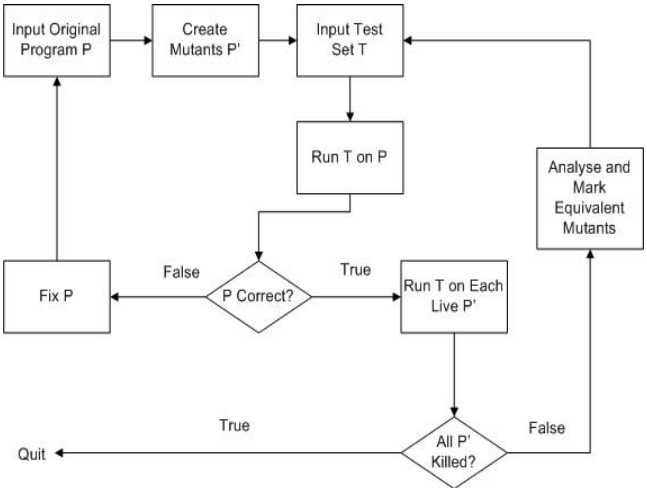


Fig. 1. Generic Process of Mutation Analysis

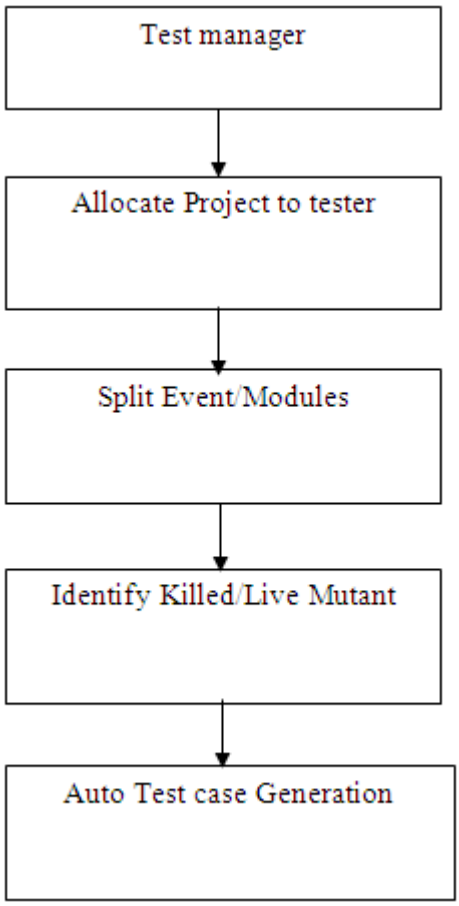


Fig. 2 Process of Data

III. TESTING SAFETY-CRITICAL SOFTWARE

Test technology is crucial for successful product development. Inappropriate or late tests, underestimated testing effort, or wrong test technology choices have often led projects to crisis and frustration. This software crisis results from neglecting the imbalance between constructive software engineering and analytic quality assurance. In this article we explain the testing concepts, the testing techniques, and the test technology approach applied to the patient monitors of the HP Omni Care family. Patient monitors are electronic medical devices for observing critically ill patients by monitoring their physiological parameters (ECG, heart rate, blood pressure, respiratory gases, oxygen saturation, and so on) in real time. A monitor can alert medical personnel when a physiological value exceeds preset limits and can report the patient's status on a variety of external devices such as recorders, printers, and computers, or simply send the data to a network. The monitor maintains a database of the physiological values to show the trends of the patient's status and enable a variety of calculations of drug dosage or ventilation and

hemodynamic parameters. Patient monitors are used in hospitals in operating rooms, emergency rooms, and intensive care units and can be configured for every patient category (adult, pediatric, or neonate). Very often the patient attached to a monitor is unconscious and is
sustained by other medical devices such as ventilators, anesthesia machines, fluid and drug pumps, and so on. These life-sustaining devices are interfaced with the patient monitor but not controlled from it. Safety and reliability requirements for medical devices are set very high by industry and regulatory authorities. There is a variety of international and national standards setting the rules for the development, marketing, and use of medical devices.
The legal requirements for electronic medical devices are, as far as these concern safety, comparable to those for nuclear plants and aircraft. In the past, the safety requirements covered mainly the hardware aspects of a device, such as electromagnetic compatibility, radio interference, electronic parts failure, and so on. The concern for software safety, accentuated by some widely known software failures leading to patient injury or death, is increasing in the industry and the regulatory bodies. This concern is addressed in many new standards or directives such as the Medical Device Directive of the European Union or the U.S. Food and Drug Administration. These legal requirements go beyond a simple validation of the product; they require the manufacturer to provide all evidence of good engineering practices during development and validation, as well the proof that all possible hazards from the use of the medical instrument were addressed, resolved, and validated during the development phases.

V.THE APPLICATION OF MUTATION TESTING

Since Mutation Testing was proposed in the 1970s, it has been applied to test both program source code (Program Mutation)and program specification (Specification Mutation) Program Mutation belongs to the category of white box based testing, in which faults are seeded into source code, while Specification Mutation belongs to black box based testing where faults are seeded into program specifications, but in which the source code may be unavailable during testing.

1) Mutation Testing for FORTRAN: In the earliest days of Mutation Testing, most of the experiments on Mutation Testing targeted Fortran. Budd et al. was the first to design mutation operators for Fortran IV in 1977. Based on these studies, a Mutation Testing tool named PIMS was developed for testing FORTRAN. However, there were no
Formal definitions of mutation operators for Fortran until 1987.In 1987, This set of mutation operators became the first set of formalized mutation operators and consequently had greater influence on later definitions of mutation operators for applying Mutation Testing to the other programming languages. These mutation operators are divided into three groups; the Statement analysis group, the Predicate analysis group and the coincidental correctness group.

2) Mutation Testing for Ada: Ada mutation operators were first proposed by Bowser in 1988. In 1997, based on previous work of Bowser's Ada mutation operators, Agrawal et al.'s C mutation operators and the design of Fortran 77 mutation operators for MOTHRA , Offutt et al. redesigned mutation operators for Ada programs to produce a proposed set of 65 Ada mutation operators. According to the semantics of Ada, this set of Ada mutation operators is divided into five groups: Operand Replacement Operators group, Statement Operators group, Expression Operators group, Coverage Operators group and Tasking Operators group.

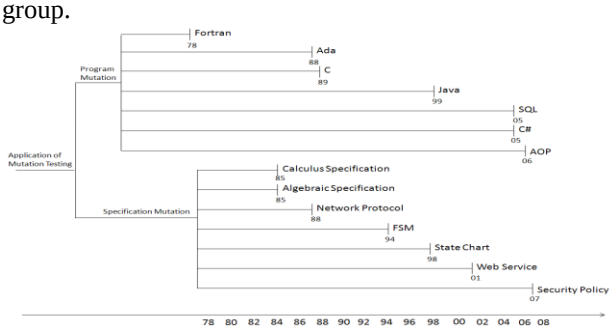


Fig 3.Publications of the Applications of Mutation Testing.

VI. CONCLUSION AND FUTURE WORK

This paper has provided a detailed survey and analysis of trends and results on Mutation Testing. The paper covers theories, optimization techniques, equivalent mutant detection, applications, empirical studies and mutation tools. There has been much optimization to reduce the cost of the Mutation Testing process. From the data we collected from and about the Mutation Testing literature, our analysis reveals an increasingly practical trend in the subject.
We also found evidence that there is an increasing number of new applications. There are more, larger and more realistic programs that can be handled by Mutation Testing. Recent trends also include the provision of new open source and industrial tools. These findings provide evidence to support the claim that the field of Mutation Testing is now reaching a mature state. Recent work has tended to focus on more elaborate forms of mutation than on the relatively simple faults that have been previously considered. There is an interest in the semantic effects of mutation, rather than the syntactic achievement of a mutation. This migration from the syntactic achievement of mutation to the desired semantic effect has raised interest in higher order mutation to generate subtle faults and to find those mutations that denote real faults. We hope the future will see a further

coming of age, with the generation of more realistic mutants and the test cases to kill them and with the provision of practical tooling to support both.

REFERENCES

[1] Y. Jia and M. Harman, "An Analysis and Survey of the Development of Mutation Testing, Software Engineering," IEEE Trans. Software Eng., vol. 37, no. 5, pp. 649-678, Sept./Oct. 2011.

[2] Functional Safety of Electronic/Programmable Electronic Safety-Related Systems, IEC 61508, Int'l Electro technical Commission, Mar. 2010.

[3] ISO 26262: Road Vehicles: Functional Safety, Int'l Organization for Standardization, June 2011.

[4] G. Jay, J.E. Hale, R.K. Smith, D.P. Hale, N.A. Kraft, and C. Ward, "Cyclomatic Complexity and Lines of Code: Empirical Evidence of a Stable Linear Relationship," J. Software Eng. and Applications, vol. 3, no. 2, 2009.

[5] Y. Jia and M. Harman, "Higher Order Mutation Testing, "Information and Software Technology, vol. 51, no. 10, pp. 1379-1393, 2009.

[6] J. Tuya, M. J. S. Cabal, and C. de la Riva, "SQL Mutation: A Tool to Generate Mutants of SQL Database Queries," in Proceedings of the 2nd Workshop on Mutation Analysis (MUTATION'06). Raleigh, North Carolina: IEEE Computer Society, November 2006, p. 1.

[7] J. Tuya, M. J. S. Cabal, and C. de la Riva, "Mutating Database Queries, "Information and Software Technology, vol. 49, no. 4, pp. 398–417,April 2007.

[8] B. H. Smith and L. Williams, "On Guiding the Augmentation of an Automated Test Suite via Mutation Analysis," Empirical Software Engineering, vol. 14, no. 3, pp.341–369,2009.

SEARCH USING WEB SERVICES AND "ON-THE-FLY" INFORMATION EXTRACTION

X.Mary Antony Jine[1], N.Mohan Prabhu[2],

1-Student, 2-Assistant professor

M.E(Software Engineering)

Mount Zion College of Engineering Technology

Email: x.a.jine@gmail.com

Abstract—The API of a Web service restricts the types of queries that the service can answer. For example, a Web service might provide a method that returns the songs of a given singer, but it might not provide a method that returns the singers of a given song. If the user asks for the singer of some specific song, then the Web service cannot be called – even though the underlying database might have the desired piece of information. This asymmetry is particularly problematic if the service is used in a Web service orchestration system. In this paper, we propose to use on-the-fly information extraction to collect values that can be used as parameter bindings for the Web service. We show how this idea can be integrated into aWeb service orchestration system.

INTRODUCTION

A. Motivation There is a growing number of Web services that provide a wealth of information. There are Web services about books (isbndb.org, librarything. com, Amazon, AbeBooks), about movies (api.internetvideoarchive.com), about music (musicbrainz.org, lastfm.com), and about a large variety of other topics. Usually, a Web service is an interface that provides access to an encapsulated back-end database. For example, the site musicbrainz.org offers a Web service for accessing its database about music albums. The Web service defines functions that can be called remotely. musicbrainz.org offers the function getSongs, which takes a singer as input parameter and delivers the songs by that singer as output. If the user wants to know all songs by Leonard Cohen, she can call getSongs with Leonard Cohen as input. The output will contain the songs Suzanne, Hallelujah, etc.

Web services play a crucial part in the trend towards datacentric applications on the Web. Unlike Web search engines, Web services deliver crisp answers to queries. This allows the user to retrieve answers to a query without having to read through several result pages. Web services can also be used to answer precise conjunctive queries, which would require several searches on the Web and joins across them, if done manually with a search engine. The results of Web services are machine-readable, which allows query answering systems to cater to complex user demands by orchestrating the services. These are advantages that Web services offer over keywordbased Web search.

Web services allow querying remote databases. However, the queries have to follow the binding patterns of the Web service functions, by

providing values for mandatory input parameters before the function can be called. In our example of musicbrainz, the function getSongs can only be called if a singer is provided. Thus, it is possible to ask for the songs of a given singer, but it is not possible to ask for the singers of a given song. If the user wants to know, e.g., who sang Hallelujah, then the Web service cannot be used to answer this question – even though the database contains the desired information. This restriction is not due to missing data, but a design choice of the Web service owner, who wants to prevent external users from extracting and downloading large fractions of its back-end database. On the client side, this is a highly inconvenient limitation, in which the data may be available, but cannot be queried in the desired way. We call this the problem of Web service asymmetry.

CONTRIBUTION

We develop a solution to the problem of Web service asymmetry. We propose to use Web-based information extraction (IE) on the fly to determine the right input values for the asymmetric Web services. For example, to find all singers of Hallelujah, we issue a keyword query "singers Hallelujah" to a search engine. We extract promising candidates from the result pages, say, Leonard Cohen, Lady Gaga, and Elvis. Next, we use the existing Web service to validate these candidates. In the example, we would call getSongs for every candidate, and see whether the result contains Hallelujah. This confirms the first singer and discards the others. This way, we can use an asymmetric Web service as if it allowed querying for an argument that its API does not support. We show how such functions can be integrated into a Web orchestration system, and how they can be prioritized over infinite chains of calls. Our technique works only if the Web provides adequate candidate entities.

PRELIMINARIES

GLOBAL SCHEMA. A Web service defines an API of functions that can be called over the Internet. Given some input values, a function returns as output a semi-structured document, usually in XML. In all of the following, we assume that the set of Web service functions is known. We also assume that all functions operate on the same, conceptually global database with a unified schema. This is an important assumption in our context, which we make in line with other works.

EXECUTION PLANS

GOAL. Our goal is to answer queries by using only function calls. This goal is in line with the works. The difficulty in answering queries lies in the fact that the query is formulated in terms of the global schema, not in terms of the functions. This is because the query expresses an information need, and not yet a constructive procedure. Since the user does not have access to the global database, we cannot execute the query directly on the tables of the global database. Rather, the algorithms automatically translate the query into query plans expressed in terms of the available Web service functions, respecting their binding pattern restrictions. This is a non-trivial endeavor that we discuss next. Different from previous work, we consider a given budget of calls. This changes the goal of the evaluation. Previous work aimed to compute the maximal number of query answers. The goal was to compute the maximal contained rewriting. Unfortunately, when the views have binding pattens, even the evaluation of conjunctive queries requires rewritings of unbound length. Thus, these works will produce pipelines of calls of an unbound length in order to obtain the maximal number of answers. This is infeasible in the context of Web services. Our goal, in contrast, is to compute the largest number of answers using the given budget of calls. Hence, we have to prioritize

calls that are likely to lead to an answer. This is different from the problem of join ordering in previous work. Therefore, we have to use a different model for the query answering process: our execution plans are ordered sequences of calls rather than ordered join plans.

OUR APPROACH TO QUERY ANSWERING

SMART FUNCTION CALLS. We will now make the notion of "guessing" formal. We aim to distinguish the guessing plan A smart function call in an execution plan is a function call whose inputs come from the query or from previous smart function calls, and whose consequences are a subset of the consequences of the following function calls.

Inverse functions can be used to answer query atoms that have an otherwise unsupported binding pattern. Yet, inverse functions are not always necessary. If, say, there is a function f that supports the desired binding pattern for a relation, then it is not necessary to add an inverse function for some other function g that does not support the desired binding pattern. However, in the context of Web services, the inverse of g would still be necessary in order to obtain as many results as possible. This is because Web services are typically incomplete. The function f may not yield all the instances that g stores. Thus, one potentially loses results if one queries only f. Even if f is complete, it can still be beneficial to have the inverse of g. This is because Web services typically come at a cost. This can be a cost in bandwidth, in time, or also in financial terms (for commercial Web services). It can be that the inverse of g is cheaper than f. In this case, the inverse of g can still be preferable to f. Now assume that there is an orchestration of functions that allows finding the input values for g, so that g delivers instances even for an unsupported binding pattern. Since Web services tend to be incomplete, this orchestration might still not find all input values of g. Thus, g might store more instances than can be obtained this way. Thus, the inverse of g is still necessary to maximize the number of results. In all of these cases, the inverse of g proves useful to have – be it to maximize the number of results or to minimize the cost of calls. Therefore, we aim to add as many inverse functions to our program as possible.

INFORMATION EXTRACTION

TEST SET. To evaluate the IE algorithms, we targeted three query types: Queries that ask for actors with a certain birth year, for actors with a certain nationality and for authors who received a certain prize. For each query type, we chose 10 arbitrary property values (10 birth years, 10 nationalities and 10 literature prizes). For each property value, we generated the keyword query that SUSIE would generate, sent it to Google and retrieved the top 10 pages. This gave us 100 pages for each test set. The pages are quite heterogeneous, containing lists, tables, repetitive structures and full-text listings of entities. We manually extracted the target entities from these pages to create a gold standard. Then, we ran the IE algorithms and measured their performance with respect to the gold standard.

The column "DB" is the naive algorithm of regarding all instances of the target type in the YAGO database as candidates. The precision and recall of the IE algorithms are nearly always in the range between 30% and 75%. Only the precision on the birth year queries is disappointing, with values below 10% (Figure 5). This is because the Google queries returned lists of all actors, not just of the ones born in a certain year. Thus, the algorithms find far too many irrelevant entities in the pages. The SMA, with its slightly higher recall, suffers particularly for the precision. We record this as a case where the information extraction approach is less practical, because the Internet does

not provide the lists of entities that the approach needs.

REAL-WORLD QUERIES

We integrated 40 functions exported by 7 Web service providers: isbndb.org, librarything.com, Amazon, AbeBooks, api.internetvideoarchive.com, musicbrainz.org, lastfm.com. We selected a variety of query templates, which can be organized in the following classes star queries with constants at the endpoints (Q1-Q2, Q7), star queries with variables and constants at the endpoints (Q3-Q4, Q8-Q10), and chain queries with constants at the endpoints (Q5-Q6, Q11). For every query template, we evaluate a set of similar queries by varying the constants. The queries were chosen such that they have different alternative ways of composing function instantiations. Usually, this leads to a high number of Web service calls.

Settings and algorithms. We distinguish two settings. In the first setting we try to answer the query using only Web services. We compare 3 different approaches. The first approach ("TD") uses a naive top-down evaluation of the queries without inverse functions. This approach implements a Prolog-style backtracking strategy. The second approach uses ANGIE for the query evaluation. ANGIE is a stateof-the-art system for top-down query evaluation with views with binding patterns. The third approach uses SUSIE, i.e.,the approach uses both Web services and inverse functions. We used the SEA algorithm for IE.

QUERY ANSWERING

Most related to our setting is the problem of answering queries using views with limited access patterns. The approach of rewrites the initial query into a set of queries to be executed over the given views. The authors show that for a conjunctive query over a global schema and a set of views over the same schema, determining whether there exists a conjunctive query plan over the views that is equivalent to the original query is NP-hard in the size of the query. This rewriting strategy assumes that the views are complete (i.e., contain all the tuples in their definition). This assumption is unrealistic in our setting with Web services, where sources may overlap or complement each other but are usually incomplete.

When sources are incomplete, one aims to find maximal contained rewritings of the initial query, in order to provide the maximal number of answers. present algorithms for rewriting a query into a Datalog program, requiring recursive Datalog even if the initial query is non-recursive. Subsequent studies proposed solutions for reducing the number of accesses. Notions of minimal rewritings have been proposed in. However, the goal remains the computation of maximal results. The guessing accesses are not eliminated nor do they have a special treatment since they relevant for this goal. The same problem was studied for different query languages: unions of conjunctive queries with negation, with additional function dependencies, or with integrity constraints. The Magic Set algorithm reduces the number of sub-queries in a bottom-up evaluation.

CONCLUSION AND FUTURE WORK

Most related to our setting is the problem of answering queries using views with limited access patterns. The approach of rewrites the initial query into a set of queries to be executed over the given views. The authors show that for a conjunctive query over a global schema and a set of views over the same schema, determining whether there exists a conjunctive query plan over the views that is equivalent to the original query is NP-hard in the size of the query. This rewriting strategy assumes that the views are complete (i.e., contain all the tuples in their definition). This assumption is unrealistic in our setting with Web services, where sources may overlap or complement each other but

are usually incomplete. When sources are incomplete, one aims to find maximal contained rewritings of the initial query, in order to provide the maximal number of answers. present algorithms for rewriting a query into a Datalog program, requiring recursive Datalog even if the initial query is non-recursive. Subsequent studies proposed solutions for reducing the number of accesses. Notions of minimal rewritings have been proposed in. However, the goal remains the computation of maximal results. The guessing accesses are not eliminated nor do they have a special treatment since they relevant for this goal. The same problem was studied for different query languages: unions of conjunctive queries with negation, with additional function dependencies, or with integrity constraints. The Magic Set algorithm reduces the number of sub-queries in a bottom-up evaluation.

REFERENCES

[1] F. M. Suchanek, G. Kasneci, and G. Weikum, "YAGO: A Core of Semantic Knowledge," in WWW, 2007.

[2] S. Auer, C. Bizer, G. Kobilarov, J. Lehmann, R. Cyganiak, and Z. Ives, "DBpedia: A nucleus for a Web of Open Data," Semantic Web, 2008.

[3] A. Rajaraman, Y. Sagiv, and J. D. Ullman, "Answering queries using templates with binding patterns," in PODS, 1995.

[4] C. Li and E. Y. Chang, "Query planning with limited source capabilities," in ICDE, 2000.

[5] C. Li, "Computing complete answers to queries in the presence of limited access patterns," VLDB J., 2003.

[6] S. Kambhampati, E. Lambrecht, U. Nambiar, Z. Nie, and G. Senthil, "Optimizing recursive information gathering plans in EMERAC," J. Intell. Inf. Syst., 2004.

[7] A. Cal`ı and D. Martinenghi, "Querying data under access limitations," in ICDE, 2008.

[8] A. Deutsch, B. Lud¨ascher, and A. Nash, "Rewriting queries using views with access patterns under integrity constraints," Theor. Comput. Sci., 2007.

[9] A. Nash and B. Lud¨ascher, "Processing unions of conjunctive queries with negation under limited access patterns," in EDBT, 2004.

[10] A. Cal`ı, D. Calvanese, and D. Martinenghi, "Dynamic query optimization under access limitations and dependencies," J. UCS, 2009.

An Algorithm for Implementing Security in Cloud

S.Anuja
Department of Computer Science and Engineering
s.anuja92@Gmail.com

Abstract— **Cloud Computing provides elastically provisioned computing, software, and service infrastructure. This elasticity allows users to outsource their computing infrastructure, growing or shrinking it as necessary. To make use of this Cloud Computing as a platform for security-sensitive applications like electronic transaction processing systems we incorporate trust based security. The electronic transaction processing system needs high quality of security to guarantee authentication, integrity, and confidentiality of information. In this paper we are introducing the factor trust level which is measured dynamically using differential equations for each host in the cloud. The providers which provide high security indulge high overhead which is not necessary for less security tasks, the trust level computed creates an opportunity to assign suitable host with less overhead .**

Index Terms — ***Cloud Computing, Direct Trust, Reputation, Trust Level.***

INTRODUCTION

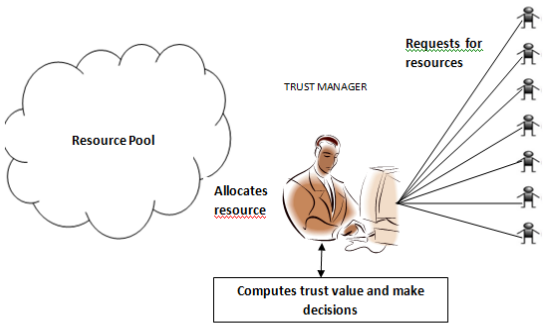
Cloud Computing is a recent technology containing a collection of computing resources present in distributed datacenters shared by several users and providing distributed services using the scalable and virtual resources over the internet. Cloud computing is a form of outsourcing. Servers in the cloud can be physical machines or virtual machines. It provides the utility services based on the pay-as-you go model. Cloud computing provides opportunity to make their serving economically optimistic. Now-a-days Electronic transaction-processing systems are widely used in banking, finance and electronic commerce take cloud as platform. The openness and computational flexibility of popular commercially available operating systems have been important factors to support the general adoption of cloud computing. In turn to successfully complete a transaction it needs support from a third party loyalty program and fraud detection analysis system, and exchanges and application complexities. A real time example is ATM withdrawal of a sum of money from a bank account. The transaction must be processed and the account balance updated holding the account to keep track of funds. These transactions should include some security services like Authentication, Confidentiality and Integrity. Applications such as e-transactions is now an important opportunity to extend the range and the productivity of existing and new companies. Security plays a major role in e-transactions. The basic security goals are confidentiality, integrity and authentication. We need a high level of security with the partnering cloud entities. In traditional way we rely on trust in network service providers, hardware vendors, software vendors, service providers, data sources etc. Now cloud provider will be just one more entity on that list. Authentication in a transaction setting means that both partners can prove to each other that they have the identity under which they have addressed each other. Very often the authentication process is a mutual authentication between two internet access devices with the assumption that the physical or legal persons using the corresponding computers have been authenticated beforehand. Integrity is the validity and the actuality of the exchanged data within a transaction context. Confidentiality is always necessary when valuable data are implied. This can be a credit card number but also data on a person's health condition or a trade secret of a company that have to remain confidential in between a restricted group.

RELATED WORK

Cloud can serve any number of users over the internet. With cloud computing, we can run all computer networks and programs as a whole without ever buying an extra piece of hardware or software. People and services or services providers are interacting with each other independently. A party might be authenticated and authorized, but this does not ensure that it exercises its authorizations in a way that is expected [4].The creation and protection of security certificates is usually not enough to ensure the necessary security levels in the cloud. Cryptographic algorithms used with cloud applications usually reduce performance and such reduction must be restricted to acceptable levels [6]. Therefore it is important that customers be able to identify trustworthy services or service providers. Trust is the main concern of consumers and service providers in a cloud computing environment[7].

SYSTEM ARCHITECTURE

Our Proposed System architecture is shown below:



Proposed System Architecture

There may be any number of users in the cloud environment. The users may demand for different services from the resource pool in cloud. The user will request the service along with its security needs to the trust manager. The proposed trust level computation is done by the trust manger in order to make the decision for providing the service to be executed in a requested security level environment.

SECURITY AND TRUST REQUIREMENTS

Good security model should be accurate, adaptive, multi-dimensional and efficient. Trust model allows identifying trusty agents and isolating untrusted agents. It specifies whether and with whom to communicate. Service providers and requestors evaluate each other after transactions. Each user has a "reputation" (feedback score) that is the summation of the numerical evaluations. Nevertheless, the factors openness and flexibility of cloud computing increase system complexity, reduce the degree of trust and introduce holes that become threats to security [7]. Marsh [9] provided a clarification of trust concepts, presented an implementable formalism for trust, and applied a trust model to a distributed artificial intelligence (DAI) system in order to enable agents to make trust-based decisions. In [10] a trusted cloud computing platform (TCCP) which enables providers to offer a closed box execution environment that guarantees confidential execution. This system allows a customer to verify whether its computation will run securely, before requesting the service to launch a VM. TCCP assumes that there is a trusted coordinator hosted in a trustworthy external entity. The TCCP guarantees the confidentiality and the integrity of a user's VM. We propose a trust model where the selection and trust value evaluation that determines whether a node is trustworthy and can be performed based on node storage space, operating system, link and processing capacity. In this paper all the trust value computations are done by a coordinator module called *trust manager*. We will consider the following trust definitions [1]:

Definition 1: Trust is a firm belief in the competence of a node to act as expected. In addition, this belief is not a fixed value associated with the node but rather it is subject to the user's behavior and can be applied only within a specific context at a given time.

Definition 2: The reputation of a user is the expectation of its behavior based on other nodes' observations or on the collected information about the user's past behavior within a specific context at a given time.

4.1 System Trust level

A trustworthiness of the service provider node is something where we can place our trust and rest assured that the trust shall not be betrayed. The trustworthiness($TL^{k}_{j,id}$) at a given time t for security service *k* between the service provider host node p_j and the service requester *id* is computed based on the direct relationship at time t as well as the reputation of user id at time t .

The trust is built on past experiences given for a specific context. We build a direct trust differential equation that is derived from the brand image [2], [3] in economics. The direct relationship at time *t* between service provider node p_j and service requester *id* is denoted as $H(j,id,k,t)$. The direct trust relationship depends on the cloud entity and user's direct interaction, changes in their environment changing , and the rate of decay as the time going on.

The direct trust can be computed as:

$$H(j,id,k,t) = \frac{dH}{dt}$$

$$\frac{dH}{dt} = \xi D(j,id,k,t) + \varphi E(j,id,k,t), -\rho H(j,id,k,t)$$

$$H(j,id,k,0) = H_0(j,id,k).$$

The parameters ρ, ξ and φ are positive, although we shall consider $\xi = 0$, $\varphi = 0$ as a limited case and ρ presents the decay rate.

The reputation is built based on the brand image trust function of user and the trust recommendations by other service provider hosts.

The reputation can be expressed as a following differential equation:

$$G(id,k,t) = \frac{dG}{dt}$$

$$\frac{dG}{dt} = \mu A(id,k,t) + v \sum_{j \varepsilon (al \ln odes)} P(j,id,t) - \delta(id,k,t),$$

$$G(id,k,0) = G_0(id,k).$$

The k^{th} trustworthiness at a given time t between the cloud service provider and the user is calculated based on the following equation:

$$TL^{k}_{j,id} = \varepsilon_j \times H(j,id,k,t) + \beta_j \times G(id,k,t) k \in (a,g,d)$$

where *a, g ,d* denote the security services like authentication, integrity and confidentiality respectively. Let the weights given to direct trust and reputation relationships be ε and β respectively. If the trustworthiness is based more on the direct trust relationship with p_j for *id* than the reputation of id, then β will be lesser and ε will be larger. Some large web application system, such as Amazon.com, eBay, All Experts provide evaluation mechanisms for the reputation of subjects and objects. For objects, reputation is the evaluation of their capability, estimating intention, and capability of meeting subjects services demands, also called objects' service satiability[5].

$$\varepsilon_j + \beta_j = 1 \quad \varepsilon_j \geq 0 \quad \beta_j \geq 0$$

V SECURITY DRIVEN SCHEDULING ALGORITHM:

- Compute the *SRank* for all tasks by traversing graph from the *exit* task
- Sort the tasks into a scheduling list by non-increasing order of *Srank*
- While *the scheduling list is not empty* do
  - Remove the first task t_i from the scheduling list
  - For each node p_j ε P do
  - Compute $EFT(t_i,p_j)$ using the equations
  - Compute $Pr(t_i,p_j)$ using the equation
- End
- Search the node set P' with $Pr(t_i,p_j)<\theta$
- Assign task t_i to the node p_j ε P' that minimize EFT of t_i.
- End

V.,EXPERIMENTAL RESULTS

The goal of the experiment is to identify the trustworthiness of the cloud entities for certain requester and their job. The implementation of this work is done by using a toolkit called C*loudSim.* To stress the evaluation, we assume that each task arriving at system requires all of the three security services. Consider a system with three service providing cloud entities and two user . The trust calculated for authentication is given as:

	USER1	USER2
Host1	0.200000	0.090000
Host2	42.000000	0.390000
Host3	0.050000	0.090000

Trust Level for Authentication

The values for same providers and requestors for integrity and confidentiality are given as:

	USER1	USER2
Host1	0.110000	0.440000
Host2	0.380000	0.440000
Host3	0.420000	0.560000

Trust Level for Integrity

	USER1	USER2
Host1	0.280000	0.170000
Host2	0.280000	0.170000
Host3	0.010000	0.030000

Trust Level for Confidentiality

Thus user1 identifies that provider with id 0 is good in providing authentication service and integrity service whereas the provider with id 2 is good in providing confidentiality.

VII.CONCLUSIONS AND FUTURE WORK

In this work , we attempt to incorporate the security awareness into tasks in cloud. We consider that it is mandatory to design and implement the security requirements of task along with the trust level for achieving good performances. Without Trust level in the security model , the following two problems may occur. First, security-sensitive applications will run at a lower security levels, thereby leading to low quality of security. Second, security-sensitive applications will be at a higher security levels with higher security overheads, which can result in poor performance. Future studies in this domain will be interesting to extend our trust level in security with security overhead models to multidimensional computing resources, such as network bandwidth, memory, and storage. The values computed here are used in scheduling for choosing appropriate provider host based on requester's QOS requirements in terms of security. The Security can be further improved by using the Berger Model.

ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression, "One of us (R. B. G.) thanks . . ." Instead, try "R. B. G. thanks". Put applicable sponsor acknowledgments

here; DO NOT place them on the first page of your paper or as a footnote.

REFERENCES

References:

[1] Xiaoyong Tang, Kenli Li, Zeng Zeng, and Bharadwaj Veeravalli ”A Novel Security-Driven Scheduling Algorithm for Precedence-Constrained Tasks in Heterogeneous Distributed systems”, IEEE TRANSACTIONS ON COMPUTERS, VOL. 60, NO. 7, JULY 2011.

[2] S. Jorgensen, S. Taboubi, and G. Zaccour, “Retail Promotions with Negative Brand Image Effects: Is Cooperation Possible?” European
J. Operational Research, vol. 150, no. 2, pp. 395-405, 2003.

[3] A.E. Cretu and R.J. Brodie, “The Influence of Brand Image and Company Reputation Where Manufacturers Market to Small Firms: A Customer Value Perspective,” Industrial Marketing Management, vol. 36, no. 2, pp. 230-240, 2007.

[4] B. Yu and M. P. Singh, “An evidential model of distributed reputation management,” International Conference on Autonomous Agents, Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1, pp. 294-301, 2002.

[5] Shouxin Wang, Li Zhang, Na Ma, Shuai Wang “An Evaluation Approach of Subjective Trust Based on Cloud Model” Software Engineering Institute Beihang University Beijing, China; accepted November 27th, 2008.

[6] H. Takabi, J. B. D. Joshi, and G. Ahn, “Security and Privacy Challenges in Cloud Computing Environments,” IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, Nov./Dec. 2010, doi:10.1109/MSP.2010.186. International Journal of Computer Science & Information Technology (IJCSIT) Vol 4, No 1, Feb 2012

[7] Zhidong Shen, Li Li, Fei Yan, and Xiaoping Wu, “Cloud Computing System Based on Trusted Computing Platform,” Intelligent Computation Technology and Automation (ICICTA), IEEE International Conference on Volume: 1, pp. 942-945. China. 2010.

[8] Zhidong Shen, Li Li, Fei Yan, and Xiaoping Wu, “Cloud Computing System Based on TrustedComputing Platform,”Intelligent Computation Technology and Automation (ICICTA),IEEE International Conference on Volume: 1, pp. 942-945. China. 2010.

[9] S. P. Marsh, “Formalising Trust as a Computational Concept”, Ph.D. Thesis, University of Stirling, 1994.

[10] N. Santos, K. Gummadi, and R. Rodrigues, “Towards Trusted Cloud Computing,” Proc.
HotCloud. June 2009.

A NEW SEARCH ENGINE FOR WEB ONTOLOGIES USING FALCONS CONCPET

Vinothini.S
First Year ME student,Computer Science And Engineering
Renganayagi varatharaj College Of Engineering
Vnsuriya5@gmail.com[3]

ABSTRACT

This project is developed about a new search engine for web ontologies using Falcons concept. It is a novel keyword based ontology search engine. The web ontologies providing concepts for domain entities and enabling semantic interoperability between applications..This proposed model helps users quickly to find their needs by using two way search. The two way searches are Object Search and Concept Search. The keywords are displayed using rank concept by popularity based scheme. This search engine also construct a virtual documents of concepts for keyword. User feedback and the usability evaluation is also reported.

INTRODUCTION:

The semantic web is used to retrieve data from the web applications. This semantic web uses the Resource Description Framework(RDF). This RDF represents a triple/graph based way for the data. The semantic interoperability depends on reusing or extending existing ontologies. By this, this ontology search is used for applications developers. There are several ontology search engines accept keyword queries and they returned matched concepts.

The returned results provide the human readable name of each concept or ontology. This cannot help users easy to find whether a concept or ontology is returned. This returned results also does not satisfy their needs. For example in the Swoogle search engine we ca give any type of queries. That returned only the xml format for the query given by the user. That returned only the XML format for the query given by the user. That XML format does not understand by the users.

For that we developed a new search engine using Falcons Concept Search. It is a novel keyword-based search engine. By using Falcons the newly developed search engine retrieves the textual description. It is matched with the keyword query given and the retrieved data is based on the rank concepts and popularity based concepts. This popularity is measured from the semantic web containing large data set. There are two types of searches in the search engine. One is the Object search and the another is Concept search. In the object search we can search the individual objects with their shape and the concept search it relates two or more objects. It is used to find users quickly understand their needs.

SYSTEM DEMONSTRATION:

In this search engine first the user have to login. For login they have to register. The register page ask some details about the users. After that the users are able to login. The Concept search is available after logged. In this the queries are given. For example the query java is given means it displays some of the links. The first link is about some of the details about the java. That are displayed based on the popularity scheme. That link is connected to the Google. Then there are some other links which displays the date they are modified. And the type of data also mentioned. The type of data includes XML or HTML format. The concept search relates two or more objects. In the home page itself there is another type of search called Object Search. That search takes each character as the object and displays some information. The user also determines to reuse the ontology. The user can also select other ontologies.

SYSTEM ARCHITECTURE:

The crawler downloads the RDF documents in the URI repository and these are parsed by jena parsing. This crawler generate a keyword index for website. Jena parsing padocuments and then given to URI repository. The quadruple store is implemented on MYSQL database. Meta analysis computes several kinds of global information and updates to the metadata. The indexer serves the proposed mode of user interaction (ie) keyword search with ontology restriction. Browsing concepts loads RDF description from quadruple store. The Browsing ontologies loads ontology metadata from quadruple store and then loads list of classes and properties contained in metadata.

The RDF document and the URI from a quadruple are stored in the quadruple store based on the MySQL database. The metadata analysis computes several kinds of global information and updated to the metadata database.

The indexer also updates the combined inverted index that serves the proposed mode of user interaction. This index consists of two inverted indexes based on Apache Lucene. A virtual document is constructed first for each concept returned. From the virtual documents a classical information retrieval data structure is created. An inverted index are built from the ontologies based on the metadata database then they serve as ontology-based result filtering. Ranking process is based on Lucene. A popularity score is attached to each concept at the indexing time. Term based similarity and the popularity of concepts and the keyword query are combined to the rank concepts at the searching time.

A query relevant structured snippet is generated for each concept returned. Most of the ontologies are recommended based on the top-ranking concepts. The browsing concepts loads the RDF description from the quadruple store for each concept requested and they present to the user. The browsing ontology loads the ontology from the quadruple store and the list of classes and properties are displayed to the user.

CONSTRUCTING VIRTUAL DOCUMENTS

The most traditional web search engines build an URI to the keyword the user search. But on the semantic web there is no such type of building search, it is described by the RDF triples. For example a concept with a creating information, the literal valued property or a entity-valued property are used. The literal valued property attach the name of the creater and the entity-valued property relate the URI to the creator. Considering those two property entity-valued property is best.

For connecting concepts with blank nodes the OWL ontology are used. This have concepts but they don't have any local names. First have to identify the description graph which is a subset of all RDF triples. The operation can be done by including all RDF triples having blank node object and the blank node which have not been included in the subset is included.

RANKING

The ranking can be done in concept ranking and the ontology recommendation. In the concept ranking the ranking score for a concept has two factors. They are keyword query q and its popularity.

Ranking
Score(c,q)=TextSim(c,q).Popularity(c)

which can be discussed by the following

(a)Query Relevance:

The vector space model is used in the query relevance (ie) The documents are represented as a vector and the components are related to the frequency in the documents. The weights of the term are extracted by the local name and the label for the concept. If the term are occur in very few documents the data set is considered as distinction feature. For a virtual document a higher weight is assigned. TextSim(c,q) is described by the cosine angle of the virtual document of vector c and the vector form q.

(b)Popularity

For a concept c, the set of RDF documents are initialized. A concept c in RDF document d contains the RDF triple and the predicate c. The score for popularity can be calculated by

popularity(c)=log(|Docs(c)|+1)+1

The another method for ranking is ontology recommendation. For every query the concepts are returned. The ranking score is calculated by adding the ranking score for each concept returned and their ontology. The nine top-ranking ontologies are verified. These popular keyword are matched with the semantic web.

GENERATING SNIPPETS

For every concept returned it provides a query-relevant snippets, that show how the concepts are matched with keyword. The snippets are help the users to easily determine their needs. The two methods of producing snippets are there. They are PD-Thread and the Generating snippets by Ranking PD-Threads.

In the PD-Threads the basic unit of snippet are in small size but they give full meaningful. The PD-Thread is the basic unit. For the description of concept c, c is the path in a description graph. For this c is the starting node and the blank node may not be an ending node.

In the second method of generating snippets by ranking PD-Threads, the ranking algorithm is used. The first step is to assign a ranking score to PD-Thread candidate. Second step is to select the top-ranking candidate by snippet. The number of PD threads has obtained three then go the step 1.

CONCLUSION

In this paper the new search engine using Falcons Concept was easily make the user to the satisfy their needs. This includes the concept-level search and the object-level search. The snippets generated for each concept returned make the users to determine their needs. Based on the both returning of concepts the structured snippets we can easily compare ontologies. User interaction is easily for search engine. The improved method of generating snippets is better present to ontology structured. It also make interesting for ontology evaluation and recommendation.

REFERENCES:

[1] L. Ding, T. Finin, A. Joshi, Y. Peng, R. Pan, and P. Kolari,"Search on the semantic web," IEEE Comput., vol.38,no. 10,pp.62-69, Oct. 2005.

[2] M. d'Aquin, C. Baldassarre, L .Gridinoc, M. Sabou, S. Angeletou, and E. Motta, "Watson: Supporting next generation semantic web applications," in Proc.IADIS Int. Conf. WWW/Internet,2007,pp.363-371.

[3] C. Anutariya, R. Ungrangsi, and V. Wuwongse, "SQORE: A framework for semantic query based ontology retrieval," in Proc. 12th Int. Conf. Database Syst. Adv. Appl.,2007,pp.924-929.

[4] C. Watters, "Information retrieval and the virtual document," J. Amer.Soc.Inf.Sci.,vol.50,no.11,pp.1028-1029, Aug. 1999.

[5] Nokia, P.Stickler,CBD--Concise BoundedcDescription. [online]. Available:http://sw.nokia.com/uriqa/CBD.html

[6] Y. Qu, W. Hu, and G. Cheng, "Constructing virtual documents for ontology matching," in Proc.15th Int. World Wide Web Conf.,2006, pp.23-31.

[7] X.Zhang, H. Li, and Y. Qu,"Finding important vocabulary within ontogy," in Proc. 1st Asian Semant. Web Conf.,2006,pp.106-112.

[8] G.Wu, J.Li, L.Feng, and K. Wang, "Identifying potentially important concepts and relations in an ontology," in Proc. 7th Int. Semantic. Web Conf., 2008,pp.33-49.

[9] H. Alani and C. Brewster,"Metrics for ranking ontologies," in Proc.4th Int. EON Workshop,2006,pp. 1-7.

[10] X.Zhang, G.Cheng, and Y. Qu,"Ontogy summarization based on the RDF sentence graph" in Proc. 16th Int. World Wide Web Conf., 2007,pp.707-716.

[11] L.Ding, T.Finin, Y.Peng, A.Joshi, P.P. da Silva, and D.L. McGuinness, "Tracking RDF graph provenance using RDF molecules," in Proc.4th Int. Semant.Web Conf.(Poster),2005,pp.1-4.

[12] G. Tummarello, C. Morbidoni, R. Bachmann-Gmir, and O. Erling,"RDF-sync:Efficient remote synchronization of RDF molecules," in Proc. 6th Int. Semant. Web Conf. 2nd Asian Semant. Web Conf., 2007, pp.537-551.

[13] A. Nenkova, L. Vanderwende, and K. McKeown, "A compositional context sensitive

multi-document summarizer: Exploring the factors that influence summarization," in Proc.29th Annu. Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval,2006,pp. 573-580.
[14] J. Brooke. "SUS--A quick and dirty usability scale," in Usability Evaluation in Industry, P.W. Jordan, B. Thomas, I.L.McClelland, and B. Weerdmeester,Eds. Boca Raton, FL:CRC Press,1996,pp.189--194.
[15] J.Z.Pan, E.Thomas and D.Sleeman,"ONTOSEARCH2:Searching and querying web ontologies," in Proc.IADIS Int. Conf.WWW/Internet,2006,pp.211-219.

QOE Enhanced Social Live Interactive Streaming

J.Ramya @ Komathi[1], Dr.D.Venkata Subramanian [2], Dr.R.Nedunchellian[3]
Dept. Computer Science & Engineering, Saveetha School of Engineering,
Saveetha University, Chennai, India.
ramya.spj@gmail.com[1]

Abstract

Globalized live streaming services have got subscribers all around the world. The rapid emergence of the mobile devices has made it a natural aspiration of such users to make social interaction with others who have got involved in the same application. The term Social TV implies the integrated support of the television and the computer technology in order to provide a group viewing experience to the users. The social interactions within the users who use such live streaming service needs to be spontaneous. The cloud computing technology has triggered enormous opportunities to facilitate the mobile live streaming of the multimedia contents with an extended support to interact with the users. The quality of service (QOS), storage and sharing are some of the issues that have to be addressed in order to provide a mobile social television in a cloud environment. The cloud technology effectively handles some of these issues by assigning proxies for the mobile users. These proxies (surrogates) for the users, operates on the base of transcoding mechanism. Also the PAAS and IAAS cloud services are keys in providing such an effective interaction based live streaming.

Keywords— Mobile Social TV, Live Streaming, Quality Of Service, Social Interactions, Cloud Computing

I. INTRODUCTION

Social TV started in the early 2000s with limited success as the creation of the shared connections was cumbersome with a remote control and the User Interface (UI) design made the interaction disruptive to the TV experience. But social networking has made Social TV suddenly feasible, since it already encourages constant connection between members of the network and the creation of likely minded groups. The shared content and activities often relate to TV content. At the same time, the smart phone market has been growing quickly. Mobile TV is the technology providing multimedia contents to the user by wireless communication. As our society is becoming increasingly mobile, there is an emerging need for content and services to become mobile as well. Within the scope of our research, we define Mobile TV as real-time transmission of traditional TV content to mobile handsets.

Mobile TV promises thrilling benefits to consumers and increased revenues for mobile telecommunications' operators, equipment suppliers and television providers. The mobile TV device should produce an image quality which is not significantly inferior to the standard established by traditional TV, even if the screen size is much smaller. The network coverage and the signal strength should be sufficiently good to give the viewer an uninterrupted service of comparable quality with traditional TV. As most mobile TV networks still are not much less

than prototypes there is still some way to go before the transmission quality is sufficiently good.

This paper proceeds as follows: Section 2 introduces the theoretical foundation of this study. Section 3 outlines the key terms and technologies. Section 4 focuses on architectural model; Finally Section 5 summarizes the results of study.

II. RELATED WORKS

Media Cloud is a general idea of integrating the multimedia services with the cloud technologies, which enables the user to access the multimedia content through the cloud computing technology. Providing multimedia service though the cloud technology faces the scalablity,Qos and heterogeneity challenges[4] .However the Content Delivery Network (CDN) and the peer to peer multimedia computing have been worked out to alleviate the problems in multimedia computing by pushing the multimedia content to the edges and to the peers respectively [4].Rings et al has proposed the idea of integrating the cloud computing with the multimedia services without the Qos provisioning. Whereas Zhu et al proposed the multimedia cloud computing which provides Qos provisioning. The working of the cloud services for the multimedia content can be differentiated and explained mainly by two ways, they are: multimedia-aware cloud and cloud aware multimedia. Here the former idea pertains to the quality of service(QOS) services for multimedia content and the later concept deals about how well the sharing, retrieval and storage of the multimedia content can utilize the cloud-computing resources for achieving a better Quality Of experience (QOE).[2] More finer framework like as Cloud Assisted Live Media Streaming have been studied to utilize the cloud resources by leasing and adjusting the cloud servers for the dynamic user demands[15].Basically the video streaming using the cloud technology relies on the transcoding mechanism, which has two mapping options like Hallsh-based and Lateness-first Mapping for reducing the jitter in the transcoding [7]. Also the Scalable Video Coding framework has also been proposed to reduce the latencies in the transcoding and to adapt to the dynamically changing network conditions [3].The work of Satyanarayanan et al. [13] have suggested the implementation of the dynamic virtual machine in carrying out the offloading to the mobile devices computations. The work of the proxy servers in the cloud technology for the multimedia or video streaming service has effectively handled the issue of the storage, processing challenges faced by some mobile devices in accessing those services [1] have seen the idea of interactive live streaming through the cloud computing technology, which provides a co-viewing experience to the users with their friends in different geographic locations. Thereby making the activity more social able. The experiments by Oehllberg et al. [6] on the social activities of a human while viewing different video contents have been inspiring but still those frameworks cannot be applied in to the mobile environments directly. The design proposed by the Coppens et al. [4] have been intended to elaborate the social interactions but it got constrained with the broadcast program channels. Reflex [7] is a mechanism to enhance spontaneity in the interaction between the users, which makes use of the Google App Engine to achieve more scalable and quality service in the social network, taking the large amount users into consideration. These interactions can be handled by the messenger service through the cloud computing technology. The video streaming through the help of cloud computing technology has been facing another significant challenge as studied by [2] ,which is the Quality of experience [2] have already proposed the idea of enhancing the quality of experience in

viewing the live video content by introducing the features like zooming, segmentation and panning but have not extended to the interactive streaming environment. Here we are proposing a framework for enriching the quality of experience to the users in a interactive live streaming, with the cloud computing as its backbone.

III.CLOUD-BASED INTERACTIVE STREAMING

The live video streaming has took a whole new dimension with the evolution of cloud computing technology. In the case of live video streaming, the cloud computing extends its support for interaction within the users and for a better quality of experience. The architecture workflow has been given as below in figure. The proxy servers or surrogates are assigned to each user who gets logged in to the cloud. These servers are provided by the Infrastructure as a service cloud. The surrogates will efficiently provide the offloading, it will be enacting as a middleware between the mobile devices and the video sources. It will be encapsulating the transcoding, segmentation and content adaptation operations. In addition to these operations the messenger, will also be handled by these surrogates, which is a key component in delivering effective interaction between the users.
The quality of experience for the users can be enhanced by the features like segmentation, zooming and content adaptations. The extensible messaging and presence protocol (XMPP), here plays a significant role in operating the transportation of the video segments and it is helpful in exchanging the metadata of these video streams like title, description.

A.Transcoding

The surrogates assigned to the users, will be handling the trancoder, which decide the encoding format for the video stream dynamically. The bit rate and the dimension of the video stream will also be decided in this module. Since MPEG-4 has been the de-facto standard for the video delivery over loosy medium, this stream will be generally followed for the implementation. FFmpeg library is fundamentally utilized by this service for generating the thumbnails.
The transcoding frameworks split the video contents into overlapping and non-overlapping group of pictures (GOP). These pictures may encircle different encoding qualities and resolutions, forming several layers. Such layers will be sliced as coding-independent content. Here 16x16 macro-blocks are framed for luma components and 8x8 MB is framed for chroma components. The granularity is decided with the parallelism in GOP level and MBs, which is divided into inter-parallelism and intra-parallelism. The simple diagrammatic illustration in the fig of the transcoding framework is given below will give a better understanding of the idea elaborated above.

(i) Inter-node Parallelism: The Inter-node parallelism manages the reduced picture nodes. The real-time transcoding is achieved through this inter-node parallelism; the transcoding jitter is an effect of the variations in the time delay of the encoding of the GOP (Group of Pictures). The encoding time is mainly estimated for the optimization problem.

(ii) Intra-node Parallelism: The Intra-node parallelism manages the individual slice of the picture node. The Intra-node parallelism is very significant in the GOP encoding and it is vital

in fixing the upper bound on the average computation time spent on the GOP encoding. Moreover this parallelism is not simply enough in reducing the access time

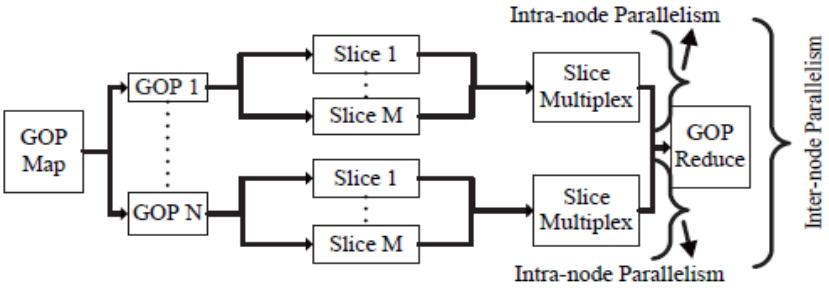


Fig.1 Transcoding Framework

B. Segmentation

The segmentation, is a feature to enhance the streamed videos, here this feature will create the list of points of scenes by identifying the scenes in the video. And by making use of the transcoding service the thumbnails for such segments will be created. Basically this feature is based on the OpenCV algorithms.

C. Zooming

This service will enable the users to zoom into the middle of the video stream. This will also be responsible in cropping of the streamed videos. This service fundamentally follows the object recognition service, which necessary in recognizing the objects in the video. The object recognizing service can enable to perform more complex zooming functionalities.

D. Messenger

This service is responsible in delivering the asynchronous message to the user from the surrogates. User will make queries periodically to the social cloud through this service, which is in connection with the social cloud. This service is also responsible in processing the plain text data, which are in xml format.

E. Gateway

The authentication of the users logged in are checked by this service, which also handles the logged in user list and maintains it in a separate database. The gateway is also responsible in reserving and destroying the surrogates based on the current work load.

F. Social Cloud Service

The social cloud service will be maintaining the data stores like Big-Table in Google App Engine, for storing all the details regarding the user records, sessions and messages. A data

store interface is used to query and manipulate the Big-table which indeed a multi-dimensional maps, stores data object as an entity entitled with multiple properties. For the video streaming it fundamentally follows the RTP protocol. The XMPP handles the metadata of the video segments. The social cloud is basically extended by the PaaS services.

G. Synchronizer

The synchronizer features the property of enabling the user to view the concerned video content in the same window as the other user in same session. This is achieved by retrieving current playback position and guides the user to adjust to that position. This is particularly concerned in providing the co-viewing experience to the users.

IV PERFORMANCE METRICS

In this proposed framework there are certain factors which affect its performance, where are here discussing some of the possible factors and the predicted performance improvements by this framework

A. Transcoding Latency

The Transcoding latency can make an impact on the entire framework if had not handled carefully. Even with the modern day's multi core processors the process of encoding is highly complex in nature. The transcoding delay can cause the delay in the access of video content for the user and it could cause even the freezing of the particular video content.

B. Power Consumption

The power consumption of the device, used for the access is significantly important, since that might well have a prime role in the working of this proposed framework in a considerable margin. The playback segment size of 10, which has been widely followed in streaming applications, was proposed by the Http Live Streaming protocol. However this segment has found to have drained the battery life significantly. Normally the power consumption factor is profiled by an Xcode tool called "Instruments".

C. Interaction Spontaneity

In this proposed framework the spontaneity of the interaction between the connected users is measured by two levels of factors. The first is the latency in the sending of the message to the surrogates and the confirmation for the message being registered in the cloud. The other is the latency in query sent by the user to reach the assigned surrogates. Also the round-trip time between the surrogates and the GAE, which also need to be taken into consideration for calculating the interaction latency in this framework.

V IMPROVEMENTS PREDICTED WITH THE FRAMEWORK

A. Battery Efficiency

To eliminate battery usage of the mobile devices this proposed architecture is aimed at providing an efficient burst transmission technique, which enables the mobile devices to operate on three states as High, Low and Intermediate. This technique fundamentally follows the Http Live streaming protocol, by which the video will be segmented by the surrogates and sent to the mobile devices on request. The mobile devices will be operating in High state when receiving the video segments and will be in Low state when remaining idle. The Intermediate state act as the transition state between these two states.

B. User Experience

Another important key aspect of this framework is the enhancement of the user experience by the features like zooming in and out the streamed video and the Scene by scene segmentation of the video stream. This enhancement is particularly achieved with the help of the XMPP protocol and RTP protocol which handles the video streaming, exchange of the metadata and video segments information. Here the metadata handler will be responsible in fetching the video segments and Playlist handler will be responsible in providing the preview thumbnails of the videos. The thumbnails, having a smaller resolution will get loaded very fast. The object recognition service is a key part in providing the zooming feature on the streamed videos.

C. Spontaneous Interactivity

Interaction is a key aspect of a social live streaming framework and this aspect is effectively handled in this proposed architecture by the means of the Messenger service, which being operated in a asynchronous way will provide spontaneous interactions between the connected users. A Big-table like data store will be made use to handle these data.

D. Scalability

As this proposed framework takes the implementation phase, a challenge will be the ability of this entire system to handle the large amount users who gets too logged into the service (i.e.) the scalability measure of this framework. Being deployed on to the cloud network, it should effectively handle this problem as well but still this area has to be addressed in the future works.

REMARKS AND FUTURE WORKS

Our work has concerned primarily in suggesting a framework integrating the social interactive live streaming with the Quality enhanced user experience. The enhancement in the QoE of the user obviously shows great scope in the further feature enhancement with the streamed video contents, like as recording the live video contents to the device, noise removal and so on. On the other side the interactive aspect of the framework has several areas to be more deeply addressed like applying memcache support and more efficient transcoding mechanism.

CONCLUSION

We conclude by proposing a framework for enriching the quality of experience to the users in an interactive live streaming, with the cloud computing as its backbone. And mobile users can import a live or on-demand video to watch from any video streaming site, invite their friends to watch the video concurrently, and chat with their friends while enjoying the video.

REFERENCE

[1] Yu Wu, Zhizhong Zhang, Chuan Wu, Zongpeng Li, Francis C.M. Lau:"Cloud MoV: Cloud-based Mobile Social TV", IEEE 2013.

[2] DejanKovachev, Yiwei Cao and Ralf Klamma,"Cloud Services for Improved User Experience in Sharing Mobile Videos", IEEE 2012.

[3] Zixia Huang, Chao Mei, Li Erran Li, Thomas Woo, "Cloud Stream delivering high-quality streaming videos through a cloud-based SVC proxy".

[4] Wen Hui1, Chuang Lin and Yang, "Media -Cloud: A New Paradigm of Multimedia Computing", KSII: Transaction on Internet and Information Systems, Vol.6, April 2012.
[5] Ramesh.B, Savitha.N, Manjunath.A.E,"Mobile Application in Multimedia Cloud Computing", Int.J.Computer Technology and Application, Vol 4(1), 97-103.Feb, 2013.

[6] Nicolas Ducheneaut, Robert.J.Moore1,Lora Oehlberg, James.D.Thornton,EricNickell,"SocialTV: Designing for Distributed, Sociable Television Viewing".

[7] Zimu Liu, Yuan Feng, Baochun Li,"Socialize Spontaneously with Mobile Applications",IEEE'12, INFOCOM proceedings.

[8] Hassnaa Moustafa and Nicolas Maréchal, Sherali Zeadally, "Mobile Multimedia Applications: Delivery Technologies", IEEE, CS(September/October 2012).

[9] H. Schwarz, D. Marpe, and T. Wiegand, "Overview of the scalable video coding extension of the H.264 AVC standard," IEEE Transaction on Circuits and Systems for Video Technology, vol. 17, no. 9, pp. 1103–1120, Sep. 2007.

[10] Z. Huang, C. Mei, L. E. Li, and T. Woo, "Cloud Stream: Delivering High-Quality Streaming Videos through a Cloud-Based SVC Proxy," in IEEE INFOCOM, 2011.

[11] Y. Wu, C. Wu, B. Li, X. Qiu, and F. C. Lau, "Cloud Media: When Cloud on Demand Meets Video on Demand," in IEEE ICDCS, 2011.

[12] Z. Wu, C. Zhang, Y. Ji, and H. Wang. Towards Cloud and Terminal Collaborative Mobile Social Network Service. 2010 IEEE International Conference

[13] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for vm-based cloudlets in mobile computing," IEEE Pervasive Computing, vol. 8, pp. 14–23, 2009.

[14] A.Carroll and G.Heiser, "An analysis of power consumption in as Smartphone," in Proc. of USENIXATC, 2010.

[15] Feng Wang, Jiangchuan Liu, and Minghua Chen, CALMS: Cloud-Assisted Live Media Streaming Globalized Demands with Time/Region Diversities".
[16] R. Schatz and S. Egger, "Social Interaction Features for Mobile TV Services, "in Proc. of 2008 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, 2008.

[17] H. Knoche, M. Papaleo, M. A. Sasse, and A. Vanelli-Coralli, "The Kindest Cut: Enhancing the User Experience of Mobile TV Through Adequate Zooming," in Proceedings of the 15th International Conference on Multimedia, ser. MULTIMEDIA '07. ACM, 2007, pp. 87–96

[18] R. Pereira, M. Azambuja, K. Breitman, and M. Endler, "An Architecture for Distributed High Performance Video Processing in the Cloud," in Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, 2010, pp. 482–489.

Decentralized Self-Adaptation Mechanism For Service Selection and Allocation Scheme in Cloud

E.Nisha M.E.,
SCAD Engineering College, Cheranmahadevi
Email id: nishaesakki17@gmail.com

Abstract—By leveraging virtual machine (VM) technology which provides performance and fault isolation, Cloud resources can be provisioned on demand in a fine-grained, multiplexed manner rather than in monolithic pieces. By integrating volunteer computing into Cloud architectures, we envision a gigantic Self-Organizing Cloud (SOC) being formed to reap the huge potential of untapped commodity computing power over the Internet. Towards this new architecture where each participant may autonomously act as both resource consumer and provider, we propose a fully distributed, VM-multiplexing resource allocation scheme to manage decentralized resources. Our approach not only achieves maximized resource utilization using the proportional share model (PSM), but also delivers provably and adaptively optimal execution efficiency. We also design a novel multi-attribute range query protocol for locating qualified nodes. Contrary to existing solutions which often generate bulky messages per request, our protocol produces only one lightweight query message per task on the Content Addressable Network (CAN). It works effectively to find for each task its qualified resources under a randomized policy that mitigates the contention among requesters.We show the SOC with our optimized algorithms can make an improvement by 15%-60% in system throughput than a P2P Grid model. Our solution also exhibits fairly high adaptability in a dynamic node-churning environment.

Index Terms—Cloud Computing, VM-multiplexing Resource Allocation, Convex Optimization, P2P Multi-attribute Range-query

1 INTRODUCTION

Cloud computing has emerged as a compelling paradigm for deploying distributed services. Resource allocation problem in Cloud systems emphasizes how to harness the multi-attribute resources by multiplexing operating systems. With virtual machine (VM) technology [1], we are able to multiplex several operating systems on the same hardware and allow task execution over its VM substrates without performance interference. Fine-grained resource sharing can be achieved as each VM substrate can be configured with proper shares of resources (such as CPU, memory, storage, network bandwidth) dynamically.

In recent years, various enhancements on resource isolation techniques [2], [13], [8] have been proposed to achieve fine-grained dynamic resource provisioning. A proportional share scheduler can be implemented based on Xen's *credit scheduler* [14] to multiplex CPU resource among virtual machines in a fair manner. The *balloon driver* [15], *difference engine* [10], *joint-VM* [8], and *virtual putty* [9], can dynamically adjust the memory resource among collocated virtual machines. The *dm-ioband* [16] can dynamically control the usage of disk I/O bandwidth among co-located virtual machines. These advanced techniques enable computing resources to be dynamically partitioned or reassembled to meet the elastic needs of end-users. Such solutions create an unprecedented opportunity to maximize resource utilization, which were not possibly applied in most Grid systems [34], [36], [19], [37], [38] that usually treat the underlying resources as indivisible ones and prevent simultaneous access to them. Today's Cloud architectures are not without problems. Most Cloud services built on top of a centralized architecture may suffer denial-of-service (DoS) attacks [3], unexpected outages, and limited pooling of computational resources. On the contrary, volunteer computing systems (or Desktop Grids) can easily aggregate huge potential computing power to tackle grand challenge science problems [4].

In view of this, we propose a novel Cloud architecture, namely *self-organizing cloud* (SOC), which can connect a large number of desktop computers on the Internet by a P2P network. In SOC, each participating computer acts as both a resource provider and a resource consumer. They operate autonomously for locating nodes with more abundant resource or unique services in the network to offload some of their tasks, meanwhile they could construct multiple VM instances for executing tasks submitted from others whenever they have idle resources. We focus on two key issues in the design of SOC: (1) the multi-attribute range query problem in a fully decentralized environment for locating a qualified node to satisfy a user task's resource demand with bounded delay and (2) how to optimize a task's execution time by determining the optimal shares of the multi-attribute resources to allocate to the tasks with various

QoS constraints, such as the expected execution time and limited budget.

As a fundamental difference to existing approaches, we formulate such a resource allocation problem to be a convex optimization problem [23]. Given a task with its resource requirements and a budget, we first prove that the optimal resource allocation on a qualified node that can minimize a task's execution time does exist. We further show that it is non-trivial to solve such a convex optimization problem directly via a brute-force strategy and the interior point method [23]. By relaxing the problem definition, we propose an algorithm to optimize the task execution time on a qualified resource node, given its preset budget and tolerable Quality of Service (QoS).

The proposed algorithm involves only $O(R2)$ adjustment steps, where R denotes the number of resource attributes (or dimensions). We further propose a *dynamic optimal proportional-share* (DOPS) resource allocation algorithm with $O(R3)$ complexity, by incorporating the *proportional share model* (PSM) [12]. The key idea is to dynamically scale the amount of resources at each dimension among running tasks proportional to their demand, such that these tasks could use up the maximum capacity of each resource type at a node. To locate qualified nodes in the SOC environment, we design a fully-decentralized range query protocol, namely *pointer-gossiping CAN* (PG-CAN), tailored for DOPS. Existing P2P desktop Grids favor CAN-based [17] or Chordbased [18] resource discovery protocols [19], [20]. Every joining node registers its static resource attributes (e.g. CPU architecture, OS version) or maximum capacity on the CAN/Chord overlay, so that other users could find the most matched node within a logarithmic (or sublinear) number of routing steps. Such a design is feasible for a P2P desktop Grid because the resources of a selected node can only be used exclusively by a single task. However, due to dynamic resource provisioning technologies used in Cloud, the frequent resource repartitioning and re-allocation (e.g., upon task arrival or completion) make it a challenging problem to locate a node containing a combination of available resources along all the R resource attributes that would satisfy the requirements of a submitted task. The proposed PG-CAN range query protocol in this work aims to find the qualified resources with minimized contention among requesters based on task's demand. It is unique in that for each task, there is only one query message propagated in the network during the entire course of discovery. This is different from most existing multiattribute range query solutions that require to propagate multiple sub-queries along multiple dimensions in parallel.

To mitigate the contention problem due to analogous queries in CAN, our range query protocol proactively diffuses resource indexes over the network and randomly route query messages among nodes to locate qualified ones that satisfy tasks' minimal demands. To avoid possibly uneven load distribution and abrupt resource over-utilization caused by un-coordinated node selection process from autonomous participants, we investigate three node selection policies, namely double-check policy [21], queuing policy [22], and extra-virtual-dimension policy [19].

The rest of the paper is organized as follows. We formulate the resource allocation problem in a VM-multiplexing environment in Section 2. In Section 3, we prove that optimal resource allocation does exist and show that our solution is optimal. In Section 4, we present our DOPS resource allocation scheme. Section 5 details the proposed range query protocol. In Section 6, we show the simulation results. We discuss related work in Section 7 and conclude with an outline of future work in Section 8.

2 OPTIMAL RESOURCE ALLOCATION

Given a task tij with its weight vector $w(tij)$ and a budget $B(tij)$, we first prove that the optimal resource allocation on a qualified node ps with its price vector $b(ps)$ does exist.

Lemma 1: The optimal allocation (denoted $r*(tij)$) exists iff (i.e., $\Longleftrightarrow$) Inequalities (6) and (7) are met.

$$b(ps)T \cdot e(tij) \leq B(tij) \quad (6)$$

Proof:

To prove $\Rightarrow$: (transport property of inequalities)

If $r*(tij)$ exists, it must satisfy Inequalities (3) and (5), thus the Inequalities (6) and (7) should hold.

To prove $\Leftarrow$: (to satisfy *Slater*'s condition [23])

If $b(ps)T \cdot e(tij)=B(tij)$ or $e(tij)=a(ps)$, then $e(tij)$ is a unique solution, which can be regarded as an optimal one. If $b(ps)T \cdot e(tij) < B(tij)$ and $e(tij) \prec a(ps)$, other than $e(tij)$, there must exist another better solution (denoted $r'(tij)$) such that $b(ps)T \cdot r'(tij) < B(tij)$ and $e(tij)\ r'(tij) \prec a(ps)$, thus $r*(tij)$ must exist according to *Slater*'s condition [23]. Similarly, if $b(ps)T \cdot e(tij) < B(tij)$ and $e(tij) \preceq a(ps)$, *Slater*'s condition can also hold by excluding the equations from the constraints (7).

We assume the qualified node ps that satisfies Inequalities (6) and (7) can be found based on tij 's expected resource vector $e(tij)$ by a resource discovery protocol (to be discussed in Section 5). Thus, we could rewrite the constraint (5) to be Inequality (8) and construct a Lagrangian function $F1(r(tij)$ That is, the optimal resource vector $r*$ could be found as long as we could satisfy the above conditions simultaneously.

In order to solve the above simultaneous equations and inequalities, there are two traditional candidate strategies:

(1) brute-force method and

(2) interior point

the method is converged with them,

If we replace Constraint (5) with Constraint (11), we could find an optimal solution through a few convex optimization steps. That is, via such a constraint relaxation, we could optimize the resource allocation for task tij on node ps without exhausting all $3R$ possible combinations like the

brute-force method or worrying about the convergence problem in the interior point method.

3 POINTER-GOSSIPING CAN

Our resource allocation approach relies on the assumption that all qualified nodes must satisfy Inequalities (6) and (7) (i.e., Lemma 1). To meet this requirement, we design a resource discovery protocol, namely *pointer-gossiping CAN* (PG-CAN), to find these qualified nodes. We choose CAN [17] as the DHT overlay to adapt to the multi-dimensional feature.

Like traditional CAN, each node (a.k.a. *duty node*) under PG-CAN is responsible for a unique *multi-dimensional range* zone randomly selected when it joins the overlay. Fig. 2 (a) illustrates an example of CAN overlay network. Suppose there are 25 joined nodes, each taking charge of a single zone. If a new node (node 26) joins, a random point such as (0.6 Gflops, 0.55GB) will be generated and its zone will be set as the new zone evenly split along a dimension from the existing zone (node 25 in Fig. 2 (a)) that contains this point. If there is only one non-overlapped range dimension between two nodes (e.g. *pi* and *pj*) and they are adjacent at this dimension, we call them *neighbors* to each other. Furthermore, if the non-overlapped range of *pi* is always no less than *pj* 's, *pi* is called *pj* 's *positive neighbor* and *pj* is called *pi*'s *negative neighbor*. In Fig. 2 (a), Node 9, 12 and 20 are positive neighbors of node 1.

Every node will periodically propagate the state-update messages about its available resource vector $a(ps)$ to the *duty node* whose zone encloses this vector. After a task *tij* generates a query (Step 1 in Fig. 2 (b)) with the constraints (6) and (7), the query message will be routed to the duty node containing the expected vector $e(tij)$. We could justify that the state messages (or state records) of all qualified nodes must be kept in those onward nodes (i.e., shadow area in Fig. 2 (b)) of the duty node.

Obviously, the searching area may still be too large for the complete resource query without flooding, so the existing solutions [19] usually adopt random-walk to get an approximated effect. However, according to our observation (to be presented), this will significantly reduce the likelihood of finding qualified resources, finally degrading the system throughput and user's QoS. Alternatively, we improve the mechanism by periodically diffusing a few pointer-messages for any duty nodes owning state-update messages (or records) to the distant nodes (with distance as $2k$ hops, where k=0,1,・・・) towards negative directions, so that these duty nodes could be more easily found. In Fig. 2, for instance, Node 4's negative pointer nodes along CPU dimension are Node 14, 3, and 23. By periodically sending pointer-recovery messages, each with empty payload outward, each node could easily maintain the connection to the negative pointer nodes. On the other hand, each query routed to the duty node will check its stored records and the pointed duty nodes. If it finds qualified resource records on the current or other pointed duty nodes, it will return those information to the requesting node; otherwise, it will continue searching next positive neighbor duty nodes.

Each duty node (such as $D1$) will cache state-update messages received from its neighbors, which are checked periodically and removed if outdated (i.e., beyond their TTL). In the meanwhile, it propagates its own identifier (such as IP) to a few randomly selected pointer nodes towards it negative direction. For those duty nodes containing valid state messages, we call them *non-empty-cache nodes*.

Basically, there are two manners to propagate the duty nodes' identifiers (or pointers) backward - *spreading manner* (Fig. 3 (a)) and *hopping manner* (Fig. 3 (b)), thus the PG-CAN can also be split into two types, namely *spreading manner based PG-CAN* (SPG-CAN) and *hopping manner based PG-CAN* (HPG-CAN). In Fig. 3 (a), the duty node $D1$ sends a pointer-message containing $D1$'s identifier to its selected pointer nodes (such as $D2$ and $D3$), notifying them that $D1$ has records. Upon receiving the message, the pointer nodes ($D2$ and $D3$) will further gossip $D1$'s identifer to their negative direction pointer nodes along next dimension. In Fig. 3 (b), the identifer of any nonempty- cache node will be forwarded from pointer node to pointer node along each dimension. Obviously, the former results in fewer number of hops for message delivery, but its identifers cannot be diffused as widely as the latter's. In fact, we can prove that the delay complexity of identifier delivery for the hopping manner is $O(\log2\ n)$ (Theorem 5), so the hopping manner is likely to be better than the spreading manner (to be confirmed in our simulation).

Theorem 5: The delay complexity of hops by hopping manner for relaying any node's index to any of its negative direction nodes is $O(\log2\ n)$, where n refers to the total number of nodes.

Note that $\log2\ n=d$ ・ $\log2\ n1d$, so our objective is to prove the delay is bounded under d $\log2\ n1d$. The strict proof can be found in our previous work [24]. Here, we just use an example (shown in Fig. 4) to illustrate the idea. In this example, suppose there are n 1 d =19 nodes along each dimension, it is obvious that the top-most node (Node 1) will take longest time (less than $O(\log(19))=4$) to diffuse its own index. Specifically, over the first hop, Node 2, 3, 5, 9, and 17 could receive the index (Node 1's identifier). Via the second hop, Node 4, 6, 7, 10, 11, and 13 could receive the relayed index. For instance, Node 7 could receive Node 1's index forwarded from Node 5 or Node 3. With just 3 hops, most of the negative-direction nodes of Node 1 could

8 CONCLUSIONS AND FUTURE WORK

This paper proposes a novel scheme (DOPS) for virtual resource allocation on a Self-Organizing Cloud (SOC), with three key contributions listed below.

• *Optimization of Task's Resource Allocation Under User's Budget*: With a realistic monetary model, we propose a solution which can optimize the task execution performance

based on its assigned resources under the user budget. We prove its optimality using the KKT conditions in the convex-optimization theory.

• *Maximized Resource Utilization based on PSM*: In order to further make use of the idle resources, we design a dynamic algorithm by combining the above algorithm with PSM and the arrival/completion of new tasks. This can give incentives to users by gaining an extra share of un-used resource without more payment. Experiments confirm achieving a super-optimal execution efficiency of their tasks is possible. DOPS could get an improvement on system throughput by

15%∼60% than the traditional methods used in P2P Grid

model, according to the simulation.

• *Lightweight Resource Query Protocol with Low Contention*:

We summarize the resource searching request as two range query constraints, Formula (6) and Formula (7). We prove them to be the sufficient and necessary conditions for getting the optimal resource allocation. Experiments confirm the designed PGCAN protocol with light-weight query overhead is able to search qualified resources very effectively. So far, we have successfully built a prototype supporting live migration of VMs between any two nodes on the Internet (even though they are behind different NATs). In the future, we will study fault-tolerance support for a (DOPS-based, PG-CAN-enabled) SOC system; we will also conduct sensitivity analysis of how violation of our model assumptions would impact the optimal resource allocation.

REFERENCES

[1] J. E. Smith and R. Nair, *Virtual Machines: Versatile Platforms For Systems And Processes*. Morgan Kaufmann, 2005.

[2] D. Gupta, L. Cherkasova, R. Gardner, and A. Vahdat, "Enforcing performance isolation across virtual machines in xen," *Proc. Seventh ACM/IFIP/USENIX Int'l Conference on Middleware (Middleware'06)*, pp. 342–362, 2006.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing,", Tech. Rep., UCB/EECS-2009-28, Feb 2009.

[4] D. P. Anderson, "Boinc: a system for public-resource computing and storage," *Proc. Fifth IEEE/ACM Int'l Workshop on Grid Computing*, pp. 4–10, 2004.

[5] P. Crescenzi and V. Kann, *A compendium of NP optimization problems*. [Online]. Available: ftp://ftp.nada.kth.se/Theory/Viggo- Kann/compendium.pdf

[6] O. Sinnen, *Task Scheduling for Parallel Systems (Wiley Series on Parallel and Distributed Computing)*, Wiley-Interscience, 2007.14

[7] O. H. Ibarra and C. E. Kim, "Heuristic algorithms for scheduling independent tasks on nonidentical processors," *J. ACM*, vol. 24, pp. 280–289, April 1977.

[8] X. Meng and et al., "Efficient resource provisioning in compute clouds via vm multiplexing," *Proc. seventh IEEE int'l conf. on Autonomic computing (ICAC'10)*, pp. 11–20, 2010.

[9] J. Sonneck and A. Chandra, "Virtual putty: Reshaping the physical footprint of virtual machines," *Proc. Int'l HotCloud Workshop in conjunction with USENIX Annual Technical Conference*, 2009.

[10] D. Gupta and et al., "Difference engine: Harnessing memory redundancy in virtual machines," *Proc. eighth Int'l USENIX Symp. On Operating Systems Design and Impl.*, pp. 309 – 322, 2008.

[11] S. Govindan, J. Choi, B. Urgaonkar, A. Sivasubramaniam, and A. Baldini, "Statistical profiling-based techniques for effective power provisioning in data centers," in *Proc. fourth ACM Conf. European Conf. on Computer systems (EuroSys'09)*, 2009, pp. 317–330.

[12] M. Feldman, K. Lai, and L. Zhang, "The proportional-share allocation market for computational resources," *IEEE Trans. on Parallel and Distributed Systems*, vol. 20, pp. 1075–1088, 2009.

[13] S. Soltesz, H. Poetzl, M. E. Fiuczynski, A. Bavier, and L. Peterson, "Container-based operating system virtualization: a scalable, highperformance alternative to hypervisors," *Proc. second ACM Int'l European Conf. on Computer Systems (Euro'07)*, 2007, pp. 275–
287.

[14] L. Cherkasova, D. Gupta, and A. Vahdat, "Comparison of the three cpu schedulers in xen," *SIGMETRICS Perform. Eval. Rev.*, vol. 35, no. 2, pp. 42–51, 2007.

[15] "The role of memory in vmware esx server 3: on line at: http://www.vmware.com/pdf/esx3 memory.pdf," Tech. Rep.

[16] dm-ioband: online at http://sourceforge.net/apps/trac/ioband.

[17] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, "A scalable content-addressable network," *Proc. ACM Int'l Conf. on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM'2001)*, pp. 161–172, 2001.

[18] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," *Proc. ACM Int'l Conf. on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM' 2001)*, pp. 149–160, 2001.

[19] J. S. Kim and et al., "Using content-addressable networks for load balancing in desktop grids," *Proc. 16th ACM Int'l Symp. On High Performance Distributed Computing (HPDC'07)*, pp. 189–198, 2007.

[20] A. Leite, H. Mendes, L. Weigang, A. de Melo, and A. Boukerche, "An architecture for P2P bag-of-tasks execution with multiple task allocation policies in desktop grids," *Proc. IEEE Int'l Conf. Cluster Computing*, pp. 1–11, Feb. 2011.

[21] Y. Drougas and V. Kalogeraki, "A fair resource allocation algorithm for peer-to-peer overlays," *Proc. 24th Int'l Conf. on Computer Communications (INFOCOM'05)*, pp. 2853–2858, 2005.

[22] D. Gross and C. M. Harris, *Fundamentals of Queueing Theory (Wiley Series in Probability and Statistics)*, Wiley-Interscience, Feb. 1998.
[23] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2009.
[24] S. Di, C.-L. Wang, W. Zhang, and L. Cheng, "Probabilistic best-fit multi-dimensional range query in self-organizing cloud," *Proc. 40th IEEE Int'l Conf. on Parallel Processing*, pp. 763–772, 2011
[25] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the art of virtualization," in *Proc. 19th ACM symp. on Operating systems principles (SOSP'03)*, 2003, pp. 164–177.
[26] Peersim simulator: http://peersim.sourceforge.net.
[27] Google cluster-usage traces: online at http://code.google.com/p/googleclusterdata.
[28] C. A. Waldspurger, "Memory resource management in vmware esx server." [Online]. Available: http://www.usenix.org/events/osdi02/tech/waldspurger.html
[29] J. P. Walters, V. Chaudhary, M. Cha, S. G. Jr., and S. Gallo, "A comparison of virtualization technologies for hpc," *Proc. 22nd Int'l IEEE Conf. on Advanced Information Networking and Applications (AINA'08)*, pp. 861–868, 2008.
[30] W. K. Mark Jelasity and M. van Steen, "Newscast computing," Vrije Universiteit Amsterdam, Tech. Rep., 2006.
[31] R. K. Jain, *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation and Modelling*, John Wiley & Sons, April 1991.
[32] J. Cao, F. B. Liu, and C. Z. Xu, "P2pgrid: integrating p2p networks into the grid environment: Research articles," vol. 19, no. 7, Chichester, UK: John Wiley and Sons Ltd., pp. 1023–1046, 2007
[33] H. Abbes, C. Cerin, and M. Jemni, "Bonjourgrid: Orchestration of multi-instances of grid middlewares on institutional desktop grids," *Proc. 23rd IEEE Int'l Symp. on Parallel & Distributed Processing (IPDPS'09)*, pp. 1–8, 2009
[34] A. Rossi, A. Singh, and M. Sevaux, "A metaheuristic for the fixed job scheduling problem under spread time constraints," *Comput. Oper. Res.*, vol. 37, pp. 1045–1054, June 2010.
[35] P. Switalski and F. Seredynski, "Generalized extremal optimization for solving multiprocessor task scheduling problem," *Proc. Seventh Int'l Conf. on Simulated Evolution and Learning*, Berlin, Heidelberg: Springer-Verlag, 2008, pp. 161–169.
[36] G. Singh, C. Kesselman, and E. Deelman, "A provisioning model and its comparison with best-effort for performance-cost optimization in grids," in *Proc. 16th ACM Symp. on High Performance Distributed Computing (HPDC'07)*, 2007, pp. 117–126.
[37] Q. Zheng, H. Yang, and Y. Sun, "How to avoid herd: a novel stochastic algorithm in grid scheduling," *Proc. 15th ACM Int'l Symp. on High Performance Distributed Computing (HPDC'06)*, Los Alamitos, pp. 267–278, 2006.
[38] C. B. Lee and A. E. Snavely, "Precise and realistic utility functions for user-centric performance analysis of schedulers," *Proc. 16th ACM Int'l Symp. on High Performance Distributed Computing HPDC'07)*, pp. 107–116, 2007.
[39] A. R. Bharambe, M. Agrawal, and S. Seshan, "Mercury: supporting scalable multi-attribute range queries," *Proc. ACM Int'l Conf. on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM'2004)*, pp. 353–366, 2004.
[40] D. Li, J. Cao, X. Lu, and K. C. C. Chen, "Efficient range query processing in peer-to-peer systems," *IEEE Trans. on Knowledge and Data Engineering*, vol. 21, no. 1, pp. 78–91, January 2009.
[41] A. Gonzalezbeltran, P. Milligan, and P. Sage, "Range queries over skip tree graphs," *Computer Communications*, vol. 31, no. 2, pp. 358–374, February 2008.
[42] S. Wang, Q. H. Vu, B. C. Ooi, A. K. Tung, and L. Xu, "Skyframe: a framework for skyline query processing in peer-to-peer systems," *J. VLDB*, vol. 18, pp. 345–362, January 2009.
[43] M. A. Arefin, M. Y. S. Uddin, I. Gupta, and K. Nahrstedt, "Q-tree: A multi-attribute based range query solution for tele-immersive framework," in *Proc. 29th Int'l Conf. on Distr. Comp. Sys. (ICDCS'09)*, pp. 299–307, 2009.
[44] J. Wang, S. Wu, H. Gao, J. Li, and B. C. Ooi, "Indexing multidimensional data in a cloud system," *Proc. ACM Int'l Conf. on Management of Data (SIGMOD'10)*, pp. 591–602, 2010.

Decentralized Self-Adaptation Mechanism For Service Selection and Allocation Scheme in Cloud

C.Saravanan[1], C.Anuradha[2]

[1]PG Scholar, SCAD Engineering College, Tirunelveli.

[2]HOD, SCAD Engineering College, Tirunelveli.

Email id: c.saravanansoft@gmail.com

Abstract—Cloud computing, with its promise of (almost) unlimited computation, storage and bandwidth, is increasingly becoming the infrastructure of choice for many organizations. As cloud offerings mature, service-based applications need to dynamically recompose themselves, to self-adapt to changing QoS requirements. In this paper, we present a decentralized mechanism for such self-adaptation, using market-based heuristics. We use a continuous double-auction to allow applications to decide which services to choose, amongst the many on offer. We view an application as a multi-agent system, and the cloud as a marketplace where many such applications selfadapt. We show through a simulation study that our mechanism is effective, for the individual application as well as from the collective perspective of all applications adapting at the same time.

Keywords—**Self-Adaptation, Market-Based, Multi-Agent Systems**

1 INTRODUCTION

Self-adaptation, as a concept, has been around for many years, in several domains like biology, chemistry, logistics, economics etc. Self-adaptivity in computer-based systems is relatively newer. Some of the first references to self-adaptive software systems are from [41], [35], [34] and [31] (where they are referred to, as autonomic systems). By self-adaptivity in software systems, we mean software that monitors itself and the operating environment, and takes appropriate actions when circumstances change. In web-applications, service-oriented architecture has often been used as a mechanism for achieving self-adaptivity [19]. Web-services allow for dynamic composition, which enables applications to switch services, without going offline. A common instance of using web-services dynamically, is applications living on the cloud, asking for computing power and bandwidth to be scaled up or down, depending on demand. However, one of the cloud's major selling points, *operational flexibility* is of little use, if applications (or organizations) have to indicate at sign-up time, the kind of services that they intend to use. On Amazon, for instance, a customer specifies during sign up whether she wants a Hi-CPU instance or a Standard On-Demand instance or a Hi-Memory instance. This assumes that an application is able to forecast its demand for computing and storage resources accurately. However, this inability to forecast is precisely what the cloud claims to address through elasticity in computing power. This is not to say that there are no flexible, demand-based pricing schemes available. Amazon's *Spot Instances* [29] is an example of how cloud providers are trying to flexibly price their services, in response to fluctuating demand over time. Applications that can adapt to fluctuating prices will be able to ensure a better return on investment. In the future, we surmise that service-pricing will depend not only on demand but also on additional attributes like performance, availability, reliability, etc. Current implementations of public clouds mainly focus on providing easily scaled-up and scaled-down computing power and storage. We envisage a more sophisticated scenario, where federated clouds with different specialized services collaborate. These collaborations can then be leveraged by an enterprise to construct an application, that is self-adaptive by changing the specific web-service it utilizes. The notion of utilizing collaborative services to satisfy a business need, is not new in itself. The recognition of Agile Service Networks (ASN) that spring up in modern business practices, is testament to this. As ASNs mature and dynamic composition becomes the norm, we posit that applications that are composed of other applications will routinely adapt to changing QoS requirements. In this paper, we propose a decentralized mechanism to address the problem.

2 OUR APPROACH

We would like to create a mechanism that allows multiple applications, constructed across a federation of clouds, to

self-adapt. We chose a market-based approach to self-adaptation, not only because it is decentralized, but also due to its easy applicability to the problem domain. Services in the cloud aremoving from a fixed-price package to a more flexible, auction-based approach [29]. This enables a self-adaptive application to change the QoS exhibited, by switching to a different ConcreteService.

2.1 Market-Based Control

Market-Based Control (MBC) essentially involves modeling the system as a marketplace, where self-interested agents use economic strategies to compete for resources. Self-interested competition, along with well-designed utility functions, allow for a decentralized means of decision making. These agents, via their competitive need to get resources, perform a parallel search through the space of decision points. MBC has been used in several contexts, as a mechanism for computing a good solution in a decentralized manner. Notable examples include Clearwater's bidding agents to control the temperature of a building [16], Ho's center-free resource algorithms [52] and Cheriton's extension to operating systems to allow programs to bid for memory [25]. Wellman's WALRAS system [49], which is highly distributed, reports high scalability. More examples include distributed Monte-Carlo simulations [47], distributed database design using market-methods for distributing sub-parts of queries [45] and proportional-share resource management technique [48]. All of these systems provide evidence of market-based control being a good candidate for distributed decision making.

2.2 Auctions

Auctions, specifically Double Auctions (DA), have increasingly been studied in Computer Science, as a mechanism of resource allocation. Daniel Friedman [22] reports on experiments where traders even with imperfect information, consistently achieve highly efficient allocations and prices. The rise of electronic commerce naturally creates a space for efficient exchange of goods, and services. There has been much work on the design space of market-institutions [51], [39], bidding strategies [17], [43], agent-based implementations of traders [30], [26], [27], [40], etc. Gupta et al [24] argue that network management, specifically for QoS issues, must be done using pricing and market dynamics. According to them, the flexibility offered by pricing mechanisms offers benefits of decentralization of control, dynamic load management and effective allocation of priority to different QoS attributes. The continuous-time variant of a DA, called *Continuous Double Auction* (CDA), is used in stock-markets and commodity exchanges around the world [32]. In a CDA, the market clears *continuously*.
That is, instead of waiting for all bids and asks to be made, matches are made as the bids and asks come in. A new bid is evaluated against the existing asks and the first ask that matches, is immediately paired off for a transaction. A CDA is known to be highly allocatively efficient [23], *i.e.*, it achieves a very high percentage of all the possible trades, between buyers and sellers. The most important property of the work in [23], is that a CDA's efficiency results from the structure of the mechanism used, rather than intelligence of the agents involved in trading. This is a very important result, since it provides us with encouragement regarding the efficiency of our mechanism.

3 EVALUATION

3.1 The Current Scenario

The current form of service-selection is provider-driven. That is, in all commercial clouds, the cloud provider uses a **posted-offer** mechanism. A posted-offer is a form of market where the supplier posts a certain price on a *takeit- or-leave-it* basis. Thus, on Amazon's *elastic cloud compute* (EC2), there are several services that are functionally identical, but priced differently. This price differentiation exists due to different QoS being exhibited by these services. In Table 10, we show a slice of Amazon's pricing for its *On-Demand Instances*. Depending on the type of job envisioned, customers purchase a basket of computational power from Amazon. However, currently, there is no mechanism to automatically switch from one kind of *On-Demand Instance* to another. Customers have to forecast the type of demand for their application in advance, and appropriately chose their package from Amazon. Any application that desires to use a particular service, has to pay the posted price. There exists no mechanism to negotiate/bargain with Amazon, on pricing or QoS of the services being offered. This has the very obvious effect of customers either over-provisioning or under-provisioning for their actual demand. If an

3.2 Empirical Study

BizInt, a small (fictional) startup company creates a new business intelligence mining and visualization application. It combines off-the-shelf clustering algorithms with its proprietary outlier detection and visualization algorithms, to present a unique view of a company's customer and competitor ecosystem. In order to exhibit a high level of performance, it decides to host its application in the cloud. Also, instead of reinventing the wheel, it uses third-party services (for clustering, etc.) that are also hosted in the same cloud. BizInt uses composite web services (Data Filtering, Clustering, Association Rule Mining and Cross-Validation) from the cloud, along with its own services (Job Submission, Outlier Detection and Visualization) to create a complete application. Soon BizInt discovers that different jobs emphasize different QoS. Some jobs want data to be processed as fast as possible, others require a high amount of security and reliability. In order to exhibit different QoS, BizInt needs to dynamically change its constituent services.

SkyCompute is a new (fictional) entrant to the field of Cloud Computing. It wants to compete with Amazon, 3Tera, Google, Microsoft and other established cloudproviders. In order to attract cost and QoS-conscious customers, SkyCompute will have to differentiate its cloud from the others. It plans to target the *Software-As- A-Service* market. Instead of providing specialist infrastructural services (like Amazon) or application frame

work services (like Google and Microsoft),it is planning to provide generically useful services like indexing, clustering, sorting, etc. Like most cloud providers, it plans to provide services with different QoS levels, so that multiple types of clients can be attracted to use it. To differentiate itself, SkyCompute plans to provide an adaptive framework, so that companies like BizInt can change their constituent services, dynamically.

3.3 Qualitative Criteria

Thus, *clobmas* must fulfill the following criteria:
1) Allows customers like BizInt to create adaptive applications
2) Generates a higher utilization of services than the posted-offer model currently followed (for Sky-Compute)

3.4 Quantitative Criteria

Since, SkyCompute is an ultra-large collection of services, clobmas must be able to scale to large numbers of applications and ConcreteServices. Since there is no public data about the kinds of workflows hosted on commercial clouds, and their corresponding service choices, we made assumptions about the variables involved in dynamic service composition. We make these assumptions based on conversations with performance consultants at Capacitas Inc., and numbers gleaned from the literature review.

4 Related Work

4.1 Dynamic Composition of Web-services

There has been a plethora of work on dynamic composition of web-services. Much early work has been done in AgFlow [54] on Quality-Aware composition of webservices [5] and [53]. The authors propose a per-serviceclass optimisation as well as a global optimisation using integer programming. [10] proposed a genetic algorithm based approach where the genome length is determined by the number of abstract services that require a choice to be made. Constraints on QoS form a part of the fitness function, as do cost and other QoS attributes. A big advantage of GAbased approach is that it is able to handle non-linear constraints, as opposed to integer programming. Also, it is scalable when the number of concrete services per abstract service increase. [2] propose an interesting mechanism for cutting through the search space of candidate web-services, by using skyline queries. Skyline queries identify *non-dominated* webservices on at least one QoS criteria. A *non-dominated* web-service means, a web-service that has at least one QoS dimension in which it is strictly better than any other web-service and at least equal on all other QoS dimensions. Determining skyline services for a particular abstract service, requires pairwise comparisons amongst the QoS vectors of all the concrete services. This process can be expensive if the number of candidate concrete services is large. Alrifai et al. consider the case where the process of selecting skyline services is done offline. This would lead to an inability to adjust to changing conditions of available services and their associated QoS values. [56] propose an interesting method to achieve a good set of concrete services, using Ant Colony Optimization (ACO). ACO involves creating virtual ants that mimic the foraging behaviour of real ants. The search space of optimal concrete services is modelled as a graph, with sets of concrete services as vertices and edges being all the possible connections between different concrete service sets. The ants attempt to complete a traversal of the graph, dropping pheromones on the edge of each concrete service visited. The path through the graph that accumulates the most pheromones represents the near-optimal path of services to use. Our approach differs from the above approaches in two respects:

1) Consideration of time as a factor: In practice, the optimal set of concrete services may not be available at the time instant that an application is searching. The set of service providers changes with time, as does the set of service consumers. This means that the optimal matching of service providers to consumers changes with time. The approaches above do not take this into account.

2) Optimality not considered: Due to the infeasibility of computing the optimal set (being NP-hard), we concentrate on finding a good solution, rather than an optimal one. A good solution is one that does not violate any QoS constraints and meets the cost constraint within a certain margin.

4.2 Self-Adaptation

Applications that use dynamic service composition should be able to continuously monitor their current QoS levels and make adjustments when either the demand for QoS changes or the cost constraint changes. The application should thus be able to respond to both internal as well as external stimuli, to trigger a change in its constituent web-services. This change needs to be both timely, as well as correct, *i.e.*, the new set of services should not violate any of the application's QoS constraints, and the change should happen as fast as possible.

Self-Adaptation in software systems is the achievement of a stable, desirable configuration, in the presence of varying stimuli. These stimuli may be environmental (in the form of workload, failure of external components, etc.) or internal (failure of internal components, changed target states, etc.). Given that the range of stimuli that affect a software system is wide, Self-Adaptation has come to mean an umbrella term that covers multiple aspects of how a system reacts [44]:
1) Self-Awareness
2) Context-Awareness
3) Self-Configuring
4) Self-Optimizing
5) Self-Healing
6) Self-Protecting
However, most approaches to self-adaptation follow a common pattern: Monitor – Analyze – Plan – Execute, connected by a feedback loop. There are two approaches to self-adaptation: centralized and de-centralized. In a centralized self-adaptive system, the analysis and planning

part are concentrated in one entity. This form of self-adaptation has the advantage of cohesiveness and low communication overhead as compared to a decentralized mechanism. The analysis and the plan can be communicated to the effectors, and feedback from obeying the plan is communicated back through the monitors (or sensors). Rainbow [14] and *The Autonomic Manager* [28] are classic examples of centralized selfadaptation. Decentralized self-adaptation, on the other hand, distributes the analysis, planning or the feedback mechanism amongst different parts of the adapting system. This automatically implies a communication overhead, since all constituent parts must coordinate their actions. However, it also provides for robustness in the presence of node failure and scalability of application size. Cheng et al [13] have advocated that the feedback loop, which is a critical part of the adaptation, be elevated to a first-class entity in terms of modelling, design and implementation. Although, this would allow for reasoning about properties of the adaptation, there are no systems that we currently know of, that provide an explicit focus on the feedback loop. Most decentralized self-adaptation systems are typically realised as a multi-agent systems wherein the agents are autonomous in their environments and implement strategies that collectively move the entire system into a desirable state. [15] have advocated separating the functional part of the system from the adaptive part, thus allowing for independent evolution of both. Baresi et al [4] describe such a system, where adaptation is considered as a cross-cutting concern, and not a fundamental part of system computation. Baresi et al. use aspect-oriented programming to implement
the Monitor and Execute part of the MAPE loop. They implement distributed analysis and planning by dividing the self-adaptive system into *supervised elements*, that perform the business logic of the application and *supervisors* that oversee how the supervised components behave and plan for adaptation. Aspect-probes form the sensors and actuators that link the supervised elements to the supervisors. [18] describe another interesting approach to decentralized self-adaptation, through self-organization. DiMarzo et al. take a bio-inspired approach and use principles of holons (and holarchy) and stigmergy to get agents in a manufacturing department to perform coordination and control. A holon is defined by [33] to be both a part and a whole. Therefore, an agent is both autonomous as well as a part of a hierarchy, which influences it. The essential idea in their work is that with such structures, order emerges from disorder, as simple interactions build on each other, to produce progressively complex behaviour. Weyns et al [50] study a decentralized self-healing system and a QoS-driven self-optimized deployment framework. Their approach is the nearest to ours. They suggest multiple decentralized models which feed into decentralized algorithms, which are in turn analyzed by decentralized analyzers. These analyzers then individually direct local effectors to make changes to the host system. These approaches, while interesting, have not explicitly considered scale of adaptation. Any approach that attempts self-adaptation on the cloud, must concern itself with scaling up to hundreds and possibly even thousands of entities. Another issue that needs to be considered, is the effect of other self-adapting systems operating in the same environment.

4.3 QoS Monitoring

Zeng [55], and Michlmayer [37] are good examples of online QoS monitoring. Zeng et al. classify QoS metrics into three categories: (a) Provider-advertised (b) Consumer-rated, and (c) Observable metrics. They provide an event-driven, rule-based model where designers can define QoS metrics and their computation logic (in terms of Event-Condition-Action rules), for observable metrics. These are then compiled into executable statecharts, which provide execution efficiency in computing QoS metrics based on service-events that are observed. Michlmayer et al. provide their QoS monitoring as a *service runtime environment*. This service runtime environment addresses service metadata, QoS-aware service selection, mediation of services and complex event processing. The authors propose two mechanisms to monitor QoS:
(a) a client-side approach using statistical sampling, and (b) a server-side approach using probes
that are present on the same host as the service. The client-side approach is non-intrusive, in terms of not needing access to the service's host.

Both approaches, Zeng and Michlmayer, use an eventbased mechanism to detect QoS values, and SLA violations, if any. This fits in neatly with our need for a non-intrusive, third-party based QoS Monitoring Engine. Our mechanism is agnostic to the actual QoS monitoring mechanism, that is used.

5 Conclusion and Future Work

Cloud-based service-oriented applications have the potential to self-adapt their QoS, depending on demand. Using a market-based mechanism maps nicely to the real-world situation of unpredictable change of QoS requirements, costs involved in adaptation and adaptation by competing applications. As the number of possible concrete services increase, the scalability of the self-adaptive mechanism becomes important. We see that the market-based mechanism consists of simple agents, is able to adapt well and yet scales linearly to the number of concrete services. We also see that it is robust in the presence of differences in demand and supply of QoS. Applications implemented as an ASN can thus scale and adapt to the changing business requirements of QoS. We have not modelled complex seller-side behaviour. Specifically, actions like deliberate violation of QoS to free up resources for making Asks with higher prices or mis-reporting of QoS available. Mechanisms like penalties and reputation management can be used to prevent seller agents from behaving dishonestly. Also, we have not modelled adaptation on the part of the market. Sellers that lie about their QoS or, are generally unattractive for transactions may lower the reputation of the marketplace. Hence, the market could take steps to ensure that it is populated, only with sellers that are likely to be sold. In future work, we aim to systematically add these

modifications to observe their effect on the collective adaptation.

REFERENCES

[1] Do slas really matter? 1-year case study.

[2] Mohammad Alrifai, Dimitrios Skoutas, and Thomas Risse. Selecting skyline services for QoS-based web service composition. *Proceedings of the 19th international conference on World wide web - WWW '10*, page 11, 2010.

[3] Danilo Ardagna and Barbara Pernici. Global and local qos constraints guarantee in web service selection. pages 805–806, 2005.

[4] Luciano Baresi, Sam Guinea, and Giordano Tamburrelli. Towards decentralized self-adaptive component-based systems. *Proceedings of the 2008 international workshop on Software engineering for adaptive and self-managing systems - SEAMS '08*, page 57, 2008.

[5] B. Benatallah, M. Dumas, Q.Z. Sheng, and a.H.H. Ngu. Declarative composition and peer-to-peer provisioning of dynamic Web services. *Proceedings 18th International Conference on Data Engineering*, pages 297–308, 2002.

[6] J.P. Brans and Ph. Vincke. A preference ranking organisation method: The promethee method for multiple criteria decisionmaking. *Management Science*, 31(6):647–656, June 1985.

[7] Ivan Breskovic, Christian Haas, Simon Caton, and Ivona Brandic. Towards self-awareness in cloud markets: A monitoring methodology. pages 81 –88, dec. 2011.

[8] R Buyya and S Pandey. Cloudbus toolkit for market-oriented cloud computing. In *Proceedings First International Conference, CloudCom 2009*, pages 22–44, 2009.

[9] Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venugopal. Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. *2008 10th IEEE International Conference on High Performance Computing and Communications*, pages 5–13, September 2008.

[10] Gerardo Canfora, Massimiliano Di Penta, Raffaele Esposito, and Maria Luisa Villani. An approach for QoS-aware service composition based on genetic algorithms. *Proceedings of the 2005 conference on Genetic and evolutionary computation - GECCO '05*, page 1069, 2005.

[11] Jorge Cardoso, Amit Sheth, and John Miller. Workflow quality of service. Technical report, University of Georgia, Athens, Georgia, USA, March 2002.

[12] Jorge Cardoso, Amit Sheth, John Miller, Jonathan Arnold, and Krys Kochut. Quality of service for workflows and web service processes. *Web Semantics: Science, Services and Agents on the World Wide Web*, 1(3):281–308, April 2004.

[13] B Cheng, R De Lemos, Holger Giese, and Paola Inverardi. Software engineering for self-adaptive systems: A research roadmap. *Software Engineering*, pages 1–26, 2009.

[14] Shang-Wen Cheng, David Garlan, and Bradley Schmerl. Architecture-based self-adaptation in the presence of multiple objectives. *Proceedings of the 2006 international workshop on Selfadaptation and self-managing systems - SEAMS '06*, page 2, 2006.

[15] SW Cheng and David Garlan. Making self-adaptation an engineering reality. *Self-star Properties in Complex Information Systems: Conceptual and Practical Foundations*, 3460:158–173, 2005.

[16] Scott H. Clearwater, Rick Costanza, Mike Dixon, and Brian Schroeder. Saving energy using market-based control. pages 253–273, 1996.

[17] D Cliff. Simple bargaining agents for decentralized market-based control. *HP Laboratories Technical Report*, 1998.

[18] Giovanna Di Marzo Serugendo, Marie-Pierre Gleizes, and Anthony Karageorgos. Self-organization in multi-agent systems. *The Knowledge Engineering Review*, 20(02):165–189, June 2005.

[19] Elisabetta DiNitto, Carlo Ghezzi, Andreas Metzger, Mike Papazoglou, and Klaus Pohl. A journey to highly dynamic, selfadaptive service-based applications. *Automated Software Engineering*, 15(3-4):313–341, September 2008.

21

[20] Leticia Duboc, David Rosenblum, and Tony Wicks. A framework for characterization and analysis of software system scalability. *Proceedings of the the 6th joint meeting of the European software engineering conference and the ACM SIGSOFT symposium on The foundations of software engineering - ESEC-FSE '07*, page 375, 2007.

[21] Torsten Eymann, Michael Reinicke, Oscar Ardaiz, Pau Artigas, Luis D´ıaz de Cerio, Felix Freitag, Roc Messeguer, Leandro Navarro, Dolors Royo, and Kana Sanjeevan. Decentralized vs. centralized economic coordination of resource allocation in grids. In *European Across Grids Conference*, volume 2970 of *Lecture Notes in Computer Science*, pages 9–16. Springer, 2003.

[22] Daniel Freidman. The double auction market institution: A survey. 1993.

[23] Dhananjay K. Gode and Shyam Sunder. Allocative efficiency of markets with zero-intelligence traders: Market as a partial substitute for individual rationality. *The Journal of Political Economy*, 101(1):119–137, 1993.

[24] Alok Gupta and DO Stahl. The economics of network management. *Communications of the ACM*, 42(9):57–63, 1999.

[25] Kieran Harty and David Cheriton. A market approach to operating system memory allocation. pages 126–155, 1996.

[26] Minghua He and Nicholas R. Jennings. Southamptontac: An adaptive autonomous trading agent. *ACM Trans. Internet Technol.*, 3:218–235, August 2003.

[27] Minghua He, N.R. Jennings, and Ho-Fung Leung. On agentmediated electronic commerce. *Knowledge and Data Engineering, IEEE Transactions on*, 15(4):985 – 1003, july-aug. 2003.

[28] IBM. An architectural blueprint for autonomic computing. June 2006.

[29] Amazon Inc. Amazon spot-instances. December 2009. http://aws.amazon.com/ec2/spot-instances/.

[30] Nick Jennings. Automated haggling: building artificial negotiators. pages 1–1, 2000.

[31] Jeffrey O. Kephart and David M. Chess. The vision of autonomic computing. *Computer*, 36(1):41–50, January 2003.

[32] Paul Klemperer. Auction theory: A guide to the literature. *JOURNAL OF ECONOMIC SURVEYS*, 13(3), 1999.

[33] Arthur Koestler. The ghost in the machine. 1989. ISBN 0-14-019192-5.

[34] MM Kokar and K Baclawski. Control theory-based foundations of self-controlling software. *Self-Adaptive Software and their Applications, IEEE Intelligent Systems*, 1999.

[35] Robert Laddaga. Creating robust software through selfadaptation. *IEEE Intelligent Systems*, 14:26–29, May 1999.

[36] Makoto Matsumoto and Takuji Nishimura. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Trans. Model. Comput. Simul.*, 8:3–30, January 1998.

[37] Anton Michlmayr, Florian Rosenberg, Philipp Leitner, and Schahram Dustdar. Comprehensive qos monitoring of web services and event-based sla violation detection. pages 1–6, 2009.

[38] Vivek Nallur and Rami Bahsoon. Design of a Market-Based Mechanism for Quality Attribute Tradeoff of Services in the Cloud . In *Proceedings of the 25th Symposium of Applied Computing(ACM SAC)*. ACM, 2010.

[39] Jinzhong Niu, Kai Cai, Simon Parsons, Enrico Gerding, and Peter McBurney. Characterizing effective auction mechanisms: insights from the 2007 tac market design competition. pages 1079–1086, 2008.

[40] Jinzhong Niu, Kai Cai, Simon Parsons, Peter McBurney, and Enrico Gerding. What the 2007 tac market design game tells us about effective auction mechanisms. *Autonomous Agents and Multi-Agent Systems*, 21:172–203, 2010. 10.1007/s10458-009-9110-0.

[41] P. Oreizy, N. Medvidovic, and R.N. Taylor. Architecture-based runtime software evolution. *Proceedings of the 20th International Conference on Software Engineering*, pages 177–186, 1998.

[42] Sarvapali D Ramchurn, Dong Huynh, and Nicholas R Jennings. Trust in multi-agent systems. *The Knowledge Engineering Review*, 19(01):1–25, 2005.

[43] a Roth and I Erev. Learning in extensive-form games: Experimental data and simple dynamic models in the intermediate term. *Games and Economic Behavior*, 8(1):164–212, 1995.

[44] Mazeiar Salehie and Ladan Tahvildari. Self-adaptive software. *ACM Transactions on Autonomous and Adaptive Systems*, 4(2):1–42, May 2009.

[45] Michael Stonebraker, Robert Devine, Marcel Kornacker, Witold

Litwin, Avi Pfeffer, Adam Sah, and Carl Staelin. An economic paradigm for query processing and data migration in mariposa. pages 58–67, 1994.
[46] Perukrishnen Vytelingum. *The Structure and Behaviour of the Continuous Double Auction*. PhD thesis, 2006.
[47] C.A. Waldspurger, T. Hogg, B.A. Huberman, J.O. Kephart, and W.S. Stornetta. Spawn: a distributed computational economy. *Software Engineering, IEEE Transactions on*, 18(2):103–117, feb. 1992.
[48] Carl A. Waldspurger and William E. Weihl. Lottery scheduling: flexible proportional-share resource management. page 1, 1994.
[49] Michael P. Wellman. A market-oriented programming environment and its application to distributed multicommodity flow problems. *J. Artif. Int. Res.*, 1(1):1–23, 1993.
[50] Danny Weyns, Sam Malek, and J. Andersson. On decentralized self-adaptation: lessons from the trenches and challenges for the future. In *Proceedings of the 2010 ICSE Workshop on Software Engineering for Adaptive and Self-Managing Systems*, pages 84–93. ACM, 2010.
[51] P Wurman. A Parametrization of the Auction Design Space. *Games and Economic Behavior*, 35(1-2):304–338, April 2001.
[52] L. Servi Y. C. Ho and R. Suri. A class of center-free resource allocation algorithms. *Large Scale Systems*, 1:51, 1980.
[53] Liangzhao Zeng, Boualem Benatallah, Marlon Dumas, Jayant Kalagnanam, and Quan Z. Sheng. Quality driven web services composition. *Proceedings of the twelfth international conference on World Wide Web - WWW '03*, page 411, 2003.
[54] Liangzhao Zeng, Boualem Benatallah, Phuong Nguyen, and Anne H. H. Ngu. Agflow: Agent-based cross-enterprise workflow management system. pages 697–698, 2001.
[55] Liangzhao Zeng, Hui Lei, and Henry Chang. Monitoring the qos for web services. pages 132–144, 2007.
[56] Wei Zhang, Carl K. Chang, Taiming Feng, and Hsin-yi Jiang. QoS-Based Dynamic Web Service Composition with Ant Colony Optimization. *2010 IEEE 34th Annual Computer Software and Applications Conference*, pages 493–502, July 2010.

A Secured Approach for Integrity Verification and Multikeyword Top-k retrieval in Cloud data

Priya. M
Master of Engineering
Department of Computer Science and Engineering
Raja college of Engineering and Technology
Sivagangai
Priyait30591@gmail.com

Mrs. H. Mari Ilang Selvi
Assistant Professor
Department of Computer Science and Engineering
Raja college of Engineering and Technology
Sivagangai
logonselvi@rediffmail.com

Abstract

Cloud computing is the technology which is used share the resources to the data centers over the internet on a pay for use basis. It is desirable to store the data on data storage servers. Even though, many searchable encryption schemes permit the users to securely search over encrypted data by using the keywords. To overcome the privacy issue such as the data leakage occurred on the cloud server, Two Round Searchable Encryption (TRSE) scheme has been used which supports for Top-k retrieval. Additionally, data integration problem may cause while transfer the file server. For that, the MD5 algorithm has introduced which will produce a 128 bit hash value and it allows us to create a hash calue from a file that can prove the integrity of the file, without storing it. It allows verify the integrity of the transmitted file by comparing the MD5 hash of the original file with the MD5 hash of the data that was received. As a result, the data integrity is ensured.

Keywords: Cloud, integrity, data privacy, relevance score, similarity relevance.

1. Introduction

Cloud computing is the dreamed vision of computing as a utility, which enables the cloud customers to remotely store their data onto the cloud and it is the indispensable viability to outsource their data from the cloud. In recent years, cloud storage service has become a faster profit growth point by providing a comparably low cost, scalable, position-independent platform for clients' data. It is desirable to store the data on data storage servers such as mail servers and file servers in an encrypted form to reduce security and privacy risks.so that the data storage servers must be fully trusted. To protect data privacy and to reduce unwanted accesses, the sensitive data has to be encrypted before outsourcing in order to provide end–to–end confidentiality assurance in the cloud and beyond. Hence, large number of data users can have access to their data stored on the cloud the data encryption becomes a very challenging task. In cloud computing, data owners may share their outsourced data with a large number of users. But, the data users are keen to retrieve only the data files they are interested in during a given session. In order to retrieve documents satisfying a certain search criterion, the user gives the server a capability that allows the server to identify exactly those documents. Document encryption, however, makes it hard to retrieve data selectively from the server. Consider, for example, a server that stores a collection of encrypted emails belonging to a user. The server is unable to determine the subset of encrypted emails defined by a search criterion. The keyword based search can be used to retrieve the files they are interested in. Although traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords without first decrypting it, these techniques support only conventional Boolean keyword search without capturing any relevance of the files in the search result. Advances in information retrieval have gone well beyond Boolean searches; scoring schemes have been widely employed to quantify and rank-order the relevance of a document to a set of query terms. To securely rank-order documents in response to a query, and develop techniques to extract the most relevant document(s) from a large encrypted data collection. To accomplish, collect term frequency information for each document in the collection to build indices, as in traditional retrieval systems for plaintext. Further secure these indices that would otherwise reveal important statistical information about the collection to protect against statistical attacks. During the search process, the

query terms are encrypted to prevent the exposure of information to the data center and other intruders, and to confine the searching entity to only make queries within an authorized scope. Utilizing term frequencies and other document information, apply cryptographic techniques such as order-preserving encryption to develop schemes that can securely compute relevance scores for each document, identify the most relevant documents, and reserve the right to screen and release the full content of relevant documents. When directly applied in large collaborative data outsourcing cloud environment, they may suffer from many drawbacks. On the one hand, inevitably sending back all the files. The other problem is that the lacking of effective mechanisms to ensure the file retrieval accuracy. Preventing the cloud from involving in ranking and entrusting all the work to the user is a natural way to avoid information leakage. However, the limited computational power on the user side and the high computational overhead precludes information security. In order to avoid the information leakage, the cloud has to do more work during the process of retrieval. The concepts used here are: Two Round Searchable Encryption and the Checksum method. In this scheme, the majority of work is done at the cloud while the user takes part in ranking, which guarantees top-k multikeyword retrieval over encrypted cloud data with high security and integrity.In this paper, mainly it dealt with the problem of integrity by uing the MD5 algoritgm which helps the data owner and the data user to create the hash value to ensure the integrity of the original file at the destination.

2. Architecture

We consider that the cloud system consisting of three different system known as cloud server, data owner, and data user that provides data services, as depicted in Fig. 1: data owner (O), data user (U), cloud server (S).

Data owner consisting of many files that they desire to retrieve on the cloud server in an encrypted form. Thus, the data owner has to create a searchable index I by using a set of m distinct keywords W= (w1,w2,...,wm) retrieved from the file collection, and store both the index I and the encrypted file collection on the cloud server. In the existing architecture, there is no technique used for the integrity problem. In this paper, I have dealt with the integrity problem that architecture has been illustrated in Fig. 2.The authorization between data owner and the data users has been done with the help of encryption technique. The user will generate a search request and submits the request with the help of the given keyword w. The search request will be submitted in the form of trapdoor Tw of the keyword w to the cloud server. This will be submitted to the cloud server and the server will be responsible for returning the desired files to the user. First of all, the data owner submits the collection of files to the cloud server in an encrypted form. While sending those files to the cloud server, he has to perform two tasks as follows. First one is, the search index is created and submits to the cloud server. Another one task is to calculate the checksum for each file and upload that too to the cloud server along with the files. After receiving the request from a user, the cloud server has to return the files to user which matches with the user request with secure ranked keyword search with integrity concern. The server should learn nothing about the file contents. The server performs the scoring process with the help of the search index I received from the data owner. This scoring result will be returned to the data owner in an encrypted form. The data owner has to

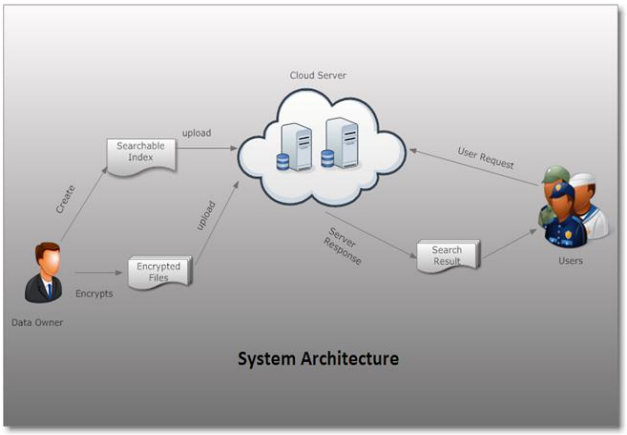


Figure 1. Retrieval of encrypted cloud data.

perform the ranking process by invoking the Top-k algorithm. This ranking result will be returned to the cloud server to retrieve the desired file. The cloud server then transfers the file to the data user. The data user calculates the checksum for the received file from the cloud server to ensure the integrity of the file. To do so, he has to compare the checksum for the received file and the checksum for the original file. If there any difference is made on the comparison result, we can conclude that the file has been modified. If the checksum calculated is same, we can sure that the file has not been modified.

3. TRSE design

The TRSE design consisting of the following algorithms: Setup, Index Build, TrapdoorGen, Score Calculate, and Rank

- *Setup*. The public keys and the secret keys are generated by the data owners.
- *Index Build.* The data owner creates the secure searchable index from the file collection C and applies the stemming and encryption to form the secure searchable index.
- *Trapdoor Gen*. The trapdoor is generated by the user from the request sent by the user. The request is encrypted into a secured trapdoor.
- *Score Calculate*. From the trapdoor, the cloud server performs the scoring operation and returns the resultant vector to the user.
- *Rank*. The resultant vector is decrypted by the user using the secret key and retrieves the files with top-k scores.
- *Verification*. The checksum is compared and the integrity is verified for the retrieved file.

4. Conclusion

In this paper, an initial attempt is to overcome the problem of supporting efficient ranked keyword search for efficiency is preserved by using the Top-k Retrieval mechanism and the integrity problem has been solved. By using the Order Preserving Searchable Encryption (OPSE), we can avoid the leakage of information and using the TRSE scheme, which fulfils the top-k retrieval over encrypted cloud data and also it will support for the multikeyword retrieval over the encrypted cloud data using the request from the user. The checksum is calculated to ensure the integrity of each file by using the MD5 algorithm. As a result, integrity is ensured and also the efficiency in retrieval can also be obtained.

Acknowledgement

The authors would like to thank the reviewers for their valuable comments that would help to improve this paper.

5. References

[1] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order Preserving Encryption for Numeric Data," *Proc. of SIGMOD*, Jun. 2004.

[2] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions,"http://www.techrunch.com/2006/12/28/gmail-disasterreports-of-madd-email-deletions/ ,Dec. 2006.

[3] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Order-preserving symmetric encryption," in *Proceedings of Eurocrypt'09, volume 5479 of LNCS*. Springer, 2009.

[4] R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Ecryption: Improved Definitions and Efficient Constructions," *Proc. ACM 13th Conf. Computer and Comm. Security (CCS), 2006.*

[5] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in *Proc. of ACNS'05*, 2005. in *Proc. of ACM CCS'06*, 2006.

[6] A. Singhal, "Modern information retrieval: A brief overview," *IEEE Data Engineering Bulletin*, vol. 24, no. 4, pp. 35–43, 2001.

[7] J. Zobel and A. Moffat, "Exploring the similarity space," *SIGIR Forum*, vol. 32, no. 1, pp. 18–34, 1998.

Green based Carbon Emissions Control for Cloud Infrastructure on Load Balancing

R.Kayathri[1]
First year M.E student[1,] Department of computer science and engineering,
[1] Renganayagi Varatharaj College of Engineering, Sivakasi.
[1]kayathriram49@gmail.com

Abstract—Large public cloud infrastructure can utilise power which is generated by a multiplicity of power plants. The cost of electricity will vary among the power plants and each will emit different amounts of carbon for a given amount of energy generated. This infrastructure services traffic that can come from anywhere on the planet. It is desirable, for latency purposes, to route the traffic to the data centre that is closest in terms of geographical distance, costs the least to power and emits the smallest amount of carbon for a given request. It is not always possible to achieve all of these goals so we model both the networking and computational components of the infrastructure as a graph and propose the Stratus system which utilises Voronoi partitions to determine which data centre requests should be routed to based on the relative priorities of the cloud operator.

Index Terms—Voronoi Partitions, Cloud Computing, Load Balancing, Carbon Emissions

1 INTRODUCTION

A variety of new services are being offered under the cloud computing paradigm. This service model involves a cloud based service provider (CBSP) providing a large pool of computational and network resources which are allocated on demand to the cloud users from the pool. Cloud users in turn can use these resources to provide services for users. The pool of resources can comprise of several data centres (DCs) at different geographical locations. There are many potential benefits to a global distribution of servers if load balancing is used correctly. Reduced latency and increased data transmission rates can be achieved by assigning clients to servers which are closer in terms of link distance. For some applications such as conference Voice-over-IP (VoIP) software and interactive online games low latency is critical in order to provide a satisfactory Quality of Service (QoS). In addition, there have been proposals to consider electricity price when load balancing [1], [2], [3] to reduce operational costs. By assigning more load to a DC which is utilising relatively cheap electricity operational costs can be lowered. This load balancing can be achieved with protocol-level mechanisms which are in use today such as dynamically generated DNS responses, HTTP redirection and the forwarding of HTTP requests. All of these have been evaluated thoroughly [4], [5], [6].

Recently the carbon emissions associated with powering DCs have become important. Greenpeace report [7] the carbon emissions of selected DCs and the percentage of their electricity generated by power plants
that use fuels which emit a relatively large amount of carbon. The carbon intensity of a power plant is the carbon emitted for a given amount of energy generated. The carbon intensity of power plants using particular fuels is detailed in [8], [9]. Currently there is little financial motivation to use green or clean energy but increasing regulation of carbon emissions and schemes like the European Union Emissions Trading Scheme (EU ETS) [10] mean that in the future it is probable that the right to emit carbon into the atmosphere will be traded as a commodity. In addition, recent work [11] suggests that on-site power generation can reduce carbon emissions and electricity cost by reducing the peak draw of a data centre from an electricity supplier.

There have been some proposals to use locally generated clean energy [12] or employ load balancing based upon the carbon intensity of the electricity supplier [13]. These proposals, however, do not consider the carbon emitted as a results of packets travelling across the network from the client to the server. While the energy consumed by the networking equipment as part of the cloud computing has been analysed [14], additional analysis is required to examine the total carbon emission caused by a cloud computing system.

In addition, other proposals for minimising carbon emissions use weather data as a metric for load balancing. While this is a useful metric for in-house generated electricity it can be inaccurate when electricity is obtained from an

external supplier as other factors affect their carbon intensity. This is discussed in greater detail in Section 5.2. Carbon emissions are seldom the sole concern of cloud operators and other factors must be considered. The electricity cost can vary considerably between different geographical regions and this fact can be exploited by cloud operators to lower the operational cost.

The manner in which a data centre is cooled can affect both the electricity cost and carbon emissions as certain schemes such as "free air cooling" require less energy and hence emit less carbon. Finally cloud operators are usually bound by service level agreement (SLA) and therefore must maintain a minimum QoS for service users.

It is not always possible to achieve the best case scenario for all of these factors as they sometimes conflict, so we formulate a graph-based approach which we call Stratus that can be used examine and control the operation of the cloud. Stratus uses Voronoi partitions which are a graph-based approach which have been used to solve similar problems in other areas such as robotics [15]. In this paper we use this approach to attempt to control the various factors which affect the operation of the cloud. This paper makes the following contributions:

- The development of a model which details the carbon emissions, electricity cost and time required for the computational and networking aspects of a service request.
- A distributed algorithm which minimises the combination of average request time, electricity cost and carbon emissions is described.
- Data for the carbon intensity and electricity price of various geographical regions and a representative set of round trip time between various geographical regions is presented.
- We evaluate the performance of our distributed algorithm using the data obtained for various scenarios.

2 RELATED WORK

There have been a number of proposals which consider the cost of electricity when determining which data centre should service requests. Qureshi et al. [1] proposed a distance-constrained energy price optimizer and presented data on energy price fluctuations and simulations illustrating the potential economic gain. Stanojevic et al. [2] detail a distributed consensus algorithm which equalises the change in the cost of energy. This is equivalent to minimising the cost of energy while maintaining QoS levels. Rao et al. [16] formulate the electricity cost of a cloud as a flow network and attempt to find the minimum cost of sending a certain amount of flow through this network. Rao et al. [17] also propose a control system which uses load balancing and server power control capabilities to minimize energy cost. Wang et al. [18] propose using a corrected marginal cost algorithm to minimize electricity cost. Mathew et al. [19] propose an algorithm which controls the number of servers online in the cloud to reduce energy consumption. It also maintains enough servers at each data center to handle current requests as well spare capacity to handle spikes in traffic. Liu et al. [3] propose distributed algorithms which minimize the sum of an energy cost and a delay cost using optimization techniques such as gradient projection to minimise the overall cost of operating the data centre. In addition, they expand their formulation to consider minimizing the sum of the social impact cost and delay cost. They define the social impact cost as a metric for environmental impact of the data centre. By examining the availability of renewable energy and directing load to the appropriate data centres they attempt to reduce the environmental impact of the data centre.

In addition, there has been some analysis of the electricity consumption of the cloud computing paradigm. Baliga et al. [14] analyse the power consumption of all the elements of this for a variety of service scenarios. Mahdevan et al. [20] examine the power consumption of network switches and consider techniques for improving the power efficiency of network switches by disabling ports and using lower data rates where possible.

There have also been some proposals which consider carbon emissions when determining where to direct service requests. Liu et al. [12] expand the model proposed in [3] to subtract locally generated clean energy from the energy cost calculation to allow data centres which have clean energy generation facilities to service more load. Doyle et al. [13] describe an algorithm that minimizes a cost function containing the carbon intensity of the electricity supplier of the data centre and average job time. Moghaddam et al. [21] attempt to use a genetic algorithm-based method with virtual machine migration to lower the carbon footprint of the cloud. Gao et al. [22] use a flow optimization based framework to control the three way trade-off between average job time, electricity cost and carbon emissions. This system, however, is only evaluated using yearly average carbon intensity values. While the system could be applied to the instantaneous carbon intensity value of an electricity supplier, the evaluation only considers the yearly average which can differ significantly from the instantaneous value.

Some of these proposals use various mathematical techniques to achieve their goals. In this work we propose the use of Voronoi partitions which are used in a number of areas. Aurenhammer details a number of applications in [23]. Durham et al. [15] use Voronoi partitions to divide an environment so that a group of robots can provide coverage.

This problem can be viewed as similar to a constrained version of the facility location problem which has been shown to be NP-hard [24]. Exact [25] and approximate [26] solvers for this problem have been thoroughly studied. These methods, however, are computationally expensive as any new demand points requires the solver to run the entire analysis from scratch. This works well for determining the

optimal site for the construction of a facility as the demand set is static. In the cloud, however, the demand for a service is constantly changing and a system that can respond to incremental change is required.

3 PROBLEM FORMULATIONS

In this section we formulate the problem. To do this we need some background notation. Namely we need to say what a graph is; what a Voronoi partition is; and how we use these ideas in the context of cloud computing.

3.1 Graph

A graph consists of a finite set of nodes and edges. Each edge is incident with two nodes. A path is an ordered sequence of points such that any consecutive pair of points is linked by an edge in the graph. In an undirected graph there is no direction associated with the edges. Hence, a path can be constructed with any edge in the graph. A weighted graph associates a label with each edge. Nodes are connected if a path exists between them.

3.2 Voronoi Partitions

Voronoi partitions are the decomposition of a set of points into subsets. These subsets are centered around points known as sites, generators or seeds. Each point in the set is added to a subset consisting of a site and all other points associated with this site. An abstract notion of distance between a point and the sites is used to determine which subset a point is associated with. A point is assigned to a subset if the distance to site is less than or equal to the distance to the other sites. For an example of Voronoi partitions used in applications (robotics) see [15].We shall now use these partitions to solve routing problem associated with load balancing in the cloud.

3.3 Voronoi Partitions of the Cloud

In our work the set of points consist of sources of requests for cloud services and data centres which service these. Voronoi partitions are then used to determine where requests are serviced. A Voronoi cell represents which sources of requests a data centre is servicing at a given time. An example of a group of sources of requests which have been partitioned between two data centres can be seen in Figure 1. In this figure each source of requests has a path to both data centres. The partition that the source of requests is a part of depends on the paths to the two data centres. The partitions are made up of sources of requests which have paths available to them with lower distances than the paths available to the other data centre.

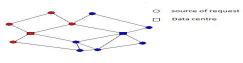


Fig. 1. Example of how sources of requests are partitioned between two data centres. Colour indicates that the node is part of a particular partition.

3.4 Problem Statement

Let |J| be a set of J geographically concentrated sources of requests and |N| be a set of N data centres. Let |Q| be a finite set of points that represent either sources of requests or data centres. These points are connected by E edges in an undirected weighted graph G = (|Q|; |E|; |w|). The weights are calculated as functions of the time required to service a fraction of the request Ti, the carbon emissions associated with servicing the fraction Gi and the electricity cost Ei if any associated with servicing the request along the edge. wi = f(Ti;Gi;Ei) = Ti + R1(Gi) + R2(Ei) where R1, R2 are the relative price functions which are used to specify the relative importance of the factors. While Ei and Gi are related, the rates at which they increase may vary significantly depending on the specifics of the cloud and hence, both must be included in the problem formation to ensure the cloud operator can operate the cloud as desired. It should be noted that the weights of the graph represent the networking and computational aspects of servicing a request.

4 CLOUD ANALYSIS

In this section we examine the variation in the costs that exist between data centres.

4.1 Electricity Cost

The price of electricity on the wholesale market depends on a number of factors. The wholesale electricity market is administered by an authority known as a Regional Transmission Organisation (RTO) in the United States and the Single Market Operator (SEMO) in Ireland. In this market, power producers present supply offers, consumers present bids and an authority in charge of the transmission network determines how the electricity should flow and sets prices. The price is determined based on the bids and offers as well as other factors such as reliability and grid connectivity. The variation of local electricity prices in different geographical regions can be exploited by cloud operators to lower operational costs [1]. To illustrate this we examine the potential savings that can be made by part of Amazons's EC2 [27] cloud. We examine the local prices of electricity suppliers located in the regions of the California, Virginia and

Ireland data centres. Pacific Gas and Electric (PG&E) is one supplier in the California region and Dominion (DOM) is a supplier in the Virginia region. We chose these as they supply electricity in the region the data centres are located. Ireland uses a single market for electricity known as SEMO and only a single price for wholesale electricity is available.

4.2 Carbon Emissions

An analysis of the carbon intensity of electricity suppliers in various geographical regions is useful when attempting to minimise the environmental impact of a cloud. To illustrate this we examine the carbon emitted by a service

which has users in a number of different geographical regions utilising the EC2 infrastructure.

The carbon intensity of an electricity supplier is calculated using the weighted average (where the power generated by the power plant is the weight used) of the carbon intensity of the power plants operated by the electricity supplier. The demand for electricity changes over the course of a day and electricity suppliers turn power plants on and off to react to the changes in the demand. A consequence of this is that the carbon intensity of an electricity supplier varies over time. It would be possible to estimate the realtime carbon intensity by examining the weighted average of the carbon intensity for all the power plants that are operating but some electricity suppliers provide a realtime carbon intensity value directly.

4.3 Cooling Cost

Cooling costs for a data centre are dependent on its design and the local climate in addition to the load placed upon it. If a data centre uses aisle containment [31] it can significantly reduce the cost of cooling the data centre. Aisle containment is the separation of the inlets and outlets of servers with a barrier such as PVC curtains or Plexiglas [32] in order to prevent air migration which adversely affects cooling costs. In addition "free air cooling" can be used. This is the use of air economizers to draw in cold air from the environment into the data centre when the climate conditions are suitable, thereby preventing the use of computer room air conditioner (CRAC) chiller units and lowering the cooling costs [33]. Water cooling [34], [35] can also be used but it is rarely used in data centres at present. In order to examine how this cost varies with demand we constructed two models of data centres in the computational fluid dynamics (CFD) simulation software Flovent [36]. These represent typical data centres which have been examined in previous research [37], [38]. One data centre used cold aisle containment and the other does not. Apart from this the data centres were of similar construction. Each data centre has dimensions 11.7m×8.5m×3.1m with a 0:6m raised floor plenum that supplies cool air through perforated floor tiles. There are four rows of servers with seven 40U racks in each case, resulting in a total of 1120 servers. The servers simulated were based on Hewlett-Packard's Proliant DL360 G3s model, which consumes 150W of power when idle and 285W at 100% utilization. From this we can determine that the total power consumption of the data centre is 168kW when idle and 319.2kW at full utilisation.

5 RESULTS

When comparing the best effort carbon scenario with the roundrobin baseline we can see that carbon emissions for a service can be reduced by 21%. If we examine the best effort electricity scenario and the roundrobin baseline we can see that the electricity cost can be reduced by 61%. There is, however, a corresponding increase in the average service request time of 7ms. If we investigate the best effort time scenario and the roundrobin baseline we can see that the average service request time can be reduced by 47%. It is also interesting to compare the three best effort scenarios. If we compare the best effort time scenario and the best effort carbon scenario we see that the latter emits 13% less carbon but has an average service request time that is 42ms higher. If we examine the best effort time scenario and the best effort electricity scenario we can see that the latter costs 58% less but has an average service request time that is 87ms higher. These comparisons are useful for the cloud operator as it allows them to see if the scenarios are feasible under SLAs and whether it is more desirable to concentrate on lower electricity costs or carbon emissions.

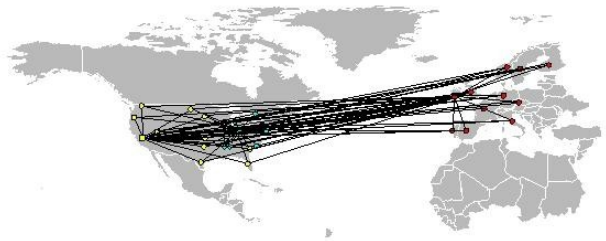


Fig. 2. Diagram of the simulation setup. The colour of the node indicates that the node is part of a particular partition.

6 CONCLUSION

We have shown that a cloud can be operated in such a manner to lower carbon emissions and operational cost. Our simulations show that there is a corresponding penalty in terms of average service request time if the cloud is run in such a fashion. Our work examines the electricity cost, carbon emissions and average service request time for a variety of scenarios. The decision concerning how to balance the various factors will depend on SLAs, government legislation and the price of carbon on trading schemes. Using this information and the specifics of the cloud the operator can run the cloud in the most desirable fashion. The nature of the service will determine if a cloud owner can implement this algorithm while conforming to service level agreements.

REFERENCES

[1] A. Qureshi, J. Guttag, R. Weber, B. Maggs, and H. Balakrishnan, "Cutting the electric bill for internet-scale systems," in Proceedings of ACM SIGCOMM, Barcelona, 17-21 August 2009, pp. 123–134.

[2] R. Stanojevi´c and R. Shorten, "Distributed dynamic speed scaling," in Proceedings of IEEE INFOCOM, San Diego, 14-19 March 2010, pp. 1–5.

[3] Z. Liu, M. Lin, A. Wierman, S. H. Low, and L. L. Andrew, "Greening geographical load balancing," in Proceeding of SIGMETRICS, San Jose, 7 June 2011, pp. 233–244.

[4] M. Conti, E. Gregori, and F. Panzieri, "Load distribution among replicated Web servers: a QoS-based approach," SIGMETRICS Performance Evaluation Review, vol. 27, no. 4, pp. 12–19, 2000.

[5] Z. M. Mao, C. D. Cranor, F. Bouglis, M. Rabinovich, O. Spatscheck, and J. Wang, "A precise and Efficient Evaluation of the Proximity between Web

Clients and their Local DNS Servers," in Proceedings of USENIX, Monterey, 10 – 15 June 2002, pp. 229–242.
[6] M. Pathan, C. Vecchiola, and R. Buyya, "Load and Proximity Aware Request-Redirection for Dynamic Load Distribution in Peering CDNs," in On the Move to Meaningful Internet Systems: OTM, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2008, vol. 5331, pp. 62–81.
[7] Greenpeace, "Make IT green cloud computing and its contribution to climate change," Retrieved February 2011, http://www.greenpeace.org/international/Global/international/planet2/report/2010/3/make-it-green-cloudcomputing.pdf.
[8] I. B. Fridleifsson, R. Bertani, E. Huenges, J. W. Lund, A. Ragnarsson, and L. Rybach, "The possible role and contribution of geothermal energy to the mitigation of climate change," O. Hohmeyer and T. Trittin (Eds.) IPCC Scoping Meeting on Renewable Energy Sources. Proceedings, pp. 59–80, 2008.
[9] M. Lenzen, "Life cycle energy and greenhouse gas emissions of nuclear energy: A review," Energy Conversion and Management, vol. 49(8), pp. 2178–2199, August 2008.
[10] "European Union Emissions Trading System," http://ec.europa.eu/clima/policies/ets/.
[11] chuangang Ren, D. Wang, B. Urgaokar, and A. Sivasubramaniam.
[12] Z. Liu, M. Lin, A. Wierman, S. H. Low, and L. L. Andrew, "Geographical load balancing with renewables," in Proceeding of GreenMETRICS, San Jose, 7 - 11 June 2011, pp. 1–5.
[13] J. Doyle, D. O'Mahony, and R. Shorten, "Server selection for carbon emission control," in Proceeding of ACM SIGCOMM Workshop on Green Networking, Toronto, 19 August 2011, pp.1–6.
[14] J. Baliga, R. W. A. Ayre, K. Hinton, and R. S. Tucker, "Green cloud computing: Balancing energy in processing, storage, and transport," Proceeding of the IEEE, vol. 99(1), pp. 149–167, 2011.
[15] J. W. Durham, R. Carli, P. Frasca, and F. Bullo, "Discrete Partitioning and Coverage Control for Gossiping Robots," IEEE Transactions on Robots, vol. 28, no. 2, pp. 364–378, 2012.
[16] L. Rao, X. Liu, L. Xie, and W. Liu, "Minimizing electricity cost: Optimization of distributed internet data centers in a multi-electricity-market environment," in Proceedings of IEEE INFOCOM, San Diego, 15 - 19 March 2010, pp. 1–9.
[17] L. Rao, X. Liu, M. D. Ilic, and J. Liu, "Distributed Coordination of Internet Data Centers Under Multiregional Electricity Markets," Proceedings of the IEEE, vol. 100, no. 1, pp. 269–282,2012.
[18] P. Wang, L. Rao, X. Liu, and Y. Qi, "D-Pro: Dynamic Data Center Operations With Demand-Responsive Electricity Prices in Smart Grid," IEEE Transactions on Smart Grid, vol. 3, no. 4, pp. 1743–1754, 2012.
[19] V. Mathew, R. K. Sitaraman, and P. Shenoy, "Energy-aware load balancing in content delivery networks," in Proceedings of IEEE INFOCOM, Orlando, 25 - 30 March 2012, pp. 954–962.
[20] P. Mahadevan, S. Banerjee, and P. Sharma, "Energy proportionality of an enterprise network," in Proceedings of ACM GreenNet, New Delhi, 30 August 2010, pp. 53–60.
[21] F. F. Moghaddam, M. Cheriet, and K. K. Nguyen, "Low Carbon Virtual Private Clouds," in Proceedings of IEEE International Conference on Cloud Computing, Washington DC, 4 - 9 July 2011, pp. 259–266.
[22] P. X. Gao, A. R. Curtis, B. Wong, and S. Keshav, "It's not easy being green," in Proceedings of SIGCOMM, Helsinki, 13 – 17 August 2012, pp. 221–222.

[23] F. Aurenhammer, "Voronoi Diagrams-a survey of a fundamental geometric data structure," ACM Computing Surveys, vol. 23,no. 3, pp. 345–405, September 1991.
[24] R. J. Fowler, M. S. PAterson, and S. L. Tanimoto, "Optimal packing and covering in the plane are NP-complete," Information processing letters, vol. 12, pp. 133–137, 1981.
[25] R. Z. Hwang, R. C. T. Lee, and R. C. Chang, "The slab dividing approach to solve the Euclidean p-center problem," Algorithmica.
[26] T. F. Gonzalez, "Clustering to minimize the maxium intercluster distance," Theoretical Computer Science, vol. 38, pp. 293–306, 1985.
[27] Amazon, "Elastic Compute Cloud," http://aws.amazon.com/ec2.
[28] "Carbon Monitoring for Action," http://carma.org/.
[29] United States Environmental Protection Agency, "eGRID," http://www.epa.gov/cleanenergy/energyresources/egrid/index.html.
[30] Eirgrid, http://www.eirgrid.com.
[31] Mikko Pervil¨a and Jussi Kangasharju, "Cold air containment," in Proceedings of ACM SIGCOMM Workshop on Green Networking, Toronto, 19 August 2011, pp. 7–12.
[32] L. A. Barroso and U. H¨ olzle, "The datacenter as a computer: An introduction to the design of warehouse-scale machines," Synthesis Lectures on Computer Architecture, 2009.
[33] D. Atwood and J. G. Miner, "Reducing data center cost with an air economizer," August 2008, http://www.intel.com/content/www/us/en/data-centerefficiency/data-center-efficiency-xeon-reducing-data-centercost-with-air-economizer-brief.html.
[34] P. Rumsey, "Overview of liquid cooling systems," 2007,http://hightech.lbl.gov/presentations/Dominguez/5 LiquidCooling 101807.
[35] A. Almoli, A. Thompson, N. Kapur, J. Summers, H. Thompson, and G. Hannah, "Computational fluid dynamic investigation of liquid rack cooling in data centres," Applied Energy, vol. 89, pp. 150–155, 2012.
[36] M. G. Corporation, "Flovent version 9.1," Wilsonville, Oregon, USA, 2010.
[37] R. K. Sharma, C. E. Bash, and C. D. Patel, "Balance of power: Dynamic thermal management for internet data centers," IEEE Internet Computing, vol. 9(1), pp. 42–49, 2005.
[38] J. Moore, J. S. Chase, P. Ranganathan, and R. Sharma, "Making scheduling "Cool": Temperature-aware workload placement in data centers," in Proceedings of USENIX, Anaheim, 10-15 April 2005, pp. 61–75.
[39] B. Chun, D. Culler, T. Roscoe, A. Bavier, L. Peterson, M. Wawrzoniak, and M. Bowman, "PlanetLab: an overlay testbed for broad-coverage services," SIGCOMM Computer Communication Review, vol. 33, no. 3, pp. 3–12, 2003.
[40] Social Bakers, "Social bakers the recipe for social marketing success," http://www.socialbakers.com/facebook-statistics/.
[41] Internet World Stats, "Internet world stats usage and population statistics," http://www.internetworldstats.com.
[42] M. Alizadeh, A. Greenberg, D. A. Maltz, J. Padhye, P. Patel, B. Prabhakar, S. Sengupta, and M. Sridharan, "Data center TCP (DCTCP)," in Proceeding of SIGCOMM, New Delhi, 30 August- 3 September 2010, pp. 63–74

Improving Resilience of Cloud Application Using Ranking Technique

M.Anand[1] ,R.Kanniga Devi[2]

1 PG Student, Department of Computer Science and Engineering, Kalasalingam University, Tamil Nadu, India,
anandsrmuniv@gmail.com
2 Department of Computer Science and Engineering, Kalasalingam University, Tamil Nadu, India,
rkannigadevi@gmail.com

Abstract— Cloud computing is a general term for anything that involves delivering hosted services over the Internet. A Fault tolerance is a setup or configuration that prevents a computer or network device from failing in the event of an unexpected problem or error. In this project work, we propose a model to analyze an optimal fault tolerant strategy to improve the resilience of cloud applications. The cloud applications are usually large scale and include a lot of distributed cloud components. Building highly efficient cloud applications is a challenging and critical research problem. To attack this challenge a component ranking frame work, named FTCloud is used for building fault tolerant cloud applications. First extract the components from the cloud application. Then, rank the critical components using the significance value. After the component ranking phase, an algorithm is projected to automatically conclude an optimal fault-tolerance strategy for the significant cloud components. Thereby, resilience of cloud application can be improved.

Keywords— Cloud application, component ranking technique, fault tolerance

1. INTRODUCTION

Cloud is a general term for anything that involves delivering hosted services over the Internet. It is getting popular in recent years. The software systems in the cloud (named as cloud applications) typically involve multiple cloud components communicating with each of them [1]. Basically cloud applications are usually huge and very complex. Regrettably, the reliability of the cloud applications is still far from perfect in real life. The requirement for highly reliable cloud applications is becoming unprecedented strong. Building highly efficient clouds becomes a critical, challenging, and urgently required research problem. The trend toward large-scale complex cloud applications makes developing fault-free systems by only employing fault-prevention techniques and fault-removal techniques exceedingly difficult. Another approach for building efficient systems, software fault tolerance [20], makes the system more robust by faults masking without removing it. One of the most well known software fault tolerance techniques is to employ functionally equivalent yet independently designed components to tolerate faults [5]. Due to the cost of developing and maintaining redundant components, software fault tolerance is usually only employed for critical systems. Different from traditional software systems, there are a lot of redundant resources in the cloud environment, making software fault tolerance a possible approach for building highly reliable cloud applications. Since cloud applications usually involve a large number of components, it is still too expensive to provide alternative components for all the cloud components. Moreover, there is probably no need to provide fault tolerance mechanisms for the non critical components, whose failures have limited impact on the systems. To reduce the cost so as to develop highly reliable cloud applications within a limited budget, a small set of critical components needs to be identified from the cloud applications. By tolerating faults of a small part of the most important cloud components, the cloud application reliability can be greatly improved. Based on this idea, we propose FTCloud, which is a component ranking framework for building fault tolerant cloud applications. the optimal fault-tolerance strategies for these significant components automatically. FTCloud can be employed by designers of cloud applications to design more reliable and robust cloud applications efficiently and effectively.

Contribution of this paper:

. This paper identifies the critical problem of locating significant components in complex cloud applications and proposes a ranking-based framework, named FTCloud, to build fault-tolerant cloud applications. We first propose ranking algorithms to identify significant components from the huge amount of cloud components. Then, we present an optimal

fault-tolerance strategy selection algorithm to determine the most suitable fault-tolerance strategy for each significant component. We consider FTCloud as the first ranking-based framework for developing fault-tolerant cloud applications.

We provide extensive experiments to evaluate the impact of significant components on the reliability of cloud applications.

2. RELATED WORK

Component ranking is an important research problem in cloud computing [41], [42]. The component ranking approaches of this paper are based on the intuition that components which are invoked frequently by other important components are more important. Similar ranking approaches include Google Page rank [7] (a ranking algorithm for web page searching) and SPARS-J [16] (software product retrieving system for Java). Different from the Page Rank and SPARS-J models, component invocation frequencies as well as component characteristics are explored in the approaches. Moreover, the target of approach is identifying significant components for cloud applications instead of web page searching (Page Rank) or reusable code searching (SPARS-J).

Cloud computing [3] is being popular. The works have been done on cloud computing, including identifies the critical to address fault tolerant strategy [32], identifies the effects of failures on user's applications, and surveying fault tolerance solutions corresponding to each class of failures [9], Too inadequate or too expensive to fit their individual requirements [34], etc. In recent years, a great number of research efforts have been performed in the area of service component selection and composition [30]. Various approaches, such as QoS-aware middle ware [38], adaptive service composition [2], and efficient service selection algorithms [37], have been proposed. Some recent efforts also take subjective information (e.g., provider reputations, user requirements, etc) to enable more accurate component selection [27]. Instead of employing non functional performance (e.g., QoS values) or functional capabilities, the approaches rank the cloud components considering component invocation relationship, invocation frequencies, and component characteristics.

.

3. SYSTEM ARCHITECTURE

Fig.1shows the system architecture of the fault-tolerance framework (named FTCloud), which includes two parts: 1) ranking and 2) optimal fault-tolerance selection. The procedures of FTCloud are as follows:

1. The system designer provides the initial architecture design of a cloud application to FTCloud. A component extraction can be done for the cloud application based on the weight value.

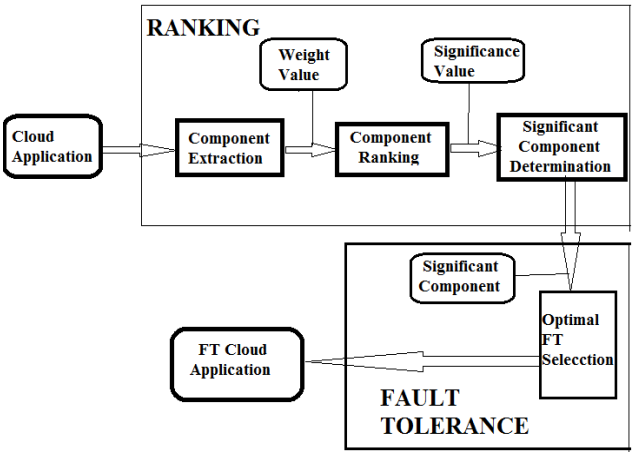


Figure:1- System Architecture

2. Significance values of the cloud components are calculated by employing component ranking algorithms. Based on the significance values, the components can be ranked.
3. The most significant components in the cloud application are identified based on the ranking results.
4. The performance of various fault-tolerance strategy candidates is calculated and the most suitable fault-tolerance strategy is selected for each significant component.
5. The component ranking results and the selected fault-tolerance strategies for the significant components are returned to the system designer for building a reliable cloud application.

4. PROPOSED WORK

4.1. SIGNIFICANT COMPONENT RANKING:

The target of significant component ranking algorithm is to measure the importance of cloud components based on available information (e.g., application structure, component invocation relationships, component characteristics, etc.).The significant component ranking includes three steps (i.e., component Extraction, component ranking, and significant component determination)

4.1.2. Component Extraction:

A cloud application can be modeled as a weighted, where a node c_i represents a component and a directed edge e_{ij} from node c_i to node c_j represents a component

invocation relationship, i.e., c_i invokes c_j. Each node c_i has a nonnegative significance value $V(c_i)$, which is in the range of (0,1). Each edge e_{ij} has a nonnegative weight value $W(e_{ij})$, which is in the range of [0,1]. The weight value of an edge e_{ij} can be calculated by

$$W(e_{ij}) = frq_{ij} / \sum_{j=1}^{n} frq_{ij} \quad (1)$$

Where frq_{ij} is the invocation frequency of component c_j by component c_i, n is the number of components, and $frq_{ij} = 0$ if component c_i does not invoke c_j. In this way, the edge e_i has a larger weight value if component c_j is invoked more frequently by component c_i compared with other components invoked by c_i. For a component extraction, C which contains n components, an n * n transition probability matrix W can be obtained by employing (1) to calculate the invocation weight values of the edges. Each entry w_{ij} in the matrix is the value of $W(e_{ij})$. $w_{ij} = 0$ if there is no edge from c_i to c_j, which means that c_i does not invoke c_j. If a component does not invoke itself, $w_{ii} = 0$. Otherwise, the value of w_{ii} can be calculated by (1). In the case that a node c_i has no outgoing edge, $w_{ij} = 1\backslash n$. For i, a single component of an application, C can be obtained by weight of an edge, $W(e_{ij})$

$$C = \forall i. \sum_{j=1}^{n} W(e_{ij}) \quad (2)$$

4.1.3. Component Ranking:

Based on the component extraction, a component ranking algorithms, named as FTCloud is proposed in this section. It employs the system structure information (i.e., the component invocation relationships and frequencies) for making component ranking and also considers the component characteristics (i.e., critical components or noncritical components) for making component ranking.Figure: 2 shows the critical and non crical components based on significance value.

4.1.4. FTCloud-Based Component Ranking:

In a cloud application, some of the components are considered to be more important which are frequently invoked by a lot of other components. Since their failures will have greater impact on the whole system. Probably, the significant components in a cloud application are the ones which have many invocation links coming in from the other important components. Inspired by the PageRank algorithm [7], we propose an algorithm to calculate the significance values of the cloud components applying the component invocation relationships and frequencies. The procedure of FTCloud-based component ranking algorithm is shown in the following steps:

1. Randomly assign initial numerical scores between 0 and 1 to the components
2. Compute the significance value for a component c_i by:

$$V(c_i) = (1-d)/n + d\sum_{k} \epsilon N(c_i) V(c_k) W(e_{ki}) \quad (3)$$

Where n is the number of components and $N(c_i)$ is a set of components that invoke component c_i. The parameter d ($0 \leq d \leq 1$) in (3) is employed to adjust the significance values derived from other components, so that the significance value of c_i is composed of the basic value of itself (i.e.,$(1-d)/n$) and the derived values from the components that invoked c_i. By (3), a component c_i has larger significance value indicating that component c_i invoked by a lot of other significant components frequently.

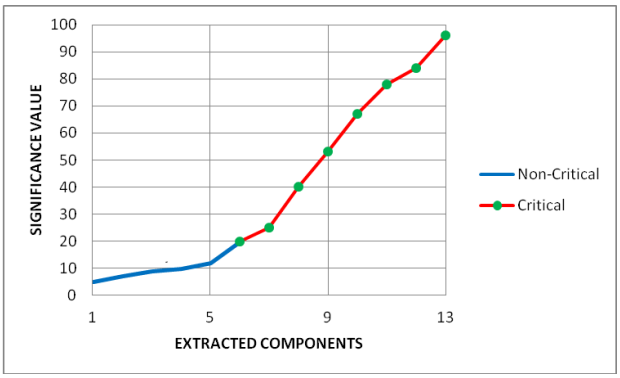


Figure:2- Significant Component Identification

4.1.5. Significant Component Determination

The components of cloud application can be ranked based on obtained significance value and the top k ($1 \leq k \leq n$) most significant components can be returned to the cloud application's designer. After that significant components can be obtained by the designer of cloud application at a time of architecture design and can employ various techniques to improve the resilience of the cloud application.

4.2. FAULT-TOLERANCE STRATEGY SELECTION

4.2.1 Fault-Tolerance Strategies

Software fault tolerance is widely adopted to increase the overall system reliability in cloud applications. Applying functionally equivalent components to tolerate component failures, thereby resilience can be improved. There are three most common

fault-tolerance methods with formulas to find out the failure probabilities of the each fault-tolerant method. The failure probability should be within the range of [0,1].

4.2.2. Recovery block(RB).

Execute a component, if fails through acceptance test, then try a next alternate component. Order the different component according to reliability. Checkpoints needed to provide valid operational state for subsequent versions (hence, discard all updates made by a component). Acceptance test needs to be faster and simpler than actual code. A recovery block fails only if all the redundant components fail.

The failure probability f of a recovery block :

$$f = \prod_{i=1}^{n} f_i \quad (4)$$

Where n is the number of alternate components and fi is the failure probability of the ith component.

4.2.3. N-version programming (NVP).

N-version programming, also known as multi version programming, all versions designed to satisfy same basic requirement. Decision of output comparison based on voting. Different teams build different versions to avoid correlated failures. When applying the NVP approach to the cloud application's component, implement the equivalent function of cloud components should be alone and involved in parallel and then final result is determined by majority voting. It will fail only if more than half of the redundant components stop working. The failure probability fi of an NVP module can be computed.

$$f = \sum_{i=(n+1)/2}^{n} F_i \quad (5)$$

Where n is the number of equivalent components (n is usually an odd number in NVP)

4.2.4. Parallel.

Parallel strategy invokes all the n functional equivalent components in parallel and the first returned response will be employed as the final decision. It fails only if all the alternate components stop working. The failure probability f of a parallel module can be computed by

$$f = \prod_{i=1}^{n} f_i \quad (6)$$

Where n is the number of alternate components and fi is the failure probability of the ith component.

Different features of fault tolerance strategies, the response time of RB and NVP strategies is not good compared with Parallel strategy in performance wise, while Parallel strategy employs the first returned response as the final decision. The required resources of RB are much lower than those of NVP and Parallel since parallel component invocations consume a lot of networking and computing resources. RB, NVP, and Parallel strategies can tolerate crash faults. NVP can also mask value faults (e.g., data corruption), the final results in NVP can be determined through majority voting.

4.2.5. Optimal FT Strategy Selection

The fault-tolerance strategies have a number of variations based on different setups. Fault tolerance method variations are applied for each and every single significant component in a cloud application and the optimal one need to be identified. For each significant component that requires a fault tolerance strategy, the designer can specify constraints (e.g., response time of the component has to be smaller than 1,000 milliseconds, etc.).Response time and cost are the two user constraints should be noted. The optimal fault-tolerance method selection problem for a cloud component with user constraints can then be formulated mathematically. First, the candidates which cannot meet the user constraints are not include. Then the fault-tolerance candidate with the best failure probability performance will be selected as the optimal strategy for component i. By the above approach, the optimal fault-tolerance method, gives the best failure probability performance and fulfill all the user constraints.

To identify optimal FT Strategy Selection:

Input: si, ti, and fi values of candidates; user constraints u1, u2;
Output: Optimal candidate index p
m: number of candidates;
for (i =1; i ≤ m; i++) do
if (si≤ u1&&ti ≤u2) then
vi = fi;
end
end
if none of the candidate meet user constraints after that
Throw exception;
end
Select vx which has minimal value from all the vi;
P= x;

Algorithm1. Optimal FT Strategy Selection

The above algorithm identifies optimal FT strategy selection for each of significant component. Based on result the designer have to apply the identified FT strategy, thus resilience of the cloud application can be improved.

5. EXPERIMENTS

5.1. Experimental Setup

The significant component ranking algorithms are implemented by java language using cloudsim tool based on hundred nodes. To find out the performance of reliability increment, we compare four approaches, which are as follows:

No FT: No fault-tolerance strategies are employed for the components in the cloud application.

Random FT. Fault-tolerance strategies are employed to mask faults of K percent components, those components are randomly selected.

FTCloud: Fault-tolerance strategies are employed to mask faults of the Top-K percent important components (using significance value). The components are ranked based on the structural information of the cloud application.

AllFT: Fault-tolerance strategies are employed for all the cloud components.

6. Component Failure Probability Impact

To learn the impact of the system resilience on cloud application, we compare RandomFT and FTCloud under probability set from 0.1 to 1 percent with a step value of 0.1 percent. Thousands node are taken for this execution. Implementation result shows cloud application failure probabilities Fig. 3.

Fig. 3 explains

FTCloud outperform RandomFT in all the application running time settings from 1 percent constantly as shown in Fig. 3

. The system resilience probabilities of the two methods become larger, when application runs. To build highly reliable cloud applications, then a larger number of significant components are needed.

. The application failure probability of FTCloud approach decreases much faster than that of RandomFT, representing that have a more efficient use of the redundant components than RandomFT, by the increase the selection of more significant components.

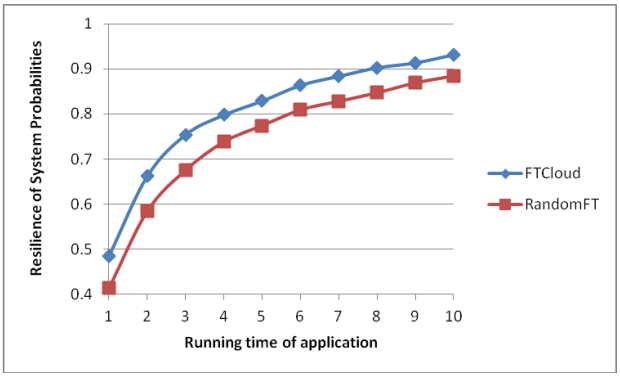


FIGURE: 3- The impact of the system resilience

7. CONCLUSION AND FUTURE WORK

This paper proposes a component ranking framework cloud application's component. The significance values of these components, how often the current component is called by other components, and the component quality.

After determine the significant components, we suggest an optimal fault-tolerance strategy selection algorithm to afford optimal fault-tolerance strategies to the significant components automatically, based on the user limits. The implementation results display the FTCloud approaches.

The current FTCloud framework can be engaged to bear crash and significance faults. In the future, we will examine more types of faults, such as Byzantine faults. Various types of fault-tolerance mechanisms can be extra into FTCloud framework effortlessly without Basic changes. We will also examine additional component ranking algorithms and add them to the FTCloud framework. Moreover, we will expand and practical FTCloud framework to other component-based systems.

In this paper, we only learn the most delegate type of software component extraction, i.e., weight value of an edge. as different applications may have dissimilar system structures, we will examine more types of component models in future work.

The future work also includes

- Allow more factors (such as invocation delay, output, etc.) when computing the weights of invocations links;
- Examining the component consistency itself moreover the invocation structures and invocation frequencies;
- More investigational testing on real-world cloud applications.
- more examination on the component malfunction correlations; and
- More new studies on collision of incorrectness of prior wisdom on the invocation frequencies and essential components.

REFERENCE

[1] "cloud computing in wikipedia," http://en.wikipedia.org/wiki/cloud_computing, 2012.

[2] d. Ardagna and b. Pernici, "adaptive service composition in flexible processes," june 2007.

[3] m. Armbrust et al., "a view of cloud computing," 2010.

[4] m. Armbrust et al., "above the clouds: a berkeley view of cloudcomputing," 2009.

[5] a. Avizienis, "the methodology of n-version pro-gramming," software fault tolerance, 1995.

[6] v. Batagelj and a. Mrvar, "pajek - program for large network analysis," 1998.

[7] s. Brin and l. Page, “the anatomy of a large-scale hypertextual web search engine,” 1998.
[8] m. Creeger, “cloud computing: an overview,”, june 2009.
[9] Huang and Abraham, “Providing Reliability as an Elastic Service in Cloud Computing”, 2011.
[10] a.p.s. de moura, y.-c. Lai, and a.e. motter, “signatures of small- world and scale-free properties in large computer programs,” 2003.
[11] c.-l. Fang, d. Liang, f. Lin, and c.-c. Lin, “fault tolerant web services,” 2007.
[12] s.s. gokhale and k.s. trivedi, “reliability prediction and sensitivity analysis based on software architecture,” 2002.
[13] s. Gorender, r.j. de araujo macedo, and m. Raynal, “an adaptive programming model for fault-tolerant distributed computing,” jan.-mar. 2007.
[14] a. Goscinski and m. Brock, “toward dynamic and attribute-based publication, discovery and selection for cloud computing,”, 2010.
[15] d. Hyland-wood, d. Carrington, and y. Kaplan, “scale-free nature of java software package, class and method collaboration graphs,” 2009.
[16] k. Inoue, r. Yokomori, t. Yamamoto, m. Matsushita, and s. Kusumoto, “ranking significance of software components based on use relations,” mar. 2009.
[17] k. Kim and h. Welch, “distributed execution of recovery blocks: an approach for uniform treatment of hardware and software faults in real-time applications,” may 1989.
[18] j. Laprie, j. Arlat, c. Beounes, and k. Kanoun, “definition and analysis of hardware- and software-fault-tolerant architectures,” july 1990.
[19] w. Li, j. He, q. Ma, i.-l. Yen, f. Bastani, and r. Paul, “a framework to support survivable web services,” 2005.
[20] m.r. lyu, software fault tolerance, wiley, 1995.
[21] m.r. lyu, handbook of software reliability engineering. Mcgraw-hill, 1996.
[22] e. Maximilien and m. Singh, “conceptual model of web service reputation,”2002.
[23] m.g. merideth, a. Iyengar, t. Mikalsen, s. Tai, i. Rouvellou, and p. Narasimhan, “thema: byzantine-fault-tolerant middleware forweb-service applications,” 2005.
[24] s.l. pallemulle, h.d. thorvaldsson, and k.j. goldman, “byzantine fault-tolerant web services for n-tier and service oriented architectures,” 2008. Zheng et al.: component ranking for fault-tolerant cloud applications.
[25] b. Randell and j. Xu, “the evolution of the recovery block concept,” software fault tolerance, m.r. lyu, , wiley,1995.
[26] p. Rooney, “microsoft’s ceo: 80-20 rule applies to bugs, not just features,” oct. 2002.
[27] s. Rosario, a. Benveniste, s. Haar, and c. Jard, “probabilistic qos and soft contracts for transaction-based web services orchestrations,” oct. 2008.
[28] j. Salas, f. Perez-sorrosal, m. Patin˜ o-marti´nez, and r. Jime´nez-peris, “ws-replication: a framework for highly available webservices,” 2006.
[29] g.t. santos, l.c. lung, and c. Montez, “ftweb: a fault tolerant infrastructure for web services,” 2005.
[30] q.z. sheng, b. Benatallah, z. Maamar, and a.h. ngu, “configurable Composition and adaptive provisioning of web services,” jan.-mar.2009.
[31] g.-w. Sheu, y.-s. Chang, d. Liang, s.-m. Yuan, and w. Lo, “afault-tolerant object service on corba,” 1997.
[32] Jing Deng and Wang et al, “Fault-Tolerant and Reliable Computation in Cloud Computing”, 2011.
[33] w.-t. Tsai, x. Zhou, y. Chen, and x. Bai, “on testing and evaluating service-oriented software,” aug. 2008.
[34] Mei et al and cho li wang,“Web product ranking using opinion mining”, 2011.
[35] g. Wu, j.wei, x. Qiao, and l. Li, “a bayesian network based qos assessment model for web services,” 2007.
[36] s.m. yacoub, b. Cukic, and h.h. ammar, “scenario-based reliability analysis of component-based software,” 1999.
[37] t. Yu, y. Zhang, and k.-j. Lin, “efficient algorithms for web services selection with end-to-end qos constraints,” 2007.
[38] l. Zeng, b. Benatallah, a.h. ngu, m. Dumas, j. Kalagnanam, and H. Chang, “qos-aware middleware for web services composition,” may2004.
[39] z. Zheng and m.r. lyu, “a distributed replication strategy evaluation and selection framework for fault tolerant web services,” 2008.
[40] z. Zheng and m.r. lyu, “a qos-aware fault tolerant middleware for dependable service composition,” 2009.
[41] z. Zheng, y. Zhang, and m.r. lyu, “cloudrank: a qos-driven component ranking framework for cloud computing,” 2010.
[42] z. Zheng, t.c. zhou, m.r. lyu, and i. King, “ftcloud: a ranking-based framework for fault tolerant cloud applications,” 2011

An Active Storage Framework Based On Storage Security In Cloud Computing

KARTHIKA.M
B.TECH-Information Technology
Latha Mathavan Engineering College
Madurai,
mkarthika93@gmail.com

RUKSHANA BEGUM.N
B.TECH-Information Technology
Latha Mathavan Engineering College
Madurai,
rukshananasarkhan@gmail.com

Abstract— **Cloud computing is the notion of outsourcing on-site available services and data storage to an off-site. Data stored in cloud contains personal information and that could be used by unauthorized person. This is due to the cached copy available at the cloud service provider cache memory. Self destruction method protects data's privacy by sanitizing the data after its usage. Both the confidential data and its copies are destroyed and unreadable after certain user's specified time. Key used for encryption and decryption also gets vanished. In this paper, active storage framework provides virtualization environment to run client's application and data is treated as objects to increase the throughput and decrease the latency.**

Index Terms— **confidential data privacy, object based activestorage, self-destructing data, Vanishing data.**

I. INTRODUCTION

Cloud computing is mainly used to solve the storage and maintenance problem. Cloud storage offers online storage and accesses it from anywhere and at any time. Few of the services in cloud render by service providers. In private cloud they have their own storage area. File lost problem is solved by the file backup process in peer to peer system. In the distributed system archived, cached, copies of the file is available at many peers. Any of the peers can act as a server to the service providers. So the copies are available forever after downloaded the required confidential file. The copies resides in the peer are in readable form. Here, limited the excessive amount or replication is required. Users are unaware of those copies available at the cache memory of the service providers. They cannot have control over the data. Such copies of the file are maintained by the service provider against accidental, legal and malicious attacks. In P2P system secret key is stored with distributed hash table (DHT). In distributed hash table it must be ensure that key actually stores the data associated with the key in each node. Routing attacks, storage and retrieval attacks violates data privacy in DHT. Sybil attacks create the fake entities and gains reputation from the honest entities.

For sharing the files and protecting privacy the concept called vanish is introduced. Vanish encapsulates the file with the pre-defined timeout. It is resistant to the attacks in viseDHT which is a centralized system. This is achieved by encrypting data with the random symmetric key and the key is not revealed to the user. Key is broken into multiple pieces and sprinkled across random nodes; distribute the key across the randomly chosen node in peer-to-peer system and finally the needed information for key retrieval is gathered to retrieve the key pieces with the encrypted data. Vanish system prevents the key pieces to be retrieved after the specified timeout.

The proposed concept in this paper is self-destructing data. There is an extensible framework for integrating multiple key-storage mechanism into a single self-destructing data system. It has the different key storage approaches to provide security against the attacks. In self-destructing data system all copies of the data permanently unreadable at the user specified time. Goals for self-destructing data are an attacker retroactively obtains a copy of the data and any relevant cryptographic keys from before the timeout there is no use because the specific data and its key are destroyed automatically, without the use of any explicit delete action by any parties involved the data disappear by its own, without need to modify any of the copies of the data, without the use of secure hardware and without relying on new and trusted external services, it provides the receiver with the minimum knowledge needed to consume the data. Our prototype attempts to meet these goals through the use of various cryptographic techniques. To increase the processor performance and to reduce the cost, object based storage system is needed. Object storage disk provides interaction between the operating system and

the storage system in the abstraction level. It separates the data and metadata to increase the throughput. It performs computation in parallel using distributed storage nodes. In active storage portion of the application is run directly on the hard disk. It reduces the data traffic and increases the processing speed.

I. RELATED WORK

In this section, we discuss related works on self-destruction of data and object based active storage. DHT [1] implements the services of the remote hash table and provides internal coordination among the nodes in peer-to-peer network. Some of the properties are scalable, distributed, decentralized and self-managing. Adenoma a privacy preserving method for mobile devices and vanish a method for creating self-destructing data. DHT [7] is exposed to attacks such as byzantine attacks, node crawling attacks and information harvesting attacks. Active Storage unit increase the process capability, reduces the data movement while searching and possible to read, write and execute the data directly on active storage. It improves host processing performance. It offers local control over the data. It checks the availability of resources and maintains the load. Computational process depends on hardware capabilities and load condition in active storage. The disadvantages are; large scale storage system aggregates many disks [2]. It has the problem of bandwidth limitation.

Object based active storage framework is built upon iSCSI OSD standards. Many data-intensive applications have small CPU and memory requirements and are attractive for execution across Active Disks. Implementing this in the form of objects allows for better portability, reusability of components, extensibility and other such advantages of object oriented programming. Object-based Storage devices have the capability of managing their storage capacity and shows file-like storage ”objects” to their hosts. These objects behave exactly like files. They can be created and destroyed and can grow and shrink their size during their lifetimes. The idea of moving the portion of application and make it to run directly on the disk. It has to be done to reduce data traffic. The client side of our application was designed to have APIs for multiple operations on an object that can exploit the parallelism offered by such a framework. The problem here is framework which does not supports any kind of objects. Currently the application supports only the list objects. User objects are placed in partitions that are represented by partition objects [3]. The average sort time is the average time required on each target node to do the read from disk and then sort. Storage administration costs will be higher than the cost of the storage systems themselves.

Vanish a system for creating messages that automatically destroy data after a period of time. It encrypts the message using the random key. Key shares are stored at the public distributed hash table. The hash table contains name, value pair. DHT deletes data and its key shares. Data is permanently available in the data is destroyed automatically. Length of the key shares depends on the key length [4]. The problem in the existing system is deployed vanish implementation is insecure. Here is a possibility of Sybil attacks. Attack occurs in the distributed hash table. Attacker able to hack the key before it ages out. In Sybil attacks the attacker pretends like user. Sybil attack is more expensive. In public DHT any peers act as a server. User trusted that vanish deletes data. So they are not deleting the sensitive data periodically [5]. Deployment of vanish does not provide the assured automatic deletion. Attacker cannot able to understand the user’s traffic towards the DHT. Vuze nodes replicate nearby 20 nodes. The solution to the above mentioned problems are using Shamir secret key it breaks the key into many n shares. If we recover the n-1 part of the key then only we can recover the data. It stores the key in the random indices. It avoids hacker to hack the entire part of the data. Vanishing data object retrieves the original plain text before expiration. Itthe private data. Third party is used to prevent the threat. Attacker cannot able to read more than the small fraction of the data.

MVSS is a storage system for active storage framework. MVSS offers a single framework for supporting various services at the device level. It provides a flexible interface for associating services to the file through multiple views of the file. Views in MVSS are generated dynamically and not stored in the physical storage. MVSS represents each view of an underlying file through the separate entry in the file system namespace. [6] MVSS separates the deployment of services from file system implementation and thus allows services to be migrated to the storage devices. Improve the storage devices performance, functions and characteristics by migrating services to disks. Direct network attachment is suggested to enable data transfer from device directly to the client rather than the server. The main advantage of disk storage is parallelism among disks and more aggregate CPU power at the disk than at the server. Active disks have the ability to reduce the bandwidth demands. The most difficult problem to implement the active storage is the migration problem. File system access data by block level. The solution to the above mentioned problem is different host level interfaces to accommodate high level services. It supports the heterogeneous platform, reusing of the existing file system and the operating system technology. It allows the application to access the new services transparently. It minimizes the changes to the operating system. MVSS supports the virtual file. Virtual file is the combination and its associated services. Each virtual file is stored in different virtual disk. Virtual disk facilitates the namespace distinctions of different views of the file, provides the solution for the caching problem.

II. SECURED KEY STORAGE AND AUTOMATIC DELETION

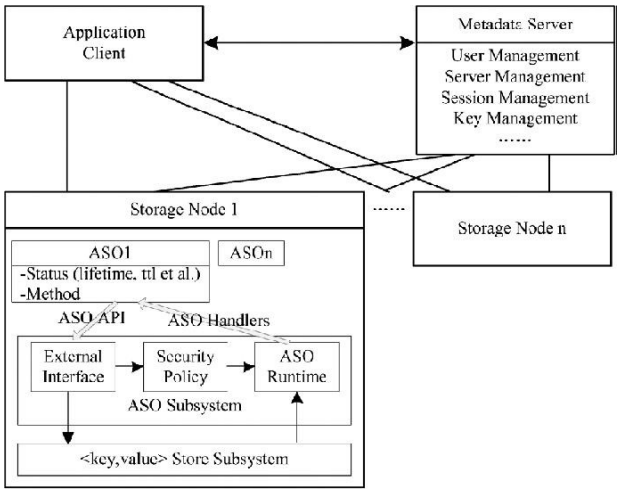


Fig. 1. Data Expiration process

the cloud because in the private cloud service providers offers few services which are needed by the users. The file is divided and stores each portion of the file in different virtual machine. Virtual machine acts as an active storage and randomly generated key for each partition. The key and file portion is associated with the corresponding up loader using the overlay network. Now the encrypted file is stored in the virtual machine. There is no storage in the agent. So it is not necessary to trust the third party. It just verifies the authorized access by the user or not. At the time of downloading the file verification procedure is done by the agent and guarantees the user to access the service. Otherwise service is denied. Along with the key the survival parameter of the key is defined. It provides the lifespan for the file. Until the key is alive user downloads the file. It facilitates the file to be more confidential. Procedure to upload the file is first to create the account and obtain the unique identity from the service provider. There is no need to convert the format of the file in cloud storage.

A. Active storage framework

In active storage framework object based interface to store and manage the equally divided key. Evaluation of self-destructing data based on its functionality and security policies. The result demonstrates that self destructing data meets all the privacy preserving goals. Object based interface achieves coordination between application server and storage devices.

B. Self data manipulation

There is no need of explicit delete actions by the user, or any other third- party storing that data. No need to modify any of the stored or archived copies of that data. The system and not controllable for the user. In distributed object-based storage system self destructing data function is used. Extensive experiments show that the proposed Self-destructing data system does not affect the normal use of storage system. The requirements of self-destructing data under a survival time by user controllable key.

C. Time parameter for secret key

A service method needs a long time to process a complicated task. A service method in the user space can take advantage of performance of the system. All the data and their copies become destructed or unreadable after a user-specified time. A self-destruct method object is associated with each secret key part and survival time parameter for each secret key part. A system creates messages that automatically self- destruct after a period of time. The user's applications should implement logic of data process and act as a client node. Once it meets the time constraints the data is deleted

.III. DESIGN

In object based storage when client application request metadata for one file from the metadata server it provides themapping functions and it is cached for future reference. It improves the throughput and reduces its latency. Mapping function consists of data associated to the particular file. reconstructs the key but the downloader cannot able to reconstruct the key. So the decryption is performed by the storage system. Next the file expiration condition verification begins.

Object based storage designed to achieve cost effective scalable bandwidth. Objects are stored on disk location. Metadata server performs prefetching so that the related objects are available in the cache memory. In metadata server client application gets permission to perform any operation. MAC is used to avoid replay attack. The response from the metadata is in the form of array. It reduces the prefetching overhead. File length is updated to the metadata server and hence it reflects the existing object based storage.

OSD represents files as the set of objects and distributed across various storage devices. Common object size is the size of the stripe unit size of the system. Object based file system improves the disk utilization. It works well on workloads of both small and large workloads. OSD provides object level interface to the files. Any client application can directly contact the OSD retrieve the objects regarding the related files. Providing direct data transfer between the storage device and client improves bandwidth. High level of security is achieved by certain cryptographic techniques and using security mechanism. Client interface manages the file system cache memory. File is divided into fixed size objects and in distributed manner. The asynchronous write operation in object based storage is cached. File lost problem due to power failure and hardware failure can be avoided by the cached copies. Object identifier used to retrieve object from disk.

In the disk location OBFS determines which in type of block object is to be stored. Object size is more than the disk utilization threshold of large blocks then large

blocks are used or else small block size is used. It updates data structure asynchronously for better performance. From the user object active storage object is derived and time to live parameter is defined. This parameter checks the policy associated to the object and meets the constraints defined to those policy. The implementation of the data process includes two processes such as file uploading and downloading.

A. File upload

At the time user uploads the file they happen to store the file and key to encrypt in the object based storage system. Intermediate verifies the authentication of the user in the private cloud. To increase the privacy activation is banned for two user upload the file with same details. The input given by the user is the file, file size, time to live for the secret key and the number of parts the file to be divided. As specified by the user the virtual machine is created for each file partition. Same configuration of the virtual machine is created at each and every node. File is divided and stored in each virtual machine. Now the secret key is generated by the virtual machine. In the storage node Shamir secret sharing algorithm provides this splitting process.

B. File download

The user who has the access permission to access the file alone downloads the content of the file. Before downloading the decryption process is performed. For decryption client gets the key from the object storage. The storage system

C. Secure Erasable Function

Secure delete function is carried out in both read and write operation in OSD. It contains set of commands to

completely overwrite all of the on the hard drive. Previous data cannot be accessible due to secure delete function. It performs sanitizing without affecting the disk capabilities.

IV. RESULT

Here it an evaluation of latency for the files of different sizes. The time taken for uploading and downloading file determines the latency. In this system during file access there is high speed from the first bit to last bit arrival rate of the file. It is evaluated with the file size. Downloaded time is divided according to the file size and makes it to the multiplication of the bytes. To the previous result overhead of sender and receiver is added.

V. CONCLUSION

A novel framework for automatic deletion of data to preserve the privacy of the confidential data is proposed in this paper. We demonstrated the approach of encrypted storage of data without explicit actions by user and provide the minimum knowledge to consume the data at the receiver side. It prevents the illegal use of the confidential data. Hence we conclude that less

based storage system.

VI. FUTURE WORK

Data and its associated key are destroyed after the expiration time of the key. Data such as file is treated as objects. When a single object is destroyed then any object referenced to that particular object gets free. Thus the reference count decreases. Instead of destroying an object as soon as its reference count falls to zero, it is added to the unreferenced list objects and periodically destroyed from the list.

VII. REFERENCES

[1] Lingfang Zeng, Shibin Chen, Qingsong Wei, and Dan Feng "SeDas: A Self-Destructing Data System Based on Active Storage Framework", *IEEE transactions onmagnetics, vol. 49, no. 6, june 2013*

[2] R. Geambasu, T. Kohno, A. Levy, and H.M.Levy, "Vanish: Increasing data privacy with self destructing data," in *Proc. USENIX Security Symp.*, Montreal, Canada, Aug. 2009, pp. 299–315.

[3] R. Wickremesinghe, J. Chase, and J. Vitter,"Distributed computing with load-managed active storage", in *Proc. 11th IEEE Int. Symp. High Performance Distributed Computing (HPDC)*, 2002, pp. 13–23.

[4] L. Qin and D. Feng,"Active storage framework for object-based storage device," in *Proc. IEEE 20th Int. Conf.Advanced Information Networking and Applications (AINA)*,2006.

[5] S. Wolchok, O. S. Hofmann, N. Heninger, E. W. Felten, J. A. Halderman, C. J. Rossbach, B. Waters, and E. Witchel, "Defeating vanish with low-cost sybil attacks against large DHEs," in *Proc. Network and Distributed System SecuritySymp.*, 2010.

[6] X. Ma and A. Reddy, "MVSS: An active storage architecture," *IEEE Trans. Parallel Distributed Syst.*, vol. 14, no. 10, pp. 993–1003, Oct. 2003.

[7] S. Rhea, B. Godfrey, B. Karp, J. Kubiatowicz, S. Ratnasamy, S.Shenker, I. Stoica, and H. Yu, "OpenDHT: A public DHT service and its uses," in *Proc. ACM SIGCOMM*, 2005.

[8] A. Acharya, M. Uysal, and J. Saltz, "Active disks: Programming model, algorithms and evaluation," in *Proc.8th Conf. Architectural Support for Programming Languages and Operating System (ASPLOS)*, Oct. 1998, pp.81–91.

Z. Niu, K. Zhou, D. Feng, H. Chai, W. Xiao, and C. Li, "Implementing and evaluating security controls for an object-based storage system," in *Proc. 24th IEEE Conf.Mass Storage Systems and Technologies (MSST)*, 2007

[11] T. Cholez, I. Chrisment, and O. Festor, "Evaluation of sybil attack protection schemes in kad," in *Proc. 3rd Int.Conf. Autonomous Infrastructure, Management and Security*, Berlin, Germany, 2009, pp. 70–82.

[12] Y. Lu,D.Du, andT.Ruwart, "QoS provisioning framework for an OSD based storage system," in *Proc. 22ndIEEE/13th NASA Goddard Conf. Mass Storage Systems and Technologies (MSST)*, 2005, pp. 28–35.

[13] C. Wang, Q. Wang, K. Ran, and W. Lou, "Privacy-preserving public auditing for storage security in cloud computing," in *Proc. IEEE INFOCOM*, 2010.

[14] Y. Tang, P. P. C. Lee, J. C. S. Luis, and R. Perlman, "FADE: Secure overlay cloud storage with file assured deletion," in *Proc. Secure Comma*, 2010.

[15]Y. Xie,K.-K. Muniswamy-Reddy, D. Feng, D. D. E. Long, Y. Kang, Z. Niu, and Z. Tan, "Design and evaluation of oasis:An active storage framework based on t10 osd

An efficient method for recognizing pose invariant faces

Jeyachandran.J.S[1] , Ashok kumar.S[2]
Pg student [1], Assistant professor [2]
Department of computer science and engineering

SMK FOMRA institute of technology, Chennai

[1]successjeya@gmail.com [2]ashok_aiht@yahoo.co.in

Abstract— The current face recognition techniques is how to handle pose variations between the probe and gallery face images., we present a method for reconstructing the virtual frontal view from a given nonfrontal face image using Markov random fields (MRFs) and an efficient variant of the belief propagation algorithm.. The alignments are performed efficiently in the Fourier domain using an extension of the Lucas–Kanade algorithm that can handle illumination variations. The problem of finding the optimal warps is then formulated as a discrete labelling problem using an MRF. The reconstructed frontal face image can then be used with any face recognition technique. The two main advantages of our method are that it does not require manually selected facial landmarks or head pose estimation. In order to improve the performance of our pose normalization method in face recognition, we present an algorithm for classifying whether a given face image is at a frontal or nonfrontal pose. Experimental results on different datasets are presented to demonstrate the effectiveness of the proposed approach.

Index Terms—Belief propagation, frontal face synthesizing, Markov random fields, pose-invariant face recognition.

I. INTRODUCTION:

Face recognition has been one of the most active research topics in computer vision and pattern recognition for more than two decades. The applications of face recognition can be found in 3D model vertices in order to synthesize the frontal view. The main drawback of this method is the dependence on the fitting of landmarks using the Active Appearance Model (AAM) On the other hand, 2D techniques do not require the 3D prior information for performing pose-invariant face recognition. The AAM algorithm proposed by Cootes et al.fits a statistical appearance model to the input image by learning the relationship between perturbations in the model parameters and the induced image errors. The main disadvantage of this approach is that each training image requires a large number of manually annotated landmarks. Gross et al. Proposed the Eigen light-field (ELF) method that unifies all possible appearances of faces in different poses within a 4D space (two viewing directions and two pixel positions). However, this method discards shape variations due to different identity as it requires a restricted alignment of the image to the

Light field space. Use an affine mapping and pose information to generate the observation space from the identity space. In the approach proposed by Castillo and Jacobs [12], the cost of stereo matching was used in face recognition across pose without performing 3D reconstruction. Sarfraz and Hellwich try to solve the problem by modeling the joint appearance of gallery and probe images across pose in a Bayesian framework. Patch-based approaches for face recognition under varying poses have received significant attention from the research community. These methods were motivated by the fact that a 3D face is composed of many planar local surfaces and thus, an out-of-plane rotation, although nonlinear under 2D imaging projection, can be approximated by linear transformations of 2D image patches. As a result, modeling a face as a collection of sub regions/patches is more robust to pose variations than the holistic appearance. In the method proposed by Kanade and Yamada, each patch has a utility score based on pixel differences, and the recognition is performed using a Gaussian probabilistic model and a Bayesian classifier. Ashraf et al. Extended this approach by learning the patch correspondences based on 2D affine transforms. The problem with

these approaches is that the transformations are optimized locally without taking into account the global consistency of the patches. In linear regressions are performed on local patches in order to telecommunication, law enforcement, biometrics and surveillance. Although there have been some early successes in automatic face recognition, it is still far from being completely solved, especially in uncontrolled environments. In fact, the performance of most of current face recognition systems drops significantly when there are variations in pose, illumination and expression

Existing methods for face recognition across pose can be roughly divided into two broad categories: techniques that rely on 3D models, and 2D techniques. In the first type of approaches, the morphable model proposed by Blanz and Vetter fits a 3D model to an input face using the prior knowledge of human faces and image-based reconstruction

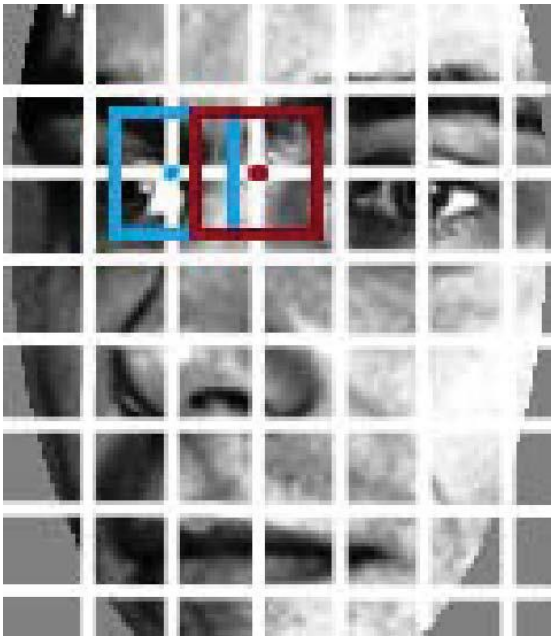
DRAWS BACKS OF ALGORTHIM.

The main drawback of this algorithm is that it requires many manually selected landmarks for initialization. Furthermore, the optimization process is computationally expensive and often converges to local minima due to a large number of parameters that need to be determined. Another recently proposed method by Biswas and Chellappa estimates the facial albedo and pose at the same time using a stochastic filtering framework and performs recognition on the reconstructed frontal faces

DISADVANTAGES OF ALGORTHIM:

The disadvantage of this approach lies in the use of an iterative algorithm for updating the albedo and pose estimates leading to accumulation of errors from step to step. Given a nonfrontal face image, the 3D pose normalization algorithm proposed by Asthana et al. Uses the pose- dependent correspondences between 2D landmark points and

Synthesize the virtual frontal view. Another approach proposed by measures the similarities of local patches by correlations in a subspace constructed by Canonical Correlation Analysis (CCA). However, the common drawback of these two algorithms is that the head pose of the input face image needs to be known a priori. Arashloo and Kittler present a method for estimating the deformation parameters of local patches using Markov Random Fields (MRFs). The disadvantage of this approach is that it depends on estimating the global geometric transformation between the template and the target images. Although designed specifically for handling expression variations in face recognition, another related work is the method proposed by Liao and Chung which formulates the face recognition problem as a deformable image registration problem using MRFs. However, this approach also depends on the extraction of salient regions from the face images. In this paper, a patch-based method for synthesizing the virtual frontal view from a given nonfrontal face image using MRFs and an efficient variant of the BP algorithm is proposed. By aligning each patch in the input image with images from a training database of frontal faces, a set of possible warps is obtained for that patch. The alignments are then carried out efficiently using an illumination invariant extension of the Lucas–Kanade (LK) algorithm in the frequency domain. The objective of the algorithm is to find the globally optimal set of local warps that can be used to predict the image patches at the frontal view.



GOALS OF MRF: This goal is achieved by considering the problem as a discrete labelling

problem using an MRF. In our approach, the cost functions of the MRF are not just the simple sum of squared differences (SSD) between patches but are modified to reduce the effect of illumination variations. The optimal labels are obtained using a variant of the BP algorithm

With message scheduling and dynamic label pruning the two main advantages of our approach over other state-of- the-art algorithms are that: it does not require manually selected landmarks, and no global geometric transformation is needed. Furthermore, we also present a method that is able to classify whether an input face image is frontal or nonfrontal. This method extracts dense SIFT descriptors from the input face image and performs classification using the Support Vector Machine (SVM) algorithm. It is used to improve the performance of our pose normalization technique in face recognition. Experimental results on the FERET CMU-PIE and Multi-PIE databases are presented to demonstrate the effectiveness of the proposed algorithm. The remainder of this paper is organized as follows. Section II describes the illumination-insensitive alignment method based on the LK algorithm. The reconstruction of the virtual frontal view using MRFs and BP is discussed in Section III. The frontal-view classification algorithm is presented in Section IV. Next, in Section V, we show the experimental results in both frontal face reconstruction and pose-invariant face recognition. Section VI concludes this paper.

ADVANTAGES IN LK ALGORTHIM:. The main advantage of the weighted LK algorithm over the original method is that illumination variations can be handled by encoding the prior knowledge of the correlation and salience of image pixels into Q. As a result, choosing an appropriate weighting matrix Q is an important problem with the weighted LK algorithm.

FRONTAL-VIEW CLASSIFICATION:

In order to avoid degrading performance when applying the proposed pose compensation technique to face recognition, it is important to be able to automatically decide if the input face image is frontal or nonfrontal. In our approach, the frontal-view classification is performed using the Support Vector Machine (SVM) algorithm First, dense Scale Invariant Feature Transform (SIFT) descriptors are extracted from image grid points in order to obtain a representation that is robust to noise and illumination variations. The dimension of the concatenated descriptor vector is reduced for efficient processing by using Random Projection (RP). Finally, an SVM is employed to decide whether the face image is at the frontal pose or not. More details about SVM can be found in

A. Dense SIFT Descriptors One of the most popular methods for extracting key points from an image is the SIFT algorithm proposed by Lowe [22]. In this algorithm, a local descriptor is created at each detected key point by forming a histogram of gradient orientations and magnitudes of image pixels in a small window. The size of the local window is usually chosen at 16 × 16. It is then divided into sixteen 4×4 sub-windows. Gradient orientations and magnitudes are estimated within each sub-window and put into an 8 bin histogram. The histograms of the sub-windows are concatenated to create a 128-dimensional feature vector (descriptor) of the keypoint.

In order to form a dense description of the input face image, local SIFT descriptors are extracted at regular image grid points, rather than only at keypoints, in the proposed approach. The advantage of this representation is that it does not depend on the matching of keypoints, which is often challenging when significant pose and illumination variations are present between the input images. This dense representation was also employed successfully for image alignment, gender classification and head-pose estimation in and respectively. Figure 2 shows the input face images at different poses and their corresponding dense SIFT descriptors. In the second row of the figure, the first three principal components of each descriptor are mapped onto the principal components of the RGB color space in order to visualize purpose. Similar to the first component is mapped into R + G + B, the second and third components are mapped into R − G and R/2 + G/2 − B, respectively.

B. Dimension Reduction Using Random Projection (RP) as the dimension of the concatenated feature vector for the whole input face image is significantly

large, techniques such as Principal Component Analysis (PCA) can be used to project the concatenated feature vector into a lower- dimensional subspace. However, due to the large dimension of the feature space, the eigenvalue decomposition of the data covariance matrix will be very computationally expensive. A more efficient way to reduce the dimension of the feature vectors is by projecting them onto a random lower-dimensional subspace. The main idea of random projection comes from the Johnson–Linden Strauss (JL) lemma.

EXPERIMENTAL RESULTS:

A. Frontal-View Classification Using Dense SIFT Descriptors The proposed frontal-view classification algorithm was trained using an SVM on 2D images generated from the 3D faces in the USF 3D database. By rotating the 3D models and projecting them into the image plane, we can synthesize the 2D face images at different viewing angles. Face images with less than ±5° in both the yaw and pitch angles are labelled as frontal. Shows the 2D face images of a person in the database generated at different poses and the visualization of their corresponding dense SIFT descriptors. As the USF 3D database contains the geometry as well as the texture information of the 3D faces, the face images at different illumination conditions can also be generated from the surface normal and albedo using the Lambert's Cosine Law. This is necessary in order for the method to handle possible illumination variations in the test images. We tested the proposed frontal-view classification algorithm on four different databases including the USF 3D

Database FERET CMU-PIE and Multi-PIE. For the USF 3D database, the synthesized face images were divided into five subsets. Four of them were used for training and the remaining subset was used for testing. It takes less than 4 seconds to perform the frontal-view classification for an input face image of size 130×150 on an Intel Xeon 2.13 GHz desktop.

Pose Invariant Face Recognition As presented in above sections, it is more computationally efficient to classify whether a face image is frontal than to synthesize its frontal view (four seconds compared to two minutes). Thus, the frontal-view classifier is an important component of the proposed pose-invariant face recognition system. Before performing the recognition, the probe image was fed to the frontal-view classifier. If the image was classified as nonfrontal, it was transformed to the frontal view using the proposed algorithm. As a result, it is possible to perform recognition by combining our algorithm and any frontal face recognition technique. As we do not require the reference set to include an example of the person in the test image, the same two hundred ba frontal images from the FERET database were used as the training set for synthesizing frontal views in all the three face recognition experiments. As in [8], if the face and both eyes cannot be detected using the cascade classifiers, a Failure to Acquire (FTA) has occurred. In this case, the frontal reconstruction is not carried out and the test image is not counted as a recognition error. The FTA rate is reported for each dataset in the recognition experiments below.

In our experiments, the Local Gabor Binary Pattern (LGBP) was selected as the face recognizer due to its effectiveness. In this method, a feature vector is formed by concatenating the histograms of all the local Gabor magnitude

Pattern maps over an input image. The histogram intersection is used as the similarity measurement in order to compare two feature vectors. More details about the application of the LGBP algorithm for face recognition can be found in

CONCLUSION In this paper, we presented a method for synthesizing the virtual frontal view from a nonfrontal face image. By dividing the input image into overlapping patches, a globally optimal set of local warps can be estimated to transform the patches

to the frontal view. Each patch is aligned with images from a training database of frontal faces in order to obtain a set of possible warps for that node. It is worth noting that we do not require the training database to include the frontal images of the person in the test image. By using an extension of the LK algorithm that accounts for substantial illumination variations, the alignment parameters are calculated efficiently in the Fourier domain. The set of optimal warps is obtained by formulating the optimization

problem as a discrete labelling algorithm using a discrete MRF and an efficient variant of the BP algorithm. The energy function of the MRF is also designed to handle illumination variations between different image patches. Furthermore, based on the sparsity of local SIFT descriptors, an efficient algorithm was also designed to classify whether the pose of the input face image is frontal or nonfrontal. Experimental results using the FERET, CMU PIE, and Multi-PIE databases show the effectiveness of the proposed approach. In the future, we plan to investigate the possibility of synthesizing the probe image not only to the frontal pose, but also to other viewing angles. This will help the algorithm become more robust to large poses in the input images. A pyramidal implementation of the LK alignment algorithm can also be incorporated into the proposed approach in order to reduce the effect of patch size on the results [52].

REFERENCES

[1] W. Zhao, R. Chellappa, P. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," ACM Comput. Surveys, vol. 35, no. 4, pp. 399–458, 2003.

[2] X. Zhang and Y. Gao, "Face recognition across pose: A review," Pattern Recognit., vol. 42, no. 11, pp. 2876–2896, 2009.

[3] M. Turk and A. Pentland, "Eigenfaces for recognition," J. Cogn. Neurosci., vol. 3, no. 1, pp. 71–86, 1991.

[4] K. Etemad and R. Chellappa, "Discriminant analysis for recognition of human face images," J. Opt. Soc. Amer. A, vol. 14, no. 8, pp. 1724–1733, 1997.

[5] P. Belhumeur, J. Hespanha, and D. Kriegman, "Eigenfaces vs. fisher- faces: Recognition using class specific linear projection," IEEE Trans. Pattern Anal. Mach. Intell., vol. 19, no. 7, pp. 711–720, Jul. 1997.

[6] V. Blanz and T. Vetter, "Face recognition based on fitting a 3D morphable model," IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 9, pp. 1063–1074, Sep. 2003.

[7] S. Biswas and R. Chellappa, "Pose-robust albedo estimation from a single image," in Proc. Comput. Vis. Pattern Recognit., Jun. 2010, pp. 2683–2690.

[8] A. Asthana, T. Marks, M. Jones, and K. Tieu, "Fully automatic pose- invariant face recognition via 3D pose normalization," in Proc. Int. Conf. Comput. Vis., Nov. 2011, pp. 937–944.

[9] T. Cootes, G. Edwards, and C. Taylor, "Active appearance models," IEEE Trans. Pattern Anal. Mach. Intell., vol. 23, no. 6, pp. 681–685, Jun. 2001.

HO AND CHELLAPPA: POSE-INVARIANT FACE RECOGNITION USING MRFs 1583

[10] R. Gross, I. Matthews, and S. Baker, "Appearance-based face recognition and light-fields," IEEE Trans. Pattern Anal. Mach. Intell., vol. 26, no. 4, pp. 449–465, Apr. 2004.

[11] S. Prince, J. Elder, J. Warrell, and F. Felisberti, "Tied factor analysis for face recognition across large pose differences," IEEE Trans. Pattern Anal. Mach. Intell., vol. 30, no. 6, pp. 970–984, Jun. 2008.

[12] C. Castillo and D. Jacobs, "Using stereo matching with general epopolar geometry for 2D face recognition across pose," IEEE Trans. Pattern Anal. Mach. Intell., vol. 31, no. 12, pp. 2298–2304, Dec. 2009.

[13] M. Sarfraz and O. Hellwich, "Probabilistic learning for fully automatic face recognition across pose," Image Vis. Comput., vol. 28, no. 5, pp. 744–753, 2010.

[14] T. Kanade and A. Yamada, "Multisubregion based probabilistic approach toward pose-invariant face recognition," in Proc. Symp. Comput. Int. Robot. Autom., Jul. 2005, pp. 954–959.

[15] A. Ashraf, S. Lucey, and T. Chen, "Learning patch correspondences for improved viewpoint invariant face recognition," in Proc. Comput. Vis. Pattern Recognit., Jun. 2008, pp. 1–8.

[16] X. Chai, S. Shan, X. Chen, and W. Gao, "Locally linear regression for pose-invariant face recognition," IEEE Trans. Image Process., vol. 16, no. 7, pp. 1716–1725, Jul. 2007.

[17] A. Li, S. Shan, X. Chen, and W. Gao, "Maximizing intra-individual correlations for face recognition across pose differences," in Proc. Comput. Vis. Pattern Recognit., Jun. 2009, pp. 605–611.

[18] S. Arashloo and J. Kittler, "Pose-invariant face matching using MRF energy minimization framework," in Proc. Energy Minimiz. Meth. Comput. Vis. Pattern Recogn. Conf., 2009, pp. 56–69.

[19] S. Liao and A. Chung, "A novel Markov random field based deformable model for face recognition," in Proc. Comput. Vis. Pattern Recognit. Conf., Jun. 2010, pp. 1–8.

[20] A. Ashraf, S. Lucey, and T. Chen, "Fast image alignment in the Fourier domain," in Proc. Comput. Vis. Pattern Recognit. Conf., Jun. 2010, pp. 1–8.

Normalization for local appearance-based face recognition," in Proc. Int. Conf. Adv. Biometr., 2009.

1584 IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 4, APRIL 2013

Rama Chellappa (F'92) received the B.E. (Hons.) degree in electronics and communication engineering from the University of Madras, Chennai, India, and the M.E. (Distinction) degree from the Indian Institute of Science, Bangalore, India, in 1975 and 1977, respectively, and the M.S.E.E. and Ph.D. degrees in electrical engineering from Purdue University, West Lafayette, IN, in 1978 and 1981, respectively. He was a Faculty Member with the Department of EE-Systems, University of Southern California (USC), from 1981 to 1991. Since 1991, he has been a Professor of electrical and computer engineering (ECE) and an Affiliate Professor of computer science with University of Maryland (UMD), College Park, where he was elected as a Distinguished Faculty Research Fellow. He is a Permanent Member with the Center for Automation Research, Institute for Advanced Computer Studies and is the Chair of the ECE Department. In 2005, he was a Minta Martin Professor of Engineering. He holds three patents. His current research interests include face recognition, clustering and video summariza- tion, 3-D modeling from video, image, and video-based recognition of objects, events and activities, dictionary-based inference, compressive sensing, domain adaptation, and hyper spectral processing.

A New Approach For Privacy Leakage Using Dpps In Cloud

Mrs.K.Kanimozhi
Final ME.,Dept. of computer science
S.Veerasamy chettiar college of engi. & Tech
Tirunelveli,India
kkgkani16@gmail.com

Mrs.S.Sankari
ME.,Dept. of compter science
S.Veerasamy chettiar college of engi. & Tech
Tirunelveli,India
sankari_smartdrass@yahoo.co.in

***Abstract*- The main objective of this project is to provide encryption for privacy preservation. The users has large volume of intermediate datasets and by encrypting all intermediate datasets will lead to high overhead and low efficiency, when they are frequently accessed or processed of encryption and decryption. The users, before outsourcing, will first build an encrypted intermediate datasets, and then outsource the encrypted collection to the cloud server. So the users outsources the encrypted form only for selected intermediate datasets to the cloud server. To get back the encrypted intermediate datasets, user acquires a corresponding key. For user privacy logging plays a very important role in the proper operation of an organization's information processing system. However, maintaining logs securely over long periods of time is difficult and expensive in terms of the resources needed. So we proposed a complete system to securely outsource log records to a cloud provider by a new cloud computing paradigm, Data protection Privacy service (DPPS) is a suite of security primitives offered by a cloud platform, which enforces data security and offers evidence of privacy to data owners.**

***Index Terms*— cloud computing, intermediate datasets, privacy preservation**.

I. INTRODUCTION

Cloud Computing as a computing model, not a technology. In this model "customers" plug into the "cloud" to access IT resources which are priced and provided "on-demand". Essentially, IT resources are rented and shared among multiple tenants much as office space, apartments, or storage spaces are used by tenants. Delivered over an Internet connection, the "cloud" replaces the company data center or server providing the same service. Thus, Cloud Computing is simply IT services sold and delivered overthe Internet.Cloud Computing vendors combine virtualization (one computer hosting several "virtual" servers), automated provisioning (servers have software installed automatically), and Internet connectivity technologies to provide the service. These are not new technologies but a new name applied to a collection of older (albeit updated) technologies that are packaged, sold and delivered in a new way. A key point to remember is that, at the most basic level, your data resides on someone else's server(s). This means that most concerns (and there are potentially hundreds) really come down to trust and control issues.

There are different types of cloud computing and are given as follows,

SaaS (Software As A Service):Is the most widely known and widely used form of cloud computing. It provides all the functions of a sophisticated traditional application to many customers and often thousands of users, but through a Web browser, not a "locally-installed" application. Little or no code is running on the Users local computer and the applications are usually tailored to fulfill specific functions.
SaaS eliminates customer worries about application servers, storage, application development and related, common concerns of IT. Highest-profile examples are Salesforce.com, Google's Gmail and Apps, instant messaging from AOL, Yahoo and Google, and VoIP from Vonage and Skype.

*PaaS (Platform as a Service) :*Delivers virtualized servers on which customers can run existing applications or develop new ones without having to worry about maintaining the operating systems, server hardware, load balancing or computing capacity. These vendors provide APIs or development platforms to create and run applications in the cloud – e.g. using the Internet.

Managed Service providers with application services provided to IT departments to monitor systems and downstream applications such as virus scanning for e-mail are frequently included in this category. Well known providers would include Microsoft's Azure, Salesforce's Force.com, Google Maps, ADP Payroll processing, and US Postal Service offerings.

*IaaS (Infrastructure as a Service):*Delivers utility computing capability, typically as raw virtual servers, on demand that customers configure and manage. Here Cloud Computing named as Randomized Efficient Distributed (RED) Protocol and Linear Hash Table (LHT) protocol. provides grids or clusters or virtualized servers, networks, storage and systems software, usually (but not always) in a multitenant architecture.

IaaS is designed to augment or replace the functions of an entire data center. This saves cost (time and expense) of capital equipment deployment but does not reduce cost of configuration,

Valuable intermediate datasets need to be stored for sharing or reuse. It build an intermediate data dependency graph (IDG) from the data provenances in scientific workflows.With the IDG, deleted intermediate datasets can be regenerated, and as such we develop a novel algorithmthat can find a minimum cost storage strategy for the intermediate datasets in scientific cloud workflowsystems.

II. CLOUD ENVIRONMENTS

Cloud computing is a model for enabling service user's ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or

service provider interaction. Cloud computing enables cloud services.

Nowadays, we have three types of cloud environments: Public, Private, and Hybrid clouds. A public cloud is standard model which providers make several resources, such as applications and storage, available to the public. Public cloud services may be free or not. In public clouds which they are running applications externally by large service providers and offers some benefits over private clouds. Private Cloud refers to internal services of a business that is not available for ordinary people. Essentially Private clouds are a marketing term for an architecture that provides hosted services to particular group of people behind a firewall. Hybrid cloud is an environment that a company provides and controls some resources internally and has some others for public use. Also there is combination of private and public clouds that called Hybrid cloud.

III. THREAT MODEL

The goal of our work is that an intruder who has complete access to the database server for some time should learn very little about the data stored in the database and the queries performed on the data.

Our trust and attack model is as follows:

1. We do not fully trust the database server because it may be vulnerable to intrusion. Furthermore, we assume that, once a database intruder breaks into the database, he can observe not only the encrypted data in the database, but can also control the whole database system. A number of query messages sent by the user, as well as the database's processing of these queries, can be observed by the intruder.
2. We assume the communication channel between the user and the database is secure, as there exist standard protocols to secure it We also trust the user's front-end program; protecting the front-end program against intrusion is outside of the scope.
3. We require all data and metadata, including user logs and scheme metadata, to be stored encrypted. (Otherwise, these may open the door for intruders.)

IV. RELATED WORK

The strategy achieves the best trade-off of computation cost and storage cost by automatically storing the most appropriate intermediate datasets in the cloud storage. [1]. With the IDG, deleted intermediate datasets can be regenerated, and as such we develop a novel algorithm that can find a minimum cost storage strategy for the intermediate datasets in scientific cloud workflow systems. The strategy achieves the best trade-off of computation cost and storage cost by automatically storing the most appropriate intermediate datasets in the cloud storage. This strategy can be utilised on demand as a minimum cost benchmark for all other intermediate dataset storage strategies in the cloud. [2]. This approach alone may lead to excessive data distortion or insufficient protection. Privacy-preserving data publishing (PPDP) provides methods and tools for publishing useful information while preserving data privacy. Recently, PPDP has received considerable attention in research communities, and many approaches have been proposed for different data publishing scenarios[3]. solve the challenging problem of privacypreserving multi-keyword ranked search over encrypted cloud data (MRSE).We establish a set of strict privacy requirements for such a secure cloud data utilization system [7]. formulate and address the problem of authorized private keyword searches (APKS) on encrypted PHRin cloud computing environments. [10].

V. PROPOSED SYSTEM

Data Protection Privacy Service improves secutity to users by enhanced logging mechanism.Securely maintaining log records over extended periods of time is very important..

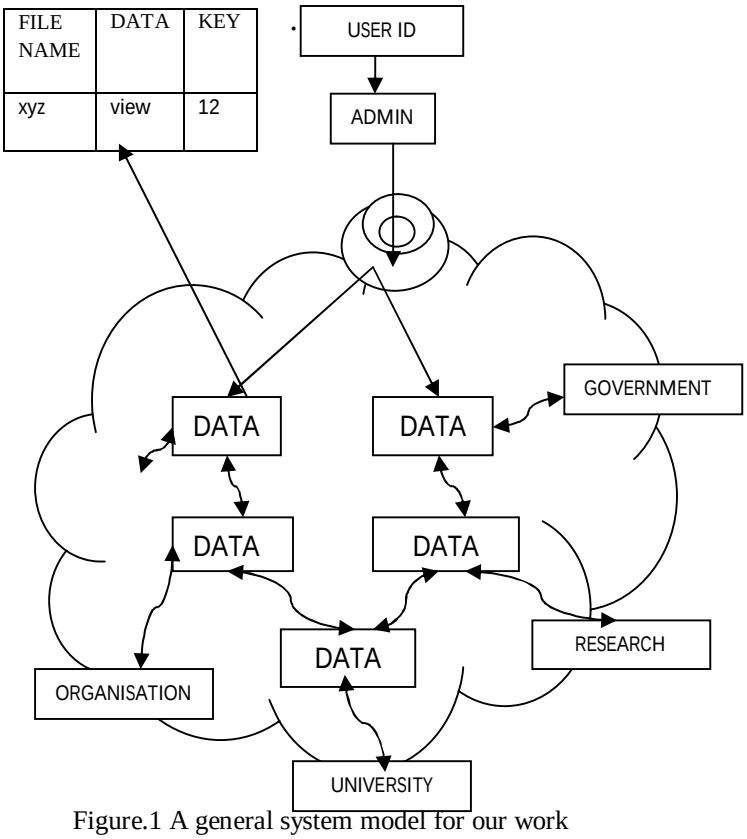


Figure.1 A general system model for our work

Delegating log management to the cloud appears to be a viable cost saving measure. In this paper, we identify the challenges for a secure cloud-based log management service.

A new cloud computing paradigm, *Data protection Privacy service (DPPS)* is a suite of security primitives offered by a cloud platform is proposed, which enforces data security and privacy and offers evidence of privacy to data owners, even in the presence of potentially compromised or malicious applications.Such as secure data using encryption, logging, and key management.

Considering a cloud data hosting service involving two different entities, as illustrated in Figure. 1: the user and the cloud server. Here university

,governmemt,organisation,researchcenter,hospital are the users and admin was considered as the cloud server. The users has intermediate datasets and outsourced to the cloud server in the encrypted form only for selected intermediate datasets.

The users, before outsourcing, will first build an encrypted intermediate datasets, and then outsource the encrypted collection to the cloud server. To getback the encrypted intermediate datasets , authorized user acquires a corresponding key.

We begin by summarizing the desirable properties that we seek from a secure log management service based on the cloud computing paradigm. We will subsequently analyze our framework against these properties.

1) *Correctness*: Log data is useful only if it reflects true history of the system at the time of log generation. The stored log data should be correct, that is, it should be exactly the same as the one that was generated.

2) *Tamper Resistance*: A secure log must be tamper resistant in such a way that no one other than the creator of the log can introduce valid entries.

In addition, once those entries are created they cannot be manipulated without detection. No one can prevent an attacker who has compromised the logging system from altering what that system will put in future log entries.

One cannot also prevent an attacker from deleting any log entries that have not already been pushed to another system. The goal of a secure audit log in this case is to make sure that the attacker cannot alter existing log entries (i.e., the precompromise log entries) and that any attempts to delete or alter existing entrie will be detected.

3) *Verifiability*: It must be possible to check that all entries in the log are present and have not been altered. Each entry must contain enough information to verify its authenticity independent of others.

If some entries are altered or deleted, the ability to individually verify the remaining entries (or blocks of entries) makes it possible to recover some useful information from the damaged log. Moreover, the individual entries must be linked together in a way that makes it possible to determine whether any entries are missing.

4) *Confidentiality*: Log records should not be casually browseable or searchable to gather sensitive information. Legitimate search access to users such as auditors or system administrators should be allowed.

In addition, since no one can prevent an attacker who has compromised the logging system from accessing sensitive information that the system will put in future log entries, the goal is to protect the precompromised log records from confidentiality breaches.

5) *Privacy*: Log records should not be casually traceable or linkable to their sources during transit and in storage.

There are three types of entities in our system:

• Users: Authorised users are able to read, write and search encrypted data residing on the remote server. Sometimes we may need to revoke an authorised user. After being revoked, the user is no longer able to access the data.

• Server: The main responsibility of the data storage server is to store and retrieve encrypted data according to authorised users' requests.

• Key management server (KMS): The KMS is a fully trusted server which is responsible for generating and revoking keys. It generates key sets for each authorised user and is also responsible for securely distributing generated key sets.

When a user is no longer trusted to access the data, the KMS revokes the user's permission by revoking his keys. Authorised users are fully trusted. They are given permissions to access the shared data stored on the remote server by the data owner. They are believed to behave properly and can protect their key sets properly.

• *The* initialisation algorithm Init(1k) *is run by the KMS which takes as input the security parameter* 1k *and outputs master public parameters* Params *and a master key set* MSK.
• *The* user key sets generation algorithm Keygen(MSK,i) *is run by the KMS which takes as input the master keys* MSK *and a user's identity* i, *generates two key sets* Kui *and* Ksi. Kui *is the user side key set for user* i *and* Ksi *is the server side key set for user* i.
• *The* data encryption algorithm Enc(Kui,D,kw(D)) *is run by a user who uses his key set* Kui *to encrypt a document* D *and a set of keywords associated* kw(D), *then outputs ciphertext* c□i (D,kw(D)).
• *The* data decryption algorithm Dec(Kui,c′ i (D))*is run by a user which decrypts* c′ i (D) *by using the user's key set and outputs* D.

VI. SECURITY ANALYSIS

We can prove the security of our scheme by using standard cryptographic techniques. Recall that for security we need to consider t queries. Suppose the uth query ($1 \leq u \leq t$) is of the format "select Aju,1 ,. . . , Aju,ℓ from T where Aju,0 = vu." We show that our basic solution only reveals j1,0, .. . , jt,0 beyond the minimum information revelation. That is, the only extra information leakage by the basic solution is which attributes are tested in the "where" conditions.

The security of our scheme derives from the security of the block cipher we use. In cryptography, secure block ciphers are modeled as pseudorandom. Here, encryption key of the block cipher is the random seed for the pseudorandom permutation.

VII. CONCLUSION AND FUTURE WORK

The proposed system uses encryption and by encrypting all intermediate data sets will lead to high overhead and low efficiency when they are frequently accessed or processed of encryption and decryption. So we encrypt part of intermediate data sets rather than all for reducing privacy-preserving cost. Logging plays a very important role in the proper operation of an organization's information processing system. However,maintaining logs securely over long periods of time is difficult and expensive in terms of the resources needed. So the privacy to data owners was given by Data protection Privacy service (DPPS).it is a suite of security primitives offered by a cloud platform, which enforces data security and privacy and offers evidence of privacy to data owners.

REFERENCES

[1] S.Y. Ko, I. Hoque, B. Cho, and I. Gupta, "Making Cloud Intermediate Data Fault-Tolerant," Proc. First ACM Symp. Cloud Computing (SoCC '10), pp. 181-192, 2010.

[2] D. Yuan, Y. Yang, X. Liu, and J. Chen, "On-Demand Minimum Cost Benchmarking for Intermediate Data Set Storage in Scientific Cloud Workflow Systems," J. Parallel Distributed Computing, vol. 71, no. 2, pp. 316-332, 2011.

[3] Data Publishing: A Survey of Recent Developments," ACM Computing Survey, vol. 42, no. 4, pp. 1-53, 2010.

[4] H. Takabi, J.B.D. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security & Privacy, vol. 8, no. 6, pp. 24-31, Nov./Dec. 2010.

[5] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583- 592, 2011.

[6] H. Lin and W. Tzeng, "A Secure Erasure Code-Based Cloud

[7] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM '11, pp. 829-837, 2011.

[8] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," Proc. 41st Ann. ACM Symp. Theory of Computing (STOC '09), pp. 169-178, 2009.

[9] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Data in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), pp. 383-392, 2011.

[10] B.C.M. Fung, K. Wang, R. Chen, and P.S. Yu, "Privacy-Preserving Data Publishing: A Survey of Recent Developments," ACM Computing Survey, vol. 42, no. 4, pp. 1-53, 2010.

[11] X. Zhang, C. Liu, J. Chen, and W. Dou, "An Upper-Bound Control Approach for Cost-Effective Privacy Protection of Intermediate Data Set Storage in Cloud," Proc. Ninth IEEE Int'l Conf. Dependable, Autonomic and Secure Computing (DASC '11), pp. 518-525, 2011.

[12] K.P.N. Puttaswamy, C. Kruegel, and B.Y. Zhao, "Silverline: Toward Data Confidentiality in Storage-Intensive Cloud Applications," Proc. Second ACM Symp. Cloud Computing (SoCC '11), 2011.

[13] K. Zhang, X. Zhou, Y. Chen, X. Wang, and Y. Ruan, "Sedic: Privacy-Aware Data Intensive Computing on Hybrid Clouds," Proc. 18th ACM Conf. Computer and Comm. Security (CCS

[14] '11), pp. 515-526, 2011.

[15] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," *Comm. ACM, vol. 53, no. 4, pp. 50-58, 2010.*

EVALUATING THE PERFORMANCE OF CLOUD DATA CENTER

M.Thanga vidya

Student
Department of Computer Science and Engineering
Regional centre of Anna University
Tirunelveli (T.N) India
thangavidya15@gmail.com

Abstract—Cloud data center management is a key challenge due to the great numbers and different strategies that can be involved, ranging from the VM placement to the migration with other clouds shows multi cloud. Performance evaluation in Cloud Computing infrastructures is required to predict and quantify the effect of the cost-benefit and the corresponding Quality of Service (QoS) experienced by the cloud users. Such analyses are not accomplished by simulation, due to the great number of parameters that have to be examined. In this paper, we present an analytical model, based on Stochastic Reward Nets (SRNs), that is both powerful to systems composed of thousands of resources and adaptable to represent different procedure and cloud-specific strategies. Several performance measures are defined and evaluated to analyze the behaviour of a Cloud data center: utilization, availability, waiting time, and responsiveness. Quantify the resiliency of infrastructure as-a-service (IaaS) cloud is also provided to take into account of load bursts.

Key words—Cloud computing, stochastic reward nets, cloud performance measures, cloud data center, resiliency.

I. INTRODUCTION

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. Cloud computing portends a major change in how we store information and run applications. Instead of running programs and data on an individual desktop computer, everything is hosted in the "cloud". Cloud computing lets you access all your applications and documents from anywhere in the world. The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams. CloudSim goal is to provide a generalized and extensible simulation framework that enables modeling, simulation, and experimentation of emerging Cloud computing infrastructures and application services, allowing its users to focus on specific system design issues that they want to investigate, without getting concerned about the low level details related to Cloud-based infrastructures and services. Cloud environment creation includes creation of number of virtual machines, data centers, and number of host in each data center, number of users, to create network topology, brokers and number of cloudlets. By using CloudSim, researchers and industry-based developers can focus on specific system design issues that they want to investigate, without getting concerned about the low level details related to Cloud-based infrastructures and services. Cloud computing data centers support for modelling and simulation of virtualized server hosts, with customizable policies for provisioning host resources to virtual machines support for modelling and simulation of federated clouds support for dynamic insertion of simulation elements, stop and resume of simulation. A suitable alternative is the utilization of simulations tools, which open the possibility of evaluating the hypothesis prior to software development in an environment where one can reproduce tests. Specifically in the case of Cloud computing, where access to the infrastructure incurs payments in real currency, simulation-based approaches offer significant benefits, as it allows Cloud customers to test their services in repeatable and controllable environment free of cost, and to tune the performance bottlenecks before deploying on real Clouds. At the provider side, simulation environments allow evaluation of different kinds of resource leasing scenarios under varying load and pricing distributions. Such studies could aid the providers in optimizing the resource access cost with focus on improving profits. In the absence of such simulation platforms, Cloud customers and providers have to rely either on theoretical and imprecise evaluations, or on try-and-error approaches that lead to inefficient service performance and revenue generation.

Cloud Computing is a promising technology able to strongly modify the way computing and storage resources will be accessed in the near future

[1]. Through the provision of on demand access to virtual resources available on the Internet, cloud systems offer services at three different levels: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). In particular, IaaS clouds provide users with computational resources in the form of virtual machine (VM) instances deployed in the provider data center, while PaaS and SaaS clouds offer services in terms of specific solution stacks and application software suites, respectively. Moreover, these services may be offered in private data centers (private clouds), may be commercially offered for clients (public clouds), or yet it is possible that both public and private clouds are combined in hybrid clouds. Cloud computing is also a pay as u go method. In the most basic cloud-service model, providers of IaaS offer computers - physical or more often) virtual machines - and other resources. IaaS clouds often offer additional resources such as a virtual-machine disk image library, raw (block) and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles. IaaS-cloud providers supply these resources on-demand from their large pools installed in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds (dedicated virtual private networks). In order to integrate business requirements and application level needs, in terms of Quality of Service (QoS), cloud service provisioning is regulated by Service Level Agreements (SLAs): contracts between clients and providers that express the price for a service, the QoS levels required during the service provisioning, and the penalties associated with the SLA violations. In such a context, performance evaluation plays a key role allowing system managers to evaluate the effects of different resource management strategies on the data center functioning and to predict the corresponding costs/benefits.

II. RELATED WORK AND MOTIVATION

Cloud systems differ from traditional distributed systems. First of all, they are characterized by a very large number of resources that can span different administrative domains. Moreover, the high level of resource abstraction allows to implement particular resource management techniques such as VM multiplexing [2] or VM live migration [3] that, even if transparent to final users, have to be considered in the design of performance models in order to accurately understand the system behavior. Finally, different clouds, belonging to the same or to different organizations, can dynamically join each other to achieve a common goal, usually represented by optimization of resources utilization. This mechanism, referred to as cloud *federation* [4], allows providing and releasing resources on demand thus providing elastic capabilities to the whole infrastructure. For these reasons, typical performance evaluation approaches such as simulation or on-the-field measurements cannot be easily adopted. Simulation [5], [6] does not allow conducting comprehensive analyses of the system performance due to the great number of parameters that have to be investigated. On-the-field experiments [7], [8] are mainly focused on the offered QoS, they are based on a black box approach that makes difficult to correlate obtained data to the internal resource management strategies implemented by the system provider. On the contrary, analytical techniques [9], [10] represent a good candidate thanks to the limited solution cost of their associated models. However, to accurately represent a cloud system an analytical model has to be:

• Powerful. In order to deal with very large systems Composed of hundreds or thousands of resources.

•Adaptable. Allowing to easily implement different strategies and policies and to represent different working conditions.

A.MOTIVATION

In this paper, we present a stochastic model, based on Stochastic Reward Nets (SRNs) [11], that exhibits the above mentioned features allowing to capture the key concepts of an IaaS cloud system. The proposed model is powerful enough to represent systems composed of thousands of resources and it makes possible to represent both physical and virtual resources exploiting cloud specific concepts such as the infrastructure elasticity. With respect to the existing literature, the innovative aspect of the present work is that a generic and comprehensive view of a cloud system is presented. Low level details, such as VM multiplexing, are easily integrated with cloud based actions such as migration, allowing to investigate different mixed strategies. An exhaustive set of performance measures are defined regarding both the system provider (e.g., utilization) and the final users (e.g., responsiveness). Moreover, different working conditions are investigated and a resiliency analysis is provided to take into account the effects of load bursts. Finally, to provide a fair comparison among different resource management strategies, also taking into account the system elasticity, a performance evaluation approach is described. Such an approach, based on the concept of system capacity presents a holistic view of a cloud system and it allows system managers to study the better solution with respect to an established goal and to opportunely set the system parameters.

III. OVERVIEW OF STOCHASTIC REWARD NET MODEL

A. Existing System

Cloud service provisioning is regulated by SLA's (service Level Agreement) SLA's: Contracts between clients and providers that express the price for a service, the QoS level required during the service provisioning and the penalties associated with the SLA violations. The cloud data center management is key problem mainly due to ranging from VM placement to federation with other clouds. Different clouds, belonging to the same or to different organizations, can dynamically join each other to achieve a common goal, usually represented by the optimization of resources utilization. This mechanism, referred to as cloud federation. Typical performance evaluation approaches such as simulation or on-the-field measurement scan not be easily adopted. Simulation does not allow to conduct comprehensive analyses of the system performance due to the great number of parameters that have to be investigated. On-the-field experiments are mainly focused on the offered QoS, they are based on a black box approach that makes difficult to correlate obtained data to the internal resource management strategies implemented by the system provider.

B. Proposed Methodology

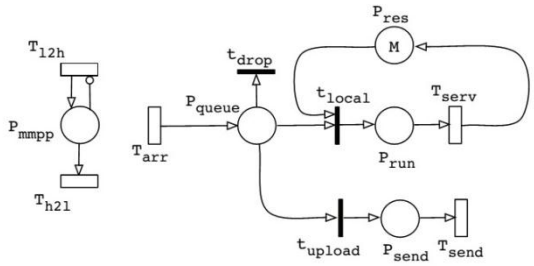


Fig. 1:- The proposed SRN cloud performance model.

Invoking complete process on the considered cloud system using SRN. In that request to the machine queue size is available then we will be on the waiting state else federation process undertaken i.e. moving request to another resource. Made some simple process on using resource includes run, resource using, back to queue and waiting for the utilization as well as the QOS to make the cost consideration between user and system manager which was recorded at data center cloud management to ease the cost producing technique. Which categorize under various phases like queue, federating VMmultiplexing.

PERFORMANCE METRICS:

This phase involves the great role. Formulate & calculating the performance metrics. The performance metrics is which Utilization, availability, waiting time, service time. Where the utilization define the presence of virtual resources. The availability defines the system accept for request when the request is processed after waiting in queue and also for the federated request. The waiting time calculation involves the request waited in the queue. That total time spend in the queue (before using the process). The service time measured when the resource start the execution. This involves the total time used the resources.

RESPONSIVENESS:

This phase helps to accept the request for a system in the given deadline. To characterize the system behaviour from both the provider(vm) and the (cloudlet)user point-of-views. Such metrics will help system designer to size and manage the cloud datacenter and they will also be determinant in the SLA definitions. Obtain the overall waiting time distribution, we need to compute the probability that a particular condition is found when request arrives. The probability that a particular condition is found when request arrives can be then obtained by the solution of the cloud performance model, in particular by summing the probabilities that the SRN is in one of the marking at steady state. Evaluation of responsiveness at SRN method represents the following above shown diagram. The queue follows the FIFO method.

RESILIENCY ANALYSIS:

To assess the resiliency of the cloud infrastructure, in particular when the load is characterized by bursts. In fact, even if the infrastructure is optimally sized with respect to the expected load, during a load burst users can experience a degradation of the perceived QoS with corresponding violations of SLAs. Even if the infrastructure is optimally sized with respect to the expected load, during a load burst users can experience a degradation of the perceived QoS with corresponding violations of SLAs. For this reason, it is needed to predict the effects of a particular load condition in order to study the ability of the system to react to an overload situation. Have to analyze the temporal phases (regular load, load burst). We propose the following transient metrics that allow us to characterize the system resiliency. (Availability at time, Instant service probability at time). The transient metrics allows characterizing the system resiliency analysis.

QUANTITATIV RESILIENCY METRICS:

Evaluating the system degradation. Maximum performance loss is measured. It is the peak of performance lost during the burst, expressed in percentage form.

$$MPL(\%) = [(Psteady - Pmin)/Psteady] \cdot 100$$

where *Psteady* and *Pmin* are the steady state.

To define the performance lost during the burst. During the resiliency analysis we are interested in the quantitative evaluation of the performance degradation experienced by the system during a load burst. Propose some temporal indices able to capture the performance degradation trend. Such indices can be applied to both the Availability and Instant service probability metrics.

V CONCLUSION

In this paper, we have presented a stochastic model to evaluate the performance of an IaaS cloud system. Several performance measures have been defined, such as availability, utilization, and responsiveness, allowing to investigate the impact of different strategies on both provider and user point-of-views. Real time example in a market-oriented area, such as the Cloud Computing, an accurate evaluation of these parameters is required in order to quantify the offered QoS and opportunely manage SLAs. Future works will include the analysis of autonomic techniques able to change on-thefly the system configuration in order to react to a change on the working conditions. We will also extend the model in order to represent PaaS and SaaS Cloud systems and to integrate the mechanisms needed to capture VM migration and data center consolidation aspects that cover a crucial role in energy saving policies.

REFERENCES

[1] R. Buyya et al., "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Gener. Comput. Syst., vol. 25, pp. 599–616, June 2009.

[2] X. Meng et al., "Efficient resource provisioning in compute clouds via vm multiplexing," in Proceedings of the 7th international conferenceon Autonomic computing, ser. ICAC '10. New York, NY, USA:ACM, 2010, pp. 11–20.

[3] H. Liu et al., "Live virtual machine migration via asynchronousreplication and state synchronization," Parallel and DistributedSystems, IEEE Transactions on, vol. 22, no. 12, pp. 1986 – 1999, dec.2011.

[4] B. Rochwerger et al., "Reservoir - when one cloud is not enough,"Computer, vol. 44, no. 3, pp. 44 –51, march 2011.[5] R. Buyya, R. Ranjan, and R. Calheiros, "Modeling and simulationof scalable cloud computing environments and the cloudsimtoolkit: Challenges and opportunities," in High Performance ComputingSimulation, 2009. HPCS '09. International Conference on, june2009, pp. 1 –11.

[6] A. Iosup, N. Yigitbasi, and D. Epema, "On the performancevariability of production cloud services," in Cluster, Cloud and GridComputing (CCGrid), 2011 11th IEEE/ACM International Symposiumon, may 2011, pp. 104 –113.

[7] V. Stantchev, "Performance evaluation of cloud computing offerings,"in Advanced Engineering Computing and Applications inSciences, 2009. ADVCOMP '09. Third International Conference on,oct. 2009, pp. 187 –192.

[8] S. Ostermann et al., "A Performance Analysis of EC2 Cloud ComputingServices for Scientific Computing," in Cloud Computing,ser. Lecture Notes of the Institute for Computer Sciences, SocialInformatics and Telecommunications Engineering. SpringerBerlin Heidelberg, 2010, vol. 34, ch. 9, pp. 115–131.

[9] H. Khazaei, J. Misic, and V. Misic, "Performance analysis of cloudcomputing centers using m/g/m/m+r queuing systems," Paralleland Distributed Systems, IEEE Transactions on, vol. 23, no. 5, pp. 936–943, may 2012.

[10] R. Ghosh, K. Trivedi, V. Naik, and D. S. Kim, "End-to-endperformability analysis for infrastructure-as-a-service cloud: Aninteracting stochastic models approach," in Dependable Computing(PRDC), 2010 IEEE 16th Pacific Rim International Symposium on,dec. 2010, pp. 125 – 132.

[11] G. Ciardo et al., "Automated generation and analysis of Markovreward models using stochastic reward nets." IMA Volumes inMathematics and its Applications: Linear Algebra, Markov Chains, and Queueing Models, vol. 48, pp. 145–191, 1993.

ESTIMATING MULTIDIMENSIONAL RESOURCES IN A CLOUD DATACENTER BY USING CLOUD SCHED

K. R. Sujithra
PG Scholar
Regional Centre Of Anna University
Tirunelveli
Email:sujithra.kr@gmail.com

ABSTRACT

In infrastructure as a service (IaaS), job scheduling is one of the keys for large-scale Cloud applications. Widespread research on all issues in physical environment is extremely challenging because it requires designers to deliberate network infrastructure and the environment, which may be outside the control. In addition, the network conditions cannot be projected or controlled. Therefore, performance evaluation of workload models and Cloud provisioning algorithms in a repeatable manner under different configurations and requirements is difficult. There is still lack of tools that permit developers to associate different resource scheduling algorithms in IaaS concerning both computing servers and user workloads. To fill this gap in tools for evaluation and modeling of Cloud environments and applications, we propose CloudSched. CloudSched can help developers recognize and discover suitable resolutions considering different resource scheduling algorithms. Different traditional scheduling algorithms considering only one factor such as CPU, which can cause hotspots or bottlenecks in many cases, CloudSched treats multidimensional resource such as CPU, memory and network bandwidth incorporated for both physical machines and virtual machines (VMs) for different scheduling algorithms.

KEYWORDS: Cloud computing, Datacenters, Dynamic and Real time resource scheduling, Load Balancing.

1 INTRODUCTION

Cloud Computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about overprovisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under provisioning for one that becomes wildly popular, thus missing potential customers and revenue [1]. Cloud computing offers utility-oriented IT services to users worldwide. Based on a pay-as-you-go model, it enables hosting of pervasive applications from consumer, scientific, and business domains [2]. Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing is used to describe variety of different types of computing concepts that involve a large number of computers that are connected through a real time communication network typically through the internet[3] . The cloud focuses on maximizing the effectiveness of the shared resources. Cloud resources are not only shared by multiple users but as well as dynamically reallocated as per demand. This can work for allocating resources to users in different time zones. In the most basic cloud service model, providers of IAAS offer computers physical or virtual machine and other resources. To deploy the applications, cloud users install operating system images and their application software on the cloud infrastructure. In this model, the cloud user patches and maintains the OS and the application software. Cloud Analyst [13] typically bill IAAS services on a utility computing basis. Cost reflects the amount of resources allocated and consumed. Examples of IAAS providers are Amazon EC2, Google compute Engine, HP cloud [5]. The purpose of toolkit is to guide information professionals in assessing cloud computing services for information use and storage and in developing a cloud computing strategy and specific cloud service requirements for their organization. The toolkit is to be used as an aide to the development of organizational strategies and requirements. It is not to be used as a standard or the sole basis for developing a formal contract. The toolkit needs to be used in conjunction with existing organizational policies and

strategies that cover information management and security, risk management, outsourcing and procurement, compliance and IT. Each organization must take into account its own operating environment and ensure that all applicable legal and regulatory requirements form part of any cloud strategy and the resulting contracts with cloud service providers. Legal and regulatory requirements will be referenced in the toolkit but it is outside the scope of this document to provide a detailed analysis. Cloud environment creation includes creation of number of virtual machines, data centers, number of host in each datacenter, number of users, to create network topology, brokers and number of cloudlets. CloudSim offers the following novel features: (i) support for modeling and simulation of large scale Cloud computing environment s , including data centers , on a single physical computing node; (ii) a self-contained platform for modeling Clouds , service brokers, provisioning, and allocations policies; (iii) support for simulation of network connections among the simulated system elements; and (iv) facility for simulation of federated Cloud environment that inter - networks resources from both private and public domains[4] . Virtual machine runs inside a Host, sharing host List with other VMs. It processes cloudlets. This processing happens according to a policy, defined by the Cloudlet Scheduler. Each VM has an owner, which can submit cloudlets to the VM to be executed. Virtual machine is a software implementation of a hardware that executes programs, applications just like real machine would do. VM are getting very important and widely used these days. This happens due to the improvements in hardware and virtualization capabilities along with the numerous benefits offered by the technology. A VM is a software implementation of a computing environment in which an OS can be installed and run. The virtual machine [14] typically emulates a physical computing environment, but request for CPU, memory, hard disk, network and other hardware resources are managed by a virtualization layer. Cloudlet stores despite all the information encapsulated in the Cloudlet, the ID of the VM running it. Datacenter [10] class is a Cloud Resource whose host List is virtualized. It deals with processing of VM queries (i.e., handling of VMs) instead of processing Cloudlet-related queries. So, even though an AllocPolicy will be instantiated in the method of the superclass, then the processing of Virtual Machines are handled by the VmAllocationPolicy. Host executes actions related to management of virtual machines (e.g., creation and destruction). A host has a defined policy for provisioning memory and bandwidth, as well as an allocation policy for virtual machines. A host is associated to a datacenter. Resource scheduling in infrastructure as a service (IaaS) is one of the keys for large-scale Cloud applications. The resource demands for different jobs fluctuate over time. The central component that manages the allocation of virtual resources for a cloud infrastructure's physical resources is known as the cloud scheduler. CloudSched is lightweight design with focus on resource scheduling algorithms. CloudSched treats multidimensional resources such as CPU, memory and network bandwidth integrated for both physical machines and VMs. **LIF** algorithm is used as a dynamic load-balance of a Cloud data center. It can help developers to identify and explore appropriate solutions considering different resource scheduling policies and algorithms.

2 RELATED WORKS:

2.1 Virtual machine

It runs inside a Host, sharing host List with other VMs. It processes cloudlets. This processing happens according to a policy, defined by the Cloudlet Scheduler. Each VM has an owner, which can submit cloudlets to the VM to be executed. Virtual machine is a software implementation of a hardware that executes programs, applications just like real machine would do. VM are getting very important and widely used these days. This happens due to the improvements in hardware and virtualization capabilities along with the numerous benefits offered by the technology. A VM is a software implementation of a computing environment in which an OS can be installed and run. The virtual machine typically emulates a physical computing environment, but request for CPU, memory, hard disk, network and other hardware resources are managed by a virtualization layer.

2.2 Cloudlet

Cloudlet stores despite all the information encapsulated in the Cloudlet, the ID of the VM running it.

2.3 Datacenter

Datacenter class is a Cloud Resource whose host List is virtualized. It deals with processing of VM queries (i.e., handling of VMs) instead of processing Cloudlet-related queries. So, even though an AllocPolicy will be instantiated in the method of the superclass, then the processing of Virtual Machines are handled by the VmAllocationPolicy.

2.4 Host

Host executes actions related to management of virtual machines (e.g., creation and destruction). A host has a defined policy for provisioning memory and bandwidth, as well as an allocation policy for virtual machines. A host is associated to a datacenter.

2.5 Resource Scheduling

Resource scheduling in infrastructure as a service(IaaS) is one of the keys for large-scale Cloud applications. The resource demands for different jobs fluctuate over time. The central component that manages the allocation of virtual resources for a cloud infrastructure's physical resources is known as the cloud scheduler. CloudSched is lightweight design with focus on resource scheduling algorithms. CloudSched treats multidimensional resources such as CPU, memory and network bandwidth integrated for both physical machines and VMs

2.6 LIF (least imbalance-level first)

LIF algorithm is used as a dynamic load-balance of a Cloud data center. It can help developers to identify and explore appropriate solutions considering different resource scheduling policies and algorithms.

3 PROPOSED METHODOLOGY:

To propose CloudSched is lightweight design with focus on resource scheduling algorithms. CloudSched treats multidimensional resources such as CPU, memory and network bandwidth integrated for both physical machines and VMs.

3.1 LIF (LEAST IMBALANCE-LEVEL FIRST) ALGORITHM

It uses LIF (least imbalance-level first) algorithm for dynamic load-balance of a Cloud data center. It can help developers to identify and explore appropriate solutions considering different resource scheduling policies and algorithms. It dynamically finds the lowest total imbalance value of the datacenter. It can easily adapt to different resource scheduling policies and algorithms. It compares different resource scheduling algorithms of both computing servers and user workloads. It provides better estimation for load-balance and energy-efficient process.

ALGORITHM

Lowest-Average-Value-First(r)

Input: Placement request r=(id, t_ s, t_e ,k);

status of current active tasks and PMs

Output: placement scheme for r and IBL_tot.

1: initialization: LowestAvg = large number;

2: **FOR** i=1:N **DO**

3: **IF** request r can be placed on PM (i)

4: **THEN**

5: compute avg(i) utilization value of PM(i) using equations (1)-(3);

6: **IF** avg(i)<LowestAvg

7: **THEN**

8: LowestAvg=avg(i);

9: allocatedPMID=i;

10: **ELSE**

11: **ENDIF**

12: **ELSE** //find nextPM

13: **ENDFOR**

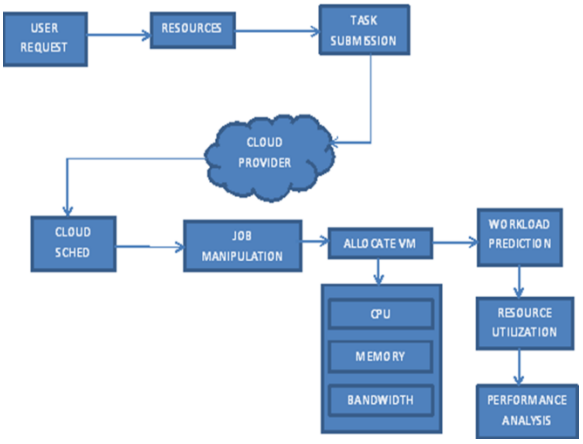
14: **IF** LowestAvg==large number L// cannot allocate

15: **THEN** put r into waiting queue or reject

16: **ELSE** place r on PM with allocatedPMID and compute IBL_tot

This algorithm shows the pseudo codes of LIF (least imbalance-level first) algorithm [28] for dynamic load-balance of a Cloud data center. Inputs to the algorithm include current VM request, status of current active tasks and physical machines. For dynamic scheduling, the output is placement scheme for request. Basically, the algorithm dynamically finds the lowest total imbalance value of the datacenter when placing a new VM request by comparing different imbalance values if the request is allocated to different physical machines. Actually,

the algorithm finds a PM with the lowest integrated-load, this will make the total imbalance-value of all servers in a Cloud data center the lowest.



4 METHODOLOGY:

4.1 CloudSim Resources Deployment:

CloudSim environment consist of i) Datacenters ii) Cloud brokers iii) Cloudlet (Jobs) iv) Virtual Machines v) Host. All components of CloudSim are required to deploy the jobs on the respective virtual machines executed in the datacenters.

(i) Cloud Environment Creation:

For performing a job we need virtual machine to run it. The data center is nothing but storing and saving the job. Data Center consists of several virtual machine, In Cloud environment components like Data center, Virtual machine, Data Broker creation, hosts, and cloudlets.

(ii)Data Center Creation:

In data center, several virtual machines, hosts, data broker, cloudlet is present. The purpose for the data center is for storing the data. The cloud service provider only provides the data center. The service provider operates the data center and then gives the services to the user; the data center is maintained by the service provider.

(iii*) Data Broker Creation:*

Data Broker, can submit the job to the data center. The cloud service provider allocates the resources to the cloudlets. For submitting the job the Broker needs ID, NAME.

4.2 *Jobs Creation and Manipulation:*

It stores, despite all the information encapsulated in the Cloudlet, the ID of the VM running it. Jobs are manipulated using offline and online dynamic scheduling algorithm. Optimal process is to manipulate and arrange the jobs in the order that present the optimal pricing Virtual Machines. Manipulation based on load prediction of each and every job submitted in the virtual machines. The jobs are created and store in data center,

Load Prediction

The load predication, within how much energy the job is done in the Virtual Machine. How much it utilizes to process the job it may be processing speed, RAM, Bandwidth. The load predication is calculated for each and every virtual machine.

4.3 *Workload Computation and Prediction:*

Measuring the Power in terms of predicting the workload by means of measuring the QoS values such as,

i) Ram.
ii) Bandwidth.
iii) Average waiting time.
iv) Queue delay.
v) Batch Job Processing.

4.4 Load Balancing using LIF Algorithm:

It uses a dynamic scheduling algorithm, called Lowest Integrated- load First (LIF), for Cloud datacenters. Here, it considers the allocation and migration of multi-type virtual machines on hosting physical machines with multi-dimensional resources. It treats multi-dimensional resource such as CPU, memory and network bandwidth integrated for both physical machines and virtual machines in real time scheduling to minimize total imbalance level of Cloud data centers. It considers imbalance value of CPU, memory & network bandwidth & also provides the average imbalance value of CPU, memory & network bandwidth.

4.5 Performance Evaluation :

The performance of the algorithm is evaluated by using Graph representation. This shows that the proposed framework is able to adapt to changes in time & cost parameter values while the other approaches cannot. The performance gap between the proposed framework and other approaches is at the high level compare to other approaches. It provides better flexibility in the VM allocation process

5 Conclusion

It provides a simulation system for modeling Cloud computing environments and evaluating a different resource scheduling policies and algorithms. It designs and implementing a lightweight simulator

combining real-time multidimensional resource information. It provides modeling and simulation of large scale Cloud computing environments, including data centers, VMs and physical machines.

6 Future Enhancement

In future, it will be possible to add more metrics to measure the quality of related algorithms. For different scheduling strategies such as utilization maximization and maximum profits, etc., of multidimensional resource, it will add more metrics. Extension to multiple federated data centers can be considered. Considering user priority and currently it considered that all users have same priority. Different priority policies can be created for users to have different priorities for certain types of VMs.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, Above the Clouds: A Berkeley view of cloud computing Univ. California at Berkley, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2009-28, Feb.10, 2009.

[2] A. Beloglazov, J. Abawajy, and R. Buyya, "Energy-aware resource allocation
heuristics for efficient management of data centers for cloud computing future generation computer systems," , vol. 28, no. 5, pp.755–768, May 2012.

[3] R. Buyya and M. Murshed, *GridSim:* A Toolkit for the Modeling and Simulation of Distributed Resource Management and Scheduling for Grid Computing. Concurrency and Computation: Practice and Experience. New York, NY, USA: Wiley, Nov.–Dec. 2002, vol. 14, pp.13–15.

[4] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. F. De Rose, and R. Buyya, CloudSim: A Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms, Software: Practice and Experience. NewYork,NY,USA: Wiley, Jan. 2011, vol. 41, pp. 23–50, 0038-0644, Number 1.

[5] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, Cloud Computing and Emerging IT Platforms: Vision, Hype, Reality for Delivering Computing as the 5th Utility. Future Generation Computer Systems. Amsterdam, The Netherlands: Elsevier Science, Jun. 2009, vol. 25, pp. 599–616.

[6] D. Economou, S. Rivoire, C. Kozyrakis, and P. Ranganathan, "Fullsystem
power analysis andmodeling for server environments, 2006," in Stanford Univ./HP Labs Workshop on Modeling, Benchmarking, Simulation (MoBS), Jun. 18, 2006, pp. 70–77.

[7] W. H. Tian, Y. Zhao, Y. L. Zhong, M. X. Xu, and C. Jing, "Dynamic and integrated load-balancing scheduling algorithms for Cloud data centers," *China Commun.*, vol. 8, no. 6, pp. 117–126, 2011.

[8] B. Wickremasinghe *et al.*, "CloudAnalyst: A CloudSim-based tool for modelling and analysis of large scale cloud computing environments," in Proc. 24th IEEE Int. Conf. Adv. Inform. Netw. Appl. (AINA'10), Perth, Australia, Apr. 20–23, 2010.

[9] T.Wood *et al.*, "Black-box and gray-box strategies for virtual machine migration," in Proc. Symp. Netw. Syst. Design. Implementation (NSDI), 2007, pp. 229–242.

[10] H. Zheng, L. Zhou, and J. Wu, "Design and implementation of load balancing in web server cluster system," J. Nanjing Univ. Aeronautics Astronautics, vol. 38, no. 3, pp. 347–351, Jun. 2006.

[11] L. Youseff *et al.*, "2008. Toward a unified ontology of cloud computing," in Proc. Grid Comput. Environ.Workshop*, GCE'08*, 2008, pp. 1–10.

[12] H. Zhu, M. Hou, C. Wang, and M. Zhou, "An efficient outpatient scheduling approach," IEEE Trans. Autom. Sci. Eng., vol. 9, no. 4, pp. 701–709, Oct. 2012.

[13] W. Tian, X. Liu, C. Jin, and Y. Zhong, "LIF: A dynamic scheduling
algorithm for Cloud data centers considering multi-dimensional resources,"
J. Inform. Comput. Sci., vol. 10, no. 12, 2013, appears in.

Integrated Detection and Localization of Multiple Spoofing Attackers in WSN

Manikandan.S[1], Alangudi Balaji.N[2]

PG Student[1], Assistant Professor[2]

Department of Computer Science and Engineering

Sethu Institute of Technology, Virudhunagar.

[1]mani2391mail@gmail.com

[2]alangudibalaji@sethu.ac.in

Abstract-Wireless spoofing attacks are occurs easily and reduce the networks performance. The node identity is verified by cryptographic authentication, due to requirements overhead conventional security approaches are not always suitable. In my paper, I propose to use spatial information, as the basis for detecting spoofing attacks, determining the number of attackers when multiple enemies masquerading as the same node identity and localizing more than one enemies. I propose to use the spatial correlation of received signal strength to detect the spoofing attacks. I then determine the number of attackers. I used Cluster-based mechanisms determine the number of attackers. The Support Vector Machines method used to increase the accuracy of determining the number of attackers. Integrated detection and localization system is used to localize the more than one attackers. I evaluated my techniques using the both an 802.11 network and an 802.15.4 network. When determining the number of attackers by using my method the result attain more than ninety percent hit rate. My localization results using algorithms provide high accuracy of localizing more than one enemies.

1 INTRODUCTION

The wireless transmission medium can access by any user, so attackers can easily access any transmission. Adversaries can easily buys a low cost wireless devices and launch a variety of attacks by using these available platforms. There are various types of attacks, from these attacks the identity based spoofing attack are said to be easy to launch and cause a serious damages to the network.In the identity based spoofing attack attackers use the same identity to transfer the data. So I propose to use spatial information, for detecting the spoofing attacks, determining the number of attackers when multiple enemies masquerading as the same node identity and localizing more than one enemies. . I propose to use the spatial correlation of received signal strength to detect the spoofing attacks. I then determine the number of attackers. I used Cluster-based mechanisms determine the number of attackers. The Support Vector Machines method used to increase the accuracy of determining the number of attackers. Integrated detection and localization system is used to localize the more than one attackers.

To use the received signal strength based spatial correlation, a physical property present in the wireless node that is difficult to falsify and they are not depends on cryptography for detecting spoofing attacks. I concerned with attackers, they have different locations than legitimate wireless nodes, and a spatial information is used to detect spoofing attacks that has a power to not only detect the

presence of the attacks but also localize the attackers.

In the existing system the cryptographic method needs reliable key distribution, management, and maintenance. It is not always possible to apply these methods because of its infrastructural and management overhead. In the existing system, cryptographic method node are said to be easily attacked, which is a serious matter. The wireless nodes are said to be easily accessible, by allowing their memory. The memory is said to be scanned by the attackers. Cryptographic method only protect the data frames. In the proposed system, to detect the attacks on wireless localization, proposed to use the direction of arrived and received signal strength of the signals to localize adversaries. In my work, I choose a group of algorithms based on RSS to perform the work of localizing more than one attackers and calculate the performance in the terms accuracy of localization.

2 RELATED WORKS

In the existing system the cryptographic method needs reliable key distribution, management, and maintenance. It is not always possible to apply these methods because of its infrastructural and management overhead. In the existing system, cryptographic method node are said to be easily attacked, which is a serious matter. The wireless nodes are said to be easily accessible, by allowing their memory. The memory is said to be scanned by the attackers. Cryptographic method only protect the data frames.

2.1 LITRETURE SURVEY

F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access Points Vulnerabilities to Dos Attacks in 802.11 Networks," 2004. From this paper I identified the Spoofing attacks can further facilitate a variety of traffic injection attacks, such as attacks on access control lists, access point (AP) attacks, and eventually Denial- of-Service (DoS) attacks. In this they describe possible denial of service attacks to infrastructure wireless 802.11 networks. The results show that serious vulnerabilities exist in different access points can easily hinder any legitimate communication within a basic service set.

D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signal prints", Sept. 2006. From this paper I found a broad survey of possible spoofing attacks, such as network resource utilization attack and denial-of-service attack. Wireless networks are vulnerable to many identity-based attacks in which a malicious device uses forged MAC addresses to masquerade as a specific client. In this paper a transmitting device can be robustly identified by its signal print. Signal prints can be defeated, such as by the use of multiple synchronized direction antennas, these situations present a challenge for an intruder.

B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," 2005. From this paper I found a most existing approaches to address potential spoofing attacks employ cryptographic schemes and the disadvantages of cryptographic schemes. They propose a secure and efficient key management (SEKM) framework for mobile adhoc network. SEKM builds a public key infrastructure (PKI) by applying a secret sharing scheme. In fact any cryptographic means is ineffective if its key management is weak. Key management is also a central aspect for security in the mobile adhoc network.

P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RF- Based User Location and Tracking System," 2000. From this paper I identified that using RSS is an attractive approach because it can reuse the existing wireless infrastructure and is

highly correlated with physical locations. Dealing with ranging methodology, range-based algorithms involve distance estimation to landmarks using the measurement of various physical properties such as RSS.

3 PROPOSED SYSTEM

In the proposed system, to detect the attacks on wireless localization, proposed to use the direction of arrived and received signal strength of the signals to localize adversaries. In my work, I choose a group of algorithms based on RSS to perform the work of localizing more than one attackers.

3.1 MODULES

- Network Analysis
- Spoofing Attack
- Attack Detection
- Localization

Network Analysis:

I initiate a fixed-length walk from the node. This walk should be long enough to ensure that the visited peers represent a close sample from the underlying stationary distribution. I then retrieve certain information from the visited peers, such as the system details and process details. It acting as source for the network .In sender used to create sends the request and received the response and destination used to receive the request and send the response for the source.

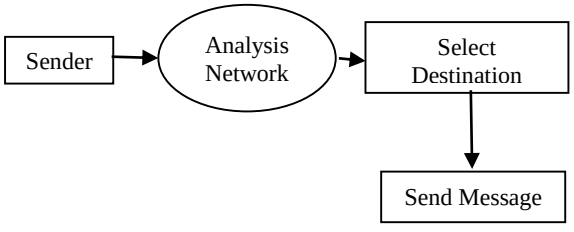


Fig 3.1 Network Analysis

Spoofing Attacks:

Spoofing attacks are easy to launch and can cause damage to the performance of a network. In an 802.11 network, it is easy for an attacker to collect a MAC address during passive monitoring and then attacker modify the MAC address by simply issuing an If config command to masquerade as another device. In the proposed system the frames like data, management, control are said to be protected. In the existing security techniques like Wired Equivalent Privacy, WiFi Protected Access, or 802.11i, such techniques can only protect the data frames, an attacker can spoof management or control frames to cause impact on networks.

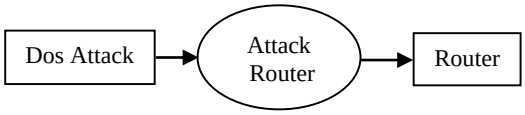


Fig 3.2 Spoofing Attack

Attack Detection:

In the attack detection instead of cryptographic based method, My work is new because none of the existing work can determine the number of attackers when there are more than one enemies masquerading as the same identity. The spatial correlation of RSS is used to detect the attack. The cluster based mechanism is used to detect the number of attackers. This mechanism is said to be improved by the support vector machine. That is the SVM is used to improve the accuracy of determining the number of attackers.

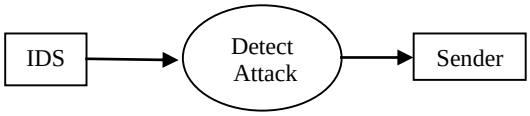


Fig 3.3 Attack Detection

Localization:

My approach can correctly localize more than one enemies even the transmission power levels of the attackers varies. Algorithm used for a localization are area based probability and RADAR gridded algorithms. Localization estimation using RSS which are about 15 feet. When the nodes are less than 15 feet apart, they have a high likelihood of generating similar RSS readings, and thus the spoofing detection rate falls below 90 percent, but still greater than 70 percent. When spoof moves closer to the attacker also increases the probability to expose itself, now the detection rate goes to 100 percent. When the spoofing node is about 45-50 feet away from the original node. The detection rate is said to be lesser.

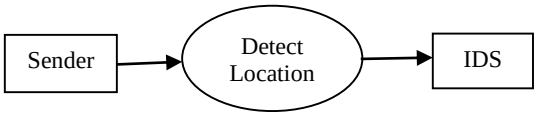


Fig 3.4 Localization

4 PERFORMANCE EVALUATION

This graph shows the packet delivery ratio. The packet delivery ratio graph consist of time as X axis and delivery ratio as a Y axis. In existing system, when the time is increases the delivery ratio is said to be reduces. In the proposed system, when the time is increases the delivery ratio is also said to be increases. So in the proposed system the delivery of the packet is said to be faster and higher than the existing system.

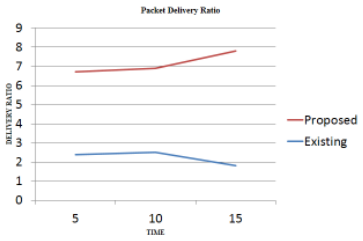


Fig 4.1 Packet Delivery Ratio

This graph shows the security performance. The security graph consist of time as X axis and security value as a Y axis. In existing system, when the time increases the security is said to be decreases. In the proposed system, when the time increases the security is also said to be increases. So in proposed system the data is said to be well secured than the existing system.

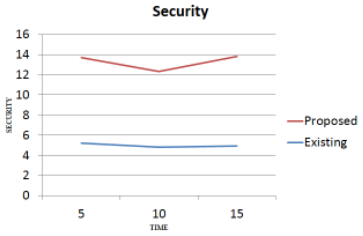


Fig 4.2 Security

This graph shows the throughput performance. The throughput graph consist of time as X axis and throughput value as a Y axis. In existing system, when the time increases the throughput is said to be decreases. In the proposed system, when the time increases the throughput is also said to be increases.

So in proposed system the throughput is said to be higher than the existing system.

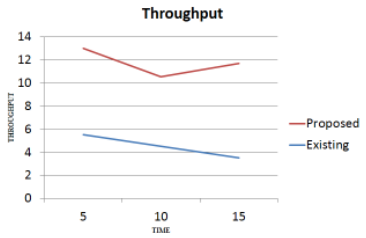


Fig 4.3 Throughput

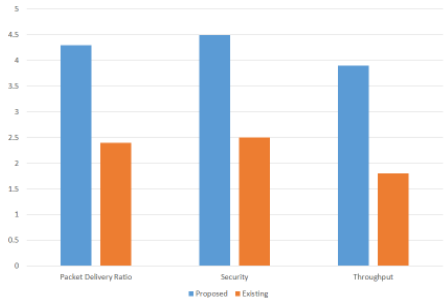


Fig 4.4 Comparison between Proposed and Existing System

Systems	Packet Delivery	Security	Throughput	Hit Rate
Proposed	54.5	75.3	70.9	95
Existing	30.3	31.5	35.8	70

Table 1 Comparison between Proposed and Existing System

5 CONCLUSION

In my work, I used a RSS based spatial correlation, a physical property presented with the wireless device that is said to be difficult to falsify and they are not depends on the cryptography method for attacks detection in WSN. For attack detection I proposed an analysis of using the spatial correlation of Received Signal Strength. I evaluate the test depends on the cluster analysis of Received Signal Strength. I can detect attacks, the number of enemies and I can localize any number of attackers even in different transmission levels and remove the attackers using my approach integrated detection and localization of multiple spoofing attackers in WSN.

6 FUTURE WORK

In the future the integrated detection and localization system can detect the attackers, calculate the number of attackers and localizing any number of enemies in different transmission levels by using the hash key algorithm. This algorithm is used to generate the hash key. The hash key is used for both the encryption and decryption. The performance of this algorithm achieves higher results, and it provide effective result in detecting the attacks, calculating the number of attackers and localizing enemies.

7 REFERENCES

[1] F. Ferreri, M. Bernaschi, and L. Valcamonici, “Access Points Vulnerabilities to Dos Attacks in 802.11 Networks,” Proc. IEEE Wireless Comm. and Networking Conf., 2004.

[2] D. Faria and D. Cheriton, “Detecting Identity-Based Attacks in Wireless Networks Using Signal prints,” Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

[3] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2005.

[4] P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RF- Based User Location and Tracking System," Proc. IEEE INFOCOM, 2000.

[5] Q. Li and W. Trappe, "Relationship-Based Detection of Spoofing-Related Anomalous Traffic in Ad Hoc Networks," Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006

[6] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.

[7] L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 4646-4651, June 2007.

[8] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," Proc. 14th ACM Int'l Conf. Mobile Computing and Networking, pp. 116-127, 2008.

[9] F. Guo and T. Chiueh, "Sequence Number-Based MAC Address Spoof Detection," Proc. Eighth Int'l Conf. Recent Advances in Intrusion Detection, pp. 309-329, 2006.

[10] L. Sang and A. Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 2137- 2145, 2008.

[11] E. Elnahrawy, X. Li, and R.P. Martin, "The Limits of Localization Using Signal Strength: A Comparative Study," Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Oct. 2004.

[12] Y. Chen, J. Francisco, W. Trappe, and R.P. Martin, "A Practical Approach to Landmark Deployment for Indoor Localization," Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Sept. 2006.

[13] J. Yang and Y. Chen, "A Theoretical Analysis of Wireless Localization Using RF-Based Fingerprint Matching," Proc. Fourth Int'l Workshop System Management Techniques, Processes, and Services (SMTPS), Apr. 2008.

[14] P. Enge and P. Misra, Global Positioning System: Signals, Measurements and Performance. Ganga-Jamuna Press, 2001.

[15] Z. Yang, E. Ekici, and D. Xuan, "A Localization-Based Anti-Sensor Network System," Proc. IEEE INFOCOM, pp. 2396-2400, 2007.

Query-Adaptive Image Retrieval Framework With Semantic Class Specific Hash Codes.

Guided by: Mrs.D.Deva kirupa Dani
O.Shameena
M.E*-Computer Science And Engineering
C.S.I Institute Of Technology
Email:meenasha41@gmail.com

Abstract— The ability of fast similarity image search based on visual similarity in a large-scale dataset is of great importance to many multimedia applications. Although hashing has been shown effective for visual search, among various hashing approaches semantic hashing (SH) has shown promising performance. It accelerates similarity search, by designing compact binary codes for a large number of images so that semantically similar images are mapped to close codes. Retrieving similar neighbours is then simply accomplished by retrieving images that have codes within a small Hamming distance of the code of the query. This project introduces an approach that enables query-adaptive ranking of the returned images with equal Hamming distances to the queries. This is achieved by firstly offline learning bitwise weights of the hash codes for a diverse set of predefined semantic concept classes. The weight learning process minimize intra-class distance while preserving inter-class relationship captured by original raw image features. Query-adaptive weights are then computed online by evaluating the proximity between a query and the semantic concept classes .With the query-adaptive bitwise weights, returned images can be easily ordered by weighted Hamming distance at a finer-grained hash code level rather than the original Hamming distance level. Experiments on a Flickr image dataset show clear improvements from this proposed approach.

INTRODUCTION

With the explosion of images on the Internet, there is a strong need to develop techniques for efficient scalable image search. While traditional image search engines heavily rely on textual words associated to the images, scalable content-based search is receiving increasing attention. Apart from providing better image search experience for ordinary Web users, large-scale similar image search has also been demonstrated to be very helpful for solving a number of very hard problems in computer vision and multimedia such as image categorization .Generally a large-scale image search system consists of two key components—an effective image feature representation and an efficient search mechanism. It is well known that the quality of search results relies heavily on the representation power of image features. The latter, an efficient search mechanism, is critical since existing image features are mostly of high dimensions and current image databases are huge, on top of which exhautively comparing a query with every database sample is comptationally prohibitive -In this work represent images using the popular bag-of-visual-words (BoW) framework , where local invariant image descriptors (e.g., SIFT) are extracted and quantized based on a set of visual words. The BoW features are then embedded into compact hash codes for efficient search. For this, we consider state-of-the-art techniques including semi-supervised hashing and semantic hashing with deep belief networks . Hashing is preferable over tree-based indexing structures (e.g., kd-tree) as it generally requires greatly reduced memory and also works better for high-dimensional samples. With the hash codes, image similarity can be efficiently measured (using logical XOR operations) in Hamming space by Hamming distance, an integer value obtained by counting the number of bits at which the binary values are different. In large scale applications, the dimension of Hamming space is usually set as a small number (e.g., less than a hundred) to reduce memory cost and avoid low recall .

Although hashing has been shown to be effective for visual search in several existing works , it is important to realize that it lacks in providing a

good ranking that is crucial for image search .As a result, hundreds or even thousands of images may share the same ranking in search result list, but are very unlikely to be equivalently relevant to the query. Although one can exhaustively compute the similarity for such candidate images to obtain exact ranking , it will significantly increase both computational cost and memory needs.

The main contribution of this paper is the proposal of a novel approach that computes *query-adaptive weights* for each bit of the hash codes, which has two main advantages. First, images can be ranked on a finer-grained hash code level since—with the bitwise weights—each hash code is expected to have a unique similarity to the queries. In other words, we can push the resolu- tion of ranking from (traditional Hamming distance level) up to (hash code level[1]). Second, contrary to using a single set of Hamming distance based on real-valued vectors (weights im- posed on the hash codes), which would bury one of the most important advantages of hashing. Instead the weights can be utilized as indicators to efficiently order the returned images (found by logical XOR operations) at hash code level.The query-adaptive bitwise weights need to be computed in real-time. To this end, we harness a set of semantic concept classes that cover many semantic aspects of image content (e.g., scenes and objects). Bitwise weights for each of the semantic classes are learned offline using a novel formulation that not only maximizes intra-class sample similarities but also preserves inter-class relationships. That the optimal weights can be computed by iterativelysolving quadratic programming problems. These pre-computed class-specific bitwise weights are then utilized for online computation of the query-adaptive weights, through rapidly evaluating the prox- imity of a query image to the image samples of the semantic classes. Finally, weighted Hamming distance is applied to evaluate similarities between the query and images in a target database. We name this weighted distance as query-adaptive Hamming distance, as opposed to the query- independent Hamming distance widely used in existing works. Notice that during online search it is unnecessary to compute the weigh.

d

RELATED WORKS

There are very good surveys on general image retrieval task.. while more effective features such as GIST and SIFT have been popular recently . In this work, we choose the popular bag-of-visual-words (BoW) representation grounded on the local invariant SIFT features. The effectiveness of this feature representation has been verified in numerous applications. Since the work in this paper is more related to efficient search, this section mainly reviews existing works on efficient search mechanisms, which are roughly divided into three categories: inverted file, tree-based indexing, and hashing.

Inverted index was initially proposed and is still very popular for document retrieval in the informational retrieval community. It was introduced to the field of image retrieval as recent image feature representations such as BoW are very analogous to the bag-of-words representation of textual documents. In this structure, a list of references to each document (image) for each text (visual) word is created so that relevant documents (im- ages) can be quickly located given a query with several words. A key difference of document retrieval from visual search, how- ever, is that the textual queries usually contain very few words. For instance, on average there are merely 4 words per query in Google web search.[2] While in the BoW representation, a single image may contain hundreds of visual words, resulting in a large number of candidate images (from the inverted lists) that need further verification—a process that is usually based on similar- ities of the original BoW features. This largely limits the appli- cation of inverted files for large scale image search. While in- creasing visual vocabulary size in BoW can reduce the number of candidates, it will also significantly increase memory usage

Indexing with tree-like structures has been frequently applied to fast visual search. a visual vocabulary tree to achieve real-time object retrieval in 40 000 images. Muja and Lowe adopted multiple randomized d-trees for SIFT feature

matching in image ap- plications. One drawback of the classical tree-based methods is that they normally do not work well with high-dimensional feature. For example, let the dimensionality be and the number of samples be , one general rule in order to have d-tree working more efficiently than exhaustive search . There are also several works focusing on improving tree-based approaches for large-scale search , where promising image search performance has been reported. Compared with these methods, hashing hasamajor advantage in speed since it allows constant-time search.

In view of the limitations of both inverted file and tree-based indexing, embedding high-dimensional image features into hash codes has become very popular recently. Hashing satisfies both query time and memory requirements as the binary hash codes are compact in memory and efficient in search via hash table lookup or bitwise operations. Hashing methods normally use a group of projections to divide an input space into multiple buckets such that similar images are likely to be mapped into the same bucket.

Although SH can achieve similar or even better performance than LSH with a fewer number of bits, it is important to under- line that these offer fine-grained ranking of search results, which is very im- portant in practice. This paper proposes a means to rank im- ages at a finer resolution. Note that we will not propose new hashing methods—our objective is to alleviate one weakness that all the hashing methods share particularly in the context of image search.

There have been a few works using weighted Hamming dis- tance for image search, including parameter-sensitive hashing . Hamming distance weighting , and the AnnoSearch. Each bit of the hash codes was assigned with a weight in the main purpose was to weigh the overall Hamming distance of local features for image matching. These methods are fundamentally different from this work. They all used *a single set* of weights to measure either the importance of each bit in Hamming space or to rescale the final Hamming distance for better matching of sets of features while designed to learn different category-specific bitwise weights offline and adapt to each query online. query-adaptive LSH, which is essentially a feature selection process that picks a subset of bits from LSH adaptively for each query. Since their aim was to further reduce search complexity by using less bits, the problem of coarse ranking remains unsolved.

unsupervised hashing techniques are not robust enough for similar image search. This is due to the fact that similarity in image search is not simply equivalent to the proximity of low-level visual features, but is more related to high-level image semantics (e.g., objects and scenes). Under this circum- stance, it is helpful to use some machine learning techniques to partition the low level feature space according to training la- bels on semantic level. Several *supervised* methods have been proposed recently to learn good hash functions .A method to learn hash functions by minimizing reconstruction error be- tween original feature distances and Hamming distances of hash codes. By replacing the original feature distances with semantic similarities, this method can be applied for supervised learning of hash functions. To learn hash func- tions based on semantic similarities of objects in images. A semi-supervised hashing algorithm that learns hash functions based on image labels. The advantage of this algorithm is that it not only utilizes given labels, but also exploits unlabeled data when learning the hash functions. It is especially suitable for the cases where only a limited number of labels are available. The idea of using a few pairwise data labels for hash function learning was also

SYSTEM FRAMEWORK

The proposed query-adaptive image search system is de- picted. To reach the goal of query-adaptive search,

investigated using an algorithm called label-regularized max- we harness a set of semantic concept classes, each with a set of representative images as shown on the left of the figure. Low-level features (bag-of-visual-words) of all the images are embedded into hash codes, on top of which we compute bitwise weights for each of the semantic concepts separately.

The weight computation process is done by an algorithm that lies in the very heart of our approach, which will be discussed later .The

flowchart on the right of Fig. 3 illustrates the process of online search. We first compute hash code of the query image, which is used to search against the images in the predefined se- mantic classes. From there we pool a large set of images which are close to the query in Hamming space, and use them to predict bitwise weights for the query (cf. Section V-

B). One assump- tion made here is that images around the query in Hamming space, collectively, should be able to infer query semantics, and therefore the pre-computed class-specific weights of these im- ages can be used to compute bitwise weights for the query. Fi- nally, with the query-adaptive weights, images from the target database can be rapidly ranked by weighted (query-adaptive) Hamming distance to the query.

HASHING

In this work two state-of-the-art hashing techniques are adopted, *semi-supervised hashing* and *semantic hashing with deep belief networks* .

Semi-Supervised Hashing

Semi-Supervised Hashing (SSH) is a newly proposed algo- rithm that leverages semantic similarities among labeled while remains robust to overfitting . The objective func tion of SSH consists of two major components, supervised em- pirical fitness and unsupervised information theoretic regular- ization. More specifically, on one hand, the supervised part tries to minimize an empirical error on a small amount of labeled data. The unsupervised term, on the other hand, provides ef- fective regularization by maximizing desirable properties like variance and independence of individual bits. Mathematically, one is given a set of points, in which a small fraction of pairs are associated with two categories of label information, and . Specifically, a pair is denoted as a neighbor-pair when share common class labels. Similarly is called a non- neighbor-pair if the two samples have no common class label. The goal of SSH is to learn hash functions

Semantic Hashing With Deep Belief Networks

Learning with deep belief networks (DBN) was initially pro- posed for dimensionality reduction . It was recently adopted for semantic hashing in large-scale search applications . Like SSH, to produce good hash codes DBN also requires image labels during training phase, such that images with the same label are more likely to be hashed into the same bucket. Since the DBN structure gradually reduces the number of units in each layer, the high-dimensional input of original image fea- tures can be projected into a compact Hamming space.

Broadly speaking, a general DBN is a directed acyclic graph, where each node represents a stochastic variable. There are two critical steps in using DBN for hash code generation, the learning of interactions between variables and the inference of observations from inputs. The learning of a DBN with multiple layers is very hard since it usually requires to estimate millions of parameters. Fortunately, it has been shown by Hinton *et al.* in that the training process can be much more efficient if a DBN is specifically structured based on the RBMs. Each single RBM has two layers containing respectively output visible units and hidden units, and multiple RBMs can be *stacked* to form a *deep* belief net. Starting from the input layer with dimension, the network can be specifically designed to reduce the number of units, and finally output compact -di- mensional hash codes. To obtain optimal weights in the entire network, the training process of a DBN has two critical stages: unsupervised pre-training and supervised fine-tuning. The greedy pre-training phase is progressively executed layer by layer from input to output, aiming to place the network weights (and the biases) to suitable neighborhoods in parameter space.

After achieving convergence of the parameters of one layer via Contrastive Divergence, the outputs of this layer are fixed and treated as inputs to drive the training of the next layer. During the fine-tuning stage, labeled data is adopted to help refine the network parameters through back-propagation. codes) within a certain neighborhood share the same label . The network parameters are then refined to maximize this objective function using conjugate gradient descent.In our experiments, the dimension of the

image feature is fixed to 500. Similar to the network architecture used in , we use a five-layer DBN of sizes , where is the dimension of the final hash codes. The training process requires to learn weights in total. For the number of training samples, we use a total number of 160 000 samples in the pre-training stage, and 50 batches of neighborhood regions with size 1000, 1000 in the fine-tuning stage.. Since param- eter training is an offline process, this computational cost is acceptable. Compared to training, generating hash codes with the learned DBN parameters is a lot faster. Using the same com- puter it requires just 0.7 milliseconds to compute a 48-bit hash code of an image.

QUERY-ADAPTIVE SEARCH

With hash codes, scalable image search can be performed in Hamming space using Hamming distance. By definition, the Hamming distance between two hash codes is the total number of bits at which the binary values are different. Specific in- dices/locations of the bits with different values are not consid- ered.. Due to this nature of the Hamming distance, practically there can be hundreds or even thousands of samples sharing the same distance to a query

To learn query-adaptive weights for each bit of the hash codes, so that images with the same Hamming distance to the query can be ordered in a finer resolution.

Learning Class-Specific Bitwise Weights

To quickly compute the query-adaptive weights, we propose to firstly learn class-specific bitwise weights for a number of se- mantic concept classes (e.g., scenes and objects). Assume that we have a dataset of semantic classes, each with a set of representative images (training data). We learn bitwise weights separately for each class, with an objective of maximizing intra-class similarity as well as maintaining inter-class relationship

is the total number of hash codes in . Notice that although the sample proximity, to some extent, was considered in the hashing methods, (1) is still helpful since weighting the hash codes is able to further condense samples from the same class. More importantly, the optimal bitwise weights to be learned here will be the key for computing the query-adaptive weights.In addition to intra-class similarity, we also want the inter-class relationship in the original image feature (BoW) space to be preserved by the weighted Hamming distance. Let denote the proximity between classes andquantifie using average BoW feature similarity of samples from classes and . Then it is expected that the weighted hash codes in the two classes should be relatively more similar if is large. This maintains the class relationship, which is im- portant since the semantic classes under our consideration are not fully exclusive. Some of them are actually highly correlated (e.g., *tree* and *grass*). and distance metric learning, although ours is particularly designed for this specific application.

LDA is a well-known method that linearly projects data into a low-dimensional space where the sample proximity is reshaped to maximize class separability. While LDA also tries to condense samples from the same class, it learns a single uniform transformation matrix to map all original -dimensional features to a lower - dimensional space. In contrast, we learn a - dimensional weight vector separately for each class.

Distance metric learning tries to find a metric such that sam- ples of different classes in the learned metric space can be better separated. Typically a single Mahalanobis distance metric is learned for the entire input space . There are also a few ex- ceptions where multiple metrics were considered, e.g., a metric was trained for each category . These methods are rel-evant in the sense that they also deal with multiple categories separately. Nevertheless, they cannot be directly applied to our problem, because the class-specific bitwise weights are in a very different form from that of distance metric matrices.

Computing Query-Adaptive Bitwise Weights

As described in Fig. 3, images and the learned weights of the predefined semantic concept classes form a *semantic database* for rapid computation of the query-adaptive bitwise weights. Given a query image and its hash codes , the objective

here is to adaptively determine a suitable weight vector , such that weighted Hamming distance (WHD) can be applied to compare with each hash code in the target database:

convergence Analysis and Implementation*:* As stated ear- lier, given all , the quadratic program in (10) is convex. Solving it with global minimization w.r.t. will always reduce the value of the energy function in (4), which will definitelnot be greater than the energy value derived from a previous iteration. In addition, it is obvious that the energy function is lower-bounded since both terms of the function are non-negative. Therefore, the iterative optimization process given in Algorithm 1 is a Block Coordi- nate Descent approach, which gradually reduces the energy and leads to convergence at a non-negative value.

In practice, to avoid long time convergence procedure, we de- fine an empirical stop condition (convergence) when the energy differenceof two successive states ,where and is set as a small value (in our experiments). Having such a stop con- dition can help avoid unneeded deep optimization that leads to almost invisible changes to the bitwise weights.

2) Connections to Existing Algorithms: We briefly discuss the differences and connections of our proposed algorithm to some well-known machine learning methods such as LDA.

To compute , we query against the semantic database based on typical Hamming distance. Semantic labels of the top- most similar images are collected to predict query se- mantics, which is then utilized to compute the query-adaptive weights. Specifically, denote as the set of the most relevant semantic classes to the query , and as the number of images (within the top list) from the class in the query. In other words, we do not need to order all the hash codes in practice; only the small subset of hash codes with a few bits different from the query is sufficient for pooling the top search results of a query image. In this way, it's possible that some of the hash codes are incorrectly excludefro the initial subset. But the true top matched hash codes with the shortest weighted distances are preserved.

Extension to Query-Adaptive Hash Code Selection

The above approach is designed to use a single set of general hash codes for image search. In this subsection, we further ex- tend our approach to the case where multiple sets of hash codes are available. Since there are multiple semantic concept classes, it is very easy to train a set of hash codes for each class by exten- sively using images containing the corresponding concept. The class-specific hash codes are expected to be more discriminative for a particular class of images. The weight learning algorithm introduced in Section I can be applied to each set of class-spe- cific hash codes to produce a separate group of bitwise weights. During online search, the semantic database is used not only for computing query-adaptive weights, but also to select a suitable set of class-specific hash codes for each query. depicts the extended framework. Given a query image, we first compute its *general* (globally trained) hash code and query against the semantic database. Like the query-adaptive weight computation process introduced earlier, we use the same set of images to predict query semantics. Hash codes trained for the dominant concept class in this selected set will be chosen. The query is then embedded into the selected class-specific hash code using hash functions trained for the corresponding concept class. Finally, the new hash code is concatenated with the gen- eral code for search, and results are sorted at binary code level based on bitwise weights predicted from a similar procedure as described in Section V.B. This new framework provides a means to adaptively select both hash codes and bitwise weights. Addi- tional computation is required in this extended framework as the query needs to be hashed twice and more bits are used in search. Fortunately, since both testing process (hash code computation) of the hashing algorithms and logical XORoperations are very efficient, this added computational cost is acceptable in general.

EXPERIMENTAL SETUP

Dataset, Training, and Performance Measurement

Conduct image search experiments using the widely adopted NUS-WIDE dataset . NUS-WIDE contains 269,648 Flickr images, divided into a training set (161,789 images) and a test set (107,859 images). It is fully labeled with 81 semantic concept classes, covering many topics from ob-jects (e.g., *bird* and *car*) to scenes (e.g., *mountain* and *harbor*). Each image in NUS-WIDE may contain multiple semantic classes. Fig. 5 shows several example images from this dataset. Notice that NUS-WIDE is one of the largest publicly available datasets with complete labels of a wide range of classes. Other well-known and larger datasets such as ImageNet and MIT TinyImages are either not fully labeled[4] or unlabeled, which are therefore not suitable for quantitative performance evaluation.

Local invariant features are extracted from all the images based on Lowe's DoG detector and SIFT descriptor . Soft- weighted bag-of-visual-words features are then computed using a visual vocabulary generated by clustering a subset of SIFT features . The concepts in NUS-WIDE are very suitable for constructing the semantic database in our approach. Therefore we use the training images to learn a general set of hash func- tions by applying labels from every class. On the same training set, we also learn the class-specific hash functions by exten- sively applying training labels from each class. Class-specific bitwise weights are learned for the general hash functions, as well as for each set of the class-specific hash functions, using the algorithm introduced in Section V. The weight learning al- gorithm is very efficient; training bitwise weights for a set of hash codes only needs 5 minutes on a regular PC (Intel Core2Duo 2.4 GHz CPU and 2GB RAM).

For performance measurement, we rank all images in the NUS-WIDE test dataset according to their (weighted) Hamming distances to each query. An image will be treated as a correct hit if it shares at least one common class label to the query. Perfor- mance is then evaluated by AP, an extended version of av- erage precision where prior probability, i.e., the proportion of relevant images in the test set to the query, is taken into account [44]. To aggregate performance of multiple queries, mean AP (MAP) is used.

EvaluationPlan

Part 1: Characteristics of hash codes based image search. At the beginning of the evaluation, experimentally verify one weakness of hash codes based image search, i.e., the coarse ranking problem, which is also the main motivation of this work.

Part 2: Query-adaptive ranking. This set of experiments evaluates the proposed framework for query-adaptive ranking of search results. Hash codes from both SSH and DBN will be adopted. Specifically, compare performance of the refined ranking (by the weighted query-adaptive Hamming distance) with original results by traditional Hamming distance, using the two different types of hash codes separately.

Part 3: Query-adaptive hash code selection. The last exper-iment tests the extension of query-adaptive search to dynamic hash code selection. Here only use SSH codes since training DBN codes for 81 concept classes is extremely slow. The purpose of this experiment is to learn how much performance gain class-specific hash codes could offer. To the best of knowledge, similar empirical analysis has never been conducted in previous studies.

RESULTS AND DISCUSSIONS

Characteristics of Hash Codes Based Search

Let us first check the number of test images with each Hamming distance value to a query. The 48-bit hash codes from DBNn are used in this experiment. Note that we will not specifically investigate the effect of code-length in this paper, since several previous works on hashing have already shown that codes of 32–50 bits work well in practice . In general, using more bits may lead to higher precision, but at the price of low recall and longer search time,averaged over 20000 randomly selected queries. As shown in the figure, the number of returned images at each Hamming distance rapidly grows with the distance values until . This verifies one nature of Hamming distance, as mentioned in the introduction, there can be different hash codes sharing the same integer distance to a query in a -dimensional

Hamming space. Consequently, the number of hash codes (and correspondingly the number of images) at each specific distance increases dramatically as grows until . For some queries, there can be as many as images sharing equal distances. This motivates the need of our proposed approach that provides ranking at a finer granularity. Although does not permutere-rank images with Hamming distance 0 to the queries, this analysis reveals that this is not a critical issue since most queries have none or just a few such images .

Query-Adaptive Ranking

On to evaluate how much performance gain can be achieved from the proposed query-adaptive Hamming distance, using 32-bit and 48-bit hash codes from both SSH and DBN (the general sets trained with labels from every class). Randomly pick 8,000 queries (each contains at least one semantic label) and compute averaged per- formance over all the queries. As shown in Fig. 7(a), (c), our approach significantly outperforms traditional Hamming dis- tance. For the DBN codes, it improves the 32-bit baseline by 6.2% and the 48-bit baseline by 10.1% over the entire rank lists. A little lower but very consistent improvements (about5%) are obtained with the SSH codes. The steady improvements clearly validate the usefulness of learning query-adaptive bit- wise weights for hash codes based image search.part of search results, using the same set of queries. The aim of this evaluation is to verify whether our approach is able to improve the ranking of top images, i.e., those with relatively smaller Hamming distances to the queries. As expected, we ob- serve similar performance gain to that over the entire list.

Looking at the two hashing methods, DBN codes are better because more labeled training samples are used (50 k for DBN vs. 5 k for SSH). Note that the comparison of DBN and SSH is beyond the focus of this work, as the latter is a semi-supervised method, which prefers and is more suitable for cases with lim- ited training samples. Direct comparison of the two with equal training set size can be found in .To see whether the improvement is consistent over the eval- uated queries, we group the queries into 81 categories based on their associated labels.

C. Query-Adaptive Hash Code Selection

Finally we evaluate query-adaptive hash code selection, following the extended framework described in Section V.C. We see obvious performance improvement from this extension, with overall gains 9.4% (32-bit) and 8.1% (48-bit) over the results obtained by query-adaptive ranking with general hash codes (15.0% and 13.7% respectively over the baseline traditional ranking). Over the upper half of search result lists, the improvement over query-adaptive ranking is very significant: 31.2% and 32.8% for 32-bit and 48-bit codes respectively. These results confirm the effectiveness of the class-specific hash codes and our query-adaptive code selection framework. In addition, we also find that the query-adaptive weights imposed on the selected class-specific hash codes do not contribute as much as that on the general hash codes (around 2%, versus 5–10% on the general codes). This is probably because the hash code selection process already takes query semantics into account by choosing a more suitable set of hash codes for each query. Although the bitwise weights can still improve result ranking, from query-adaptive perspective very limited additional information can be further attained.While promising, it is worth noting that the query-adaptive hash code selection framework incurs additional computation and memory cost. First, query images need to be hashed twice and search needs to be performed with more bits, which—as mentioned in Section V.C—are generally acceptable since hashing algorithms and bitwise operations are efficient. Second and more importantly, in order not to affect real-time search, we also need to pre-load the class-specific codes of all database samples, which would require 81 times of the memory needed by the general codes. Although this is still much less than that needed by original raw features, the requirement is nontrivial when very large database is in use. Therefore we conclude that class-specific hash codes are useful for improved performance, but this introduces a trade-off between search performance and memory usage that needs to be carefully considered in real-world applications, e.g., per

application needs and hard- ware configuration.

CONCLUSION

We have presented a novel framework for query-adaptive image search with hash codes. By harnessing a large set of pre- defined semantic concept classes, our approach is able to predict query-adaptive bitwise weights of hash codes in real-time, with which search results can be rapidly ranked by weighted Ham- ming distance at finer-grained hash code level. This capability largely alleviates the effect of a coarse ranking problem that is common in hashing-based image search. Experimental results on a widely adopted Flickr image dataset confirmed the effec- tiveness of our proposal.

To answer the question of "how much performance gain can class-specific hash codes offer?", we further extended our framework for query-adaptive hash code selection. Our findings indicate that the class-specific codes can further improve search performance significantly. One drawback, nevertheless, is that nontrivial extra memory is required by the use of additional class-specific codes, and therefore we recommend careful examination of the actual application needs and hardware environment in order to decide whether this extension could be adopted.

REFERENCES

[1] A. Torralba, R. Fergus, and W. Freeman, "80 million tiny images: A large data set for nonparametric object and scene recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 30, no. 11, pp. 1958–1970, Nov. 2008.

[2] J. Sivic and A. Zisserman, "Video Google: A text retrieval approach to object matching in videos," in *Proc. IEEE Int. Conf. Computer Vision*, 2003.

[3] D. Lowe, "Distinctive image features from scale-invariant keypoints," *Int. J. Comput. Vision*, vol. 60, no. 2, pp. 91–110, 2004.

[4] J. Wang, S. Kumar, and S.-F. Chang, "Semi-supervised hashing for scalable image retrieval," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, 2010.

[5] G. Hinton and R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," *Science*, vol. 313, no. 5786, pp. 504–507, 2006.

[6] R. Salakhutdinov and G. Hinton, "Semantic hashing," in *Proc. Work- shop of ACM SIGIR Conf. Research and Development in Information Retrieval*, 2007.

[7] J. L. Bentley, "Multidimensional binary search trees used for associa- tive searching," *Commun. ACM*, vol. 18, no. 9, pp. 509–517, 1975.

[8] A. Torralba, R. Fergus, and Y. Weiss, "Small codes and large image databases for recognition," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, 2008.

[9] Y. Weiss, A. Torralba, and R. Fergus, "Spectral hashing," in *Adv.Neural Inf. Process. Syst.*, 2008.

[10] J. Wang, S. Kumar, and S.-F. Chang, "Sequential projection learning for hashing with compact codes," in *Proc. Int. Conf. Machine Learning*, 2010.

Spam Message Detection Using Effective Spot System

G.Mariammal
PG Scholar
Infant Jesus College of Engineering
Thoothukudi.
Email:mariammalswe@gmail.com

Dr.S.Allwin, M.E., Ph.D.
Associate professor
Infant Jesus College of Engineering
Thoothukudi.
Email:allwinstephen@gmail.com

***ABSTRACT*- Develop an effective spam zombie detection system named SPOT. In the network SPOT can be used to monitoring outgoing messages. Using internet some attacker try to spread the spams or malware in order to collect the information about the network. The detection of the compromised machines in the network that are involved in the spamming activities is known as spam zombie detection system. The detection system can be used to identify the misbehavior of the person using Spam zombie detection system. We will create a framework to identify the message from the various persons. This system will record the information of the IP address using SPOT Detection Algorithm. We also compare the performance of SPOT with two other spam zombie detection algorithms based on the count and percentage of spam messages originated or forwarded by internal machines. Using these above techniques we will avoid and block the person who sends the spam's message.**

Index term— SPOT System, SPOT Detection Algorithm, Count-threshold, Percentage-threshold.

I. INTRODUCTION

Existence of the large number of compromised machines is the major security challenge on the internet. Compromised machines have been increasingly used to launch various security attacks such as spamming and spreading malware, DDoS, and identity theft [6]. Then identifying and cleaning compromised machines in a network remain significant challenges for system administrators of networks of all sizes. Mainly focus on the detection of the compromised machines in a network that are used for sending spam messages, which are commonly referred to as spam zombies. A Spam zombie is the detection of the compromised machines in the network that are involved in the spamming activities [6]. Given that spamming provides a critical economic incentive for the controller of the compromised machines to recruit these machines, it has been used to observe that many compromised machines are involved in spamming [9][10][12]. A number of recent research efforts have studied the aggregate global characteristics of spamming botnets such as the size of botnets and the spamming patterns of botnets, based on the sampled spam messages received at a large email service provider [12]. The main aim is to develop a tool for system administrators to automatically detect the compromised machines in their networks in an online manner. Normally in the network the local generated outgoing messages cannot provide the aggregate large-scale spam view required by these approaches [5]. These approaches cannot support the online detection requirement in the environment. The nature of sequentially observing outing messages gives rice to the sequential detection problem. We will develop a spam zombie detection system, named SPOT.

The Spot can be used to monitoring outgoing messages. SPOT is designed based on a statistical method called Sequential Probability Ratio Test (SPOT).

SPRT is a powerful statistical method that can be used test between two systems sequentially in our case machine is compromised versus the machine is not compromised and another case based on outing messages.

Both the false positive and false negative probabilities of SPRT can be bounded by user-defined thresholds. SPOT system can be used to select the desired thresholds to control the false positive and false negative rates of the system.

We develop the SPOT detection system, the system administrators can be used to automatically identifying the compromised machines in their networks. Evaluate the performance of the SPOT system based on a two-month e-mail trace collected in a large US campus network.

Based on evaluation studies show that SPOT is an effective and efficient system in automatically detecting compromised machines in a network [11].

In addition, SPOT only needs a small number of observations to detect a compromised machine. Majority of spam zombies are detected with as little as three spam messages. At the time of comparison, we also design and study two other spam zombie detection algorithms based on the number of spam messages and the percentage of spam messages originated or forwarded by internal machines.

Also compare the performance of SPOT with the two other detection algorithms to explain the advantages of the SPOT system.

A. Analysis

SPOT Tool will be useful for the Administrators of a Organization for detecting the Spamming Machines that is Compromised Machines in their Organization. Spam Zombie Detection System can easily find the Spammers who are all involved in spamming activities without deviation.

II. RELATED WORK

In the related work we discuss the detection of compromised machines. The characterizing spamming botnet by leveraging both spam payload and spam server traffic properties. We developed a spam signature generation framework called *AutoRE* to detect botnet-based spam emails and botnet membership [12]. Our in-depth analysis of the identified botnet revealed several interesting finding regarding the degree of email obfuscation, properties of botnet IP addresses, sending patterns, and their correlation with network scanning traffic [1]. To group bots into botnets we look for multiple bots participating in the same spam email campaign. We have applied our technique against a trace of spam email from Hotmail web mail services.

In this trace, we have successfully identified hundreds of botnet. We present new finding about botnet sizes and behavior while also confirming other researcher's observations derived by different methods. In addition, using this information combined with a three-month Hotmail email server log, we were able to establish that 97% of mail servers setup on dynamic IP addresses sent out solely spam emails, likely controlled by zombies [2]. Moreover, these mail servers sent out a large amount of spam- counting towards over 42% of all spam emails to Hotmail. These results highlight the importance of being able to accurately identify dynamic IP addresses for spam filtering, and we expect similar benefits of it for phishing site identification and botnet detection. To our knowledge, this is the first successful attempt to automatically identify and understand IP dynamics.

We reveal one salient characteristic of proxy-based spamming activities, namely packet symmetry, by analyzing protocol semantics and timing causality [6]. Based on the packet symmetry exhibited in spam laundering, we propose a simple and effective technique, DBSpam, to on-line detect and break spam laundering activities inside a customer network [8].

We provide the first comprehensive study on the received: header field of spam emails to investigate, among others, to what degree spammers can and do forge the trace information of spam emails. Also report our findings and discuss the implications of the findings on various spam control efforts, including email sender authentications and spam filtering [3].

We find that most spam is being send from a few regions of IP address space, and that spammers appear to be using transient "bots" that send only a few pieces of email over very short periods of time. Finally, a small, yet non-negligible, amount of spam is received from IP addresses that correspond to short-lived BGP routes, typically for hijacked prefixes. These trends suggest that developing algorithms to identify botnet membership, filtering email messages based on network-level properties, and improving the security of the internet routing infrastructure, may prove to be extremely effective for combating spam [9].

A. Problem Formation and Assumptions

In the network formulate the spam zombie detection problem. We discuss the network model and assumptions can be used to make in the detection problem. Fig.1 describes the logical view of the network model. Assume that messages originated from machine inside the network. The message will pass the developed spam zombie detection system. This assumption can be achieved in a few different scenarios.

In the network assume that the machine has been either compromised or normal (that is, not compromised). The term compromised machine is denoted as spam zombie. The detection system assumes that the behavior of a compromised machine is different from that the normal machine based on the messages sending. Based on the higher probability the compromised machines are generating a spam message compare to the normal machine. Once a decision is reached, the detection system reports the result, and further action can be taken. We assume that a content-based spam filter is developed at the detection system. The outgoing message can be classified as either a spam or nonspam using the detection system. None of existing spam filters can achieve perfect spam detection accuracy. They all suffer from both false positive and false negative errors. The false negative rate of spam filter measures the percentage of spam messages that are misclassified.

The false positive rate measures the percentage of nonspam message that are misclassified. We assume that a sending machine m as observed by the spam zombie detection system is an end-user client machine. It is not a mail relay server.

.

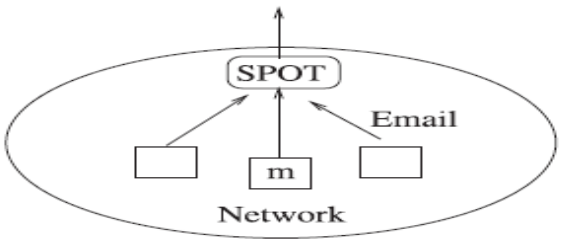


Fig 1 Network Model

B. Sequential Probability Ratio Test

SPRT can be used to monitor the network performance. The goal of the SPRT is to decide which hypothesis is correct as soon as possible. SPOT is designed based on a powerful statistical method called Sequential Probability Ratio Test. SPRT has bounded false positive and false negative error rates.

The SPRT is the powerful statistical method that can be used to test between two systems sequentially. In our case machine is compromised versus the machine is not compromised another case based on the outgoing messages. Provide the necessary background on the Sequential Probability Ratio Test for understanding the proposed spam zombie detection system. SPRT is a statistical method for testing a simple null hypothesis against a single alternative hypothesis.

SPRT can be considered as a one-dimensional random walk with two user-specified boundaries corresponding to the two hypotheses. Based on simple and powerful statical tool, SPRT has a number of compelling and desirable features that lead to the widespread applications of the technique in many areas. Before the SPRT terminates smaller error rate tends to require a large number of observations. The user can balance the performance and cost of an SPRT test. In second, has been provide that SPRT minimizes the average number of the required observations for reaching a decision for a given error rate, among all Sequential and non sequential statistical tests.

III. SPAM ZOMBIE DETECTION ALGORITHMS

In this section we develop three spam zombie detection algorithm. First one is SPOT, which utilizes the Sequential Probability Ratio Test. We discuss the impacts of SPRT parameters on SPOT in the content of spam zombie detection. The other two spam zombie detection algorithms are developed based on the number of spam messages and the percentage of spam messages sent from an internal machine.

A. Spot Detection Algorithm

SPOT is designed based on the powerful statistical tool called SPRT. In the below, we describe the SPOT detection algorithm. When an outgoing messages arrives at the SPOT detection system. After the outgoing message reach to the SPOT detection system the sending machine's IP address is recorded.

Based on the recorded IP address, then the message is classified as either spam or nonspam by the content- based spam filter. For each observed IP address, SPOT maintains the logarithm value of the corresponding probability ratio Λ_n. A and B the algorithm determines if the corresponding machine is compromised, normal, or a decision cannot be reached and additional observations are needed.

Algorithm 1:

Step 1: Outgoing message arrives at SPOT
Step 2: Get IP address of sending machine *m*
Step 3: //all following parameters specific to machine *m*
Step 4: Let *n* be the message index
Step 5: Let $X_n = 1$ if message is spam, $X_n = 0$ otherwise
Step 6: **if** ($X_n = = 1$) **then**
Step 7: // spam, 3
Step 8: $\Lambda_n + = \ln \theta_1 / \theta_0$
Step 9: **else**
Step 10: // nonspam
Step 11: $\Lambda_n + = \ln (1-\theta_1) / (1-\theta_0)$
Step 12: **end if**
Step 13: **if** ($\Lambda_n \geq B$) **then**
Step 14: Machine *m* is normal. Test is reset for *m*.
Step 15: **else if** ($\Lambda_n \leq A$) **then**
Step 16: Machine *m* is normal. Test is reset for *m*.
Step 17: $\Lambda_n = 0$
Step 18: Test continues with new observations
Step 19: **else**
Step 20: Test continues with an additional observation
Step 21: **end if**

From the viewpoint of network monitoring, it is more important to identify the machine that has been compromised than the machines that are normal. After a machine has been identified as compromised, then these compromised machines are added into the list of potentially compromised machines that system administrators can go after to clean.

Also record the message-sending behavior of the machine. Before the machine is cleaned and removed from the list, the SPOT detection system does not need to further monitor the message-sending behavior of the machine.

Currently the machine has been normal may get compromised at a later time. We need to continuously monitor machines that are determined to be normal by SPOT. Once such a machine is identified by SPOT, the records of the machine in SPOT are reset, in particular, the value of Λ_n is set to zero, so that a new monitoring phase starts for the machine.

B. Spam Count and Percentage-Based Detection Algorithm

In this section, we present two different algorithms in detecting spam zombies. First one is based on the number of spam messages and another the percentage of spam messages send from an internal machine. We refer to them as the count-threshold (CT) detection algorithm and the percentage-threshold (PT) detection algorithm.

In CT, the time is partitioned into fixed length *T*. A threshold parameter C_s specifies the maximum number of spam message that be originated from a normal machine in any time. The system monitors the number of spam messages *n*. That message can be originated from a machine. If $n > C_s$ then the algorithm declares that the machine has been compromised.

Similarly, in PT detection algorithm, the time is partitioned into fixed length *T*. In each internal machine in each time PT monitors two e-mail properties. The first one is

based on the percentage of spam messages send from a machine. Then the second one is based on the total number of messages. Let N and n denote the total messages and spam messages originated from a machine m within a time. Then PT declares machine m as being compromised if $N \geq C_a$ and $n/N > P.C_a$ is the minimum number of messages that a machine must send. Then P is the user-defined maximum spam percentage of a normal machine.

C. Dynamic IP Addresses

For simplicity ignored the potential impact of dynamic IP addresses and assumed that an observed IP corresponds to a unique machine. In the following, we discuss how well the three algorithms fair with dynamic IP addresses. Formally evaluate the impacts of dynamic IP addresses on detecting spam zombies using a two-month e-mail trace collected on a large US campus network. Extremely the SPOT can work in the environment of dynamic IP addresses. We have noted three or four observations are sufficient for SPRT to reach a decision for the vast majority of cases. If a machine is compromised, more than three or four spam messages will be sent before the user shutdowns the machine and the corresponding IP address gets reassigned to a different machine. Therefore, the dynamic IP addresses will not have any significant impact on the SPOT.

Dynamic IP addresses can have a greater effect on the other two detection algorithm Ct and PT. In first, both required the continuous monitoring of the sending behavior of a machine for at least a specified time.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the three detection algorithm based on performance of SPOT, performance of count threshold and the performance of percentage threshold.

A. Performance of SPOT

In this section, evaluate the performance of SPOT based on the collected e-mails. The infected messages are only used to confirm if a machine is compromised in order to study the performance of SPOT. Infected messages are not used by SPOT. SPOT relies on the spam messages instead of infected messages to detect if a machine has been compromised to produce the result. Infected messages are more likely to be observed during the spam zombie detection system. To improve the performance the infected messages can be easily incorporated into the SPOT system. Table 1 shows the performance of SPOT detection system.

B. Performance of Count Threshold

Table 2 shows the performance of count threshold which include the machine IP addresses, count threshold value and the machine status. Use the same methods to confirm detection or identify a missed IP address as we have done with the SPOT detection algorithm. In the machine IP address status has denote the machine IP addresses. In the count threshold value status the value of the count threshold value can be defined. Then in the machine status can be define, if the machine is compromised or uncompromised, based on the performance.

C. Performance of Percentage Threshold

Table 3 shows the performance of Percentage Threshold which includes the machine IP address, count threshold, percentage threshold and also the machine status. First note that the methods to confirm detection or identify a missed IP address are different from the ones used in SPOT, CT and PT. From the table we can see that, CT and PT performance. In the machine IP address status has denote the performance of the machine IP address. In the count and the percentage threshold define the threshold value in the table. In the machine status has been defined, if the machine is compromised or the machine is uncompromised.

TABLE 1
SPAM SENDING MACHINE DETAIL

From IP	Total	Non Spam	Spam
127.0.0.1	3	3	0
127.0.0.1	1	1	0
124.0.2.1	20	2	18
124.0.2.2	15	12	3
124.0.2.1	8	7	1

TABLE 2
NORMAL SPAM'S COUNT FOR THRESHOLD

FROM IP	COUNT THRESHOLD VALUE	MACHINE STATUS
127.0.0.1	0	UNCOMPROMSED
127.0.0.1	2	COMPROMSED
124.0.2.1	0	UNCOMPROMSED
124.0.2.2	5	COMPROMSED
124.0.2.1	0	UNCOMPROMSED

TABLE 3
NORMAL SPAM PERCENTAGE -40%

FROM IP	COUNT THRESHOLD	PERCENTAHGE THRESHOLD	MACHINE STATUS
127.0.0.1	0	0%	UNCOMPROMSED
127.0.0.1	7	95%	COMPROMSED
124.0.2.1	0	0%	UNCOMPROMSED
124.0.2.2	3	100%	COMPROMSED
124.0.2.1	0	0%	UNCOMPROMSED

V. EXPERIMENTAL AND RESULT

A mail system machines are involved in the mail transactions. The machine which is entering into the network will be monitored by the SPOT. It will monitor the spam messages sent by the system. If the message exceeded the level in the sense SPOT will do some process and decide that system as Spam Zombie. This detection is based on the

outgoing messages. SPOT is a lightweight compromised machine detection system.

SPOT detection can be used to identify the compromised machine quickly. It also minimizes the number of required observations to detect a spam zombie. System administrators can automatically detect the compromised machines in their network in an online manner.

VI. CONCLUSION

In this paper, we developed an effective spam zombie detection system named SPOT. In the network the SPOT can be used to monitoring outgoing messages. SPOT was designed based on a simple and powerful statistical method named as Sequential Probability Ratio Test (SPRT). SPRT can be used to detect the compromised machines that are used to involve in the spamming activities. SPRT can be used to minimize the number of required observations to detect a spam zombie. SPOT is an effective and efficient system in automatically detecting compromised machines in a network. Also the SPOT outperforms two other detection algorithm based on the number and percentage of spam messages sent by an internal machine.

REFERENCES

[1] Bacher.P, Holz.T, Kotter.M, and Wicherski.G, "Know Your Enemy: Tracking Botnets 2011.

[2] Chen.Z, Chen.C, and Ji.C, (2007) "Understanding Localized-Scanning Worms," Proc. IEEE Int'l Performance, Computing, and Comm. Conf. (IPCCC '07), 2007.

[3] Droms.R, "Dynamic Host Configuration Protocol," IETF RFC 2131, Mar. 1997.

[4] Duan.Z, Dong.Y, and Gopalan.K, "DMTP: Controlling Spam through Message Delivery Differentiation," Computer Networks, vol. 51, pp. 2616-2630, July 2007.

[5] Duan.Z, Gopalan.K, and Yuan.X, (2006) "Behavioral Characteristics of Spammers and Their Network Reachability Properties," Technical Report TR-060602, Dept. of Computer Science, Florida State Univ., June 2006.

[6] Duan.Z, Gopalan.K, and Yuan.X, (2007) "Behavioral Characteristics of Spammers and Their Network Reachability Properties," Proc.IEEE Int'l Conf. Comm. (ICC '07), June 2007.

[7] Gu.G, Perdisci.R, Zhang.J, and Lee.W, (2008) "BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection," Proc. 17th USENIX Security Symp. July 2008.

[8] Gu.G, Porras.P, Yegneswaran.V, Fong.M, and Lee.W, (2007) "BotHunter: Detecting Malware Infection through Ids-Driven Dialog Correlation," Proc. 16th USENIX Security Symp. Aug. 2007.

[9] Gu.G, Zhang.J, and Lee.W, (2008) "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic," Proc. 15th Ann. Network and Distributed System Security Symp. (NDSS '08), Feb. 2008.

[10] Ianelli.N and Hackworth.A, "Botnets as a Vehicle for Online Crime," Proc. First Int'l Conf. Forensic Computer Science, 2006.

[11] John.J.P, Moshchuk.A, Gribble.S.D, and Krishnamurthy.A, (2009) "Studying Spamming Botnets Using Botlab," Proc. Sixth Symp.Networked Systems Design and Implementation (NSDI '09), Apr. 2009.

[12] Jung.J, Paxson.V, Berger.A, and Balakrishnan.H, (2004) "Fast Portscan Detection Using Sequential Hypothesis Testing," Proc. IEEE Symp.Security and Privacy, May 2004.

[13] Klensin.J, "Simple Mail Transfer Protocol," IETF RFC 2821, Apr. 2001.

[14] Markoff.J, "Russian Gang Hijacking PCs in Vast Scheme," The New York Times, Aug. 2008.

[15] Resnick.P, "Internet Message Format," IETF RFC 2822, Apr. 2001.

[16] Radosavac.S, Baras.J.S, and Koutsopoulos.I, (2005) "A Framework for MAC Protocol Misbehavior Detection in Wireless Networks,"Proc. Fourth ACM Workshop Wireless Security, Sept. 2005.

[17] Ramachandran.A and Feamster.N, (2006) "Understanding the Network- Level Behavior of Spammers," Proc. ACM SIGCOMM, pp. 291-302, Sept. 2006.

[18] Sanchez.F, Duan.Z, and Dong.Y, (2010) "Understanding Forgery Properties of Spam Delivery Paths," Proc. Seventh Ann. Collaboration, Electronic Messaging, Anti-Abuse and Spam Conf. (CEAS '10), July 2010.

[19] SpamAssassin, "The Apache SpamAssassin Project," http:// spamassassin.apache.org, 2011.

[20] Wald.A, Sequential Analysis. John Wiley & Sons, 1947.

[21] Wetherill.G.B and Glazebrook.K.D, Sequential Methods in Statistics. Chapman and Hall, 1986.

[22] Wood et al.P, "MessageLabs Intelligence: 2010 Annual Security Report," 2010.

[23] Xie.Y, Xu.F, Achan.K, Gillum.E, Goldszmidt.M, and Wobber.T, "How Dynamic Are IP Addresses?" Proc. ACM SIGCOMM, Aug. 2007.

[24] Xie.Y, Xu.F, Achan.K, Panigrahy.R, Hulten.G, and Osipkov.I, "Spamming Botnets: Signatures and Characteristics," Proc. ACM SIGCOMM, Aug. 2008.

[25] Xie.M, Yin.H, and Wang.H, (2008) "An Effective Defense against Email Spam Laundering," Proc. ACM Conf. Computer and Comm. Security, Oct. /Nov. 2006.

[26] Zhuang.L, Dunagan.J, Simon.D.R, Wang.H.J, Osipkov.I, Hulten.G, and Tygar.J.D, "Characterizing Botnets from Email Spam Records," Proc. First Usenix Workshop Large-Scale Exploits and Emergent Threats, Apr. 2008.

GNP BASED FUZZY CLASS ASSOCIATION RULE MINING

J.Maheswari[1]

First year M.E student[1] Department of computer science and engineering

[1]Renganayagi varatharaj college of engineering,Sivakasi.

[1]Umaram.sweety8@gmail.com

Abstract

As the Internet services spread all over the world,many kinds of security threats are increasing. Therefore,existing Intrusion Detection Systems (IDS) facing very serious issue for the Internet users for their day to day online transactions, like Internet banking, online shopping, foreign exchange and trading stocks. Genetic Algorithm is used to identify various attacks on different type of connections. This algorithm takes into consideration of different features in network connections such as protocol type, duration, service, to generate a classification rule set. Each rule set identifies a specific type of attacks. A novel fuzzy class-association rule mining method based on Genetic Network Programming (GNP) is used for detecting such network intrusions. By combining fuzzy set theory with GNP, the proposed method can deal with KDDCup99 mixed dataset that contains both discrete and continuous attributes. This method focuses on building distribution of normal and intrusion accesses based on fuzzy GNP. In an application of intrusion detection the training dataset contains both normal connections and several kinds of intrusion connections. GNP examines all the tuples of the connections in the dataset to pick up the rules to be stored in two independent rule pools; normal pool and intrusion pool. Fitness function is defined, higher fitness of a rule results in high Detection Rate (DR) and low Positive False Rate (PFR), which means probability of intrusion is high in the connection. By using this data can be classified into normal class, intrusion class.

Keywords:Genetic Network Programming, Class-association-rule mining, Fuzzy membership function, Intrusion detection, KDDCup99 dataset.

1. INTRODUCTION

Now a day's many kinds of systems over the Internet such as online shopping, Internet banking, trading stocks and foreign exchange, and online auction have been developed. However, due to the open society of the Internet, the security of our computer systems and data is always at risk. The extensive growth of internet has prompted network intrusion detection to become a critical
component of infrastructure protection mechanisms. Network intrusion detection can be defined as identifying a set of malicious actions that threaten the integrity, confidentiality and availability of a network resource. Intrusion detection is traditionally divided into two categories, i.e., misuse detection and anomaly detection. Misuse detection mainly searches for specific patterns or
sequences of programs and user behaviors that match well-known intrusion scenarios [1].
In 1987 Dorothy E. Denning proposed intrusion detection as is an approach to counter the computer and networking attacks and misuses [2]. It is highly difficult to provid complete security to the system though we have several protection techniques. In the network accessing and exchanging the information may be easy but providing the security for the information is difficult. Intrusion detection recognizes the unauthorized access to the network, mischievous attacks on the computer systems. To recognize the attacks and detect the intrusions the intrusion detection technology is more useful.
Intruders can be classified into two types as External Intruder or Internal Intruder. The unauthorized users who enter the system and make changes to the system and access the resource in the network without

authorization, is an external intruder. The intruder in the network without user accounts trying to attack the system is an internal
intruder. Intrusion detection systems are classified into two types Misuse detection and Anomaly detection. Intrusion detection with known patterns is called misuse detection. Identifying the abnormalities from the normal network behaviors is called anomaly detection. Hybrid detection systems combine both the misuse and anomaly detection systems. The network traffic and individual packets for mischievous traffic is tested by a network based IDS. An intrusion detection system is a device or software application that monitors network and/or system
activities for malicious activities or policy violations and produces reports.

While, anomaly detection develops models of normalnetwork behaviors, and new intrusions are detected by evaluating significant deviations from the normal behavior. KDD99Cup [3] is widely used as training and testing datasets for the evaluation of IDSs. Data mining generally refers to the process of extracting useful rules from large amount of data. The recent rapid development in data mining contributes to developing wide variety of algorithms suitable for network intrusion detection problems. Intrusion detection can be thought of as a classification problem: where each pattern classified as normal or a particular kind of intrusion.

2. INTRUSION DETECTION OVERVIEW

The below sections give a short overview of networking attacks and classifications
.

2.1 Networking Attacks

This section is an overview of the four major categories of networking attacks. Every attack on a network can comfortably be placed into one of these groupings [5].

1)Denial of Service (DoS): A DoS attack is a type of attack in which the hacker makes a computing or memory resources too busy or too full to serve legitimate networking requests and hence denying users access to a machine e.g. apache, smurf, neptune, ping of death, back, mail bomb, UDP storm etc. are all DoS attacks.
2) Remote to User Attacks (R2L): A remote to user attack is an attack in which a user sends packets to a machine over the internet, which he/she does not have access to in order to expose the machines vulnerabilities and exploit privileges which a local user would have on the computer e.g. x lock, guest, xnsnoop, phf, sendmail dictionary etc.
3) User to Root Attacks (U2R): These attacks areexploitations in which the hacker starts off on the system with a normal user account and attempts to abuse vulnerabilities in the system in order to gain super user privileges e.g. perl, xterm.
4) Probing: Probing is an attack in which the hacker scans a machine or a networking device in order to determine weaknesses or vulnerabilities that may later be exploited so as to compromise the system. This technique is commonly used in data mining e.g. saint, port sweep, mscan, nmap etc.

2.2 Classification of Intrusion Detection

Intrusions Detection can be classified into two main categories. They are as follow:
1) Host Based Intrusion Detection: HIDSs evaluate in formation found on a single or multiple host systems, including contents of operating systems, system and application files.

2)Network Based Intrusion Detection: NIDSs evaluate in formation captured from network communications, analyzing the stream of packets which travel across the network. As host-based systems rely heavily on audit trails, they become limited by these audit trails, which are not provided by the manufacturers who design the intrusion detection system itself. As a result, theses trails may not necessarily support the needs of the intrusion detection system. Network-based intrusion detection systems offer a different approach. These systems collect information
from the network itself, rather than from each separate host. They operate essentially based on a wiretapping concept; information is collected from the network traffic stream, as data travels on the network segment. The intrusion detection system checks for attacks or irregular behavior by inspecting the contents and header information of all the packets moving across the network [6]. 3.

GNP-BASEDFUZZYCLASS ASSOCIATION RULE MINING

A class-association rule mining algorithm based on GNP has been proposed [7]. GNP and its class association rule mining are briefly explained as follows.

3.1 Framework of Genetic Network Programming

GNP is one of the evolutionary optimization techniques, which uses directed graph structures instead of strings and trees. The phenotype and genotype expressions of GNP are shown in Figure 1. GNP is composed of three types of nodes: start node, judgment node, and processing node. Judgment nodes, J1 , J2 ,…, Jm (m is the total number of judgment functions), serve as decision functions that return judgment results so as to determine the next node. Processing nodes, P1, P2. . . , Pn (n is the total

number of processing functions), serve as action/processing
functions. The practical roles of these nodes are predefined and stored in the function library by
supervisors. Once GNP is booted up, the execution starts from the start node, then the next node to be executed is determined according to the connection between nodes and a judgment result of the current activated node. Figure 1 also describes the gene of a node in a GNP individual. NTi represents the node type such as 0 for start node, 1 for judgement node and 2 for processing node. ID i serves as an identification number of a judgement or processing node, for example, NTi=1 and IDi=2 represents node function J2. Ci1, Ci2…., Cij denote the node numbers connected from node i. The total number of nodes in an individual remains the same
during every generation [1]. **Diagram**

Three kinds of genetic operators, i.e., selection, mutation, and crossover, are implemented in GNP.
1) Selection: Individuals are selected according to their fitness.
2) Crossover: Two new offspring are generated from two parents by exchanging the genetic information. The selected nodes and their connections are swapped each other by crossover rate Pc.
3) Mutation: One new individual is generated from one original individual by the following operations. Each node branch is selected with the probability Pm1 and reconnected to another node. Each node function is selected with the probability Pm2 and changed to another one.

3.2 GNP-Based Class-Association Rule

A judgment node in GNP has a role in checking an attribute value in a tuple [6]. Candidate class-association rules are represented by the connection of judgement nodes. An example of the representation is shown in Figure 2.**diagram**

Processing node P1 serves as the beginning of class-association rules. A1=1, A 2=1, and A3=1 denote the judgment functions. If a tuple satisfies the condition of the judgment function, Yes-side branch is selected and the condition of the next judgment function is examined in order to find longer rules. No-side is connected to processing node P2 to start examining other rules.
Therefore, the branch from the judgment node representsthe antecedent part of class-association rules, while the fixed consequent part can be predefined. are examined by the node transition in Figure 2.
$(A1=1) \Rightarrow (C=1)$
$(A1=1) \wedge (A2=1) \Rightarrow (C=1)$
$(A1=1) \wedge (A2=1) \wedge (A3=1) \Rightarrow (C=1)$
$(A1=1) \Rightarrow (C=0)$
$(A1=1) \wedge (A2=1)) \Rightarrow (C=0)$
$(A1=1) \wedge (A2=1)) \wedge (A3=1) \Rightarrow (C=0)$
The procedure of examining tuples is as follows. The first tuple in the database is read and the node transition starts from processing node P1. Then, if Yes-side branch is selected, the current node is transferred to the next judgment node. If No-side branch is selected, the current node is transferred to processing node P2 to find other rules. The same procedure is repeated until the node transition started from the last processing node Pn is finished. After examining the first tuple in the database, the second tuple is read and the node transition starts from processing node P1 again. Finally, all the tuples are examined by repeating the above node transitions. Note
that the number of judgment functions (J1, J2,…) equals the number of attributes (A1, A2,…) in the database.

3.3 Sub attributes Utilization

Network connection data have their own characteristics, such as discrete and continuous attributes, and these attribute values are important information that cannot be lost. We introduce a sub attribute-utilization mechanism concerning binary, symbolic and continuous attributes to keep the completeness of data information. Binary attributes are divided into two sub attributes corresponding to judgment functions. For example, binary attribute A1 (=land) was divided into A_11 (representing land=1) and A_12 (representing land=0). The symbolic attribute was divided into several sub attributes, while the continuous attribute was also divided into three sub attributes concerning the values represented by linguistic terms (low, middle, and high) of fuzzy membership functions predefined for each continuous attribute. Figure 3 shows a division example of the three attributes.**diagram**

In the conventional GNP-based class-association rule mining, only discrete attributes with value 1 are considered. In the proposed method, all the values such as 0 and 1 for binary attributes and text values for symbolic attributes are considered.

3.4 Rule Extraction by GNP with Fuzzy Membership Functions

GNP examines the attributes of tuples at judgment nodes and calculates the measurements of association rules at processing nodes [7]. Judgment nodes judge the values of the assigned sub attributes, e.g., Land=1, Protocol=tcp, etc. The GNP-based fuzzy class-association rule mining with sub attribute utilization successfully combines discrete and

continuous values in a single rule. An example of the node transition in the proposed method is shown in Figure 4. P1 is a processing node that serves as a starting point of class association rules and connects to a judgment node. The Yes-side of the judgment node is connected to another judgment node, while the No-side is connected to the next processing node. Judgment nodes shown here have the functions that examine the sub attributes including both discrete and continuous attributes. In Figure 4, judgment node J1 examines the value of thebinary sub attribute land=1, J2 examines the value of the symbol sub attribute protocol=tcp, and J3 examines the fuzzy membership value of the continuous sub attribute count=Low. In the case of binary and discrete attributes (J1 and J2), GNP selects Yes-side branch and goes to the next judgment node if "land=1 is Yes" or "count=Low is Yes," otherwise, the current node is transferred to processing node P2 to start examining other rules. In the case of continuous attribute (J3), after calculating the fuzzy membership value of the sub attribute, the value is regarded as a probability of selecting Yes-side branch. When No-side branch is selected, the current node is transferred to processing node P2. The total number of tuples moving to Yes-side at each judgment node is memorized in the processing node from which rule extraction starts. In Fig. 4, N is the number of total tuples
in the database, and a, b, and c are the number of tuples moving to Yes-side at each judgment node. In an application of misuse detection, the training database contains both normal connections and several kinds of intrusion connections. Thus, GNP examines all the tuples of the connections in the database and counts the numbers a, b, c, a(1), b(1), c(1), a(2), b(2), and c(2), where a, b, and c are the numbers of tuples moving to Yes-side at the judgment nodes, a(1), b(1), and c(1) are those with class C=1 (normal) and a(2), b(2), and c(2) are those with class
C =2 (intrusion).

Table 1
Result of Crisp Data Mining with K=0.5 Intrusion Detection

From the above experiment, it is able to create a rule thatcould successfully classify all 773 sample network connections. Along with this, it also classifies 181 normal connections and 13 as network connection attacks among 194 normal connections. For the same intrusion detection
connections 579 our Intrusion Detection System(IDS) classifies 15 as normal connection and 564 as intrusion connection. Figure 6 shows different parameter analysis for sample data.

5. CONCLUSION

The paper represents an efficient Intrusion-Detection model based on Fuzzy Class-Association rule mining using Genetic Network Programming from KDD99CUP data set. Discrete and continuous attributes are consistently used to extract many good rules for
classification. In future Deterministic Finite State Automata (DFA) can be used on binary attributes to detect intrusion of network connections.

References

[1] Shingo Mabu, Ci Chen, Nannan Lu, Kaoru Shimada and Kotaro Hirasawa, "An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming" IEEE Transactions On Systems, Man, And Cybernetics-Part C: Applications And Reviews, VOL. 41, NO. 1, January 2011

[2] B. Uppalaiah, K. Anand, B. Narsimha, S. Swaraj, T. Bharat, "Genetic Algorithm Approach to Intrusion Detection System", IJCST Vol. 3, Issue 1, Jan.-March 2012

[3] Kddcup1999data[Online].Available:kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[4] M. Crosbie and G. Spafford, "Applying genetic programming to intrusion detection", presented a the AAAI Fall Symp. Series, AAAI Press, Menlo Park, CA, Tech. Rep. FS-95-01, 1995.

[5] Mohammad Sazzadul Hoque1, Md. Abdul Mukit and Md. Abu Naser Bikas, "A Implementation of Intrusion Detection System Using Genetic Algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[6] Bace, Rebecca Gurley: Intrusion Detection. Copyright 2000 by Macmillan Technical Publishing, ISBN 1-57870-185-6.

[7] K. Shimada, K. Hirasawa, and J. Hu, "Genetic network programming with acquisition mechanism of association rules", J. Adv. Comput. Intell. Intell. Inf., vol. 10, no. 1, pp. 102–111, 2006.

[8] J. G.-P. A. El Semaray, J. Edmonds, and M. Papa, "Applying data mining of fuzzy association rules to network intrusion detection," presented at the IEEE Workshop Inf., United States Military Academy, West Point, NY, 2006.

[9] Mr. Bahubali Akiwate received a Bachelor of Engineering degree in Computer Science and
Engineering from Bahubali College of Engineering, Shravanabelagola, affiliated to VTU, Belgaum, during the year 2009. He completed M.Tech Degree in Digital communication and
Networking from Gogte Institute of Technology,

Belgaum, from the same University, during the year 2011. He is working as an assistant professor in Computer Science and Engineering Department of K. L.\ E. College of Engineering and Technology, Chikodi since from September-2011.

[10] Mr. Mallappa Gurav received the Bachelor of Engineering degree in Computer Science and Engineering from Basaveshwar Engineering College, Bagalkot, affiliated to VTU, Belgaum, during 2010. He is persuing M.Tech at Gogte Institute of Technology, Belgaum, under Visvesvaraya Technological University, Belgaum. Currently he is working as an assistant professor in Computer Science and Engineering Department of K. L. E. College of Engineering and Technology, Chikodi since from 2010.

AN IMPROVING TECHNIQUE OF LOCATION IDENTIFICATION USING LATITUDE AND LONGITUDE-VERIFICATION

T.Amala christina
PG Scholar
Infant Jesus College of Engineering
Thoothukudi.
Email:amalachristina@gmail.com
.

M.Nagalingarajan,ME.,
Assistant Professsor,
Infant jesus college of Engineering
Thoothukudi

ABSTRACT- A Privacy-Preserving Location proof Updating System (APPLAUS) in which colocated Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server. Periodically changed pseudonyms are used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server. We also develop user-centric location privacy model in which individual users evaluate their location privacy levels and decide whether and when to accept the location proof requests. In order to defend against colluding attacks, we also present betweenness ranking-based and correlation clustering-based approaches for outlier detection. APPLAUS can be implemented with existing network infrastructure, and can be easily deployed in Bluetooth enabled mobile devices with little computation or power cost. Extensive experimental results show that APPLAUS can effectively provide location proofs, significantly preserve the source location privacy, and effectively detect colluding attacks.

Index Terms—Location-based service, location proof server location privacy, pseudonym, colluding attacks

I. INTRODUCTION

Location-based services take advantage of user location information and provide mobile users with various resources and services. Nowadays, more and more location-based applications and services require users to provide location proofs at a particular time. For example, "Google Latitude" and "Loopt" are two services that enable users to track their friends' locations in real time. These applications are location-sensitive since location proof plays a critical role in enabling these applications.

There are many kinds of location-sensitive applications. One category is location-based access control. For example, a hospital may allow patient information access only when doctors or nurses can prove that they are in a particular room of the hospital [2].

Another class of location-sensitive applications require users to provide past location proofs [6], such as auto insurance in which auto insurance companies offer discounts to drivers who can prove that they take safe routes during their daily commutes, police investigations in which detectives are interested in finding out if a person was at a murder scene at some time, and location-based social networking in which a user can ask for a location proof from the service requester and accepts the request only if the sender is able to present a valid location proof. The common theme across these location sensitive applications is that they offer a reward or benefit to users located in a certain geographical location at a certain time. Thus, users have the incentive to cheat on their locations.

PRELIMINARIES

In this paper focus on mobile networks where mobile devices such as cellular phones communicate with each other through Bluetooth. In our implementation, mobile devices periodically initiate location proof requests to all neighboring devices through Bluetooth. After receiving a request, a mobile node decides whether to exchange location proof, based on its own location proof updating requirement and its own privacy consideration.

Pseudonym

As commonly used in many networks, we consider an online Certification Authority (CA) run by independent trusted third party which can preestablish credentials for the mobile devices. Similar to many pseudonym approaches, to protect location privacy, every mobile node i registers with the CA by preloading a set of M public/private key pairs.

Threat Model

We assume that an adversary aims to track the location of a mobile node. An adversary can have the same credential as a mobile node and is equipped to eavesdrop communications. We assume that the adversary is internal, passive, and global. By internal, we mean that the adversary is able to compromise or control individual mobile device and then communicate with others to explore private information, or individual devices may collude with each other to generate false proofs.

Location Privacy Level

In this paper, we use multiple pseudonyms to preserve location privacy; i.e., mobile nodes periodically

change the pseudonym used to sign messages, thus reducing their long term linkability. To avoid spatial correlation of their location, mobile nodes in proximity coordinate pseudonym changes by using silent mix zones [7], [8], or regions where the adversary has no coverage [4]. Without loss of generality, we assume each node changes its pseudonyms from time to time according to its privacy requirement. If this node changes its pseudonym at least once during a time period (mix zone), a mix of its identity and location occurs, and the mix zone becomes a confusion point for the adversary.

II. RELATED WORK

Recently, several systems have been proposed to provide end users the ability to prove that they were in a particular place at a particular time. . The solution in relies on the fact that nothing is faster than the speed of light in order to compute an upper bound of a user's distance. Capkun and Hubax [5] propose challenge-response schemes, which use multiple receivers to accurately estimate a wireless node location using RF propagation characteristics. In [3], the authors describe a secure localization service that can be used to generate unforgeable geotags for mobile content such as photos and video. However dedicated measuring hardware or high-cost trusted computing module are required. Saroiu and Wolman [6] propose a solution suitable for third-party attestation, but it relies on a PKI and the wide deployment of WiFi infrastructure. Different from these solutions, APPLAUS uses a peer-to-peer approach and does not require any change to the existing infra-structure. . However, this service does not reveal the actual location information to the service provider thus can only provide location proofs between two users who have actually encountered. APPLAUS can provide location proofs to third-party by uploading real encounter location to the untrusted server while maintaining location privacy. All the above techniques cloak a node's locations with its current neighbors by trusted central servers which is vulnerable to DoS attacks or to be compromised. Different from them, our approach does not require the location proof server to be trustworthy. There are lots of existing works on location privacy in wireless networks. In [11], the authors propose to reduce the accuracy of location information along spatial and/or temporal dimensions. This basic concept has been improved by a series of works [10], [12]. All the above techniques cloak a node's locations with its current neighbors by trusted central servers which is vulnerable to DoS attacks or to be compromised. Different from them, our approach does not require the location proof server to be trustworthy. Xu and Cai [30] propose a feeling-based model which allows a user to express his privacy requirement. One important concern here is that the spatial and temporal correlation between successive locations of mobile nodes must be carefully eliminated to prevent external parties from compromising their location privacy. The techniques in [1], [9] achieve location privacy by changing pseudonyms in regions called mix zones.

III. MODELING AND ALGORITHM

THE LOCATION PROOF UPDATING SYSTEM

In this section, we introduce the location proof updating architecture, the protocol, and how mobile nodes schedule their location proof updating to achieve location privacy in APPLAUS.

Architecture

In APPLAUS, mobile nodes communicate with neighboring nodes through Bluetooth, and communicate with the untrusted server through the cellular network interface. Based on different roles they play in the process of location proof updating, they are categorized as Prover, Witness, Location Proof Server, Certificate Authority or Verifier. The architecture and message flow of APPLAUS is shown in Fig. 1.

- **Prover:** the node who needs to collect location proofs from its neighboring nodes. When a location proof is needed at time t, the prover will broadcast a location proof request to its neighboring nodes through Bluetooth. If no positive response is received, the prover will generate a dummy location proof and submit it to the location proof server.

- **Witness:** Once a neighboring node agrees to provide location proof for the prover, this node becomes a witness of the prover. The witness node will generate a location proof and send it back to the prover.

- **Location proof server:** As our goal is not only to monitor real-time locations, but also to retrieve history location proof information when needed, a location proof server is necessary for storing the history location proofs.

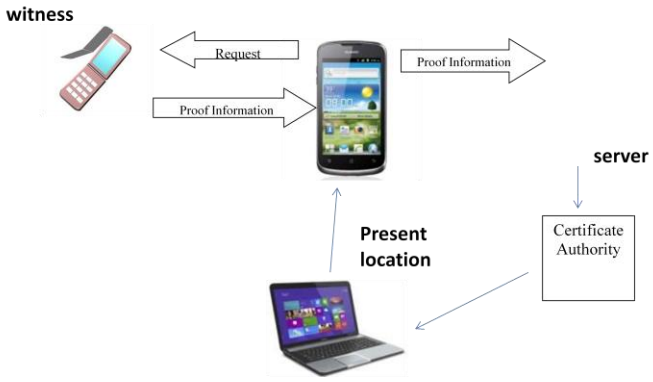


Fig 1: Location proof updating architecture and message flow.

- Every mobile having Bluetooth system it's to send request to the arounding Bluetooth devices give latitude in present location.
- After receiving latitude of Bluetooth system it will send the latitude and longitude value to the server.
- Server not only monitor real time location and Also retrieve history location proof information.
- In this data loading into the server and is transfer to certificate verified location.
- Every mobile node registers with the CA and pre-loads a set of public and private key pairs before entering the network.
- Verifier to verify the latitude and longitude value and produced witness of the user location.
- This system effectively find the colluding attacks.

Protocol

When a prover needs to collect location proofs at time t, it executes the protocol to obtain location proofs from the neighboring nodes within its Bluetooth communication range. Each node uses its M pseudonyms $P_i^{M}{}_{¼1}$ as its identity throughout the communication. The prover broadcasts a location proof request to its neighboring nodes through Bluetooth according to its update scheduling. The request should contain the prover's current pseudonym P_{prov}, and a random number R_{prov}.

The witness decides whether to accept the location proof request according to its witness scheduling. Once agreed, it will generate a location proof for both prover and itself and send the proof back to the prover. This location proof includes the prover's pseudonym P_{prov}, prover's random number R_{prov}, witness's current time stamp T_{witt}, witness's pseu-donym P_{witt}, and their shared location L. This proof is signed and hashed by the witness to make sure that no attacker or prover can modify the location proof and the witness cannot deny this proof. It is also encrypted by the server's public key to prevent from traffic monitoring or eavesdropping.

After receiving the location proof, the prover is responsible for submitting this proof to the location proof server. The message also includes prover's pseudonym P_{prov} and random number R_{prov}, or its own location for verification purpose. An authorized verifier can query the CA for location proofs of a specific prover. This query contains a real identity and a time interval. The CA first authenticates the verifier, and then converts the real identity to its corresponding pseudonyms during that time period and retrieves their location proofs from the server. In order not to expose correlation between pseudonyms to the location server, CA will always collect enough queries from k different nodes before a set of queries are sent out.

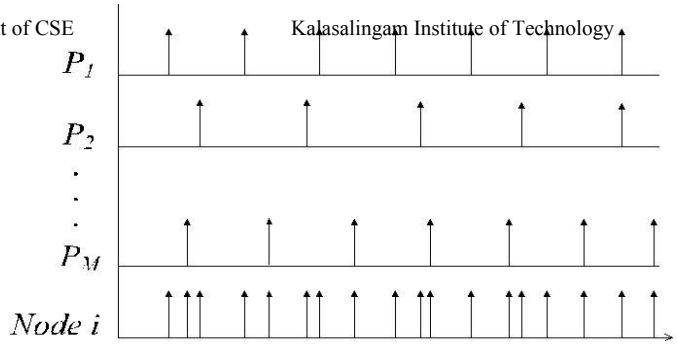


Fig. 2. Example of individual pseudonym update versus entire node update.

Definition 1 (Separation of privacy knowledge). The knowledge of the privacy information is separately distributed to the location proof server, the CA, and the verifier. Thus, each party only has partial knowledge.

The privacy property of our protocol is ensured by the separation of privacy knowledge: the location proof server only knows pseudonyms and locations, the CA only knows the mapping between the real identity and its pseudonyms, while the verifier only knows the real identity and its authorized locations. Attackers are unable to learn a user's location information without integrating all the knowledge. Therefore, compromising either party of the system does not reveal privacy information.

Scheduling Location Proof Updates

As discussed before, the adversary may obtain complete coverage and track nodes throughout the entire network, by compromising the location proof server and obtain all history location proofs. Therefore, we need to appropriately design and arrange the location proof updating schedules for both prover and witness so that no source location information related to individual user is revealed even if the server is compromised.

Algorithm 1. Location Proof Update Scheduling for the prover

```
Input: updating parameter _;
    generate M distinct parameter _1; _2; _ _ _ ; _M such
    that _1 þ _2 þ _ _ _ þ _M ¼ _
    for each pseudonym i do
        while current timestamp t follows Poisson
        distribution with _i do
          send location proof request
          if request is accepted then
              submit location proof
          else
              generate and submit dummy proof
          end if
    end while
end for
```

$$SINR_{ij} = \frac{P_i \cdot g_{ij}}{\sum_{k \neq i} P_k \cdot g_{kj} + N}$$

The difference between them indicates the privacy loss if this location proof request is accepted. The location proof request is only accepted when the privacy loss is less than a predefined threshold. The drawback of the user-centric model is that nodes may have misaligned incentives (i.e., different privacy requirement), which can lead to failed attempts to obtain enough location proofs. We use dummy proofs in Algorithm 1 to deal with failed attempts. The detailed scheduling protocol for witness is presented in Algorithm 2.

Algorithm 2. Scheduling Location Proof Updates at Witnesses

Input: time t of incoming location proof request;

1: calculate location privacy loss _ assuming the incoming request is accepted
2: if _ > _, _ is pre-defined location privacy loss threshold then
3: deny location proof request
4: else
5: accept location proof request
6: end if

IV. PERFORMANCE EVALUATION

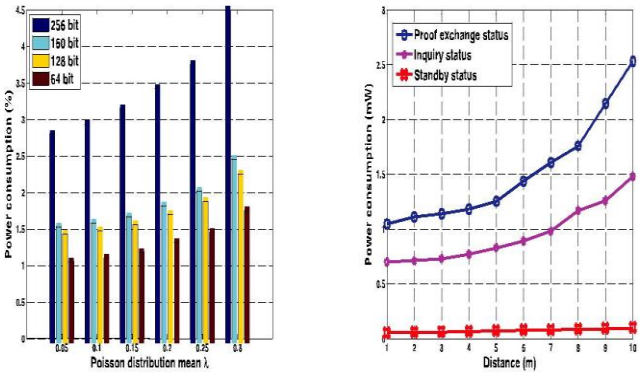


Fig 3:Power consumption for different Bluetooth status

It measure the CPU utilization of our client code using a monitoring application, which allows one to monitor the CPU usage of all the processes running on the phone. When the application is in standby, the CPU utilization is about 0.5 percent, indicating that listening to incoming Bluetooth inquiries requires very low computa-tion. The CPU utilization goes to 3 and 5 percent, respectively, when communicating with another device and with the server, due to using different communication interfaces. We observe that the CPU utilization reaches the highest level of 10 percent when a location proof packet is generated, in which heavy computations such as authenti-cation and encryption/decryption are involved.

CONCLUSIONS

In this paper, we proposed a privacy-preserving location proof updating system called APPLAUS, where colocated Bluetooth enabled mobile devices mutually generate loca-tion proofs and upload to the location proof server. We use statistically changed pseudonyms for each device to protect source location privacy from each other, and from the untrusted location proof server. We also develop a user-centric location privacy model in which individual users evaluate their location privacy levels in real time and decide whether and when to accept a location proof exchange request based on their location privacy levels. To the best of our knowledge, this is the first work to address the joint problem of location proof and location privacy. To deal with colluding attacks, we proposed betweenness ranking based and correlation clustering-based approaches for outlier detection. Extensive experimental and simulation results show that APPLAUS can provide real-time location proofs effectively. Moreover, it preserves source location privacy and it is collusion resistant.

REFERENCES

[1] A.R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," IEEE Security and Privacy, 2003.
[2] W. Luo and U. Hengartner, "Proving Your Location Without Giving Up Your Privacy," Proc. ACM 11th Workshop Mobile Computing Systems and Applications (HotMobile '10), 2010.
[3] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-Based Trust for Mobile User-Generated Content: Applications Challenges and Implementations," Proc. Ninth Work-shop Mobile Computing Systems and Applications, 2008.
[4] L.P. Cox, A. Dalton, and V. Marupadi, "SmokeScreen: Flexible Privacy Controls for Presence-Sharing," Proc. ACM MobiSys, 2007.
[5] S. Capkun and J.-P. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," Proc. IEEE INFOCOM, 2005.
[6] S. Saroiu and A. Wolman, "Enabling New Mobile Applications with Location Proofs," Proc. ACM 10th Workshop Mobile Computing Systems and Applications (HotMobile '09), 2009.
[7] M. Li, R. Poovendran, K. Sampigethaya, and L. Huang, "Caravan: Providing Location Privacy for VANET," Proc. Embedded Security in Cars (ESCAR) Workshop, 2005.
[8] U. Brandes, "A Faster Algorithm for Betweenness Centrality," J. Math. Sociology, vol. 25, no. 2, pp. 163-177, 2001.
[9] M. Gruteser and D. Grunwald, "Anonymous Usage of

Location-Based Services through Spatial and Temporal Cloaking," Proc. ACM MobiSys, 2003.

[10] B. Gedik and L. Liu, "A Customizable K-Anonymity Model for Protecting Location Privacy," Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS), 2005.

[11] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking," Proc. ACM MobiSys, 2003.

[12] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.C. Herrera, A.M. Bayen, M. Annavaram, and Q. Jacobson, "Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring," Proc. ACM MobiSys, 2008.

Real Time Event Detection and Earthquake Reporting in Social Network

T.Sibiya Angeline,
Department of CSE,
SCAD Engineering College, Cheranmahadevi.

Abstract—The enormous amount of information stored in unstructured texts cannot simply be used for further processing by computers, which typically handle text simple sequences of character strings. Therefore, specific (pre-) processing methods and algorithms are required in order to extract useful patterns. Text mining refers generally to the process of extracting interesting information and knowledge from unstructured text. In this article, we discuss text mining as a young and interdisciplinary field in the intersection of the related areas information retrieval, machine learning, microblogging, particle filtering, and especially data mining. This paper reports the comparison and summary of various researches in a Social Network.

Keywords: Text Mining, Machine Learning, Microblogging, Data Mining, Social Network.

I. INTRODUCTION

The amount of data kept in computer files and data bases is growing at a phenomenal rate. At the same time users of these data are expecting more sophisticated information from them. A marketing manager is no longer satisfied with the simple listing of marketing contacts but wants detailed information about customers' past purchases as well as prediction of future purchases. Simple structured / query language queries are not adequate to support increased demands for information. Data mining steps is to solve these needs. Data mining is defined as finding hidden information in a database alternatively it has been called exploratory data analysis, data driven discovery, and deductive learning .In the data mining communities, there are three types of mining: data mining, web mining, and text mining. The mining data may vary from structured to unstructured. Data mining mainly deals with structured data organized in a database while text mining mainly handles unstructured data/text. Web mining lies in between and copes with semi structured data and/or unstructured data. The definition of Text Data can be simple: It is equivalent to text analytics, refers to the process of deriving high-quality information from text. In this paper we describe text mining as a truly interdisciplinary method drawing on information retrieval, machine learning, and especially data mining..

[1]http://www.techcrunch.com/2009/08/03/twitter-reaches-44.5-million-people-worldwide-in-june-comscore/
[2]According to a report from Nielsen.com.

We are focusing on reporting systems of an earthquake in a real time nature in a social network called twitter. Target event is detected and classified by using keywords in tweets that we are going to use.

II. TEXT MINING

Text mining (TM) seeks to extract useful information from a collection of documents. The tasks of text mining includes,

Information Retrieval: Retrieval of documents in response to a "query document"(as a special case, the query document can consist of a few keywords)

Document Classification: It defines Classification of documents into predefined categories (classes).

Organizing documents: Unsupervised process through which documents are classified into groups called clusters.

Information Extraction: Information Extraction involves identification of certain entities in the text, their extraction and representation in a pre-specified format.

III. TWITTER

Twitter, a popular micro-blogging service, has received much attention recently. It is an online social network used by millions of people around the world to stay connected to their friends, family members and co-workers through their computers and mobile phones. Twitter asks one question, "What are you doing?" Answers must be fewer than140 characters. A status update message, called a *tweet*, is often used as a message to friends and colleagues. A user can follow other users; and her followers can read her tweets.
which renders the links of the network as directed. Twitter users have increased rapidly. They are currently estimated as 44.5 million worldwide[1]. Monthly growth of users has been 1382% year-on-year, which makes Twitter one of the fastest-growing sites in the world[2]. Twitter is categorized as a micro-blogging service. Micro-blogging [1] is a form of blogging that allows users to send brief text updates or micro-media such as photographs or audio clips. It analyze the network structure of the twitter. By mapping each user's latitude and longitude to a continent location we can extract the origin and destination location for every edge.

An important common characteristic among micro-blogging services is its real-time nature. We detect such event occurrence in real-time by monitoring tweets?" [7]. It proposes an event notification system that monitors tweets and delivers notification promptly.

A. Application of Twitter

"Why Twitter?" is definitely the most popular follow-up question. There are many great uses for Twitter, but even once you understand that Twitter has grown beyond a micro-blogging service to become a social messaging platform, it can still leave you wondering why you might want to use it.

Several of the benefits of Twitter and why they can help your businesses succeed.

- Personal
- Market Research
- Free Press Release
- Customer Satisfaction

Developing Your Business on Twitter

IV. LITERATURE SURVEY

To detect a target event from Twitter, we search from Twitter and find useful tweets. Some tweets are not truly descriptions of the target event, but they are not real-time reports of the events. Therefore, it is necessary to clarify that a tweet is truly referring to an actual contemporaneous earthquake occurrence, which is denoted as a positive class.

A. Event detection by Semantic Analysis

It is analyzed[8] that particular properties of learning with text data and identifies why SVM's are useful for this tasks. They are fully automatic, eliminating the need for manual automatic tuning. The first step is to transform the documents which typically of strings of characters into a representation suitable for learning algorithm and the classification task.Information retrieval research suggests that the word stem works very well..

SVM works well for text categorization because of High dimensional input space, few irrelevant features, Document vectors are sparse, Most text categorization problems are linearly separable. Location estimation[22] is important in ubiquitous computing because location is an important part of a user's context.

It is generally understood as the task of identifying mentions of rigid designators[9] from text belonging to named-entity types such as persons, organizations and locations Proposed solutions to NER fall into three categories: 1) The rule-based 2) the machine learning and 3) hybrid methods. NER task can be naturally divided into two subtasks, i.e., boundary detection and type classification. Related work can be roughly divided into three categories: NER on tweets, NER on non-tweets

Given a tweet as input, our task is to identify both the boundary and the class of each mention of entities of predefined types**.** Named entity classification was identified as a particularly challenging [10] task on Twitter. Due to their terse nature, tweets often lack enough contexts to identify the types of the entities they contain. most words found in tweets are not part of an entity, we need a larger annotated dataset to effectively learn a model of named entities.

B. Particle filtering by Bayesian tracking

A more advanced algorithm with re-sampling difference equations are used to model the evolution of the system with time, and measurements are assumed to be available at discrete times. For dynamic state estimation [11], the discrete-time approach is widespread and convenient. The state-space approach to time-series modeling focuses attention on the state vector of a system. The state vector contains all relevant information required to describe the system under investigation. For example, in tracking problems, this information could be related to the kinematic characteristics of the target.

The sequential importance sampling (SIS) algorithm is a Monte Carlo (MC) method that forms the basis for most sequential MC filters developed over the past decades. The key idea is to represent the required posterior density function by a set of random samples with associated weights and to compute estimates based on these samples and weights.

C. Information Diffusion

People share their experiences and opinions about products and services in their blogs and knowledge-sharing sites**.** The regarding knowledge-sharing sites, relations among customers are analyzed in various ways. Information about customer experiences flows through social relations [12]. Users share their experiences with their friends and colleagues. They might exchange that information with their friends online. We must describe the evolution model of trust and rating.

Researchers, identified influentials on Twitter, we have ranked users by the number of followers and by PageRank [3] and found two rankings to be similar. If we rank by the number of retweets, then the ranking differs from the previous two rankings, indicating a gap in influence inferred from the number of followers and that from the popularity of one's tweets. Ranking by retweets exposes the influence of other media in a novel perspective. We have trending topics and reported on the temporal behavior of trending topics and user participation. We then classify the trending topics based on the active period and the tweets and show that the majority (over 85%) of topics are headline or persistent news in nature

Strong earthquakes are often preceded by a period of accelerating seismic activity expressed by intermediate magnitude earthquakes [13], namely 'preshocks'. It has been shown that a proper measure of the process, described, is the Benioff strain. It represents a reliable measure of the preshock seismicity at time t. The main purpose of the present paper is to identify elliptical critical regions

associated with strong (M>6.0) earthquakes in particular and surrounding area.

D. Relation between each other in social networks

The linked structures of social networks do not reveal actual interactions among people. Scarcity of attention and the daily rhythms of life and work makes people default to interacting with those few that matter and that reciprocate their attention. The study of social interactions [2] within Twitter reveals that the driver of usage is a sparse and hidden network of connections underlying the declared" set of friends and followers. In order to find out how relevant a list of \friends" is to members of the network; we collected and analyzed a large data set from the Twitter social network.

The Microblogging covers either general suggestions on how to use Twitter [6] in the classroom or analyses properties of the network and conversations without a focus on learning.

E. Emerging topics on twitter

We recognize the primary role of Twitter and a novel topic detection technique was proposed that permits to retrieve in real-time the most emergent topics expressed by the community [14]. First, we extract the contents (set of terms) of the tweets and model the term life cycle according to a novel aging theory intended to mine the emerging ones. A term can be defined as emerging if it frequently occurs in the specified time interval and it was relatively rare in the past. In this system, as information producers, people post tweets for a variety of purposes, including daily chatter, conversations, sharing information/URLs and reporting news, defining a continuous real-time status stream about every argument. we recognize this primary information role of Twitter and provide a new method to extract the emerging topics by analyzing in real-time the emerging terms expressed by the community. The real-time social content can also be seen as a sensor that captures what is happening in the world

The Retweeting [4] has become a convention inside Twitter, participants retweet using different styles and for diverse reasons. retweeting, has yet to be analyzed. Structurally, retweeting is the Twitter-equivalent of email forwarding where users post messages originally posted by others. This convention has no uniform grammar. Retweeting is also an important practice to analyze because of the larger issues it raises concerning authorship, attribution, and communicative fidelity.

The Twitter is indeed used extensively for political deliberation [5].We find that the mere number of messages mentioning a party reflects the election result. Moreover, joint mentions of two parties are in line with real world political ties and coalitions. An analysis of the tweets' political sentiment demonstrates close correspondence to the parties' and politicians' political positions indicating that the content of Twitter messages plausibly reflects the offline political landscape. First, we examine whether Twitter is a vehicle for online political deliberation by looking at how people use microblogging to exchange information about political issues. Second, we evaluate whether Twitter messages reflect the current offline political sentiment in a meaningful way. Third, we analyze whether the activity on Twitter can be used to predict the popularity of parties or coalitions in the real world.

A connect measures of public opinion measured from polls with sentiment measured from text [15]. We analyze several surveys on consumer confidence and political opinion over the 2008 to 2009 period, and find they correlate to sentiment word frequencies in contemporaneous Twitter messages. We find that a relatively simple sentiment detector based on Twitter data replicates consumer confidence and presidential job approval polls.

A semantic and distributed approach of micro-blogging [17] describes the features, methods and architecture of a distributed Semantic Web microblogging system, as well as the implementation of an initial prototype of this concept that provides ways to leverage microblogging with the Linked Data Web guidelines.

F. e-Learning

The reason which was furthermore mentioned are fast and easy community building in e-learning. The world will turn more and more mobile. Knowledge workers will act in a global world without static borders. They interact more and more in virtual teams [16], distributed all over the world. Mobile learning can also be defined as learning with books because they are mobile too, but today mobile learning often means learning with digital mobile devices like PDAs or cell phones.

G. Search Engine Queries

The measure of spatial dispersion, indicating whether it has highly local interest or broader regional or national appeal. interest in a topic can be tight diffusely over a broader region [18]; it can have one geographic "center" or several; it can move over time. To characterize queries according to this continuum of possible geographic traits, we need a model and a source of data rich enough to be able to discover subtle distinctions in 'spatial properties' concentrated at a particular location or spread. This `model` is probabilistic.

More research work is conducted on weblogs, which considers blogs not only as a new information source, but also as an appropriate tested for many novel research problems and algorithms. Weblogs were considered as online diaries published and maintained [19] by individual users, ordered chronologically with time stamps, and usually associated with a profile of their authors. Compared with traditional media such as online news sources (e.g., CNN online) and public websites maintained by companies or organizations (e.g., Yahoo!), weblogs have several unique characteristics: 1) the content of weblogs is highly personal and rapidly evolving. 2) Weblogs are usually associated with

the personal information of their authors, such as age, geographic location.

H. Flickrs

Methods were investigated for placing photos uploaded to Flickr on the World map [20]. Due to the massive production of affordable GPS-enabled.

Cameras and mobile phones, location metadata such as latitude and longitude are automatically associated with the content generated by users. Users have the opportunity to spatially organize and browse their personal media, and photo sharing services are leading the growing enthusiasm for personal location-awareness

Semantics of tags was extracted and, unstructured text-labels assigned to resources on the Web, based on each tag's usage patterns [21]. Tags usually manifest in the form of a freely-chosen, short list of keyword associated by a user with a resource such as a photo, web page, or blog entry.

Some researchers search query's dominant location (QDL) and propose a solution to correctly detect it. QDL is geographical location(s) associated with a query in collective human knowledge [23], i.e., one or few prominent locations agreed by majority of people who know the answer to the query. Challenges in detecting queries' dominant locations lie in that QDL is a subjective and collective measure. It is the location existing in the collective human knowledge. The location name contained in the query string may or may not mean a geographical location.

V. PROPOSED SCHEME

We present an investigation of the real-time nature of Twitter that is designed to ascertain whether we can extract valid information from it. We propose an event notification system that monitors tweets and delivers notification promptly using knowledge from the investigation. In this research, we take three steps: first, we crawl numerous tweets related to target events; second, we propose probabilistic models to extract events from those tweets and estimate locations of events; finally, we developed an earthquake reporting system that extracts earthquakes from Twitter and sends a message to registered users.

A. Semantic Analysis of Tweets

We are detecting an event here. As described in this paper, we target event detection. An event is an arbitrary classification of a space-time region. An event might have actively participating agents, passive factors, products, and a location in space/time. We target events such as earthquakes, typhoons, and traffic jams, which are readily apparent upon examination of tweets. These events have several properties.

1. They are of large scale (many users experience the event).
2. They particularly influence the daily life of many people (for that reason, people are induced to tweet about it)
3. They have both spatial and temporal regions (so that real-time location estimation is possible).

Such events include social events such as large parties, sports events, exhibitions, accidents, and political campaigns. They also include natural events such as storms, heavy rains, tornadoes, typhoons/hurricanes/cyclones and earthquakes. We designate an event we would like to detect using Twitter as a target event. In this section, we explain how to detect a target event using Twitter. First, we crawl tweets including keywords related to a target event. From them, we extract tweets that certainly refer to a target event using devices that have been trained with machine learning. Second, we detect a target event and estimate the location from those tweets by treating Twitter users as "social sensors."

B. Temporal Model

Each tweet has its own post time. When a target event occurs, how do the sensors detect the event? We describe the temporal model of event detection.

First, we examine the actual data that presents the respective quantities of tweets for a target event: an earthquake. It is apparent that spikes occur in the number of tweets. Each corresponds to an event occurrence. Specifically regarding an earthquake, more than 10 earthquakes occurred during the period. The distribution is apparently an exponential distribution

C .Spatial Model

Each tweet is associated with a location. We describe a method that can estimate the location of an event from sensor readings.

A Particle filter is used here for estimating the target location. The Sequential Importance Sampling (SIS) algorithm is a Monte Carlo method that forms the basis for particle filters. The SIS algorithm consists of recursive propagation of the weights and support points as each measurement is received sequentially. Techniques has been made for the fast process. Therefore, we must decrease the time complexity of methods used for location estimation.

V.CONCLUSION

This paper has provided a more current evaluation and update of text mining research available. In this article, we tried to give a brief introduction to the broad field of text mining .Therefore, we motivated this field of research, gave a more formal definition of the terms used herein and presented a brief overview of currently available text mining methods, their properties and their application to specific problems. Even though, it was impossible to describe all algorithms and applications in detail within the (size)limits of an article, we think that the ideas discussed and the provided references should give the interested reader a rough overview of this field and several starting points for further studies.

REFERENCES

[1] A. Java, X. Song, T. Finin, and B. Tseng, "Why We Twitter: Understanding Microblogging Usage and Communities," Proc.Ninth WebKDD and First SNA-KDD Workshop Web Mining and Social Network Analysis (WebKDD/SNA-KDD '07), pp. 56-65, 2007.

[2] B. Huberman, D. Romero, and F. Wu, "Social Networks that Matter: Twitter under the Microscope," ArXiv E-Prints, http://arxiv.org/abs/0812.1045, Dec. 2008.

[3] H. Kwak, C. Lee, H. Park, and S. Moon, "What is Twitter, A Social Network or A News Media?" Proc. 19th Int'l Conf. World Wide Web(WWW '10), pp. 591-600, 2010.

[4] G.L. Danah Boyd and S. Golder, "Tweet, Tweet, Retweet: Conversational Aspects of Retweeting on Twitter," Proc. 43rd Hawaii Int'l Conf. System Sciences (HICSS-43), 2010.

[5] A. Tumasjan, T.O. Sprenger, P.G. Sandner, and I.M. Welpe,"Predicting Elections with Twitter: What 140 Characters Reveal About Political Sentiment," Proc. Fourth Int'l AAAI Conf. Weblogs and Social Media (ICWSM), 2010.

[6] K. Borau, C. Ullrich, J. Feng, and R. Shen, "Microblogging for Language Learning: Using Twitter to Train Communicative and Cultural Competence," Proc. Eighth Int'l Conf. Advances in Web Based Learning (ICWL '09), pp. 78-87, 2009.

[7] T. Sakaki, M. Okazaki, and Y. Matsuo, "Earthquake Shakes Twitter Users: Real-Time Event Detection by Social Sensors,"Proc. 19th Int'l Conf. World Wide Web (WWW '10), pp. 851-860,2010.

[8] T. Joachims, "Text Categorization with Support Vector Machines: Learning with Many Relevant Features," Proc. 10th European Conf.Machine Learning (ECML '98), pp. 137-142, 1998.

[9] X. Liu, S. Zhang, F. Wei, and M. Zhou, "Recognizing Named Entities in Tweets," Proc. 49th Ann. Meeting of the Assoc. for Computational Linguistics: Human Language Technologies (HLT '11), pp. 359-367, June 2011.

[10] A. Ritter, S. Clark Mausam, and O. Etzioni, "Named Entity Recognition in Tweets: An Experimental Study," Proc. Conf. Empirical Methods in Natural Language Processing, 2011.

[11] M. Arulampalam, S. Maskell, N. Gordon, and T. Clapp, "A Tutorial on Particle Filters for Online Nonlinear/Non-Gaussian Bayesian Tracking," IEEE Trans. Signal Processing, vol. 50, no. 2,pp. 174-188, Feb. 2002.

[12] Y. Matsuo and H. Yamamoto, "Community Gravity: Measuring Bidirectional Effects by Trust and Rating on Online Social Networks," Proc. 18th Int'l Conf. World Wide Web (WWW '09),pp. 751-760, 2009.

[13] E. Scordilis, C. Papazachos, G. Karakaisis, and V. Karakostas,"Accelerating Seismic Crustal Deformation before Strong Mainshocks in Adriatic and Its Importance for Earthquake Prediction,"J. Seismology, vol. 8, pp. 57-70, http://dx.doi.org/10.1023/B:JOSE.0000009504.69449.48, 2004.

[14] M. Cataldi, L. Di Caro, and C. Schifanella, "Emerging Topic Detection on Twitter Based on Temporal and Social Terms Evaluation," Proc. 10th Int'l Workshop Multimedia Data Mining (MDMKDD '10), pp. 1-10, 2010.

[15] B. O'Connor, R. Balasubramanyan, B.R. Routledge, and N.A.Smith, "From Tweets to Polls: Linking Text Sentiment to Public Opinion Time Series," Proc. Int'l AAAI Conf. Weblogs and Social Media, 2010.

[16] M. Ebner and M. Schiefner, "Microblogging - More than Fun?"Proc. IADIS Mobile Learning Conf., pp. 155-159, 2008.

[17] A. Passant, T. Hastrup, U. Bojars, and J. Breslin, "Microblogging: A Semantic Web and Distributed Approach," Proc. Fourth Workshop Scripting for the Semantic Web (SFSW '08), http://data. semanticweb.org/workshop/scripting/2008/paper/11, 2008.

[18] L. Backstrom, J. Kleinberg, R. Kumar, and J. Novak, "Spatial Variation in Search Engine Queries," Proc. 17th Int'l Conf. World Wide Web (WWW '08), pp. 357-366, 2008.

[19] Q. Mei, C. Liu, H. Su, and C. Zhai, "A Probabilistic Approach to Spatiotemporal Theme Pattern Mining on Weblogs," Proc. 15th Int'l Conf. World Wide Web (WWW '06), pp. 533-542, 2006.

[20] P. Serdyukov, V. Murdock, and R. van Zwol, "Placing Flickr Photos on a Map," Proc. 32nd Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR '09), pp. 484-491, 2009.

[21] T. Rattenbury, N. Good, and M. Naaman, "Towards Automatic Extraction of Event and Place Semantics from Flickr Tags," Proc.30th Ann. Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR '07), pp. 103-110, 2007.

[22] J. Hightower and G. Borriello, "Particle Filters for Location Estimation in Ubiquitous Computing: A Case Study," Proc. Int'lConf. Ubiquitous Computing (UbiComp '04), pp. 88-106, 2004.

[23] X. Xie, Y. lu, Lee Wang "Detecting Dominant Location from search Queries." 2009.

An Efficient Data Fusion Technique In Wireless Sensor Network

Karthikeyan B
Sathyabama University
Chennai-India
gurukarthi27@gmail.com

ABSTRACT

Remote sensor system is gathering of vast amounts of wire-less sensor hubs to gather data from their sensing ter-down pour. Remote sensor hubs are electric cell controlled mechanisms energy saving is dependably critical to the lifetime of remote sensor net-work. As of late numerous calculations are accessible to track energy saving issues in remote sensor system to expand life time of system the calculations are top-down methodology and lowest part up approach yet there are issues with this systems. The master postured procedure is a deferral cognizant strategy for remote sensor network utilizing customary rest and wake periods. The target of proposed system structure is to minimize delay and to increase lifetime of remote sensor system. The proposed system formation procedure is rest and wake period with top-down approach

Keywords:
Top-Down approach, Bottom-Up approach, Sleep and Wake Periods.

INTRODUCTION

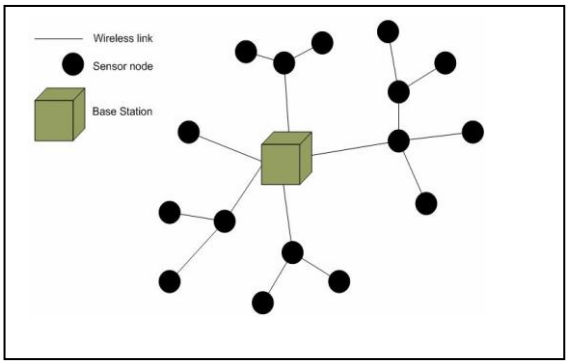
Solid versatility, far reaching sensing scope, and high fault tolerance are a percentage of the one of a kind points of interest of wire-less sensor systems. Remote sensor systems comprise of large amounts of remote sensor hubs, which are minimal, light-weighted, and electric cell controlled units that could be utilized as a part of virtually nature. In light of these extraordinary characteristics, sensor hubs are typically conveyed close to the focuses of investment in order to do short proximity sensing.The information gathered will undergoing-system techniques and after that come back to the client who is usually located in a remote site. More often than not, remote sensor nodes are found in compelling situations, where are excessively unfriendly for maintenance. Sensor hubs must monitor their rare vigor by all means and stay animated with a specific end goal to keep up the obliged sensing scope of the environment.[1]generally bunching is utilized to spare the vigor of the hub. A network with grouping is accumulation of numerous bunches. Inside each cluster there is bunch head(CH) and group member(CM). The cluster head is dependable to gather information from group member directly or in multihop way. By utilizing this the amount of node involved in transmission is reduced there four obliged vigor is also least.Wireless sensor network (WSN) is an emerging technology that has resulted in a variety of applications. Many applications such as health care, medical diagnostics, disaster management, military surveillance and emergency response have been deploying such networks as their main monitoring framework. Basically, a wireless sensor network consists of a number of tiny sensor nodes connected together through wireless links. Some more powerful nodes may operate as control nodes called base stations. Often, the sensing nodes are referred to as ''motes‟ while base stations are sometimes called “sinks‟. Each sensor node can sense data such as temperature, humidity, pressure from its surroundings, conduct simple computations on the collected data and send it to other neighboring nodes through the communication links. The sensing nodes known as ''motes‟ are represented by black spheres and are responsible for observing the surrounding environment whereas the cube represents a control node known as ”sink‟ which serves as the base station.

RELATED WORK

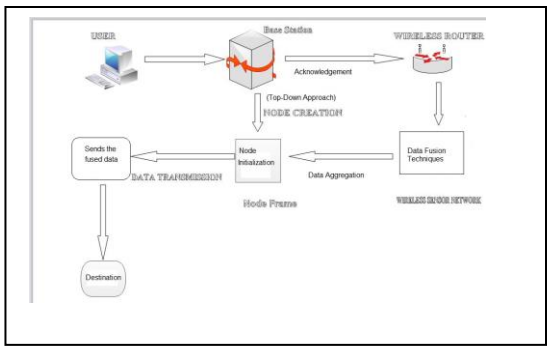
In remote sensor system most extreme vigor is used in wire-less communication. The vigor used is specifically proportional to relating separation. The long separation correspondence of node with base station is bad thought. One approach to lessen energy is by utilizing grouping calculation. The Clustering algorithm works as follows 1)Organization of hubs into group. 2)With the bunch one node chose as group head and other are bunch part. 3)The cluster head gather information from bunch part, join together packet by utilizing data/decision combination strategy. Submit intertwined information to remote base station.

Here bunch head just take an interest in long transmission therefour energy of other hub is reduced.Research has been directed on reducing vigor by forming cluster with proper system structure. Heinzelman et al. Proposed a bunching calculation called LEACH Low-Energy adaptive Clustering Hierarchy [1]. The LEACH convention is a hierarchical convention in which most hubs transmit to cluster heads. The operation of the LEACH convention comprises of two phases:

1)The Setup stage. In setup stage the bunch heads are selected. The group head aggregate, layer, forward information bundle to the base station. Every hub verifies if it will become a group head, in this round, by utilizing a stochastic algorithm at each one round. Assuming that a hub turns into a group head for one time, it can't get to be bunch set out again toward q rounds, where q is the craved rate of group heads. From that point, the probability of a hub to wind up a cluster head in each one round is1/q. This turn of bunch heads prompts an adjusted energy consumption to all the hubs and thus to a more extended lifetime of the system.The Steady State Phase. In the Steady State phase, the information is sent to the base station. The length of time of the steady state stage is longer than the span of the setup phase in request to minimize overhead. Also, each one hub that is not a cluster head chooses the closest bunch head and joins that cluster.



After that the group head makes a timetable for every hub in its bunch to transmit its information. The principle playing point of Leach is that it outflanks accepted correspondence conventions, in terms of vigor dispersal, simplicity of design, and system lifetime/quality of the system. Giving such a low energy, wireless circulated convention will help prepare in a WSN. How ever, LEACH utilization single-jump steering where every node can transmit specifically to the bunch head and the sink. Therefore, it is not prescribed for systems that are conveyed in large regions. Moreover, the dynamic bunching may comes about to extra overhead, e.g. head changes, promotions and so forth., which may lessen the addition in vigor consumption. [2]Low-Energy Adaptive Clustering Hierarchy Centralized (LEACH-C): The LEACH-C uses the base station for cluster formation, not at all like LEACH where hubs self-design them-selves into clusters. Initially in the LEACH-C, the Base Station(BS) gets data in regards to the area and energy level of every hub in the system. After that, utilizing this information, the BS discovers a decided beforehand number of bunch heads and designs the system into clusters. The group groupings are decided to minimize the vigor needed for non-group head nodes to transmit their information to their separate bunch heads. The changes of this calculation contrasted with LEACH are the accompanying: 1)The BS uses its worldwide learning of the network to transform groups that require less vigor for data transmission. Dissimilar to LEACH where the amount of cluster heads differs from round to adjust because of the absence of global coordination around hubs, in LEACH-C the amount of cluster heads in each one round equivalents a decided beforehand optimal value.[2]Threshold delicate Energy Efficient sensor Network protocol(TEEN): The TEEN is a progressive convention intended for the conditions like sudden changes in the sensed traits such as temperature. The responsiveness is critical for time-critical applications, in which the system is worked in a reactive mode. The sensor system building design in TEEN is based on a progressive assembling where closer hubs structure bunches and this process goes on the second level until the sink is reached. In this plan the bunch head telecasts to its parts the hard Threshold (HT) and the Soft Threshold (ST). The HT is a threshold esteem for the sensed characteristic. It is irrefutably the value of the quality past which, the hub sensing this worth must switch on its transmitter and report to its bunch head. The ST is a little change in the quality of the sensed ascribe which triggers the hub to switch on its transmitter and transmit. The nodes sense their surroundings constantly. The first run through a parameter from the quality set achieves its hard limit esteem, the node switches on its transmitter and sends the sensed information. The sensed value is archived in an inner variable in the hub, called the sensed quality (SV). The fundamental point of interest of TEEN is that it works well in the conditions like sudden changes in the sensed attributes, for example, temperature. Then again, in vast area networks and when the amount of layers in the chain of importance is small, TEEN has a tendency to expend a great deal of vigor, due to long distance transmissions. Additionally, when the amount of layers increases, the transmissions get to be shorter and overhead in the setup stage and also the operation of the system exist.[2]Lindsey and Raghavendra proposed an alternate bunching algorithm called PEGASIS Power-Efficient Gathering in Sensor information Systems. The PEGASIS convention is chain based protocol and change in LEACH convention. In PEGASIS each hub correspond just with a close-by neighbour to send and get bundle. It alternates transmitting to the base station, thus reducing the measure of vigor used for every round. By utilizing voracious calculation we can structure a chain considering starting hub haphazardly or base station. By minimizing the number of bunch heads, the vigor expended in long distance transmission is further minimized. In general, the PEGASIS protocol displays twice or more execution in comparison with the LEACH convention However, the PEGASIS protocol causes the excess information transmission since one of the nodes on the chain has been chosen. Not at all like LEACH, the transmitting distance for the greater part of the hubs is diminished in PEGASIS. Experimental effects indicate that PEGASIS furnishes change by factor 2 contrasted with LEACH convention for 50m x 50m network and change by element 3 for 100m x 100m system. The PEGASIS convention, be that as it may, has a basic issue that is the redundant transmission of the information. The reason for this issue is that there is no attention of the base stations area about the vigor of hubs when one of hubs is chosen as the head node.[2]Tan and Korpeoglu created PEDAP, which is dependent upon the idea of a base crossing tree (MST). Additionally minimizing the measure of long separation transmission, the communication distances around sensor hubs are minimized[1]. Fonseca etal. Proposed the gathering tree convention (CTP). The CTP is a kind of inclination based tracking convention which utilizes expected transmissions (ETX) as its steering angle. ETX is the number of needed transmissions of a bundle vital for it to be received without lapse. Ways with low ETX are required to have high throughput. Hubs in a system utilizing CTP will always pick a way with the most minimal ETX. By and large, the ETX of a path is corresponding to the comparing way length. Therefore, CTP can significantly decrease the correspondence separations around sensor nodes[1]. Another critical methodology is Top-Down approach. In top-Down approach all hubs take an interest in transmission by using this deferral might be minimized. The generally approach is going to execute at base station. Base station is dependable for all the exercises. The an alternate methodology is Bottom-Up approach. In Bottom-Up methodology join the



group of the same size to gather. It is adaptable than Top-Down methodology. In Bottom-Up approach the base station is chosen from around hubs depending on energy of node.

DATA FUSION METHOD

Wireless Sensor system hold extensive number of remote sensor nodes to gather data from different hubs. Remote sensor nodes are electric cell fueled gadgets vigor sparing is dependably important to the lifetime of remote sensor system. Here we are going to arrange the remote hubs in such way that the deferral is minimum and vigor of hub is devoured less by utilizing different algorithm to sort out the nodes. The calculation we are going to use Top-Down methodology utilizing general rest and wake periods nodes. The calculation we are going to use Top-Down methodology utilizing general rest and wake periods.

1.1)Mathematical Model

Remote sensor hub could be made of utilizing three major units, namely the microcontroller unit(MCU), the transceiver unit(TCR), and the sensor board(SB). Each of which expend a certain measure of vigor while working. The vigor consumed by remote sensor hub i might be given as

$$E_{j\_SN} = E_{j\_MCU} + E_{j\_TCR} + E_{j\_SB} \quad (1)$$

where Ej-MCU denotes vigor devoured by microcontrol unit, Ej-TCR denotes vigor devoured by transreceiver and Ej-SB denotes vigor by sensor board. The Ej-TCR can be further classified as

$$E_{j\_TCR} = E_{j\_TCR\_RX} + E_{j\_TCR\_TX}(d_j) \quad (2)$$

here Ej-TCR-RX represents vigor devoured by transreceiver in appropriating mode, while Ej-TCR-TX(dj) speaks to energy consumed by the transreceiver to transmit for separation of dj. The Total vigor devoured by a system of N hubs is given by

$$E_{TOT}(N) = \sum_{j=1}^{N} E_{j\_MCU} + E_{j\_TCR\_RX} + E_{j\_TCR\_TX}(d_j) + E_{j\_SB} \quad (3)$$

Normally Ej-MCU, Ej-TCR, Ej-TCR –RX are consistent. But Ej-TCR-TX(dj) is capacity of dj which is relies on upon network structure. Therefour (3) might be adjusted as

$$E_{TOT}(N) = C_1 + \sum_{j=1}^{N} E_{j\_TCR\_TX}(d_j) \quad (4)$$

Here C1is steady. The Ej-TCR-TX(dj) could be further expressed as

$$E_{j\_TCR\_TX}(d_j) = E_{j\_TCR\_EC} + E_{j\_TCR\_PA} d_j^2 \quad (5)$$

where Ej-TCR-EC is the vigor used by TCR's electronic circuitry, while Ej-TCR-PA is the vigor devoured by power amplifier of TCR both are consistent therefour (4) might be expressed as

$$E_{TOT} = C_1 + C_2 + C_3 \sum_{j=1}^{N} d_j^2 \quad (6)$$

Here C1and C2are steady Here (6) shows that aggregate energy utilized of system could be minimized by diminishing separation. To organize hub with least remove the proposed calculation is top-Down methodology with periodic rest and wake periods.

3.2 Top-Down Approach with periodic slumber and wake periods

In this approach, the base station is accepted to have the coordinates of all sensor hubs in the system. The algorithm is set to execute at base station. At the last base station will inform to all hubs make an information association from the appropriate network structure. To build the system for N = 20andn = 21is straightforward. For systems with N = 2pnodes, p=2,3,.. the algorithm is indicated below

1) The calculation begins with recognizing the entire system as a completely joined system. In this paper, the term connected refers to the presence of an information connect between two wireless sensor hubs which is utilized to transmit information bundles in the data collection forms. Two remote sensor hubs are characterized as disconnected from one another if there does not exist any direct data interface between them. For a network of N = 2pnodes where p=2,3,.. every hub will begin with degree equivalent to N − 1. The hubs will structure the set Gs= 1set k = N/2.

2) Select k hubs from set Hs= 1 to structure set Hs+ 1, such that d2i,jis maximized. Here di,j represent geological distance between hubs i and j. Whatever is left of the hubs from Hs= 1 will from set Hs+1. The calculation will then evacuate all connections among hubs inside Gs+ 1. Set cycles s=s+1 and b=b/2.

3) Repeat step 2 until k < 2 set r.

4) Nodes with degree N-r structure set L. Hubs with degree greater than N-r structure set U such that set L and set U are of the same number of hubs. Every hub in set L is just associated with a single hub in set U. Set r=r*2

5) Repeat step 4 until r=n

1.RESULT AND DISCUSSION

Top-Down methodology have some burden's as takes after All nodes are taking part in the transmission by utilizing this postponement can be minimized yet arrange lifetime can't enhanced to improve this we can utilize rest and wake period with top-down approach by utilizing this base hub set to partake in the data transfer so lifetime of system is

progressed. Steps in Sleep And Wake Period With Top-Down Approach:

1) Initially All hubs are not partake in transmission. Only few hubs are wake-up initially.
2) After some time rest hub gets to be initiate and take participate in the transmission.
3) When the new hubs are added the way to impart to base station is figured once again.
4) Likewise the working rest and wake period with top-down approach take place.

CONCLUSION

In this paper, a deferral mindful information gathering system structure and formation calculation are proposed. The proposed system formation calculation is top-down methodology with slumber and wake periods. The execution of proposed system calculation is com-pared with top-down methodology. The proposed system structure minimized postpone in correspondence and increase lifetime of network. The proposed system structure can profoundly diminish the data collection time while keeping the aggregate correspondence distance and the system lifetime at least values.

REFERENCES

[1] C.M.Lau Chi-Tsun Cheng, Chi K. Tse ”A delay-aware data collection network structure for wireless sensor networks”. IEEE SENSORS JOURNAL,VOL. 11, NO. 3, MARCH 2011

[2] Nikolaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados, Senior Member,IEEE ”Energy-Efficient Routing Protocols in Wireless Sensor Networks:A Survey”. IEEE COMMUNICATIONS SURVEYS TUTORIALS, ACCEPTED FOR PUBLICATION,2012 IEEE

[3] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, An ap- plication-specific protocol architecture for wireless microsensor net- works, IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660670, Oct. 2002.

[4] S. Lindsey and C. S. Raghavendra, PEGASIS: Powerefficient gath- ering in sensor information systems, in Proc. IEEE Conf. Aerosp., Big Sky, MT, USA, Mar. 2002, vol. 3, pp. 11251130.

[5] H. Tan and . Krpeoglu, Power efficient data gathering and aggre- gation in wireless sensor networks, ACM SIGMOD Record, vol. 32, no. 4, pp. 6671, Dec. 2003.

[6] R. Fonseca, O. Gnawali, K. Jamieson, S. Kim, P. Levis, and A. Woo, The collection tree protocol, TinyOS Enhancement Proposals (TEP), vol. 123, Dec. 2007.

[7] D. S. J. D. Couto, High-Throughput routing for multihop wireless networks, Ph.D. dissertation, Dept. Elect. Eng. Comput. Sci., Massa- chusetts Inst. Technol., Cambridge, MA, 2004

[8] O. Tekdas, J. H. Lim, A. Terzis, and V. Isler, Using mobile robots to harvest data from sensor fields, IEEE Wireless Commun. Mag., vol. 16, no. 1, pp. 2228, Feb. 2009.

[9] A. Manjeshwar and D. P. Agrawal, TEEN: A routing protocol for enhanced efficiency in wireless sensor networks, in Proc. 15th Int. Symp. Parallel Distrib. Process., (IPDPS 2001), San Francisco, CA, Apr. 2001, pp. 20092015.

[10] A. Manjeshwar and D. P. Agrawal, APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks, in Proc. 16th Int. Symp. Parallel Distrib. Process., (IPDPS 2002), Fort Lauderdale, FL, Apr. 2002, pp. 195202. .

DETECTION OF CAR LICENSE PLATE BY USING VEDA METHOD

P.S. Benitta
Assistant Professor
Department of ECE
T. J. Institute of Technology
Ph. No: 9551612780
Mail id: benishaiju@gmail.com

B.Karthick
P.G. Scholar
Department of ECE
T. J. Institute of Technology
Ph. No. 9894680654
Mail id: karthi.hits@gmail.com

Abstract-This paper proposes a fast method for car-license plate detection (CLPD) and presents three main contributions. The first contribution is that we propose a fast vertical edge detection algorithm (VEDA) based on the contrast between the grayscale values, which enhances the speed of the CLPD method. After binarizing the input image using adaptive thresholding (AT), an unwanted-line elimination algorithm (ULEA) is proposed to enhance the image, and then, the VEDA is applied. The second contribution is that our proposed CLPD method processes very-low-resolution images taken by a web camera. After the vertical edges have been detected by the VEDA, the desired plate details based on color information are highlighted. Then, the candidate region based on statistical and logical operations will be extracted. Finally, an LP is detected

I. INTRODUCTION

The term digital image refers to processing of a two dimensional picture by a digital computer. In a broader context, it implies digital processing of any two dimensional data. A digital image is an array of real or complex numbers represented by a finite number of bits. An image given in the form of a transparency, slide, photograph or an X-ray is first digitized and stored as a matrix of binary digits in computer memory. This digitized image can then be processed and/or displayed on a high-resolution television monitor. For display, the image is stored in a rapid-access buffer memory, which refreshes the monitor at a rate of 25 frames per second to produce a visually continuous display.

II. IMAGE PROCESSING FUNDAMENTAL

1 Digital image processing refers processing of the image in digital form. Modern cameras may directly take the image in digital form but generally images are originated in optical form. They are captured by video cameras and digitalized. The digitalization process includes sampling, quantization. Then these images

are processed by the five fundamental processes, at least any one of them, not necessarily all of them.

III. PRO POSED SYSTEM

This paper has three contributions: The VEDA is proposed and used for detecting vertical edges. In this paper, the color input image is converted to a grayscale image, and then, adaptive thresholding (AT) is applied on the image to constitute the binarized image. After that, the ULEA is applied to remove noise and to enhance the binarized image. Next, the vertical edges are extracted by using the VEDA. The next process is to detect the LP; the plate details are highlighted based on the pixel value with the help of the VEDA output. Then, some statistical and logical operations are used to detect candidate regions and to search for the true candidate region. Finally, the true plate region is detected in the original image.

IV. GRAYSCALE

In photography and computing, a grayscale or greyscale digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest.

Grayscale images are distinct from one-bit bi-tonal black-and-white images, which in the context of computer imaging are images with only the two colors, black, and white (also called bilevel or binary images). Grayscale images have many shades of gray in between. Grayscale images are also called monochromatic, denoting the presence of only one (mono) color (chrome). Grayscale images are often the result of measuring the intensity of light at each pixel in a single band of the electromagnetic spectrum (e.g. infrared, visible light, ultraviolet, etc.), and in such cases they are monochromatic proper when only a given frequency is captured. But also they can be synthesized from a full color image; see the section about converting to grayscale

V.BINARIZATION

A binary image is a digital image that has only two possible values for each pixel. Typically the two colors used for a binary image are black and white though any two colors can be used. The color used for the object(s) in the image is the foreground color while the rest of the image is the background color. In the document scanning industry this is often referred to as bi-tonal.

Binary images are also called bi-level or two-level. This means that each pixel is stored as a single bit (0 or 1). The names black-and-

white, B&W, monochrome or monochromatic are often used for this concept, but may also designate any images that have only one sample per pixel, such as grayscale images.

VI. UNWANTED LINE ELIMINATION ALGORITHM

A 3 × 3 mask is used throughout all image pixels. Only black pixel values in the thresholded image are tested. Once, the current pixel value located at the mask center is black, the eight-neighbor pixel values are tested. If two corresponding values are white together, then the current pixel is converted to a white value asa foreground pixel value. The output after the ULEA is performed, whereby many unwanted lines are removed from the image. This kind of image is nearly ready for a better segmentation process.

VII. VEDA (Vertical Edge Detection Algorithm)

The advantage of the VEDA is to distinguish the plate detail region, particularly the beginning and the end of each character. Therefore, the plate details will be easily detected, and the character recognition process will be done faster. After thresholding and ULEA processes, the image will only have black and white regions, and the VEDA is processing these regions. The idea of the VEDA concentrates on intersections of black–white and white–black. A 2 × 4 mask is proposed for this process. The center pixel of the mask is located at points (0, 1) and (1, 1). By moving the mask from left to right, the black–white regions will be found. Therefore, the last two black pixels will only be kept. Similarly, the first black pixel in the case of white–black regions will be kept.

VIII. SNAPSHOTS

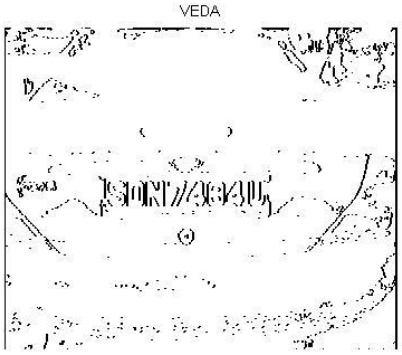
1.1.1 INPUT IMAGE

1.1.2 GRAYSCALE IMAGE

1.1.3.THRESHOLDIMAGE

1.1.4. ULEA IMAGE

1.1.5.VEDA



IX CONCLUSION

We have proposed a new and fast algorithm for vertical edge detection, in which its performance is faster than the performance of Sobel by five to nine times depending on image resolution. The VEDA contributes to make the whole proposed CLPD method faster. We have proposed a CLPD method in which data set was captured by using a web camera. We employed those images taken from various scenes and under different conditions. VEDA-based CLPD is better in terms of the computation time and the detection rate.

X FUTURE ENHANCEMENT

As a future work, the VEDA based and Sobel based CPLD can be compared in terms of the computation time or processing time, detection rate, accuracy, algorithm complexity. Further we can use canny edge detector for the edge detection.

XI REFERENCES

1 H. Bai and C. Liu, "A hybrid license plate extraction method based on edge statistics and morphology," in Proc. 17th Int. Conf. Pattern Recognit., Cambridge, U.K., 2004, pp. 831–834.

2 M. Fukumi, Y. Takeuchi, H. Fukumoto, Y. Mitsura, and M. Khalid, "Neural network based threshold determination for Malaysia license plate character recognition," in Proc. 9th Int. Conf. Mechatron. Technol., 2005, pp. 1–5.

3 R. Parisi, E. D. Di Claudio, G. Lucarelli, and G. Orlandi, "Car plate recognition by neural networks and image processing," in Proc. IEEE Int. Symp. Circuits Syst., 1998, pp. 195–198.

4 T. Naito, T. Tsukada, K. Yamada, K. Kozuka, and S. Yamamoto, "Robust license-plate recognition method for passing vehicles under outside environment," IEEE Trans. Veh. Technol., vol. 49, no. 6, pp. 2309–2319, Nov. 2000.

5 H.-H. P. Wu, H.-H. Chen, R.-J. Wu, and D.-F. Shen, "License plate extraction in low resolution video," in Proc. IEEE 18th Int. Conf. Pattern Recognit., Hong Kong, 2006, pp. 824–827.

6 J.-W. Hsieh, S.-H. Yu, and Y. S. Chen, "Morphology-based license plate detection from complex scenes," in Proc. 16th Int. Conf. Pattern Recognit., Quebec City, QC, Canada, 2002, pp. 176 179.

7 J. R. Parker and P. Federl, "An approach to license plate recognition," in Proc. Visual Interface, Kelowna, BC, Canada, 1997, pp. 178–182.

8 H. Zhang, W. Jia, X. He, and Q. Wu, "A fast algorithm for license plate detection in various conditions," in Proc. IEEE Int. Conf. Syst., Man, Cybern., Taipei, Taiwan, 2006, pp. 2420–2425.

9 Z.-X. Chen, Y.-L. Cheng, F.-J. Chang, and G.-Y. Wang, "Automatic license-plate location and recognition based on feature salience," IEEE Trans. Veh. Technol., vol. 58, no. 7, pp. 3781–3785, Sep. 2009.

10 K. Debi, H.-U. Chae, and C. K.-H. Jo, "Parallelogram and histogram based vehicle license plate detection," in Proc. IEEE Int. Conf. Smart Manuf. Appl., Gyeonggi-do, Korea, 2008, pp. 349–353.

11 S.-L. Chang, L.-S. Chen, Y.-C. Chung, and S.-W. Chen, "Automatic license plate recognition," IEEE Trans. Intell. Transp. Syst., vol. 5, no. 1, pp. 42–53, Mar. 2004.

12 D. Bradley and G. Roth, "Adaptive thresholding using the integral image," J. Graph. Tools, vol. 12, no. 2, pp. 13–21, Jun. 2007.

13 F. Shafait, D. Keysers, and T. M. Breuel, "Efficient implementation of local adaptive thresholding techniques using integral images," in Proc. Doc. Recognit. Retriev., 2007, pp. 681510-1–681510-6.

14 P. D. Wellner, "Adaptive thresholding for the DigitalDesk," Rank Xerox Ltd., Birmingham, U.K., Tech. Rep. EPC-1993-110, 1993.

15 F. Porikli and O. Tuzel, "Fast construction of covariance matrices for arbitrary size image windows," in Proc. Int. Conf. Image Process., 2006, pp. 1581–1584.

Archaic Locality by segmentation in Statistical Brokering System

S.Sabeena[#1], P.Joyce Beryl Princess[#2]

#1 PG scholar, CSE Department, SCAD CET, Cheranmahadevi, TamilNadu

#2 Assistant Professor, CSE Department, SCAD CET, Cheranmahadevi, TamilNadu

sabismarty@gmail.com , joyshenry@gmail.com

Abstract **---- Information brokering system helps to answer the client queries from the requested data servers. some organizations like healthcare and law enforcement want to conserve their own data at the time of data sharing between the organizations. Because an antagonist can discover the characteristics of the location from the query substance. And there is a chance that the broker functionality may be outsourced. We introduce Location Preserving Information Brokering(LPIB) to preserve the location effectively without violating users data privacy. It identifies the antagonist enter into the system and mystifying them using fake substance.**

Index Terms---Access Control Enforcement, Content Based Query Routing, Information Brokering, Query Fragmentation.

I. INTRODUCTION

Along with the detonation of information collected by the organization, the organization have to preserve their own data privacy. Without proper management of data collected by the organization the client's privacy may be severely breached[1]. Many efforts have been residential to conserve the data but the privacy is still a challenging one. Traditional privacy protection mechanism simply removing client's personal information or using anonymization[3] technique fails to deal with privacy protection of data. It leads to a key management overhead. It is rigid to fabricate and not reliant on cryptography as the basis of data privacy. Most of the existing system focusing on data veracity and secrecy, does not focusing on privacy effectively. It adopt either query-answering model[9], where peers are fully independent[10] and are managed by a smaller amount of autonomy but lacks system wide synchronization.

In such a scenario, sharing a complete data with other providers is not possible. To address this problem, federated database technology have been proposed. This is not scalable while storing and maintaining of data. In k_anonymization, Locality Sensitive Hashing (LSH)[2] reduces the dispensation instance in querying progression but same abuser may assign to multiple cloaks. It leads to malicious actions. With near-uniform randomness the anonymization has to be maintained. It develop a suite for scalable and efficient cloaking. Since the system capability may be demoralized to conceal the user identity. Mixzones[5] are to be introduced to enhance user privacy. It uses middleware mechanism to prevent tracking of long-term user movements. If applications are to be untrusted the pseudonyms are to be inward and it may collapse the system concert. The false positioning of data(Dummies) are to be created to preserve the privacy of user location. If dummies are created randomly it can be easily identified.

Take healthcare system as an example, it assist access to and retrieval of data across combined healthcare providers. The participating organization cannot share complete data with this provider, since its data is legally confidential or publicly proprietary. Location information contain much more information than query content. At the time of data sharing between the providers the adversary can

find the identity of the requestor from the query location. It may collapse a system security. In our previous study, *Information Brokering System*(IBS) preserve sensitive and autonomous data by creating data-centric overlay that consists of data sources and a set of brokers. Information providers are connected to set of brokers. The client foremost presumptuous the query to the broker and it may routed according to the metadata until it reaches the exact server. While IBS approach consider on integrity and confidentiality but fails to achieve privacy. Because there is a chance that the broker functionality may be outsource to multiple person they are not involved in the organization.

In this article, we present a novel approach for *Location Preserving Information Brokering*(LPIB) to solve the problem for privacy conservation. It is a superimpose infrastructure consisting of three types of brokering components. They are *brokers, coordinators* and *focal clout*. The brokers works as a misnomer that searches information for client and retort to their appeal. Coordinators are associated with tree configuration as of the brokers. The brokers split the queries into segments and assign to multiple coordinators. This exertion collaboratively to enforce secure routing. Focal clout decides whether it is valid or invalid user pierce into the system. To achieve the location preservation, the proposed LPIB make sure that the nosy coordinators does not infer any information from the data disclosed to it. Experimental results shows that LPIB provides location preservation with no significant overhead and exceedingly superior scalability.

The rest of the paper is organized by the threats in location preserving scenario in section II, and declare related work in Section III. In Section IV, we present a novel schemes for location preservation. We analyse and evaluate the performance of location preservation and security in Section V, and conclude our work in Section VI.

II. THE PROBLEM

A. The System and Hazard Model

In a location preserving brokering, there are three types of stakeholders. They are data owners, data providers and data requestors. The privacy of a location may be inferred from the data where it come from. Data owners be in possession of having personal information regarding them and they are expecting privacy from the providers. Data providers own the data of data provider and contribute to the data requestors that they necessitate. Data requestors can get the response from the data providers for their queries.

Locality attack. An antagonist can presume the identity of a requester from the query location. At the time of routing there may be a chance for the adversary to get the location information. If they get the location information there is a chance that the data owner's private information may have to be distorted. This may perhaps conspire largely the system concert.

Example: Anne sends an ER to Newyork hospital. Doctor queries for her medical testimony through the brokering system. Since Anne has a symptom of leukemia, the query having two predicates:[name="Anne"] and[symptom="leukemia"]. If a adversary can guess the location of a requestor, it act as a inventive user and get the information. Using this information it may crumple the intact system.

B. Solution Overview

To address the need for location privacy vulnerabilities, we introduce Location Preserving Information Brokering(LPIB). First the queries are sent to the broker, according to the metadata the queries are routed in anticipation of reaching the right server. At this time the queries are encrypted and splitted as fragments and these are assigned to various coordinators concerned in the brokering system. When the user pierce into the system to get the information from the broker, focal clout checks whether it is legitimate or non-legitimate user enter into the system. If a legitimate user enter into the system the coordinators decrypt the query and forward it to the end user. Otherwise it forward the user to the fake location. Thus LPIB provides finest privacy by mystifying the antagonist with the help of fake substance.

III. BACKGROUND

A. Related Work

Privacy Preserving Location Query Protocol(PLQP) allows diverse levels of location query in a encrypted form. This is efficient to apply in a mobile platform but the lowest

level corresponds to nothing and highest level corresponds to exact location[3]. Order Preserving Symmetric Encryption(OPSE) properly utilizing cryptographic archaic but this shore up only boolean search exclusive of capturing any relevance to the data[2]. It is desirable to store data in a encrypted form in servers for security purpose. In this scenario, the opponent cannot learn anything about the plaintext. This is provably secure, efficient and practical but it only support O(n) stream cipher and block cipher operations.

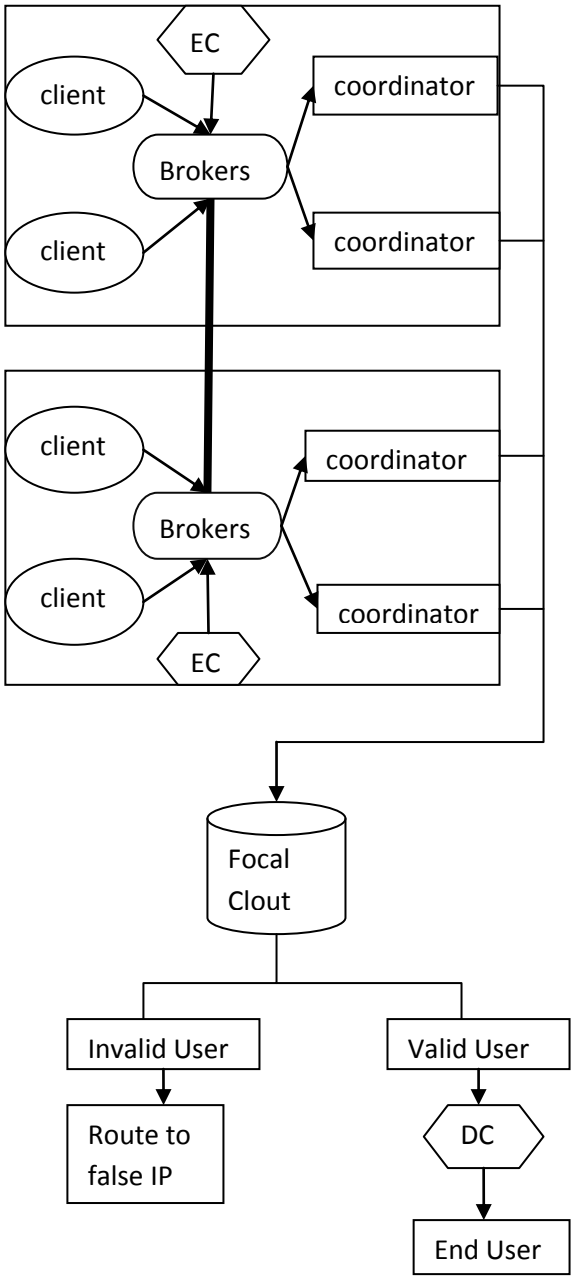
Authorized Private Keyword Search provides efficient multi-dimensional keyword search. Anonymous selection algorithm that selects a query requestor with near-uniform randomness, to secure anonymity. This ensures high degree of QOS and privacy and there is a chance of misusing of agents. Mixzones[5] are to be used to enhance user privacy and to enhance user identity. For that it use middleware mechanism. If applications are untrusted they may collude. False positioning of data(Dummies)[4] are to be created so that data provider cannot distinguish true positioning of data. If dummies are created randomly it can easily identified.

IV. LOCATION PRESERVING INFORMATION BROKERING SCHEME

This scheme is to preserve the location effectively by the means of LPIB. Fig 4.1 shows the overview of LPIB. This include brokers, coordinators and focal clout. The queries that are splitted that are encrypted and consign to several coordinators concerned in the brokering system. The decisions that are engaged by the focal clout whether it is valid or invalid user enter into the system to decrypt the query and presumptuous it to the end user. To preserve the location from the invalid user, it is the way to confusing them using fake objects.

A.Query Generation

The Client is the end user who sends query to the Server. The Client may send data to the Server send query to retrieve data from the Server. A process for generating SQL queries to retrieve requested information from a database.. If on the other hand the required table does not exist in the current query, a sub-query that navigates associations from the tables involved in the current query to the required on is added, and the "WHERE" condition is added to the required table within the sub-query. Queries are generically defined



EC--- Encryption Centre
DC--- Decryption Centre

Fig 4.1 Overview of LPIB scheme

with metadata. The metadata identifies specific queries and specific parameters associated with a given query. When a query instance is desired, parameter values are dynamically acquired and used to populate portions of the metadata associated with a desired query. It is the phase that the queries find their desired value and get responded for the request.

B. Query Fragmentation And Cloaking

Data servers and requestors from different organizations connect to the system through local brokers. A

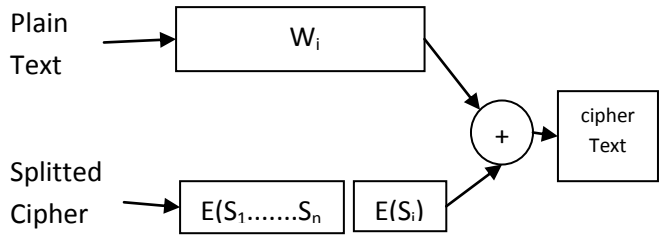


Fig 4.2 Splitting Operation

local broker functions as the "entrance" to the system. It authenticates the requestor and hides his identity from other PPIB components. The brokers, acting as mix anonymizer, are mainly responsible for user authentication and query forwarding. It would also permute query sequence to defend against local traffic analysis. Brokers are interconnected through coordinators.

Algorithm 1: Query Fragmentation

Input: Transition State S
Output: Fragment Address:address
1: For each symbol k in S.StateTTabe do
2: address=deployFragment
(S.StateTTable(k).nextState)
3:D=CreareDummyAcceptState()
4: D.nextState<--- address
5: S.StateTTable(k).nextState<---D
6: end for
7: F=CreateFragment()
8: F.addFragment(S)
9: C=getCoordinator()
10:C.assignFragment(F)
11:return C.address

It is an attempt to hide the network name from being broadcast publicly. Many routers come with this option as a standard feature in the setup menu accessed via a web browser. Although network cloaking may stop some inexperienced user from gaining access to AP.

C. Safe Routing

Coordinators are responsible for content-based query routing and access control enforcement. With privacy-preserving considerations, we cannot let a coordinator hold any rule in the complete form. Instead, a novel automaton segmentation scheme is proposed to divide (metadata) rules into segments and assign each segment to a coordinator. Coordinators operate collaboratively to enforce secure query routing. Fig 4.2 shows the splitting operation. A query segment encryption scheme is further proposed to prevent coordinators from seeing sensitive predicates. This scheme divides a query into segments, and encrypts each segment in a way that to each coordinator en route only the segments that are needed for secure routing are revealed.

D. Focal Clout

Focal clout handles key management and metadata maintenance. With the highest level of trust, it holds a global view about the key management. Except the query session keys created by the user, other keys are generated and maintained by the FC. The data servers are treated as a unique party and share a pair of public and private keys. while each of the coordinator has its own pairs of level key and commutative level key. Along with the fragmentation and deployment process, the FC creates key pairs of coordinators at each level and assigns the private keys with the fragments. The level keys need to be revoked in a batch once a certificate expires or when a coordinator at the same level quits the system.

V.PERFORMANCE ANALYSIS

A. processing Time

At the time of query forwarding, the time it takes for encryption and assign to each coordinator are noticed. Fig 5.1 shows the processing time. If original user enter into the system it decrypts the query and forward it to the enduser. This time also uniquely noticed and the processing time are to be evaluated.

B. File Size

The file that the broker must contain have to be noticed. Thus we have to evaluate how much time it has to be

information provider and the requestor. Client is the owner of the file having their personal information.

C. No of splits per file

The file containing information that are to be splitted and assign to each coordinator involved in the system. Our system calculates how much split it takes according to the file size. This work is to reduce the coordinator and ensure a security and privacy.

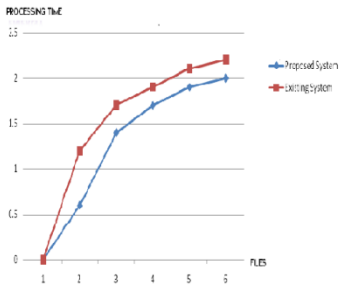


Fig 5.1. Estimate the processing time in LPIB

VI.CONCLUSION

With little consideration on privacy of user, and data existing system suffering from hazards. For that we introduce LPIB , a new approach to preserve privacy by mystifying the adversary by using fake objects. This analysis shows that it is very defiant to locality attack and evaluations shows it is efficient and scalable.

REFERENCES

[1]Xiang-Yang,taeho Juny "Search Me If You Can:Privacy-preserving Location Query Service" proceedings IEEE INFOCOM 2013.

[2]T. Hashem and L. Kulik, “Safeguarding location privacy in wireless ad-hoc networks,” Ubicomp 2007: Ubiquitous Computing, pp. 372–390,2007.

[3] K. Vu, R. Zheng, and J. Gao, “Efficient algorithms for k-anonymous location privacy in participatory sensing.” in IEEE INFOCOM, 2012.

[4] H. Kido, Y. Yanagisawa, and T. Satoh, “Protection of location privacy using dummies for location-based services,”in 21st international conference on Data Engineering workshop,2005.

[5] A. Beresford and F. Stajano, “Mix zones: User privacy in location-aware services,” in Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004, pp. 127–131.

[6] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, “Swing &swap: user-centric approaches towards maximizing location privacy,” in Proceedings of the 5th ACM workshop on Privacy in electronic society,2006, pp. 19–28.

[7] Jie Yang, Yingying Chen, Wade Trappe, Jerry Cheng,″ Determining the Number of Attackers and Localizing Multiple Adversaries in Wireless Spoofing Attacks", in proceedings of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2009.

[8] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, “Preventing location-based identity inference in anonymous spatial queries,” IEEE Transactions on Knowledge and Data Engineering, vol. 19, no. 12, pp.1719–1733, 2007.

[9] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, “Preventing location-based identity inference in anonymous spatial queries,” IEEE Transactions on Knowledge and Data Engineering, vol. 19, no. 12, pp.1719–1733, 2007.

[10] C. Chow, M. Mokbel, and X. Liu, “A peer-to-peer spatial cloaking algorithm for anonymous location-based service,” in Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems, 2006, pp. 171–178.

HYBRID IMAGE RETRIEVAL SYSTEM USING MARKOV CHAIN

T.Usha[#1]

[#]*Student*
Department of Computer Science and Engineering
Regional Centre of Anna University
Tirunelveli (T.N) India
[1]ushaselvi07@gmail.com

***Abstract*— Efficient access to ever growing image collection becomes Keystone in image retrieval. This hybrid image retrieval system is to improve the process of finding the desired image by query as a text or image. The probablistic approach based Markov chain used to find the relation between the image by their keywords and the features of the image. At first the images are retrieved based on the keywords. (i.e)For text query, the Markov chain is constructed based on the keyword relation it quantify the logical connection between keywords. In this project hybrid image retrieval is proposed. To improve the image retrieval process. So for image query, the Markov chain is constructed by the feature extraction value of the image. This feature extraction, consider the image colour histogram and texture value of the image. So the image retrieval process is improved by considering both of the visual and textual features of the image on the Markov chain.**

***Keywords*— *Text-Based Image Retrieval, Content-Based Image Retrieval, Color Moments, Markov chain, Hierarchical clustering*.**

I. INTRODUCTION

Image retrieval techniques are divided into two text-based and content-based categories. In text-based algorithms, some special words like keywords are used. Keywords and annotations should be assigned to each image, when each image is stored in a database. The annotation operation is time consuming and tedious. In addition, it is subjective. Furthermore, the annotations are sometimes incomplete and it is possible that some image features may not be mentioned in annotations . To overcome on mentioned limitation, Content-Based Image Retrieval (CBIR) techniques have been proposed. In a CBIR system, images are automatically indexed by their visual contents through extracted low-level features, such as shape, texture, color, size However, extracting all visual features of an image is a difficult task and there is a problem namely semantic gap in the semantic gap, presenting high-level visual concepts using low-level visual concept is very hard. In order to alleviate these limitations, some researchers use both techniques together using different features. This combination improves the performance compared to each technique separately .a ground truth standard image dataset. The rate of the accuracy of the proposed system has been improved in comparison to text-based and content-based methods. This paper is organized as follows. the next session focuses on the related works in the field. In section 3, content-based image retrieval systems have been explained. In section 4, the combination technique has been explained. Section5 presents the implementation and experimental results and finally, in section 6, the conclusions have been presented.

II. RELATED WORK

In the some systems, a content-based approach is combined with a text-based approach. As an example Blobworld system, automatically segments each image into regions, which correspond to objects or parts of objects in an image. In this system, users can view the results of the segmentation of both the query image and the returned results highlighting how the segmented features have influenced the retrieval results [2]. QBIC system supports queries based on example images. The visual features used in the system include color, texture, and shape. In this system, color was represented using a k-bin color histogram and the texture was described by an improved tamura texture the visual features [3]. In the Visual SEEK, a system uses two content-based and text-based queries. The system uses color and texture visual features. The color feature is represented by color set, texture based on wavelet transform, and spatial relationship between image regions. A binary tree was used to index the feature vectors [4]. Chabot uses a relational database management system called postgres, which supports search through a combination of text and color [5] and Photobook, computes features vectors for the image characteristics, which are then compared to compute a distance measure utilizing one of the systems matching algorithms, including euclidean, mahalanobis, divergence, vector space angle, histogram, Fourier peak, wavelet tree

distances and user-defined matching algorithms via dynamic code loading [6].

In [7], a system has presented a combination of text-based and content-based algorithms. For text retrieval, the Apache Lucene engine has been used and for content-based retrieval, images have been segmented to different areas and regions and histogram has calculated for each section.

III. THE PROPOSED SYSTEM

Annotation-Based Image Retrieval (ABIR) systems are an attempt to incorporate more efficient semantic content into both text-based queries and image captions.[1]Markov chain is a probabilistic approach for annotation based image retrieval. In this approach Markov chain is constructed based on keyword of the image, for quantify the logical connection between the keywords. It fully explore the correlation between the label of image. Hybrid image retrieval system is proposed to improve the image retrieval process. Because the image retrieval is based on CBIR only means it is fail to meet a users need due to the semantic gap.So in hybrid system the Markov chain is constructed for visual as well as textual features.Visual feature is based on the image colour, texture and edge of the image. Textual feature based on image keywords.

IV .Hybrid image retrieval system using markov chain:

Image retrieval

In hybrid image retrieval systems query based image retrieval (QBIR) as well as content based image retrieval both are performed. In QBIR users search for images by issuing queries, each query being an ordered set of keywords. then search engine are semantically refined, responds with a list of images. The user can download or ignore the returned images and issue a new query instead. In this process of image retrieval the system perform simply the keyword matching.so it does not perform the better image retrieval because it will retrieve images randomly.In CBIR, users Search for images by giving query as a image based on colour,texture,edge of the query image the system will retrieve the image .

b) Construction of Aggregate Markov chain for textual features

Keyword probability distribution:

The user implicitly relates retrieved images to query by assuming markovian chain transitions. If user relates I(i) to query q(i) where keyword k2 follows k1 and this occurs m times then the one step transition probability is being updated P(k1,k2) is being updated using recurrent formula.

$$p_i(k_1,k_2)=\frac{Mp_i(k_1,k_2)+m}{M+m}.$$

This procedure construct a markov chain where each keyword to a state .each time a keyword appears means it's state counter is advanced, if another keyword follows in the same query means their interstate link counter is also advanced.Markov chain for each image will be denoted by ∏(i).

Keyword clustering

User puts certain keywords together in a query implicitly the keywords relative to each other regardless of the images that may or may not be picked by this user. To solve this zero-frequency problem by clustering the keyword space into similar keywords.For this purpose, the Aggregate Markovian Chain is constructed in this step. Aggregate markov chain is constructed by using all the queries asked by all users and the selected images keywords.The purpose of the AMC is to model keyword relevance. Markov kernel will used to cluster the keyword .Kernel of the markov chain is query keywords.

c) Construction of Aggregate Markov chain for visual features

Feaure extraction of image (colour,texture,edge)
Color histogram

The main method of representing color information of images in CBIR systems is through color histograms [8]. A color histogram is a type of bar graph, where each bar represents a particular color of the color space being used. Statistically, a color histogram is a way to approximate the joint probability of the values of the three color channels. The most common form of the histogram is obtained by splitting the range of the data into equally sized bins. Then for each bin, the number the colors of the pixels in an image that fall into each bin are counted and normalized to total points, which gives us the probability of a pixel falling into that bin. One of the main drawbacks of the color histogram is that it does not take into consideration the spatial information of pixels. Thus very different images can be considered similar because they have similar color distributions. An improvement of the color histogram method includes the cumulated color histogram [11], proposed by Stricker and Orengo. Their results demonstrated the advantages of the proposed approach over the conventional color histogram approach. However the approach has the disadvantage that in case of more than one dimensional histograms, there is no clear way to order bins.

Color moments

Color moments are one of the best color describers. Most of the color distribution information is captured by the three low-order Moments. Suppose an image has N and M pixels. The first-order moment (μ) calculates the mean color, the second-order Moment ( ) calculates the standard deviation, and the third-order moment calculates the skewness ( ) of color. These three moments are extracted using the following mathematical formulation [14, 22].

$$\mu-\frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{M}f_{ij}$$

$$\sigma = \left(\frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{M}(f_{ij} - \mu_i)^2\right)^{\frac{1}{2}}$$

$$\theta = \left(\frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{M}(f_{ij} - \mu_i)^3\right)^{\frac{1}{3}}$$

Where fij is the value of pixel in the ith row and jth column of the image.

Texture feature

Texture is an important property in image retrieval and is a regional descriptor in the retrieval process. The texture descriptor provides measures, such as smoothness, coarseness and regularity [13, 17, 18]. Texture description algorithms are divided into some categories, such as structural and statistical. Statistical methods, including Fourier power spectra, co-occurrence matrices, tamura features, word decomposition, Markov random field, fractal model, and filter-based techniques, such as Gabor and wavelet transform, characterize texture by the statistical distribution of the image intensity [16, 20, 21, 22]

Gabor filters

Gabor filters consists of a group of wavelets each of which capturing energy at a specific resolution and orientation. Therefore, Gabor filters are able to capture the local energy of the entire signal or image. The Gabor filter has been widely used to extract image features, especially texture features [18]. Daugman discovered that Gabor filters provide optimal Heisenberg joint resolution in visual space and spatial frequency. For this reason, Gabor filters have been successfully employed in many applications including image coding, texture segmentation, retina identification, document analysis, target detection, fractal dimension measurement, line characterization, edge detection, image representation, and others.

Wavelet Transform

Another multi-resolution approach, wavelet transforms, have been used most widely in many aspects of image processing. A wide range of wavelet-based tools and ideas have been proposed and studied for noise removal from images, image compression, image reconstruction, and image retrieval. The multi-resolution wavelet transform has been employed to retrieve images in [19]. The wavelet features do not achieve high level of retrieval accuracy. Therefore, various methods have been developed to achieve higher level of retrieval accuracy using wavelet transform. Wavelet features computed from discrete wavelet coefficients.

d) Hierarchical clustering:

The hierarchical clustering6 is performed as follows:

1. The *n* images in the database are placed in *n* distinct clusters. These clusters are indexed by {*C*1, *C*2,..., *Cn*}. For the *k*th cluster, the set *Ek* contains all the images contained in that cluster and *Nk* denote the number of images in the cluster.*Ek*={*k*} and *Nk =1* for *k*=1,2,...,*n*.
2. Two clusters *Ck* and *Cl* are picked such that the similarity measure *Sk,l* is the largest. (The similarity measure between two clusters is defined in the following subsection). These two clusters are *merged* into a new cluster *Cn+1*. This reduces thetotal number of unmerged clusters by one. *En+1* is updated to *En+1*={*Ek*U*El*} and *Nn+1* is updated to *Nn+1=Nk+Nl*. Out of the two children of *Cn+1*, one is referred to as the right child *RCn+1=k* and the other as the left child *LCn+1=l*. The similaritymeasures between the new cluster *Cn+1* and all the other unmerged clusters are computed as discussed below.
3. Steps 2 and 3 are repeated until the number of clusters has reduced a required number or the largest similarity measure between clusters has dropped to some lower threshold.mean value of colour,texture is used to construct the Markov chain for visual features.

E .Optimization of Aggregate Markov chain

For text query the AMC (Aggregate Markov Chain) will be used to cluster the keyword space and define explicit relevance links between the keywords by means of this clustering.This clustering task is linked to the convergence characteristics of the AMC chain by evaluating the series

$$F_G(n) = \sum_{k=0}^{n} P_G^k$$

where PG is the AMC kernel. A suitable termination condition stops the series at the desired n where the slow convergence has taken over, but not before the rapid convergence has finished. The value of the determinant of is used as a termination condition since the clusters in the rows of will drop its rank and the determinant will become close to zero.For image query the optimization based on the hierarchical clustering .This is used to find the termination of the Markov chain.

F .Finding MSI distance

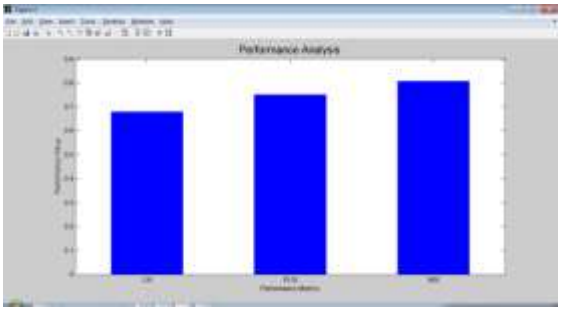
Let x and y two images represented by their respective steady state probability row vectors π_x ,$\pi_y$be the covariance matrix of the zero-mean transpose expected fractional occupancies matrix of theAggregate Markov Chain (AMC), calculated at the desired n. Then the MSI distance between images x and y is defined as

$$d(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{\pi}_x - \boldsymbol{\pi}_y)\Sigma(F_G{}^T)(\boldsymbol{\pi}_x - \boldsymbol{\pi}_y)^T$$
$$= \boldsymbol{\delta}_{xy}\Sigma(F_G{}^T)\boldsymbol{\delta}_{xy}^T,$$

where the dimensionality of and has been extended to that of by filling in with zeros the respective coordinates.

IV. Experimental Results

In this section we present the results of our experiment. Hybrid image retrieval system is proposed to improve the image retrieval process. The relevant images are retrieved using markov chain approach. By constructing the markov chain model images are retrieved with deeper dependencies of user satisfaction . To improve the image retrieval process by considering visual features as well as textual features of the image on the markov chain . Finally, to observe the performance the image retrieval it better reflect the user preferences and satisfaction.



System	Ground Truth Images	Precision vs Recall
Markovchain for textual features	90%	0.83
Hybrid image retrievalsystem using markov chain	90%	0.88

Conclusion

Hybrid image retrieval system is to improve the image retrieval process by Markov chain approach.In this approach the markov chain is constructed for visual features as well as textual features .By combining both features of the image ,it improve the image retrieval process..Because the image retrieval is based on CBIR only means it is fail to meet a users need due to the semantic gap .So in hybrid system the Markov chain is constructed for visual as well as textual features. Visual feature is based on the image colour, texture and edge of the image. Textual feature based on image keywords.This image retrieval is better reflect user preferences and satisfaction. It achieve better precision Vs recall compared to the existing system.

References

[1] Mining User Queries with Markov Chains:Application to Online Image Retrieval
Konstantinos A. Raftopoulos, Member, IEEE, Klimis S. Ntalianis, Dionyssios D. Sourlas, and Stefanos D. Kollias, Member.

[2] Belongie, S., Carson, C., Greenspan, H. and Malik, J. (1998). Color And Texture-Based Image Segmentation Using Em and Its Application To Content-Based Image Retrieval, In Processing of 6th International Conference on Computer Vision.

[3] Flickner, M., Sawhney, H., Niblack, W. and Yanker, p. (1995). Query By Image And Video Content: The Qbic System. Computer. 23–32.

[4] Smith, J. R. and Chang, S. (1996). Visual seek: A Fully Automated Contentbased Image Query System. In Processing of 4th Acm International Conference on Multimedia. 211–218.

[5] Virginia, E. and Stonebraker, M. (2005). Chabot: Retrieval from a relational database of images. IEEE Computer. 28(9), 40-48.

[6] Pentland, A., Picard, R. W. and Sclaroff, S. (1994). Photobook: Contentbased Manipulation of Image Databases, In Spie Storage And Retrieval Image and Video Databases. 2185, 34-47.

[7] Demerdash, O., Kosseim, L. and Bergler, S (2008). CLaC at ImageCLEFphoto 2008, ImageCLEF Working Notes.

[8] Andrysiak, T. and Chora´S, M. (2005). Image Retrieval Based on Heirarchical Gabor Filter. International Journal on Applied Mathematics and Computer Science. 15, 471–480.

[9] Choras, R. (2007). Image Feature Extraction Techniques And Their Application For Cbir and Biometrics System, International Journal of Biology And Biomedical Engineering, 1, 6-16.

[10] Akoushideh, A. and Shahbahrami, A. (2010). Accelerating Texture Features Extraction Algorithms using FPGA Architecture. International Conference on ReConFigurable Computing and FPGAs. 232-237.

[8] Swain, M. J. and Ballard, D. H. 1991. Color indexing. International Journal of Computer Vision. 7(1), 11–32.

[9] Rui, Y., Huang, T. S., and Chang, S.-F. 1999. Image retrieval: Current techniques, promising directions, and open issues. Journal of Visual Communication and Image Representation. 10(1), 39–62.

[10] Long, F., Zhang, H. J. and Feng, D. D. 2003. Fundamentals of Content-based Image Retrieval. Multimedia Information Retrieval and Management. D. Feng Eds, Springer.

AVOIDANCE OF JAMMING ATTACKS IN WIRELESS NETWORK

S.Vidhya[1]
First year M.E student[1,] Department of computer science and engineering
[1] Renganayagi varatharaj college of engineering, Sivakasi.
[1]vidhyanila@gmail.com

Abstract-Wireless medium are very vulnerable to intentional interference attacks, typically referred to as jamming. This intentional interference with wireless transmissions can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks. Jamming attacks can be divided into two types,external threat model and internal threat model. External threat model is vastly studied in literature. Adversaries with internal knowledge of protocol specifications and network secrets have been considered in this work. This type of adversaries can launch low-effort jamming attacks that are difficult to detect and counter. The selective jamming attacks can be launched by performing real-time packet classification at the physical layer. The problem of selective jamming attacks in wireless networks is considered. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. To mitigate these attacks, three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes are proposed. They are A Strong Hiding Commitment Scheme,Hiding Based On Cryptographic Puzzles,An AONT-based Hiding Scheme. The security of our methods and evaluate their computational and communication overhead.

Keywords—Selective Jamming, Denial-of-Service, Wireless Networks, Packet Classification.

I. INTRODUCTION

The objective of our project is to mitigate the attacks in real time packet classification using cryptographic puzzle scheme. To check the feasibility of realtime packet classification for launching selective jamming attacks, under an internal threat model. Such attacks are relatively easy to actualize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes.

This project is about uninterrupted availability of the wireless medium is availed to wireless networks to interconnect participating nodes. Wireless networks are highly vulnerable to multiple security threats. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. In the proposed system, internal threat model is consider. Under Jamming attacks, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses.

Three schemes have been developed that prevent classification of transmitted packets in real time. These schemes rely on the joint consideration of cryptographic mechanisms with PHY-layer attributes.

II. EXISTING SYSTEM:

Jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of highpower interference signals.

Anti-jamming techniques rely extensively on spread-spectrum (SS) communications, or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats). SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to

the communicating parties. These methods can only protect wireless transmissions under the external threat model.

Always-on strategy has the continuous presence of unusually high interference levels makes this type of attacks easy to detect

DRAWBACKS:

- Jamming attacks under internal threat model is not considered.
- Always-on strategy has disadvantages such as, first the adversary has to expend a significant amount of energy to jam frequency bands of interest.

III. PROPOSED SYSTEM:

In proposed system, the problem of jamming under an internal threat model has been considered. Adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack has been designed. The adversary exploits the internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. A jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow.

Modules:

- Adversary Design
- Real Time Packet Classification
- A Strong Hiding Commitment Scheme
- Cryptographic Puzzle Hiding Scheme
- Hiding Based On All-Or-Nothing Transformations

Adversary Design:

Adversary is in control of the communication medium and can jam messages at any part of the network of his choosing. The adversary can operate in full-duplex mode, thus being able to receive and transmit simultaneously. When the adversary is introduced, the data packets from the node cannot be reached at receiver.

Real Time Packet Classification:

At the Physical layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinterleaved and decoded to recover the original packet m. Nodes A and B communicate via a wireless link. Within the communication range of both A and B there is a jamming node J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B.

A Strong Hiding Commitment Scheme:

A strong hiding commitment scheme, which is based on symmetric cryptography. First, S (Sender) constructs commit(message) the commitment function is an off-the-shelf symmetric encryption algorithm is a publicly known permutation, and k is a randomly selected key of some desired key length s The committed value m is the packet that S wants to communicate to R. To transmit m, the sender computes the corresponding commitment/decommitment pair (C, d), and broadcasts C. The hiding property ensures that m is not revealed during the transmission of C. To reveal m, the sender releases the decommitment value d, in which case m is obtained by all receivers, including J.

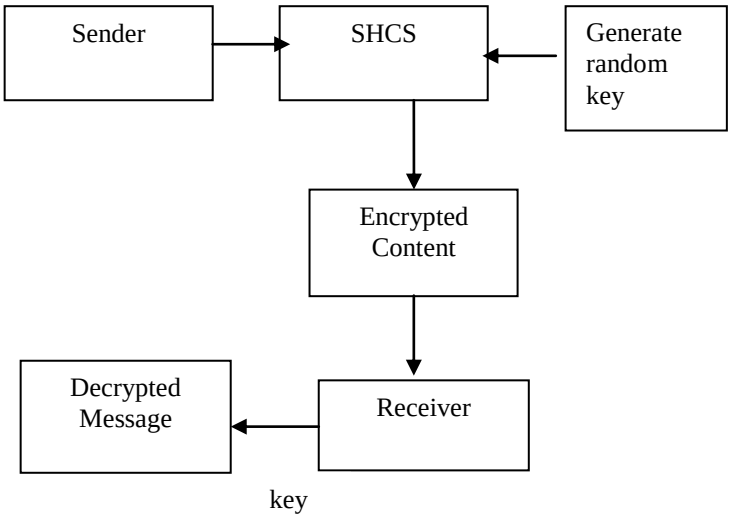


Figure 1: Strong Hiding Commitment Scheme

Cryptographic Puzzle Scheme:

A sender S have a packet m for transmission. The sender selects a random key k , of a desired length. S generates a puzzle (key, time), where puzzle() denotes the puzzle generator function, and tp denotes the time required for the solution of the puzzle. Parameter is measured in units of time, and it is directly dependent on the assumed computational capability of the adversary, denoted by N and measured in computational operations per second.After generating the puzzle P, the sender broadcasts (C, P). At the receiver side, any receiver R solves the received puzzle to recover key and then computes the packet. Server to solve the puzzle in time tp and solved puzzle should be correct get the data packet at server.

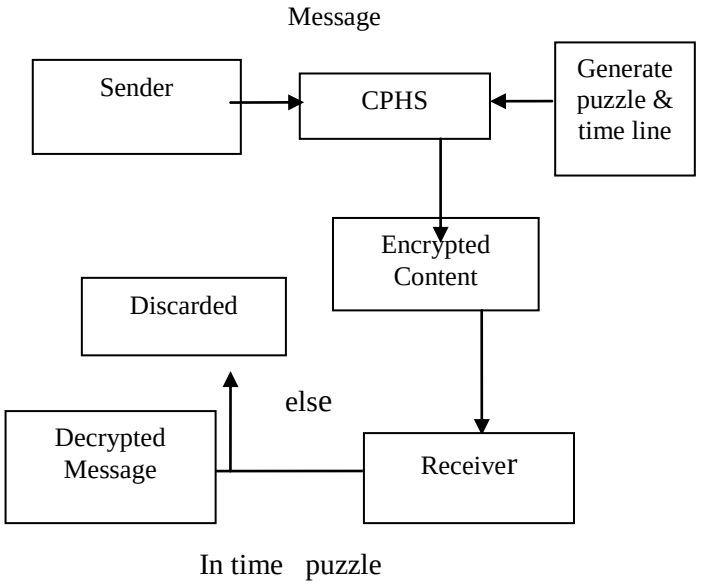


Figure 2: Cryptographic Puzzle Scheme

All or Nothing Transformation Scheme:

The packets are pre-processed by an AONT before transmission but remain unencrypted. The jammer cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied. Packet m is partitioned to a set of x input blocks m = {m1, m2,m3….},which serve as an input to an The set of pseudo-messages m = {m1, m2,m3,…..} is transmitted over the wireless medium.

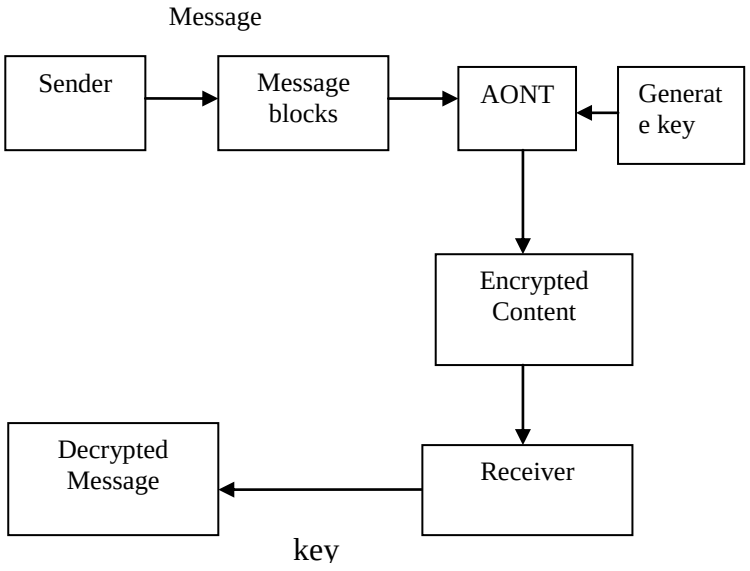


Figure 3: All or Nothing Transformations

IV. IMPLEMENTATION

The system design is targeted towards the implementation of the project. This project is implemented using JAVA.

In this application, to implement Sender and Receiver model. Java Swing for designing GUI is used. To develop a application, which could be deployed in network, where sender can send data to receiver and receiver receives the data in secure manner. To study preventive Jamming attacks under three special cases such as All Or Noting Transformations, Cryptographic Puzzles, Strong Hiding Commitment Schemes. In this work, one receiver, one intermediate node, which is assumed to be the attacker under two cases block and unblock.

When a sender wants to send a data to receiver, sender hides the data and sends in secure manner. There are four techniques used to for hiding the data, which are Strong hiding Commitment Scheme, Cryptography puzzle based

hiding scheme, All or nothing based scheme & Normal Node. An attacker module is designed to show the impact of data jamming. The message hiding technique is followed to send data by avoiding jamming attack.

V. RESULT:

The result of this project is that the User Interface will be viewed when the user runs the java application. In the result, observed that packets are sent from sender to receiver by preventing the attacks.

The proposed system overcomes the key disadvantage of the existing system. It uses internal threat model in the wireless network**.**

VI. CONCLUSION:

In this paper, the Selective jamming attacks in wireless networks have been studied. Then showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. Then evaluated the impact of selective jamming attacks on network protocols such as TCP and routing. Three schemes have been proposed that transform a selective jammer to a random one by preventing real-time packet classification. The schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations (AONTs) with physical layer characteristics.

VI. REFERENCES

1. T. X. Brown, J. E. James, and A. Sethi(2006). "Jamming and sensing of encrypted wireless ad hoc networks". In Proceedings of MobiHoc, pages 120–130.

2. M. Cagalj, S. Capkun, and J.-P. Hubaux(2007). " Wormhole- based antijamming techniques in sensor networks". IEEE Transactions on Mobile Computing, 6(1):100–114.

3. Wenyuan Xu, Wade Trappe, Yanyong Zhang "The feasibility of launching and detecting jamming attacks in wireless networks "Rutgers University, 73 Brett Rd., Piscataway, NJ 08854.

4. T. Dempsey, G. Sahin, Y. Morton, and C. Hopper(2009). "Intelligent sensing and classification in ad hoc networks" a case study. Aerospace and Electronic Systems Magazine, IEEE, 24(8):23–30.

5. A.Chan, X. Liu, G. Noubir, and B. Thapa(2007)."Control channel jamming: Resilience and identification of traitors". In Proceedings of ISIT.

LOCATION AWARE SERVICES USING PROXY APPROACH IN MOBILE ENVIRONMENT

T.Punnaivanathal @ Revathy[1],
PG Scholar, SCAD Engineering College,
Tirunelveli.
Email:revathy1404@gmail.com

C.Karpagavalli[2],
Assistant professor SCAD Engineering College
Tirunelveli.

ABSTRACT

In Mobile environment client submits queries to server and waits for server answer. Server process the clients query and cache the valid regions to reduce the number of queries submitted by the client. In the previous approaches the client wait for long time for the server to compute the valid region. To reduce server load this paper provides an agent, the intermediate between client and server. This Proxy creates EVR and answers the queries without communicating server. Proxy maintains object cache and provide answers to both window and nearest neighbor queries. This paper proposed the algorithms to create EVR fast and efficiently than previous proposed methods.

Indexed terms: Mobile environment, valid region, Proxy, object cache and estimated valid region.

1.INTRODUCTION

Data mining has attracted a great deal of attention in the information industry and in society as a whole in recent years. Wide availability of huge amounts of data and the imminent need for turning such data into useful information an knowledge. Data mining can be viewed as a result of the natural evolution of information technology. Data mining is defined as finding hidden information in a database alternatively it has been called exploratory data analysis, data driven discovery and deductive learning. The tasks of data mining are classification, prediction, estimation and clustering.

Location aware applications deliver online content to users based on their physical location. Various technologies employ GPS, cell phone infrastructure, or wireless access points to identify where electronic devices such as mobile phones or laptops are, and users can choose to share that information with location-aware applications. Those applications can then provide users with resources such as a "you are here" marker on a city map, reviews for restaurants in the area, a nap alarm that's triggered by your specific stop on a commuter train, or notices about nearby bottlenecks in traffic. Applications might also report a user's location to friends in a social network, prompting those nearby to meet for coffee or dinner. While such applications create a highly targeted marketing opportunity for retailers, they also provide increased social connectivity and enhanced environmental awareness, offering users a location-based filter for online information.

Location-aware services is an important application in mobile environment. Spatial queries is one of the most important LASs. Spatial queries can be divided into several categories including Nearest Neighbor (NN) queries and window queries. An NN query is to find the nearest data object with respect to the location at which the query is issued (referred to as the query location of the NN query). For example, a user may launch an NN query like "show the nearest coffee shop with respect to my current location ". On

the other hand, a window query is to find all the objects within a specific window frame. An example window query is “show all restaurants in my car navigation window”.

In Mobile environment clients submit queries to server and wait for server response. Two approaches are used to answer the queries:

i)Server based approach

ii)Proxy based approach

In Server based approach client sends query to the server directly. Server processes the query submitted by the client and produces the query result to the client. This method is suitable if the number of queries submitted by the client is high. When the number of queries increases then query processing time of the server is also increased i.e. the burden of the server increases. Then the client have to wait for longer time to get query result.

In Proxy Based approach, a proxy, an intermediate device is located between client and server. Here Client sends the query to server via proxy. Proxy stores the result of the queries which are answered by the server previously. When the client submits continuous queries then proxy provides answer to the queries without consulting server. So the server load is reduced by this method. Object cache is maintained by the proxy to store the information about result object.

2. SYSTEM ARCHITECTURE

The proposed system architecture for NN and window query processing shown in figure . The system architecture consists of three parts: 1) the LBS server, 2) proxies, and 3) the mobile clients. The LBS server is responsible for managing static data objects and answering the spatial queries submitted by the proxies.

The LBS server is assumed not to provide VRs. Each of the deployed proxies supervises one service area and provides EVRs of NN queries and EWVs (vector form of EVRs) of window queries for mobile clients in the service area. Each base station serves as an intermediate relay for queries and query results between mobile clients and the associated proxy. Base stations, proxies, and the LBS server are connected by a wired network. A mobile client maintains a cache to store the query results and the corresponding EVRs. When a mobile client has a spatial query, the mobile device first examines whether the current location is in the EVR of the stored result. If so, the stored result remains valid and the mobile device directly shows it to the client. Otherwise, the mobile device submits the query, which is received and then forwarded by the base station, to the proxy. For the received query, the proxy will return the query result as well as the corresponding EVR to the client.

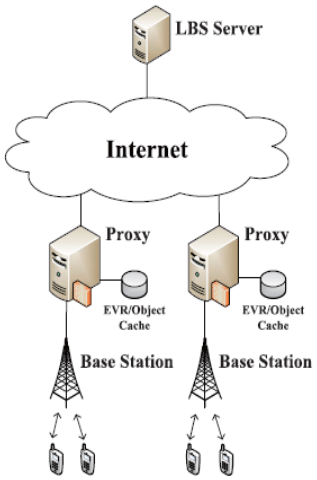


Fig. 2. System architecture.

3. PROXY DESIGN

A proxy builds EVRs of NN queries and EWVs of window queries based on NN query history and available data objects, respectively. The proxy maintains an object cache and two index structures: an EVR-tree for NN queries and a grid index for window queries, as illustrated in Fig. 3. The two index structures share the data objects in the object cache. The EVR-tree is an R-tree (or its variants) composed of EVRs where each EVR is wrapped in a minimum bounding box (MBR). An EVR consists of the region vertices with respect to a data object and a pointer to the corresponding object entry in the object cache. When an NN query point q is located in an EVR of the EVR-tree, the proxy retrieves the corresponding object from the object cache to answer the query.

On the other hand, the service area is divided into m x n grid cells managed by the grid index. Grid cells are classified into two categories: fully cached cells and uncached cells. All grid cells are initialized to uncached. The proxy marks a cell as fully cached when all the objects within the cell are received. The corresponding grid index entry of a fully cached cell caches the object pointers to the associated object entries in the object cache. The purpose of fully cached and uncached cells is to realize the stored object distribution, enabling the proxy to create EWVs of window queries effectively. When receiving a window query, the proxy obtains the result and creates the corresponding EWV by retrieving stored objects in the surrounding fully cached cells. Although the EVR-tree and the grid index are designed for NN and window queries respectively, these two index structures mutually support each other.

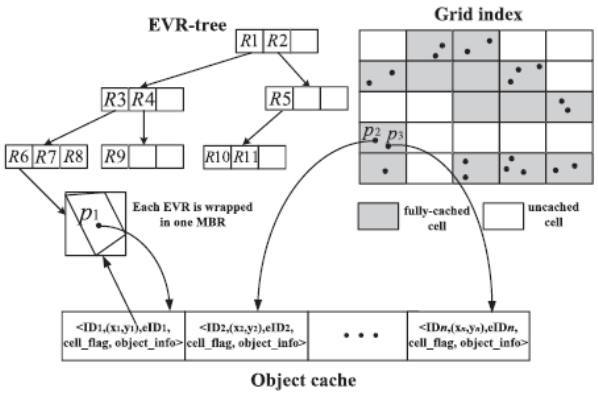


Fig. 3. Object cache, EVR-tree, and grid index.

4. QUERY PROCESSING

4.1. EVR TREE and GRID INDEX

The proxy maintains an object cache and two index structures: an EVR-tree for NN queries and a grid index for window queries. The two index structures share the data objects in the object cache. The EVR-tree is an R-tree composed of EVRs where each EVR is wrapped in a minimum bounding box (MBR). An EVR consists of the region vertices with respect to a data object and a pointer to the corresponding object entry in the object cache. When an NN query point is located in an EVR of the EVR-tree, the proxy retrieves the corresponding object from the object cache to answer the query.

On the other hand, the service area is divided into m x n grid cells managed by the grid index. Grid cells are classified into two categories: fully cached cells and uncached cells. All grid cells are initialized to uncached. The proxy marks a cell as fully cached when all the objects within the cell are received. The corresponding grid index entry of a fully cached cell caches the object pointers to the associated object entries in the object cache. The purpose of fully cached and uncached cells is to realize the stored object distribution, enabling the proxy to create EWVs of window queries effectively.

4.2. EVR CREATION FOR NN QUERIES

In mobile environment more clients submits their queries to the server for processing. Then server provides valid region for the client queries to reduce the number of queries submitted by the clients. Here proxy creates estimated valid regions (EVRs), which are the subregions of the corresponding VRs, for the clients. With the proxy architecture, the clients still can enjoy the benefits of EVRs even if the LBS server does not provide VRs. EVR is created by using EVR_creation algorithm.

4.3. EVR EXTENSION

The proxy provides answer to the NN spatial queries based on the created EVR. When client submits the query to proxy via base station the proxy checks whether the data object presents in the current EVR of the EVR tree in object cache. If the object is not in the current EVR then proxy sends the query to the LBS server.

The LBS server then process the query and provides the appropriate answer tho the proxy. After receiving the result from the server, proxy calculates the distance of the object from the current EVR. Based on the calculated value proxy determines how much the window size should be extended. Then proxy extends the EVR based on the EVR_extension

algorithm. The results of the queries are then updated in the object cache maintained by the proxy.

4.4. EWV CREATION

Estimated Window Vector (EWV) is the representation of EVR in the window form, which achieves larger EVRs. In the previous approaches EVR is created in the polygon shape. The polygon shaped EVRs are extremely small and ineffective. To overcome the drawbacks of polygon shaped EVRs, this paper proposed the data objects indexed by grid index and EVR representation in the form of vectors. Here the window created is in the rectangle shape, to estimate the valid regions. Due to rectangle shape, the EWV can be set effectively.

The EWV is created based on two conditions. 1) all answer objects must remain valid within the estimated window region and 2) no outer objects will be encountered when searching the objects in the window region. The data objects outside the query window are called outer objects.

4.5.EXTENSION TO RANGE QUERIES

The proposed approach is able to support range queries whose query region is circular. To resolve a range query, the main idea is to transform the range query to a window query and then address the window query with the window query processing algorithm.

After transforming the range queries in the form of window query, the proxy checks if the object present in the current EWV region of grid index. If the query result is not present in the object cache, the proxy submits the new window query to request the required answer objects from the LBS server. After receiving the result from the LBS server, the proxy extends the window region and updates the grid index with new values.

CONCLUSION:

This paper Creates EVR fast and more effective for NN queries and also creates EWV for window queries even cache size is small. For NN queries EVR creation algorithm is used to create EVR and EVR Extension algorithm is used for EVR extension. For Window queries EWV creation algorithm is used to create EWV. Extension to range queries algorithm is used for EMV extension. These algorithms provide mutual support between NN and window query . So the performance of objects at high moving speed is enhanced. Proxy produces query answers quickly.

REFERENCES:

[1] B. Zheng and D.L. Lee, "Processing Location-Dependent Queries in a Multi-Cell Wireless Environment," Proc. Second ACM Int'l Workshop Data Eng. for Wireless and Mobile Access, 2001.

[2]. D. Lee, B. Zheng, and W.-C. Lee, "Data Management in Location-Dependent Information Services," IEEE Pervasive Computing, vol. 1, no. 3, pp. 65-72, July-Sept. 2002.

[3]. B. Zheng, J. Xu, and D.L. Lee, "Cache Invalidation and Replacement Strategies for Location-Dependent Data in Mobile Environments," IEEE Trans. Computers, vol. 15, no. 10, pp. 1141-1153, Oct. 2002.

[4].J. Zhang, M. Zhu, D. Papadias, Y. Tao, and D.L. Lee, "Location-Based Spatial Queries," Proc. ACM SIGMOD Int'l Conf. Management of Data, pp. 443-454, 2003.

[5]. B. Zheng, J. Xu, W.-C. Lee, and D.L. Lee, "On Semantic Caching and Query Scheduling for Mobile Nearest-Neighbor Search," Wireless Networks, vol. 10, no. 6, pp. 653-664, Dec. 2004.

[6]. X. Yu, K.Q. Pu, and N. Koudas, "Monitoring k-Nearest Neighbor Queries over Moving Objects," Proc. 21st Int'l Conf. Data Eng., pp. 631-642, 2005.

[7]. X. Gao, J. Sustersic, and A.R. Hurson, "Window Query Processing with Proxy Cache," Proc. Seventh IEEE Int'l Conf. Mobile Data Management, 2006.

[8]. S. Nutanong, R. Zhang, E. Tanin, and L. Kulik, "The V - Diagram: A Query-Dependent Method for Moving kNN Queries," Proc. VLDB Conf., pp. 1095-1106, 2008.

[9]. K.C.K. Lee, W.-C. Lee, H.V. Leong, B. Unger, and B. Zheng, "Efficient Valid Scope for Location-Dependent Spatial Queries inMobile Environments," J. Software, vol. 5, no. 2, pp. 133-145, Feb.2010.

UNITIAL DESIGN BASED KEY PRE-DISTRIBUTION SCHEME FOR WIRELESS SENSOR NETWORKS

SUBA.S
PG Scholar
Infant Jesus College of Engineering
Thoothukudi
Email: Suba.msu@gmail.com

R.Jasmine Sugitha
Assistant Professor
Infant Jesus College of Engineering
Thoothukudi
Email:sugi.smile56@gmail.com

***ABSTRACT*-Given the sensitivity of the potential applications of wireless sensor networks, security emerges as a challenging issue in these networks. Because of the resource limitations, symmetric key establishment is one favorite paradigm for securing WSN. One of the main concerns when designing a key management scheme for WSN is the network scalability. In this paper, new highly scalable key establishment scheme was proposed for WSN. For that purpose, we make use, for the first time, of the unital design theory. The basic mapping from unitals to pair wise key establishment allows to achieve an extremely high network scalability while degrading, however, the key sharing probability. An enhanced unital-based pre-distribution approach was proposed which provides high network scalability and good key sharing probability. The obtained results show that our approach enhances considerably the network scalability while providing good overall performances. Our solutions reduce significantly the storage overhead at equal network size compared to existing solutions.**

Index Terms—Wireless sensor networks, security, key management, network scalability, resource optimization.

I. INTRODUCTION

Nowadays, wireless sensor networks (WSN) are increasingly used in numerous fields such as military, medical and industrial sectors; they are more and more involved in several sensitive applications which require sophisticated security services [1]. Due to the resource limitations, existing security solutions for conventional networks could not be used in WSN. So, the security issues became then one of the main challenges for the resource constrained environment of WSN.

The establishment of secure links between nodes is then a challenging problem in WSN. The public key based solutions, which provide efficient key management services in conventional are unsuitable for WSN because of resource limitations. Some public key schemes have been implemented on real sensors [2][3][4], however most researchers believe that these techniques are still too heavyweight over actual sensors' technology because they induce an important communication and computation overhead [5]. Symmetric key establishment is then one of the most suitable paradigms for securing exchanges in WSN.

In this Paper we are interested in particular in the scalability of symmetric key pre-distribution schemes. Existing research works either allow supporting a low number a nodes or degrading the other network performances including resiliency, connectivity and storage overhead when the number of nodes is important**.** In contrast to these solutions, our goal is to enhance the scalability of WSN key management schemes without degrading significantly the other network performances. To achieve this goal, we propose to use, for the first time, the unital design to construct and pre-distribute key rings. First, we explain the unital design and we propose a basic mapping from unitals to key pre-distribution for WSN.

Analytic calculations that the resulting basic scheme allows to achieve extremely high network scalability while degrading, however, the key sharing probability.

For this, we propose an enhanced unital-based construction in order to maintain a good key sharing probability while enhancing the network scalability. We carried out analytic calculations and simulations to compare the efficiency of the enhanced proposed approach against basic schemes with respect to important performance criteria: storage overhead, network scalability, session key sharing probability and average secure path length. The obtained results show that at equal key ring size, our approach enhances considerably the network scalability while providing good overall performances. Moreover, we show that given a network size, our solutions reduce significantly the key ring size and then the storage overhead compared to existing solutions.

The remainder of this paper is organized as follows We define in section 2 the metrics used to evaluate and compare key pre-distribution schemes and we summarize the used symbols. Section 3 presents some related works. We give in section 4 a background on

unital design while we present, in section 5, the basic mapping to key pre distribution and analyze the performances of the resulting scheme. In section 6, we present the enhanced unital-based construction. In section 7, we evaluate the performances of the enhanced scheme and compare it to the existing ones with respect to various performance criteria; we provide and discuss theoretical and simulation results. Finally, section 8 ends up this paper with some conclusions and future works.

II. RELATED WORKS

Key management problem in WSN has been extensively studied in the literature and several solutions have been proposed. Many classifications of existing symmetric key management schemes can be found in [6][7][8]. Eschenauer and Gligor proposed in [9] the basic Random Key Pre-distribution scheme denoted by RKP. In this scheme, each node is pre-loaded with a key ring of k keys randomly selected from a large pool S of keys. After the deployment step, each node exchanges with each of its neighbors the list of key identifiers that it maintains in order to identify the common keys. If two neighbors share at least one key, they establish a secure link and compute their session secret key which is one of the common keys. Otherwise, if neighboring nodes do not have common keys, they should determine secure paths which are composed of successive secure links. This basic approach is CPU and energy efficient but it requires a large memory space to store the key ring. Moreover, if the network nodes are progressively corrupted, the attacker may discover a large part or the whole global key pool. Hence, a great number of links will be compromised.

Chan et al. proposed in [10] the Q-composite scheme which enhances the resilience of RKP. In this solution, two neighboring nodes can establish a secure link only if they share at least Q keys. The pair wise session key is calculated as the hash of all shared keys concatenated to each other. This approach enhances the resilience against node capture attacks because the attacker needs more overlap keys to break a secure link. However, this approach degrades the probability of session key sharing neighboring nodes must have at least Q common keys to establish a secure link.

Chan et al. proposed also in [10] a perfect secure pair wise key pre-distribution scheme where they assign to each possible link between two nodes i and j a distinct key ki,j. Prior to deployment, each node is pre-loaded with p*n keys, where n is the network size and p is the desired secure coverage probability. Hence, the probability that the key ki,j belongs to the key set of the node i is p. Since we use distinct keys to secure each pair wise link, the resiliency against node capture is perfect and any node. that is captured reveals no information about links that are not directly connected to it. The main drawback of this scheme is the non scalability because the number of the stored keys depends linearly on the network size. In addition, this solution does not allow the node post-deployment because existing nodes do not have the new nodes' keys.

Du et al. proposed in an enhanced random scheme assuming the node deployment knowledge. Nodes are organized in regional groups to which is assigned different key pools and each node selects its k keys from the corresponding key pool. The key pools are constructed in such a way that neighboring ones share more keys while pools far away from each other share fewer keys. This approach allows to enhance the probability of sharing common keys because the key pools become smaller. Moreover, the network resiliency is improved since if some nodes of a given region are captured, the attacker could discover only a part of the corresponding group key pool. However, the application of this scheme is restrictive since the deployment knowledge of a WSN is not always possible.

Liu and Ning proposed a new pool based polynomial pre-distribution scheme for WSN. This approach can be considered as an extension of the basic RKP scheme where nodes are pre-loaded with bivariate polynomials instead of keys. A global pool of symmetric bivariate polynomials is generated off-line and each node is preloaded with a subset of polynomials. If two neighboring nodes share a common polynomial, they establish a direct secure by computing the polynomial value at the neighbor identifier; else, they try to find a multi-hop secure path. This approach allows computing distinct secret keys, so the resilience against node capture is enhanced. However, it requires more memory to store the polynomials and induces more computational overhead. Yu and Guan [14] used the Blom's scheme to key pre-distribution in group-based WSN.

Liu et al. proposed in SBK, a self-configuring key establishment scheme for WSN. SBK distinguishes two kinds of nodes: service nodes and worker ones. After the deployment, sensor nodes differentiate their role thanks to a pre-loaded bootsrap program. Service nodes generate a key space using a polynomial-based or the matrix-based model. Then, they distribute the corresponding keying shares to at most worker nodes. Authors propose for that to use a computationally asymmetric channel based on Rabins public key cryptosystem while shifting the large amount of computation overhead to the service nodes. This induces a high load on service nodes which are sacrificed. SBK assumes that all nodes are deployed at the same time

and that they are coarsely time synchronized to to start the bootstrapping procedure simultaneously. it assumes also that the network is secured and no active attacks can be launched during the bootstrapping procedure. SBK gives good performances including scalability, resilience and connectivity between worker nodes as far as the assumptions are verified.Deterministic key pre-distribution schemes ensure that each node is able to establish a pair-wise key with all its neighbors.

LEAP makes use of a common transitory key which is preloaded into all nodes prior to deployment of the WSN. The transitory key is used to generate pairwise session keys and is cleared from the memory of nodes by the end of a short time interval after their deployment. LEAP is based on the assumption that a sensor node, after its deployment, is secure during a time T_{min} and cannot be compromised during this period of time. LEAP is then secure as far as this assumption is verified.

In new key management scheme for grid group WSN. Intra-region secure communications are guaranteed thanks to a SBIBD key pre-distribution while inter-region communications are ensured by special nodes called agents. Furthermore, authors propose to enhance the Camtepe scheme in order to avoid key identifier exchanges. For that, they index all nodes and keys and propose a mapping between node indexes and key indexes.

The main strength of the proposed scheme is the establishment of unique secret pairwise keys between connected nodes. However, this does not ensure a perfect network resilience. Indeed, the attacker may construct a part of the global set of keys and then compute pairwise secret keys used to secure external links where the compromised node are not involved. Moreover, the proposed scheme provides a low session key sharing probability which does not exceed 0.25 in the best case as we prove later. Another drawback of this solution is the network scalability which reaches only 2q2 = O(k2) where k is the key ring size.

We focus in this work on the scalability of key management schemes for WSN. Basic schemes giving a perfect network resilience [10] achieve a network scalability of O(k) where k is the key ring size. Design based schemes as the SBIBD and the trade based ones allow to achieve a network scalability of O(k2). So, large scale networks cannot be supported because the key ring size may be increased which is not suitable due to memory constraints in WSN. In this work we propose new solutions achieving a network scalability of O(k4) when providing good overall performances. For this purpose, we make use, for the first time, of the unital design in order to predistribute keys. We show that the basic use of unital design enhances considerably the scalability of key pre-distribution while decreasing the probability of sharing common keys. we propose a solution which ensures high network scalability while maintaining a good probability of sharing common keys.

.

III. A BASIC MAPPING FROM UNITALS TO KEY PRE-DISTRIBUTION FOR WIRELESS SENSOR NETWORK

At the best of our knowledge, we are the first who propose the use of unital design for pre-distribution in WSN. This scheme may also be generalized to all resource constrained wireless networks where key pre-distribution should be useful. In this section, develop a naive and scalable key pre-distribution scheme based on unital design. We propose a basic mapping in which we associate to each point of the unital a distinct key, to the global set of points the key pool and to each block a node key ring. We can then generate from a global key pool of $|S| = m^3 + 1$ keys, $n = b = m^2 (m^3 + 1)/(m+ 1)$ key rings of $k = m + 1$ keys each one.

TABLE I
MAPPING FROM UNITAL DESIGN TO KEY DISTRIBUTION

UNITAL DESIGN	KEY DISTRIBUTION
X: Point Set	S : Key Pool
Blocks	Key Rings($<KR_i>$)
Size of the Object Set X : $V=m^3+1$	Size of the Key Pool S: $\|S\| = m^3+1$
Number Of Generated Blocks : $b=m^2(m^2-m+1)$	Number Of Generated Key rings : $n=m^2(m^2-m+1)$

After the deployment step, each two neighboring nodes exchange their key identifiers in order to determine eventual common key. Using this basic approach, each two nodes share at most one common key. Indeed, referring to the unital properties, each pair of keys is contained together in exactly one block which implies that two blocks cannot share more than one point. Hence, if two neighboring nodes share one common key, the latter is used as a pairwise key to secure the link; otherwise, nodes should determine secure paths which are composed of successive secure links.

A. Storage Overhead

When using the proposed naive unital based version matching a unital of order m, each node is pre-loaded

with one key ring corresponding to one block from the design. Hence, each node is pre-loaded with (m+1) disjoint keys. The memory required to store keys is then $l \times (m + 1)$ where l is the key size.

B. Network Scalability

From construction, the total number of possible key rings when using the naive unital based scheme is $n = m^2 \times (m^2 - m + 1)$, this is then the maximum number of supported nodes.

C. Session Key Sharing Probability

When using the basic unital mapping, we know that each key is used in exactly m2 key rings among the $m^2 \times (m^2 - m + 1)$ possible key rings. Let us consider two nodes u and v randomly selected. The node u is preloaded with a key ring KRu of m+1 different keys. Each of them is contained in $m^2 - 1$ other key rings. Knowing that each two keys occur together in exactly one block, we find that the blocks containing two different keys of KRu are completely disjoint. Hence, each node shares exactly one key with $(m + 1) \times (m^2 - 1)$ nodes among the $m^2(m^2 - m + 1) - 1$ other possible nodes, Then, the probability Pc of sharing a common key is of them is contained in $m^2 - 1$ other key rings. Knowing that each two keys occur together in exactly one block, we find that the blocks containing two different keys of KRu are completely disjoint. Hence, each node shares exactly one key with $(m + 1) \times (m^2 - 1)$ nodes among the $m^2(m^2 - m + 1) - 1$ other possible nodes, Then, the probability Pc of sharing a common key is :

$$P_c = \frac{(m+1)^2}{m^3+m+1}$$

D. Summary and Discussion

The evaluation of this naive solution shows clearly that the basic mapping from unitals to key pre-distribution improves greatly the network scalability which reaches O(k4) compared to other schemes like SBIBD and trade ones having a scalability of O(k2) where k is the key ring size. Moreover, given a network size n this naive scheme allows to reduce the key ring size up to $\sqrt[4]{n}$. However, this naïve solution degrades the key sharing probability which tends to O(1/k). In order to improve the key sharing probability of the naive unital based scheme while maintaining a good scalability improvement, we propose in the next section an enhanced construction for key management schemes based on unital design.

IV. A NEW SCALABLE UNITAL-BASED KEY PRE-DISTRIBUTION SCHEME FOR WSN

In this section, we present a new enhanced unital-based key pre-distribution scheme for WSN. In order to enhance the key sharing probability while maintaining high network scalability, we propose to build blocks using unital design and to pre-load each node with a number of blocks picked in a selective way. Before the deployment step, we propose to generate blocks of a m order unital design, each block matches a key set. We propose then to pre-load each node with t completely disjoint blocks, t is then a protocol parameter that we will discuss later. The aim of our construction is to enhance the key sharing probability between neighboring nodes and then decrease the average secure path length as we show later. We propose in algorithm 1 a random block
distribution allowing to pre-load t disjoint blocks in each sensor node.

Step 1: Generate $B = <B_q>$, Key Sets
corresponding to Blocks of a Unital
Design of order m
Step 2: for each $Node_i$ do
Step 3: $KR_i = \{\}$
Step 4: while $(KR_i \leq t(m+1))$ do
Step 5: pick B_q from B
Step 6: if $(KRi \cap B_q) =$ □ then
Step 7: $KR_i = KR_i \cup B_q$
Step 8: $B = B\text{-}B_q$
Step 9: end

Algorithm 1: A random approach of unital block pre- distribution in the enhanced unital-based scheme

After the deployment step, each two neighbors exchange their key identifiers in order to determine common keys. Contrary to the basic approach, each two nodes may share more than one key when using the proposed construction. Indeed, each node is pre-loaded with t disjoint blocks which mean that each two nodes share up to t2 keys. If two nodes share one or more keys, we propose to compute the pair wise secret key as the hash of all their common keys concatenated to each other. The used hash function may be *SHA-1* [24] for instance. This approach allows enhancing the network resiliency since the attacker needs more overlap keys to break a secure link. Otherwise, when neighbors do not share any key, they should find a secure path composed of successive secure links. The major advantage of this enhanced version is the improvement of the key sharing probability. As we will show later, this approach allows to achieve a high secure connectivity coverage since

each node is pre-loaded with t disjoint blocks. Moreover, this approach increases resiliency through the composite pairwise secret keys witch reinforce secure links. In addition, we show that we maintain high network scalability compared to existing solutions although it remains lower than that of the naive version.

V. CONCLUSION

In this paper, a new highly scalable key pre-distribution scheme for WSN. We make use, for the first time, of the unital design theory. We showed that a basic mapping from unitals to key pre-distribution allows to achieve an extremely high network scalability while degrading the key sharing probability. We proposed then an enhanced unital-based construction which gives birth to a new key management scheme providing high network scalability and good key sharing probability. We conducted analytic calculation and intensive simulations to compare our solutions to existing ones which showed that our approach enhances significantly the network scalability when providing good overall performances. As future work, we plan to deepen the analysis of our parameter choice in order to suggest values given the best tradeoff. In addition, we attend to analyze more network performances of our solution like the network resilience against node capture attacks.

REFERENCES

[1] B. Maala, Y. Challal, and A. Bouabdallah, "Hero: Hierarchcal Key Management Protocol for Heterogeneous WSN," in Proceedings IFIP WSAN,pp.125-136,2008

[2] C. Castelluccia and A. Spognardi, "A Robust Key Pre-Distribution Protocol for multi-phase Wireless Sensor Networks," in Proc. 2007 IEEE Securecom, pp. 351–360.

[3] D. Liu and P. Ning, "Establishing Pair Wise Keys in Distributed Sensor Networks," in Proc. 2003 ACM CCS, pp. 52–61.

[4] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," in IEEE SP, pp. 197–213, 2003.

[5] S. A. C¸ Amtepe and B. Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks," IEEE/ACM Trans. Netw., vol. 15, pp.346–358, 2007.

[6] S. Ruj and B. Roy, "Key predistribution using combinatorial designs for grid-group deployment scheme in wireless sensor networks," ACM Trans. Sensor Netw., vol. 6, no. 4, pp. 1–4:28, Jan. 2010.

[7] S. Zhu, S. Setia, and S. Jajodia, "Leap: efficient security mechanisms for large-scale distributed sensor networks," in Proc. 2003 ACM CCS, pp. 62–72.

[8] T. Choi, H. B. Acharya, and M. G. Gouda, "The best keying protocol for sensor networks," in Proc. 2011 IEEE WOWMOM, pp. 1–6.

[9] W. Bechkit, Y. Challal, and A. Bouabdallah, "A new scalable key predistribution scheme for WSN," in Proc. 2012 IEEE ICCCN, pp. 1–7.

[10] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in Proc. 2004 IEEE INFOCOM, pp. 586–597.

A NOVEL CROSS LAYERED ENERGY EFFICIENT ROUTING

A Wireless network Based Scheme

A. Sivalakshmanan
Department of Computer Science and Engineering
Jerusalem College of Engineering
Chennai, Tamilnadu, India
Siva.swerocker@gmail.com

B. Jaishanthi
Department of Computer Science and Engineering
Jerusalem College of Engineering
Chennai, Tamilnadu, India

***Abstract*— MANET is the Mobile Ad-Hoc network in which the mobile nodes are self configured, self administered and self organizing. The characteristic of the MANETS are multi-hop routing, limited power, dynamic topology, distributed operations and light weight terminals. Routing is the process of providing path between the source and destination for the packet delivery, there are 3 types of routing available they are proactive, reactive and hybrid routing. The Optimal stopping rule algorithm is implemented in DSDV protocol provides a particular timeslot for packet transfer to takes place. We propose cross layer design in AODV protocol. In a cross layer design the control over two layers or more layers can yield a significant performance improvement. In this each node maintain a routing table and which includes the routing information and energy of nodes. Based upon the energy information of nodes the packet transfer takes place between nodes. The energy information provided is used by MAC layer and Network layer. This cross layer technique using AODV protocol is implemented and evaluated and compared with simple AODV protocol using NS2 simulator. Result has been revealed that the performance behavior of using cross layer design in AODV protocol has been significantly improved.**

***Index Terms*—DSDV protocol, Optimal stopping rule algorithm, AODV routing protocol and Cross layer.**

I. INTRODUCTION

Mobile adhoc network (MANET) is a network in which the nodes are self-configuring, self-organizing and self-administered. The nodes forming a temporary/short lived network without any fixed infrastructure where all nodes are free to move about arbitrary. Nodes must behave as a routers, take part of discovery and maintenance of routes to other nodes in the network. [2] Wireless links in MANETS are highly error prone and can go down frequently due to mobility of nodes. Stable routing is a very critical in dynamic environment in mobile Ad-hoc Network [3].

So mobile ad-hoc network (MANET) is a self-configuring network of mobile router (and associated host) connected by wireless link – the union of which form a random topology. The routers are free to move randomly and organize themselves at random

Such network may operate in a standalone fashion, or may be connected and quick deployment make suitable for emergency situation like natural or human induced disasters, military conflicts, emergency medical situation.[4]

The rest of paper is organized as follows. In section 2 and section 3 provides a brief description about routing protocols and cross layer design. In section 4 the existing work is described in area of energy efficient routing is described. Section 5 provides a brief description of AODV protocol. Section 6 and 7 provides a detailed description of energy estimation and implementation of cross layer design.

II. ROUTING PROTOCOL IN MANET

A routing protocol is used to transmit a packet to a destination via number of nodes and numerous routing protocols have been proposed for such kind of ad-hoc network. These protocols find a route for packet delivery and to the correct destination. The routing protocols can be broadly classified into three types as:

A. Proactive protocols

In proactive routing protocol, each node maintain routing information to every other node (or nodes located in specific part) in the network. Different table usually maintain routing information. These tables maintained are periodically updated and/or if the network topology changes. The protocols in proactive are differentiated in way with routing information is maintained. Furthermore, each routing protocol may maintain different number of tables. The advantage is that routes will always be available on request.

B. Reactive protocols

On-demand routing protocols were designed to reduce the overheads in proactive protocols by maintaining information for active routes only. The routes are determined and

maintained for nodes that require sending data to a particular destination. Route discovery usually occurs by forwarding a route request packets through the network. When a node with a route to destination (or the destination itself) is reached a route reply is sent back to the source node using through bi-directional links. Therefore, the route discovery overhead will grow by 0(N+M).

C. Hybrid protocols

In hybrid protocols are a new type of protocol, which are both proactive and reactive in nature. These protocols provide scalability by allowing nodes with close proximity to work together to form some sort of backbone to reduce route discovery overheads. This is achieved mostly by proactively maintaining routes to nearby nodes and determining routes to far away nodes using a route discovery strategy. Most hybrids projected are zone based mostly, which suggests that the network is divided or seen as variety of zones by every node.

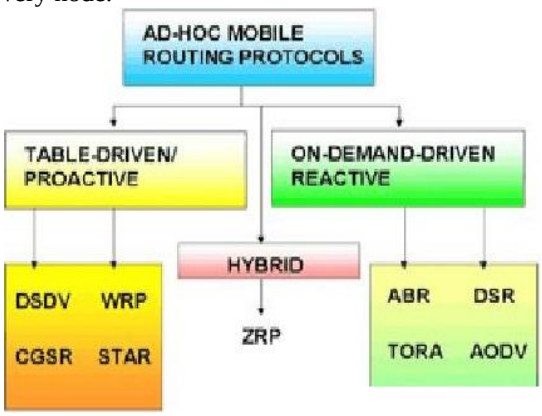


Fig. 1. Ad-Hoc Routing protocols

III. CROSS LAYER DEIGN

Wireless networks represent technologies with growing interest and exceptions within the world of communications. This projected new challenges within the style of communication protocol, which are required to adapt to new feature of the networking environment like shared channels, limited bandwidth, high error rates, increased latency, and mobility.

Traditionally, protocol architectures follow strict layering principles, which provide an attractive tool for designing interoperable system for fast deployment and efficient implementation of OSI model was developed to support standardization of network architecture using the layers model. A protocol at a given layer is implemented by a (software, firmware, or hardware) entity, which communicates with other entities (on other networked systems) implementing the same protocol using protocol data unit. Due to lack of coordination among layers limited the performance of such architectures in front of the peculiar challenges posed by wireless nature of the transmission links. To overcome such limitations, cross layer design was proposed. The core idea is to maintain functionalities associated to the original layers but to allow coordination, integration and joint optimization of protocols crossing different layers.

The cross layer is the information sharing between layers in order to obtain highest possible adaptively. The operation between the multiple layers to combine the resources and create a network that is highly adaptive .this cross layer allows the upper layer to adapt the strategy to varying link and network condition. Each layer characterized with same parameter they are passed to adjacent layer to help them to determine the best operation modes that best suits channel, network and application.

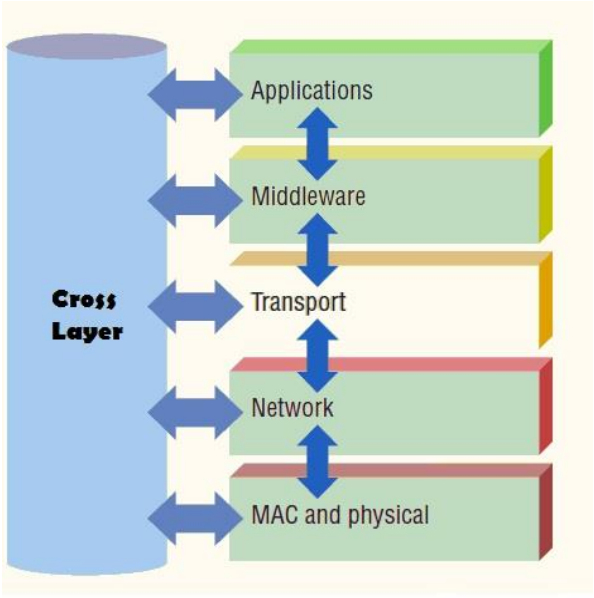


Fig. 2. Cross layer design

IV. RELATED WORK

Shirali *et.al.* [7] propose a schemes to sleep based topology called cluster based energy conservation algorithm in this algorithm each nodes broadcast a discovery message with node ID and estimated lifetime. After a while the node that has longest lifetime among its neighbors, declares itself as a cluster-head. Each node that is not a cluster head and has received cluster-head messages from more than one cluster-head, declares itself as a gateway node. The node except the cluster-head go to sleep mode to save more energy and this techniques can be implemented over non stationary nodes. M.Grossglauser *et.al.* [8] there are n nodes if a source is in need of providing a packets transfer to destination node, single hop routing may not be possible with nodes, if the nodes cannot directly communicate with destination node then communication is provided via intermediate nodes. The mobility of nodes is increased with relay nodes this usage of relay nodes pose the major drawback of providing an not efficient end to end data transfer. P. Bellavista *et.al.* [9] proposed Mobeyes techniques used in VANET for urban environment. The node sense the event i.e. capturing image, process sensed data i.e. capturing license plate and route

messages to other vehicles. The mobile collector node harvests the data and the mobile monitor node sense the data in vehicles. This technique poses drawback of increase of nodes with the increase in harvesting information. Flooding takes place with the nodes. Piyusha Gupta *et.al.* [10] for 'n' identical randomly located nodes, each capable of transmitting at W bits per second and from a wireless network. Every node all over the domain to share whatever portion of the channel its utilizing with nodes in its local neighborhood that is reason for constriction in capacity. Splitting channel and accessing via spatial directivity in antenna. The drawback posed is nodes must be less, due to mobility of node link failure and delays will be more. P. R. Kumar *et.al.* [11] for ad hoc network and hybrid network nodes are close to each other, the common power level adopted, with n nodes, the saptio temporal scheduling of transmission and their ranges. The nodes perform power control for transmission the appropriate choice of power level for communication is chossed. This scales better with multihop hybrid wireless network. This poses a major drawback while providing single hop packet transfer. G. B. Giannakis *et.al.* [12] Scheduling plays an important role in providing quality of service support to multimedia communications in various kinds of wireless sensor networks. The AMC and priority scheduler algorithm is proposed, Adaptive modulator coding provides a maximum transmission rate by adjusting transmission modes and priority scheduler assign a channel based upon channel quality, connection with highest priority is scheduled each time. The channel having low priority will not be scheduled. Dharma *et.al.* [13] propose a Directional routing protocol provides a cross layer interaction between the MAC layer and routing. The main feature of DRP includes an efficient route discovering, establishing and maintaining directional routing and neighborhood table. This DRP is implemented over the top of existing MAC layer. Directional routing table is updated with the routes travelled by packets and Directional neighborhood table is implemented in MAC layer updated using packets. The drawback posed by DRP is the reception of more redundant packets and routing is not energy efficient.

V. SELECTION OF PROTOCOL: AODV

The table driven routing protocols have the advantage of having an available route always ready to the destination. But it comes with cost of consuming a big part of overhead. Thus an appropriate routing protocol for MANET s should imply a reasonable overhead. On the other hand, the reactive routing protocols reduce the overhead traffic by creating a route only when it is required. When a route is no longer used in reactive protocol, it is simply expunged from the routing table.

Considering the aforesaid fact Ad Hoc On-Demand Distance Vector (AODV) routing protocol is selected for improving performance.

Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol uses an on-demand approach for finding routes. As a result, a route is established only when it is required by a source node for transmitting data packets. The destination sequence number is used to identify the most recent path. The source node and the intermediate node store the next hop information to each flow for data packet transmission. In AODV, each routing table entry contains the following information:

- Destination
- Next hop
- Number of hops
- Destination sequence number
- Active neighbors for this route
- Expiration time for the route table entry

Expiration time, also called lifetime, is reset each time the route has been used. The new expiration time is the sum of the current time and a parameter called active route timeout.

These AODV protocol terminologies are active routes i.e. the route toward the destination that has the routing table entry is marked as valid, destinations the address to which the packet is forwarded, forwarding node i.e. the node sends the data packets destined for another node, forward route is the route setup to send the data packets, originating node is a node that initiates a route discovery message, reverse route is a route setup to forward RREP packets and sequence number is the monotonically increasing number maintained by each node to determine freshness of the information contained from the originating node.

The AODV protocol message formats are

- Route request message
- Route reply message
- Route error message

A. Route request message

A node disseminates a RREQ when it determines that it needs a route to destination and does not have one available. Before forwarding RREQ, the originating node buffers the RREQ ID and the Originator IP address. The destination sequence number field in route request message is last known destination sequence number for this destination and is copied from the destination sequence number field in the routing table. The originator sequence number in the RREQ message is node's own sequence number. RREQ ID field is incremented by one from the last RREQ ID used by current node. The originating node should not generate more than RREQ_RATE LIMIT RREQ messages per second. After forwarding a RREQ, a node waits for RREP. If the route is not received within NET-TRAVESAL-TIME milliseconds, the node may try again to discover a route by forwarding another RREQ. When the node receives the RREQ, it creates or updates a route to the previous hop. Hop count of RREQ ID incremented. The originator sequence number from RREQ is updated while forwarding.

B. Route reply message

A node generates RREP if it is a destination. When generating a RREP message, a node copies the destination IP address and the originator sequence number form the RREQ message into the corresponding fields in RREP message. The RREP is forwarded back toward the node which originated the

RREQ message, hop count field is incremented by one at each hop. If the node generating RREP is an intermediate node then it copies its own sequence number for the destination into the destination sequence number field in RREP message. The neighbour node updates the forward route entry by placing the last hop node into the precursor list for the forward route entry. The life time field of RREP is calculated by subtracting the current time from the expiration time in its route table entry.

C. Route error message

The Route Error message is initiated in three situation if it detect link break for the next hop of an active route in its routing table, if it gets a data packet destined to a node for which it does not have an active route and if it receives a RERR from a neighbor for one or more active routes. The node first generates the list of unreachable destination consisting of unreachable neighbor as the next hop. Some of unreachable destination in the list could be used by neighbor nodes, and it may necessary to send a new RERR. The neighbor node(s) that should receive the RERR are all those that belong to a precursor list of at least one of unreachable destination(s) in the newly created RERR. Just before transmitting RERR, certain updates are made on routing table.

VI. ENERGY ESTIMATION

The recent research in energy efficient routing protocols for ad hoc network. We classify the power efficient routing protocols into four categories based on their path selection schemes. The first set of protocols use the energy cost for transmission as the cost for transmission as the cost metric and aim to save energy consumption per packet. However, such protocols do not take the nodes energy capacity into account. Thus energy is not fair among nodes in network. The second set protocols use the remaining energy capacity as the cost metric, which means that the fairness of energy consumption becomes the main focus. But, these protocols cannot guarantee the energy consumption is minimized. The third set of protocol are similar to second set, but use estimated lifetime instead of node energy capacity as the route selection criteria.

One of the key challenges in deployment of mobile adhoc networks is how to prolong the lifetime of networks. The lifetime of adhoc network is limited by the battery energy in wireless devices. Energy depletion of nodes can interrupt communication and even worse, cause network portioning. Thus energy efficiency is critical for the design of network protocols.

In order to both minimize the energy consumption per packet and maximize the network lifetime, several protocol are proposed in recent research.[15] A cross layer design for AODV protocol is proposed for providing energy efficient routing over nodes. This scheme has two steps, first the discovery of all possible routes during the route discovery phase and for each node remaining energy is found with cross layer implementation.

The energy of node is estimated with the use of transmission power and reception power, some amount of time is consumed for the transmission or the reception of packet.

$$dEng = P\_tx * txtime. \quad (1)$$

The energy consumed for sending the packet is the product of energy to be consumed for each transmission and the time estimated for transmitting the packets.

$$dEng = P\_rcv * rcvtime. \quad (2)$$

The energy consumed for reception of the packet is the product of energy to be consumed for each reception and the time estimated for receiving the packets.

$$energy = energy - dEng. \quad (3)$$

The remaining energy of the nodes is the reduction of energy for the transmission or the reception of packet form the initial energy. The initial energy of the node is the amount of energy that is available before particular transmission or reception of packets.

VII. IMPLEMENTATION OF CROSS LAYER DESIGN

The remaining energy of the node has been estimated with the transmission and the reception of each packet. The energy information must be forwarded to neighbor node to provide the energy based routing. The AODV protocol uses the RREQ packet for the route discovery process, energy information about the nodes are embedded with RREQ and forwarded to the neighbor nodes. Each node in the network maintain a routing table this table is usually used for providing routing information to forward the data packets. In the proposed scheme the routing table used will also include the additional information i.e. remaining energy of node(s).

Cross layer design can be realized between multiple layers or between just two layers. The cross layer design can be based in any combination of two protocol layers. Interestingly merging multiple protocol layers is not just a theoretical concept but has been seriously considered in real time practice. For example the upcoming routing protocol is being developed as on of the critical module in the MAC layer. Such as merge between routing and MAC layer provides a great potential to carry out optimization between MAC and routing within the same protocol layer.

A routing protocol of multihop wireless network determines path for any packet from its source to destination. In its simplest form, a routing protocol can just consider connectivity between nodes, i.e., as long as route can be maintained, a routing path is set up. However to enhance performance, other routing metrics and mechanism must be taken into account. For example, a routing protocol may need to consider minimum hop count, lowest traffic load, etc. however, such type of layered design approaches are still suboptimal in performance. The reason is that the behavior of MAC protocol taken into account. Thus, no matter how the

routing protocol is optimized. If underlying MAC does not provide satisfying performance, then the overall performance perceived by the protocol can be poor.

A MAC protocol aims to provide medium access opportunity to nodes sharing the same medium, given any condition of traffic load, interference, noise, and topology of network. However, traffic load, interference, and so on are closely related to a routing protocol. Thus performance of a MAC protocol can be significantly impacted by routing protocol.

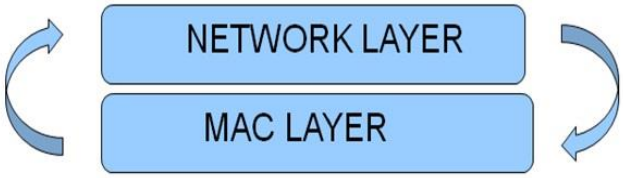


Fig. 3. Cross Layer Design for MAC and Network Layer

In order to achieve the best network performance, routing and MAC must be jointly optimized. The Routing/MAC cross layer can be done in a simple loosely coupled scheme. The routing table maintains the energy information of the neighbor nodes. The MAC compares the remaining energy of neighbor nodes maintained with a threshold value. The less energy node address is forwarded to the network layer, the network layer removes the less energy node form the route toward destination.

VIII. PERFORMANCE EVALUATION

In this section our simulation effort presented to evaluate and compare the performance of the protocols that we described previously in section

A. Simulation scenario

We implemented our programs based on the NS2. Recently NS2 has been the predominant simulator in wireless communication researches. In order to evaluate the performance of the protocols as the networks size scale up, each experiment was carried out on the square simulation fields of three different scales of mobile nodes. 20 nodes were chosen to represent ad hoc network. Nodes were generated at random time as if few nodes were entering into the topology. Nodes were moving at constant random speed. Radio propagation model was used was two Ray Ground. Antenna model used was Omni Antenna. Movement was linear and node speed was constant for a simulation.

B. Node Characteristics

1. Link layer Type : Logical link type(LL)
2. MAC type : 802_11
3. Queue type :Drop-Tail
4. Network interface type : Wireless
5. Channel type : Wireless

C. Performance Metrics :

The following performance are evaluated :

1. Packet delivery ratio : The ratio of the data packets delivered to the destinations to those generated by CBR sources. The ratio between the number of packets originated by the “application layer” CBR sources and number of packets received by the CBR sink at final destination.

2. Average end to end delay : This includes all possible delays caused by buffering during route discovery latency, queuing at interface queue, delays during retransmission at MAC, and propagation and transfer times.

3. Throughput : This denote the number of packets from source that a destination receives in time slot.

IX. CONCLUSION

In this research paper, an effort was made to provide Cross layer design for AODV protocol provides a energy efficient routing among nodes in networks. This proposed scheme poses major advantage of using only the node having higher energy in the route towards destination. The delay will be reduced, throughput is increased and packet delivery ratio is increased. Finally simulation result shows that cross layer implementation over AODV protocol is more efficient.

X. ACKNOWLEDGMENT

I would like to express my sincere gratitude to my guide Mrs. B. Jaishanthi, Senior Assistant Professor, Department of Computer Science and Engineering, for her guidance, constant encouragement and support. Her extensive vision and creative thinking has been a source of inspiration for me since this time.

XI. REFERENCE

[1] Spyridon Vassilaras, Gregory S.younof, Shortest route mobility assited packet delivery with soft maximum delay gaurentees in MANETS.

[2] Vijay kumar1 and Ashwani kush.”A New scheme for secured on demand routing” IISTE Network and complex systems ,Vol 2, No.2, 2012.IISN 2224-610X(paper), 2225-0603 (Online).

[3] Sunil Taneja &Ashwani kush”Perfomance evaluation of DSR and AODV over UDP and TCp connections” International Journal of computing and bussiness Research (IJCBR), Volume 1, No. 1December . 2010.

[4] Donatas Sumyla, Moble Ad-Hoc Networks, 03/20/2006. Available. http://ecom.umfk.mane.edu/MMobile%20Ad.pdf

[5] Keneth Holter, “Wireless Extension to OSPF: Implementation of the overlapping relays prposal”, Master

thesis , Department of Infrmatcs, University of Oslo, Norway, 2nd May.

[6] S. Corson & J. Macker "Mobile Ad hoc networking: Routing protocol perfomance issue and evaluation consideration ", RFC 2501, Oct. 1999.

[7] Mina Shirali, Nasrin Shirali, Mohammed Reza Neybodi "Sleep based Topology control in Adhoc Network by using fitness aware learning automata".

[8] A. Agarwal, P. R. Kumar, "Capacity bounds for ad-hoc and hybrid wireless networks", ACM SIGCOMM Computer communcation Review 34 (3) (2004) 71-81. Special issue on science of networking design.

[9] M. Grossglauser , D. Tse, Moblity increase the capacity capacity of ad-hoc network, in: proc. IEEE INFOCOM 1360-1369, 2001.

[10] U. Lee, B. Zhou, M. Gerla, E. Magistretti, P. Bellavista, A. Corradi, Mobeyes: smart mobs for urban monitoring with a vehicular sensor network, IEEE Wireless Communications 13 (5) (2006) 52–57.

[11] P. Gupta, P. R. Kumar, "The capacity of wireless network", IEEE Transaction on informatonal theory 46 (2) (2000) 388-404

[12] Qingwen Liu, Xin Wang, "Cross layer scheduling algorithm with QOS support in wireless network", IEEE transaction on vechcilar technology, Vol. 55. No. 3. May 2006.

[13] Dharma p. Agarwal, Tarun Joshi, "A ross layer approach for desgning DRP in MANETS"

[14] Ljuan Cao, Teresa ahlberg, Yu Wang " Prefomance evaluation of energy effcient ad hoc routng protcol".

HANDOVER BASED NOVEL CHANNEL ADAPTIVE ROUTING IN MANETs

R.Sobana Devi
P.G.Scholar,Computer Science and Engineering
Renganayagi Varatharaj College Of Engineering
sobanasekar@gmail.com

Abstract— Radio link fluctuations is a difficult task in packet transmission in mobile ad hoc networks. To overcome this we are proposing a new protocol called novel channel adaptive routing protocol which reduces channel fading. The proposed channel used to select stable links for route discovery by using average non fading duration technique and handoff strategy maintains reliable connections. This protocol provides a dual-attack for avoiding unnecessary route discoveries, predicting path failure leading to handoff and then bringing paths back into play when they are again available, rather than simply discarding them at the first sign of a fade.

Keywords- Mobile ad hoc networks, Average non-fading duration, Routing protocols, Channel adaptive routing.

1 INTRODUCTION

An ad hoc network is a mobile, multi-hop wireless network with no stationary infrastructure. The autonomous and self-configuring nature of ad hoc networks provide several advantages such as fast and easy deployment, little or no reliance on a pre-existing infrastructure and cost-effectiveness. Until recently, ad-hoc networks found application mainly in the military and emergency management. A significant amount of current research has been directed to designing efficient dynamic routing protocols for ad hoc networks. The challenge here is to reduce routing overheads in spite of the changing topology. This is a critical issue as both link bandwidth and battery power are premium resources. Several new protocols focused on the issue of overhead reduction without compromising on application-visible performance metrics.

A mobile ad-hoc network or MANET is a collection of mobile nodes sharing a wireless channel without any centralized control or established communication backbone. They have no fixed routers with all nodes capable of movement and arbitrarily dynamic. These nodes can act as both end systems and routers at the same time. When acting as routers, they discover and maintain routes to other nodes in the network. The topology of the ad-hoc network depends on the transmission power of the nodes and the location of the mobile nodes, which may change from time to time levels. One of the main problems in ad-hoc networking is the efficient delivery of data packets to the mobile nodes where the topology is not pre-determined nor does the network have centralized control. Hence, due to the frequently changing topology, routing in ad-hoc networks can be viewed as a challenge. In cellular telecommunications, the term handover or handoff refers to the process of transferring an ongoing call or data session from one channel connected to the core network to another. In any mobile phone conversation your call is passed from one cell to another in order to keep the signal strong. This process of handing the call from one cell to another is called a handoff (or handover in some countries). It is *how* this transfer takes place that defines the difference between soft and hard.

Routing protocols for ad hoc networks can be classified broadly as either proactive, reactive, or hybrid (combining both behaviors).In table-driven or proactive routing protocols, consistent and up-to-date routing information of the network topology of all nodes is maintained at each node with respect to the time. The major drawback of these approaches is that the maintenance of unused paths may occupy an important part of the available bandwidth if the topology changes frequently. In on-demand or reactive routing protocols, the routes are created on requirement basis. To find a path from source to destination, it invokes the route discovery mechanisms. Reactive routing protocols have some inherent limitations. First, since routes are only maintained while in use, it is usually required to perform a route discovery before packets can be exchanged between communication peers. This leads to a delay for the first packet to be transmitted. Second, even though route maintenance for reactive algorithms

is restricted to the routes currently in use, it may still generate an important amount of network traffic when the topology of the network changes frequently. Finally, packets to the destination are likely to be lost if the route to the destination changes.

Many MANET routing protocols exploit multihop paths to route packets. The probability of successful packet transmission on a path is dependent on the reliability of the wireless channel on each hop. Ad-hoc On-demand Vector Routing (AODV) is a reactive protocol that discovers routes on an as needed basis using a route discovery mechanism. It uses traditional routing tables with one entry per destination..Ad-hoc On-demand Multipath Distance Vector Routing (AOMDV) protocol is an extension to the AODV protocol for computing multiple loop-free and link-disjoint paths. The mobile node which is move from one base station to another at that time only the signal fading happened. We call this protocol Channel-Aware AOMDV (CA-AOMDV). Note that this protocol is intended to improve on AOMDV in conditions where the channel can be reasonably allowed for. CA-AOMDV protocol used to avoid signal fading. This protocol use specific, timely, channel quality information allowing us to work with the ebb-and-flow of path avail-ability. This approach allows reuse of paths which become unavailable for a time, rather than simply regarding them as useless, upon failure, and discarding them. We utilize the channel average non fading duration (ANFD) as a measure of link stability, combined with the traditional hop-count measure for path selection. The average fading duration (AFD) is utilized to determine when to bring a path back into play, allowing for the varying nature of path usability instead of discarding at initial failure.

2. BACKGROUND

Existing routing protocols in ad-hoc networks utilize the single route that is built for source and destination node pair. Due to node mobility, node failures and the dynamic characteristics of the radio channel, links in a route may become temporarily unavailable, making the route invalid. The overhead of finding alternative routes mounts along with additional packet delivery delay. This problem can be solved by use of multiple paths between source and destination node pairs, where one route can be used as the primary route and the rest as backup.

2.1 AODV

Ad-hoc On-demand Distance Vector Routing (AODV) is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. When a link fails, a routing error is passed back to a transmitting node, and the process repeats. Much of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network. For example, each request for a route has a sequence number. Nodes use this sequence number so that they do not repeat route requests that they have already passed on. Another such feature is that the route requests have a "time to live" number that limits how many times they can be retransmitted. Another such feature is that if a route request fails, another route request may not be sent until twice as much time has passed as the timeout of the previous route request.

The main advantage of this protocol is having routes established on demand and that destination sequence numbers are applied for find the latest route to the destination. The connection setup delay is lower. One disadvantage of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also, multiple Route Reply packets in response to a single Route Request packet can lead to heavy control overhead. Another disadvantage of AODV is unnecessary bandwidth consumption due to periodic beaconing.

2.2 AOMDV

Ad-hoc On-demand Multipath Distance Vector Routing (AOMDV) protocol is an extension to the AODV protocol for computing multiple loop-free and link disjoint paths. The routing entries for each destination contain a list of the next-hops along with the corresponding hop counts. All the next hops have the same sequence number. This helps in keeping track of a route. For each destination, a node maintains the advertised hop count, which is defined as the maximum hop count for all the paths, which is used for sending route advertisements of the destination. Each duplicate

route advertisement received by a node defines an alternate path to the destination. When a route advertisement is received for a destination with a greater sequence number, the next-hop list and the advertised hop count are reinitialized. AOMDV can be used to find node-disjoint or link-disjoint routes. To find node-disjoint routes, each node does not immediately reject duplicate RREQs. Each RREQs arriving via a different neighbor of the source defines a node-disjoint path. This is because nodes cannot be broadcast duplicate RREQs, so any two RREQs arriving at an intermediate node via a different neighbor of the source could not have traversed the same node. In an attempt to get multiple link-disjoint routes, the destination replies to duplicate RREQs, the destination only replies to RREQs arriving via unique neighbors. After the first hop, the RREPs follow the reverse paths, which are node disjoint and thus link-disjoint. The trajectories of each RREP may intersect at an intermediate node, but each takes a different reverse path to the source to ensure link disjointness.

The advantage of using AOMDV is that it allows intermediate nodes to reply to RREQs, while still selecting disjoint paths. But, AOMDV has more message overheads during route discovery due to increased flooding and since it is a multipath routing protocol, the destination replies to the multiple RREQs those results are in longer overhead.

3. CHANNEL AWARE AOMDV

We introduce an enhanced, channel-aware version of the AOMDV routing protocol. The key aspect of this enhancement, which is not addressed in other work, is that we use specific, timely, channel quality information allowing us to work with the ebb-and-flow of path availability. This approach allows reuse of paths which become unavailable for a time, rather than simply regarding them as useless, upon failure, and discarding them.

A. Channel Average Non Fading Duration

We utilize the channel average non fading duration (ANFD) as a measure of link stability, combined with the traditional hop-count measure for path selection. The protocol then uses the same information to predict signal fading and incorporates path handover to avoid unnecessary overhead from a new path discovery process.

B. Average Fading Duration

The average fading duration (AFD) is utilized to determine when to bring a path back into play, allowing for the varying nature of path usability instead of discarding at initial failure. This protocol provides a dual attack for avoiding unnecessary route discoveries, predicting path failure leading to handoff and then bringing paths back into play when they are again available, rather than simply discarding them at the first sign of a fade.

3.1 Route Discovery

As in AODV, when a traffic source needs a route to a destination, the source initiates a route discovery process by generating a RREQ. Since the RREQ is flooded network-wide, a node may receive several copies of the same RREQ. In AODV, only the first copy of the RREQ is used to form reverse paths; the duplicate copies that arrive later are simply discarded. Note that some of these duplicate copies can be gainfully used to form alternate reverse paths. Thus, *all* duplicate copies are examined in CA-AOMDV for potential alternate reverse paths, but reverse paths are formed only using those copies that preserve loop-freedom and disjointness among the resulting set of paths to the source. When an intermediate node obtains a reverse path via a RREQ copy, it checks whether there are one or more valid forward paths to the destination. If so, the node generates a RREP and sends it back to the source along the reverse path; the RREP includes a forward path that was not used in any previous RREPs for this route discovery. In this case, the intermediate node does not propagate the RREQ further. Otherwise, the node re-broadcasts the RREQ copy if it has not previously forwarded any other copy of this RREQ *and* this copy resulted in the formation/updation of a reverse path. When the destination receives RREQ copies, it also forms reverse paths in the same way as intermediate nodes. However, it adopts a somewhat 'looser' policy for generating a RREP. Specifically, the destination generates a RREP in response to every RREQ copy that arrives via a loop-free path to the source even though it forms reverse paths using only RREQ copies that arrive via loop-free *and* disjoint alternate paths to the source. The reason behind the looser RREP generation policy at the destination is as follows. The RREQ flooding mechanism, where each node locally broadcasts a RREQ once, suppresses some RREQ copies at intermediate nodes and duplicates other RREQ copies. When an intermediate node receives a RREP, it follows route update rules form a loop free and disjoint forward path to the destination, if possible; else, the RREP is dropped. Supposing that the intermediate node forms the forward path and has one or more valid reverse paths to the source, it checks if any of those reverse paths was not previously used to send a RREP for this route discovery. If so, it chooses one of those unused reverse paths to forward the current RREP; otherwise, the RREP is

simply dropped. Note that our choice of forwarding the RREP along a unique reverse path, as opposed to duplicating it along all available reverse paths, does not hurt CA-AOMDV route discovery latency. This is because the latency of a route discovery is determined by the amount of time source has to wait before it obtains the *first* route, and RREPs in CA-AOMDV (as with AODV) use fairly reliable ARQ-based unicast MAC layer transmissions. On the contrary, duplicating the RREP will cause a route cutoff problem similar to that mentioned above, reducing the number of disjoint paths found at the source.

3.2 Route Maintenance

Route maintenance in CA-AOMDV is a simple extension to AODV route maintenance. Like AODV, CA-AOMDV also uses RERR packets. A node generates or forward a RERR for a destination when the *last* path to the destination breaks. CA-AOMDV also includes an optimization to *salvage* packets forwarded over failed links by re-forwarding them over alternate paths. This is similar to the packet salvaging mechanism in DSR. The timeout mechanism similarly extends from a single path to multiple paths although the problem of setting proper timeout values is more difficult for CA-AOMDV compared to AODV. With multiple paths, the possibility of paths becoming stale is more likely. But using very small timeout values to avoid stale paths can limit the benefit of using multiple paths. In our experiments, we use a moderate setting of timeout values and additionally use HELLO messages to proactively remove stale routes. Thus, the timeouts in the current version of CA-AOMDV primarily serve as a soft-state mechanism to deal with unforeseen events such as routing table corruption and to a lesser extent for promptly purging stale routes. In another work, we have devised an adaptive timeout selection mechanism for purging stale cached routes in DSR, which can be applied to CA-AOMDV with appropriate modifications. As an alternative, timeout selection can be based on analytical characterization.

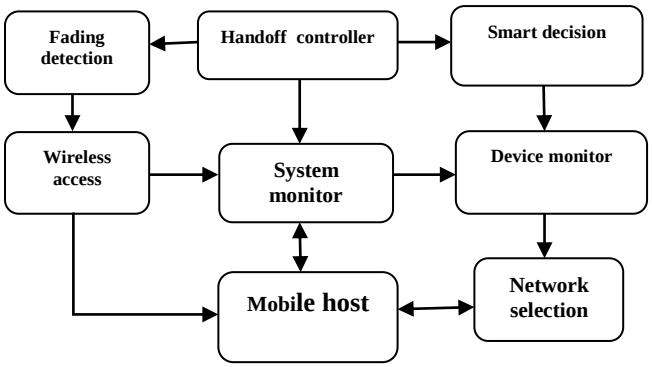


Fig-1: Block diagram of Proposed Technique.

The Fig-1 shows the block diagram of proposed technique which contains ,Fading Detection helps to determine the signal strength of each node & to determine successful handover. Hand off Controller determines the hand off requirement to the nearest possible node. Smart Decision helps to handle making decisions to transfer data to nearby agent. Wireless access helps in defining access to nodes during hand off. System Monitor Helps in monitoring the whole network which indulges in channel aware routing & handover. Device Monitor Helps in evaluating the values successful data transfer. Mobile Host is the MANET(Mobile ADHOC Node). Network Selection Implies choosing from home to foreign agent.

4. SIMULATED RESULTS

4.1 Packet Delivery Ratio

Data packet delivery ratio can be calculated as the ratio between the number of data packets that are sent by the source and the number of data packets that are received by the sink. To evaluate network traffic load performance, we fixed maximum speed at 1 m/s, varying source packet rate from 5 to 40 packets/s. All other parameters were as in the previous section. Fig. 2 shows variation of packet delivery ratio (PDR) with increasing packet rate, while Fig. 3 shows variation of average end-to-end delay with increasing packet rate. Both protocols have decreased PDR with increasing packet rate. For low traffic loads, increased packet rate prolongs the average end-to-end delay. After a certain point, the packet delays decrease with increasing packet rate

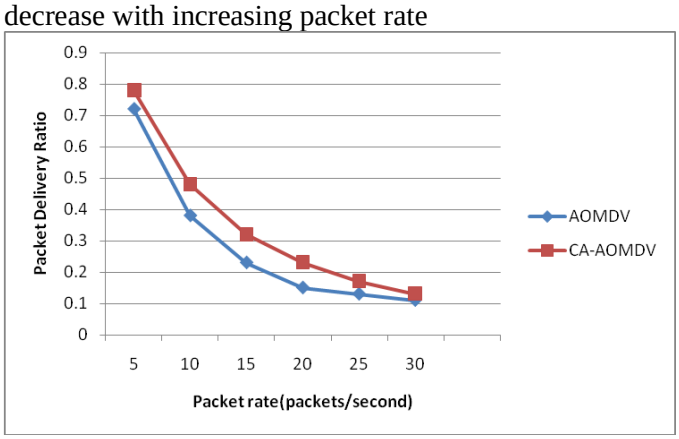


Fig-2:Packet Delivery Ratio comparison between CA-AOMDV and AOMDV

4.2 End to End Delay

CA- End-to-end delay refers to the time taken for a packet to be transmitted across a network from source

to destination. The decrease of average end-to-end delay in Fig. 3 occurs because, at higher packet rate, more packets are dropped due to congestion. For both PDR and average end to- end delay, AOMDV outperforms AOMDV. For a packet rate of 20 packets/second, there is a 34.1 percent improvement of packet delivery ratio and 18.7 percent improvement of the average end-to-end delay.

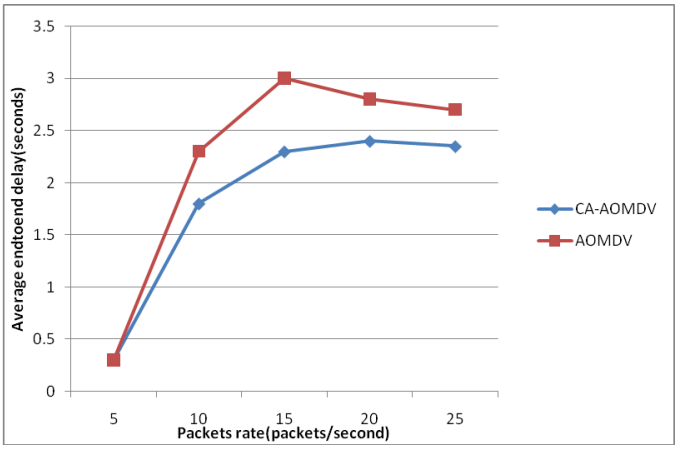


Fig-3:Average End to End Delay Comparison between CA-AOMDV and AOMDV.

5. CONCLUSION

A channel-based routing metric is proposed which utilizes the average non fading duration, combined with hop-count, to select stable links. A channel-adaptive routing protocol, CA-AOMDV, extending AOMDV, based on the proposed routing metric, is introduced. During path maintenance, predicted signal strength and channel average fading duration are combined with handoff to combat channel
fading and improve channel utilization. A new theoretical expression for the lifetime of the multiple reusable path system used in CA-AOMDV is derived. Theoretical expressions for routing control overhead and packet delivery ratio also provide detailed insights into the differences between the two protocols. Simulation results show that CA-AOMDV outperforms AOMDV in practical transmission environments.

ACKNOWLEDGMENT

I would like to thank our respective head of the department Prof. Dr. Ravi PhD and our respective guide Mrs.J.Preskilla Angel Rani M.E, Assistant professor and all who help us to complete the project successfully.

REFERENCES

1. Xiaoqin Chen, Haley M. J ones, and Dhammika Jayalath," Channel-Aware Routing in MANETs with Route Handoff" IEEE transactions on mobile computing, vol. 10, no. 1, Januar y 2011.
2. A.B. Mnaouer, L. Chen, C.H. Foh, and J.W. Tantra, "OPHMR: An Optimized Polymorphic Hybrid Multicast Routing Protocol for MANET," IEEE. Trans. Mobile Computing, vol. 5, no. 6, pp. 503-514, May 2007.
3. S. Panichpapiboon, G. Ferrari, and O. K. Tonguz, "Optimal transmit power in wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 5, no. 10, pp. 1432–1447, 2006.
4. S. Jiang, D. He, and J. Rao, "A prediction-based link availability estimation for routing metrics in MANETs," IEEE/ACM Transactions on Networking, vol. 13, no. 6, pp. 1302–1312, 2005.
5. S. Jain and S.R. Das, "Exploiting Path Diversity in the Link Layer in Wireless Ad Hoc Networks," Proc. Sixth IEEE Int'l Symp. World of Wireless Mobile and Multimedia Networks (WoWMoM), pp. 22-30,June 2005.
6. M.R. Souryal, B.R. Vojcic, and R.L. Pickholtz, "Information Efficiency of Multihop Packet Radio Networks with Channel-Adaptive Routing," IEEE J. Selected Areas in Comm., vol. 23, no. 1,pp. 40-50, Jan. 2005
7. Z.R. Zaidi and B.L. Mark, "Real-Time Mobility Tracking Algorithms or Cellular Networks Based on Kalman Filtering," IEEE Trans. Mobile Computing, vol. 4, no. 2, pp. 195-208, Feb. 2005.
8. P. Samar, M.R. Pearlman, and Z.J. Haas, "Independent Zone Routing: An Adaptive Hybrid Routing Framework for Ad Hoc Wireless Networks," IEEE/ACM Trans. Networking, vol. 12, no. 4,pp. 595-608, Aug. 2004.
9. Awerbuch, D. Holer, and H. Rubens, "High Throughput Route Selection in Multi-Rate Ad Hoc Wireless Networks," Proc. Conf. Wireless On-Demand Network Systems (WONS), pp. 251-269, March 2004.
10. J.E. Garcia, A. Kallel, K. Kyamakya, K. Jobmann, J.C. Cano, and P. Manzoni, "A Novel DSR-Based Energy-Efficient Routing Algorithm for Mobile Ad-Hoc Networks," Proc. 58th IEEE Vehicular Technology Conf., vol. 5, pp. 2849-2854, 2003.
11. Z. Zaidi and B. Mark, "A Mobility Tracking Model for Wireless Ad Hoc Networks," Proc.

Wireless Comm. and Networking Conf. (WCNC), pp. 1790-1795, March 2003.
12. O. Tickoo, S. Raghunath, and S. Kalyanaraman, "Route Fragility: A Novel Metric for Route Selection in Mobile Ad Hoc Networks, "Proc. IEEE Int'l Conf. Networks (ICON), pp. 537-542, Sept. 2003
13. M. Park, J. Andrews, and S. Nettles, "Wireless Channel-Aware Ad Hoc Cross-Layer Protocol with Multiroute Path Selection Diversity," Proc. IEEE Vehicular Technology Conf. (VTC)-Fall, vol. 4,pp. 2197-2201, Oct. 2003
14. Gerharz, C. de Waal, M. Frank, and P. Martini, "Link stability in mobile wireless ad hoc networks," In Proceedings of IEEE Conference on Local Computer Networks, Nov. 2002
15. M.K. Marina and S.R. Das, "On-Demand Multipath Distance Vector Routing in Ad Hoc Networks," Proc. Ninth Int'l Conf. Network Protocols (ICNP), pp. 14-23, Nov. 2001
16. R.J. Punnoose, P.V. Nikitin, and D.D. Stancil, "Efficient Simulation of Ricean Fading within a Packet Simulator," Proc. IEEE Vehicular Technology Conf. (VTC), vol. 2, pp. 764-767, Sept. 2000

A Fascinating technique for the innovation of Vampire Attack in Wireless Sensor Ad Hoc Network

S.Blessy Vedha
PG scholar , CSE Department
SCAD CET, Cheranmahadevi, TamilNadu
blessyvedha@gmail.com

P.Petchimuthu
Professor , CSE Department,
SCAD CET, Cheranmahadevi, TamilNadu

***Abstract*-- Network action is the major contribution of scientific investigations. The brutal force on vampire attack decreases the energy from the nodes and does not allow communication between the nodes. It deprives the entire network by reducing the energy of a particular node, the node loses the capacity to live. Prior we focus on rejection of communication. Vampire attacks belief in many belongings of switching and routing protocols. There are many protocols to prevent many attacks but the vampire is devastate and hard to discern. We inspect the techniques to recognize this attack and to reconfigure the connection using wireless sensor ad hoc network.**

Index Terms: Ad hoc networks, Rejection of communication, wireless sensor networks

I.INTRODUCTION

Ad hoc specifies the network that is no generalised and used for a specific task or purpose. It is mainly used in military purposes produced for peculiar situations and used in many organisation, universities, committees etc. Ad hoc does not depend on previous infrastructure. It also denotes a group of network where all the nodes are having equal strength. IEEE 802.11 wireless network also specifies the ad hoc networks. The network admonishes the conditions on environment, functions in the organisations. Wireless sensor network played an extremely important role in daily life of humans. Deficiency of capability may lead to environment misfortune, lacking of energies. The capability of network is very important and it should satisfy various properties. Owing to wireless ad hoc network it is susceptible to Denial of service (DOS) attacks.

Many systematic plans are adopted to prevent the network from many attacks. In this paper we explore about vampire attack and initially consider a network that contains nearly 100 nodes. Fix a base station at the place that is equally distant from the sides or outer boundaries. Authorize the nodes to communicate with a base station. When each node communicates with base station, it cannot response to every node because of overload. The nodes can be of three types' dead nodes, active nodes or alive nodes, normal nodes. The job activity of active nodes is it consumes huge amount of energy and act as an active part in the network. The normal nodes have a normal behaviour and the purpose of these nodes is to transmit a data from one node to other node. Dead nodes that are present in the network have no avail and the presence of dead node detach the communication. It reduces the energy of the node and disconnects the transmission. We propose a cluster head and cluster head communicates with cluster group members and the base station. It acts as intermediately between cluster group members and the base station. The cluster head is elected randomly using a threshold equation. Threshold varies between different values and threshold will be greater than or equal to the value at every time. Threshold value will be the exact value and it accepts only the very closest or nearest value to that particular value. The nodes are calculated using heterogeneous energy levels. The nodes having the closely related values can be assembled in cluster group members. It can be clustered into small groups.

II. RELATED WORKS

Rate limiting and the elimination of insider adversaries as capable solutions are maintained, the competition inside the networks are avoided [5]. By analysing the vulnerabilities we can design a new protocol using DOS susceptibility. It is resilient to individual node failure, since the time is not specified it can be destroyed at any time. Ad hoc network support static infrastructure and it offers monitoring of home health care. Increasing the efficiency and effectiveness of MAC and routing protocol problems are cause on behalf of bandwidth and memory. Sleep deprivation torture is power exhaustion also it never leaves the node from entering into low power sleep cycle; it reduces the battery power faster. End-to-end encryption is impractical [1]. Research problems may include the privacy and security issues. Injected messages are prevented by proper authentication. Initiate the small number of connection for legitimate clients and minimal load and it does not send large amount of data over the life time. While forwarding the packets authentication of client before server commits any resources is necessary, it creates a new opportunities for DOS attacks because authentication protocol usually require the client to store previous session state. Initially the client should commit its resources and the server must verify the client before allocate the resources. [7]. Focusing on the transport layer rather than routing protocols and owing to the poor design implementation vulnerability may occur. The system performance can be avoided an approach of sledge hammer is

discussed. It transmits a high rate of packet towards the attacked node. On other hand it is a composition of diagnostic modelling, gathering of replication and experiments on the internet. While transmission it throttle the TCP flows to ideal rate [8]. Maintenance of logical separation between links connecting end-user and mesh user and we consider two properties, loose source routing where any forwarding node can reroute the packet if it knows the shorter path to the destination but it is not efficient. Another property is no backtracking property, it hold if and only if the packet is moving very closer to the destination with every hop round [3]. Quality of service (QOS) degradation and Reduction of Quality (ROQ) attacks are not permitted. It covers active attacks and covers all possible failures and it is challenging to satisfy in high speed routers [4]. It does not have much capacity to send data, only minimum packet should be allowed or it causes to be overload. Server should verify the client and then make the full authority of authentication [10]. Intrusion Tolerant Routing in Wireless Sensor Network (INSENS) does not depend on detecting intrusions although it minimizes the communication, computation and storage. Design and implementation is very tedious process [9]. Researches based on Denial Of Sleep (DOS) concentrates only on MAC layer while it focus mainly on data confidentiality, integrity and heavily ignoring the availability [6]. Rushing attack results in denial of service when used against network routing protocols. Development and analysis of new secure route is employed and another limitation is the secure protocols cannot find a valid path, so there is a lack of privacy and security in sensor network [2].

III. EXISTING SYSTEM

Secure efficient distance vector routing of mobile wireless ad hoc networks (SEAD) is existing secure routing protocols [11]. Initially, we have a deep research on susceptible on existing protocols. We provide confidential measures to avert, vampire attacks are orthogonal to those used to protect routing infrastructure. Existing work of carousal attack, since the opponent composes the packet in loops it sends the packet in circles so by chance it takes a maximum time to send a packet to destination sometimes it may lose the information but no immediate cognition is provided. The next attack also aimed at source routing, the opponent creates ersatz lengthy routes possibly traversing every hop of node in the network. The stretch attack maximizes the packet length, causes the packet to be processed by the number of nodes and independent of hop count. Throughout the forwarding phase, every decision is completed autonomously by each node. When delivery a packet, a node determines the subsequently hop by judgment of the most significant bit of its deal with that differs from the message originator's address. If there is time consumption then we may assume that the output data will not exactly be a right data. To avoid such type of consumption we are placing cluster head among the nodes.

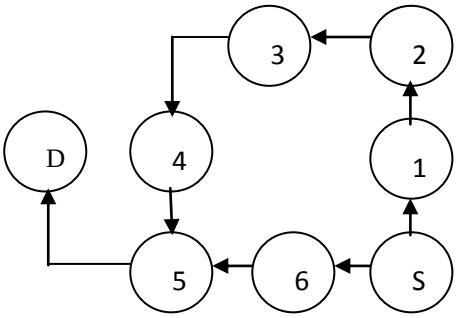


Fig.1. stretch attack

S is the source node and D is the destination where the source node may send the packet to destination through the path 6 and 5. While passing the information if the source node takes the path of S-6-5-D then there will be no loss of packet. If there is an attack then it make the packet to circulate in the network it may leads to a loss of information or the packet will never reach the destination at a particular time.

We assume the messages have their own path at which they are generated from source to destination. The attacks are maximized by combining the competitor node in the network or by sending many packets. The first preservation mechanism is loose source routing, where the forwarding node can reroute the packet if it knows the shorter path to destination, but it is not efficient in global network. So we move on to no backtracking property, here the node hold the packet if the packet moves strictly closer to the destination otherwise it will not handle the packet and it reduces the discussed vampire attack in harmful flooded detection. Researches based on Denial of Sleep (DOS) concentrates only on MAC layer while it focus mainly on data confidentiality, integrity and heavily ignoring the availability. Rushing attack results in denial of service when used against network routing protocols. Development and analysis of new secure route is employed and another limitation is the secure protocols cannot find a valid path, so there is a lack of privacy and security in sensor network. It explores resource depletion attacks at the routing protocol deposit, which everlastingly render inoperative networks by hastily draining nodes' battery power. Earlier we discuss about forward packet algorithm in order to prevent the network from vampire attack and we cannot completely overcome this attack but recommend some intuition to surmount this attack. We find that all examined protocols are susceptible to Vampire attacks, which are overwhelming, complicated to classify, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. "Snooze deficiency makes suffer" the projected attack prevents nodes from arriving a low-power siesta rotation, and thus reduces their batteries more rapidly.

A.Topology discovery

Topology discovery is based on time limited duration in which each node in the network will declare their own presence by broadcasting its certificate identity or by public key and it is signed by its trusted authority. Cluster combine preferentially with the fewest adjoining group, which may be a solitary node. We may consider of groups performing as personality nodes, with judgement made using protected cooperative computation. Nodes will demand to stick together with the smallest group in their surrounding area, with competition broken down by cluster IDs, which are computed communally by the complete group as a deterministic purpose of entity member IDs. During packet forwarding phase, all judgement are made autonomously by every node.

When unloading a packet, a node figure out the subsequent hop by judging the most momentous bit of its address that diverges from the message originator's address Thus, every forwarding event shortens the logical distance to the destination, since node addresses should be strictly closer to the destination.

IV.PROPOSED SYSTEM

Our major contributions are to detect the vampire attack in the node and remove the node from the network. So the connections will be detached, the communication between the nodes will be stopped. To avoid this we elect a cluster head where the cluster group members communicate with cluster head and the base station. The attack can be avoided and we can achieve better efficiency. Energy calculation of every node is taken and if there is an attack we can remove the attack using LEACH (Low Energy Adaptive Clustering Hierarchy) and reconfigure the overall connection in the network. Node placement describes how the nodes are placed to construct the wireless sensor ad hoc network topology in wireless sensor ad hoc network. The wireless sensor ad hoc network mainly contains the node, cluster head and base station. The node can be the dead node or active node or normal node. The type of the node is identified by its energy level. Cluster creation mainly concentrates on the cluster creation in wireless sensor ad hoc network. The cluster contains group of sensor nodes and each group contains a cluster head to gather the information send by all of its cluster group members. The cluster is formed by heterogeneous energy levels. The cluster head is elected using the threshold equation. This equation determines the fairly accurate value and not the too highest or too lowest. It selects the cluster head among the cluster group members. Cluster group members of a cluster have similar energy levels. The proposed system is planned to implement the heterogeneous wireless sensor ad hoc network .The proposed wireless sensor ad hoc network uses the LEACH (Low Energy Adaptive Clustering Hierarchy) protocol to transfer the data among cluster nodes and base station. However, recall that sending any packet automatically constitutes amplification.

Leach Algorithm

To increase the life time of the network we use hierarchal routing protocol for wireless sensor networks. LEACH is the first network protocol to use hierarchal routing. It is based on topology control and also in wireless sensor network; LEACH allows the nodes to communicate with each other nodes. It is based on hierarchal network; it introduces a individual functionalities, adaptive grouping protocol that equally supplies energy to each node. The high density wireless sensor nodes are grouped into clusters and to prevent exorbitant power consumption, he cluster head is elected randomly. All the nodes are supposed to be uniform and energy circumstantial force. It reduces data aggregation energy used for data transmission. The purpose of data aggregation is to reduce the number of transmission. Benefit of confined coordination and the managing capacity of clustering and the nodes has the capability to determine which nodes in the network can become a cluster head at each node. The judgment of the node by selecting a random of # between 0 and 1

If # < T (n)

The node is considered to be cluster head p is the optimal election probability of each node and it is said to be 0.1. T (n) is the threshold value and *rmax* is the maximum number of rounds, G is the ground node from the cluster head. Every one of node determines to be a cluster head (CH) in 1/p rounds and it is the probability of becoming a cluster head. The probability of cluster head is enlarging, since there is an eligibility of a node to become a cluster head in subsequent rounds.

```
If (T (n) <= (p/ (1-p* mod(r, round (1/p)))))

        S (i).G=round (1/p)-1

Distance=sqrt( (S(i).xd-(S(n+1).xd) )^2 +
        (S(i).yd-(S(n+1).yd) )^2 );

        C (cluster).distance=distance;

         C (cluster).id=i;

         Cluster=cluster+1;

         Etx(i)=(Eelec+Eamp*distance*distance)*k;

         S (i).E=S (i).E-Etx(i)-EDA;
```

T(n) refers to threshold of each nodes and p refers a probability. G determines the ground value, s(i) deals with the energy calculation of a single node. Now the distance is calculated for each node and allots an id for each node. Etx is

the energy used for transmitter and receiver.EDA is the data aggregation, it is used to reduce the number of transmission Calculate the minimum distance between the nodes and store in a temporary set. Place the initial value of 0 for a dead node and at each rounds the dead nodes are incremented by one. If not the node will be normal node or active node and energy calculation is done.

Etx(i)=(Eelec+Eamp*min_dis*min_dis)*k;
S (i).E=S(i).E-Etx(i);

distance = sqrt ((netXloc (i) - netXloc(j)) ^2 + (netYloc (i) - netYloc(j))^2);

Xloc is the location of x and calculating the distance by applying the sqrt formula. The graph is drawn according to the leach transmission algorithm.

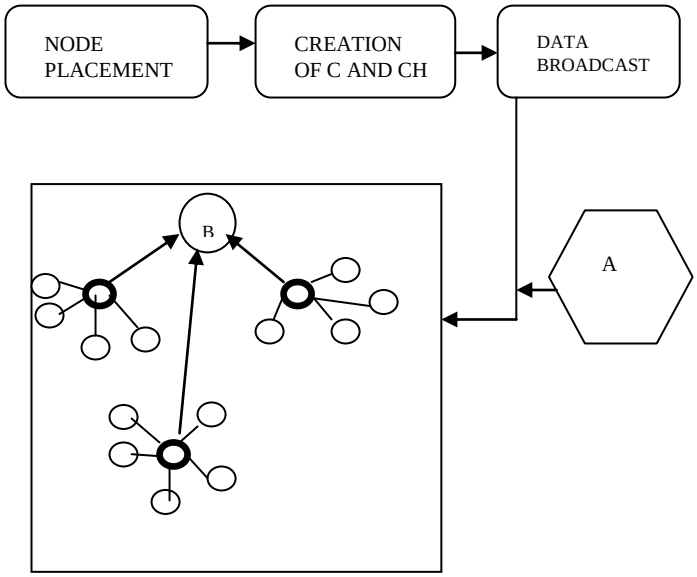


Fig.2. Architecture diagram for leach algorithm

After placing nodes in the network, the nodes are supposed to gather according to their heterogeneous energy levels. A cluster head is elected and we allow only the cluster head to communicate with the base station. Fig 2 represents the architecture diagram or the way of processing if there is emerge of an attack (A).

Non cluster head nodes must receive the messages during the announcement period. At a later phase, they decide a cluster to belong for this round by choosing a cluster head that needs minimum communication energy. CH establishes TDMA schedule also LEACH protocol uses CDMA to reduce the obstruction between the clusters. It also calculates the energy of every single node. Functionalities of this algorithm comprise cluster infrastructure, election of cluster head using threshold equation, adaptation of clustering membership, data aggregation is employed, and cluster head act as an intermediate for the base station and cluster group members. Estimate the maximum distance and minimum distance of each node from ground and the ground value is initiated as a null value.

V.PERFORMANCE EXAMINATION

When compared to the denial of communication, sleep deprivation torture etc our performance on clustering of nodes using LEACH protocol is professional. The existing deal with lot of time consumption, wastage of energies and lose of information that is the correct message is not delivered as an output. If the messages are produced then it will take a lot of time. So when we are passing a plenty of messages the network becomes very inefficient. Additional packet verification constraints for intermediate nodes also maximize workstation development, overwhelming time, and additional energy. Obviously there is nothing to be gained in entirely no competitor environments, excluding in the occurrence of still a small number of malevolent nodes, the increased transparency becomes advisable when bearing in mind the possible damage of Vampire attacks. Power expenses for cryptographic operations at transitional hops is, regrettably, much superior than broadcast or obtain visual projection, and much more dependent on the detailed chipset inured to build the sensor. Sequence signatures are to some extent more mysterious creation, and entail bi linear maps, potentially requiring especially costly calculation than other asymmetric cryptosystems. It can direct to several nodes being detached from the network for a period of time, and is essentially the appearance of incriminate restricted. Even though we discarded rate restrictive earlier than, it is adequate here whereas innovation should devour a miniature portion of administration moment in time compared to packet forwarding. Simulation results illustrate that depending on the position of the adversary, network force expenses for the duration of the forwarding period for 30 nodes. The security properties are nothing but the adversary cannot challenge the recursive federation algorithm by inserting, making corrections or tumbling packets.

We analyze the recital of our procedure beneath molest and to explore techniques to improve the progress in efficiency, and to expand our operation.

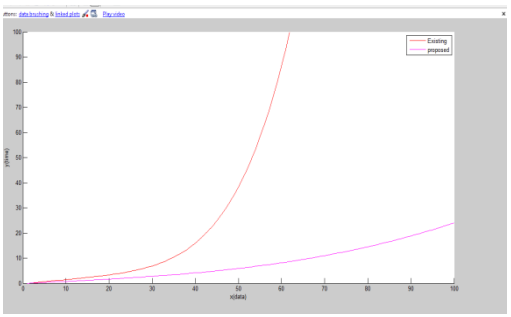


Fig.3. Performance Analysis

Graph of Performance Analysis deals with time consumption of an output from existing system and proposed system. We analyse the graph (fig 3) by giving various inputs.

IV. CONCLUSION

In this paper, we explore the detection of vampire attack using LEACH protocol. By clustering of each node and electing the central head, innovative group of resource expenditure attacks that employ routing protocols to everlastingly put out of action in ad hoc wireless sensor networks by depleting nodes' battery power. These defects do not rely on fastidious protocols or implementations, but relatively represents the vulnerabilities in a quantity of admired procedure program. Vampire attacks verify the packets consistently to formulate advancements towards their destinations. We have not obtained a complete reasonable explanation for Vampire attacks during the topology unearthing phase, but suggested various perceptions regarding harmful boundaries potential. To reconfigure the overall connection in the network to improve its efficiency and to estimate the damage bounds using topology discovery phase are left as future work.

REFERENCES

[1]. Eugene Y. Vasserman and Nicholas Hopper "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks,feb 2013

[2]. Y.-C. Hu, D.B. Johnson, and A. Perrig, " Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proc. Second ACM Workshop Wireless Security (WiSE), 2003.

[3]. B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure Sensor Network Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf., 2006.

[4] S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford, "Path- Quality Monitoring in the Presence of Adversaries," Proc. ACM SIGMETRICS Int'l Conf. Measurement and Modeling of Computer Systems, 2008.

[5] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.

[6] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE Trans. Vehicular Technology, vol. 58, no. 1, pp. 367-380, Jan. 2009.

[7] T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int'l Workshop Security Protocols, 2001.

[8] A. Kuzmanovic and E.W. Knightly, "Low-Rate TCP-Targeted Denial of Service Attacks: The Shrew vs. the Mice and Elephants," Proc. SIGCOMM, 2003.

[9] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks," Computer Comm., vol. 29, no. 2, pp. 216-230, 2006.

[10] D.R. Raymond and S.F. Midkiff, "Denial-of- Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, pp. 74-81, Jan.-Mar. 2008.

[11] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications, 2002.

Unital-Based Key Pre-distribution Scheme for Enhanced Security in SET Protocols

D.Veenadevi
Department of Computer Science and Engineering.
Raja College of Engineering and Technology.
Madurai, India.
veenu233@gmail.com

G.D.Kesavan
Assistant Professor, Department of Computer science and Engineering.
Raja College of Engineering and Technology.
Madurai, India.
gdkesav@gmail.com.

Abstract **- Key management scheme act as a basic root for providing security services in wireless sensor networks. However, Key management becomes one of the main problems in WSNs because of the limitations in the resources and sensitivity in several applications. But clustering mechanism provides good network scalability and better network performance in WSNs. In this paper we discuss about the key management schemes applied in SET protocols for CWSNs, and propose an enhanced unital-based key pre-distribution scheme which provides enhanced security. The unital scheme applied in SET protocols provides high key sharing probability while enhancing the network scalability. It allows multiple encryptions in the intermediate nodes by generating unital blocks which provide enhanced security than the existing key management scheme in SET protocols. The result shows enhanced security in SET protocols than the existing key management scheme and overall improved performance using unital-based key pre-distribution scheme.**

Index Terms:-Cluster-based wireless sensor networks, SET protocols, key sharing, security, network scalability, unital design theory.

I. INTRODUCTION

Many application areas like military, agriculture, medical, motivate the development of wireless sensor networks. Wireless sensor network (WSN) consists of group of sensors for monitoring the physical conditions of the environment and record them for analyzing. Environmental conditions like pressure, sound speed, temperature are measured using wireless sensor networks. Mobility of nodes, heterogeneity of nodes, withstand in harsh environmental conditions are the characteristics of wireless sensor networks. A WSN consists of sensor nodes with various equipment like antenna, battery, circuits etc. Depending on certain parameters the prices of the sensor nodes may varies. Wireless sensor networks have some problems like limited power, high power consumption, security problems. Many energy efficient protocols are used to solve these problems. These protocols are based on clustering techniques.

Clustering means set of clusters. Wireless sensor network have many organizational units. Cluster act as the organizational units in WSNs. Every cluster elects a cluster head (CH). The CH aggregates the data and sends them to base station. Providing security to many secure protocols is a challenging issue. Designing key management leads to some issues. In this paper we discuss the key management schemes applied in SET protocols [1] for CWSNs, and applies an enhanced unital-based key pre-distribution scheme which provides high network scalability and secure key sharing between intermediate nodes in cluster based WSNs.

II.SET PROTOCOLS

Providing security to many secure protocols is a challenging issue. Many existing secure transmission protocols apply the symmetric key management for security. But it creates some problems like orphan node problem which is discussed in paper [1].

This problem occurs when a node does not share a pair wise key with others in its preloaded key ring [1]. This problem increases the overhead of transmission and system energy consumption by raising the number of CHs. The SET protocols (SET-IBS and SET-IBOOS) solve the orphan node problem in the secure data transmission with a symmetric key [1].The contributions of the existing SET protocols works are as follows.

- Two **S**ecure and **Eff**icient data **T**ransmission (SET) protocols for CWSNs, was implemented. They are called as SET-IBS and SET-IBOOS.
- The SET-IBS and SET-IBOOS applies digital signature to the message packets work in order to authenticate the encrypted sensed data and applying the key management for security.
- Using ID-based cryptography, secure communication is provided in SET-IBS .The ID information are the user public keys.
- The SET protocols such as SET-IBS and SET-IBOOS are used to solve the orphan node using symmetric key management in the secure data transmission. The orphan node problem is solved by using the ID-based crypto-system that guarantees security requirements, and proposes SET-IBS by using the IBS scheme [1].

The additively homomorphic encryption scheme is adopted to encrypt the plaintext of sensed data, in which a specific operation performed on the plaintext is equivalent

to the operation performed on the cipher text. The following figure 1 shows the SET protocols system design.

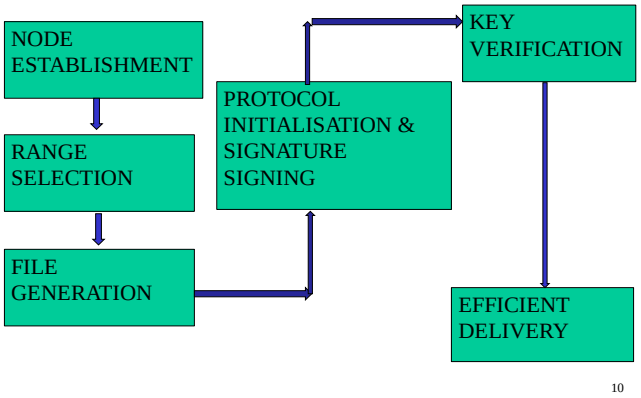


Figure 1: SET protocols system design

A. Node deployment

It involves deployment of multiple nodes .Election of cluster head varies after every specific time period. Sink node or Base Station acts as the destination node. The BS (as a trust authority) generates a master key (MSK) and public parameters pram. It involves the transfer of a file. Giving an ID string, a sensor node generates a private key sek ID associated with the ID using MSK.The source node performs signature signing. Any file being in movement within a cluster reaches another partition only through the path involving its cluster head.

B. Key Management for Security

The base station broadcasts the master or public key to all nodes. Based on the master and ID value, Individual Secret key is generated. Upon node revocation, the BS broadcasts the compromised node IDs to all sensor nodes. The additively homomorphism encryption scheme was adopted to encrypt the plaintext of sensed data.

C. Protocol Operation

Corresponding private pairing parameters are preload. Either SET-IBS or SET-IBOOS scheme was selected .For fair energy consumption nodes are randomly elected as CHs in each round. Sink node accepts the message once the signature value of source is valid. The characteristics of the SET protocols are compared with other secure data transmission protocols which are explained as follows.

- *Key management:* The protocol uses key cryptographies which consist of both symmetric and asymmetric keys for achieving secure data transmission.
- *Neighborhood authentication*: By allowing authenticating each other the data transmission and access can be secure in SET protocols but it is limited in other secure protocols.
- *Storage cost:* The requirement of the keys used for providing security which is stored in sensor node's memory is comparatively low in SET protocols .
- *Network scalability*: It is comparatively high when compared with the other secure protocols because when the larger network scale increase, orphan node appears in the network will be more.
- *Communication overhead:* During communication the data packets contain security overhead which is comparatively high in SET protocols.
- *Computational overhead:* cost for the energy used and computation efficiency will be comparatively high than other secure protocols.
- *Attack resilience:* The protocols can protect against both active and passive type of attacks.

In this SET PROTOCOLS the energy consumption was given more importance. The SET-IBS and SET-IBOOS provide maximum energy consumptions for the nodes for efficient data transmission. The simulation results shows using these protocols are more worthful than the protocols compared with it .However, the key management schemes used in SET protocols provides good security but it is not given more importance. General symmetric and asymmetric key management schemes were applied. These schemes allows only one encryption and decryption process which doesn't provide a high security among data transmission.

III.KEY MANAGEMENT SCHEMES IN SET PROTOCOLS

Generally key management is the process of establishing and managing the keys in the cryptosystems. Key management scheme act as a basic root for providing security services in wireless sensor networks. However, Key management becomes one of the main problems in WSNs because of the limitations in the resources and sensitivity in several applications. Symmetric key establishment becomes suitable for secure key exchanges in WSNs. However due to the absence of some infrastructure facilities it doesn't have trusted third party. So most existing solutions are based on key pre-distribution. In this section the symmetric and asymmetric key management schemes which are applied in SET protocols and their general works are discussed. In paper [2] symmetric schemes are discussed. In this work symmetric schemes are classified into two types. They are probabilistic schemes and deterministic schemes.

A. Probabilistic Scheme: To achieve secure data transmission between sensor nodes secure link is needed. Each two neighboring node provide this secure link with low probability otherwise secure path should be established.

The basic Random Key Pre-distribution scheme was proposed in paper [3] .CPU and energy efficient are the basic

approach which requires large memory for storing key rings. Great number of secure links needs to be getting comprised due to the network corruption in the nodes.

In paper [4] a protocol called Q-composite scheme has been proposed. It enhances the network resilience Of Random Key Pre-distribution scheme. Ki,j = Hash(Ks1| |Ks2| |...||Ksq) where Ks1,Ks2, ...Ksq are the q0 shared keys between the two nodes i and j (q0 _ Q) is used for calculating pair wise session key .The secure connectivity coverage gets degraded because for establishing secure link the neighboring node needs at least Q common keys. The proposed scheme provides a unique secret pair wise keys .It also provide low key sharing probability and imperfect network resilience.

B. Deterministic Scheme: It provides pair wise keys with all the neighboring nodes. Determinism is guaranteed by providing many solutions.

In paper [5] an enhanced approach is proposed for storing (n + 1)/2 keys at each node. A hash function based key establishment is used for storing half of the symmetric keys for nodes but remains non scalable. Likewise papers[6] and [9] also proposed some schemes for key storing which is not efficient .In SET protocols the communication overhead is deterministic whereas probabilistic for other secure protocols.

The asymmetric schemes also provide some problems. Diffie Hellman key exchange is one of the earliest practical examples of key exchange implemented within the field of cryptography. It is vulnerable to attacks where an intruder intercepts messages between sender and receiver. It assumes the third party that is the attacker. It solves the discrete logarithm but there are some expensive operations need to be performed and it is only used for generating secret keys .RSA (Rivest Shamir Adleman) is a best known & widely used public-key scheme. It provides security due to cost of factoring large numbers.

Many researchers have been researching RSA algorithms. Those discussions can be seen in [7] [8].These papers provide some methods or implementation techniques for improving RSA algorithm. This paper [7] presents the architecture and modular multiplication for RSA public key algorithm. Montgomery's algorithm is used. It avoids the traditional division operation and uses shift and addition operations to perform modular multiplication .In paper [8] analysis for the RSA public key protocol in the framework of membrane computing to develop a membrane model of RSA algorithm with performance improvement has been discussed. The performance of the proposed algorithm of RSA using membrane computing is simulated using software written in C++(using visual c++).It compared the performance to the performance of normal RSA on the same platform [8].Some uses c++ language and other uses some other algorithm. Thus both schemes have been discussed and in order to improve security in SET protocols we applied a unital-based key pre-distribution scheme .The section IV and V describes the concept of unital scheme and section VI and VII describes how the unital scheme works in SET protocols and its performance.

IV.NAIVE UNITAL-BASED KEY PRE-DISTRIBUTION SCHEME

This section deals with the naive unital based key pre-distribution scheme (NU-KP) by using unital deign theory which is proposed in paper [2].WSNs faced many problems like storage overhead, key sharing probability etc .When the key sharing probability is high security risk will be less. The key sharing problem can be solved by generating unital blocks corresponding to the key rings. When designing key rings it affects some performance metrics like low network scalability, secure connectivity and storage overhead. The unital deign theory allows to generate unital blocks corresponding to the key rings.

A simple scalable key pre-distribution scheme based on unital designs is proposed in paper [2].Before the deployment phase the source node generate the unital blocks for the corresponding key rings. Each node is then pre-load with a distinct key ring as well as with the corresponding key identifiers.each node can share at most one common key by using this approach. But according to the unital properties that two blocks cannot share more than one key. To share more one common key it is necessary to determine secure link, Storage overhead, Network scalability, Direct secure connectivity coverage has been analyzed using the naive unital-based key pre-distribution scheme. The evaluation results proposed in paper [2] gives high network scalability which reaches O(k4), the key ring size up to $4\sqrt{n}$.This solution gives low key sharing probability of O(1/k).In order to improve key sharing probability enhanced unital-based key pre-distribution scheme is used which maintains good key sharing probability while enhancing the network scalability.

V.UNITAL-BASED KEY PRE-DISTRIBUTION SCHEME

In order to improve key sharing probability the unital based key pre-distribution scheme (U-KP) generates a unital block and pre-loads each node in the network with a number of blocks created. We generate blocks of some order of unital design corresponding to the key rings. The each node is preload with completely disjoint sets. There will be only one unital block for each node that is pre-load and each share at most one key [2].But in U-KP,each node gets pre-load with unital blocks of disjoint .

Once the node gets deployed in order to determine the common key each node exchanges their key identifiers. If two neighboring nodes share one or more keys, we compute the pair wise secret key as the hash of all their common keys connected to each other. This approach provides high key sharing probability by pre-loading each node with the key rings.

This shows multiple encryption process in the intermediate nodes. By allowing multiple encryption process the security gets enhanced. Moreover it achieves good network resilience. This enhanced unital-based key pre-distribution scheme is applied in SET protocols during protocol initialization. It provides enhanced security than the

existing scheme. The storage overhead, Network scalability, Direct secure connectivity coverage improved results is explained as follows.

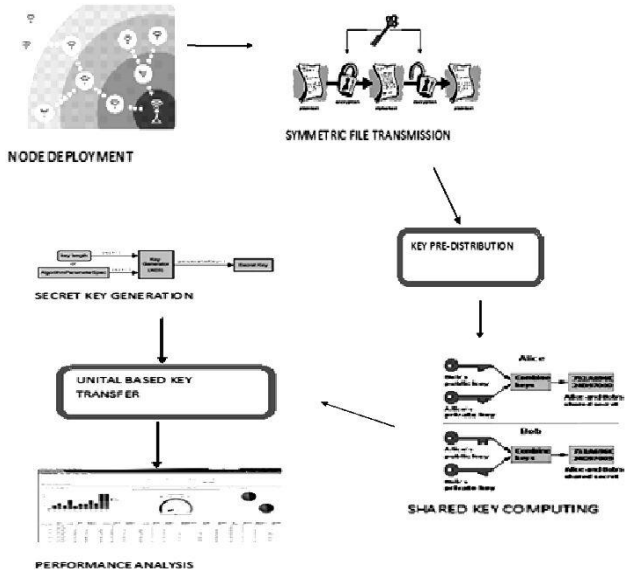


Fig .2. Enhanced unital based key pre- distribution scheme design

- *Storage overhead*: When using the unital scheme of order m, we pre-loaded each node with t(m+1) distinct keys. So, the memory required to store keys is then equal to l × t × (m + 1), where l is the key size [2].
- *Network scalability*: Since each node is pre-loaded with t blocks from the m2 × (m2 −m+1) possible blocks of the unital design, the maximum number of key rings that we can reach is equal to n = m2 /t (m2 −m+1) [2].
- *Direct secure connectivity coverage*: it provides very good secure connection.

VI. UNITAL–BASED KEY PRE-DISTRIBUTION SCHEME IN SET PROTOCOLS

In SET protocols asymmetric scheme is applied for encryption and decryption process. For enhancing the security in SET protocols the unital –based key pre distribution scheme is applied. The IBS performs setup at the BS, key extraction and signature signing ,verification at the data receiving nodes and IBOOS scheme performs setup at the BS, key extraction , offline and online signing at the data and verification at the destination nodes. During protocol initialization the BS generate the encryption keys with the key identifiers. It also generates a unital blocks with a set of pair keys .it is transmitted to each and every node in between the source and the destination node. Giving an ID using MSK the first intermediate node starts mapping the key values in the unital blocks received with the key values it have and encrypt the message with the key and send it to the next node. The process continues until it reaches destination node. The destination node decrypts the message with the key values of every intermediate node (backward to forward). Finally it decrypt the message using the source node key. Then the sink node accepts the message once it matches the signature of the source node .Unital blocks have a set of key values which can't be known to other nodes only the key values assigned for it can be seen. It allows multiple encryptions for every intermediate node. So the there will be enhanced security for data transmission in SET protocols than using asymmetric key management. The network scalability, storage overhead, secure connectivity range will be enhanced using unital scheme. The network resilience and network scalability gets enhanced by using unital scheme in SET protocols as shown in the Figure 3 and 4.

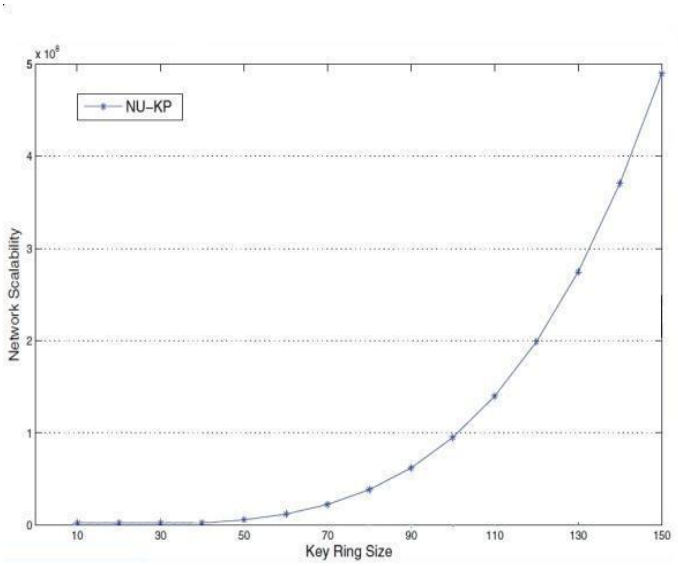


Fig .3. Network scalability compared to the key ring size

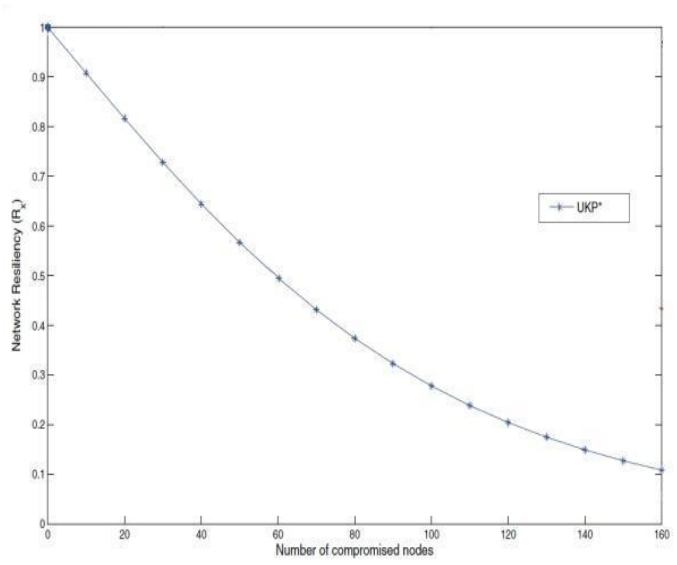


Fig .4. Network resiliency compared with number of nodes.

VII.PERFORMANCE OF UNITAL-BASED KEY PRE-DISTRIBUTION

The SET-IBS and SET-IBOOS are efficient in communication and applying the ID-based crypto-system, which provides security in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. However it doesn't provide enhanced security for the sensor nodes .But the unital-based key pre-distribution scheme allows the source node to generate an unital blocks which have a set of key values. So multiple encryptions is allowed and it also produce high key sharing probability which leads to enhanced security for data transmission. The unital scheme also provides high network scalability and overall performance will be improved in set protocols using unital scheme.

VIII .CONCLUSION

In this paper we discussed the SET protocols (SET-IBS and SET-IBOOS) and key management schemes applied. In CWSNs SET protocols. We used unital-based key pre-distribution scheme for achieving enhanced security in SET protocols. This scheme generates unital blocks and naïve mapping is done with distinct key identifiers. It allows multiple encryptions which increases key sharing probability and provides enhanced security than the existing key management scheme in SET protocols. The network scalability, storage overhead, secure connectivity range will also get enhanced using unital scheme. Then the performance has been analyzed and the result shows enhanced security for SET protocols using the unital based key pre-distribution.

REFERENCES

[1] Huang Lu, Jie Li, Mohsen Guizani,"Secure and Efficient Data Transmission for cluster-based Wireless sensor Networks",IEEE Trans,vol.pp,year 2013.

[2] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, Vahid Tarokh,"A Highly Scalable Key Pre-distribution scheme foW ireless Sensor Networks",vol.12,No.2,year 2013.

[3] L. Eschenauer and V.D. Gligor. A key-management scheme for distributed sensor networks. In *ACM CCS*, pages 41–47, 2002.

[4] D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In *ACM CCS*, pages 52–61, 2003.

[5] Choi, H. B. Acharya, and M. G. Gouda. The best keying protocol for sensor networks. In *IEEE WOWMOM*, pages 1–6,2011.

[6] S. Zhu, S. Setia, and S. Jajodia. Leap: efficient security mechanisms for large-scale distributed sensor networks. In *ACM CCS*,pages 62–72, 2003.

[7] Sushanta Kumar Sahu, Manoranjan Pradhan, "Implementation of Modular multiplication for RSA Algorithm",International conference on Communication Systems and Network Technologies,year 2011.

[8] Salah Zaher, Amr Badr & Ibrahim Farag,Tarek Abd Elmageed,"Performance Enhancement of RSA Cryptography Algorithm by Membrane Computing",vol.2,year 2012.

[9] S. A. C¸ amtepe and B. Yener. Combinatorial design of key distribution mechanisms for wireless sensor networks. *IEEE/ACM Transactions on Networking*, 15:346–358, 2007.

[10] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney. A key management scheme for wireless sensor networks using deployment knowledge. In *IEEE INFOCOM*, pages 586–597, 2004.

Localized Detection of Replication Attack in Mobile Sensor Networks

Mrs.M.Kalavathi[1], Ms.M.Jeyalakshmi [2]
[1]Pursuing M.E in Computer Science from SCAD Engineering College, Cheranmahadevi
[2]Asst.Prof. SCAD Engineering College, Cheranmahadevi

Abstract – Wireless sensor network is a group of sensor nodes which is used for monitoring and recording the physical conditions of the environment. In this paper focus is on the node replication attack and it's detection. In our existing system using two methods such as witness finding and another one is velocity exceeding. From this witness finding technique ,energy and communication cost will be high due to occurrence of communication. Next, discuss about velocity exceeding, it depends upon time synchronization. In this paper proposed a localized algorithm for detection of Node Replication Attack in Mobile sensor networks [2]. Localized algorithm such as Extremely Efficient Detection(XED) and Efficient Distributed Detection(EDD). Both algorithm achieves balance among storage, computation, and communication overheads, which are all O(1). It has unique characteristics, Such as network-wide time synchronization avoidance and network-wide revocation avoidance.

Index terms - Wireless Sensor Network, Node Replication attack, Mobile Sensor Network

I.INTRODUCTION

A. Wireless Sensor Network

Wireless sensor network(WSN) is a network made of numerous small independent sensor nodes. Size of a Sensor node is 35 mm, it consisting of a battery, radio, sensors, and a minimal amount of on-board computing power. The nodes self-organize their networks, rather than having a pre-programmed network topology. Because of the limited electrical power available, nodes are built with power conservation in mind, and generally spend large amounts. Requirements of wireless LAN is Small in size and low power consumption, Concurrency–intensive operation, Diversity in design and usage.

Application of WSN are area monitoring, environmental monitoring, air quality monitoring, forest fire detection, water quality monitoring, green house monitoring, natural disaster prevention etc.

B .Node Replication Attack

Usually, the sensor networks are unattended and the sensor nodes are not equipped with the tamper-resistance hardware so that the adversary can capture one sensor node, fabricate many replicas having the same identity (ID) from the captured node, and then place these replicas back into the strategic positions in the network for further malicious activities. This is called as *node replication attack*. Since the credentials of replicas are all the clones from the captured nodes, the replicas can be considered as legitimate members of the network, which make detection difficult. From the security point of view, the node replication attack is considerably harmful to the networks, because having legitimate keys, the replicas controlled by the adversary can easily launch the insider attacks, without easily being detected [13]. Detecting replicas in static environments are not useful in identifying replicas in mobile environments. Static technique indicated in [12].

C. Mobile Sensor Network

Mobile sensor network means sensors become widely deployed, some sensors may be enhanced with mobility, Such mobile sensors may be more powerful and can re-charge themselves automatically. It becomes feasible and applicable. Detecting node replication in a mobile sensor network algorithm Proposed in [2].

II. LITERATURE REVIEW

In existing system node replication detection schemes depend primarily on centralized mechanisms[1] with single points of failure, or on neighborhood voting protocols that fail to detect distributed replications. To overcome this limitations uses RM,LSM protocols proposed in [11] adopts Witness based scheme . Both protocols based on and seek to minimize power consumption by limiting communication, while still operating within the extremely limited memory capacity of typical sensor nodes. But it's storage cost high and high communication overhead. SDC and P-MPC [16] can be thought of as the cell versions of RM and LSM. Compared to RM and LSM, which forward location claims node by node, SDC and P-MPC forward location claims cell by cell.

RED protocol [3], [4] is more energy, memory, and computationally efficient and that it detects node replication attacks with higher probability. This protocol applicable for less number of routing nodes only. Next new effective and efficient scheme, called SET [5], to detect such clone attacks. The key idea of SET is to detect clones by computing set operations (intersection and union) of exclusive subsets in the network. First, SET securely forms exclusive unit subsets among one-hop neighbors in the network in a distributed way. This secure subset formation also provides the authentication of nodes' subset membership. SET is an appealing solution in sensor networks due to its efficiency and low communication overhead. Major disadvantage of this scheme is each sensor will be required to keep the unique fingerprint information, it cannot establish pair wise keys. To improve on the communication cost of the previous protocol, use

Deterministic multicast protocol [16] that only shares a node's location claim with a limited subset of deterministically chosen "witness" nodes. When a node broadcasts its location claim, its neighbors forward that claim to a subset of the nodes called witnesses. The witnesses are chosen as a function of the node's ID. If the adversary replicates a node, the witnesses will receive two different location claims for the same node ID. conflicting location claims become evidence to trigger the revocation of the replicated node. Unfortunately, all of the above methods are only for static sensor network, and are not useful if nodes have mobility.

Ho *et al.* [6] propose a centralized detection algorithm for mobile sensor networks using Sequential Probability Ratio Test. If we observe that a mobile node's speed is over the maximum speed, it is then highly likely that at least two nodes with the same identity are present in the network. Specifically, we perform the SPRT on every mobile node using a null hypothesis that the mobile node hasn't been replicated and an alternate hypothesis that it has. We show in this work how to configure upper and lower limits that allow the system to choose the right hypothesis for fast, accurate detection. Major drawback of this approach is Each time the maximum speed of the mobile node is not reached . The preliminary version [13] of this paper presents the first distributed detection algorithm for mobile networks based on a simple challenge-and-response strategy. Nevertheless, its detection effectiveness is vulnerable to the collusive replication TDD and SDD [12]provide high detection accuracy and excellent resilience against smart and colluding replicas, have no restriction on the number and distribution of replicas, and incur low communication/computation overhead.

Time synchronization is needed by almost all detection algorithms [3], [6], [11], [12], [13], [15]. Nevertheless, it is still a challenging task to synchronize the time of nodes in the network, even though loose time synchronization is sufficient or the detection purpose.. it would be desirable to remove this requirement. TinyECC[8],[9],[10] is to provide a ready-to-use, publicly available software package for ECC-based PKC [7] operations that can be flexibly configured and integrated into sensor network applications. many security services and protocols in traditional networks.

III. PROPOSED SYSTEM

our proposed localized algorithms(XED,EDD) [2] are used to detect node replication attacks in mobile sensor networks.
Advantages of our proposed algorithms include

- Localized Detection: localized algorithm is a particular type of distributed algorithm. Each node can communicate with only its one-hope neighbor. This characteristic is reducing the communication overhead significantly.
- Efficiency and Effectiveness: The XED and EDD algorithms can identify replicas with high detection accuracy.
- Network-Wide Revocation Avoidance: The revocation of the replicas can be performed by each node without flooding the entire network with the revocation messages.
- Time Synchronization Avoidance: The time of nodes in the network does not need to be synchronized.

A. XED

In localized algorithm[2] one sensor node meets another sensor node at an earlier time and sends a random number to at that time, then when and meet again, can ascertain whether this is the node met before by requesting the random number. Replicated node sends the newest random number. so we identify the replication node. Same strategy applied for all nodes in a sensor network. It consists of two steps, offline step and online step etc.

Offline Step :
It means procedure is executed before sensor deployment. It consists of $L_r^{(u)}$, $L_s^{(u)}$ are used to keep the received random numbers. $\mathcal{B}^{(u)}$ set representing the nodes having been blacklisted by u. $\mathcal{B}^{(u)}$ is initialized to be empty.
Online Step:
It means procedure is executed after sensor deployment. In this step to check received random number is same or not, same means choose α value for the genuine node otherwise consider as replicated node. This algorithm proposed in[2].
Algorithm : XED-On-line-Step
//This algorithm is performed by the node u at each time t
// v_1 …. v_d are the neighbors of u
//$\{ v_1 \ldots v_d \} \notin \mathcal{B}^{(u)}$
1. **Send** $L_r^{(u)}[v_1], \ldots, L_r^{(u)}[v_d]$ to v_1 …. v_d respectively
2. **Receive** $L_r^{(v1)}[u], \ldots, L_r^{(vd)}[u]$
3. for k = 1 to d
4. if $h(L_s^{(u)}[v_k]) = L_r^{(vk)}[u])$
5. Choose $\alpha \in [1, 2^b - 1]$ and set $L_s^{(u)}[v_k] = \alpha$
6.Calculate $h(\alpha)$ and send $h(\alpha)$ to v_k
7. else
8. Set $\mathcal{B}^{(u)} = \mathcal{B}^{(u)} \cup \{ v_k \}$

Description:
When u encounters v, it first checks if v is in the blacklist $\mathcal{B}^{(u)}$. This means that is considered a replica by u and v refuses to communicate with . If not, the following procedures are followed. They exchange the random numbers $L_r^{(u)}[v]$ and $L_r^{(v)}[u]$ .u checks if $L_r^{(v)}[u]$ is the random number u sent to v last time. This can be accomplished by verifying if $h(L_s^{(u)}[v]) = L_r^{(v)}[u]$ holds. Node v is added into $\mathcal{B}^{(u)}$ if the verification fails. Otherwise, the same procedure, including randomly generating a new α , computing $h(\alpha)$, sending to $h(\alpha)$, and replacing the old $L_r^{(u)}[v]$ with a new $L_r^{(u)}[v] = \alpha$, is performed. For the replica that does not possess the correct random number, due to the one way property of the cryptographic hash function, the probability of successful verification is only $1/2^b - 1$. The same procedure applies for node v.

XED algorithm cannot be useful multiple replicas are able to reply with the correct random number to encountered genuine nodes accordingly. This weakness will be solved in EDD algorithm.

B. EDD

EDD scheme is composed of two steps: an offline step and an online step.

Offline Step:

The offline step is performed before sensor deployment. In this algorithm[2] maximum number of times y_1 that node encounters a specific node V , should be limited with high probability during a fixed period of time, while the minimum number of times y_2 that encounters the replicas with the same ID v , should be larger than a threshold ψ during the same period of time. According to these observations, if each node can discriminate between these two cases, it has the ability to identify the replication.

Algorithm : EDD –Off-line-Step

1. Set T = 1 and $\mathcal{B}^{(u)} = \Phi$, u € [1,n]
2.set $L^{(u)}[i] = 0$, $1 \leq i \leq n$, u € [1,n]
3.**repeat**
4.T = T + 1
5.calculate μ_1 , μ_2 , σ_1^2 and σ_2^2
6.Set $y_1 = \mu_1 + 3\sigma_1^2$ and $y_2 = \mu_2 - 3\sigma_2^2$
7. until $y_1 < y_2$
8.Set $\psi = \frac{y2 - y1}{2}$

Description:

The array $L^{(u)}$ of length (n-1) is used to store the number of encounter with every other node in a given time interval. Set $\mathcal{B}^{(u)}$ contains the IDs having been considered by u as replicas. Let μ_1 and μ_2 be the expected number of encounters with the genuine and replication nodes . Let σ_1^2 and σ_2^2 be the corresponding variances of genuine and replication nodes. Calculate μ_1 and μ_2. Here, an intrinsic assumption for the calculation of y_1 and y_2 is that the random variables representing the number of encounters with genuine nodes and replicas are Gaussian distributed. Since the length T of the time interval is positively proportional to both the time required to detect the replicas and to the storage overhead. T is required to be the smallest value where each node can distinguish the replicas from the genuine nodes. i.e. $y_1 < y_2$. Now set threshold ψ used for discrimination between the genuine node and replication node.

Online Step:

Threshold value is calculated for each node in EDD offline step. In online step ,Once again to check each node greater than threshold value means that node will be added into the blacklist. Otherwise consider as genuine node.

Algorithm: EDD-On-line- Step

//This algorithm is performed by the node u at each time t
// v_1 …. v_d are the neighbors of u
// $\{ v_1 \ldots v_d \} \notin \mathcal{B}^{(u)}$
1.broadcast beacon b_u // b_u = (u) contains the ID of u
2.if $t \neq t_0$
3. receive beacons $b_{v1}, \ldots\ldots\ldots b_{vd}$
4.for k = 1 to d
5. $L^{(u)}[v_k] = L^{(u)}[v_k] + 1$
6. if $L^{(u)}[v_k] > \psi$ then set $\mathcal{B}^{(u)} = \mathcal{B}^{(u)} \cup \{ v_k \}$
7. else // $t \neq t_0$
8. Set $L^{(u)}[v_k] = 0$, k = 1 , ……, n

Description:

Each node locally maintains a counter t to record the elapsed time after the beginning of each time interval. After T time units is reached, i.e. t > T , the counter t should be reset. we simply use " $t = t_0$ " to represent that the time being considered is the beginning of a new time interval. Every time a node encounters another node, the corresponding value in the list $L^{(u)}[v]$ is increased by 1. The node v can be blacklisted by u at any time as long as $L^{(u)}[v]$ is above the threshold ψ . It is highly unlikely that the number of encounters with the genuine node will be larger than ψ. Blacklist contains set of replication nodes.

IV. SIMULATION RESULTS

Our proposed algorithm was implemented in TCL(Tool Command Language) and runs on NS2.There are 3 modules are implemented.

1. Find Clustering head

Several sensor nodes are dispersed in a network. Fig 6.1. Shows the group of nodes forms cluster. Determine cluster head in an network

2. Identify nodes in a XED Blacklist

In each cluster having attacker node and malicious node. Split the attacker list and malicious list. Attacker list having attacker nodes. and Malicious list having malicious nodes. We are applying XED algorithm online step to form blacklist. It contains attacker nodes.

3. Find EDD Online Vote list

Depends upon no of votes for each node to split the attacker list and malicious list .After EDD online step are applied to forms blacklist contains nodes it should be larger than threshold value. This is the final black list.

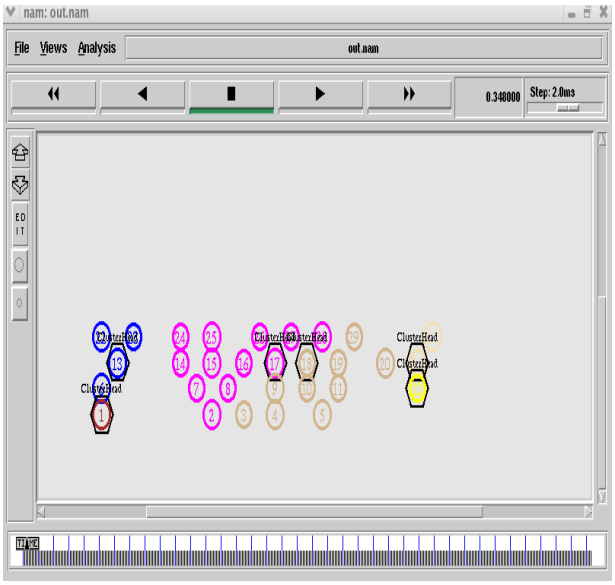


Fig.4.1 Detecting clustering head in a sensor network

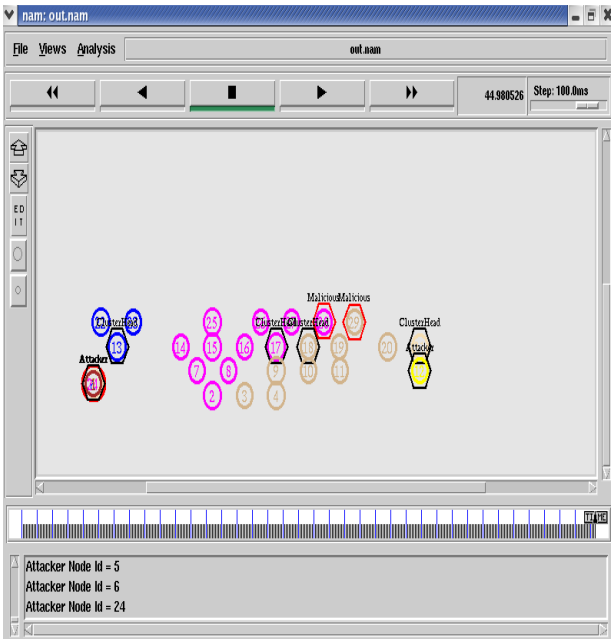


Fig.4.3 Node repositioning after forming final blacklist using EDD

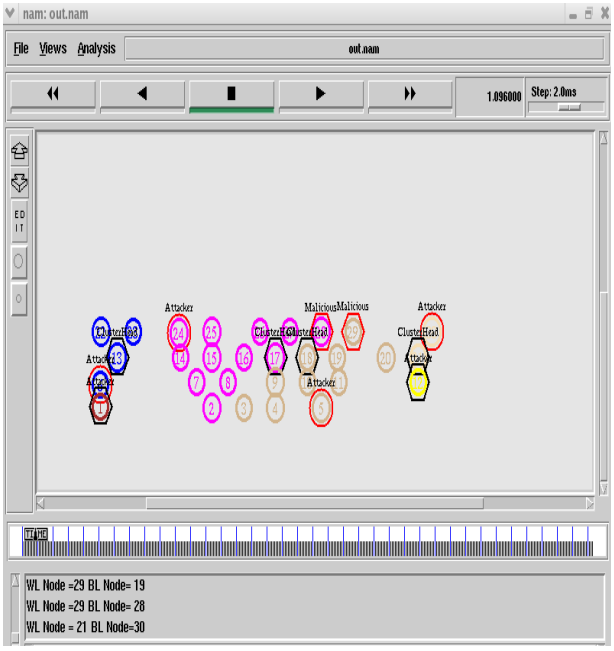


Fig.4.2 Detecting attacker and malicious nodes using XED online step

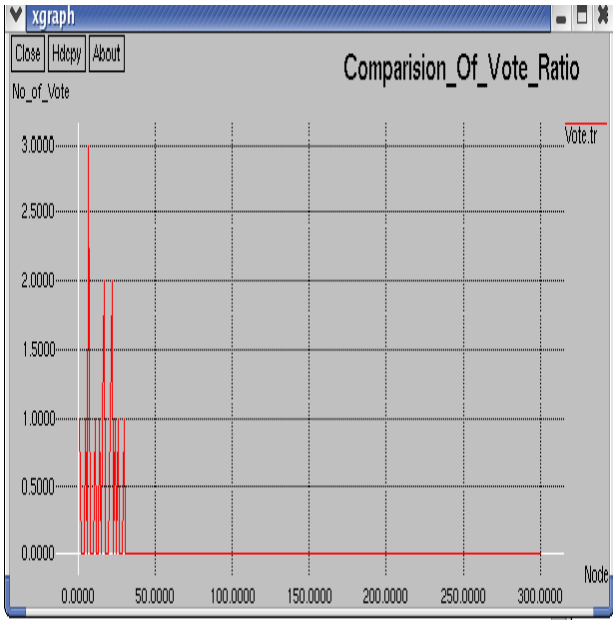


Fig. 4.4 Comparision of vote ratio

To take EDD online vote list .Find comparison of no of votes for all nodes as shown in Fig.4.4. Node may be a attacker Node, malicious node.

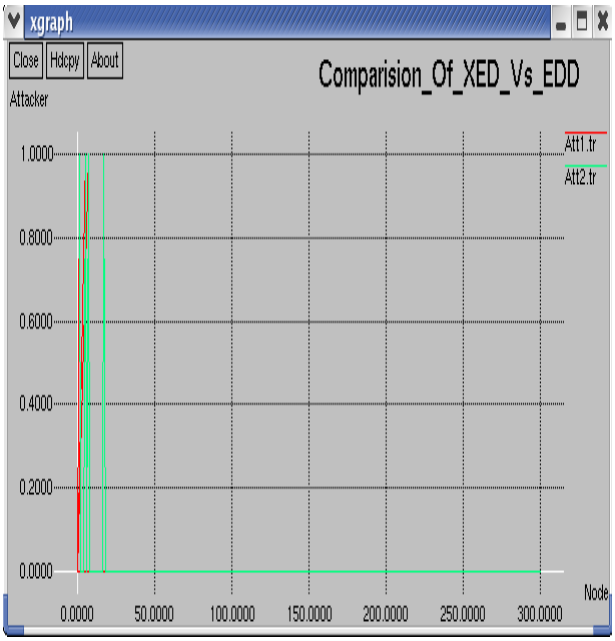


Fig.4.5 Comparison of XED Vs EDD algorithm attacker nodes

We are applying XED, EDD algorithm to find attacker nodes and compare that node as shown in Fig.4.5

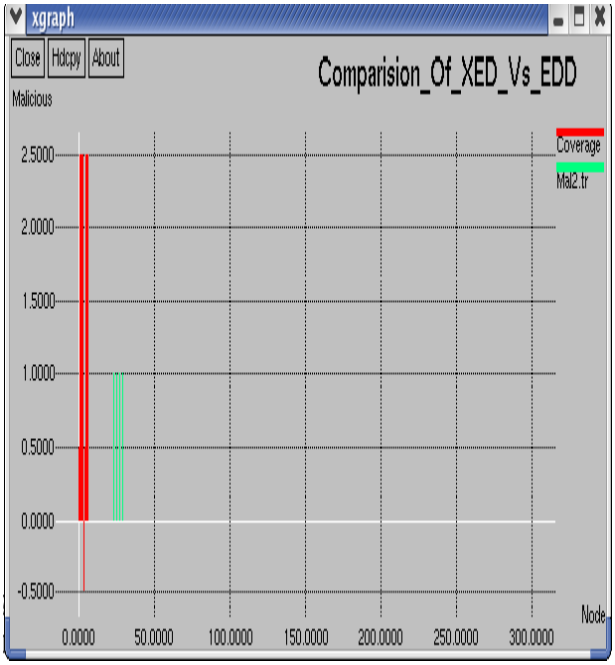


Fig.4.6 Comparision of XED Vs EDD algorithm malicious nodes, Coverage

We are using XED , EDD algorithm to split attacker list and malicious list. Compare malicious nodes with coverage as shown in Fig.4.6

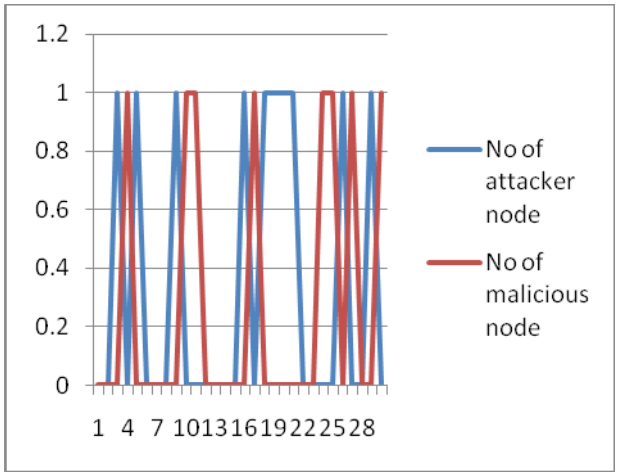


Fig4.7 Comparision of attacker nodes and malicious nodes using XED algorithm

XED algorithm is used to form blacklist. In Blacklist contains attacker nodes.Compare the no of attacker node,malicious node as shown in Fig.4.7.

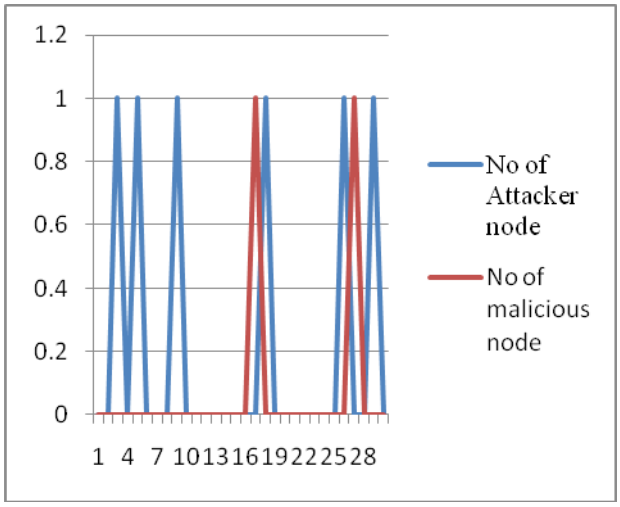


Fig.4.8 Comparision of attacker nodes and malicious nodes using EDD Algorithm

EDD algorithm is used to form final blacklist.It verify the attacker and malicious list based on votelist.Compare the no of attacker node,malicious node as shown in Fig.4.8.

V. CONCLUSION

In this paper, two replica detection algorithms for mobile sensor networks, XED and EDD[2] are proposed. Although XED is not resilient against collusive replicas, its detection framework, challenge-and-response, is considered novel as compared with the existing algorithms. Notably, with the novel encounter-number detection approach, which is fundamentally different from those used in the existing algorithms, EDD not only achieves balance among storage, computation, and communication overheads [2].In future more concentrates on the node security.

REFERENCES :

[1] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proceedings of IEEE Symposium on Security and Privacy*, May 2003.

[2] Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu and Sy-Yen Kuo,"Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks,IEEE transaction on Information Foresics and security , vol.8,No.5,May2013.

[3] M. Conti, R.Di Pietro, L. V. Mancini, andA.Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in *Proc. ACMInt. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc)*, Montreal, Canada, 2007, pp. 80–89.

[4] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," *IEEE Trans. Depend. Secure Comput.*, vol. 8, no. 5, pp. 685–698, Sep./Oct. 2011.

[5] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in *Proc. Int. ICST Conf. Security and Privacy in Communication Networks (Securecomm)*, Nice, France, 2007, pp. 341–350.

[6] J. Ho,M.Wright, and S. K. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis," in *Proc. IEEE Int. Conf. Computer Communications (INFOCOM)*, Brazil, 2009, pp. 1773–1781.

[7] S. Kent and R. Atkinson. IP authentication header. IETF RFC 2402, November 1998.

[8] A.Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in *Proc. Int. Conf. Information Processing in Sensor Networks (IPSN)*, Missouri, USA, 2008, pp.245–256.

[9] D. J. Malan, M. Welsh, and M. D. Smith, "Implementing public-key infrastructure for sensor networks," *ACM Trans. Sensor Network*, vol.4, no. 4, pp. 1–23, 2008.

[10] J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil attack in sensor networks: Analysis and defenses. In *Proceedings of IEEE Conference on Information Processing in Sensor Networks (IPSN)*, Apr. 2004.

[11] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE Symp. Security andPrivacy (S&P)*, Oakland, CA, USA, 2005, pp. 49–63.

[12] K. Xing and X. Cheng, "From time domain to space domain: Detecting replica attacks in mobile ad hoc networks," in *Proc. IEEE Int. Conf. Computer Communications (INFOCOM)*, SanDiego,CA, USA, 2010, pp.1-9

[13] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Mobile sensor network resilient against node replication attacks," in *Proc. IEEE Conf. Sensor, Mesh, and Ad Hoc Communications and Networks (SECON)*, California, USA, 2008, pp. 597–599, (poster)

[14] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Efficient and distributed detection of node replication attacks in mobile sensor networks," in *Proc. IEEE Vehicular Technology Conf. Fall (VTC-Fall)*, Anchorage, AK, USA,2009, pp. 1–5.

[15] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," *IEEE J.Sel. Areas Commun.*, vol. 28, no. 5, pp. 677–691, Jun. 2010.

[16] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient Distributed Detection of Node Replication Attacks in Sensor Networks," *ACSAC*, 2007.

VERTICAL HANDOFF DECISION AND MERIT NETWORK SELECTION ACROSS HETEROGENEOUS WIRELESS NETWORKS

Hari Nainyar Pillai. C*, Dr. Arun. E**,

naresh.hari180@gmail.com , arun@gmail.com

***Abstract*— Next generation wireless networks must be able to coordinate services between heterogeneous networks through multi-mode mobile terminals. Such heterogeneity poses a challenge to seamless handover since each access network has different operations. In this paper, the policies of multiple metrics for handoff to permit connectivity across UMTS and WLAN/WiMAX are designed. Moreover, how to select an optimal target network is an important issue to balance against the network condition and user preference. The considered metrics for hand off initiation include the predicted received signal strength (RSS) of neighbor networks and dwell time. The RSS is predicted by back propagation neural network which is beneficial to perform handoff early. Dwell time value depends on the user speed and moving pattern. The policy for triggering a handoff is that the RSS conditions are consistently true during dwell time. Policies in the merit function are presented to select an optimal network. The weighting factors in the merit functions are dynamic to neighbor networks.**

1. INTRODUCTION

A significant challenge for fourth generation (4G) wireless networks is to coordinated different types of existing networks as depicted. This provides users with a wide range of services across different media through a single mobile terminal.

* II Year M.E CSE ,Ponjesly College of Engineering

**Professor, CSE, Ponjesly College of Engineering.

For example, characteristics of 802.11 WLAN, 802.16 WiMAX and 3G cellular such as UMTS can be complementary. Each network characteristics are summarized. This universal wireless access requires the design of intelligent vertical handoff decision algorithms to allow the device to receive services even as it moves between different network access points. Currently, there are various standardization bodies include the 3GPP, 3GGP2 and the IEEE 802.21 MIH Working Group. IEEE 802.21 provides the protocols to support cross layer interaction but it does not consider factors to efficiently make handoff initiation and find an optimal target network.

Cellular systems exploit the fact that the power of a transmitted signal falls off with distance, the same frequency channel can be allocated to users at spatially-separate locations with minimal interference. A cellular system divides a geographical area into adjacent, non-overlapping “cells.” Cells assigned the same channel set are spaced apart so that interference between them is small.

Each cell has a centralized transmitter and receiver (called a base station) that communicates with the mobile units in that cell, both for control purposes and as a call relay. All base stations have high-bandwidth connections to a mobile telephone switching office (MTSO), which is itself connected to the public-switched telephone network (PSTN). The handoff of mobile units crossing cell boundaries is typically handled by the MTSO, although in current systems some of this functionality is handled by the base

stations and/or mobile units. The original cellular system design was finalized in the late 1960's and deployed in the early 80's. The large and unexpected growth led to the development of digital cellular technology to increase capacity and improve performance.

Paging systems now allow a short digital message, including a phone number and brief text, to be sent to the page as well. In paging systems most of the complexity is built into the transmitters, so that pager receivers are small, lightweight, and have a long battery life. The network protocols are also very simple since broadcasting a message over all base stations requires no routing or handoff. The spectral inefficiency of these simultaneous broadcasts is compensated by limiting each message to be very short. Paging systems continue to evolve to expand their capabilities beyond very low-rate one-way communication.

Current systems are attempting to implement two-way, "answer-back" capability. This requires a major change in pager design, since it must now transmit signals in addition to receiving them, and the transmission distances can be quite large. Uncontrollable development of wireless and mobile communication technology aims to provide the seamless continuous connection to access various wireless technologies and to have connection with the best network which provides the best quality of service (QoS). Each application requires different QoS, so the network selection may vary accordingly. To achieve this goal and to select the best network for a mobile terminal when moving from one network to another, it is necessary to have a good decision making algorithm which decides the best network for a specific application that the user needs based on QoS parameter. This paper presents an overview of handoff types, handoff process, and classification of vertical handoff, parameters required, existing work and the comparison table.

The proposed system consists of two steps:

1) Receive signal strength(RSS) prediction by propagation.
2) Vertical Handoff Algorithms and Target Network Selection.

2. RECEIVE SIGNAL STRENGTH PREDICTION BY PROPAGATION.

Received Signal Strength (RSS) is used to help a mobile node know whether it moves closer to or away from the monitored network. By comparing the strength of the predicted RSS of each neighbor network, it can assist to find the target network that the mobile node is moving in the overlap area. Also Dewell time the traditional handoff decision policy which is based on RSS, hysteresis and threshold can cause a serious ping-pong effect.

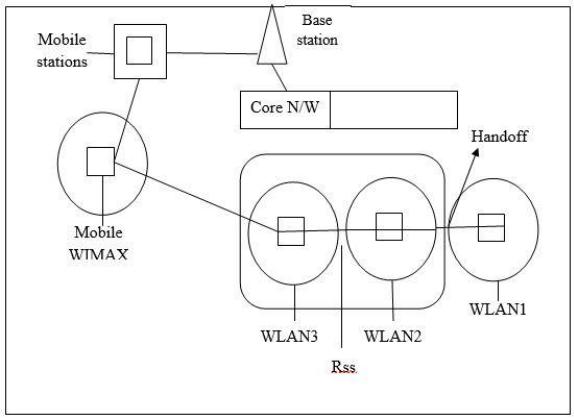


Fig 1. Architecture Diagram.

By comparing the strength of the predicted RSS of each neighbor network, it can assist to find the target network that the mobile node is moving in the overlap area. a mobile node is moving from network 1 toward either network 2 or 3. The strength of predicted RSS can assist to find the target

network that is moving in the overlap area. Knowing RSS of neighbor networks ahead of time and if the current RSS of the serving network is lower than the threshold, then the mobile node can performs handoff early. Thus, it results in a better connection quality and a low dropping probability as well while it moves in the overlap area. We use the back-propagation training algorithm for a two layer network to predict the future RSS.

2.1 Dwell Time

The traditional handoff decision policy which is based on RSS, hysteresis and threshold can cause a serious ping-pong effect. To alleviate handoffs evoked too frequently, handoff would be performed if the conditions continue to be true until the timer expires. Dwell time is used as a timer which is adjusted according to the movement of the mobile node. The dwell time should be extended if the movement direction is irregular.

3.VERTICAL HANDOFF ALGORITHM AND TARGET NETWORK SELECTION.

Our proposed vertical handoff algorithm between UMTS and WLAN/WiMAX networks. The handoff policy for non-real time service is to attempt to connect WLAN/WiMAX as long as possible due to higher data rate provided. The preferred handoff point for non-real time services is the first time the PRSS from WLAN/WiMAX reaches an acceptable level. For real time applications (e.g. Voice over IP), handoff should be performed as rapid as possible in order to minimize the delay.

3.1 Handoff from UMTS to WLAN /WiMAX.

The downward vertical handoff algorithm which a mobile node using services in UMTS network could always enter to WLAN/WiMAX to obtain a higher QoS at a less cost. Each step has the following policies.

1. The preferred handoff point for non-real time services is the first time the PRSS from WLAN/WiMAX PRSSW reaches an acceptable level.

2. The preferred handoff point for real time services is the last time the PRSSW reaches the acceptable level.

3. If one of above two policies is true, we continue to check the condition. If the condition fails before the dwell timer expires, the handoff process is reset, otherwise go on.

4. 4. In this step, the RSS of a mobile received from WLAN/WiMAX is being increase. Then, we check if the mobile node is moving out of the coverage UMTS network by where RSSUMTS is the RSS that the mobile node receives from the UMTS base station, and RSSth, UMTS is the RSS threshold in the UMTS network.

5. The network with the largest merit value among the candidates is selected as the target network

3.2 Handoff from WLAN/WiMAX to UMTS or to another WLAN/WiMAX.

When a mobile node stays in WLAN/WiMAX, the policies to decide whether a handoff is performed are as follows:

1) The preferred handoff point for non-real time services is the last time the RSS in the serving WLAN/WiMAX network RSSserv,W falls below the acceptable level.

2) The preferred handoff point for real time service is the first time the RSSserv,W degrades to the threshold RSS values.

3) In this step, RSSserv,W becomes weak. Find out candidate networks that have strong PRSS last for the dwell time duration by PRSStarg.

4) The handoff should now be triggered. The candidate networks are the networks having strong RSS and the merit function more than zero.

4. PERFORMANCE EVALUATION

The heterogeneous wireless networks consist of UMTS, WLAN and WiMAX overlaid. The mobility of a mobile node is fixed according to the path from point A to point D. The user speed is constant at 5m/s. The service is running at 64 kbps. The selected network at each point has the largest Fn.

The vertical handoff occurred at location A is from UMTS to WiMAX1. Thus, the Fn value of WiMAX1 is more than that of UMTS. At the location B, there are three networks available but WLAN1 is the optimal target network. WLAN1 has the largest Fn value due to the policy to prolong the time users stay in WLAN. Between UMTS and WiMAX2, WiMAX2 is the selected target network when the mobile node is moving out WLAN1 at location C.

Consider the last location D where the mobile node is going from WLAN2 to WLAN3. Accordingly, WLAN3 is the correct target network and has the highest Fn. The results indicate that the proposed PRSS+ Merit approach can trigger handoff if needed and choose the optimum target network as well. The hysteresis margin (H) between WLAN/WiMAX and UMTS is 10 dBm and threshold (T) in UMTS is -107 dBm and threshold (T) in WLAN/WiMAX is -102 dBm.

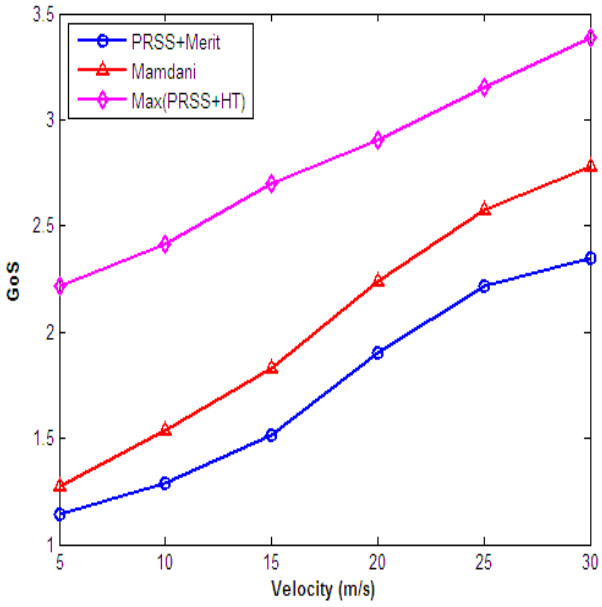


Fig 2. Handoff Decision Performance

In case of UMTS-to-WLAN/WiMAX handoff, the distances are 37, 52, 75 meters by using PRSS+Merit, Mamdani and Max(PRSS+HT) methods, respectively. The PRSS+Merit algorithm decides to handoff before other methods.

Moreover, the PRSS+Merit algorithm early hand offed the mobile node before the location E where is the boundary of entering the WLAN1. The distance between the location E and the initial point is 50 meters. In the second handoff from WLAN/WiMAX-to-another WLAN/WiMAX network, the results can be analyzed similar to the first handoff.

5. CONCLUSION

I proposed the vertical handoff decision algorithm enabled by the policies of

the handoff metrics. The handoff policies are different when a mobile node stays in UMTS and WLAN/WiMAX networks. To predict a mobile node is moving away from the monitored wireless networks, the PRSS is obtained by the back propagation neural network. Dwell time depending on the mobile node movement is used to check the continuity of the RSS conditions to be true long enough. After handoff is triggered, the network is selected by the largest merit value. The weights in the merit function are dynamic to the changes of the metrics values. The proposed policy-enabled vertical handoff and network selection outperforms other two approaches in reducing the number of vertical handoffs, probabilities of call dropping, GoS and increasing the utilization of WLAN networks.

REFERENCES

[1] J. McNair and M. Fang, "Vertical Handoffs in Fourth-Generation Multi network Environments", *IEEE Wireless Communications, Vol. 11, No. 3*, pp. 8-15, 2004.

[2] M. Kassar, B. Kervella. and G. Pujolle. "An Overview of Vertical Handover Decision Strategies in Heterogeneous Wireless Networks", *Computer Communications, Vol. 31*, pp. 2607-2620, 2008.

[3] V. Kumar, and N. Tyagi "Media Independent Handover for Seamless Mobility" in IEEE 802.11 and UMTS based on IEEE 802.21, *3rd IEEE International Conference on Computer Science and Information Technology,* , pp. 474-479, 2010.

[4] Wang, K. Katz, and R. Giese. "Policy-Enabled Handoffs Across Heterogeneous Wireless Networks" *2nd IEEE Workshop on Mobile Computing Systems and Applications Proceeding,* , pp. 51-60, 1999.

[5] L. Xia , J. Ling-ge, H. Chen . and Hong-wei J. "An Intelligent Vertical Handoff Algorithm in Heterogeneous Wireless Networks," International Conference on Neural Networks and Signal Processing", pp. 550 – 555, 2008.

AN EFFECTIVE INTRUSION DETECTION SYSTEM FOR MANET

M.Kalai Selvi
PG Scholar
Infant Jesus College of Engineering
Thoothukudi.
Email:kalaisree90@gmail.com

Dr.S.Allwin, M.E., Ph.D.
Associate professor
Infant Jesus College of Engineering
Thoothukudi.
Email:allwinstephen@gmail.com

***ABSTRACT*- MANET is a self-configuring infrastructure network of mobile devices connected by wireless network it equipped with both a wireless transmitter and a receiver that communicate each other bidirectional wireless either directly or indirectly. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches.**

***Index term*—** Digital Signature, digital signature algorithm (DSA), Enhanced Adaptive Acknowledgment (AACK) (EAACK), Mobile Ad hoc Network (MANET).

I. INTRODUCTION

DUE TO THEIR natural mobility and scalability, wireless networks are always preferred since the first day of their invention. By definition, Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET is capable of creating aself-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations.

Considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious attackers can easily compromise MANETs by inserting malicious or no cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS).

A. Problem Definition

Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision.In this section, we discuss these three weaknesses in detail. In a typical example of receiver collisions after node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such case, node A overhears that node B has successfully forwarded Packet 1 to node C but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.In the case of limited transmission power, in order to preserve its own battery resources, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong enough to be received by node C. For false misbehavior report, although node A successfully overheard that node B forwarded Packet 1 to node C, node A still reported node B as misbehaving. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one

or two nodes to achieve this false misbehavior report attack. As discussed in previous sections, TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehavior attack. In this research work, our goal is to propose new IDS specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false misbehavior problem.

A. Receiver Collisions

In a typical example of receiver collisions, after node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such case, node A overhears that node B has successfully forwarded Packet 1 to node C but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

B. Limited Transmission Power

In this case of limited transmission power, in order to preserve its own battery resources, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong enough to be received by node C.

C. False Misbehavior Report

For false misbehavior report, although node A successfully overheard that node B forwarded Packet 1 to node C, node A still reported node B as misbehaving, as shown in Fig. 6. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack.

As discussed in previous sections, TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehavior attack. In this research work, our goal is to propose new IDS specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false misbehavior problem. Furthermore, we extend our research to adopt a digital signature scheme during the packet transmission process. As in all acknowledgment-based IDSs, it is vital to ensure the integrity and authenticity of all acknowledgment packets.

II. RELATED WORK

Wireless communication represents a major industrial stake in the coming years. It offers numerous usages and helps industry save operating costs as well as improving operational efficiency. WiFi (IEEE 802.11 WLANs) and Bluetooth technologies (IEEE 802.15-WPANs) have known tremendous development and have penetrated small office and home office as well as large enterprise office. These general-public wireless technologies may find their limited usage in industrial installations because of harsh environments, electromagnetic compatibility and interference issues, safety and information technology (IT) security constraints, and battery autonomy. The Optimization of Communication for Ad hoc Reliable Industrial networks (OCARI) project in which we try to develop a wireless sensor communication module running an industrial ad hoc mesh networking protocol.

MANETs not only introduces new security concerns but also exacerbates the problem of detecting and preventing aberrant behavior. Existing ID for MANETs capitalize on the collaborate nature of mobile ad-hoc routing. Research also revealed that the routing protocols typically employed by mobile ad-hoc networks lack sufficient functionality to enable robust m, hence we have added modules that provide the necessary functionality. First property is that each node in the net1l'Ork maintains a list containing the addresses of those nodes with which it is in immediate proximity or on the path from a source to a destination. Tile notion of "snooping" is also employed in DSR, which is used for "reflecting shorter routes" as an optimization of the route maintenance process.

The routing protocol is to have an efficient route establishment between a pair of nodes, so that messages can be delivered in a timely manner. Bandwidth and power constraints are the important factors to be considered in current wireless network because multi-hop ad-hoc wireless relies on each node in the network to act as a router and packet forwarder. Routing protocols used in wired network cannot be used for mobile ad-hoc networks because of node mobility. The ad-hoc routing protocols are divided into two classes: table driven and demand based. This paper reviews and discusses routing protocol belonging to each category. The most important wireless communication mechanisms among all. MANET does not have a fixed infrastructure, every single node in the network works as both a receiver and a transmitter. MANET does not require any fixed infrastructure and it is capable of self configuring, these unique characteristics made MANET ideal to be deployed in a remote or mission critical area like military use or remote exploration. Open medium and wide distribution of nodes in MANET leave it vulnerable to various means of attacks.

Mobile wireless ad hoc networks have different characteristics from wired networks and even from standard wireless networks, there are new challenges related to security issues that need to be addressed. The node that is overhearing and reporting itself is malicious, and then it can cause serious impact on network performance**.** The proposed system is its ability to discover malicious nodes which can

partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network.

Piezoelectric materials become a strong candidate for energy generation and storage in future applications**.** The use of piezoelectric polymers in order to harvest energy from people walking and the fabrication of a shoe capable of generating and accumulating the energy.

The electronics needed to increase energy transfer and storage efficiency. Circuit operates stand-alone, and it extracts the piezoelectric strain energy independent of the load and piezoelectric parameters without using any external sensor. Controller uses the piezoelectric voltage as a feedback and regulates the rectified voltage to adaptively improve the extracted power. The simplicity of the circuit facilitates the development of efficient piezoelectric energy harvesters for low-power applications such as wireless sensors and portable devices.

The problem of incorporating security mechanisms into routing protocols for ad hoc networks. Canned security solutions like IPSec are not applicable. Develop a security mechanism to protect its routing information. We also briefly discuss whether our techniques would also be applicable to other similar routing protocols and about how a key management scheme could be used in conjunction with the solution that we provide.

Efficient water management is a major concern in many cropping systems in semiarid and arid areas. Describes details of the design and instrumentation of variable rate irrigation, a wireless sensor network, and software for real-time in-field sensing and control of a site-specific precision linear-move irrigation system. Communication signals from the sensor network and irrigation controller to the base station were successfully interfaced using low-cost Bluetooth wireless radio communication.

Propose a methodology for optimizing a solar harvester with maximum power point tracking for self-powered wireless sensor network (WSN) nodes. Maximizing the harvester's efficiency in transferring energy from the solar panel to the energy storing device. The instantaneous power collected by the panel helping the harvester design and optimization procedure. Detailed modeling of the harvester is proposed to understand basic harvester behavior and optimize the circuit. Experimental results based on the presented design guidelines demonstrate the effectiveness of the adopted methodology.

III. INTRUSION DETECTION SYSTEM IN MANET'S

As discussed before, due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, IDS should be added to enhance the security level of MANETs. If MANET can detect able to completely eliminate the potential damages caused by compromised nodes at the first time. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK, and Adaptive Acknowledgment (AACK).

A. Watchdog

Watchdog proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater.Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold the Watchdog node reports it as misbehaving. In this case, the Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field.

Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme .Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions;3) limited transmission power; 4) false misbehavior report;5) collusion; and 6) partial dropping.

B. TWOACK

With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed is one of the most important approaches among them. On the contrary to many other schemes, TWOACK is neither an enhancement nor aWatchdog-based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination.

Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic

Source Routing (DSR) . The working process of TWOACK is shown in Fig. 1: Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same process applies to every three consecutive nodes along the rest of the route.

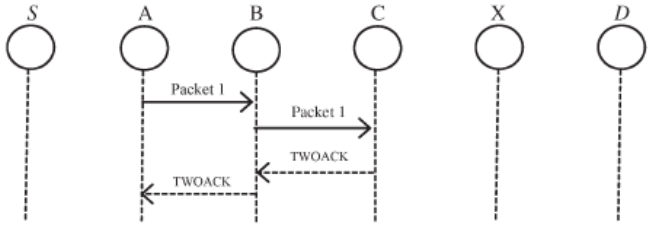


Fig 1 TWOACK Scheme

The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network. However, many research studies are working in energy harvesting to deal with this problem.

C. AACK

Based on TWOACK, proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. In the ACK scheme shown in Fig. 2, the source node S sends out Packet 1 without any overhead except 2 b of flag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

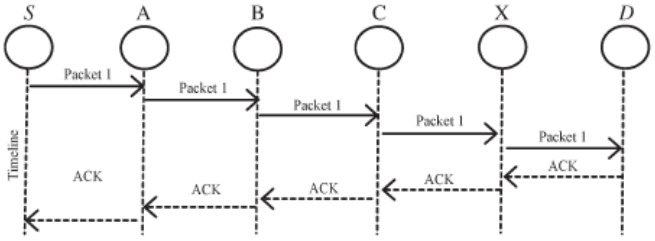


Fig 2 ACK Scheme

In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this concern, we adopt a digital signature in our proposed scheme named Enhanced AACK (EAACK).

D. Digital Signatures

Digital signatures have always been an integral part of cryptography in history. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. The development of cryptography technique has a long and fascinating history.

The security in MANETs is defined as a combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and nonrepudiation. Digital signature is a widely adopted approach to ensure the authentication, integrity, and nonrepudiation of MANETs. It can be generalized as a data string, which associates a message (in digital form) with some originating entity, or an electronic analog of a written signature. Digital signature schemes can be mainly divided into the following two categories. 1) Digital signature with appendix: The original message is required in the signature verification algorithm. Examples include a digital signature algorithm (DSA) .*2)* Digital signature with message recovery: This type of scheme does not require any other information besides the signature itself in the verification process. Examples include RSA.

IV. SCHEME DESCRIPTION

In this section, we describe our proposed EAACK scheme in detail. We extend it with the introduction of digital signature to prevent the attacker from forging acknowledgment packets. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior

report authentication (MRA). Distinguish different packet. types in different sche Distinguish different packet types in different schemes, we included a 2-b packet header in EAACK. Each communication process,both the source node and the destination node are not malicious.

A. ACK

ACK is basically an end-to-end acknowledgment scheme. Part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. The packet transmission from node S to node D is successful. The packet transmission from node S to node D is successful.

B. S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al.* Three consecutive nodes work in a group to detect misbehaving nodes. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

C. MRA

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

D. Digital Signature

EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted.

V. CONCLUSION

The per node throughput capacity of MANET is determined by adjusting the transmission range and limiting the packet redundancy. Transmission power of each node is manipulated to amend to specified transmission range and limited packet redundancy limit. Increasing the transmission power increases the throughput capacity. This in turn increases the life time of the network. The optimized throughput capacity of each node is determined which helps in delivering the packets efficiently in the dynamic network topology.

REFERENCES

[1] Al Agha.K, Bertin.M.-H, Dang.T, Guitton.A, Minet.P, Val.T, and Viollet.J.-B, (2009) "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[2] Jayakumar.G and Gopinath.G, (2007) "*Ad hoc* mobile wireless networks routing protocol—A review," *J. Comput. Sci.*, vol. 3, no. 8, pp. 574–582, 2007.

[3] Kang.N, Shakshuki.E, and Sheltami.T, (2011) "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis,Singapore, Mar. 22–25, 2011, pp. 488–494.

[4] Kim.Y, (2008) "Remote sensing and control of an irrigation system using a distributed wireless sensor network," *IEEE Trans. Instrum.Meas.*, vol. 57,no. 7, pp. 1379–1387, Jul. 2008.

[5] Nasser.N and Chen.Y, (2007)"Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in *Proc. IEEE Int.Conf. Commun.* Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[6] Parker.J,Undercoffer.J, Pinkston.J, and Joshi.A, (2004) "On intrusion detection and response for mobile ad hoc networks," in *Proc. IEEE Int. Conf.*Perform., Comput., Commun., 2004, pp. 747–752.

[7] Rocha.J.G, Goncalves.L.M, Rocha.P.F, Silva.M.P, and Lanceros-Mendez.S, (2010) "Energy harvesting from piezoelectric materials fully integrated in footwear," *IEEE Trans. Ind. Electron.*, vol. 57, no. 3, pp. 813–819, Mar. 2010.

[8] Tabesh. A and Frechette.L.G, (2010)"A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," *IEEE Trans. Ind. Electron.* vol. 57, no. 3, pp. 840–849, Mar. 2010.

[9] Zapata.M and Asokan.N, (2002) "Securing *ad hoc* routing protocols," in *Proc.*ACM Workshop Wireless Secur, 2002, pp. 1–10.

Efficient Video Transmission over Mobile Ad Hoc Network Using Priority Scheduling Algorithm

D. Mano Abraham [1], S.P. Tamizhselvi [2]
Department of Computer Science and Engineering,
College of Engineering, Guindy, Anna University Chennai
[1] manoabraham@ymail.com
[2] tamizh8306@gmail.com

***Abstract*- Mobile ad hoc networks (MANETs) are becoming more essential to wireless communications due to growing popularity of mobile devices. However, MANETs do not seem to effectively support multimedia applications and especially video transmission. This paper presents a cross-layer mechanism for efficient video transmission over this type of networks. The proposed mechanism consists of a priority-scheduling algorithm, at the network layer, and the use of the IEEE 802.11e standard at the MAC layer. The priority-scheduling algorithm takes into account the frame type of the MPEG-4 video file in order to provide different priorities to the most important video packets. At the MAC layer, the IEEE 802.11e protocol assigns the highest priority to video applications to reduce delay and packets losses due to other competing traffic. This design is easily implemented in any ad hoc wireless network as an extension on the AODV MANET routing protocol. Simulation results conducted with the network simulator ns-2 show the advantages of the proposed design.**

I. INTRODUCTION

Mobile Ad hoc NETworks (MANETs) are becoming more essential to wireless communications due to growing popularity of mobile devices. A node in MANETs could act as a router while having also the possibility of being the sender or receiver of information. The ability of MANETs to be self-configured and form a mobile mesh network by using wireless links make them very suitable for a number of cases that other type of networks cannot operate. Although, node mobility is a very useful feature for users, it results in a very dynamic topology in which routing can become a very complicated task. An important usage scenario of MANETs could be a disaster area or any kind of emergency, in which the fixed infrastructure has been destroyed or is very limited. However, one major key issue related to multimedia applications is how to guarantee an acceptable level of Quality of Service (QoS) to the end users. In MANETs, the challenges are even higher due to known limitations of the wireless medium and the frequent link failures, as mobile nodes move independently. Over the last few years, new protocols were designed and standardized in an effort to increase the transmission rates of the wireless medium. The IEEE 802.11e protocol [1] with QoS enhancements is an international standard that is already implemented in MAC chipsets by a number of vendors. The efforts for the enhancements of the IEEE 802.11 protocol aim at creating a wireless environment in which, data transmission can be achieved at higher bit rates and longer distances while meeting the QoS criteria posed by applications with delay constrains, like multimedia transmission.

A second major issue in wireless ad hoc networks is related to efficient routing in an environment in which the network topology dynamically changes over time. Over the last years, a sufficient number of routing protocols have been developed by the research community. Each protocol has its own routing strategy and its performance varies depending on network conditions like the density of nodes in a specific area, their speed and direction. Most of these protocols do not take into account the limitations and the special requirements posed by the served applications.

In [2], the effects of various mobility models on the performance of Dynamic Source Routing (DSR) [3] and Ad Hoc On-Demand Distance Vector (AODV) [4] routing protocols are studied. The experimental results illustrate that the performance of a routing protocol varies across different mobility models, node densities and the length of data paths.

Another performance evaluation of three widely used MANET routing protocols (Destination-Sequenced Distance Vector DSDV [5], AODV and DSR) with respect to group and entity mobility models is presented in [6]. Simulation results indicate also that the relative ranking of routing protocols may vary, depending on the mobility model.

In [7], a QoS-aware self-configured adaptive framework is presented to provide video-streaming services over MANETs. The routing algorithm periodically updates a set of paths, classifies them according to a set of metrics, and arranges a multipath-forwarding scheme. This proposal operates in a different way under highly

dynamic states than under more static situations, seeking to decrease the probability of having broken links and improving the service performance, while using lower signaling overhead.

Matinetal. [8] Addresses the use of multi-hop as an alternative to conventional single hop transmission in order to increase the quality of real time video streaming over MANETs. The use of the IEEE 802.11e Enhanced Distributed Channel Access (EDCA) function improves the overall performance of the high priority traffic in MANETs, by using the access control mechanisms of the MAC layer.

In [9], priority assignment mechanisms are considered for implementing priority treatment of packets in a MANET using the DSR routing protocol based on a modified IEEE 802.11 MAC layer operating in the distributed mode. The mechanism includes priority queuing and several methods for providing important messages an advantage in contenting for channel access. In [10] an integrated cross-layer optimization algorithm is proposed in order to maximize the decoded video quality in a multi-hop wireless mesh network with QoS guarantees. Finally, it is investigated in [11] whether or not the operating conditions in a city are likely to permit video streaming. It is found that AODV outperforms DSR over the Manhattan grid model.

In this paper, we focus on improving peer-to-peer communication in MANETs by supporting real-time multimedia transmission. The main idea is to exploit the multimedia coding information from the application layer and use a scheduling policy, so that the most important video packets enjoy the highest priority. At the MAC layer, traffic classes are treated in a different way based on QoS criteria. The proposed cross-layer mechanism introduces some modifications at the procedures of the AODV queuing system. AODV uses a simple First Input First Output (FIFO) queue for all incoming packets from the upper layer. Therefore, all packets are treated with the same way regardless of its importance or delay related constrains.

The applicability of our design can be found in applications with bandwidth, delay and jitter constraints, while keeping at a minimum level the requirements imposed by intermediate stations. The main contribution of this work is the cross-layer mechanism that combines the features of the IEEE 802.11e protocol with a video-based priority-scheduling algorithm. The novelty is also supported by choosing the Manhattan mobility model. Another important contribution is the mixture of network and video-centric metrics in an effort to better assess the video quality at the end user. The simulation results show that the proposed design improves QoS when compared with the performance of the legacy IEEE 802.11e protocol. The rest of the paper is organized as follows: In the next section, we present the overall architecture of the proposed cross-layer mechanism. Section III discusses the simulation environment and presents the evaluation results. We conclude the paper with notes for future work in Section IV.

II. Proposed Cross-Layer Mechanism

In this section, we describe the proposed cross-layer mechanism for video transmission over MANETs. We can distinguish two main areas in which, we prioritize traffic, depending on the importance of the transmitted packets:

- At the network layer, we apply a scheduling policy in which, each incoming packet from the upper layers receives different priority depending on the video frame type.
- At the MAC layer, we differentiate the access of the various applications, based on QoS criteria.

This design (Figure. 1) is based on the attributes of voice and video streaming applications, which are characterized by different tolerance in terms of end-to-end delay. It is obvious that a real time service, like video transmission, requires much less delay than a file transfer application. A way to maximize network performance is to prioritize traffic depending on traffic classes.

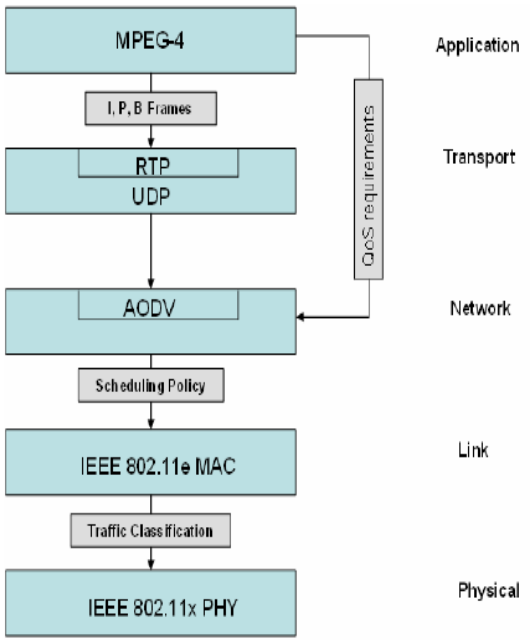


Figure 1. Cross-layer design

That means that a packet with higher priority should be treated completely differently from a packet with low priority in order to be delivered first. In highly loaded MANETs that usually consist

of a large number of nodes, or when the bandwidth is limited, there is a significant possibility for the transmitted packets to be dropped from the queues in the mobile nodes.

Priority Scheduling is a popular method for implementing priority queues. Each traffic class has its own queue, in which packets are ordered. This ordering affects directly the way that packets are served and removed from the queue. In the case of a queue that contains video packets the ordering is done by utilizing the frame type information and the assigned priority.

We consider the transmission of video files encoded by a MPEG-4 video encoder that generates three types of video frames. I-frames are the least compressed and contain information from encoding a still image. P-frames are more compressed than I-frames and encoded from the previous I or P-frames. B-frames are the least important in the video sequence and use information from previous and forward frames.

The following algorithm describes the above idea. Instead of using a first-in first-out queue (FIFO) at the MAC layer, we insert the packets in the queue by taking into account the importance of the frame. The most important frames are placed in the top positions in the queue, while other packet types are placed in the tail. The processing of packets is based on the rule that the packet in the head of the queue has to be served first. If the queue exceeds the size limit and needs to drop a packet, then it always drops the one in the tail.

```
enque(packet) {
if(packet.isVideo() ) {
while(nextPacket.isVideo() AND
nextPacket.priority <
packet.priority ) {
position=position+1;
}
insertToQueue(packete, position)
} else {
insertToQueue(packete, tail)
}
if(queue.size() > limit ) {
dropTail()
}
}
```

Algorithm 1. Enqueue function

The IP datagrams are also marked based on the underlying application type. This is a simpler task in mesh networks than in wired with fixed infrastructure, in which different administrative domains may exist in a path between video sender and receiver(s). Ad hoc networks provide this flexibility as every node in the network acts also as router. The main function for providing QoS support in IEEE 802.11e protocol is the Enhanced Distributed Coordination Function (EDCF). This function is responsible for managing the wireless medium in the Contention Period (CP) and enhances the Distributed Coordination Function (DCF) function of the legacy IEEE 802.11 protocol. Therefore, we implement four different data Traffic Classes (TCs) and video traffic is assigned with the highest priority amongst other applications that operate in the wireless network.

III. Performance Evaluation

Most of the related work has been evaluated through simulations conducted with the ns-2 [12] network simulator. These evaluations are mainly based on "classic" network metrics (throughput, delay, packet losses, etc). Our evaluation combines both network and media-centric metrics. For the purpose of this work, we use the Peak Signal to Noise Ratio (PSNR) to assess the quality of the received video file at the end user. PSNR is a derivative of Signal to Noise Ratio (SNR) and computes the maximum possible signal energy to the noise energy, which results in a higher correlation with the subjective quality perception than the conventional SNR.Equation (1) gives the definition of the PSNR of a source image s and destination image d [13]:

$$PSNR(s,d) = 20\log\frac{V_{peak}}{MSE(s,d)} \text{ in dB}$$

where (1)

$V_{peak} = 2^k - 1$, k bit color depth

$MSE(s,d)$ = mean square error of s and d

In order to conduct a number of realistic experiments with real video files, we use the Evalvid [14] tool-set in conjunction with ns-2. For our simulations, we use a YUV raw video, which consists of 7319 frames and has duration of 365 seconds. The network topology simulates the Manhattan grid mobility model, which is based on the Manhattan city model with uniform sized building blocks. The Manhattan grid mobility model can be considered as an ideal model to represent the conditions of a big city. The simulation area is 2000x2000 meters in a 4x4 grid. Inside this area, there are 300 mobile nodes representing moving vehicles that are actually the transmitters and receivers of the video file. The moving speed varies from 0 to 20m/sec, having a mean value of 15m/sec. The video transmission is based on the Real-time Transport Protocol (RTP) [15] that is designed for audio and video delivery over IP networks. Table I summarizes the simulation parameters.

A. Performance of the Scheduling Algorithm without any background traffic

In this simulation, it is assumed that there is only one active video transmission in the network, without any other data traffic. Thus, transmitted packets are either video or routing packets. We run two different simulation scenarios, with 802.11g and 802.11e protocols, respectively. The aim of this simulation it to evaluate the mechanism which provides enhance protection to I-frames. The comparison shows how the adaptation on the packet queues affects video transmission.

Figure 2. PSNR Performance evolution graph

TABLE II
SIMULATION RESULTS WITHOUT BACKGROUND TRAFFIC

Radio type	**802.11g**	**802.11e**
Overall packet delivery ratio	69.7%	75.2%
Average end to end delay (all packets)	499ms	343ms

As Figure. 2 indicates, the implemented adapted queue results to a significant reduction of the losses of I–frames, at the cost of a slight increase of P and B-frame losses. In contrast, packet losses remain almost the same for every type of video packets when using the normal FIFO queue.

The metrics for overall packet losses and end-to-end delay are mostly related to the network conditions and are not affected by the adaptations of the scheduling mechanism for video packets. In addition, when using the 802.11e protocol, the routing packets are transmitted with the highest priority improving the AODV performance. Apart from the above network metrics, we use PSNR to evaluate the efficiency of the proposed mechanism. Figure. 3 shows that the implemented adapted queue leads to a significant improvement of PSRN measurements both on the 802.11g and 802.11e networks. As expected, the 802.11e network provides better results compared to 802.11g due to 802.11e QoS features. All the above improvements increase the end user experience.

B. Performance of the Scheduling Algorithm with background traffic

In this scenario, we use the same video transmission with the previous simulation. However, this time there are 20 TCP connections in the network. The amount of data that each node transfers during the simulation lifetime is about 910 kilobytes. In addition, we run two different simulation scenarios with 802.11g and 802.11e networks, respectively. Our objective is to evaluate the implemented priority queue which provides high priority to video packets. The packet types in this case are falling under the following categories; routing, video and background data packets.

Figure. 3 shows that the implemented adapted queue leads to a significant improvement of PSRN measurements both in 802.11g and 802.11e networks. It is important to mention that the resulting end user experience does not deteriorate by the background traffic as indicated by the PSNR values.Finally, we show the impact of traffic prioritization to the reception rate. The cases of adaptations on the queuing system are omitted since any changes to the scheduling policy do not affect the real transmission rate.

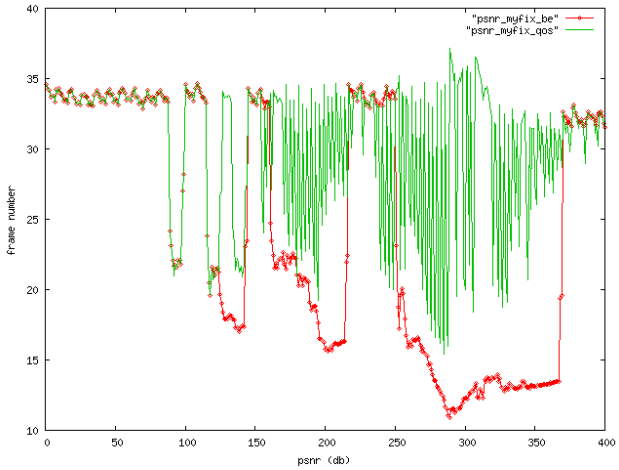


Figure 3. Cumulative receiver rate for video transmission

IV. CONCLUSIONS AND FUTURE WORK

In this paper, we focused on improving video transmission over MANETs. The main idea was to exploit the multimedia coding information from the application layer in order to use a scheduling policy at the network layer so that the most important video packets could enjoy the highest priority. In order to evaluate the performance of the proposed cross-layer mechanism we conducted a number of simulations with the network simulator ns-2. Our findings were very encouraging and indicated the efficient operation of the adapted queue on providing high priority to video packets.

The utilization of the 802.11e Traffic Classes (TCs) was proved very efficient in environments in which video transmission competed for network resources with background TCP traffic. The easiness of setting and utilizing the 802.11e QoS features to MANETs in which all nodes act as routers made that protocol an indispensable network feature of any MANET implementation.

Our future work includes the comparison of the proposed design with other priority schemes for MANETs and the evaluation of the proposed mechanism under more complicated MANETs and

simulation scenarios. Another important area which left for future work is to include the transport layer in the cross-layer design in an effort to adapt the video transmission rates based on the network conditions.

We believe that this will further increase the QoS that is finally offered to the end user.

REFERENCES

[1] IEEE 802.11 WG, Part 11: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements".

[2] V. Timcenko, M. Stojanovic and S.B. Rakas, "MANET routing protocols vs. mobility models: performance analysis and comparison", Proceedings of the 9th WSEAS international conference on Applied informatics and communications, p. 271-276, 2009.

[3] D. Johnson, Y. Hu and D. Maltz, The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, RFC 4728, February 2007.

[4] C. Perkins and E. Belding-Royer, Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561, July 2013.

[5] C. E. Perkins and P. Bhagwat "Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Computer Communications Review, pp. 234-244, October 1994.

[6] B. Divecha, A. Abraham, C. Grosan and S. Sanya, "Impact of Node Mobility on MANET Routing Protocols Models", Journal of Digital Information Management, 2007.

[7] M. A. Igartua and V. C. Frías, "Self-configured multipath routing using path lifetime for video-streaming services over Ad Hoc networks", Computer Communications 2010, Volume 33, Issue 15, pp. 1879-1891,2010.

[8] M. Matin and N. Naaji, "Performance Analysis with Enhanced Distributed Channel Access (EDCA) in IEEE 802.11e for Real Time Video Streaming (MPEG-4) in Multi-hop MANET", Journal of Communication and Computer. Vol. 7, no. 4, pp. 24-29, Apr il 2010.

[9] X. Pallot and L. E. Miller, "Implementing message priority policies over an 802.11 based mobile ad hoc network", IEEE Military Communications Conf. (MILCOM), pp. 860 - 864, 2001.

[10] Y. Andreopoulos, N. Mastronarde and M. van der Schaar, "Cross-Layer Optimized Video Streaming Over Wireless Multihop Mesh Networks", Selected Areas in Communications, IEEE Journal on Selected Areas in Communications, IEEE Journal on, Vol. 24, No. 11, pp. 2104-2115, 2006.

[11] N. Qadri, M. Altaf, M. Fleury, M. Ghanbari and H. Sammak, "Robust Video Streaming over an Urban VANET", IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, pp.429-434, 2009.

[12] The UCB/LBNL network simulator, software online: http://www.isi.edu/nsnam/ns/

[13] J. Cavers, "Mobile Channel Characteristics", Kluwer Academic, 2000.

[14] J. Klaue, B. Rathke and A. Wolisz, "EvalVid – A Framework for Video Transmission and Quality Evaluation", Proceedings of the 13th International Conference on Modeling, Techniques and Tools for Computer Performance Evaluation, Urbana, Illinois, 2003.

[15] H., Casner, S., Frederick and R., Jacobson, RFC 3550: "RTP: A transport protocol for real-time applications", Schulzrinne, V. (eds.), July 2003.

Efficient Data Broadcast Using One-To-All and All-To-All Broadcast Algorithm in Wireless networks

Steffy vetha J,
M.E.Computer and communication,
Infant Jesus college of Engineering
Keelavallanadu, Tuticorin District, India.
Vetha.am@gmail.com

Sugirtha.M. M.E
Computer Science
Infant Jesus college of Engineering
Keelavallanadu, Tuticorin District, India.
Sugi.smile90@gmail.com

Abstract **- Broadcast communication is a key requirement for WSNs Broadcast communication, which forms the basis of all communication in wireless networks. In multihop wireless networks, however, interference at a node due to simultaneous transmissions from its neighbors makes it important to design a minimum-latency broadcast algorithm, which is known to be NP-complete. A simple 12-approximation algorithm for the one-to-all broadcast problem that improves latency Problem in the one-to-all broadcast algorithm. This leads to better performance with a collision free broadcasting. The all-to-all broadcast crisis where each node sends its own message to all other nodes. For all-to-all broadcasting the performance is improved by using Collect and Distribute, Interleaved Collect and Distribute algorithm. The message transmission in the wireless network using one-to-all and all-to-all broadcast algorithm gives best result. But it is not enough for very large multihop networks, so in future it can be implemented for very large multihop networks in efficient manner to reduce latency and collision-free and to find the latency time in wireless networks.**

Index Terms— Wireless networking, approximation algorithms, broadcast algorithms, wireless scheduling.

I INTRODUCTION

Broadcasting refers to a method of transferring a message to all recipients simultaneously. Broadcasting can be performed as a high level operation in a program, for example broadcasting Message Passing Interface or it may be a low level networking operation. Interference is a fundamental limiting factor in wireless networks. When two or more nodes transmit a message to a common neighbor at the same time, the common node will not receive any of these messages. In such a case, we say that collision has occurred at the common node. Interference range may be even larger than the transmission range, in which case a node may not receive a message from its transmitter if it is within the interference range of another node sending a message. Approximation algorithms are used to find approximate solutions to optimization problems. Approximation algorithms are often associated with NP-hard problems; since it is unlikely that there can ever be efficient algorithms for solving NP-hard problems. Ideally, the approximation is optimal up to a small constant factor. One of the earliest broadcast mechanisms proposed in the literature is flooding [1], [2], where every node in the network transmits a message to its neighbors after receiving it. Although flooding is extremely simple and easy to implement, Ni et al. [3] show that flooding can be very costly and can lead to serious redundancy, bandwidth contention, and collision: a situation known as broadcast storm.

A. Our Contributions

We present algorithms for ONE-TO-ALL and ALL-TO-ALL broadcasting problems. In one-to-all broadcast, there is a source that sends a message to all other nodes in the network. In all-to-all broadcast each node sends its own message to all other nodes. Even the one-to-all

broadcasting problem is known to be NP-complete [4]. For both problems, we develop approximation algorithms, which improve the previous results. ONE-TO-ALL BROADCAST problem, it present a simple approximation algorithm that achieves a 12-approximate solution, thereby improving the approximation guarantee of 16. Our algorithm is based on the algorithm of Gandhi et al. [4] and incorporates the following two ideas that lead to the improvement: 1) processing the nodes greedily—in non increasing order of the number of receivers, and 2) allowing nodes to transmit more than once. For the ALL-TO-ALL BROADCAST problem it present two algorithms (called CDA and ICDA) with approximation guarantees of 20 and 34, respectively, thereby improving the approximation guarantee of 27. In ICDA, all nodes are scheduled to participate in transmissions as early as possible. Our algorithms achieve up to 37 percent improvement on end-to-end latency over existing schemes.

II RELATED WORKS

Several techniques have been proposed for broadcasting in wireless networks. In order to reduce the broadcast redundancy and contentions, they make use of nodes' neighborhood information and determine whether a particular node needs to transmit a message [5], [6]. There has been some work on latency-constrained broadcasting in wired networks [7] and some results do exist for radio networks whose models are essentially the same as ours. This result does not directly extend to ad hoc networks which are modeled by a restricted class of geometric graphs called disk graphs. Gandhi et al. [4] show that minimizing broadcast latency in wireless networks is NP-complete and then present an approximation algorithm for one-to-all broadcasting.

A. Network Model

When the interference range and the transmission range are identical, a wireless network can be modeled as a unit disk graph (UDG), G(V,E). The nodes in V are embedded in the plane. Each node u has a unit transmission range. Let uj; vj denote the Euclidean distance between u and v. We assume that time is discrete. We assume that every message transmission occupies a unit time slot: i.e., the latency of a single successful transmission is one unit of time. We say that there is a collision at node w, if w hears a message from two transmitters at the same time. In such a case, we also say that the two transmissions interfere at w. A node w receives a message collision free iff w hears the message without any collision.

B. Problem Statement:

Disk graph G= (V, E) and a set of messages M=(m1; m2; . . .;mn).A set of sources for these messages are taken as sources: (sj|sj is the source of message j). A node can transmit message j only after it receives message j collision free. A schedule specifies, for each message j and each node i, the time at which node i receives message j collision free and the time at which it transmits message j. If a node does not transmit a message then its transmit time for that message is 0. The latency of the broadcast schedule is the first time at which every node receives all messages. The number of transmissions is the total number of times every node transmits any message. The goal is to compute a schedule in which the latency is minimized. For that one-to-all and many-to-all broadcasting is used. One-to-all broadcasting is the operation where there is one source node s which has a message to send all other nodes. In all-to-all broadcasting each node v has its own message m to send all other nodes.

III. ONE-TO-ALL BROADCAST ALGORITHM

This algorithm takes the input and a source node s. If a node u is parent node of the node w then u is responsible for transmitting the message to w without any collision. This algorithm leads to significantly improved approximation guarantee are 1. Processing node in a greedy manner 2. Allowing a node to transmit more than once. It leads to guarantee that receiver node will receive the message collision free by overcoming broadcast problem. This algorithm first constructs BFS Tree. In BFS the non increasing order of nodes are the primary nodes. The children of the primary nodes are secondary nodes. In ONE-TO-ALL BROADCAST, the transmissions are scheduled in two phases. In Phase 1, nodes are considered one level at a time starting from Level 0. Only those primary nodes

that have a child will transmit the message in this phase. In Phase 2, transmissions are scheduled to send the message to all other nodes. In Phase 1, The Primary nodes that doesn't have child will transmit in the phase 2.

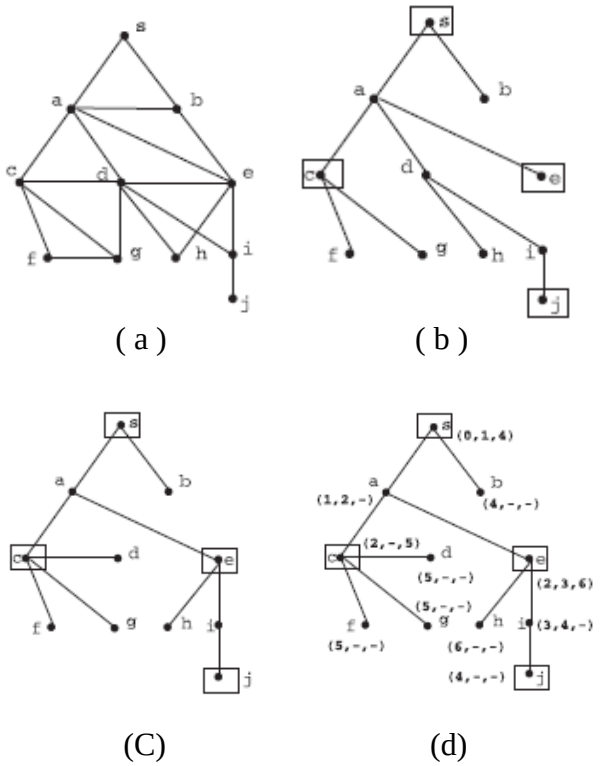


Fig. 1. An illustration of our algorithm. (a) Shows the example network.(b) Shows the BFS tree, (c) Shows the broadcast tree, (d) Shows the transmission schedule.

IV. ALL-TO-ALL BROADCAST ALGORITHM

In all to all broadcast, every node in the network will transmits the message to every other node in the network. To overcome problem we change the value in approximation ratio as 20 and 34 using Collect and Distributed Algorithm (CDA) and Interleaved Collect and Distribute Algorithm (ICDA). In terms of transmission overhead, our algorithm shows that both CDA and ICDA consistently use fewer transmissions than existing one.

A. Collect-and-Distribute Algorithm (CDA)

The algorithm consists of 2 phases. In phase 1, source node collects all the packets by performing upward transmissions. In the Phase 2, source node broadcasts all the n packets to all other nodes via downward transmissions.

Phase 1. The source node collects all messages. The algorithm is as follows: first construct a BFS tree from s, and sort messages in non decreasing order of the level in the BFS tree. That is, messages that are closer to s appear first in the sorted list. Let us assume that message j be the jth message in the sorted order. The latency of the collection algorithm is at most reduced.

Phase 2. We construct a broadcast tree. Next, we describe transmission scheduling algorithm. In the algorithm by Gandhi et al. [4], the root node collects all messages and performs one-to-all broadcasting for each message. The root node needs to wait until the previous message reaches the level before initiating a broadcast for another message to make sure there are no collisions in their algorithm. In this algorithm, we find a schedule by a vertex coloring, which makes sure that all the nodes with the same color can broadcast a message without collision, and show that 17 colors are enough to obtain a collision-free schedule. Then computing the broadcast tree and let k1, k2 be the number of colors. We define a super step for k time slots. In each superstep, the first k1 slots are for scheduling transmissions from primaries, and the remaining k2 slots will be for secondary's. Each primary with color i is only allowed to transmit in the ith slot of a primary slot in a superstep. Each secondary receiving a packet in a superstep transmits the received packet in the corresponding secondary slot in the same superstep.

B. Interleaved Collect-and-Distribute Algorithm (ICDA)

In the early stages of the algorithm, until s receives all the messages and starts propagating them, most nodes are idle, thus increasing the broadcast time significantly. Thus it describes an algorithm in which all nodes participate in broadcasting as soon as possible so as to minimize the broadcast time. A node v receives a message m forwarded originally from its descendant x in the broadcast tree and relays it to its parent to deliver the message to the root nodes. The children of v can also receive the message when v broadcasts it. Using the broadcast tree constructed as in CDA, we schedule transmissions for each node as follows: as in CDA, we define a superstep but in a slightly

different way. That is, in each superstep, every node transmits at most one message (either upward or downward). Instead of finishing all upward transmissions first, we mix upward or downward transmissions in each superstep with preferences given to upward transmissions.

C. Results for One-to-All Broadcast

While we have experimented with various settings, we only report a set of representative results in the rest of this section. In Fig. 2, we present the average approximation ratios when we vary the number of nodes within a fixed-size square 1000 m _ 1000 m. Our proposed algorithm consistently outperforms existing schemes by 12-40 percent. Specifically, in the 400-node scenario, the average approximation ratio of our algorithm is 1.74, which is around 21 percent smaller than that of GPM (2.22) and PBS (2.21) and 40 percent smaller than that of EBS (2.92). Approximation ratio of our scheme goes up slightly, but the performance improvement over existing schemes is similar or larger.

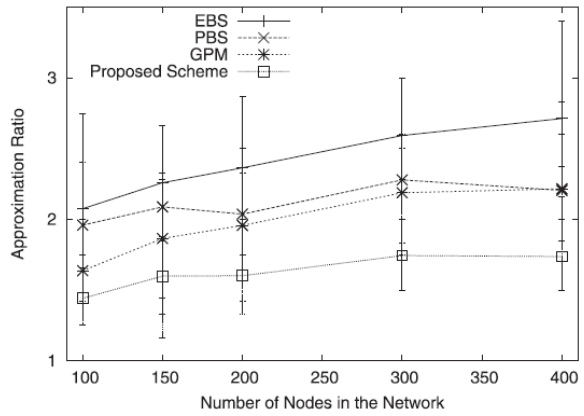


Fig.2. Average approximation ratio of one-to-all broadcast. A fixed-size square of (1000 m *1000 m) used.

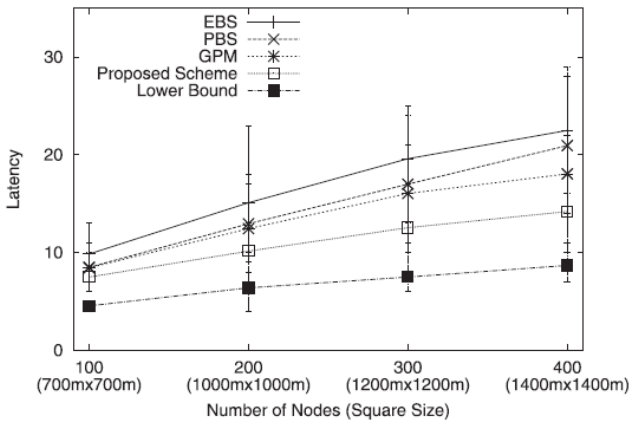


Fig.3. Average latency of one-to-all broadcast. We vary the square size to keep the node density similar.

In Fig. 3, we present the average values of actual latency for broadcast algorithms as well as the height of BFS tree (i.e., lower bound). It varies both the number of nodes and the square size, so that the average number of neighbors is maintained similar. Observe that the proposed algorithm consistently outperforms existing schemes by 11-37 percent.

D. Results for All-to-All Broadcast

In Fig. 4, we present the average approximation ratio of our all-to-all broadcast schemes (CDA and ICDA), MSB and IGA that vary the number of nodes and the square size. Observe that the performance of CDA and ICDA in practice is much better than the analytical bound (20 and 34). CDA performs well when the network size is small However, the performance difference between CDA and MSB becomes smaller in larger Networks.

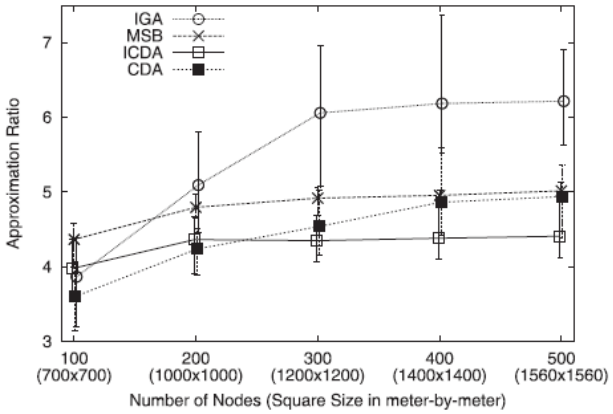


Fig. 4. Average approximation ratio of all-to-all broadcast. Node count and square size varies.

CONCLUSIONS

Thus an approximation algorithm for broadcasting in wireless networks was implemented. Our algorithm for ONE-TO-ALL BROADCASTING gives a 12-approximate Solution and the algorithms for ALL-TO-ALL BROADCASTING give approximation ratios of 20 and 34. But it is not enough for very large multihop networks, so in future it can be implemented for very large multihop networks in efficient manner to reduce latency and collision-free and to find the latency time in wireless networks.

REFERENCES

[1] C.Ho,K.Obraczka, G. Tsudik, and K. Viswanath , "Flooding for Reliable Multicast in Multi-Hop Ad Hoc Networks,"Proc. Third Workshop Discrete and Algorithms Methods for Mobile Computing And Comm., pp. 64-71, 1999.

[2] J. Jetcheva, Y. Hu, D. Maltz, and D.Johnson, "A Simple Protocol for Multicast and Broadcast in Mobile Ad Hoc Networks," IETF Internet draft, July 2001.

[3] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The Broadcast Storm Problem in a Mobile Ad Hoc Network," Proc. ACM/IEEE MobiCom, pp. 151-162, 1999.

[4] R. Gandhi, A. Mishra, and S.Parthasarathy, "Minimizing Broadcast Latency and Redundancy in Ad Hoc Networks," IEEE/ACM Trans. Networking, vol. 16, no. 4, pp. 840-851, Aug. 2008.

[5] W. Peng and X. Lu, "AHBP: An Efficient Broadcast Protocol for Mobile Adhoc Networks," J. Science and Technology, vol. 16,pp. 114-125, 2000.

[6] J. Sucec and I. Marsic, "An Efficient Distributed Network-Wide Broadcast Algorithm for Mobile Adhoc Networks," technical report, Rutgers Univ., 2000.

GSM BASED MOVING MESSAGE USING LCD DISPLAY

P.ARUNPANDIYAN [1] & N.SURESHGOPAL[2] & S.SUNDARKUMAR[3] & N.IBRAHIM RAJA[4]
1UG Student , Dept of Electrical and Eelectronics Engineering ,
2 UG Student , Dept of Electrical and Eelectronics Engineering,
3UG Student , Dept of Electrical and Eelectronics Engineering,
4UG Student , Dept of Electrical and Eelectronics Engineering
Kalasalingam Institute of Technology, Krishnankoil
Email : nammalvar198@gmail.com ,sundarkumar.akptc193@gmail.com,
arunponraj014 @gmail.com, ibrahim1319912@gmail.com

ABSTRACT:

The current trend of information transfer in the campus, it is seen that important notice take time to be displayed in the notice boards. This latency is not expected in most of the cases and must be avoided. We want to control everything and without moving an inch. The electronics displays which are currently used are programmable displays which need to be reprogrammed each time. This makes it inefficient for immediate information transfer. The main aim of this project will be to design a SMS driven automatic display board which can replace the currently used programmable electronic display.

Keyword:- GSM, Interface, Message, Modem, Receiver, Transmitter.

I.INTRODUCTION

The GSM cellular phone has grown from a luxury item owned by the rich to something so common that one out of five Filipinos already owns one. This is amazing when we look at the fact that our country is a developing one with almost half our population living below the poverty line. This continuously growing popularity of the GSM cell phone has spurred the growth of the country's cellular network infrastructure lcd by the two major players, Ayala owned Globe Telecom, and PLDT‟s Smart Cellular.[3].It is proposed to design receiver cum display board which can be programmed from an authorized mobile phone. The message to be displayed is sent through a SMS from an authorized transmitter. The microcontroller receives the SMS, validates the sending Mobile Identification Number (MIN) and displays the desired information. Started off as an instantaneous News display unit, we have improved upon it and tried to take advantage of the computing capabilities of microcontroller. The GSM based display board can be used as an add-on to these display boards and make it truly wireless. The display board programs itself with the help of the incoming SMS with proper validation. Such a system proves to

be helpful for immediate information transfer. Required LCD display is to be used for example 2x16,4x32.

II.GSM COMMUNICATION MODULE GSM:

Global System for Mobile Communications originally *Grouped Special Mobile*), is a standard set developed by the European telecommunication standard (ETSI) to describe technologies for second generation (or "2G") digital cellular network. Developed as a replacement for first generation analog cellular networks, the GSM standard originally described a digital, circuit switched network optimized for duplex(communication) voice telephony. The standard was expanded over time to include first circuit switched data transport, then packet data transport via GPRS. Packet data transmission speeds were later increased via EDGE. The GSM standard is succeeded by the third generation (or "3G") UMTS standard developed by the 3GPP. GSM networks will evolve further as they begin to incorporate fourth generation (or "4G") LTE advanced standards. "GSM" is a trademark owned by the GSM association. The GSM Association estimates that technologies defined in the GSM standard serve 80% of the world's population, encompassing more than 5 billion people across more than 212 countries and territories, making GSM the most ubiquitous of the many standards for cellular networks

This GSM modem is a highly flexible plug and play GSM 850 900 / GSM 1800 / GSM 1900 modem for direct and easy integration RS232, voltage range for the power supply and audio interface make this device perfect solution for system integrators and single user. It also comes with license free integrated Python. Python is a powerful easy to learn programming language. Such a Python driven terminal is 5 times better and faster and 5 times cheaper than standard PLC/RTU with communication interface and external GSM / GPRS modem. Voice, Data/Fax, SMS, DTMF, GPRS, integrated TCP/IP stack and other features like the GSM / GPRS modules on this home page.

III.GSM CARRIER FREQUENCIES

GSM networks operate in a number of different carrier frequency ranges (separated into GSM frequency for 2G and UMTS frequency bands for 3G), with most 2G GSM networks operating in the 900 MHz or 1800 MHz bands. Where these bands were already allocated, the 850 MHz and 1900 MHz bands were used instead (for example in Canada and the United States). In rare cases the 400 and 450 MHz frequency bands are assigned in some countries because they were previously used for first-generation systems. Most 3G networks in Europe operate in the 2100 MHz frequency band.

Regardless of the frequency selected by an operator, it is divided into time division multiplexing

for individual phones to use. This allows eight full-rate or sixteen half-rate speech channels per radio frequency. These eight radio timeslots (or eight burst transmission periods) are grouped into a time division multiple access frame. Half rate channels use alternate frames in the same timeslot. The channel data rate for all 8 channels is 270.833 kbit/s, and the frame duration is 4.615 ms. The transmission power in the handset is limited to a maximum of 2 watts in GSM850/900 and 1 watt in GSM1800/1900.

GSM MODEM CHARACTERISTICS

- Quad GSM GPRS modem (GSM 850 /900/1800 / 1900)
- Designed for GPRS, data, fax, SMS and voice applications
- Fully compliant with ETSI GSM Phase 2+ specifications (Normal MS)
- License free Python interpreter with free of charge programming tools

GSM MODEM INTERFACES

- RS232 through D-TYPE 9 pin connector, RJ11 for I2C, SPI and GPIO
- Power supply through Molex 4 pin connector
- SMA antenna connector
- Toggle spring SIM holder
- Red LED Power on, Green LED status of GSM / GPRS module

GSM MODEM GENERALCHARACTERISTICS

- **Input voltage**: 5V-30V
- **Current**: 8mA in idle mode, 150mA in communication GSM 900 @ 12V, 110mA in GSM 1800 @ 12V
- **Temperature range**: Operating -30 to +85 degree Celsius.

IV LCD DISPLAY

A liquid crystal display (LCD) is a thin, flat electronic visual display that uses the light modulating properties of liquid crystals (LCs). LCDs do not emit light directly. Liquid crystal displays (LCDs) are a passive display technology. This means they do not emit light; instead, they use the ambient light in the environment. By manipulating this light, they display images using very little power. This has made LCDs the preferred technology whenever low power consumption and compact size are critical.

They are used in a wide range of applications, including computer monitors, television, instrument panels, aircraft cockpit displays, signage, etc. They are common in consumer devices such as video players, gaming devices, clocks, watches, calculators, and telephones. LCDs have displaced cathode ray tube (CRT) displays in most applications. They are usually more compact, lightweight, portable, less expensive, more reliable, and easier on the eyes.

LCD DISPLAY IMAGE

PIN INFORMATION OF LCD

Pin No	Symbol	Details
1	GND	Ground
2	Vcc	Supply Voltage +5V
3	Vo	Contrast adjustment
4	RS	0->Control input, 1-> Data input
5	R/W	Read/ Write
6	E	Enable
7 to 14	D0 to D7	Data
15	VB1	Backlight +5V
16	VB0	Backlight ground

VALGORITHM TO SEND DATA TO LCD:

1.Make R/W low

2.Make RS=0 ;if data byte is command

RS=1 ;if data byte is data (ASCII value)

3.Place data byte on data register

4.Pulse E (HIGH to LOW)

5.Repeat the steps to send another data byte

LCD INITIALIZATION

Working of LCD depend on the how the LCD is initialized. We have to send few command bytes to initialize the lcd. Simple steps to initialize the LCD.

1. **Specify function set**:

Send **38H** for 8-bit,double line and 5x7 dot character format.

2. **Display On-Off control**:

Send **0FH** for display and blink cursor on.

3. **Entry mode set**:

Send **06H** for cursor in increment position and shift is invisible.

4. **Clear display**:

Send **01H** to clear display and return cursor to home position.

VI. FUTURE ENHANCEMENT

A commercial model can be able to display more than one message at a time. In our system we are sending messages via GSM network and displaying on a LCD by utilizing AT commands. The same principle can be applied to control electrical appliances at a distant location. Robots can be controlled in a similar fashion by sending the commands to the robots. This can be used for spy robots at distant locations, utilized by the military to monitor movement of enemy troops.

REFERENCES

I. Gao ,W., Zhang, G. and Jiang, X. “Study Implementation of Agricultural SMS Management System”. In Proceedings of IEEE International Conference on Information Technology and Computer Science, 13-17 October 2009, Beijing, China, pp. 1-4, 2009.

II. Shereen , N. Z. and Rozumah , B. “Mobile Phone use Amongst Student in University in Malaysia: It correlates and relationship to Psychological Health”. European Journal of Scientific Research. Vol. 37. No.2. pp. 206 – 218, 2009

LOCAL TEXTURE AND GLOBAL STATISTICAL FEATURES BASED IMAGE AUTHENTICATION SCHEME

Mrs. M. Nava Barathy, M.E
Assistant Professor,
Regional Centre of Anna University, Tirunelveli.
Email: navabarathyp@gmail.com

P. Thanuja
PG Scholar
Regional Centre of Anna University, Tirunelveli.
Email: tanswathi@gmail.com

***Abstract*— In this paper, we propose a robust hashing method is proposed for detecting image forgery which includes removal, insertion, replacement of objects, abnormal colour modification and locating the forged area. Global and Local features are used in forming the hash sequence. The Zernike moments and Image Co-occurrence Histogram (ICH) are used for finding the global features. A local feature includes position and texture information of salient regions in the image. In feature extraction and hash construction, secret keys are introduced for image authentication. The hash of the test image is compared with that of a reference image. The hash of the test image is compared with that of a reference image. The hash distance is compared with two kinds of pre-defined thresholds, to determine whether the image is applicable for mal-function. By decomposing the hashes, the type of image forgery and location of forged areas can be determined.**

***Keywords*— Image hash, perceptual robustness, saliency, Zernike moments, image authentication, Image Co-occurrence Histogram (ICH) .**

I.INTRODUCTION

With widespread use of image editing software, images are modified. This has become an important issue in our day-to-day life. Image hashing is a technique that extracts a short sequence from the image to represent its contents, and therefore can be used for image authentication. If the image is modified maliciously, the hash must be changed significantly. Meanwhile, unlike hash functions in cryptography such as MD5 and SHA-1 that are extremely sensitive to slight changes in the input data, the image hash should be robust against normal image processing. In general, a good image hash should be reasonably short and robust to ordinary image manipulations, and sensitive to tampering. It should also be unique for different images. That is, it should have significantly different hash values, and secure. So, that any unauthorized person cannot break the key and coin the hash. To meet all the requirements simultaneously, especially perceptual robustness and sensitivity to tampering, is a main challenging task.

Here, we present a saliency model based on the image co-occurrence histogram (ICH) that has been used for object Recognition. The ICH concurrently encodes both global pixel occurrence and local co-occurrence of pixel pairs within a neighborhood window. Visual saliency, which is often perceived by global "uncommonness" and local "discontinuity" with respect to the surroundings, can therefore be determined based on the low-frequency pixel occurrence and co-occurrence information. The ICH-based saliency model has several advantageous characteristics. First, it is fast and has potential for use in real-time applications. Second, it requires minimal parameter tuning and is very easy to implement. Third, it is robust and tolerant to image scale variation. Last but not least, it captures both local and global saliency information and demonstrates superior accuracy in predicting human fixations.

Many image hashing methods have been proposed. Zhenjun Tang et al. [1] develop a global method using nonnegative matrix factorization (NMF). The image is first converted into a fixed-sized pixel array. A secondary image is obtained by rearranging pixels and applying NMF to produce a feature-bearing coefficient matrix, which is then coarsely quantized. The obtained binary string is scrambled to generate the image hash.

Vishal Monga et al. [2] apply NMF to pseudo-randomly selected sub-images. They construct a secondary image, and obtain low-rank matrix approximation of the secondary image with NMF again. The matrix entries are concatenated to form an NMF-NMF vector. The inner products of the NMF-NMF vector and a set of weight vectors are calculated. Because the final hash comes from the

secondary image with NMF, their method cannot locate forged regions. In analyzing the NMF-NMF method.

In [3], a wavelet-based image hashing method is developed. The input image is partitioned into non-overlapping blocks, and the pixels of each block are modulated using a permutation sequence. The image undergoes pixel shuffling and then wavelet transform. The sub-band wavelet coefficients are used to form an intermediate hash, which is permuted again to generate the hash sequence. This method is robust to most content-preserving operations and can detect tampered areas.

Fouad Khelifi et al. [4] propose a robust and secure hashing scheme based on virtual watermark detection. The method is robust against normal image processing operations and geometric transformation, and can detect content changes in relatively large areas.

Wenjun Lu and Min Wu [5] SIFT features are encoded into compact visual words to estimate geometric transformations, and block-based features are used to detect and localize image tampering.

Xiang et al. [6] propose a method using invariance of the image histogram to geometric deformations. It is robust to geometric attacks, but cannot distinguish images with similar histograms but different contents.

Swaminathan *et al.* [11] propose an image hash method based on rotation invariance of Fourier-Mellin transform and present a new framework to study the security issues of existing image hashing schemes. Their method is robust to geometric distortions, filtering operations, and various content-preserving manipulations.

In the present paper, we propose a method combining advantages of both global and local features. The objective is to detect image forgery including removal, insertion, replacement of objects, abnormal colour modification, and for locating the forged area using image hashing method. We use Zernike moments and Image Co-occurrence Histogram(ICH) of the luminance/chrominance components to reflect the image's global characteristics. Extract local texture features from salient regions in the image to represent contents in the corresponding areas. Distance metrics indicating the degree of similarity between two hashes are defined to measure the hash performance. Two thresholds are used to decide whether a given image is an original or malicious image of a reference image, or is simply a different image. The method can be used to locate tampered areas and it tells the nature of tampering, e.g., replacement of objects or abnormal modification of colors. Compared with some other methods using global features or local features only. The proposed method has better overall performance, especially the ability of distinguishing regional tampering from content-preserving processing.

II GLOBAL & LOCAL FEATURE EXTRACTION

A. Zernike Moments

Zernike Moments (ZM) of order n and repetition m of a digital image I (ρ, θ) are defined as [7]:

$$Z_{n\,m} = \frac{n+1}{\pi} \sum\sum I(\rho, \theta)\, V^{*}_{n\,m}(\rho, \theta) \quad (\rho, \theta) \in \text{Unit disk} \tag{1}$$

Where $V^{*}_{n\,m}(\rho, \theta)$ is a Zernike polynomial of order n and repetition m

$$V^{*}_{n\,m}(\rho, \theta) = R_{n\,m}(\rho) e^{jm\theta} \tag{2}$$

Where $\{ R_{n\,m}(\rho)\}$ is a radial polynomial in the form of

$$R_{n\,m}(\rho) = \sum_{s=0}^{(n-|m|)/2} (-1)^{s} \frac{(n-s)!}{s!\left(\frac{n+|m|}{2}-s\right)!\left(\frac{n-|m|}{2}-s\right)!} \rho^{n-2s} \tag{3}$$

Here, is a non-negative integer and m is an integer satisfying the conditions: n-|m| is even and $|m| \leq n$.
Suppose α is a rotation angle, and $Z_{n\,m}$ and $Z^{(r)}_{n\,m}$.The ZM of the original and rotated images respectively:

$$Z^{(r)}_{n\,m} = Z_{n\,m} e^{-jm\alpha} \tag{4}$$

Thus, the magnitude of ZM is rotation invariant, while the phase changes with the angle:

$$\arg(Z^{(r)}_{n\,m}) = \arg(Z_{n\,m}) - m\alpha \tag{5}$$

B. Image Co-Occurrence Histograms

The image histogram represents the distribution of image values. It has a number of good properties, for example, robustness to image noise, rotation, scale variation, and so on. The traditional 1D image histogram captures only the image value occurrence, whereas information about the local spatial composition of image pixels is completely discarded (which is instead very important to the perception of an image). We show that a two-dimensional (2D) ICH is capable of capturing both occurrence and co-occurrence of image pixels and can be used to calculate a good measure of visual saliency.

Consider a single-channel integer image I. Let IK = {1,2,…,k} be a set of k possible image values within I (k is 256 for an 8-bit integer image). H, the ICH of the image I, is defined as follows:

$$H = [h(m, n)],\ m, n \in IK, \tag{6}$$

Where H is a symmetric square matrix of size k * k. An ICH element h (m, n) is the co-occurrence count of image values m and n within a square neighborhood window of size z. H is constructed as follows. For each image pixel with a value of m, all image pixels within the local neighborhood window are examined one by one. If a neighboring pixel has a value of n,

the ICH element h (m, n) is increased by one. The ICH is built after all image pixels within I are examined.

The ICH captures both occurrence and co-occurrence of image values as defined in (6). In particular, each image value will pair with itself to account for many diagonal elements of the ICH through which global occurrence information is captured. At the same time, each pixel will also pair with a number of neighboring pixels to account for non-diagonal elements of the ICH through which local co-occurrence information is captured. The neighborhood size z can be set between 1 and 4 without affecting the performance

C. Texture Features

Texture is an important feature. In [8] and [9], the authors propose six texture features relating to visual perception: coarseness, contrast, directionality, line-likeness, regularity and roughness. In this work, we use coarseness C_1 and contrast C_2 as defined below, plus skewness and kurtosis, to describe the texture properties. To evaluate coarseness around a pixel at (x, y), the pixels in its neighborhood sized $2^k * 2^k$ are averaged:

$$A_k(x, y) = \frac{1}{2^{2k}} \sum_{i=x-2^k}^{x+2^k-1} \sum_{j=y-2^k}^{y+2^k-1} g(i, j), \quad k=0,1,\ldots,5 \tag{7}$$

Where g(i, j), is the gray-level of pixel (i, j). At each point (x, y), differences between pairs of the average values of non-overlapping neighborhoods on opposite sides of the pixel in horizontal and vertical directions.
For horizontal direction,

$$E_{k,h}(x, y) = |A_k(x+2^{k-1},y) - A_k(x-2^{k-1},y)| \tag{8}$$

For vertical direction,

$$E_{k,v}(x, y) = |A_k(x,y+2^{k-1}) - A_k(x,y-2^{k-1})| \tag{9}$$

For that point, find the size that leads to the highest difference value and call it $S_{opt}(x, y)$.

$$S_{opt}(x, y) = \arg\max_{K=0,\ldots,5;d=h,v} E_{k,d}(x, y) \tag{10}$$

Take average of S_{opt} over a region, and call it coarseness of that region, C_1.

Contrast describes the degree of image brightness variation, calculated from variance σ^2 and the fourth-order moment μ_4 of the gray values within the region:

$$C_2 = \sigma^2 \mu_4^{-4} \tag{11}$$

C. Salient Region Detection

A salient region in an image is one that attracts human visual attention. Information in an image can be viewed as a sum of two parts: that of innovation and that of prior knowledge. The information of saliency is obtained when the redundant part is removed. Log spectrum of an image, is used to represent general information of the image. Because log spectra of different images are similar, there exists redundant information in Log spectrum of an image.

$$A(f) = h_l * L(f) \tag{12}$$

Where, L(f) - Log spectrum of an image, A(f) denote the redundant information defined as convolution between L(f) and an l*l low-pass kernel h_l.

Spectral residual representing novelty of the image, B(f), can be obtained by subtracting A(f) from L(f), which is then inversely Fourier transformed to give a saliency map $S_M(x)$:

$$S_M(x) = F^{-1}[B(f)] = F^{-1}[L(f)-A(f)] \tag{13}$$

We choose a threshold equal to three times of the mean of $S_M(x)$ to determine the salient regions.

III PROPOSED HASHING METHOD

Here, we describe the proposed image hashing scheme and the procedure of image authentication using the hash. The hash is formed from Zernike moments to represent global properties of the image, and the texture features in salient regions to reflect local properties.

A. Image Hash Construction

Image hash generation has following steps, referring Figure 1.

1. Preprocessing: The image is first rescaled to a fixed size and and converted from RGB to the YCbCr representation. The aim of rescaling is to ensure that the generated image hash has a fixed length and the same computation complexity. Y and |Cb-Cr| are used as luminance and chrominance components of the image to generate the hash. We choose F=256 as an appropriate trade-off.

2. Global Feature Extraction: Zernike moments and Image Co-occurrence Histogram (ICH) of Y and |Cb-Cr| are calculated. We choose n=5. Further, since $Z_{n,-m} = Z_{n,m}$, only $Z_{n,m}$ $(m \geq 0)$ is needed. We do not use $Z_{0,0}$ as it represents the average intensity. we have Zernike moments in total. Magnitudes of the Zernike moments are rounded and used to form a global vector, $Z' = [Z_y Z_c]$. The elements in Z' are not more than 255. A secret key K_1 is used to randomly generate a row vector X_1 with 22 random integers in [0, 255]. The encrypted global vector Z is obtained as $Z = [(Z'+X_1) \bmod 256]$.

3. Local Feature Extraction: *K* largest salient regions are detected from the luminance image Y. The coordinates of top

left corner, and width/height of each circumscribed rectangle are used to form a K-element vector $P^{(k)}$ (k=1,….k) , representing the position and size of each salient region.

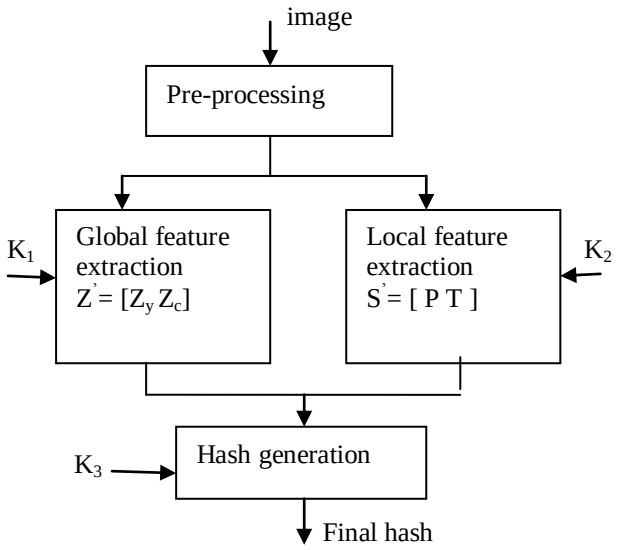


Figure 1. Block diagram of the image hashing method.

Local texture features of each salient region including coarseness C_1 and contrast C_2 , skewness, and kurtosis are computed and rounded to give a 6-element vector $t^{(k)}$ (k=1,…6). If an image has less than 6 salient regions, the positions and texture features of the missing ones are set to zero. The position/size and texture vectors of all salient regions together form a local feature vector $S' = [P T] = [P^{(1)}…P^{(6)} t^{(1)}….t^{(6)}]$, which contains 48 integers. A secret key K_2, is used to randomly generate a row vector containing 48 random integers in [0, 255]. An encrypted local vector S is then obtained by $S = [(S' + X_2) \bmod 256]$.

4. Hash Construction: The global and salient local vectors are concatenated to form an intermediate hash, namely $H' = [Z\ S]$, which is then pseudo-randomly scrambled based on a secret key to produce the final hash sequence H. Table I gives the constitution of an image hash of 70 integers. Since all integers are in the range of [0, 255], the hash is bits long.

B. Image Authentication

In image authentication, the hash of a trusted image, H_0 , is Available and called the reference hash. The hash of a received image to be tested, H_1, is extracted. The image authentication process is performed in the following way.

1) Feature Extraction: Pass the test image through the steps as described in section 1 to obtain the intermediate hash without encryption, namely $H'_1=[Z_1 P_1 T_1]$.

2) Hash Decomposition: With the secret keys K_1, K_2 and K_3, restore the intermediate hash from the reference hash to obtain $H'_0 = [Z_0 P_0 T_0]$, which is a concatenated feature sequence of the trusted image. Decompose it into global and local features.

3) Salient Region Matching: Check if the salient regions found in P_1 of the test image match those P_0 in of the trusted image. If the matched areas of a pair of regions are large enough, the two regions are considered as being matched. Reshuffle the texture vectors by moving the matched components in each of the texture vector pair to the left-most and, for notational simplicity, still call them T_0 and T_1.

4) Distance Calculation and Judgment: To define the hash distance, a feature vector V, is formed by concatenating the global feature vector Z and the reshuffled texture feature vector T, namely V = [Z T]. The vector P does not contribute to the distance calculation but will be used to locate forged regions. The hash distance between the test image and the reference is the Euclidean distance between V_0 and V_1:

$$D = \|V_1 - V_0\| \tag{14}$$

In practice, the global structure of an image represented by Zernike moments and Image Co-occurrence Histogram (ICH) is sufficient to distinguish similar from dissimilar. To minimize the adverse influence of saliency detection inaccuracy, we omit T in calculating the hash distance for similar images:

$$D \approx \|Z_1 - Z_0\| \triangleq D_G \tag{15}$$

Having defined the hash distance, we can use it first to distinguish similar and dissimilar images according to a threshold τ_1. We then need to further determine whether the test image is a tampered version of the reference image, or simply a different one. The test image is judged as tampered if $D \le \tau_2$. Otherwise it is a completely different image.

C. Determination of Thresholds

To Determine a threshold for differentiating two sets of data, A and B, we need to know the PDF of samples. The chi-square test is used for the purpose. Assume that the data satisfy one of several common distributions: Poisson, lognormal, and normal, and apply the chi-square test to find which is the closest. The statistic X^2 is calculated . To perform the chi-square test, a sufficiently large number of test images are needed. The original image downloaded from the internet and captured with digital cameras. The operations include gamma correction with γ= 1.1 and 1.15, JPEG compression with Q= 30 and 80, zero-mean Gaussian noise contamination with σ^2= 0.01 and 0.001, scaling with factors 0.5 and 1.5, and rotation by 1° and 5°.Chi-square tests show that the distance values between similar images follow the exponential distribution with a mean of 1.88. The distances between forged images and their original versions follow the lognormal distribution with a mean of 3.46 and standard deviation 0.88. Those between different images follow the gamma distribution with a mean of 10.3 and standard deviation 8.16.

Therefore we choose τ_1= 7 and τ_2=50 as the thresholds in this work to differentiate similar, forged, and different images.

D. Forgery Classification and Localization

Having found that a test image is a fake, the next work is to locate the forged region and tell the nature of forgery. Four types of image forgery can be identified: removal, insertion and replacement of objects, and unusual color changes. Forgery classification and localization are performed as follows, and schematically.

Decode H_0 and H_1 into components representing global and local features, and find the number of matched salient regions R and the numbers of salient regions in the reference and test images, M_0 and M_1.

1. If $M_0 > M_1 = R$, some objects have been removed from the received test image.

2. If $M_1 > M_0 = R$, the test image contains some additional Objects.

3. If $M_1 = M_0 = R$, check the luminance and chrominance components in the Zernike moments and calculate the following distances:

$$\gamma Z_c = ||Z_{c1}-Z_{c0}|| , \ \gamma Z_y = ||Z_{y1}-Z_{y0}||$$

If γZ_c is greater than γZ_y by a threshold τ_c , the test image contains substantial color changes with respect to the reference image while the luminance changes are considerably smaller. Thus the test image is judged as being tampered with unusual color modifications.

4. If $M_1 = M_0 = R$ and (γZ_c - γZ_y) is less than τ_c , the test image contains replaced objects because in this case luminance changes are dominant.

5. If $M_0 > R$ and $M_1 > R$, some of the salient regions are not matched.

IV PERFORMANCE EVALUATION

Performance of the proposed method is basically due to the Combination of global and local features. The former reflect the overall structure of the image, and the latter, based on content saliency, are used to identify and characterize changes in visually important regions. The proposed method can differentiate similar (i.e., perceptually the same), forged, and different images. Over-all performance of the proposed method, which generates hashes with the third shortest length, is robust against several normal processing manipulations, and can detect and locate small area tampering. The proposed method has shown stronger ability to distinguish content-preserving operations from regional forgery than the other two methods. All three methods can distinguish forgery from normal operations such as JPEG coding, additive noise and scaling because these only cause tiny changes to the image contents. It is observed that the hash has good ability in distinguishing these operations from regional forgery. Note that, in calculating ROC, the false negative (FN) and false positive (FP) errors are errors in differentiating between similar and forged images rather than between similar and different images.

$$P_{FN} = \frac{\text{Number of forged images judged as natural images}}{\text{Total number of forged images}} \quad (16)$$

$$P_{FP} = \frac{\text{Number of natural images judged as forged images}}{\text{Total number of natural images}} \quad (17)$$

V. CONCLUSION

In this paper, an image hashing scheme is developed using both global and local features. The Zernike moments and Image Co-occurrence Histogram (ICH) are used for finding the global features. A local feature includes position and texture information of salient regions in the image. Hashes produced with the proposed method are robust against common image processing operations (i.e., brightness adjustment, scaling, small angle rotation, and JPEG coding and noise contamination. Collision probability between hashes of different images is zero. The proposed scheme has a reasonably short hash length and good ROC performance. The method described in this paper is aimed at image authentication. The hash can be used to differentiate similar, forged, and different images. At the same time, it can also identify the type of forgery and locate fake regions containing salient contents. In the image authentication, The hash of the test image is compared with that of a reference image. The hash distance is compared with two kinds of pre-defined thresholds, to determine whether the image is applicable for mal-function. By decomposing the hashes, the type of image forgery and location of forged areas can be determined. It should be stressed that the success of image authentication using the proposed scheme depends to a large extent on the accuracy of saliency detection.

REFERENCES

[1] Z. Tang, S.Wang, X. Zhang, W.Wei, and S. Su, "Robust image hashing for tamper detection using non-negative matrix factorization," J. Ubiquitous Convergence Technol., vol. 2, no. 1, pp. 18–26, May 2008.

[2] V. Monga and M. K. Mihcak, "Robust and secure image hashing via non-negative matrix factorizations," IEEE Trans. Inf. Forensics Security,vol. 2, no. 3, pp. 376–390, Sep. 2007.

[3] F. Ahmed, M. Y. Siyal, and V. U. Abbas, "A secure and robust hash based scheme for image authentication," Signal Process., vol. 90, no.5, pp. 1456–1470, 2010.

[4] F. Khelifi and J. Jiang, "Perceptual image hashing based on virtual watermark detection," IEEE Trans.

Image Process., vol. 19, no. 4, pp. 981–994, Apr. 2010.
[5] W. Lu and M.Wu, "Multimedia forensic hash based on visual words," in Proc. IEEE Conf. on Image Processing, Hong Kong, 2010, pp.989–992.
[6] S. Xiang, H. J. Kim, and J. Huang, "Histogram-based image hashing scheme robust against geometric deformations," in Proc. ACM Multimedia and Security Workshop, New York, 2007, pp. 121–128.
[7] Z. Chen and S. K. Sun, "A Zernike moment phase based descriptor for local image representation and matching," IEEE Trans. Image Process., vol. 19, no. 1, pp. 205–219, Jan. 2010.
[8] T. Deselaers, D. Keysers, and H. Ney, "Features for image retrieval: A quantitative comparison," in Lecture Notes in Computer Science, 2004,vol. 3175, pp. 228–236, Springer.
[9] H. Tamura, S. Mori, and T. Yamawaki, "Textural features corresponding to visual perception," IEEE Trans. Syst., Man, Cybern., vol.8, no. 6, pp. 460–472, Jun. 1978.
[10] V. Monga, A. Banerjee, and B. L. Evans, "A clustering based approach to perceptual image hashing," IEEE Trans. Inf. Forensics Security, vol.1, no. 1, pp. 68–79, Mar. 2006.
[11] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 215–230, Jun. 2006.
[12] X. Hou and L. Zhang, "Saliency detection: A spectral residual approach," in Proc. IEEE Int. Conf. Computer Vision and Pattern Recognition, Minneapolis, MN, 2007, pp. 1–8.
[13] J. Huang, S.R. Kumar, M. Mitra, W.J. Zhu, and R. Zabih, "Image Indexing Using Color Correlograms," Proc. IEEE Conf. Computer Vision and Pattern Recognition, pp. 762-768, 1997.
[14] A. Rao, R.K. Srihari, and Z. Zhang, "Spatial Color Histograms for Content-Based Image Retrieval," Proc. 11th IEEE Int'l Conf. Tools with Artificial Intelligence, pp. 183-186, 1999.
[15] P. Chang and J. Krumm, "Object Recognition with Color Co-occurrence Histograms," Proc. IEEE Conf. Computer Vision and Pattern Recognition, pp. 498-504, 1999.
[16] S. Lu and J.H. Lim, "Saliency Modeling from Image Histograms," Proc. European Conf. Computer Vision, pp. 321-332, 2012.

ENERGY EFFICIENT TARGET TRACKING IN SENSOR NETWORKS

Ms.A.Bindhu
Assistant Professor
Department of ECE
T. J. Institute of Technology
Ph. No: 8056283141
Mail id: bindhu_mail@yahoo.com

AYSWARYA.P.NAIR
P.G. Scholar
Department of ECE
T. J. Institute of Technology
Ph. No. 8056161735
Mailid:ayswaryarevathy@gmail.com

Abstract— Scheduling sensor activities is an effective way to prolong the lifetime of wireless sensor networks (WSNs). The paper explores the problem of wake-up scheduling in WSNs where sensors have different lifetime. A novel Probability-Based Prediction and Sleep Scheduling (PPSS) strategy is proposed to prolong the network lifetime with full coverage constraint, tracking performance can be improved if the target motion can be predicted and nodes along the trajectory can be proactively awakened. PPSS strategy improves energy efficiency of proactive wake up. The designing starts with a target prediction, based on the prediction results PPSS then precisely selects the nodes to awaken and reduces their active time, so as to enhance energy efficiency. PPSS algorithm is enhanced to detect and Track multiple mobile targets with improved energy efficiency. A recently published Energy-Efficient Local Wake-up Scheduling in Wireless Sensor Networks are used for comparison. Simulation results reveal that PPSS yields better performance compared with the Energy-Efficient Local Wake-up Scheduling algorithm.

I. INTRODUCTION DOCUMENT

A wireless sensor network (WSN) consists of a large number of sensors which are densely deployed over a large area. Each sensor monitors a physical environment and communicates via wireless signals. With the advancements in hardware miniaturization and wireless communication technologies, WSNs have been used in various applications such as education, warfare, and traffic monitoring. Regardless of the applications, extending the network lifetime is a critical issue in WSNs. This is because the sensors are battery-powered and generally difficult to be recharged. Unlike detection, a target tracking system is often required to ensure continuous monitoring, i.e., there always exist nodes that can detect the target along its trajectory. In target tracking applications, idle listening is a major source of energy waste. To reduce the energy consumption during idle listening, duty cycling is one of the most commonly used approach in which Sensor nodes are put into sleep state for most of the time, and only wake them up periodically. Sometimes, the sleep pattern of nodes may also be explicitly scheduled, i.e., forced to sleep or awakened on demand. This is usually called sleep scheduling. One effective way to prolong the network lifetime is to schedule sensors wake-up activities. In WSNs, sensors commonly have two operation modes, i.e., active mode and sleep mode. A sensor in active mode can perform its monitoring task and therefore needs to consume a relatively large amount of energy. On the contrary, a sensor in sleep mode does not perform the sensing task and consumes little energy. Therefore, by appropriately scheduling sensors to be in low-energy sleep mode and waking them up when necessary, the network lifetime can be prolonged. In the literature, various efforts have been made on optimizing the wake-up scheduling in WSNs.

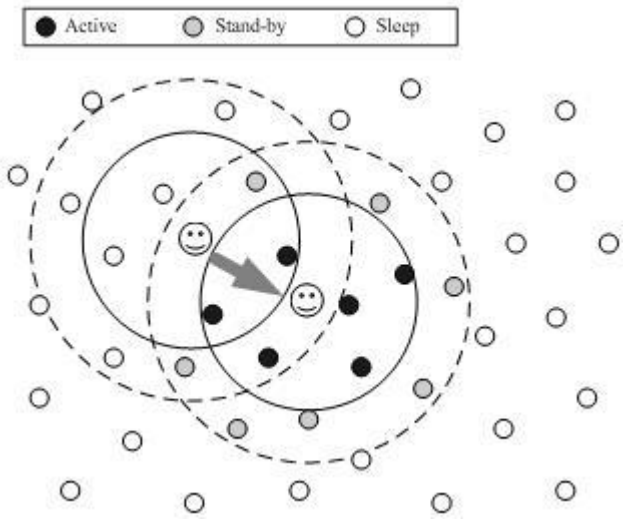


Fig1 Scheduling sleep pattern based on Target prediction.

A probability-based target prediction and sleep scheduling protocol (PPSS) is presented to improve the efficiency of proactive wake up and enhance the energy efficiency with limited loss on the tracking performance. With a target prediction scheme, PPSS not only predicts a target's next location, but also describes the probabilities with which it moves along all the directions. Target prediction of PPSS provides a directional probability as the foundation of differentiated sleep scheduling in a geographical area. Then, based on the prediction results, PPSS enhances energy efficiency by reducing the number of proactively awakened nodes and controlling their active time in an integrated manner. This will improve the scalability of PPSS for large-scale WSNs. Thus PPSS aims at improving the overall performance on energy efficiency and tracking performance using sleep scheduling. The simulation results reveal that the proposed PPSS yields very promising performance.

.

II. RELATED WORK

Energy efficiency has been extensively studied either independently or jointly with other features. In [7], the authors proposed, analyzed, and evaluated the energy consumption models in WSNs with probabilistic distance distributions to optimize grid size and minimize energy consumption accurately. In [5], the authors proposed a distributed, scalable, and localized multipath search protocol to discover multiple node-disjoint paths between the sink and source nodes, in which energy was considered as constraint so that the design is feasible for the limited resources of WSNs.As one of the most important applications of WSNs,target tracking was widely studied from many perspectives.

First, tracking was studied as a series of continuous localization operations in many existing efforts.Second, target tracking was sometimes considered as a dynamic state estimation problem on the trajectory, and Bayesian estimation methods, e.g., particle filtering, were used to obtain optimal or approximately optimal solutions. Third, in some cases, target tracking was considered as an objective application when corresponding performance metrics, e.g., energy efficiency [1] or real-time featurewere the focus. Fourth, a few efforts were conducted based on real implementation, and emphasized the actual measurement for a tracking application [4]. Finally, a few target tracking efforts did not explicitly distinguish tracking from similar efforts, such as detection [1] and classification [4].Although sleep scheduling and target tracking have been well studied in the past,

only a few efforts [1], [2]investigated them in an integrated manner. In [1], the authors utilize a "circle-based scheme" (Circle) to schedule the sleep pattern of neighbor nodes simply based on their distances from the target. In such a legacy Circle scheme, all the nodes in a circle follow the same sleep pattern, without distinguishing among various directions and distances. In[12], Jeong et al. present the MCTA algorithm to enhance energy efficiency by solely reducing the number of awakened nodes. MCTA depends on kinematics to predict the contour of tracking areas, which are usually much smaller than the circles of Circle scheme. However, MCTA keeps all the nodes in the contour active without any differentiated sleep scheduling.

Kinematics describes the motion of objects without considering the circumstances that cause the motion, while dynamics studies the relationship between the object motion and its causes . In fact, most of past work about target prediction uses kinematics rules as the foundation, even for those that use Bayesian estimation methods. MCTA algorithm presented is just an example of kinematics-based prediction. Another example is the Prediction-based Energy Saving scheme (PES). It only uses simple models to predict a specific location.

III. PROPOSED METHOD

In the proposed concept, it is possible to save more energy by reducing energy consumption i.e., if it is able to predict the probability by which the Mobile target moves, the sensors along that direction can be made active and putting rest of the sensors in sleep mode, so we can save comparatively more energy than the existing work, this can be achieved by creating a Local Active Environment and sleep scheduling. for e.g., a wireless sensor which detects the mobile target will create a Local active environment i.e., by awakening the neighbor sensors or next hop sensors and sensors in the routing table to send the information about the target to the base station, putting the remaining sensors to sleep mode. By this way the sensors that are close to mobile target will predict the direction in which mobile target moves and creates a Local Active Environment dynamically each time the target moves. Thus the energy efficiency is increased to great extent compared to the Existing works which maximizes the network lifetime.

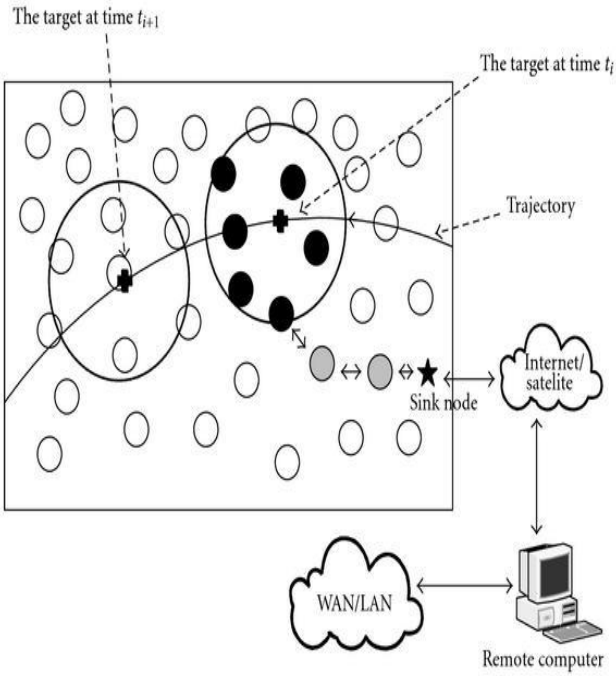


Fig 2 Detects and Tracks the Mobile Target and sends the information to the Sink node.

The problem of wake-up scheduling in WSNs where sensors have different lifetime is explored. A novel Probability-Based Prediction and Sleep Scheduling (PPSS) strategy is proposed to prolong the network lifetime with full coverage constraint. PPSS is designed based on proactive wake up: when a node (i.e., alarm node) detects a target, it broadcasts an alarm message to proactively

awaken its neighbor nodes (i.e.,awakened node) to prepare for the approaching target. To enhance energy efficiency, we modify this basic proactive wake-up method to sleep-schedule nodes precisely. Specifically, Probability based prediction and sleep scheduling selects some of the neighbor nodes (i.e., candidate node) that are likely to detect the target to awaken. On receiving an alarm message, each candidate may individually make the decision on whether or not to be an awakened node, and if yes, when and how long to wake up.

Two approaches are utilized to reduce the energy consumption during this proactive wake-up process:

1. Reduce the number of awakened nodes.

2. Schedule their sleep pattern to shorten the active time.

First, the number of awakened nodes can be reduced significantly, because: 1) those nodes that the target may have already passed during the sleep delay do not need to be awakened;

2) nodes that lie on a direction that the target has a low probability of passing by could be chosen to be awakened with a low probability.

For this purpose, a concept of awake region and a mechanism for computing the scope of an awake region is introduced.Second, the active time of chosen awakened nodes can be curtailed as much as possible, because they could wake up and keep active only when the target is expected to traverse their sensing area. For this purpose, we present a sleep scheduling protocol, which schedules the sleep patterns of awakened nodes individually according to their distance and direction away from the current motion state of the target. Both of these energy reducing approaches are built upon target prediction results. Unlike the existing efforts of target prediction develop a target prediction model based on both kinematics rules and probability theory.

Kinematics-based prediction calculates the expected displacement of the target in a sleep delay, which shows the position and the moving direction that the target is most likely to be in and move along. Based on this expected displacement, probability-based prediction establishes probabilistic models for the scalar displacement and the deviation. Once a target's potential movement is predicted,we may make sleep scheduling decisions based on these probabilistic models: take a high probability to awaken nodes on a direction along which the target is highly probable to move, and take a low one to awaken nodes that are not likely to detect the target.

Components Of Probability Based Prediction And Sleep Scheduling

1. Target Prediction.

The proposed target prediction scheme consists of three steps: current state calculation, kinematics-based prediction, and probability based prediction. After calculating the current state, the kinematics-based prediction step calculates the expected displacement from the current location within the next sleep delay, and the probability-based prediction step establishes probabilistic models for the scalar displacement and the deviation.

In the real world, a target's movement is subject to uncertainty, while at the same time it follows certain rules of physics. This apparent contradiction is because: 1) at each instant or during a short time period, there is no significant change on the rules of a target's motion; therefore, the target will approximately follow kinematics rules;

2) However, a target's long-term behavior is uncertain and hard to predict,e.g., a harsh brake or a sharp turn cannot be predicted completely with kinematics rules. In fact, even for a short term, it is also difficult to accurately predict a target's motion purely with a physics-based model. However, the prediction

is absolutely helpful for optimizing the energy efficiency and tracking performance tradeoff. Thus, a probabilistic model is considered to handle as many possibilities of change of the actual target motion as possible.

2. Awakened node reduction.

The number of awakened nodes is reduced with two efforts: controlling the scope of awake regions, and choose a subset of nodes in an awake region.The life cycle of awake regions is described as follows:

i. Creation.

On detecting a target, a sensor node will check its own status to determine if it is an awakened node in an existing awake region. If yes, it justifies if the target is leaving the current awake region. If no previous awake region exists or if

the target is leaving the current awake region, the node runs an alarm node election algorithm. If this node is elected as the alarm node, it broadcasts an alarm message to all the candidate nodes. On receiving this alarm message, each candidate node individually decides if it is in the scope of this awake region and whether or not to schedule the sleep pattern. Finally, a new awake region is formed when every awakened node schedules their sleep patterns specifically for the approaching target.

ii. Maintenance.

If an awake region exists and the target is not going to move out of the current awake region, the node keeps active without sleep scheduling operations, and the awake region remains unchanged.

iii. Dismissal.

As time progresses, the sleep patterns of awakened nodes will automatically recover back to the default pattern; thus, the awake region will be dismissed automatically. There is no explicit dismissal mechanism needed. Usually, a sensor node's transmission range R is far longer than its sensing range r. Thus, when the nodes are densely deployed to guarantee the sensing coverage, a broadcast alarm message will reach all the neighbors within the transmission range. However, some of these neighbors can only detect the target with a relatively low probability, and some others may even never detect the target. Then, the energy consumed for being active on these nodes will be wasted. A more effective approach is to determine a subset among all the neighbor nodes to reduce the number of awakened nodes.

During the sleep delay, the target may move away from the alarm node for a distance. Then, it is unnecessary for nodes within this distance to wake up, since the target has already passed by. Meanwhile, all the nodes in an awake region must in the one-hop transmission range of the alarm node. Therefore, an awake region should be in a ring shape,i.e., the part between two concentric circles.Beyond the effort that limits the awakened nodes within an awake region, the number of awakened nodes can be further reduced by choosing only some nodes in the awake region as awakened nodes.

Based on prediction on the target's moving directions, the probabilities that the target moves along various directions are different. Obviously the number of awakened nodes along a direction with a lower probability could be less than the number along a direction with a higher probability. By choosing an awakened node based on a probability related to the moving directions, awakened nodes can be reduced significantly.

3. Active time control.

Based on the probabilistic models that are established with target prediction, PPSS schedules an awakened node to be active, so that the probability that it detects the target is close to 1. After reducing the number of

awakened nodes, energy efficiency can be enhanced further by scheduling the sleep patterns of awakened nodes, as not all the awakened nodes need to keep active all the time. We schedule the sleep patterns of awakened nodes by setting a start time and an end time of the active period. Out of this active period, awakened nodes do not have to keep active. Therefore, the time that an awakened node has to keep active could be reduced compared with the Circle scheme.

V. CONCLUSION

The wake-up scheduling of sensors has significant impact on the lifetime and coverage of a WSN. A duty-cycled sensor network, proactive wake up and sleep scheduling can create a local active environment to provide guarantee for the tracking performance. Thus efficiently schedule sleep and wake up patterns for each sensors based on the probability of the direction in which the Mobile Target moves.

By effectively limiting the scope of local active environment (i.e., reducing low value-added nodes that have a low probability of detecting the target), PPSS improves the energy efficiency with an acceptable loss on the tracking performance. In addition, the design of PPSS protocol shows that it is possible to precisely sleep-schedule nodes without involving much physics. Simulation results on different networks demonstrate that the proposed PPSS yields better performance than the previous defined protocol.

REFERENCES

[1] Julian Winter , Yingqi Xu Wang-Chien Lee "Prediction-Based Strategies For Energy Saving In Object Tracking Sensor Networks" Proc. IEEE Int'l Conf. Mobile Data Management, Pp. 346-357, 2004.

[2] Chao Gui and Prasant Mohapatra "Power Conservation And Quality Of Surveillance In Target Tracking Sensor Networks" Proc. 10th Ann. Int'l Conf. Mobile Computing and Networking, pp. 129-143, 2004.

[3] J.Jeong, T.Hwang "MCTA:Target Tracking Algorithm Based On Minimal Contour In Wireless Sensor Networks" Proc. IEEE INFOCOM, pp. 2371-2375, 2007.

[4] Abtin Keshavarzian, Huang Lee, Lakshmi Venkatraman "Wakeup Scheduling In Wireless Sensor Networks" Proc. IEEE Mobihoc, pp. 322-333, 2006.

[5] G. de Veciana and J. Stine, "Improving energy efficiency of centrally controlled wireless data networks," Wireless Networks, 8(6), pp. 681- 700, 2002.

[6] N. G. Bourbakis, A. Pantelopoulos "A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol.40, no.1, pp.1-12, Jan. 2010.

[7] M. Haenggi, M. llyas and I. Mahgoub, "Opportunities and challenges in Wireless sensor Networks," in Handbook of Sensor Network: Compact Wireless and Wired Sensing Systems, eds., Boca Raton, FL, pp. 1.1-1.14, CRC Press, 2004.

DUAL PURPOSE ATM MACHINE BASED FINGERPRINT

R.Saranya [1],J.Sathiya[2] ,and S.Brindha [3]

[1&2]PG students - Department of Electronics and Communication Engineering, [3]Asst prof. Department of ECE

Renganayagi Varatharaj College of Engineering, Sivakasi.

saranmgr@gmail.com[1],sathiyasri.raji@gmail.com[2],ssdbrindha10@gmail.com[3]

ABSTRACT

This project "ATM Based Voting System Using Finger Print" is used to enter our vote through ATM machines. The voter can belong to any district but can vote at the place where he is staying. In future this type of system can reduce the unnecessary confusion in the voters list and the election works. The voter can register his vote from the nearby ATM machine. Once the finger print is placed, the details of the voter are taken from the main server through the controller. This type of system is useful for the public to put the vote from any part of the state. This system can reduce the insufficient and increase the percentage of polling.

INTRODECTION

In this designed system ATM based voting system is implemented in which voting can be done from any state or district by the voter's from the place where they are staying. As we are implementing biometrics such as finger print recognisation which can't be stolen and separate visualizing camera have to be module. In our system automatic counting of results is programmed so no need to spend separate time for counting the votes. Less manpower is enough in this designed system. It is less expensive compared to E-voting and ballot box voting.

ROLE OF CONTROLLER AND READER

In this project we use PIC 16F877A controller. It is a 40 pin IC. When the signal receives from the finger print scanner controller will display the details of the people in the LCD display. We enter the coding for the whole project in the IC. In this IC we connect the ATM machine in a port and the voting machine in another port.

When a finger placed on the sensor, the controller will display the details like name, age, gender etc. then it asks the pin number for the ATM card. If the number is correct, it will display the options. If the user needs to vote, he will enter the corresponding data. Then it displays the nominees name and their symbol. Then the user will put his vote and save them.

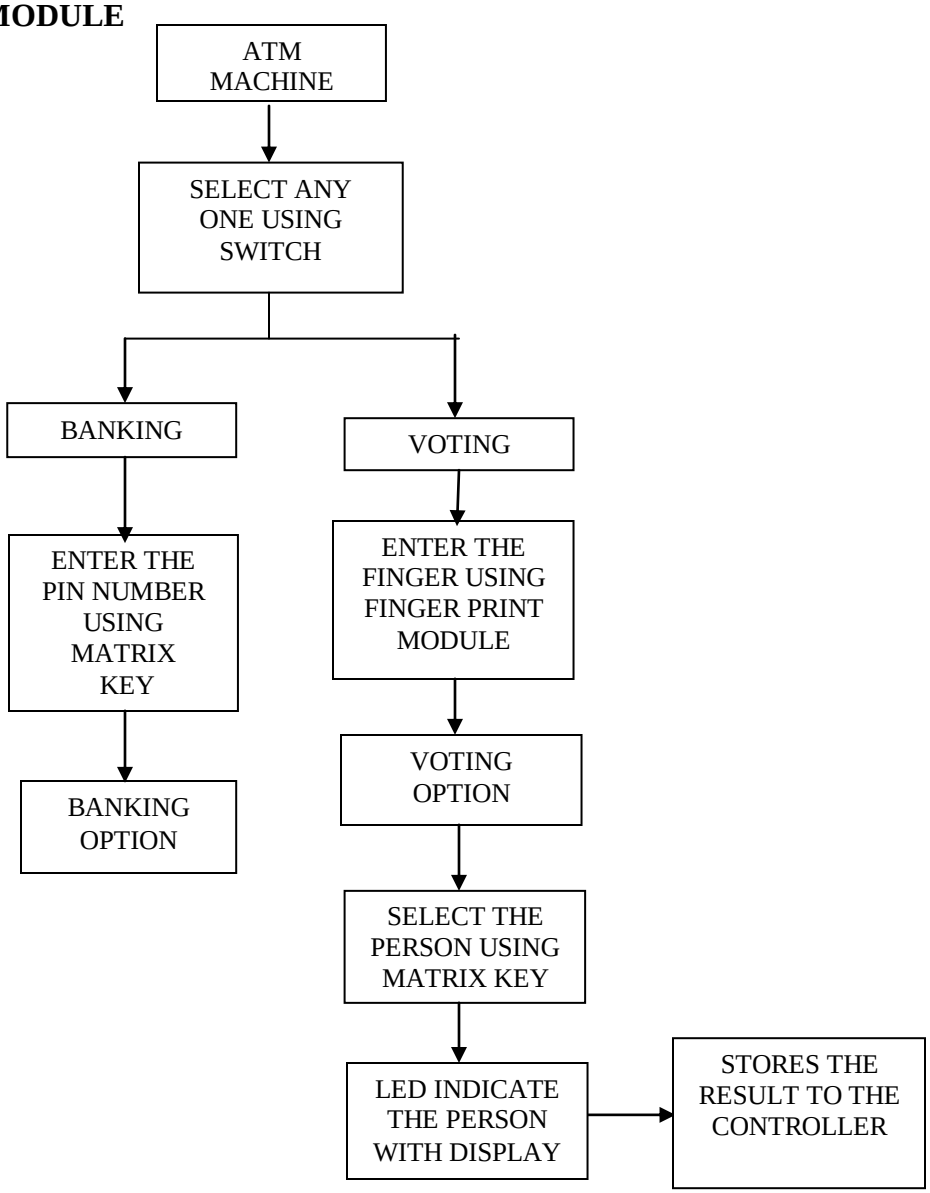
CONCEPT OF VOTING SYSTEM

In general, The ATM based universal voting system using fingerprint consist of microcontroller PIC16F877A is used in this project, which is used to control and read the function of the voting machine. The ATM machine is interfaced with the general purpose port of the controller and the finger print reader is connected to the other port of the controller. The finger prints of the citizens are prerecorded in each district and the address and the details of the corresponding citizen will be stored in the main server. When the voter place his finger on the reader, the finger print module reads

the finger print and it is processed by the controller, which displays the details of the voter. The controller displays the details like name of the voter, gender, age and the district where he belongs. In the next set the controller displays the nominees with their symbols. The voter can register his vote according to the displayed details

such drawbacks can be overcome in this designed real time project module

FLOW CHART MODULE



It seems plausible to imagine that computerized methods for ballot casting and tabulation could alert the voter to mistakes. For example, by flagging over voting, when more candidates are chosen than his allowed, and by reducing under voting when some selections are skipped. New vote tallying systems, which counts the marks made on ballots, should be faster, more accurate, and cost effective, and better able to prevent certain types of tampering than older products.

Because of the alarming frequency and impact of the mal functions of voting systems, in recent years and number of vulnerability analysis exercises have been carried out against voting systems to determine if they can be compromised in order to control the results of an election.

Technically voter card voting can be used but some drawback such as theft of card and scratches in card will not access for voting these such drawbacks can be overcome in this designed real time project module.

SYSTEM ANALYSIS

EXISTING SYSTEM

In this existing system electronic voting is implemented. As such many drawbacks have been caused because of this existing system such as malpractices like duplication of voter's id proof then unnecessary confusion voters list and the election works. Huge manpower is required to safeguard the electronic voting machine. The voter may be at some other place so that they can't vote from the place where they are staying which leads to decrease in polling rate. In this system two to three days will be needed to announce the election results. The cost used to implement the E-voting system is high compared to the designed system. To overcome these drawbacks we designed a system as a real time.

PROPOSED SYSTEM

In this designed system ATM based voting system is implemented in which voting can be done from any state or district by the voter's from the place where they are staying. As we are implementing biometrics such as finger print recognisation which can't be stolen and separate visualizing camera have to be module. In our system automatic counting of results is programmed so no need to spend separate time for counting the votes. Less manpower is enough in this designed system. It is less expensive compared to E-voting and ballot box voting.

SYSTEM STUDY

Feasibility study

The feasibility of the project is analyzed in this phase is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the designed system is to be carried out. This is to ensure that the designed system is not a burden to the government. For feasibility analysis, some understanding of the major requirements for the system is essential. Three key considerations involved in the feasibility analysis are,

- Economic feasibility
- Technical feasibility
- Social feasibility

ECONOMICAL FEASIBILITY:

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the government can pour into the development of the system is limited. The expenditures must be justified. Only the customized products had to be purchased.

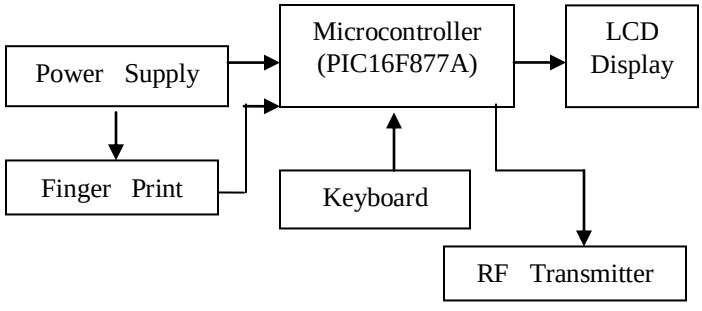
TECHNICAL FEASIBILITY:

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. This will lead to high demands being placed on the government. The designed system must have a modest requirement, as only minimal or null changes are required for implementing the system.

SOCIAL FEASIBILITY:

The aspect of study is to check the level of acceptance of the system by the government. The people must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the user depends on that are employed to educate the user about the system and to make familiar with it.

BLOCK DIAGRAM



FUTURE ENHANCEMENTS

In this paper as we are using biometrics which can't be changed till death for further more accurate specification Iris and voice recognition can also be implemented instead of finger print recognition. If this project come in use number of ATM centers with touch screen will increase which make people life more comfortable for banking as well as voting.

REFERENCES

1. Pynchon and Garber,"Sarasota's Vanished Votes: An Investigation into the Cause of Uncounted Votes in the 2006 Congressional District 13 Race in Sarasota County, Florida", Florida Fair Elections Center Report, January 2008.

2. P.Neumann,"Security Criteria for Electronic Voting", in proceedings of the National Computer Security Conference, 1993.

3. K.P.Yee,"Building Reliable Voting Machine Software", Ph.D.dissertation, University of California, Berkeley, 2007.

4. N.Sastry and D.Wagner,"Designing Voting Machines for Verification", in proceedings of the USENIX Security

5. T.Kohno, A.stubblefield, A.Rubin, and.Wallach, Analysis of an Electronic Voting System", in Proceedings of the IEEE Symposium on Security and Privacy,2004,pp.27-40.

6. W.Vigna,g; Software Engineering,IEEE Transaction Accepted for the future Publication, Volume PP,Forthcoming,2009 Pages:1-24.

7. A.Rubin,"Security considerations for Remote Electronic Voting", Communications of the ACM, vol.45, no.12, pp39-44, 2002.

8. Michael J.Radwin, "An untraceable, universally verifiable voting scheme," 1995.

9. Safevote, "Voting System Requirements", Safevote, Inc. and the Bell, 2001. 2
10. Sako, Kazue and Kilian, Joe, "Receipt-free Mix-Type voting Scheme: A Practical Solution to the Implementation of a Voting Booth," EUROCRYPT'95, vol921, Lecture Notes in Computer Science, pp.393-403, Springer-Verilog, 1995.
11. Susan King Roth, "Disenfranchised by design: voting systems and the election process," Information design Journal, vol.9, no.1, 1998.
12. Pedro A.D. Rezoned, "Electronic Voting Systems-Is Brazil Abed of its Time?," RSA Laboratories, Volume7, no.2,2004.

EFFICIENT INTRA NETWORK ROUTING WITH CHANNEL COMMUNICATION IN WIRELESS MESH NETWORKS

Azhagu Lakshmi S[1] ,
[1]Final Year ME, Dept. of CSE, S.Veerasamy
Chettiar College Of Engg & Tech, Puliangudi
E-Mail: anbualgu41@gmail

Dhakshana Moorthy K[2]
[2]Assistant Professor ,Dept. of CSE, S.Veerasamy
Chettiar College Of Engg & Tech, Puliangudi
E-mail: dhakshanam83@gmail.com

Abstract: **Multicasting can be an effective routing service in wireless mesh networks (WMNs). WMNs require efficient and reliable multicast communication, i.e., with high delivery ratio but with less overhead among a group of recipients. In Multi-Rate multi-Channel Multicast with intra-flow Network Coding (RCMNC), which solves the joint channel assignment, rate selection and flow allocation problems for multi-hop intra flow network coding multicast. In RCMNC mesh environments, when the number of nodes gets increased there is a possibilities for congestion. To mitigate the issue QoS with congestion control Algorithm is introduced to monitor the system that detect when and where congestion occurs.**

Key Words: **Wireless Mesh Networks. Wireless multi-hop networks, multi-radio.**

I.INTRODUCTION

A wireless mesh network(WMN) is a wireless network made up of radio nodes organized in a mesh topology. Each node forwards messages on behalf of the other nodes. Mesh networks can "selfheal", automatically re-routing around a node that has lost power . A wireless network is any type of computer network that uses wireless data connections for connecting network nodes.Wireless networking is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure. Wireless mesh networks (WMN), an emerging technology, may bring the dream of a seamlessly connected world into reality. WMN can easily and wirelessly connect entire cites using inexpensive, existing technology. Traditional networks relay on a small number of networks to run faster, because local packets don't have to travel back to a central server.

A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may but need not connect to the Internet.

Many stationary routers in a WMN are now equipped with multiple network interfaces to utilize orthogonal channels [2] and relay data via multi-hop forwarding to various destinations [3]. In light of the above trend, a number of works (e.g., [4]–[6]) have improved the allocation of network resources, such as routing paths, channels and transmission bit-rates, to maximize the throughput of uni cast traffic in a WMN.

The intra-flow NC approaches in [7] mainly focus on system design and implementation issues in a single channel single-rate mesh. However, without an optimized resource allocation scheme, it is difficult to fully unveil the advantage of intra-flow NC in the latest multi-rate multichannel wireless network, because the capacity of a mesh network is closely related to how traffic is flowed at which physical transmission bit-rate on what channel. With this observation in mind, we explore a new optimization problem, RCMNC, to maximize the throughput for multi-Rate multi-Channel Multicast with intra-flow Network-Coding in WMNs, and this work is orthogonal and complementary to the previous studies [9] [7]. The problem is challenging due to various tradeoffs between channel assignment and rate selection in a multi-channel multi-rate mesh network with intra-flow NC.

A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh

routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may but need not connect to the Internet.

II. EXISTING SYSTEM

2.1 Intra-flow network coding

Wireless network coding has been shown to reduce the number of transmissions by exploiting the broadcast nature of the wireless medium. Multiple packets may be encoded into a single packet when their respective next hops have enough information to decode them. Previous research has shown that packets belonging to different flows may be encoded (interflow coding) when they are passing through a common router. Similarly, it has also been shown that coding packets of the same flow (intra-flow coding) may provide better reliability by not relying on the reception of any single packet. In this work, we first present IMIX, an intra-flow wireless network coding scheme which has the potential to save transmissions and therefore improve network throughput. The main idea of inter-flow coding is to leverage the abundant packet overhearing opportunities in wireless networks in order to reduce redundant transmissions, and to improve performance by having a node combine multiple unicasts into a single broadcast. The first system design and implementation of intra-flow NC for both wireless unicast and multicast They therefore propose *CodeOR*, which transmits multiple batches concurrently, and analyze how to improve the performance by tuning the number of batches that should be sent concurrently. The problem is challenging due to various tradeoffs between channel assignment and rate selection in a multi-channel multi-rate mesh network with intra-flow NC.Nodes must find an efficient way to contend for the wireless channel bandwidth and cooperatively deliver coded packets so that all the multicast destinations can decode the packets successfully and achieve a high throughput

2.2 Multipath Routing in Wireless Mesh Networks

Wireless Mesh Networks are envisioned to support the wired backbone with a wireless backbone for providing internet connectivity to residential areas and offices. A novel multi-path hybrid routing protocol, Multipath Mesh (MMESH), that effectively discovers multiple paths. We also propose elegant traffic splitting algorithms for balancing traffic over these multiple paths to synergistically improve the overall performance. in WMNs, traffic is primarily routed either towards the IGWs or from the IGWs to the APs. Thus if multiple APs choose the best path towards a gateway, the traffic in this path increases. As more traffic is routed through a best route, it increases the load on the intermediate MRs and thereby deteriorating the overall performance of the path. As can be noticed this performance degradation is due to the traffic build up on certain hot paths. But, if we utilize multiple paths to balance the traffic, such a situation would seldom occur. We propose to exploit these multiple paths to synergistically improve the overall performance in a WMN.

2.3 Channel Assignment in Wireless Mesh Networks

The wireless mesh network is envisaged to be one of the key components in the converged networks of the future, providing flexible high bandwidth wireless backhaul over large geographical areas. While single radio mesh nodes operating on a single channel suffer from capacity constraints, equipping mesh routers with multiple radios using multiple non overlapping channels can significantly alleviate the capacity problem and increase the aggregate bandwidth available to the network. However, the assignment of channels to the radio interfaces poses significant challenges. The goal of channel assignment algorithms in multiradio mesh networks is to minimize interference while improving the aggregate network capacity and maintaining the connectivity of the network. In this article we examine the unique constraints of channel assignment in wireless mesh networks and identify the key factors governing assignment schemes, with particular reference to interference, traffic patterns, and multipath connectivity. After presenting taxonomy of existing channel assignment algorithms for WMNs, we describe a new channel assignment scheme called MesTiC, which incorporates the mesh traffic pattern together with connectivity issues in order to minimize interference in multradio mesh networks

2.4 Multirate Multi-Channel Environment

In a multirate wireless network, low data rate nodes consume proportionately more channel resources than high data rate nodes, resulting in low overall network performance. The use of multiple non-overlapping frequency channels in multirate wireless networks can overcome the performance degradation by having nodes communicate on different channels based on their data rates. However, no effort has been invested to utilize the multiple channels for a multirate wireless network. We introduce the Data Rate

Adaptive Channel Assignment (DR-CA) algorithm for a multichannel multirate single-hop wireless network to provide higher network throughput and network efficiency. The main idea is to assign links having same or comparable data rates on the same channel to minimize the wastage of channel resources due to interference between high data links and low data rate links. We also design a new Intermediary Multichannel Layer (IML) which resides between network layer and link layer, at which we implement the DR-CA algorithm. The IML design requires no modifications to the underlying MAC layer and upper layers of the network stack. We define new performance metrics-channel efficiency and network efficiency for a multichannel multirate wireless network. Using OPNET simulations, we show that the multichannel enhancement using our proposed algorithm provides significant performance improvement in terms of network throughput, channel efficiency, and network efficiency over existing approaches in multirate wireless networks. Under heavy load condition, the network efficiency using DR-CA algorithm reaches 90% of the maximum limit. To the best of our knowledge, this is the first work to utilize the benefits of multiple channels in the multirate wireless network environment.

III. PROPOSED SYSTEM

We propose a congestion method, Integrating QoS with congestion control Algorithm is introduced to decrease delay and packet loss when the bandwidth is high.

3.1 Congestion Control

Congestion control Algorithm used to improve the Quality of Service when a link or node is carrying so much data.QoS with congestion control Algorithm is introduced to decrease delay and packet loss when the bandwidth is high. There is a possibility for congestion when the number of nodes gets increased. a new optimization problem, RCMNC, to maximize the throughput for multirate multi-channel multicast with intra-flow NC, and prove that it is NP-hard. We jointly consider channel assignment, rate selection and flow allocation to properly solve the problem.

3.2 Integrate Congestion Control Algorithm

To avoid co-channel interference or leakage interference from adjacent channels, each node uses 802.11 carrier sense to detect whether the channel is occupied by neighboring nodes. If the detected signal amplitude is lower than the carrier sense threshold, nodes can contend for the idle medium using 802.11 random backoff, and the winner can go forwarding the coded packet. Since each forwarder might experience different channel conditions and have different numbers of neighboring nodes, the performance of such intra-flow network coding mainly depends on how many packets each forwarder needs to send. In MORE, each node performs a credit-based heuristic approach to determine whether it should forward a coded packet in a single-rate single-channel network.

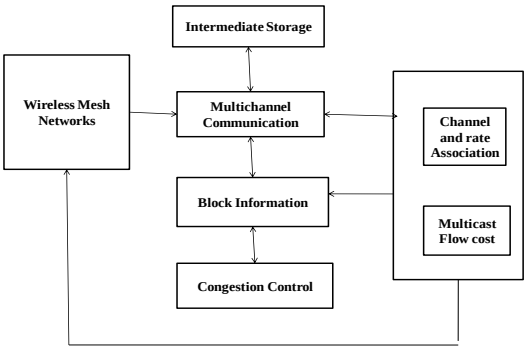


Figure 1: Congestion Control

Our problem also requires the edges in the same broadcasting conflict clique to share the bandwidth. Therefore, to solve the *node-capacitated* min-cost flow problem, we design an algorithm that first transforms the *node-capacitated* problem to a *link-capacitated* problem, and then propose a variant of the cycle-canceling algorithm [33] to solve the resulting *link-capacitated* min-cost flow problem in a lossy wireless environment. To realize the above approach, we reformulate the original model graph G as a flow graph GF such that the node capacity bound in G can be transformed to the link capacity bound in GF.

IV. EXPERIMENTAL DATA

We have succeeded to find efficient algorithms to solve several important problems such as SHORTHEST PATHS, NETWORK FLOWS. We have seen, most of practical graph or network problems are N P-complete and hard to solve. In such a case, it may be interesting to solve a simplified problem to obtain approximations or bounds on the initial hardest problem. Consider the following optimization problem where $f : R^n \rightarrow R$ and $S \subseteq R^n$:

Minimize f(x)
subject to $x \in S$

A relaxation of the above problem has the following form:

Minimize $f_R(x)$
subject to $x \in S_R$

where $f_R : R^n \rightarrow R$ is such that $f_R(x) \leq f(x)$ for any $x \in S$ and $S \subseteq S_R$. It is clear that the

optimal solution f ∗ R of the relaxation is a lower bound of the optimal solution of the initial problem. In previous section, the considered problems are such that S = X ∩{0,1}n where X ⊆Rn (or X ⊆Qn) and the fractional relaxation corresponds to consider fR = f and SR =X.

A large number of these problems have an underlying network structure. The idea of the Lagrangian Relaxation is to try to use the underlying network structure of these problems in order to use these efficient algorithms. The Lagrangian Relaxation is a method of decomposition: the constraints S = S1∪S2 of the problems are separated into two groups, namely the'easy' constraints S1 and the'hard' constraints S2. The hard constraints are then removed, i.e., SR =S1 and transferred into the objective function, i.e., fR depends on f and S2.

4.1 Experimental Results and Comparison

To compare integrating congestion control algorithm If the detected signal amplitude is lower than the carrier sense threshold, nodes can contend for the idle medium using 802.11 random backoff, and the winner can go forwarding the coded packet. Since each forwarder might experience different channel conditions and have different numbers of neighboring nodes, the performance of such intra-flow network coding mainly depends on how many packets each forwarder needs to send. In MORE, each node performs a credit-based heuristic approach to determine whether it should forward a coded packet in a single-rate single-channel network.

4.2 The Lagrangian Relaxation Technique

The Lagrangian dual of an optimization problem and show that the solution of the Lagrangian dual provides a lower (resp., upper) bound of the initial minimization (resp., maximization) problem. Moreover, in the case of (convex) linear programmes, the optimal solution of the Lagrangian dual coincides with the optimal solution of the initial problem. Also, the bound obtained thanks to the Lagrangian relaxation is at least as good as the one obtained from fractional relaxation.

Lagrangian dual

Consider the following integer linear programme:

$$\text{Minimize } cTx$$
$$\text{subject to}$$
$$Ax=b$$
$$x\in X$$

The Lagrangian relaxation procedure uses the idea of relaxing the explicit linear constraints by bringing them into the objective function with associated vector μ called the Lagrange multiplier. We refer to the resulting problem

$$\text{Minimize } cTx+\mu T(Ax-b)$$
$$\text{subject to}$$
$$x\in X$$

as the Lagrangian relaxation or Lagrangian subproblem or the original problem (12.3), and we refer to the function $L(\mu) =\min\{cTx+\mu T(Ax-b)|\ x\in X\}$, as the Lagrangian function.

V. CONCLUSION AND FUTURE WORK

A multi-rate multichannel intra-flow network coding scheme for multicast. We formulate an optimization model that considers the channel assignment, rate selection and flow allocation problems jointly to maximize the network coding gain for a wireless mesh network supporting multiple bit-rates and channels Congestion control Algorithm used to improve the Quality of Service when a link or node is carrying so much data. QoS with congestion control Algorithm is introduced to decrease delay and packet loss when the bandwidth is high.

VI. REFERENCES

[1] D. S. Lun, M. Medard, and R. Koetter, "Network Coding for Efficient Wireless Unicast," in *Proc. of International Zurich Seminar on Communications (IZS)*, 2006.

[2] S. Biswas and R. Morris, "ExOR: Opportunistic Multi-Hop Routing for Wireless Networks," in *Proc. of ACM SIGCOMM*, 2005

[3] R. Draves, J. Padhye, and B. Zill, "Routing in Multi-Radio, Multi- Hop Wireless Mesh Networks," Proc. ACM MobiCom, pp. 114-128, 2004

.[4] C.T. Chou and A. Misra, "Low Latency Multimedia Broadcast in Multi-Rate Wireless Meshes," Proc. First IEEE Workshop Wireless Mesh Networks (WiMesh '05), in Conjunction with IEEE Sensor and Ad Hoc Comm. and Networks (SECON '05), 2005

.[5]R. Srikant, The Mathematics of Internet Congestion Control. Birkhauser, 2003

[6] A. Eryilmaz and R. Srikant, "Joint congestion control, routing and mac for stability and fairness in wireless networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 8, pp. 1514–1524, August 2006

[7] M. Neely, "Optimal backpressure routing for wireless networks with multi-receiver diversity," in Conference on Information Science and Systems, March 2006.

[8] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "MORE: A network coding approach to

opportunistic routing," in MIT-CSAIL-TR-2006-049, 2006
[9] K. Zeng, W. Lou, and H. Zhai, "On end-to-end throughput of opportunistic routing in multirate and multihop wireless networks," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 816–824
.[10] D. Traskov, N. Ratnakar, D. S. Lun, R. Koetter, and M. Medard, "Network coding for multiple unicasts: An approach based on linear optimization," in *Proc. IEEE ISIT*, Jul. 2006, pp. 1758–1762.
[11] S. Sengupta, S. Rayanchu, and S. Banerjee, "An analysis of wireless network coding for unicast sessions: The case for coding-aware routing," in *Proc. IEEE INFOCOM*, May 2007, pp. 1028–1036
[12] D. S. Lun, M. Medard, and R. Koetter, "Efficient operation of wireless packet networks using network coding," in *Proc. IWCT*, Jun. 2005.

Providing Secure Communication Scheme Using Cluster in Networks

G.Sheeba

PG Scholar, Computer Science And Engineering

Renganayagi Varatharaj College of Engineering

cbakrishnan@gmail.com

***Abstract*--- Providing Secure Communication Scheme Using Cluster in Networks for large scale dense ad-hoc networks combines the advantages of the time management and secure message transfer. By creating cluster to reduce overhead and ensure scalability. Multicast traffic within a cluster employs a one-way hash function chain in order to authenticate the message source. Each cluster uses a unique subset of keys to look for its distinct combination of valid Signature in the message in order to authenticate the source. In particular the provided network services need to achieve the following security goals:**

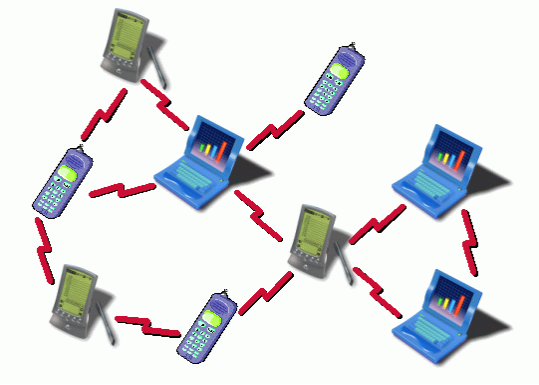
(1) Confidentiality, to protect data during message transfer.

(2) Message integrity, to prevent tampering with transmitted messages.

Therefore, authenticating the source and ensuring the integrity of the message traffic become a fundamental requirement for the operation and management of the network.

I. INTRODUCTION

Ad-hoc networks are becoming an effective tool for many mission critical applications such as troop coordination in a combat field, situational awareness, etc. These applications are characterized by the hostile environment that they serve in and by the multicast-style of communication traffic. Group communication is considered a critical service in adhoc networks due to their inherently collaborative operations, where the nodes cooperate in network management and strive to accomplish common missions autonomously in highly unpredictable environment without reliance on infrastructure equipment. Connecting to files on other computers and/or the Internet without the need for a wireless router is the main advantage of using an ad hoc network. Because of this, running an ad hoc network can be more affordable than a traditional network. No expensive infrastructure must be installed. Use of ad-hoc networks can increase mobility and scalability. Creating an ad hoc network from scratch requires a few settings changes and no additional hardware or software. If needed , to connect multiple computers quickly and easily, then an ad hoc network is an ideal solution. It is well suited to free unlicensed spectrum.



Wireless communication enables information transfer among a network of disconnected, and often mobile, users. Popular wireless networks such as mobile phone networks and wireless LANs are traditionally infrastructure-based, i.e. base stations, access points and servers are deployed before the network can be used. In contrast, ad hoc networks are dynamically formed amongst a group of wireless users and require no existing infrastructure or pre-configuration

Ad-Hoc Networks

The dynamic and self-organizing nature of ad hoc networks makes them particular useful in situations where rapid network deployments are required or it is prohibitively costly to deploy and manage network infrastructure.

I. PROBLEM STATEMENT

This problem statement defines about that it will authenticating the source, ensuring the integrity of the message traffic and scalability for large scale dense adhoc networks. A systematic classification of these clustering schemes enables one to better understand and make improvements. In mobile ad hoc networks, the movement of the network nodes may quickly change the topology resulting in the increase of the overhead message in topology maintenance. Protocols try to keep the number of nodes in a cluster around a pre-defined threshold to facilitate the optimal operation of the medium access control protocol. The clusterhead election is invoked on-demand, and is aimed to reduce the computation and communication costs. A large variety of approaches for ad hoc clustering have been developed by researchers which focus on different performance metrics. **A unique ID is assigned to each node. Nodes know the ID of its neighbors and clusterhead is chosen following some certain rules as given below.**

A. Lowest ID cluster algorithm (LIC)

LIC is an algorithm in which a node with the minimum *id* is chosen as a clusterhead. Thus, the *ids* of the neighbors of the clusterhead will be higher than that of the clusterhead. A node is called a gateway if it lies within the transmission range of two or more clusterheads. Gateway nodes are generally used for routing between clusters. Each node is assigned a distinct *id*. Periodically, the node broadcasts the list of nodes that it can hear (including itself).

• A node which only hears nodes with *id* higher than itself is a clusterhead.

• The lowest-*id* node that a node hears is its clusterhead, unless the lowest-*id* specifically gives up its role as a clusterhead (deferring to a yet lower *id* node).

• A node which can hear two or more clusterheads is a gateway.

• Otherwise, a node is an ordinary node. The Lowest-ID scheme concerns only with the lowest node *ids* which are arbitrarily assigned numbers without considering any other qualifications of a node for election as a clusterhead. Since the node *ids* do not change with time, those with smaller *ids* are more likely to become clusterheads than nodes with larger *ids*. Thus, drawback of lowest ID algorithm is that certain nodes are prone to power drainage due to serving as clusterheads for longer periods of time.

B. Security in Ad-Hoc Networks

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wireline networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open

peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. These challenges clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. In this article consider a fundamental security problem in MANET: the protection of its basic functionality to deliver data bits from one node to another. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. There are basically two approaches to protecting MANETs: proactive and reactive. The proactive approach attempts to prevent an attacker from launching attacks in the first place, typically through various cryptographic techniques.

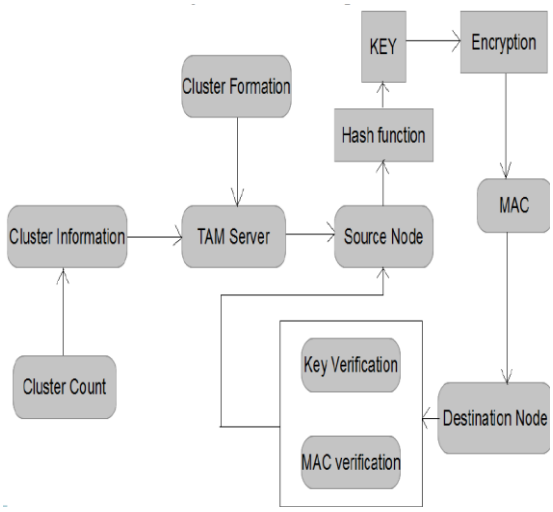
C. Digital signature

Digital signature is based on asymmetric key cryptography (e.g., RSA),which involves much more computation overhead in signing decrypting and verifying encrypting operations. It is less resilient against DoS attacks since an attacker may feed a victim node with a large number of bogus signatures to exhaust the victim's computation resources for verifying them. Each node also needs to keep a certificate revocation list (CRL) of revoked certificates. However, a digital signature can be verifiedby any node given that it knows the public key of the signing node. This makes digital signature scalable to large numbers of receivers. Only a total number of *n* public/private key pairs need be maintained in a network of n nodes

II. SYSTEM ARCHITECTURE

Cross-cluster multicast traffic includes message authentication codes (MACs) that are based on a set of keys. Each cluster uses a unique subset of keys to look for its distinct combination of valid MACs in the message in order to authenticate the source.

The asymmetry property denotes that a receiver can verify the message origin using the MAC in a packet without knowing how to generate the MAC. This property is the key for preventing impersonation of data sources.



System Design

III. CRYPTOGRAPHIC ALGORITHM

Source and message authentication is the corroboration that a message has not been changed and the sender of a message is as claimed to be. This can be done by sending a (1) Cryptographic digital signature, or (2) Message Authentication Code (MAC) . The first involves asymmetric cryptography and often needs heavy computation both at the sender and the receiver. The latter involves creating a message and source specific MAC that can be verified by the receiver. Thus,

the MAC implicitly ensures message and source integrity. In unicast, a shared secret key is used for MAC generation. Unfortunately, the use of a single shared key in multicast makes the group vulnerable to source impersonation by a compromised receiver. Dealing with multicast as a set of unicast transmissions each with a unique shared key is the most inefficient approach for addressing this concern.

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES-256 respectively. As well as these differences AES differs from DES in that it is not a feistel structure. Recall that in a feistel structure, half of the data block is used to modify the other half of the data block and then the halves are swapped. In this case the entire data block is processed in parallel during each round using substitutions and permutations.

A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key. This description of the AES algorithm therefore describes this particular implementation.

Rijndael was designed to have the following characteristics:

• Resistance against all known attacks.
• Speed and code compactness on a wide range of platforms.
• Design Simplicity.

The input is a single 128 bit block both for decryption and encryption and is known as the **in** matrix. This block is copied into a **state** array which is modified at each stage of the algorithm and then copied to an output matrix . Both the plaintext and key are depicted as a 128 bit square matrix of bytes. This key is then expanded into an array of key schedule words(the **w** matrix). It must be noted that the ordering of bytes within the **in** matrix is by column. The same applies to the **w** matrix.

IV. ADAPTATION OF KEY GENERATION AND DIGITAL SIGNATURE

Cryptographic digital signatures use public key algorithms to provide data integrity. When you sign data with a digital signature, someone else can verify the signature, and can prove that the data originated from you and was not altered after you signed it. For more information about digital signatures, see Cryptographic Services.

A. MD5 Algorithm

MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits fewer than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 2^{64}.

The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted *A*, *B*, *C* and *D*. These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, termed *rounds*; each round is composed of 16 similar operations based on a non-linear function *F*, modular addition, and left rotation. Figure 1 illustrates one operation within a round. There are four possible functions *F*; a different one is used in each route.

B. *Key Generation*

Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted.

C. *Cyclic redundancy code*

A cyclic redundancy check (CRC) is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Blocks of data entering these systems get a short check value attached, based on the remainder of a polynomial division of their contents; on retrieval the calculation is repeated, and corrective action can be taken against presumed data corruption if the check values do not match.

CRCs are so called because the check (data verification) value is a redundancy (it expands the message without adding information) and the algorithm is based on cyclic codes. CRCs are popular because they are simple to implement in binary hardware, easy to analyze mathematically, and particularly good at detecting common errors caused by noise in transmission channels. Because the check value has a fixed length, the function that generates it is occasionally used as a hash function. CRCs are specifically designed to protect against common types of errors on communication channels, where they can provide quick and reasonable assurance of the integrity of messages delivered.

V. CONCLUSION

Securing such traffic is of great importance, particularly authenticating the source and message to prevent any infiltration attempts by an intruder. In this project, security was achieved by usage of cryptographic algorithm and time management by creation of clusters. Exploits network clustering in order to cut overhead and ensure scalability. which pursues a two tired hierarchical strategy combining both time and secret-information asymmetry in order to achieve scalability and resource efficiency .A detailed analysis, design and implementation is successfully developed.

Multiple factors make multicast authentication in ad-hoc networks very challenging. Ad-hoc networks are becoming an effective tool for many mission critical applications such as troop coordination in a combat field, situational awareness, etc. These applications are characterized by the hostile environment that they serve in and by the multicast-style of communication traffic. Therefore, authenticating the source and ensuring the integrity of the message traffic become a fundamental requirement for the operation and management of the network.

VI. REFERENCES

[1] H. Yang, *et al.*, "Security in mobile ad-hoc wireless networks: challenges and solutions," *IEEE Wireless Commun. Mag.*, vol. 11, no. 1, pp. 1536–1284, Feb. 2004.

[2] Perrig, *et al.*, "Efficient and secure source authentication for multicast," in *Proc. 2001 Network Distributed System Security Symposium*.

[3] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P. Spilling, "A survey of key management in ad hoc networks," *IEEE Commun. Surveys & Tutorials*, vol. 8, no. 3, pp. 48–66, Dec. 2006.

[4] M. Youssef, A. Youssef, and M. Younis, "Overlapping multihop clustering for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*,vol. 20, no. 12, pp. 1844–1856, Dec. 2009.

[5] R. Azarderskhsh and A. Reyhani-Masoleh, "Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks,"*EURASIP J. Wireless Commun. Netw.*, vol. 2011, article ID 893592, 2011.

[6] L. Wang and F. Gao, "A secure clustering scheme protocol for MANET," in *Proc. 2010 International Conf. Multimedia Inf. Netw. Security*.

[7] R. Canetti *et al.*, "Multicast security: a taxonomy and efficient constructions," in *Proc. 1999 IEEE INFOCOM*.

[8] F. R. Yu, H. Tang, P. Mason, and F. Wang, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks," *IEEE Trans. Netw. Service Management*, vol. 7, no. 4, pp. 258–267, Dec. 2010.

[9] Ratish Agarwal et al / International Journal on Computer Science and Engineering Vol.1(2), 2009, 98-104

[10] E. Royer, and C. E. Perkins, "Multicast operation of the ad hoc ondemand distance vector routing protocol", In the proceedings of MobiCom, pages 207-218, Aug. 1999.

[11] Sung-Ju Lee, William Su, and Mario Gerla, "On- demand multicast routing protocol (ODMRP) for ad hoc networks", Internet Draft, draftietfmanet-odmrp-02.txt, 2000.

[12] Mauve, M., Füßler, H., Widmer, J., Lang, T., "Poster: Position-Based Multicast Routing for Mobile Ad-Hoc Networks", In Proceedings of Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing: MobiHoc, 2003.

[13] G. Hanaoka, T. Nishioka, Y. Zheng, and H. Imai, "A hierarchical non-interactive key-sharing scheme with low memory size and high resistance against collusion attacks," *Computer J.*, vol. 45, no. 3, pp. 293–303, 2002.

[14] M. Younis, K. Ghumman, and M. Eltoweissy, "Location-aware combinatorial key management scheme for clustered sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 17, no. 18, pp. 865–882, Aug. 2006.

[15] E. C. H. Ngai and M. R. Lyu, "An authentication service based on trust and clustering in wireless ad hoc networks: description and security evaluation," in *Proc. 2006 IEEE International Conf. Sensor Networks, Ubiquitous, Trustworthy Computing*.

[16] Y. Lu, B. Zhou, F. Jia, and M. Gerla, "Group-based secure source authentication protocol for VANETs," in *Proc. 2010 IEEE GLOBECOM Workshop Heterogeneous, Multi-hop Wireless Mobile Networks*.

[17] M. Youssef, A. Youssef, and M. Younis, "Overlapping multihop clustering

for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 12, pp. 1844–1856, Dec. 2009.
[18] J. Y. Yu and P. H. J. Chong, "A survey of clustering schemes for mobile ad hoc networks," *IEEE Commun. Surveys & Tutorials*, vol. 1, no. 1, pp. 31–48, 2005.
[19] P. B. Velloso, *et al.*, "Trust management in mobile ad hoc networks using a scalable maturity-based model," *IEEE Trans. Network Service Management*, vol. 7, no. 3, Sep. 2010.
[20] R. Azarderskhsh and A. Reyhani-Masoleh, "Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2011, article ID 893592, 2011.
[21] L. Wang and F. Gao, "A secure clustering scheme protocol for MANET," in *Proc. 2010 International Conf. Multimedia Inf. Netw. Security*.
[22] L. Junhai, Y. Danxia, X. Liu, and F. Mingyu, "A survey of multicast routing protocols for mobile ad-hoc networks," *IEEE Commun. Surveys & Tutorials*, vol. 11, no. 1, pp. 78–91, first quarter 2009.
[23] M. Younis, O. Farrag, and S. Lee, "Cluster mesh based multicast routing in MANET: an analytical study," in *Proc. 2011 IEEE International Conf. Commun.*.
[24] D. Balfanz, *et al.*, "Talking to strangers: authentication in ad-hoc wireless networks," in *Proc. 2002 Network Distrib. System Security Symposium*.
[25] K. Marzullo and S. Owicki, "Maintaining the time in a distributed system," in *Proc. 1983 ACM Symposium Principles Distrib. Computing*.
[26] A. Savvides, C. C. Han, and M. Srivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proc. 2001 ACM International Conf. Mobile Computing Netw.*, pp. 166–179.
[27] The Network Simulator - ns-2. Available: http://www.isi.edu/nsnam/ns/
[28] G. Angione, P. Bellavista, A. Corradi, and E. Magistretti, "A *k*-hop clustering protocol for dense mobile ad-hoc networks," in *Proc. 2006 IEEE International Conf. Distrib. Computing Systems Workshop*.
[29] E. M. Royer and C. Perkins, "Multicast ad-hoc on-demand distance vector (MAODV) routing," Internet Draft, University of California, Charles E. Perkins Nokia Research Center, July 2000.
[30] Y. Zhu and T. Kunz, "MAODV implementation for NS-2.26," Technical Report SCE-04-01, Dept. of Systems and Computing Engineering, Carleton University, Jan. 2004.

MOBILE AD-HOC NETWORK IN ACO

R.Shanmugapriya[1]
First year M.E students[1,] Department of computer science and engineering
[1] Renganayagi varatharaj college of engineering, Sivakasi.
[1]rspriyait011@gmail.com.

Abstract-Ants as other living systems have interactions or communications, which can be more or less stochastic. In the present paper we analyse how the level of errors during communication interferes with development and efficiency of recruitment process. When an ant walking to and from food source, it leaves some chemicals on the ground. When they have chosen a way out of other then they choose this with probability. But this probability depends on Pheromone. The study of the application of ACO to problems on online routing in telecommunication network. This class of problems has been identified in the hypothesis as the most appropriate for the application of the multi-agent, distributed and adaptive nature of the ACO architecture. We are using best-effort traffic in mobile ad-hoc networks is still under development ,but quite extensive results and comparison with a popular state-of-the-art algorithm are reported .In this paper an algorithm for routing in mobile ad-hoc networks based on ideas from the ant colony optimization is proposed .Ant behaviours match with node of ad-hoc network. Ant colony is also a distributed system as ad-hoc .Ants communicates indirectly by environment. There may be a possibility get solution for routing algorithm in ad-hoc networks by ant colony optimization. Mobile ad-hoc network consists of mobile hosts equipped with wireless communication devices. This algorithm is used to reduce the delay, increase the performance of the job and identify the shortest path from source to destination node.

Keywords—Ant colony optimization, node, channel.

I. INTRODUCTION

Ant Colony Optimization is a technique for optimization. The inspiring source of ant colony optimization is the foraging (shortest path network routing combinational optimization) behaviour of real ant colonies. This behaviour is exploited in artificial ant colonies for the search of approximate solutions to discrete optimization problems, to continuous optimization problems and to important problems in telecommunications such as routing and load balancing. Ad-hoc wireless network must be capable to self-organize and self –configure due to the fact that the mobile count routing often chooses routes that have significantly less capacity then the best paths that exist in the network .Most of the existing MANET protocols optimize hop count as building a route selection.

Mobile Ad-hoc networks inherit the common problems of wireless networking in general and add their own constraints specific to ad-hoc routing. Hence the primary goal in a mobile network is to efficiently establish one or more routes between two nodes so that they can communicate reliably. Such a network is characterized by the following challenges

1. The network topology can change dynamically due to the random movement of nodes.
2. Also any node may leave/join the network and the protocol must adapt accordingly
3. Although no guarantee of service can be provided, the protocol must be able to maximize the reliability of packet.

Network management of such a mobile network is hence a very big challenge. Also the fast changing nature and

the ad-hoc necessity of the network prevents the choice of a centralized solution which can decide the best route to route packets and at the same time minimize the different parameters like congestion, load, etc .Also no single node can take up the job of centralized manager due to the limited energy and processing capabilities of mobile nodes. The design of ad-hoc networks faces many unique challenges. Most of these arise due to two principle reasons. The first is that all nodes in an ad-hoc network, including the source node(s),the corresponding destination, as well as the routing nodes forwarding traffic between them, may be mobile .As the wireless transmission range is limited ,the wireless link between a pair of neighbouring nodes break as soon as they move out of range. Hence, the network topology, that is defined by the set of physical communication links in the network (wireless links between all pairs of nodes that can directly communicate with each other) can change frequently and unpredictably.

One of the major challenges in ad-hoc network is the security of connection between hosts in the network. The field of security for ad-hoc networks is at a very premature stage and this issue as to be thoroughly studied before mobile ad-hoc network system can be practically deployed in real world application. Therefore mobile ad-hoc networks are suitable for temporary communication links the biggest challenge in this kind of networks is to find a path between communication end points .This paper copes with, perform ability issues of nodes communication, independently from the causes behind service degradation. We aim at optimizing both performance and reliability measures by improving

- The throughput of data transfer through a lightweight mechanism.
- The quality of data transfer, so as to provide continuous network connectivity.

Mean while, unlike wired or wireless cellular networks, every mobile node has a limited transmission range. Therefore, two mobile nodes can communicate with each other directly, only if they are in the transmission range of each other.

To communicate with a peer outside its transmission range, a mobile node has to rely on one or more intermediate peers as relay. Due to the free movement of mobile nodes, both direct and indirect connection between peers can be disconnecting very frequently.

II. EXISTING SYSTEM:

The existing system is usually called a time-free asynchronous distributed system prone to process crashes .In these systems, a system designer can only assume an upper bound on the number of processes that can crash and, consequently, design protocols relying on the assumption that at least processes are alive. The protocol has no means to know whether a given process is alive or not.

Existing system using a algorithm is called as single processor scheduling algorithm. The main drawback of this algorithm is taking long time on data transmission between source to destination node and high delay. Since each ant takes more time to reach the destination. The main drawback of the existing paper is a single job value changes then also affect for total job value performance.

Drawbacks:

- More time take on data transmit between source and destination
- High delays occur in this kind of transmission.

III. PROPOSED SYSTEM:

Our model provides upper-layer applications with process state information according to the current system synchrony .The underlying system model is hybrid, comprised of a synchronous part and an asynchronous part. However, such a composition can vary over time in such a way that the system may become totally synchronous or totally asynchronous.

Modules:

- Identify the status of Node
- Message Transmission
- Change status
- Update status

Identify the Status Node:

In Figure.1, we identify the Node is weather live or not. In this process we easily identify the status of the node and also easily identify the path failure.

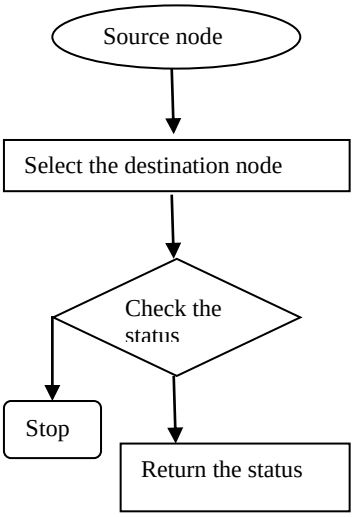


Figure 1: Identify the status of node

Message Transmission:

Figure 2; in this module we just transfer the message to the destination or intermediate nodes.

The intermediate node just forwards the message to destination.

The receiver receives the message and sends the Ack.

Change Status:

In this Module we identify the changed status of node. The Status is

- Live
- Uncertain
- Down

Update Status:

In this module we update the status of the node. Then only we can identify whether the node is live or not.

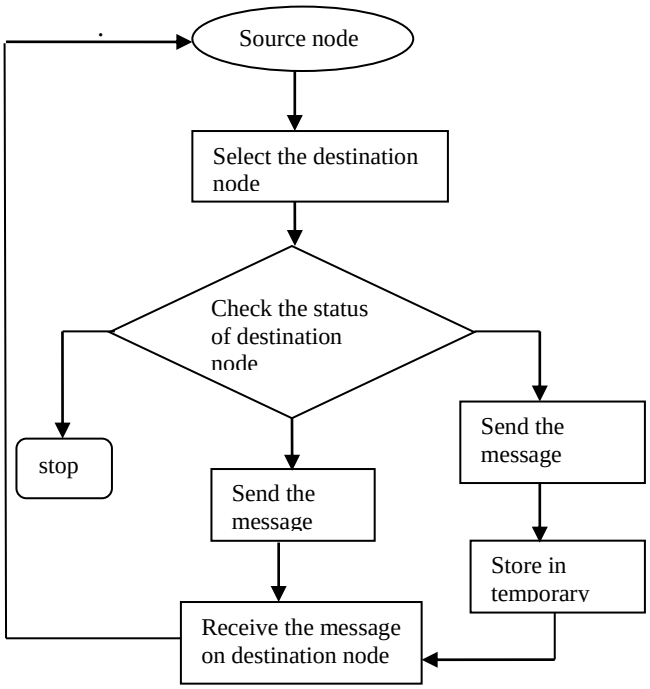


Figure2: Message Transmission

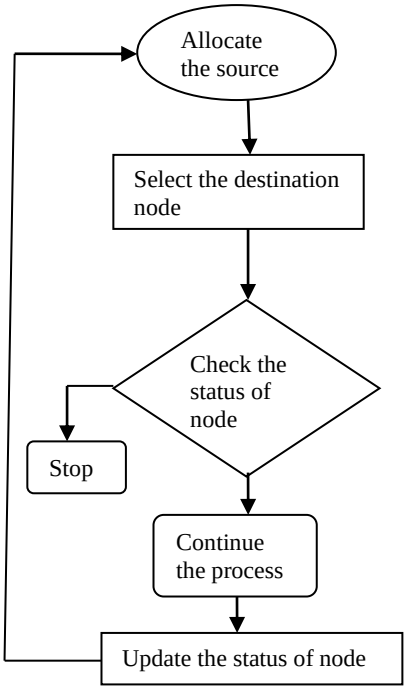


Figure 3: Update the status

The second module is also called as Message Transmission. Source node sends a request to destination node.

First, check if the destination node present or not. Three condition available in this module. They are,

- If the destination node present, then the message is send to destination node. This node sends Acknowledgment to Source node.
- If the destination node Uncertain, then the message is send to one of the temporary storage memory. This memory sends the message to destination node.
- If the destination node is alive. Then the process is stop

The third module of the project is updating the status of node. After the message transmission, the destination node will be change. The main process of the module is change and updates the status of the node. A single destination node will be change for next source node communicates to other place of the node. The main advantage of my project is, identify the shortest path on data transmission between source and destination node. Then decrease the delay of the transmission and also increase the performance of the job value. The destination node receive the message and send the Acknowledgment to source node .Mobile ad-hoc network solve the many unique challenges. Mainly, it has no any limitation. Therefore it has no any base station or access point. It also works in wired or wireless communication network.

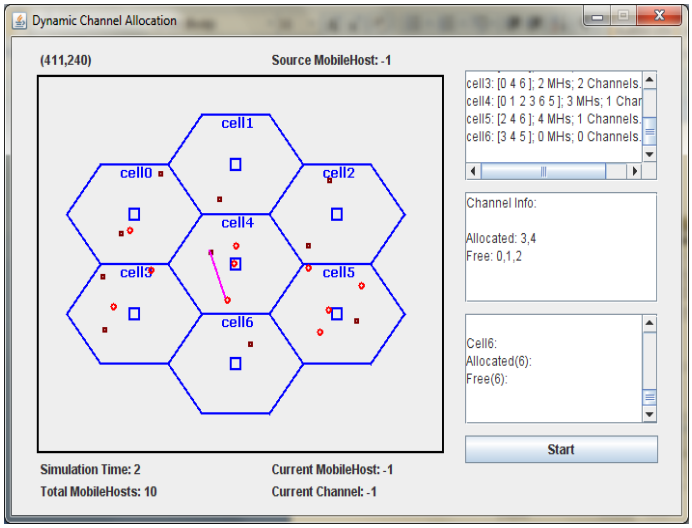
IV. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve change over and evaluation of change over methods.

Implementation is the process of converting a new system design into operation. It is the phase that focuses on user training, site preparation and file conversion for installing a candidate system. The important factor that should be considered here is that the conversion should not disrupt the functioning of the organization.

V. RESULT:



VI. CONCLUSION:

For the purpose of Ant colony optimization in mobile ad-hoc network, communicate between the nodes without need for any limitation (i.e, any base station).Three modules are using in this project. First module is, identify the status of node. Second module is, transmit the message between the two nodes, Third module is, update the status of node. These modules can increase the performance of the job value.

VII. REFERENCES

1. J.L. Denebourg, J.M. Pasteels J.C. Verhaeghe, ”Probabilistic behaviour in ants: A Strategy of errors?”J.Theoret.Biol. vol.105, pp.
2. Bibhash Roy, ”Ant colony based Routing for Mobile Ad-Hoc networks.vol.3, 2079-8407.
3. Ajay C solai jawahar, ”Ant colony optimization for Mobile Ad-Hoc network.
4. M. Dorigo and T. St” utzle ,Ant colony optimization .The MIT Press,2004.
5. M.Dorigo ,and L.M.Gambardella, ”Ant colonies for the travelling salesmen problem” Bio systems,43:73-81,1997.
6. J.L.Denebourg and S.Goss, ”Collective patterns and decision making, ”Ethology &Evolution,vol.1,pp.295-311,1989.
7. M.Dorigo, V.Maniezzo, and A.ColorniThe ant system: optimization by a colony of cooperating agents, ”IEEE Transactions on systems, Man, and Cybernetics-Part B,vol.26,no.1,pp.29-41,1996.

DIGITAL WATERMARKING SYSTEM FOR VIDEO AUTHENTICATION USING FPGA

S.V.Arthick Santhosh[1], Ms.Shani Sulaiman[2]

1. PG Student, Dhaanish Ahmed College Of Engineering

aarthicksanthosh@gmail.com

2. Assistant Professor, Dhaanish Ahmed College Of Engineering

Abstract: A video watermark is an indelible pattern embedded in video content that is imperceptible to the eye. By embedding a unique watermark into video material, content owners can identify copies of their materials. Every watermarking system has some very important desirable properties. Some of these properties are often conflicting and we are often forced to accept some trade-offs between these properties depending on the application of the watermarking system. This paper presents a digital watermarking system that can insert invisible, semi fragile watermark information into compressed video frames. The experiment result shows that the digital watermark is non-Perceptible, the watermark has been attacked.

IndexTerms:Invisible watermarking, data hiding, video authentication.

1. INTRODUCTION

Watermark is a kind of marker covertly embedded in a noise tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright information can be extracted even if it Authenticated.

2. CLASSIFICATION OF WATERMARKS

According to the domain in which video WM is performed, WM processing methods can be classified into two categories spatial domain and frequency domain. In the spatial domain, directly applying minor changes to the values of the pixels in a minor way is mainly used. This technique makes the embedded information hardly noticeable to the human eye. For example, pseudo-random WM works by a simple addition of a small amplitude pseudo-noise signal to the original media data.

WM is embedded in the transform coefficients and then it is inversely transformed to receive the watermarked data. The frequency domain methods are more robust than the spatial domain techniques.

WM techniques can also be divided into three different types: visible, invisible robust and invisible fragile. Different applications have different requirements. Sometimes a certain application requires a WM to be visible, so that the embedded watermark appears visible to a casual viewer. Invisible robust WMs are primarily used in applications such as copyright protection, which require the algorithm to be as robust as possible so that severe modifications and degradations cannot remove the watermark.

Conversely, invisible fragile is designed to reflect even slightest manipulation or modification of the media data, since the embedded watermark can easily become altered or destroyed after common attacks, such as lossy compression, cropping and spatial filtering.

3. EXISTING SYSTEM

In an existing system a watermarking algorithm that performs the broadcaster’s logo insertion as a

visible watermark in the DCT domain. The robustness of DCT watermarking arises from the fact that if an attack tries to remove watermarking at mid-frequencies, it will risk degrading the fidelity of the image because some perceptive details are at mid-frequencies. In the system architecture, the "watermark embedding" module performs the watermarking process. After that procedure, watermarked video frames are obtained. The rest of the units of the architecture essentially perform MPEG-4 compression of the video. The system has a controller which generates addressing and control signals to synchronize all components of the system.

4. PROPOSED SYSTEM

The proposed system comprises of four main modules such as video camera, video compression, watermark generation and water mark embedding.

Video camera is used to capture the video frames. The captured video frame is temporarily stored in the memory buffer, and then each block of the frame data is continuously processed by the video compressor units using DCT and quantization cores.

In the video compression technique, a video sequence is divided into multiple groups of pictures representing sets of video frames which are neighboring in display order. An encoded MPEG-2 video sequence is made up of two frame-encoded pictures: intra-frames and inter-frames. P-frames are forward prediction frames and B-frames are bidirectional prediction frames. Within a typical sequence of an encoded GOP, P-frames may be 10% of the size of I-frames and B frames are about 2% of the I-frames.

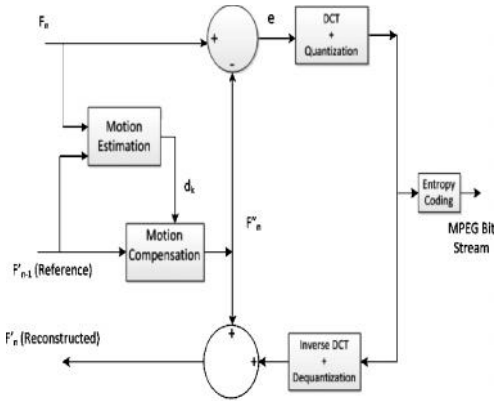


Fig.1 Block diagram of hybrid DPCM/DCT coding scheme

Differential Pulse Code Modulation (DPCM) is used to reduce temporal redundancy and DCT is used to reduce the spatial redundancy and this can be shown in Fig 1. Here, an input video frame F_n is compared with a reference frame F'_{n-1} and a motion estimation function finds a region in F'_{n-1} that matches the current macro-block in F_n. The offset between the current macro-block position and the chosen reference region is a motion vector, d_k. Based on this d_k, a motion compensated prediction F''_n is generated, and it is then subtracted from the current macro-block to produce a residual or prediction error. Motion compensation is an algorithmic technique employed in the encoding of video data for video compression. Motion compensation describes a picture in terms of the transformation of a reference picture to the current picture.

For proper decoding this motion vector, d_k has to be transmitted as well. The spatial redundancy in the prediction error of the predicted frames, and the I-frame is reduced by the following operations such as each frame is split into blocks of 8 × 8 pixels that are compressed using the DCT followed by quantization and entropy coding.

In the watermark generation the primitive watermark sequence is encoded into each frame and used with secret keys. Primitive watermark pattern is defined as the meaningful identifying sequence for each video frame. Hence this video frame contains time stamp, date, camera ID, frame serial number. The

manipulation such as frame exchange and substitution will be detected by specific watermark. The block diagram of the proposed novel watermark generator shown in Fig 2.

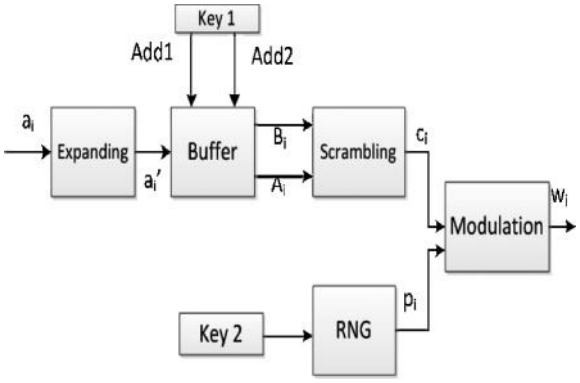


Fig.2 Block Diagram of proposed watermark generator

Watermark sequence c_i a pseudorandom sequence and thus difficult to detect, locate, and manipulate. A secure pseudorandom sequence p_i used for the modulation can be generated by an RNG structure using the Key 2.

Watermark embedding is done only in the I frames. It is understandable since B and P frames are predicted from I frames. If all I, B, P frames are watermarked, the watermarked data of the previous frame and the one of the current frame may accumulate, resulting in visual artifacts during decoding procedures. To avoid such a major issue, within each GOP of MPEG-2 video stream, only the I-frame is identified to be watermarked.

5. SIMULATION RESULT

The result for the behavioral simulation of the proposed system is shown below.

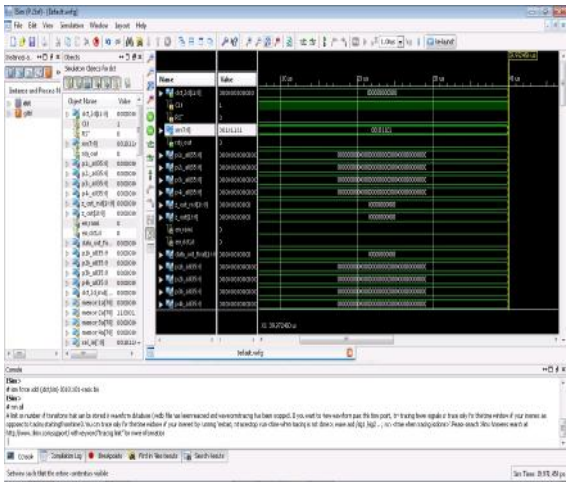


Fig.3 simulated output of compressed video frame

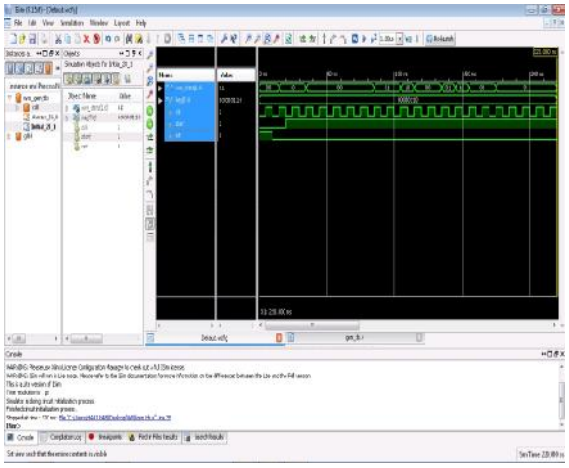


Fig.4 Simulated output of watermark generated

6. CONCLUSION

Digital watermarking holds significant promise as one of the keys to protecting proprietary digital content in the coming years. At its heart is the concept of embedding information inside a digital object such that the embedded information is inseparably bound to the object and the embedded information describes who may legally use and/or distribute the object, as well as who legally owns the object. Experimental result shows the simulation result of digital watermarking using Discrete cosine Transform in VHDL. This can be implemented on a FPGA / CPLD board and converted into a chip. As the explanations above show DCT is a better method to implement digital watermarking than FFT, SVD etc.

7. FUTURE IMPLEMENTATION

Future research should concentrate on applying the watermarking algorithm to other modern video compression standards, such as MPEG-4/H.264, so that it can be utilized in various commercial applications as well. Embedding the watermark information within high resolution video streams in real time is another challenge.

8. REFERENCE

[1] L.D.Strycker, P.Termont, J. Vandewege, J. Haitsma, A. Kalker, M. Maes, and G. Depovere, "Implementation of real-time digital watermarking process for broadcast monitoring on Trimedia VLIW

processor," Proc. Inst. Elect. Eng. Vision, Image Signal Process., vol. 147, no. 4, pp. 371–376, Aug. 2000.

[2] N. J. Mathai, A. Sheikholesami, and D. Kundur, "Hardware implementation perspectives of digital video watermarking algorithms," IEEE Trans. Signal Process., vol. 51, no. 4, pp. 925–938, Apr. 2003.

[3] N. J. Mathai, A. Sheikholesami, and D. Kundur, "VLSI implementation of a real-time video watermark embedder and detector," in Proc. Int. Symp. Circuits Syst., vol. 2. May 2003, pp. 772–775.

[4] T. H. Tsai and C. Y. Wu, "An implementation of configurable digital watermarking systems in MPEG video encoder," in Proc. Int. Conf. Consumer Electron., Jun. 2003, pp. 216–217.

[5] M. Maes, T. Kalker, J. P. Linnartz, J.Talstra, G. Depoyere, and J. Haitsma, "Digital watermarking for DVD video copy protection," IEEE Signal Process. Mag., vol. 17, no. 5, pp. 47–57, Sep. 2000.

[6] Y. Shoshan, A. Fish, G. A. Jullien, and O. Yadid-Pecht, "Hardware implementation of a DCT watermark for CMOS image sensors," in Proc. IEEE Int. Conf. Electron. Circuits Syst., Aug. 2008, pp. 368–371.

[7] G. Petitjean, J. L. Dugelay, S. Gabriele, C. Rey, and J. Nicolai, "Towards realtime video watermarking for systems-on-chip," in Proc. IEEE Int. Conf. Multimedia Expo, vol. 1. 2002, pp. 597–600.

A SMART LOCALIZATION TECHNIQUE FOR A ROBOTIC VEHICLE

Veerabaghu[1], U.T.Sasikala[2]
1. PG Scholar, Dhaanish Ahmed College of Engineering,
c.veerabaghu@gmail.com.
2. Assistant Professor, Dhaanish Ahmed College of Engineering,
utsasikala@gmail.com.

Abstract: It is important to obtain the real-time location of an autonomous ground robotic vehicle in both indoor and outdoor environment. In this paper the robot identifies the real-time localization through a set of self-integrated inexpensive sensors and infrequent GPS-augmentation. In which the robot identifies the local relative position with the help of accelerometer, the magnetic field sensor and the rotation sensors, whereas the GPS-augmentation is used to identify the global location and also corrects drifting errors.

Keywords: Accelerometer, Magnetic field sensor, Motor rotation sensors, GPS.

1. INTRODUCTION

In today's world, Robot plays a vital role in various fields which is uncomfortable to human beings or else it is difficult to human involvement, and finally the cost is expected to be as low as possible. process. At present robot have various applications such as industrial operations, Medical application, military operations, tour guide, and transportation so on. For these applications it is better that the robot is kept as small as possible to pass through narrow way such as a tunnel. To fulfill this process, it is important that the robotic vehicle has to obtain its accurate localization in real time. But at the same time there are some problems or difficulty in frequent calibration or managing external facilities, whereas these problems can be avoided with the help of self-contained positioning system for the robot.

For designing such robots the some of these things has to be considering that the localization system should be completely integrated onto the robot, hence the system should works on both indoors and outdoors without any human involvement.

2. EXISTING SYSTEM

The localization of autonomous ground robotic vehicle can be obtained with the help of radio signals or visual processing. Thus when the robot uses radio signals such as infrared, laser, RFID, etc. which requires a set of external devices to generate or receive radio signal as the reference nodes, these external devices should have known positions. Whereas the accuracy of the system is strongly depends upon proper calibration of the reference devices and the target node. At the same time if the robot uses vision techniques for mobile robot navigation, in that system the performance is strongly depend upon the environment in which the robot operates and the localization suffers frequent failure as well as the system requires a known map of the environment.

3. PROPOSED SYSTEM

In the proposed system a low-cost, self-contained localization system for the small-sized ground robotic vehicle has been designed, in which the robot vehicle can be localized with a hybrid approach consisting of infrequent absolute positioning through a GPS receiver and local relative positioning based on a inertial sensors. All these sensors are installed on the robotic vehicle. The motor rotation sensors are to detect the rotational movement of the motors and thus infer the travel distance of the robot. An embedded microcontroller inside the robot vehicle takes central control of these sensors and is also responsible for computing the current absolute position. In this autonomous robot, a small size camera is used to capture the photos of the unexplored area,

where human cannot go easily. This type of operation is mainly used in the military application and so on. After capturing the image the remote location can be analyzed from the remote area. The functional block diagram I shown in the Fig.1

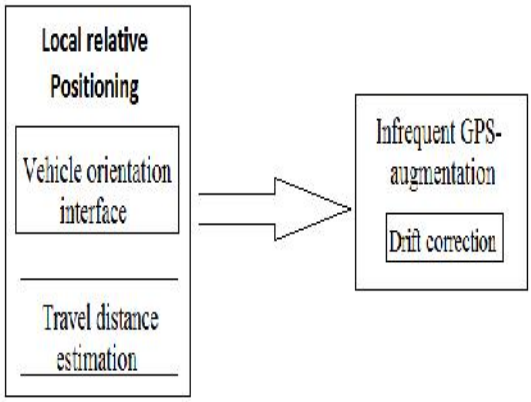


Fig.1 Block Diagram of the system.

4. FUNCTIONS OF THE SYSTEM

The local relative positioning components measure instantaneous 3D moving direction through both the accelerometer and the magnetic field sensor. It also measure the momentary travel distance for every small amount of time elapse through the rotation sensors attached to the vehicle motors. With the moving direction data together with the momentary travel distance, an estimate of the movement vector has been obtained. However, this type of robot has encountered a few major technical issues that arise in practical applications. One lies in the distinction between the world reference system and the on-board relative reference system. Another factor that impacts the localization practice is the way the robotic vehicle operates the motors to move a further complication comes from the cumulative error. In order to measure the local relative position of the system various reference frames has been setup to determine the current orientation of the robot. This robot consists of four different reference frames which are used to obtain the localization accurately; they are ROBOT Frame, Vehicle Body Frame, Accelerometer Body Frame and Magnetic Sensor Body Frame.

ROBOT Frame is used as the reference frame when deciding the momentary moving orientation of a ground robotic vehicle. It consists of three axes such as the X axis roughly points east, the Y axis points towards the magnetic north pole, the Z axis points outwards into the sky.

Accelerometer Body Frame and Magnetic Sensor Body Frame are the references frames with which the three dimensional sensing readings are interpreted from an accelerometer and a magnetic sensor respectively. These frame change as the vehicle moves.

It is important to know the momentary travel distance so as to compute the momentary relative movement The rotation sensor attached to a motor continually measures the rotating angle. Let r be the rotation sensor reading in degrees, d is the wheel's diameter and then the travel distance of the wheel's movement is rπd/360. In the case of slippage and obstacle, a few recent research projects have been developed to handle such issues using methods such as sensing modalities and obstacle avoidance.

The important issue needed to address is relates to the way the robotic vehicle operates its motors. It is common that a robotic vehicle may make turns or follow a curved path through adjusting its two sides of motors at different speeds and even in reverse direction.

It is also important that after implement these things in a robot, the robot is quite comfortable to obtain the real time localization of the system. Hence the camera fixed in the robot may help us to obtain the images of the unexplored area

5. SIMULATION RESULT

The project is simulated with the help of Proteus software, in which the speed of the robot, direction in which the robot moves and also GPS location of the robot has been calculated and Displayed with the

help of LCD. The simulated output is shown in Fig.2.

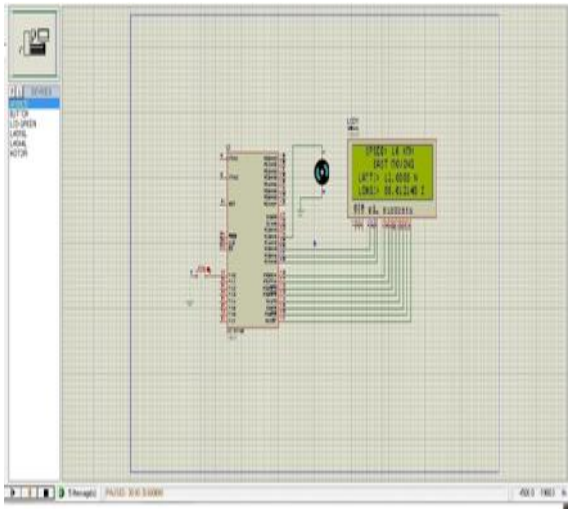


Fig.2 Simulated Output.

CONCLUSION

In this project, a low-cost, self-contained, accurate localization system for robotic vehicles has been proposed. The hardware device uses easily available component at low cost. This proposed system is self-contained in that it virtually requires no external devices or external facility management and that it needs no prior information.

FUTURE WORK

In my current work, I uses camera in the robot to capture the images of the unexplored area where human cannot go. In which due to various lightning condition of the environment, there is a chance of occurrence of various noise in an image. Hence some of the noise removal algorithm is used to implement in the image to acquire a better image.

REFERENCES

[1] Yuichiro Tod and Naoyuki Kubota," Self-Localization Based on multiresolution Map for Remote Control of Multiple Mobile Robots" IEEE Transactions On Industrial Informatics, pp.1772-1779, VOL. 9, NO. 3, August 2013.

[2] J. Paek, J. Kim, and R. Govindan, "Energy-Efficient Rate-Adaptive GPS-Based Positioning for Smartphones," Proc. Eighth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '10), pp. 299-314, 2010.

[3] Dylan F. Glas, Takayuki Kanda, Hiroshi Ishiguro and Norhiro Hagit, "Simultaneous People Tracking and Localization for Social Robots Using External Laser Range Finders," IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 846-853, Oct.2009.

[4] L. Thiem, B. Riemer, M. Witzke, and T. Luckenbach, "RFID-Based Localization in Heterogeneous Mesh Network" Proc. Sixth ACM Conf. Embedded Network Sensor Systems (SenSys '08), pp. 415-416, 2008.

[5] L.Thiem, B.Riemer, M. Witzke and T.Luckenbach, "RFID-Based Localization in Heterogeneous Mesh Network" Proc. Sixth ACM Conf. Embedded Network Sensor Systems (SenSys '08), pp. 415-416, 2008.

[6] N. Petrellis, N. Konofaos, and G.Alexiou,"Target Localization Utilizing the Success Rate in Infrared Pattern Recognition," IEEE Sensors J., vol. 6, no. 5, pp. 1355-1364, Oct. 2006.

[7] Daniel Gohring and Hans-Dieter Burkhard, "Multi Robot Object Tracking and Self Localization Using Visual Percept Relation", International Conference on Intelligent Robots and Systems, pp. 31-36, October 9 - 15, 2006.

[8] N. Schmitz, J. Koch, M. Proetzsch, and K. Berns, "Fault Tolerant 3D Localization for Outdoor Vehicles," Proc. IEEE/RSJ Int'l Conf. Intelligent Robots and Systems, pp. 941-946, Oct. 2006.

Automatic Segmentation of Scaling in 2-D Psoriasis Skin Images

M.Thamilselvan
Assistant Professor
Department of ECE
T. J. Institute of Technology
Mail id: mthamilselvan@gmail.com

R.P. Durgadevi
P.G. Scholar
Department of ECE
T. J. Institute of Technology
Mail id:

Abstract—:- Psoriasis is a chronic inflammatory skin disease that affects over 3% of the population. Various methods are currently used to evaluate psoriasis severity and to monitor therapeutic response. As an integral part of developing a reliable evaluation method for psoriasis, an algorithm is presented for segmenting scaling in 2-D digital images. The algorithm is believed to be the first to localize scaling directly in 2-D digital images. The scaling segmentation problem is treated as a classification and parameter estimation problem. A Markov random field (MRF) is used to smooth a pixel-wise classification from a support vector machine (SVM) that utilizes a feature space derived from image color and scaling texture.

I. INTRODUCTION

PSORIASIS is a chronic skin disease that affects an estimated125 million people worldwide [1], which manifests as red and scaly patches of itchy skin. The scaling results from an enhanced rate of epidermal cell production manifesting anywhere from a few spots to a large area of plaque, typically found on *erythema*, or red inflamed skin [2]. At present there is no known cure for psoriasis and, as a consequence, much effort has been expended on treatments to control the symptoms of psoriasis. However, there is no accepted treatment for psoriasis symptoms and different physicians will
treat the same symptoms differently [3]. A key factor in the improvement of psoriasis treatment is the ability to compare the efficacy of treatments across a broad range of conditions [4]. To be meaningful, such comparisons must be reliable requiring that the assessment of psoriasis severity is also reliable. Reliable tests are important to dermatologists for assessing treatments and to companies who want to improve their treatments. Currently, psoriasis severity is assessed by deriving a *severity score* [4]–[6]. The most widely used is the PASI score based on the area and severity of erythema, the area and severity of the creamy colored flaky skin, or *scaling*, in the lesions and the thickness of the lesion. PASI scores are estimated by inspecting the psoriatic lesions visually and relying on the clinicians' expertise to derive meaningful scores. The result is unavoidable inter- and intra-observer difference in severity scores. It is possible for two clinicians to derive two different severity scores using the same scoring technique for the same psoriatic lesion.

Reliable and reproducible severity scores are essential for comparing psoriasis treatments and furthering psoriasis treatment research. Most, if not all [4]–[7], psoriasis assessment methods rely on a visual estimation of the area and severity of the main psoriatic symptoms of erythema and scaling. Consequently, any computer based analysis method for assessing psoriasis severity using 2-D digital images must identify erythema and scaling as a precursor to further analysis. The paper presents what we believe to be the first algorithm to automatically segment scaling directly from skin and erythema in 2-D digital images. The approach is to reduce the problem of segmenting scaling to a binary classification problem by removing erythema from consideration and then classifying the remaining pixels as either skin pixels or scaling pixels. any computer based analysis method for assessing psoriasis severity using 2-D digital images must identify erythema and scaling as a precursor to further analysis. The paper presents what we believe to be the first algorithm to automatically segment scaling directly from skin and erythema in 2-D digital images. The approach is to reduce the problem of segmenting scaling to a binary classification problem by removing erythema from consideration and then classifying the remaining pixels as either skin pixels or scaling pixels. The feature space used in the classification is derived from the color contrast between scaling and erythema, and the image texture describing the roughness of scaling which is determined by the aggregated result from a bank of Gabor filters. Our evaluation indicates that our combination of Markov random fields (MRFs) with support vector machines using an appropriate feature space can solve a wide range of scaling segmentation problems that include variations in lighting conditions, variations in skin type and variations in the types of psoriatic lesions.

A. An Overview of the Algorithm

Scaling typically appears as white or creamy colored scales on regions of red and inflamed skin (erythema) but can also appear in isolation without

the accompanying erythema. When psoriasis appears without the accompanying erythema it appears as discernibly white or creamy flakes on normal skin. Scaling

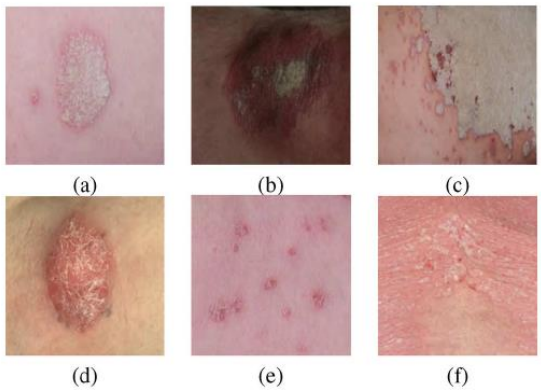


Fig. 1. Examples of scaling in psoriasis lesions. (a) Scattered scaling in plaque psoriasis. (b) Patched scaling in plaque psoriasis. (c) Extensively covered scaling in plaque psoriasis. (d) Scaling in guttate psoriasis. (e) Scaling in pustular psoriasis. (f) Scaling in erythrodermic psoriasis.

can present as small spots or as patches scattered within erythema. Fig. 1 shows some examples of the variation in the appearance of scaling. The variation makes it difficult to identify scaling boundaries through more conventional boundary detection algorithms and as a consequence we use a pixel based classification and labelling approach. Moreover, the color of scaling may be very similar to that of normal skin, especially if the skin is fair, making it difficult to differentiate between scaling and normal skin using on color alone. However, the rough textured surface of scaling is markedly different from normal skin. The algorithm uses a feature space derived from both color and texture to classify pixels. The result is a pipeline that is essentially a pix l labelling algorithm that identifies scaling in 2-D digital skin images without the need for locating psoriasis first. It is composed of two main stages: 1) a feature extraction stage and 2) a scaling segmentation stage. The two stages are described as follows (see Fig. 2).

Step 1) The algorithm first analyzes skin color and in texture using an appropriately chosen color pace and

B. The Computer Assisted Scoring of Psoriasis Severity

The computer assisted analysis of psoriasis lesions has received significant attention in recent years, but most of the work has focused on segmenting soriasis lesions from normal skin and specifically for plaque psoriasis. The problem of segmenting scaling has received much less attention. Röing, Jacques, and Kontinen [8] provide an interactive method for segmenting psoriasis lesions from normal skin using color thresholding. Gomez *et al.* [9] apply a quadratic discriminant analysis to separate psoriasis lesions based on a color analysis. However, both of these methods are not robust to disturbances caused by shadows. Taur *et al.* [10] use texture and color analysis in combination with a neuro-fuzzy classifier to segment psoriasis lesions, but not scaling. The color features are derived from the hue and saturation components in the image and the texture features of skin is graded according to a fuzzy texture spectrum. A key feature of [10] is that the training sets are derived from the image using a *moving window* to find homogeneous regions of normal skin and psoriasis. The algorithm is improved in [11] to decrease the computational complexity. The drawback of the Taur *et al.* algorithm is in the localization of homogenous regions in the selection of training data. The method for identifying homogeneous regions is reliable for large window sizes but is less accurate detecting small spotshaped psoriasis lesions. To the best of our knowledge, there are few algorithms that deal with scaling segmentation directly as we do here. One of the few is implemented by Delgado *et al.* [12] where scaling is segmented from psoriatic lesions using a clustering method, but the accuracy of this method depends on the initial segmentation of psoriatic lesions. Moreover, the algorithm is susceptible to uneven illumination.

C. An Overview of the Paper

The remainder of this paper is structured as follows. In Section II we design a multi-scale center-surround filter for detecting color contrast between scaling and erythema. We also design a bank of Gabor filters to describe the textures that correlate strongly with scaling. The scaling segmentation method is described in Section III in which a classifier that combines the hyperplane from a SVM with aMRF is developed to first classify pixels and then smooth the result by taking the spatial context into account. Section III also describes how the training sets are collected directly from the image being analyzed through a soft-constrained -means. Section IV provides the segmentation results and experimental validation of the algorithms, Section V discusses the results, and in Section VI we conclude.

III. CONCLUSION

In this paper, we present a general framework for automatic localizing scaling in psoriasis images. The result indicates that our algorithm makes progress towards the aim of automatic scaling segmentation. Scaling localization is implemented by a semi-supervised classification in this study. Two features are used: one is the scaling contrast map, which enhances the conspicuousness of scaling against erythema, and the other is a Gabor feature, which

differentiates between scaling and normal skin based on image texture. Training sets for the classification are collected by a soft-constrained -means to avoid the human interference. At the end, we combine the advantages of the SVM and the MRF to separate scaling from skin images. The SVM shows good performance in classification, but does not involve spatial information. Normal skin pixels around psoriatic lesion boundaries exhibit similar texture features to scaling, and are usually misclassified by the SVM. By integrating the SVM into our adaptation of the MRF, the internal structure of images are considered and that increases the classification accuracy. The results from our method are compared with the traditional SVM and the MRF. The proposed algorithm shows good performance as is presented in the specificity and dice evaluation. Even though the sensitivity analysis is weaker, the total accuracy from the dice evaluation is always stronger. Moreover, when we compare the algorithm to manually collected training sets, the proposed method presents a slightly weaker sensitivity to the SVM and the MRF. However, better specificity and dice evaluation are achieved when compared to the SVMand the MRF. Notice that the specificity and dice measurements of our method are very close to the case for training sets that are manually selected. This result validates the performance of the soft-constrained -means, through which the training sets are automatically collected. In the future, we will further investigate the algorithms for training set collection to improve the classification results. Moreover, scaling features need to be researched further, especially for the very vague scaling, which remains difficult to be detected using the algorithm in this paper.

STUCK-AT FAULTS TESTING USING REVERSIBLE SEQUENTIAL CIRCUITS

V.Prem Kumar
Assistant Professor
Department of ECE
T. J. Institute of Technology
Ph. No: 9840642218
Mail id: premkumar43@gmail.com

J.Sunitha Benzy
P.G. Scholar
Department of ECE
T. J. Institute of Technology
Ph. No. 9941279967
Mailid:sunithabenzy@gmail.com

Abstract— In this paper, we propose the design of two vectors testable sequential circuits based on conservative logic gates. The proposed sequential circuits based on conservative logic gates outperform the sequential circuits implemented in classical gates in terms of testability. Any sequential circuit based on conservative logic gates can be tested for classical unidirectional stuck-at faults using only two test vectors. The two test vectors are all 1s, and all 0s. The designs of two vectors testable latches, master-slave flip-flops and double edge triggered (DET) flip-flops are presented. The importance of the proposed work lies in the fact that it provides the design of reversible sequential circuits completely testable for any stuck-at fault by only two test vectors, thereby eliminating the need for any type of scan-path access to internal memory cells. The reversible design of the DET flip-flop is proposed for the first time in the literature.

I. INTRODUCTION DOCUMENT

We propose the design of testable sequential circuits based on conservative logic gates. The proposed technique will take care of the fan-out (FO) at the output of the reversible latches and can also disrupt the feedback to make them suitable for testing by only two test vectors, all 0s and all 1s. In other words, circuits will have feedback while executing in the normal mode. However, in order to detect faults in the test mode, our proposed technique will disrupt feedback to make conservative reversible latches testable as combinational circuits. The proposed technique is extended toward the design of two vectors testable master-slave flip flops and double edge triggered (DET) flip-flops. Thus, our work is significant because we are providing the design of reversible sequential circuits completely testable for any unidirectional stuck-at faults by only two test vectors. The reversible design of the DET flip-flop is proposed for the first time in the literature. Further, we implemented the Fredkin gate in the QCA technology and observed that all 0s and all 1s test vectors cannot provide 100% fault coverage for single missing/additional cell defect in the QCA layout of the Fredkin gate. Thus, to have the 100% fault coverage for single missing/additional cell defect by all 0s and all 1s test vectors, we identified the QCA devices in the QCA layout of the Fredkin gate that can be replaced with fault tolerant components to provide the 100% fault coverage.

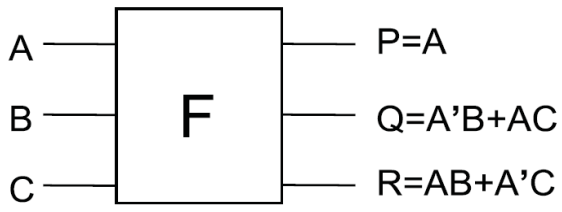


Fig 1 Fredkin gate

II. RELATED WORK

. Any nano technologyhaving applications of reversible logic such as based on nano-CMOS devices, NMR based quantum computing, or

now at low power molecular QCA computing, all are susceptible to high error rates due to transient faults. With respect to this paper on reversible sequential circuits, the design of reversible sequential circuits is addressed in the various interesting contribution in which the designs are optimized in terms of various parameters such as the number of reversible gates, garbage outputs, quantum cost, delay etc. To the best of our knowledge the offline testing of faults in reversible sequential circuits is not addressed in the literature. In this paper we present the design of reversible sequential circuits that can be tested only by using two test vectors, and all 0's and all 1's, for any unidirectional stuck at faults. Further the approach of testing based on conservative logic is extended toward the design of non reversible sequential circuits based on MX-cqca.

III. PROPOSED METHOD

In this paper, we propose the design of two vectors testable sequential circuits based on conservative logic gates. The proposed sequential circuits based on conservative logic gates outperform the sequential circuits implemented in classical gates in terms of testability. Any sequential circuit based on conservative logic gates can be tested for classical unidirectional stuck-at faults using only two test vectors. The two test vectors are all 1s, and all 0s. The designs of two vectors testable latches, master-slave flip-flops and double edge triggered (DET) flip-flops are presented. The importance of the proposed work lies in the fact that it provides the design of reversible sequential circuits completely testable for any stuck-at fault by only two test vectors, thereby eliminating the need for any type of scan-path access to internal memory cells. The reversible design of the DET flip-flop is proposed for the first time in the literature.

A. QCA computing

It provides a promising technology to implement reversible logic gates. The QCA design of Fredkin gate using the four-phase clocking scheme in which the clocking zone is shown by the number next to D (D0 means clock 0 zone, D1 means clock 1 zone, and so on). It can be seen that the Fredkin gate has two level MV implementation, and it requires 6 MVs and four clocking zones for implementation. The number of clocking zones in a QCA circuit represents the delay of the circuit (delay between the inputs and the outputs). Higher the number of clocking zones, lower the operating speed of the circuit. In QCA manufacturing, defects can occur during the synthesis and deposition phases, although defects are most likely to take place during the deposition phase. Researchers have shown that QCA cells are more susceptible to missing and additional QCA cell defects. The additional cell defect is because of the deposition of an additional cell on the substrate. The missing cell defect is due to the missing of a particular cell. Researchers have been addressing the design and test of QCA circuits assuming the single missing/additional cell defect model.

B. Fault coverage

Fault coverage refers to the percentage of some type of fault that can be detected during the test of any engineered system. High fault coverage is particularly valuable during manufacturing test, and techniques such as Design For Test (DFT) and automatic test pattern generation are used to increase it. In electronics for example, stuck-at fault coverage is measured by sticking each pin of the hardware model at logic '0' and logic '1', respectively, and running the test vectors. If at least one of the outputs differs from what is to be expected, the fault is said to be detected. Conceptually, the total number of simulation runs is twice the number of pins (since each pin is stuck in one of two ways, and both faults should be detected). However, there are many optimizations that can reduce the needed

computation. In particular, often many non-interacting faults can be simulated in one run, and each simulation can be terminated as soon as a fault is detected.

C. Automatic test pattern generation

ATPG (acronym for both Automatic Test Pattern Generation and Automatic Test Pattern Generator) is an electronic design automation method/technology used to find an input (or test) sequence that, when applied to a digital circuit, enables automatic test equipment to distinguish between the correct circuit behavior and the faulty circuit behavior caused by defects. The generated patterns are used to test semiconductor devices after manufacture, and in some cases to assist with determining the cause of failure The effectiveness of ATPG is measured by the amount of modeled defects, or fault models, that are detected and the number of generated patterns. These metrics generally indicate test quality (higher with more fault detections) and test application time (higher with more patterns). ATPG efficiency is another important consideration. It is influenced by the fault model under consideration, the type of circuit under test (full scan, synchronous sequential, or asynchronous sequential), the level of abstraction used to represent the circuit under test (gate, register-transistor, switch), and the required test quality.

D. Stuck-at fault model

In the past several decades, the most popular fault model used in practice is the single stuck-at fault model. In this model, one of the signal lines in a circuit is assumed to be stuck at a fixed logic value, regardless of what inputs are supplied to the circuit. Hence, if a circuit has n signal lines, there are potentially 2n stuck-at faults defined on the circuit, of which some can be viewed as being equivalent to others. The stuck-at fault model is a logical fault model because no delay information is associated with the fault definition. It is also called a permanent fault model because the faulty effect is assumed to be permanent, perhaps depending on operating conditions (e.g. temperature, power supply voltage) or on the data values (high or low voltage states) on surrounding signal lines. The single stuck-at fault model is structural because it is defined based on a structural gate-level circuit model. A pattern set with 100% stuck-at fault coverage consists of tests to detect every possible stuck-at fault in a circuit. 100% stuck-at fault coverage does not necessarily guarantee high quality, since faults of many other kinds such as bridging faults, opens faults, and transition faults.

This paper proposed reversible sequential circuits based on conservative logic that is testable for any unidirectional stuck-at faults using only two test vectors, all 0s and all 1s. The proposed sequential circuits based on conservative logic gates outperform the sequential circuit implemented in classical gates in terms of testability. The sequential circuits implemented using conventional classic gates do not provide inherited support for testability. Also as the complexity of a sequential circuit increases the number of test vector required to test the sequential circuit also increases. For example, to test a complex sequential circuit thousand of test vectors are required to test all stuck-at-faults, while if the same sequential circuit is build using proposed reversible sequential building blocks it can be tested by only two test vectors, all 0s and all 1s. Thus, the main advantage of the proposed conservative reversible sequential circuits compared to the conventional sequential circuit is the need of only two test vectors to test any sequential circuit irrespective of its complexity.

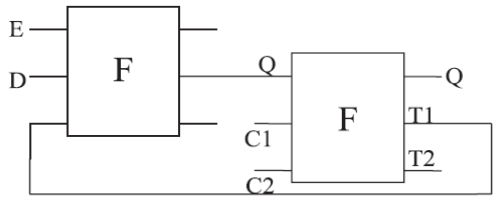


Fig 2 Design of negative enable Testable D latch

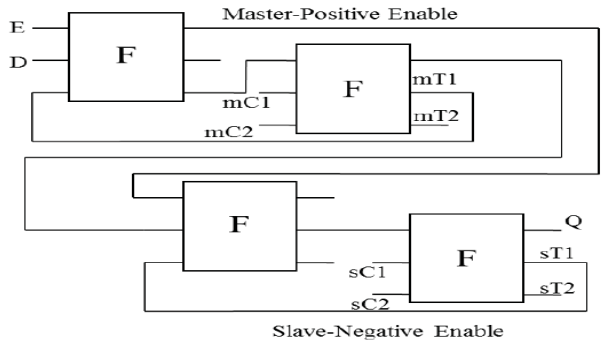


Fig 3 Fredkin gate based testable reversible master slave D flip flop

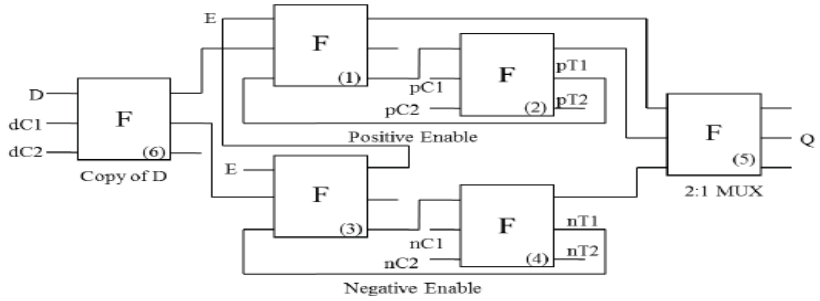


Fig 4 Fredkin based DET flip flop

V. CONCLUSION

This paper proposed reversible sequential circuits based on conservative logic that is testable for any unidirectional stuck-at faults using only two test vectors, all 0s and all 1s. The proposed sequential circuits based on conservative logic gates outperform the sequential circuit implemented in classical gates in terms of testability. The sequential circuits implemented using conventional classic gates do not provide inherited support for testability. Hence, a conventional sequential circuit needs modification in the original circuitry to provide the testing capability. Also as the complexity of a sequential circuit increases the number of test vector required to test the sequential circuit also increases. For example, to test a complex sequential circuit thousand of test vectors are required to test all stuck-at-faults, while if the same sequential circuit is build using proposed reversible sequential building blocks it can be

tested by only two test vectors, all 0s and all 1s. Thus, the main advantage of the proposed conservative reversible sequential circuits compared to the conventional sequential circuit is the need of only two test vectors to test any sequential circuit irrespective of its complexity. The reduction in number of test vectors minimizes the overhead of test time for a reversible sequential circuit. The proposed work has the limitation that it cannot detect multiple stuck-at-faults as well as multiple missing/additional cell defects. In conclusion, this paper advances the state-of-the-art by minimizing the number of test vectors needed to detect stuck-at-faults as well as single missing/additional cell defects.

REFERENCES

1. J. Ren and V. K. Semenov, "Progress with physically and logically reversible superconducting digital circuits," IEEE Trans. Appl. Superconduct.,vol. 21, no. 3, pp. 780–786, Jun. 2011.

2. S. F. Murphy, M. Ottavi, M. Frank, and E. DeBenedictis, "On the design of reversible QDCA systems," Sandia National Laboratories, Albuquerque, NM, Tech. Rep. SAND2006-5990, 2006.

3. H. Thapliyal and N. Ranganathan, "Reversible logic-based concurrently testable latches for molecular QCA," IEEE Trans. Nanotechnol., vol. 9, no. 1, pp. 62–69, Jan. 2010.

4. P. Tougaw and C. Lent, "Logical devices implemented using quantum cellular automata," J. Appl. Phys., vol. 75, no. 3, pp. 1818–1825, Nov. 1994.

5. P. Tougaw and C. Lent, "Dynamic behavior of quantum cellular automata," J. Appl. Phys., vol. 80, no. 8, pp. 4722–4736, Oct. 1996.

6. M. B. Tahoori, J. Huang, M. Momenzadeh, and F. Lombardi, "Testing of quantum cellular automata," IEEE Trans. Nanotechnol., vol. 3, no. 4,pp. 432–442, Dec. 2004.

7. G. Swaminathan, J. Aylor, and B. Johnson, "Concurrent testing of VLSI circuits using conservative logic," in Proc. Int. Conf. Comput. Design, Cambridge, MA, Sep. 1990, pp. 60–65.

8. E. Fredkin and T. Toffoli, "Conservative logic," Int. J. Theor. Phys., vol. 21, nos. 3–4, pp. 219–253, 1982.

9. P. Kartschoke, "Implementation issues in conservative logic networks," M.S. thesis, Dept. Electr. Eng., Univ. Virginia, Charlottesville, 1992.

10. G. Swaminathan, "Concurrent error detection techniques using parity," M.S. thesis, Dept. Electr. Eng., Univ. Virginia, Charlottesville, 1989.

MAXIMIZING PROFIT FOR OPTIMAL MULTI-SERVER CONFIGURATION IN CLOUD COMPUTING

K.Mariammal[#1]

[#]*Student*
Department of Computer Science and Engineering
Regional Centre of Anna University

Tirunelveli (T.N) India

[1]natureindia.k.v@gmail.com

ABSTRACT: Economics of cloud becomes an effective and efficient way of computing resources. Increasing the profit of service provider includes service charge and business cost. Amount of service, workload, service level agreement, quality of service, energy consumption are considered for the profit maximization.Two server speed and power models are considered, namely, the idle-speed model and the constant-speed model.Probability density function of the waiting time of the newly arrived service is described. Service charge for the expected service request is calculated. Gain for the one unit of time is also calculated. To maximize the service Provider profit using analytical method. By incorporating the method, Dynamic Scheduling and Pricing Algorithm to minimize the average queuing delay.

KEYWORDS: cloud computing, multi-server system, pricing model, response time, service charge, waiting time, profit.

1. INTRODUCTION

Cloud Computing is a computing paradigm in which different computing resources such as infrastructure, platforms and software applications are made accessible over the Internet to remote user as services [1]. Infrastructure-as-a-Service (IaaS) cloud providers, such as Amazon EC2 [2], IBM Cloud [3], Go Grid [4], Nepho Scale [5], Rack space [6] and others, deliver, on-demand, operating system (OS) instances provisioning computational resources in the form of virtual machines deployed in the cloud provider data center. Cloud computing is able to provide the most cost-effective and Energy efficient way of computing resources management and computing services provision. Cloud computing turns information technology into Ordinary commodities and utilities by using the pay-per-use pricing model [3], [5], [18]. However, cloud computing will never be free [8], and understanding the economics of cloud computing becomes critically important .Cloud computing Environment is a three tier structure [15], which consists of infrastructure vendors, service providers, and consumers. The three parties are also called cluster nodes, cluster managers, and consumers in cluster computing systems [21], and resource providers, service providers, and clients in grid computing systems [19]. An infrastructure vendor maintains basic hardware and software facilities. A service provider rents resources from the infrastructure vendors, builds appropriate multi-server systems, and provides various services to users. A consumer submits a service request to a service provider, receives the desired result from the service provider with certain service-level agreement, and pays for the service based on the amount of the service and the quality of the service. A service provider can build different multi-server systems for different application domains, such that service requests of different nature are sent to different multi-server systems. Each multi-server system contains multiple servers, and such a multi-server system can be devoted to serve one type of service requests and applications. An application domain is characterized by two basic features, i.e., the workload of an application environment and the expected amount of a service. The configuration of a multi-server system is characterized by two basic features ,i.e., the size of the multi-server system (the number of servers) and the speed of the multi-server system (execution speed of the servers).
The pricing model of a service provider in cloud computing is based on two components, namely, the income and the cost. For a service provider, the income (i.e., the revenue) is the service charge to users, and the cost is the renting cost plus the utility

cost paid to infrastructure vendors. A pricing model in cloud computing includes many considerations, such as the amount of a service (the requirement of a service), the workload of an application environment, the configuration (the size and the speed) of a multi-server system, the service-level agreement, the satisfaction of a consumer (the expected service time), the quality of a service (the task waiting time and the task response time), the penalty of a low-quality service, the cost of renting, the cost of energy consumption, and a service provider's margin
and profit. The profit (i.e., the net business gain) is the income minus the cost. To maximize the profit, a service provider should understand both service charges and business costs, and in particular, how they are determined by the characteristics of the applications and the configuration of a multi-server system. The service charge to a service request is determined by two factors, i.e., the expected length of the service and the actual length of the service. The expected length of a service (i.e., the expected service time) is the execution time of an application on a standard server with a baseline or reference speed. The longer (shorter, respectively) the expected length of a service is, the more (less, respectively) the service charge is. The actual length of a service (i.e., the actual service time) is the actual execution time of an application. The actual length of a service depends on the size of a multi-server system, the speed of the servers (which may be faster or slower than the baseline speed), and the workload of the multi-server system. penalty for a service provider to break a service-level agreement. If the actual service time exceeds certain limit (which is service request dependent), a service will be entirely free with no charge. The cost of a service provider includes two components, i.e., the renting cost and the utility cost. The renting cost is proportional to the size of a multi-server system, i.e., the number of servers. The utility cost is essentially the cost of energy consumption and is determined by both the size and the speed of a multi-server system. The faster (slower, respectively) the speed is, the more (less, respectively) the utility cost is. To calculate the cost of energy consumption, we need to establish certain server speed and power consumption models. To increase the revenue of business, a service provider can construct and configure a multi-server system with many servers of high speed. Since the actual service time (i.e., the task response time) contains task waiting time and task execution time, more servers reduce the waiting time and faster servers reduce both waiting time and execution time. However, more servers (i.e., a larger multiserver system) increase the cost of facility renting from the infrastructure vendors and the cost of base power consumption. the problem of optimal multi-server configuration for profit maximization in a cloud computing environment. Such that our optimization problem can be formulated and solved analytically. Then finally used in Dynamic Scheduling and Pricing (Dyn-SP). Proposing a joint optimization of scheduling and pricing decisions for delay-tolerant batch services to maximize the service provider's long-term profit. Dyn-SP produces a close-to-optimal average profit while bounding the job queue length in the data center. Then perform a trace-based simulation study to validate Dyn-SP. Focusing on dynamically scheduling and pricing for batch services that exhibit a high degree of scheduling flexibility due to the delay-tolerant nature, then aim at developing an efficient online algorithm to maximize the service provider's long-term profit in a random environment. Proposing a provably-efficient online algorithm, Dynamic Scheduling and Pricing (Dyn-SP), this can be implemented using the currently available information without the necessity of predicting the future.

2. RELATED WORK

Cloud computing has recently received considerable attention and is widely accepted as a promising and ultimate way of managing and improving the utilization of data and computing center resources and delivering various computing and IT services. Server consolidation is an effective cloud computing approach to increasing the efficient usage of computer server resources in order to reduce the total number of servers or server locations that an organization requires. By centralized management of computing resources, cloud computing delivers hosted services over the Internet, such that access to shared hardware, software, databases, information, and all resources are provided to users on-demand. In a data center with multiple servers, the aggregated performance of the data center can be optimized by load distribution and balancing. Cloud-based applications depend even more heavily on load balancing and optimization than traditional enterprise applications. For end users, load balancing capabilities will be seriously considered when they select a cloud computing provider. For end users, load balancing capabilities will be seriously considered when they select a cloud computing provider. For cloud providers, load balancing capabilities will be a source of revenue, which is directly related to service quality (e.g., task response time). Hence, an efficient load balancing strategy is a key component to building out any cloud computing architecture. The problem of optimal power allocation and load distribution for multiple heterogeneous multi-core server processors across clouds and data centers .We define two important research problems which

explore the power performance trade off in large-scale data centers from the perspective of optimal power allocation and load distribution. to formulate optimal power allocation and load distribution for multiple servers in a cloud of clouds as optimization problems. Our problems are defined for multiple multi-core server processors with different sizes, and certain workload.

Power constrained performance optimization – Given a power constraint, our problem is to find an optimal power allocation to the servers (i.e., to determine the server speeds) and an optimal workload distribution among the servers, such that the average task response time is minimized and that the average power consumption of the servers does not exceed the given power limit.

Performance constrained power optimization – Given a performance constraint, our problem is to find an optimal power allocation to the servers (i.e. ,to determine the server speeds) and an optimal workload distribution among the servers ,such that the average power consumption of the servers is minimized and that the average task response time does not exceed the given performance limit.

Cloud computing service provider serves users' service requests by using a multi-server system, which is constructed and maintained by an infrastructure vendor and rented by the service provider. Users (i.e., customers of a service provider) submit service requests (i.e., applications and tasks) to a service provider, and the service provider serves the requests (i.e., run the applications and perform the tasks) on a multi-server system. The first-come-first-served (FCFS) queuing discipline is adopted. The waiting time is the source of customer dissatisfaction. A service provider should keep the waiting time to a low level by providing enough servers and/or increasing server speed, and be willing to pay back to a customer in case the waiting time exceeds certain limit.

2.1 POWER CONSUMPTION

Power dissipation and circuit delay in digital CMOS circuits can be accurately modeled by simple equations, even for complex microprocessor circuits. CMOS circuits have dynamic, static, and short-circuit power dissipation; however, the dominant component in a well-designed circuit is dynamic power consumption P (i.e., the switching component of power), which is approximately $P=acv^2f$, where a is an activity factor, C is the loading capacitance, V is the supply voltage, and f is the clock frequency [6]. There are two types of power consumption models. They are **Idle speed model** In this type the speed of the server is zero at that time there is no task to perform in the server. The idle server also consumes some basic power. **Constant speed model** All the servers are run at certain speed limit. It will maintain the speed at the time of no task to perform.

2.2 WAITING TIME

Customer dissatisfaction is based on the waiting time. Waiting time of the request is the starting point of the delay. Calculate the average for waiting time of service request. It will calculate the waiting time of the request in queue. The delay of the resource is not considered in the waiting time. Notice that a multi-server system with multiple identical servers has been configured to serve requests from certain application domain. Therefore, we will only focus on task waiting time in a waiting queue and do not consider other sources of delay, such as resource allocation and provision, virtual machine instantiation and deployment, and other overhead in a complex cloud computing environment. Average waiting time of a service request is , W= T-X W Average waiting time T- Average task response time X- Mean of the random variable.

2.3 SERVICE CHARGE

If all the servers have a fixed speed s, the execution time of a service request with execution requirement r is known as x =r/s. The response time to the service request is T=W +x=W +r/s. The response time T is related to the Service charge to a customer of a service provider in cloud computing. To study the expected service charge to a customer, we need a complete specification of a service charge based on the amount of a service, the service-level agreement, the satisfaction of a consumer, the quality of a service, the penalty of a low-quality service, and a service provider's margin and profit. Let s0 be the baseline speed of a server. We define the service charge function for a service request with execution requirement r and response time T to be

$$C(r, T) = \begin{cases} ar, if (0 \le T \le \frac{cr}{s0}) \\ ar - d\left(T - \frac{cr}{s0}\right), if \left(\frac{cr}{s0} < T \le \frac{a}{d} + \frac{c}{s0}\right) r; \\ 0, if\ T > \left(\frac{a}{d} + \frac{c}{s0}\right) r: \end{cases}$$

The above function is defined with the following rationales:

- If the response time T to process a service request is no longer than (c/s0)r=c(r/s0) where the constant c is a parameter indicating the service-level agreement, and the constant s0 is a parameter indicating the expectation and satisfaction of a
- consumer, then a service provider considers that the service request is processed successfully with high quality of service and charges a customer ar ,which is linearly proportional to the task execution requirement r (i.e., the amount

of service), where a is the service charge per unit amount of service (i.e., a service provider's margin and profit).

- If the response time T to process a service request is longer than (c/s0)r but no longer than (a /d+ c/s0)r then a service provider considers that the service request is processed with low quality of service and the charge to a customer should decrease linearly as T increases. The parameter d indicates the degree of penalty of breaking the service-level agreement.
- If the response time T to process a service request is longer than (a/d+c/s0)r , then a service provider considers that the service request has been waiting too long, so there is no charge and the service is free.

2.4 NET BUSINESS GAIN

Since the number of service requests processed in one unit of time is λ in a stable M/M/m queuing system, the expected service charge in one unit of time is λC, which is actually the expected revenue of a service provider. Assume that the rental cost of one server for unit of time is β. Also, assume that the cost of energy is per Watt. The cost of service provider is the sum of the cost of infrastructure renting and the cost of energy consumption, i.e.,. βm+ P. Then, the expected net business gain(i.e., the net profit) of a service provider in one unit of time is G = λ C-(βm+ P)which is defined as the revenue minus the cost. There are two situations that cause negative business gain. In the first case, there is no enough business (i.e., service requests). In this case, a service provider should consider reducing the number of servers m and/or server speed s, so that the cost of infrastructure renting and the cost of energy consumption can be reduced. In the second case, there is too much business (i.e., service requests). In this case, a service provider should consider increasing the number of servers and/or server speed, so that the waiting time can be reduced and the revenue can be increased. However, increasing the number of servers and/or server speed also increases the cost of infrastructure renting and the cost of energy consumption. Therefore, we have the problem of selecting the optimal server size and/or server speed so that the profit is maximized.

3 OVERVIEW OF PROFIT MAXIMIZATION MODEL

3.1 EXISTING SYSTEM

Service provider serves users' service requests by using a multi-server system. We consider two server speed and power consumption models namely the idle speed and the constant-speed model .Power consumption at idle and constant speed model is calculated. The waiting time of the request in the queue forget response is then calculated. Calculate the service charge to a customer based on the amount of a service, SLA, satisfaction QOS, penalty of a low-quality service etc .This methodology is not enough for find the optimal resource. So the time consumption for execute the job in resource is very high. The accuracy of the result is also low. And the speed of the resource is also low.

3.2 PROPOSED SYSTEM

Present an online algorithm "Dynamic Scheduling and Pricing"("Dyn-SP"), whose performance is provably "good" compared to that of the optimal offline policy with T -slot look ahead information, based on the recently developed Lya-punov optimization [36]. The intuition of Dyn-SP is to trade the queuing delay for profit improvement by using the batch job queue length as a guidance for making scheduling and pricing decisions: batch service demand is reshaped using pricing as a lever to adapt to the data center management and batch jobs are processed only when the queue length becomes sufficiently large and/or electricity prices are sufficiently low. The parameter $V \geq 0$ is a control variable which we refer to as profit-delay parameter, and it can be tuned to different values to trade the queuing delay for the service provider's long-term profit.

- Effect of V on the service provider's pricing decision: Let us consider two extreme cases: $V \to 0$ and $V \to \infty$. When $V \to 0$, the batch jobs cannot tolerate any delays (i.e., essentially they become interactive jobs) and hence, as can be seen from (13), the service provider always set sp (t)= p max such that no one uses its batch service. On the other hand, when $V \to \infty$, average queuing delay is not a concern and we can notice from (14) that the service provider always chooses its price $p(t) \in [0, p_{max}]$ such that its profit b (p(t)) p (t) is maximized.
- Effect of V on the service provider's scheduling decision: For simplicity, we focus on the scenario in which the electricity price is given by $\varphi(t) \cdot [d(t) + f(d(t)) - y(t)]^+$, where φ(t) is the real-time electricity price and y (t) is the available renewable energy supply. Then, if $\varphi(t) \leq q(t) V (1+\gamma)$ is satisfied where γ is the required cooling power per unit number of active servers, the service provider will try to schedule as many batch jobs as possible to process.

ALGORITHM: Dyn-SP Algorithm

1: At the beginning of every time slot t, observe the current environment information (i.e., φ_i (t) , W (t) , C (t) and y (t)) and the current queue length q (t)

2: Choose p(t) ∈ [0 ,p_{max}] to minimize b (t) · [q (t) − V p(t)] = b(p(t)) · [q (t) − V p(t)] , (13) where b(t)= b (p (t)) is the demand function for batch services satisfying (10)

3: Choose d (t) ∈ [0 ,d_{max}] to minimize

$V \cdot r (\varphi (t) , [d (t)+f (d (t)) − y (t)])^{+} − q (t) d (t)$ (14)

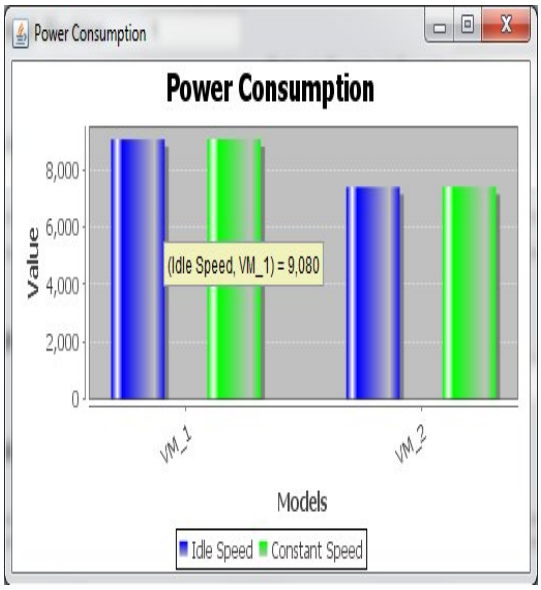
where r (φ (t) , [d(t)+f (d (t)) − y (t)]+) is the electricity cost

4: Update q (t) according to (1)

Algorithm takes Jobs (cloudlets) and its queue lengths as the inputs. It calculates the time slots for each and every jobs which is being submitted in the Virtual machines in datacenters. Also predicts the data workloads for the jobs submitted in VMs and calculate the pricing process based on the workload which in turn results in electricity cost of VM model. We present Dyn-SP algorithm for profit maximization in terms of predicting and computing the workload which represents the cheaper or less electric cost VM. QOS or quality of services also measured in terms of bandwidth, execution time, MIPS.

4. SIMULATION AND RESULTS

Cloud-sim goal is to provide a generalized and extensible simulation framework that enables modeling, simulation, and experimentation of emerging Cloud computing infrastructures and application services, allowing its users to focus on specific system design issues that they want to investigate, without getting concerned about the low level details related to Cloud-based infrastructures and services. The cloud provides access to the necessary computing resources for this onetime event in a flexible manner. In general, cloud-based simulation tasks can be conducted in parallel, for multiple purposes. Recently, cloud computing emerged as the leading technology for delivering reliable, secure, fault-tolerant, sustainable, and scalable computational services, which are presented as Software, Infrastructure, or Platform as services (SaaS, IaaS, PaaS). Moreover, these services may be offered in private data centers (private clouds), may be commercially offered for clients (public clouds), or yet it is possible that both public and private clouds are combined in hybrid clouds.



If it is X axis indicate the value the power in watts, and Y-axis indicate the models of the Virtual Machine (VM).

5. CONCLUSION

A pricing model for cloud computing which takes many factors into considerations, such as the requirement r of a service, the workload _ of an application environment, the configuration (m and s) of a multi-server system, the service level agreement c, the satisfaction (r and s0) of a consumer, the quality of a service, the penalty d of a low-quality service, the cost of renting, the cost of energy consumption, and a service provider's margin and profit. By using an M/M/ m queuing model, we formulated and solved the problem of optimal multi server configuration for profit maximization in a cloud computing environment. Our methodology can be applied to other pricing model.

6. REFERENCES

[1] M. Armbrust et al., "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report No. UCB/EECS-2009-28, Feb. 2009.

[2] R. Buyya, D. Abramson, J. Giddy, and H. Stockinger, "Economic Models for Resource Management and Scheduling in Grid Computing,"

Concurrency and Computation: Practice and Experience, vol. 14, pp. 1507-1542, 2007.

[3] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the Fifth Utility," Future Generation Computer Systems, vol. 25, no. 6, pp. 599-616, 2009. A.P. Chandrakasan, S. Sheng, and R.W. Brodersen, "Low-Power CMOS Digital Design," IEEE J. Solid-State Circuits, vol. 27, no. 4, pp. 473-484, Apr. 1992.

[4] B.N. Chun and D.E. Culler, "User-Centric Performance Analysis of Market-Based Cluster Batch Schedulers," Proc. Second IEEE/ ACM Int'l Symp. Cluster Computing and the Grid, 2002.

[5] D. Durkee, "Why Cloud Computing Will Never be Free," Comm. ACM, vol. 53, no. 5, pp. 62-69, 2010.

[6] R. Ghosh, K.S. Trivedi, V.K. Naik, and D.S. Kim, "End-to-End Performability Analysis for Infrastructure-as-a-Service Cloud: An Interacting Stochastic Models Approach," Proc. 16th IEEE Pacific Rim Int'l Symp. Dependable Computing, pp. 125-132, 2010.

[7] K. Hwang, G.C. Fox, and J.J. Dongarra, Distributed and Cloud Computing. Morgan Kaufmann, 2012.

[8] "Enhanced Intel SpeedStep Technology for the Intel Pentium M Processor,"White Paper, Intel, Mar. 2004.

[9] H. Khazaei, J. Misic, and V.B. Misic, "Performance Analysis of Cloud Computing Centers Using M/G/m/m+r Queuing Sys-tems," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 5, pp. 936-943, May 2012.

[10] L. Kleinrock, Queueing Systems: Theory, vol. 1. John Wiley and Sons, 1975.

[11] Y.C. Lee, C. Wang, A.Y. Zomaya, and B.B. Zhou, "Profit-Driven Service Request Scheduling in Clouds," Proc. 10th IEEE/ACM Int'l Conf. Cluster, Cloud and Grid Computing, pp. 15-24, 2010.

[12] K. Li, "Optimal Load Distribution for Multiple Heterogeneous Blade Servers in a Cloud Computing Environment," Proc. 25th IEEE Int'l Parallel and Distributed Processing Symp. Workshops, pp. 943-952, May 2011.

[13] K. Li, "Optimal Configuration of a Multicore Server Processor for Managing the Power and Performance Tradeoff,"J. Supercomput-ing, vol. 61, no. 1, pp. 189-214, 2012.

[14] P. Mell and T. Grance, "The NIST Definition of Cloud Comput-ing," Nat'l Inst. of Standards and Technology,http://csrc.nist. gov/groups/SNS/cloud-computing/, 2009.

[15] F.I. Popovici and J. Wilkes, "Profitable Services in an Uncertain World,"Proc. ACM/IEEE Conf. Supercomputing,2005.