IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 2, April 2014.
www.ijiset.com
ISSN 2348 - 7968

IDENTIFYING THE INTRUDERS USING N-GSH AND SRT IN WIRELESS SENSOR NETWORK

D. Nagamany Abirami[#1], V. Nirmala[#2], A. Punitha*[3], S. Lakshmi*[4]

[#]*Assistant Professor*
Department Of Computer Science and Engineering,
Manakula Vinayagar Institute of Technology, Pondicherry University.

[*]*Assistant Professor*
Department Of Information Technology,
Manakula Vinayagar Institute of Technology, Pondicherry University.

***Abstract*— Packet dropping and modification are the common attacks that can be launched by an adversary to disrupt communication in wireless sensor networks. Many schemes have been proposed to mitigate or tolerate such attacks but very few can effectively and efficiently identify the intruders. To address this problem, we propose a simple yet effective scheme, which can identify misbehaving forwarders that drop and modify packets. Most of the bad nodes can be identified by our heuristic ranking algorithm. The alert message will be send to all the users in the network if there is any misbehaving actions occurred. Then the misbehaved node will be blocked and the messages cannot reach to that misbehaved nodes.**

***Keywords*— Packet droppers, Packet Modifiers, Sensor network, intruder detection.**

I. INTRODUCTION

In a Wireless Sensor Network [1], a sensor monitor the environment, detects the intruders, produce data and involves in forwarding the information towards a sink. In a hostile environment the sensor node performs the task in monitoring. An adversary may launch various attacks to disrupt the communication. Among these two attacks are common they are packet dropping and packet modification. To locate the packet droppers and modifiers, it has been proposed that nodes continuously monitor the environment or forwarding behaviours. If the neighbours are misbehaviours the approaches can be extended to identify the bad nodes.

In this paper we propose a scheme to identify the packet droppers and modifiers immediately after the misbehaving activities occurs. For every sensor node, the node categorization algorithm, heuristic algorithm and detour algorithm can be performed to identify the intruders.

II. ALGORITHMS

The algorithms are used to identify the packet droppers and modifiers, and blocked the identified intruders.

A. NODE CATEGORIZATION

In every round [1], for each sensor node u, the sink keeps tracks of the number of packets sent from u, the sequence numbers of these packets, and the number of flips in the sequence numbers of these packets,(i.e., the sequence number changes from a large number such as Ns-1 to a small number such as 0).In the each round, the sink calculates the dropping ratio for each node u. Suppose nu,max is the most recently seen sequence number nu,flip is the number of sequence number flips and nu,rcv is the number of received packets. The dropping ratio in the round is calculated as follows:

$$Du = \frac{Nu,flip * Ns + nu,max + 1 - nu,rcv}{Nu,flip * Ns + Numax + 1}$$

Based on the dropping ratio of every sensor node and the tree topology, the sink identifies the nodes that are droppers for sure and that are possibly droppers. For this purpose, a threshold θ is first introduced. We assume that if a node's packets are not intentionally dropped by forwarding nodes, the dropping ratio of this node should be lower than θ .Note that should be greater than 0, taking into account dropping caused by incidental reasons such as collisions. The first step of the identification is to mark each node with "+" if its dropping ratio is lower than θ or with "-"otherwise. After then, for each path from a leaf node to the sink, the nodes' mark pattern in this path can be decomposed into any combination of the following basic patterns, which are also illustrated in figure.

- + {+}: a node and its parent node are marked as "+".
- + - {-}*: a node is marked as "+", but its one more continuous immediate upstream nodes are marked as "-".
- - {+}: a node is marked as"+", but its parent node is marked as "+".
- - {-}: a node and its parent node are marked as"-".

For each of the above cases, we can infer whether a node.

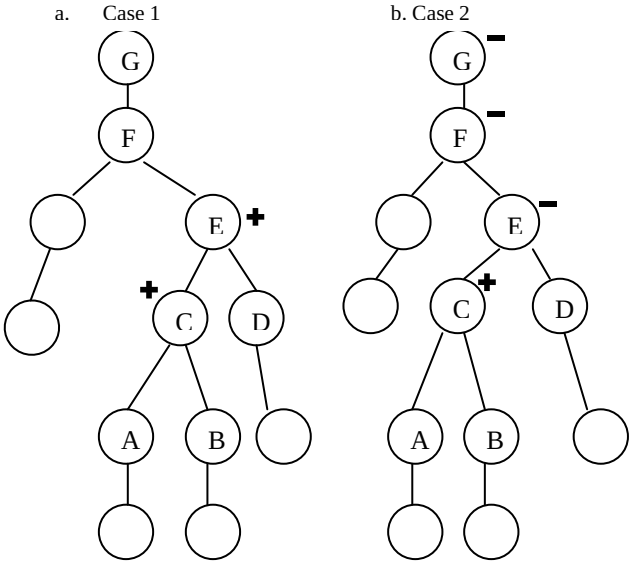
ISSN 2348 - 7968

1. Has dropped packets(called bad for sure),
2. Is suspected to have dropped packets(called suspiciously bad),
3. Has not been found to drop packets(called temporarily good),or
4. Must have not dropped packets (called well for sure).

Case 1: + {+}.The node and its parent node do not drop packets along the involved path, but it is unknown whether they drop packets on other forwarding paths. Therefore, the sink infers that these nodes are temporarily good. For example, in Fig.1a, node C and E are marked "+"and are regarded as temporarily good. A special case is, if a leaf node is marked as "+", it is safe to infer it as good since it cannot drop other's packets.

Case 2:+ - {-}.In the case, all nodes marked as "-" must be bad for sure. To show the correctness of this rule, we prove it by contradiction without loss of generality, we examine the scenario illustrated in Fig.1b, where node C is marked as "+", and nodes E, F and G are marked as"-", there must be some upstream nodes are at least one hop above E, i.e., At least two hops above C. It is impossible for them to differentiate packets from E and C, so they cannot selectively drop the packets from E while forwarding the packets from C. Even if C and he bad upstream node collude, they cannot achieve this. Therfore E must be bad. Similarly, we can also conclude that F and G are also bad.

Case 3: - {+}.In this case, either the node marked as "-"or its parent marked as "+" must be bad. But it cannot be further inferred whether 1) only the node with"-"is bad 2) only the node. Therefore, it is concluded that both nodes are suspiciously bad. The correctness of this rule can also be proved by contradiction. Without loss generality, let us consider the scenario shown in Fig.1c, where node C is marked as "-", and node E is marked as "+".Now suppose both C and E is good, and hence there must marked exist at least one upstream node of E which is a bad node that drops the packets sent by V. However, it is impossible to find such an upstream node since nodes F and G land other upstream nodes cannot selectively drop packets from node C while forwarding packets from node E. Hence either node C is bad or node E is bad in this case.



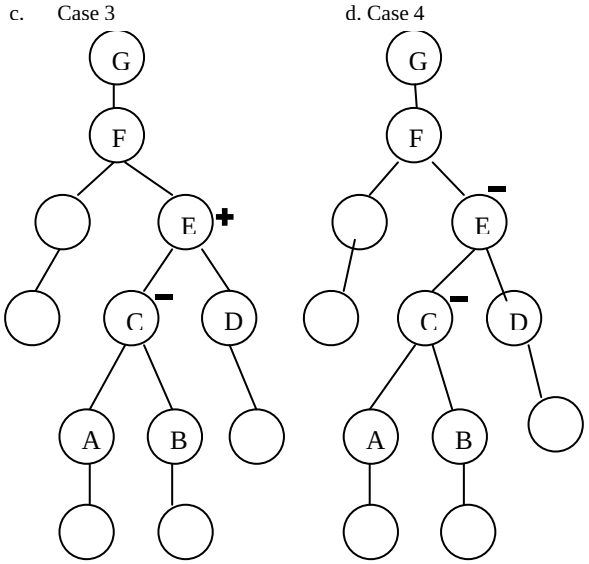


Fig. 1 Node status pattern

Case 4:- {+}.In this case, every node marked with "-"could be bad or good conservatively, they have to be considered as suspiciously bad. On the other hand, suppose v is a child of u and they are both marked as '-".If the dropping ratio of u is larger than that of v by at least θ (i.e., dy < dv and>θ, recalling that θ is a threshold used to tolerate incidental droppings), node u is bad for sure, otherwise, both u and v are suspiciously bad with "+" is bad.

B. GSH ALGORITHM

Identify bad nodes from the potentially large number of suspiciously bad nodes [1], the sink runs GSH algorithm. In this paper, we propose a simple yet effective scheme to catch both packet droppers and modifiers. In this scheme, a routing tree rooted at the sink is first established. When sensor data is transmitted along the tree structure towards the sink, each packet .The format of the small packet marks is deliberately designed such that the sink can be obtain very useful information from the marks. Specifically based on the packets marks, the sink can figure out the dropping ratio associated with every sensor node, and then runs our proposed node categorization algorithm to identify nodes that are droppers/modifiers for sure or suspicious droppers/modifiers

GLOBAL RANKING-BASED (GR) METHOD

The GR method is based on the heuristic that, the more times a node are identified as suspiciously bad, the more likely it is a bad node. With this method, each suspicious node u is associated with an accused account which keeps track of the times that the node has been identified as suspiciously bad nodes. To find out the most likely set of suspicious nodes after n rounds of detection, all suspicious nodes are ranked based

on the descending order of the values of their accused accounts. The node with the highest value is chosen as a most likely bad node and all the pairs that contain this node are removed from S1, . . . , Sn, resulting in new sets. The process continues on the new sets until all suspicious pairs have been removed.

STEPWISE RANKING-BASED (SR) METHOD

It can be anticipated that the GR method will falsely accuse innocent nodes that have frequently been parents or children of bad nodes: as parents or children of bad nodes, according to previously described rules in Cases 3 and 4, the innocents can often be classified as suspiciously bad nodes. To reduce false accusation, we propose the SR method. With the SR method, the node with the highest accused account value is still identified as a most likely bad node. However, once a bad node u is identified, for any other node v that has been suspected together with node u, the value of node v's accused account is reduced by the times that u and v have been suspected together. This adjustment is motivated by the possibility that v has been framed by node u. After the adjustment, the node that has the highest value of accused account among the rest nodes is identified as the next mostly like bad node, which is followed by the adjustment of the accused account values for the nodes that have been suspected together with the node. Note that, similar to the GR method, after a node u is identified as bad, all suspicious pairs with format (u,*) are removed from S1, . . . , Sn. The above process continues until all suspicious pairs have been removed.

HYBRID RANKING-BASED (HR) METHOD

The GR method can detect most bad nodes with some false accusations while the SR method has fewer false accusations but may not detect as many bad nodes as the GR method. According to HR, the node with the highest accused account value is still first chosen as most likely bad node. Thus, the accusation account value is considered as an important criterion in identification, as in the GR method; meanwhile, the possibility that an innocent node being framed by bad nodes is also considered by not choosing the nodes which are always being suspected together with already identified bad nodes, as in the SR method.

C. SELECTED ROUTING TREE

The SRT (Selected Routing Tree) is used to select the path to send the packet. The DAG (Directed Acyclic Graph) which generates the possible paths for all the nodes in the network, then the Selected Routing Tree will distribute those paths to all the nodes in the network. The packet can be send through various paths. Each and every node in the network uses various paths for sending the packets. For that the selected routing tree will be helpful for selected the paths.

III. EXISTING SYSTEM

In the existing system they identify the packet dropping and modification occurred. The identified misbehaving nodes will not know to the other nodes in the network, so the nodes will send the packets again to the misbehaving node. The identification of misbehaving node is slow in the existing system. The routing tree generated also will be slow in the existing system. The DPSTN [5] (Detection of Packet Dropping attacks for Wireless Sensor Networks) monitors paths and detects whether any node on a path drops packets. Once the packet dropping is detected, the alternate path for communication will be chosen. This will increase the communication cost and also path selection cost.

IV. PROPOSED SCHEME

In the proposed work the receiver will send the alert message to the sender when they identify by packet droppers and modifiers. The alert message will be send to all the nodes in the network, so the nodes in the network will be aware of the misbehaving node and the packet cannot be send again to the misbehaving node through that path. The identification of dropping and modification will be identified correctly. If there is any misbehaving action like packet dropping and modification occurred in any of the node, the modified packet will forward to the sender. The server will identify the misbehaving node and list the misbehaving node, packet dropping, modification and also list the path in which the modification and dropping is occurred. Each and every node having different key. The nodes will encrypt the packet using own key and using own encryption technique. The server will decrypt the packet by using the corresponding user key.

A. SYSTEM ARCHITECTURE

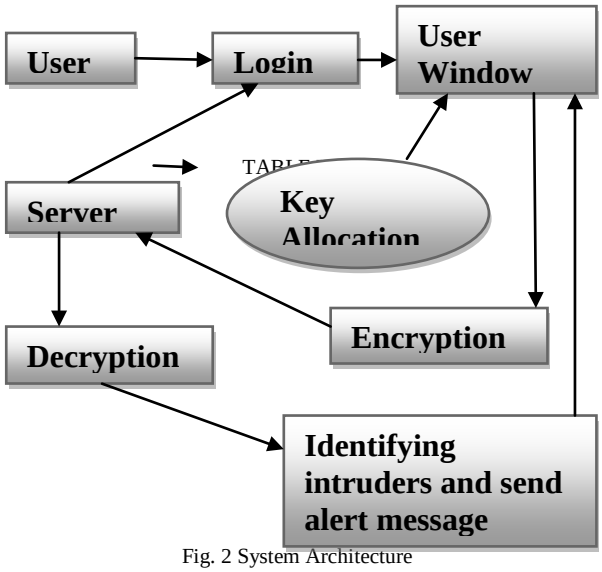


Fig. 2 System Architecture

The overall system process is defined in the system architecture. The user and sever has to login to enter into the system. Then the server will generate the key and send to all the nodes in the network. The sender node will be chosen by the server and then the file is attached by the sender node. The sender node will split up to into packets and encrypt the packet using key. The Selected Routing Tree is used to select the possible paths and distribute those paths to all the nodes in the network. The sender will select the particular path to send the encrypted packet. The packet will be transmitted along that path and will reached the destination. If there is any modification or dropping occurs then the server will identify that and send the alert message to all the nodes in the network. if there is any modification of dropping is occurred then server will decrypt the packet and get the original packet.

V. PERFORMANCE APPRAISAL

The comparison of finding packet droppers and modifiers in sensor network between the existing and the proposed system has been analysed and given as the comparative study below. The routing tree based on the path and the distance has been analyzed and the better performance of finding the intruders is given based on throughput, packet loss and alert message.

A Selected Routing Tree scheme is proposed for selecting the possible paths for all the nodes in the network and distributes it. Despite its simplicity, this scheme is shown to be capable of finding out who is the dropper or modifier in the particular selected path. Moreover, it is proved that this scheme routes messages via selected paths and only the encrypted message is sent to the destination. The demonstration of this scheme shows how the packets travelling the particular address with the respective Internet protocol (IP). But in existing work, they gave demo in Network simulator without representing any alert message to the required the sender.

The packet is decrypted at the final stage using key. Initially, the large size of text file can be splitted and each splitted packet is encrypted using ASCII which makes the intruders difficult in finding packets. The DAG graph is achieved to find the path for sending the spitted packets. In our system, defines the intermediate for path each node between sender and receiver. This updated definition of intermediate is also more convenient for the context of message routing because the messages are received from a node and given to another node on the way towards the destination. Here, the socket network represent the period over which the node holds the message. By combining SRT protocol with the GHS algorithm gives the results with real trace driven demonstration is more efficient when compared to node categorization algorithm. To show the benefits of the proposed metric, the project proposes Selected Routing Tree (SRT) scheme in which the messages are routed over DAG.

A. SECURITY GRAPH WIHOUT ALERT MESSAGE

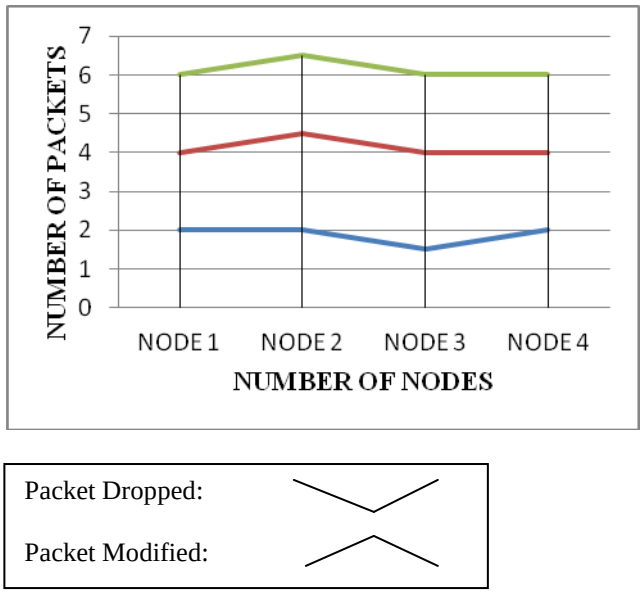
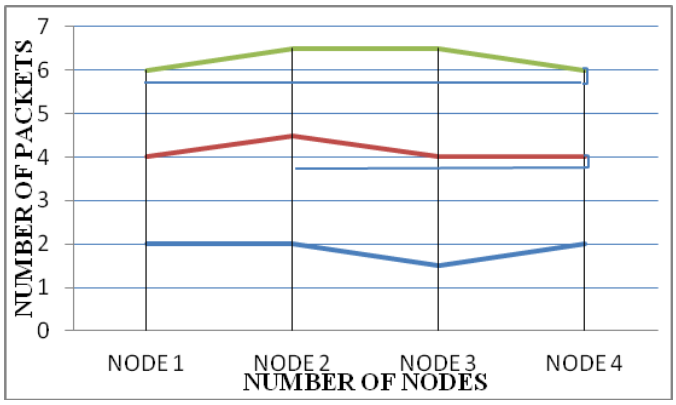


Fig 3: Security graph without alert message

The above line graph show in Fig: 3 (Existing system) where the packet dropping and modification occurs. The line moves upward represent modification and downward represent dropping but never these drawbacks ever knows to sender or receiver.

The conventional method uses the path between the nodes to transfer the data to be from the source to destination. But the proposed method implies that the dropped message can be identified better than the older method in all means by using the Alert message from server or destination. The socket network involves in sending packets parallel through a selected path from sender to receiver.

B. SECURITY GRAPH WITH ALERT MESSAGE



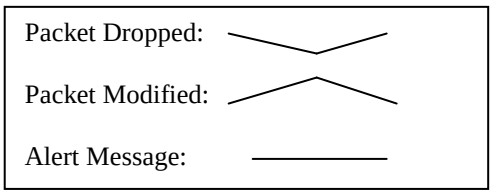


Fig 4: Security graph with alert message

The above line graph show in Fig: 4 (Propose system) where the packet dropping and modification occurs. The line moves upward represent modification and downward represent dropping occurs. It represent who dropped and modified when the packet dropping and modification occurs suddenly alert message can be sent to the particular node.

In the existing system the destination find the packet can be dropped and modified but never represent where packet dropped and modified. Thus, the proposed system represent where the packet drawbacks and who performed the misbehaviour actions over the nodes. While sending packet to the node it must be encrypted using algorithm and also key can be assigned for each node. Even if the misbehaving actions occur the node can be easily identified using a secret key which is also not implemented in existing system. The throughput is the average rate of successful in finding the intruders over a communication channel.

The data delivered to the nodes through the network mode of transferring involves the message delivery that need to be considered. The nodes initially send the messages to the next node or final node according to the selected path. In this demonstration each node can be represented with one modifier and dropper. If the packet is dropped in one node, that packet can be modified in another node. This misbehaving action is finally finds by the destination and send alert message to the modified and dropped node with the help of IP address. The conventional system achieved less task compared to proposed system. Thus we can come to a conclusion that the Selected Routing Tree along with GSH and node categorization algorithm is efficient compared to existing system algorithm.

VI. CONCLUSION

The packet dropping and modification are the common attacks in the wireless sensor networks that can be identified easily by using node categorization algorithm and GSH algorithm. The possible path for each and every node will be generated by using the selected routing that will increase the communication speed and also decrease the communication cost. Our system provides the high level of security for sending the packet through the network. The user and server has to login into their system for communicating. The node will send the encrypted packet through the selected path to the server. The server will identify the intruders in the path and list the intruder nodes and path in which the packet is modified or dropped. Our system identifies the intruders in a few seconds and sends the alert message to all the nodes in the network. The alert message will be useful for the nodes to know which node is the modified or dropped node. The node cannot send the packet again to the intruder nodes and the nodes cannot use the same path for sending the packet next time. In future, this can be implemented by using various algorithms and also can use the several routing path for packet transmission. We can also transmit image files, audio and video files in the future enhancement.

REFERENCES

[1] Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang, and Wensheng Zhang, “Catching Packet Droppers and Modifiers in Wireless Sensor Networks”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 5, MAY 2012.

[2] Culler, D. E and Hong, W., “Wireless Sensor Networks”, Communication Of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[3] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” *the First IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, May 2003.

[4] M. Kefayati, H.R. Rabiee, S.G. Miremadi, and A. Khonsari, “Misbehavior Resilient Multi Path Data Transmission in Mobile Ad-Hoc Networks,” Proc. Fourth ACM Workshop Security of Ad Hoc and Sensor Networks (SASN ’06), 2006.

[5] V. Bhuse, A. Gupta, and L. Lilien, “Dpdsn: Detection of packet-dropping attacks for wireless sensor networks,” *In the Trusted Internet Workshop, International Conference on High Performance Computing*, December 2005.

[6] Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S.,“A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks”, to appear in IEEE ICNEWS 2006.

[7] R. Roman, J. Zhou, and J. Lopez, “Applying Intrusion Detection Systems to Wireless Sensor Networks,” Proc. IEEE Third Consumer Comm. Networking Conf. (CCNC), 2006.

[8] H. Chan and A. Perrig, “Security and Privacy in Sensor Networks,” Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[9] F. Liu, X. Cheng, and D. Chen, "Insider Attacker Detection in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2007.

[10] K. Ioannis, T. Dimitriou, and F.C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks," Proc. 13th European Wireless Conf., 2007.

[11] J.M. Mccune, E. Shi, A. Perrig, and M.K. Reiter, "Detection of Denial-of-Message Attacks on Sensor Network Broadcasts," Proc. IEEE Symp. Security and Policy, 2005.

[12] B. Yu and B. Xiao, "Detecting Selective Forwarding Attacks inWireless Sensor Networks," Proc. 20th Int'l Symp. Parallel and Distributed Processing (IPDPS), 2006.

[13] B. Xiao, B. Yu, and C. Gao, "Chemas: Identify Suspect Nodes in Selective Forwarding Attacks," J. Parallel and Distributed Computing, vol. 67, no. 11, pp. 1218-1230, 2007.

[14] X. Zhang, A. Jain, and A. Perrig, "Packet-Dropping Adversary Identification for Data Plane Security," Proc. ACM CONEXT Conf(CoNEXT'08), 2008.

[15] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "Secmr—A Secure Multipath Routing Protocol for Ad Hoc Networks," Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, 2007.

[16] M. Just, E. Kranakis, and T. Wan, "Resisting Malicious Packet Dropping inWireless Ad Hoc Networks," Proc. Int'l Conf. Ad-Hoc Networks and Wireless (ADHOCNOW '03), 2003.

[17] S. Ganeriwal, L.K. Balzano, and M.B. Srivastava, "Reputation- Based Framework for High Integrity Sensor Networks," ACM Trans. Sensor Networks, vol. 4, no. 3, pp. 1-37, 2008.

[18] K.Liu ,J.Deng, P.K.Varshney, and K. Balakrishnan, "AnAcknowledgmentBased Approach for the Detection of Routing Misbehavior in Manets," IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.

[19] B. Barak, S. Goldberg, and D. Xiao, "Protocols and Lower Bounds for Failure Localization in the Internet," Proc. Eurocrypt, 2008.

[20] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei,"Reputation and Trust-Based Systems for Ad Hoc and Sensor Networks," Proc. Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks, 2008.