IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 6, August 2014.
www.ijiset.com
ISSN 2348 – 7968

A Review of 'MANET's Security Aspect and Challenges with Comprehensive Study of SIDS for Discovering Malicious Nodes

Rashmi Mahajan[1] , Prof. S. M. Patil[2]
[1] Department of Electronics Engineering, Datta Meghe College of Engineering, Mumbai University, Airoli, Navi Mumbai 400708, Maharastra, India

[2] Department of Electronics Engineering, Datta Meghe College of Engineering, Mumbai University, Airoli, Navi Mumbai 400708, Maharastra, India

Abstract
Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. 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. This makes MANET vulnerable to various attacks, packet dropping attack attack is one of the possible attack. It is very hard to detect and prevent it. To prevent from packet dropping attack, detection of misbehavior links and selfish nodes plays a vital role in MANETs . In this paper, a comprehensive investigation on detection of misbehavior links and malicious nodes is carried out along with that we focus on the study of the routing protocols. Also included fundamental security problem of protecting the multihop network connectivity between mobile nodes in a MANET. We identify the security issues related to this problem, discuss the challenges to security design, and review the state-of-the-art security proposals that protect the MANET link- and network-layer operations of delivering packets over the multihop wireless channel.
Keywords: *MANET, IETF, AODV, DSDV, DSR, AACK , EAACK.*

1. Introduction

Ad hoc networking is not a new concept. As a technology for dynamic wireless networks, it has been deployed in military since 1970s. Commercial interest in such networks has recently grown due to the advances in wireless communications. A new working group for MANET has been formed within the Internet Engineering Task Force (IETF), aiming to investigate and develop candidate standard Internet routing support for mobile, wireless IP autonomous segments and develop a framework for running IP based protocols in ad hoc networks. The recent IEEE standard 802.11 has increased the research interest in the area of ad hoc networking which is receiving more attention from academia, industry, and government. Since these networks pose many complex issues, there are many open problems for research and significant contributions. A Mobile Adhoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others needs the aid of intermediate nodes to route their packets. Each of the node has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations.

1.1 MANETs characteristics

a). Distributed operation:
b). Multi hop routing:
c). Autonomous terminal:
d). Dynamic topology:
e). Light-weight terminals: The nodes at MANET are mobile with less CPU capability, low power storage and small memory size.
f). Fast deployment: When compared to WLANs, ad hoc networks are very convenient and easy to deploy requiring less manual intervention since there are no cables involved.

1.2 Advantages of MANET

Popularity of MANET increasing day by day due to following advantages :

- They provide access to information and services regardless of geographic position.
- Independence from central network administration. Self- configuring network, nodes are also act as routers. Less expensive as compared to wired network.
- Scalable—accommodates the addition of more nodes.
- Improved Flexiblibility Robust due to decentralize administration.
- The network can be set up at any place and time.

[1][2]

2. MANET Security Aspects

ISSN 2348 – 7968

2.1 MANET'S VULNERABILITY

Vulnerability is a weakness in system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network.vulnerabilities are as follows:

- Lack of centralized management:
- Scalability:
- Cooperativeness:
- Dynamic topology:
- Limited power supply:
- Bandwidth constraint:
- Adversary inside the Network:
- No predefined Boundary:

2.2 MANET'S SECURITY SERVICES

A MANET is a network consisting of a collection of nodes capable of communicating with each other without help from infrastructure of the network. Security Services are as follows

i). Authentication:-Correct identity is known to the communicating partner.

ii). Confidentiality: - Message information is kept secure from unauthorized party.

iii). Integrity: - Message is unaltered during communication.

iv). Non Repudiation: - The origin of the message cannot deny having sent the message.

v). Availability: - The normal service provision in face of all kind of attacks. Security means the security mechanism for all protocols involved in this (MANET) service to protect the basic function of MANET means security during bit transfer from one node to another.

2.3 MANET's CHALLENGES

i) Limited bandwidth: Wireless link continue to have significantly lower capacity than infrastructure networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.

ii) Dynamic topology: Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.

iii) Routing Overhead: In wireless adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

iv) Hidden terminal problem: The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

v) Packet losses due to transmission errors: Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni-directional links, frequent path breaks due to mobility of nodes.

vi) Mobility-induced route changes: The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.

vii) Battery constraints: Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.

viii) Security threats: The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.[3][4][5]

2.4 LAYERS INVOLVES IN MANET

i) Application Layer: - Detecting and preventing virus, worms, malicious codes, application abuses.

ii) Transport Layer: - Authentication and securing end-to end communications through data encryption.

iii) Link Layer: - protecting the wireless MAC protocol and providing link layer security support.

iv) Physical Layer: - Providing signal jamming denial of service attacks.

3. SECURITY: - "Means of securing a weakest link"

ISSN 2348 – 7968

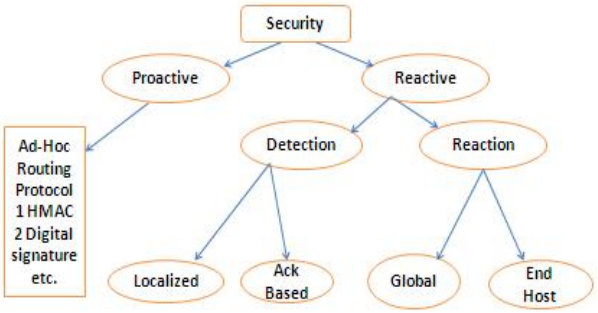

Fig. 1 Security Approches Used in MANET

Fundamental challenge in security design for MANET is to maintain network performance with full security strength, because when more security features are introduced in the network Increases computation, communication and management overhead .This can affect the network performance. Security involves two approaches:

A. Proactive: - This approach attempt to thwart security threats in the first place through various cryptographic techniques.

B. Reactive: - First detect the threat react accordingly.

There are three aspects in the field of Ad-Hoc network security:

- Intrusion Detection Systems (IDS),
- Secure routing
- Authentication Access via key management

The present research focuses on building a solution that combines these three aspects applied to the reactive routing *protocol AODV (Ad-Hoc On Demand Distance Vector Routing)*. [6][7]

3.1 MANET'S ROUTING PROTOCOLS

Ad-Hoc network routing protocols are commonly divided into three main classes; *Proactive* , *reactive* and *hybrid* protocols as shown in figure.

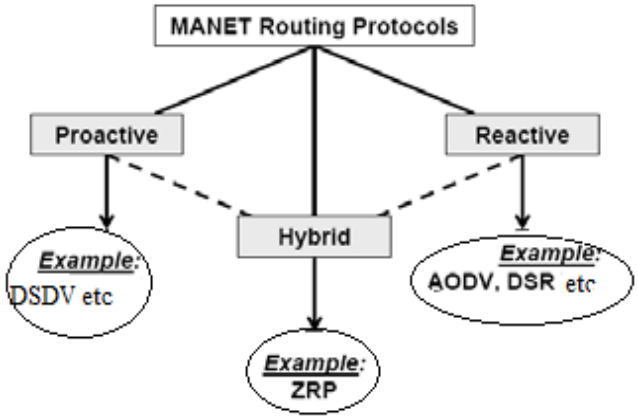

Fig. 2 Classification of MANET routing protocols

i) Proactive Protocols: Proactive, or table-driven routing protocols. In proactive routing, each node has to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view. Example of such schemes are the conventional routing schemes: Destination sequenced distance vector (DSDV). They attempt to maintain consistent, up-to-date routing information of the whole network. It minimizes the delay in communication and allow nodes to quickly determine which nodes are present or reachable in the network.

ii) Reactive Protocols: Reactive routing is also known as on-demand routing protocol since they do not maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery occurs by flooding the route request packets throughout the network. Examples of reactive routing protocols are the Ad-hoc On-demand Distance Vector routing (AODV) and Dynamic Source Routing (DSR).

iii) Hybrid Protocols: They introduce a hybrid model that combines reactive and proactive routing protocols. The Zone Routing Protocol (ZRP) is a hybrid routing protocol that divides the network into zones. ZRP provides a hierarchical architecture where each node has to maintain additional topological information requiring extra memory[8]

3.2 SECURITY THREATS

The wireless Channel is accessible to both legitimate network users and malicious attackers. There is no well defined place where traffic monitoring or access control mechanism scan be deployed so the boundary that separates the inside network from the outside world becomes blurred.

3.2.1. The existing ADHOC routing protocols such as ADHOC on Demand distance vector (AODV), Dynamic Source Routing (DSR), Wireless MAC protocols such as (802.11) do not provide a trusted environment so a malicious attacker can readily become a router and disrupt network operations by disobeying the protocol specifications.

3.2.2. The attacker may advertise a route with a smaller distance metric than the actual distance to the destination.

3.2.3. By attacking routing protocol the attacker can attract traffic towards certain destination in the nodes under their

control and cause the packet to be forwarded along a route that is not optional

3.2.4. The attacker can create routing loops in the network and introduce severe network congestion and channel contention in certain areas.

3.2.5. Many colluding attracters may even prevent a source node from finding any route to the destination and partition the Network.

3.2.6. The attacker may further subvert existing nodes in the network or fabricate its identity and impersonate.

3.2.7. A pair of attacker nodes may create a wormhole and shortcut the normal flows between each other

3.2.8. The attacker may target the route maintenance process and advertise that an operational link is broken.

3.2.9. One more problem is the attacker along an established route may drop the packet, modify the content of packet or duplicates the packets it has already forwarded.

3.2.10. Denial of service: Attack via network layer packet blasting ,in which the attacker injects a large amount of junk packets in to the network, these packets waste a significant portion of the network resources and introduce severe wireless channel contention and network congestion in MANET . The wireless Channel is a band width constraints and also shared among multiple networking entities. The computational capacity of the mobile node is also a constrained. [9]

3.3 SECURITY MESUREMENTS IN MANET

Due to the absence of a clear line of defense, a complete security solution for MANET should involve both approaches. So the way to check the security is *Prevention, Detection and Reaction.* Try to increase the difficulties for the attacker to penetrate the system but intrusion free system is not feasible, so the detection component play a important role to detect the attacker so that proper action can be taken to avoid persistent adverse effects.

3.3.1 ***Prevention****:-*

It can be achieve by secure Adhoc routing protocols that prevent the attackers form installing incorrect routing states at other nodes .These protocols employ different cryptographic primitives

A. HMAC (Massage authentication codes)
B. Digital Signature
C. Hash Chain

3.3.2 ***Detection****:-*

Because the wireless channel is open, each node can perform localized detection by overhearing ongoing transmission and evaluating the behaviour of its neighbours but its accuracy is limited by a no. of factors such as channel error, interference and mobility. A *malicious node* may also abuse the security solutions and intentionally accuse legitimate nodes, In order to address such issues, the detection results at individual nodes can be integrated and refined in a distributed manner to achieve consensus among a group of nodes. An *alternative approach relies on explicit acknowledgement* from the destination and/or intermediate nodes to the source so that the source can figure out where the packet was dropped.

3.3.3 ***Reaction****:-*

Once a malicious node is detected certain actions are triggered to protect the network from future attacks launched by this node the reaction component is related to the prevention component in the security system. Once multiple nodes in a local neighbourhood have reached consensus that one of their neighbours is malicious, they collectively revoke the certificate of the malicious node. The malicious node is isolated in the network as it cannot participate in the routing or packet forwarding.[4][9]

3.4 PACKET DROPPING ATTACK

This type of attack is denial of service attack in which a node in the network will drop the packets instead of forwarding them, which is shown in the fig 3 The packet dropping attack is very hard to detect and prevent because it occurs when the node becomes compromised due to a number of different causes. The packet dropping attack in MANETs can be classified into several categories in terms of the strategy adopted by the malicious node to launch the attack.

- The malicious node can intentionally drop all the forwarded packets going through it (black hole).
- It can selectively drop the packets originated from or destined to certain nodes that it dislikes.
- A special case of black hole attack dubbed gray hole attack is introduced. In this attack, the malicious node retains a portion of packets (one packet out of N received packets or one packet in a certain time window), while the rest is normally relayed.

ISSN 2348 – 7968

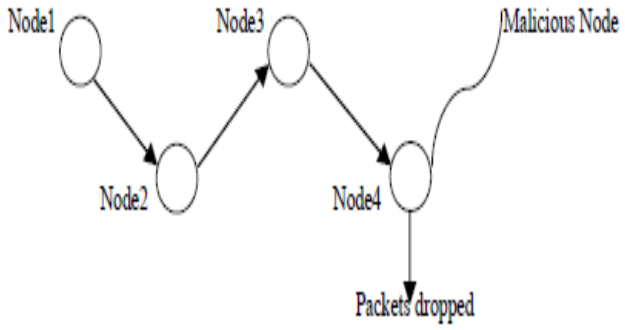

Fig 3. Packet dropping attack

The compromised node will broadcast the message that it has the shortest path towards a destination to initiate packet dropping attack. Hence, all packet transmissions will be directed through the compromised node, and the node is able to drop the packets. If the malicious node attempts to drop all the packets, the attack can be identified through common networking tools. Moreover, when other routers notice that the compromised router is dropping all packets, they will generally begin to remove that router from their forwarding table. Hence, there is no packet transmission through the compromised node. However, it is often harder to detect the packet dropping attack, if the malicious router begins dropping packets on a specific time period or over every *n* packet, because some packet transmission still flows across the network. For the prevention of packet dropping attack, detection of selfish nodes plays a vital role in MANETs.

4. "Selfish Nodes Detection and Routing Misbehavior in MANETs using SIDS" - A LITERATURE REVIEW

Recently, several secure intrusion detection (SIDS) approaches were proposed to deal with malicious attacks. In this section some of the existing SIDS approaches which are mainly used for detecting malicious nodes and mitigating routing misbehavior are discussed.

4.1 Routing Misbehavior in Mobile Adhoc Networks (Watchdog-pathrater)

Most of the routing protocols in mobile adhoc networks have limitations in transmission. So the nodes in MANET assume that other nodes always cooperate with each other to relay packets. This gives opportunities to attackers to achieve the significant impact on the network with one or two compromised nodes. To solve this problem intrusion detection system should added enhanced security level. This paper proposed an intrusion detection system called watchdog. *It aims to improve the network throughput with the presence of malicious nodes*. Watchdog consists of two parts namely, watchdog and pathrater. It is responsible to detect the malicious nodes misbehaviours in the network. Watchdog system has a failure counter; it is increased while the next node fails to forward the packet.

*Watchdog:*Watchdog serves as IDS for MANETs. It is responsible for detecting malicious node misbehaviours in the network by overhearing the next node's transmission. It is capable of detecting misbehaving nodes rather than links. It detects malicious misbehaviours 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.

Pathrater: Pathrater is used here as response system. It uses the feedback given by the watchdog part about the malicious misbehaviours of the node. It cooperates with routing protocol to avoid the reported malicious nodes in future transmission. Many implementation shows that watchdog scheme is efficient. It is capable of detecting misbehaving nodes rather than links[10].

4.2 CONFIDANT- Cooperation Of Nodes: Fairess in Dynamic Ad-hoc NeTworks

Buchegger and LeBoudec [11] proposed an extension to DSR protocol called CONFIDANT (Cooperation of Nodes, Fairness In Dynamic Ad-hoc Networks), which is similar to Watchdog and Pathrater. Each node observes the behaviors of neighbor nodes within its radio range and learns from them. This system also solves the problem of Watchdog and Pathrater such that misbehavior nodes are punished by not including them in routing and not helping them on forwarding packets. Moreover, when a node experiences a misbehaving node, it will send a warning message to other nodes in the network, defined as friends, which is based on trusted relationship. Figure 4 shows the components of the CONFIDANT protocol, which are the Monitor, the Trust Manager, the Reputation System, and the Path Manager. The process of how they work can be divided into two parts: the process to handle its own observations and the process to handle reports from trusted nodes. The monitor uses a "neighborhood watch" to detect any malicious behaviors within its radio range, i.e., no forwarding, unusually frequent route update

ISSN 2348 – 7968

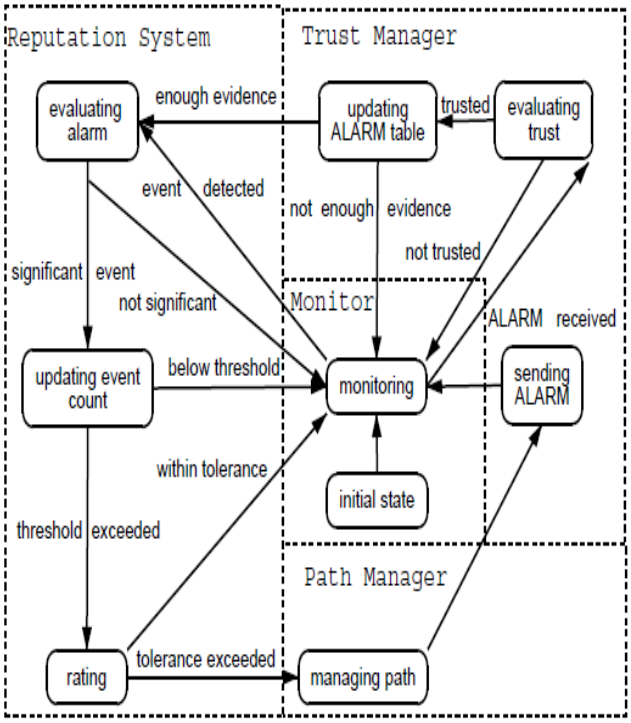

Fig. 4 components of the CONFIDANT protocol

etc. (This is similar to the watchdog in the previous scheme) If a suspicious event is detected, the monitor then reports to the reputation system. At this point, the reputation system performs several checks and updates the rating of the reported node in the reputation table. If the rating result is unacceptable, it passes the information to the path manager, which then removes all paths containing the misbehavior node. An ALARM message is also sent by the trust manager to warn other nodes that it considers as friends [11].

4.3 CORE- collaborative reputation mechanism to enforce node cooperation in mobile ad hoc n/w

Marjan et. Al [12] proposed a technique for detecting selfish nodes. These nodes force other nodes to cooperate with them. This technique is similar to CONFIDANT is based on monitoring system and reputation system. In this technique each node receives reports from other nodes. The difference between CORE and CONFIDANT is that CORE only allows positive reports to pass through, but CONFIDANT allows negative reports. This means that CORE prevents false reports. Therefore, it prevents a DoS attack which CONFIDANT can not do.

CORE differs from the watchdog-pathrater scheme as follows:

- in CORE misbehaving nodes are stimulated to contribute to the network operations in order to be able to use network services, the pathrater mechanism helps a legitimate user to avoid using misbehaving nodes;
- CORE is a generic mechanism that can be integrated with several network and application layer functions whereas the watchdogpathrater scheme is specifically designed for routing;
- unlike the pathrater technique the reputation mechanism in CORE does not allow a node to distribute negative ratings about other nodes, so unlike the pathrater technique, CORE can resist to simple denial of service attacks that use the security mechanism itself[12].

4.4 Collaborative Security Architecture

Patcha [13] used an extension approach to the watchdog approach. In this approach, the nodes in the network are classified into trusted and ordinary nodes. The nodes which are involved in initial network formation are called as trusted nodes. The nodes which are joining later in to the network are called as ordinary nodes. The ordinary node can be promoted as trusted node if the node proves its trustworthiness. Another assumption in this approach is that all the trusted nodes should not be a malicious or selfish node. The watchdog nodes are selected from the set of trusted nodes for a given period of time based on the node energy, available node storage capacity and node computing power. The watchdog node has the additional duty to monitor other nodes in the network for a fixed period of time to detect the malicious behavior. Watchdog node maintains two threshold values SUSPECT_THRESHOLD and ACCEPTANCE_THRESHOLD to measure the trustworthiness of the non trusted nodes. If any node crosses the SUSPECT_THRESHOLD, it will be declared as malicious node by the watchdog node. If a node crosses the ACCEPTANCE_THRESHOLD, it will be declared as trusted node. The existing AODV protocol was extended with six extra packet types send_data, nodes_neighbors, trusted_enc_request, trusted_enc_reply, is_watchdog and is_malicious to implement the security. However, the additional packet types increases the network overhead.[13]

4.5 Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile Ad Hoc Network

ISSN 2348 – 7968

In this paper a new intrusion detection system is proposed called ExWatchdog system to overcome the weakness of watchdog system. ExWatchdog is an extension of Watchdog and its function is also detecting intrusion from malicious nodes and reports this information to the response system, Routeguard. It aims to detect nodes that falsely report other nodes as misbehaving. ExWatchdog has two parts: Watchdog and routeguard. Either in watchdog or routeguard, each node updates ratings of nodes it knows according to the information provided by any node in the network. If a node send a false report that says other nodes as misbehaving. A malicious node could partition the network by claiming that some nodes following it in the path are misbehaving. ExWatchdog detection system solve this problem. The source node first searches a path that has no malicious node in it from the routing table. If there is not such a path available, the source then launch a Route Discovery to find a new one. After finding a path, the source sends the message using the found path. Upon receiving the message, destination node will search its own table to see if there is a match. If there is not a matching entry in the table, it means the node is malicious and the destination node returns a message to the source confirming that the malicious node is really malicious. If there is, destination node then compares the sum field of the passing in message with the one found in the table. If the two sums equal, it means that the malicious node forwards all packets that the source sends thus it is not malicious. On the contrary, if the two sums are not equal, the node falsely report might be malicious. Routeguard will use this information to update the rating of corresponding node. It discovers malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. The main feature of 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.[14][15]

4.6 Cross layer approach

Djenouri [16] used a cross-layer approach to detect data packet droppers. In this approach, the two parts of the monitoring protocol are used in network layer and MAC layer. Each node monitors the forwarding of each packet it transmits, like watchdog approach. To reduce the network overhead, for each received packet the node transmits two-hop ACK integrated with MAC ACK. To prevent an intermediate node from falsifying two-hop ACK, public key distribution is used in this approach. To reduce the cost of this approach, random two-hop ACK is used. In this approach, a random ACK is transmitted in every three consecutive nodes instead of transmitting ACK for every data packet. A node will select an even number if it needs an ACK, otherwise it will select an odd number. This approach increases the network overhead due to public key distribution.[16]

4.7 Video Transmission Enhancement in presence of Misbehaving Nodes in MANETs

This paper proposes a novel intrusion detection system, which is an adaptive acknowledgment scheme (AACK) with the ability to detect misbehaved nodes and avoid them in other transmissions. It is an acknowledgement based scheme which can be considered as a combination of scheme called TACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACKnowledge (ACK). In this system source node 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 receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node along the reverse route. Within a predefined time period, if the source node receives this ACK acknowledgment packet, then the packet transmission from source node to destination node is successful. Otherwise, the source node will switch to TACK scheme by sending out a TACK packet. Misbehaving nodes that exhibit abnormal behaviours can disrupt the network operation and affect the network availability by refusing to cooperate to route packets due to their selfish or malicious behaviour. The aim of AACK scheme is to overcome watchdog weaknesses due to collisions and limited transmission power and also to improve TWOACK scheme. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead. 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. AACK reduces the network overhead than the TWOACK scheme while maintaining the same network throughput.[17][18]

4.8 Acknowledgement Based Routing Misbehaviour Detection

In semiautonomous mobile sensor networks, since human operators may be involved in the control loop, particular improper actions may cause accidents and result in catastrophes. For such systems, this paper proposes a command filtering framework to accept or reject the

human-issued commands so that undesirable executions are never performed. In the present approach, Petri nets are used to model the operated behaviors and to synthesize the command filters for supervision. This paper proposes the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehaviour and to mitigate their adverse effect. It is used to detect some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. 2ACK scheme send twohop acknowledgment packets in the opposite direction of the routing path. It is a network-layer technique to detect misbehaving links rather than nodes and to mitigate their effects. The 2ACK scheme detects misbehaviour through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route. 2ACK transmission takes place for every set of triplets along the route. Therefore, only the first router from the source will not serve as a 2ACK packet sender. The last router just before the destination and the destination will not serve as 2ACK receivers. To reduce additional routing overhead only a fraction of the received data packets are acknowledged in the 2ACK scheme.

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. Source send data packet to receiver. Receiver generates the 2ACK packet back to sender. Retrieval of 2ACK packet within a predefined time period indicates successful transmission otherwise both destination and intermediate nodes are reported as malicious.[19][20]

4.9 Detecting Forged Acknowledgements in MANETs

MANET suffers from the threat that it fails to detect misbehaving node when the attackers are smart enough to forge the acknowledgement packets. In this paper, we introduce a intrusion detection scheme with digital signature algorithm to provide secure transmission against false misbehavior report and partial dropping. This intrusion detection system assumes the link between in the network is bidirectional. Misbehaving nodes also lies in the network. It assumes misbehaving nodes are intermediate nodes; they are neither the source node nor the destination node. In routing stage they cooperate with other nodes but they drop the packets instead of forwarding to next node. After dropping the packets the misbehaving node generate a forge acknowledgement and sent to source node in order to conceive the source node. When the source node sends out the data packet it registers the packet ID and sent time. After receiving packet destination node need to send acknowledgement packet with packet id to source. Successful reception of acknowledgement packet at source the transmission is comp leted andconfirmed. After certain time period the source node does not receive the acknowledgement from destination it switch to secure acknowledge mode. In this scheme, for every three consecutive nodes along the transmission route, the third node is required to send back an S-ACK packet back to the first node to confirm receiving the packet. In this system the third node is required to sign this S-ACK packet with its own digital signature. The intention of doing this is to prevent the second node from forging the S-ACK packet without forward the packet to the third node. This is really dangerous as the malicious node can create a black-hole in the network without being detected. When the first node receives this S-ACK packet, it verifies the third node's signature with the predistributed public key. On the other hand, if no S-ACK packet is received within a predefined time period; the first node will report both second node and the third node as malicious. When the source node receives the malicious report, instead of trusting the report immediately and marks the nodes as malicious, it requires the source node to switch to MRA mode to confirm. The source node switches to MRA mode by sending out an MRA packet to the destination node via a different route. If such route does not exist in the cache, the source will find a new route. For extreme conditions when there are no alternative routes from source node to the destination node, this detection system, by default, accepts the misbehaving report [21].

4.10 EAACK-A Secure Intrusion Detection System For MANETs

MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range [2]. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. The open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks.

In this paper it proposes a new system called EAACK-Enhanced Adaptive ACKnowledgement is specially

ISSN 2348 – 7968

designed for MANETs to detect the attackers. EAACK is an acknowledgement based scheme. EAACK is an acknowledgment-based IDS. This scheme makes use of digital signature. It requires all acknowledgment packets to be digitally signed. This new system requires acknowledgement for the every packet sent to the receiver with the signature. First after sending packets to the receiver it waits for the acknowledgement. Within the predefined time interval the source received the acknowledgement from receiver then the packet transmission is successful. Otherwise the source node will switch to the secure acknowledgement mode.

In secure acknowledgement mode every consecutive three nodes work together to detect the misbehaving nodes in the route. Every third node in the group needs to give acknowledgement to the first node. If any node fails to send acknowledgement is marked as malicious node. Then the source node switches to misbehaviour report authentication (MRA) mode.

In MRA mode, source node first searches its local knowledge base for the alternative path to the destination. Upon receiving MRA packet, destination node will searches for any received MRA is stored; if it stored then ignore the new packet and the node which sends that packet marked as malicious. Otherwise the nodes marked as malicious in the packet are removed from the route in future transmission. This system uses the digital signatures to authenticate the acknowledgement packets. Digital signatures prevent the acknowledgement packets to be forged. The sender of the acknowledgement packet must sign the packet and after the reception of the packet receiver will verify the authenticity of the packet. This new system reduces the packet dropping attack; it is the major security threat. In case of limited transmission power, receiver collision, false misbehavior rate EAACK is a preferred IDS than the existing approaches [22].

5. CONCLUSION

When it comes to ad-hoc networks, we refer to a technology which consists of wireless telecommunications network of dynamic topology, where a set of mobile communication nodes such as routers interact among themselves, passing on information without relying on any fixed infrastructure. Given this description, we find some limiting characteristics that make the Ad-Hoc wireless networks, very vulnerable to intruders and attacks that can damage the integrity of the network. Features such as the limited ability to process nodes, limited bandwidth, and an interaction that requires each node to be involved in decision making network make these networks a comprehensive field of study in communications. In our study, we have found that necessity of secure routing protocol is still a burning question. There is no general algorithm that suits well against the most commonly known attacks. However, in short, we can say that the complete security solution requires the prevention, detection and reaction mechanisms applied in MANET. In this paper we discussed various Security Aspects of MANETs & have done literature survey for detecting the malicious nodes misbehaviors in mobile adhoc network (MANET). This paper shows the overview of various intrusion detection systems to detect the malicious nodes and analyze the attacks in the network and provide security against those attacks in order to provide efficient packet transmission without modification, dropping and partial dropping of packets using an efficient intrusion detection system.

References

[1] Y. Zhou, Y. Fang and Y. Zhang, “Securing wireless sensor networks: a survey”, *IEEE Commun. Surveys Tutorials*, vol. 10, num. 3, pp. 6-28,2008.

[2] E. Cayirci and C. Rong, “Security in Wireless Ad Hoc and Sensor Networks”, *book published by Wiley*, 2009.

[3] Y. Wang, G. Attebury and B. Ramamurthy, “A survey of security issues in wireless sensor networks”, *IEEE Commun. Surveys and Tutorials*,vol. 8, num. 2, pp. 2–23, 2006.

[4] G. Padmavathi and D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, *InternationalJ. Computer Science*, vol. 4, num. 1, pp. 1–9, 2009.

[5] R. Akbani, T. Korkmaz and G.V.S Raju. "Mobile Ad hoc NetworkSecurity", Lecture Notes in Electrical Engineering, vol. 127,pp. 659-666, Springer, 2012 – here1

[6] C.Perkins, E. Belding-Royer and S. Das, “*Ad-Hoc On-Demand Distance Vector (AODV) Routing*”, RFC3561, July 03.

[7] Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Networks” *IEEE Communications Magazine • October 2002*

[8] Mohseni, S.; Hassan, R.; Patel, A.; Razali, R, “Comparative review study of reactive and proactive routing protocols in MANETs”, *4th IEEE International Conference on Digital Ecosystems and Technologies*, 304-309, 2010.

[9] Y. Hu, D. Johnson, and A. Perrig, “SEAD: Secure efficient distance vector routing for mobile wireless adhoc networks,” *in Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl.*, 2002.

[10] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” *inProc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA*, 2000, pp. 255–265.

[11] S. Buchegger and J.-Y. L. Boudec, “Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks)," in MOBIHOC'02, 2002.

[12] P. Michiardi and R. Molva, “CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," *in CMS'2002, Communication and Multimedia Security 2002 Conference*, September 26-27, 2002

ISSN 2348 – 7968

[13] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad-hoc networks," in *Proc.Radio Wireless Conf.*, 2003, pp. 75–78.
[14] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile adhoc network," *in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland,* Jun. 24–28, 2007, pp. 1154–1159
[15] Hasswa, A.; Zulkernine, M.; Hassanein, H., "Routeguard: an intrusion detection and response system for mobile ad-hoc networks," Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob'2005), *IEEE International Conference on* , vol.3, no., pp. 336-343 Vol. 3, 22-24 Aug. 2005
[16] D. Djenouri, N.Badache, Cross-Layer Approach to Detect Data Packet Droppers in Mobile Ad-Hoc Networks, IWSOS 2006, LNCS 4124, pp.-163-176, 2006.
[17] A Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, H. Mouftah,"AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement", *2010 24th IEEE International Conference on Advanced Information Networking and Applications*
[18] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs,"*Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.
[19] Balakrishnan, K.; Jing Deng; Varshney, V.K., "TWOACK: preventing selfishness in mobile ad hoc networks," *Wireless Communications and Networking Conference, 2005 IEEE* , vol.4, no., pp. 2137-2142 Vol. 4, 13-17 March 2005
[20] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for thedetection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May2007.
[21]. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," *in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore*, Mar. 22–25, 2011, pp. 488–494.
[22] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK- A Secure Intrusion Detection System for MANETs" *IEEE trans*. Vol.60, no.3, MAR, 2013.