A Protected Interruption Discovery Scheme for Manet

Kathiresan[1] Venkatesan[2]
[1]PG Scholar [2]Assistant Professor
[1, 2] Information Technology Department
[1, 2]Veltech Multitech Dr Rangarajan Dr Sakunthala Engineering College, Chennai

Abstract--- Protecting the network layer from malicious attacks is an important and challenging security issue in mobile ad hoc networks (MANETs). In this paper, a security mechanism is proposed to defend against Cooperative Black Hole Attack and packet dropper on the well-known AODV routing protocol in MANETs. In this paper we proposed an approach for better analysis and improve security of AODV, which is one of the popular routing protocols for MANET. Our scheme is based on AODV protocol which is improved by deploying DRI table to identify black hole nodes and packet-monitoring algorithm to overhear the next hop's action to identify selfish node in MANET.

Keywords: Black Hole, Gray Hole, Cross Layer Design, DSR, Intrusion Detectio, security, routing and AODV

I. INTRODUCTION

Intrusion detection is the act of detecting unwanted traffic on a network or a device. An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies. Many IDS tools will also store a detected event in a log to be reviewed at a later date or will combine events with other data to make decisions regarding policies or damage control. One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN).

In such a network, a set of mobile nodes are connected to a fixed wired backbone. WLANs have a short range and are usually deployed in places such universities, companies, cafeterias, etc. However, there is still a need for communication in several scenarios of deployment where it is not feasible to deploy fixed wireless access points due to physical constraints of the medium.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. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly.

II. LITERATURE REVIEW

A brief literature review was done with this domain and they are listed below;

A. Video transmission enhancement in presence of misbehaving nodes in MANETs

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. The end-to-end acknowledgment scheme in ACK is shown below. In the ACK scheme shown below, 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 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.

B. Catching Packet Droppers and Modifiers in Wireless Sensor Networks

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 are transmitted along the tree structure toward the sink, each packet sender or forwarder adds a small number of extra bits, which is called packet marks, to the packet.

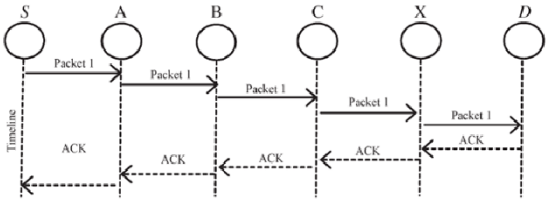

Fig. 1: AACK

The format of the small packet marks is deliberately designed such that the sink can obtain very useful information from the marks. Specifically, based on the packet 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 are suspicious droppers/modifiers. As the tree structure dynamically changes every time interval, behaviors of sensor nodes can be observed in a large variety of scenarios. As the information of node behaviors has been accumulated, the sink periodically runs our proposed heuristic ranking algorithms to identify most likely bad nodes from

suspiciously bad nodes. This way, most of the bad nodes can be gradually identified with small false positive.

C. A simple, cheat-proof, credit-based system for mobile ad-hoc networks

In this paper, we propose Sprite, a simple, cheat-proof, credit-based system for mobile ad-hoc networks with selfish nodes, our system also uses credit to provide incentive to selfish nodes. However, one of the novel and distinguishing features is that our system does not need any tamper-proof hardware at any node. At a high level, the basic scheme of our system can be described as follows. When a node receives a message, the node keeps a receipt of the message. Later, when the node has a fast connection to a Credit Clearance Service (CCS), it reports to the CCS the messages that it has received/forwarded by uploading its receipts. The CCS then determines the charge and credit to each node involved in the transmission of a message, depending on the reported receipts of a message. The design of our system needs to address two main issues.

III. SYSTEM DESIGN

A. Existing System

Existing solutions for identifying misbehaving nodes either use some form of per-packet evaluation of peer behavior or provide cooperation incentives to stimulate participation. Incentive-based approaches do not address the case of malicious nodes who aim at disrupting the overall network operation. On the other hand, per-packet behavior evaluation techniques are based on either transmission overhearing issuance of per-packet acknowledgements these

Monitoring operations must be repeated on every hop of a multichip route, thus leading to high communication overhead and energy expenditure. Moreover, they fail to detect dropping attacks of selective nature, since intermediate monitoring nodes may not be aware of the desired selective dropping pattern to be detected. The problem with the 2ACK algorithm is that it can detect the misbehaving link but cannot decide upon which one of the nodes associated with that link are misbehaving When we sending our data to destination in the techniques will not give more security, we don't know the accurate selfish node in our infrastructure Ad-hoc network so in this also main drawback of our wireless Network.

B. Proposed System

Our proposal is based on a path based scheme that is node does not watch every node in the neighbor only observe next hop in the current route path. We optimize AODV protocol with extra fields in the routing table such as timestamp, current transmission time .The packet monitoring algorithm implement in every node participant in the transmission path. The monitoring node should calculate the overhear rate when packet forward to the next node if the rate is higher than the threshold ,the monitoring node then set a neighbor node as suspicious node . further testing would be conducted as this suspicious node must be false due to network traffic might loss of packet. Neighbour node send couple of packet and overhear a neighbor node if suspicious node set more than two for same node then it mark as a malicious node then the node isolated from the network.

C. System Architecture

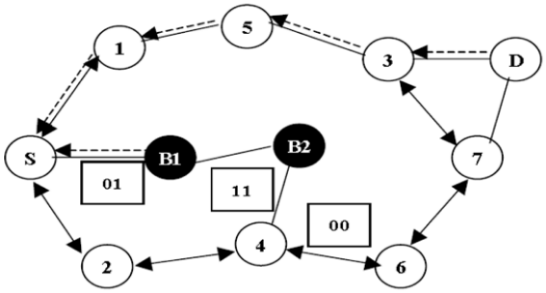

Fig. 2: System Architecture

D. Modules involved

There are three modules involved in this process they are; Aodv Route Discovery, Suspicious node identification and Malicious node identification. AODV Route Discovery: The AODV Routing protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path. The major difference between AODV and Dynamic Source Routing (DSR) stems out from the fact that DSR uses source routing in which a data packet carries the complete path to be traversed. However, in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission. In an on-demand routing protocol, the source node floods the *RouteRequest* packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single *RouteRequest*. The major difference between AODV and other on-demand routing protocols is that it uses a *destination sequence number* (DestSeqNum) to determine an up-to-date path to the destination. A node updates its path information only if the *DestSeqNum* of the current packet received is greater or equal than the last *DestSeqNum* stored at the node with smaller hopcount.

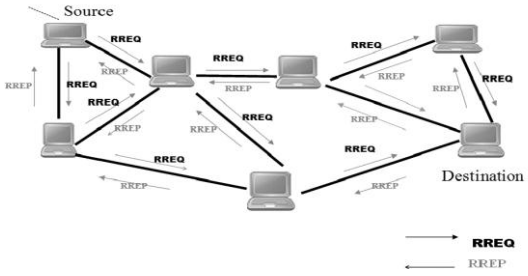

Fig. 3: Route request

Suspicious node identification: Each node operating as monitoring node when the data packet sent to the neighbour node will keep record for each of its neighbour node in a routing table,every node should overhear its neighbor until its forward the packet,if the forwarding rate is higher then the threshold value but still its not forward the packet ,the monitoring node set neighbour node as suspicious node. Threshold value can be calculated based on first packet transmission time calculated based on the own clock of monitoring node. Each and every packet we calculate the average threshold time ,onlyif neighbour node is not suspicious node each node act as a monitoring node when it forward the packet to its neighbor node.

Threshold time=Tt,

Current transmission time=Ct,
Tt=(previous packet transmission time +threshold time)/2

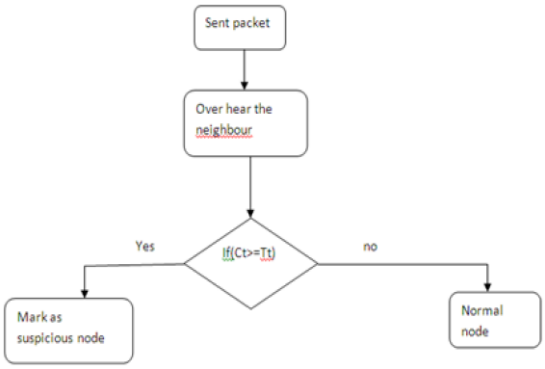

Fig. 4: suspicious node

Malicious node identification: If one node is mark as a suspicious node cannot guarantee that the node should be suspicious .so we further send a packet continuously and over hear its neighbor node .if its not forward its packet then the monitoring check the neighbour node is already mark as suspicious node if its marked then neighbour node set as malicious node and isolated from the network. And monitoring node inform to all neighbour node.

IV. A PATH-BASED DETECTING METHOD

A. *Detection Algorithm*

Our proposal is based on a path based scheme. That is, a node does not watch every node in the neighbor, but only observes the next hop in current route path. For example, in Figure 5, S is the source node; D is the destination node; and A is a black hole. Node S is sending data packets to node D through the path S, A, B, D. In our scheme, Node S only watches Node A, which is the next hop; but does not care Node 1 and Node 2.

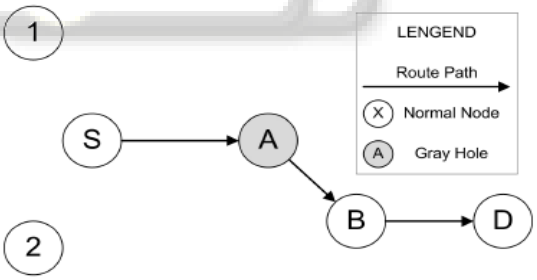

Fig. 5: A path based detection scheme

To implement the algorithm, every node should keep a FwdPktBuffer, which is a packet digest buffer. The algorithm is divided as follows; When a packet is forwarded out, its digest is added into the FwdPktBuffer and the detecting node overhears.Once the action that the next hop forwards the packet is overheard, the digest will be released from the FwdPktBuffer. In a fixed period of time, the detecting node should calculate the overhear rate of its next hop and compare it with a threshold. We define overhear rate in the Nth period of time as OR(N).

$$OR(N) = \frac{\text{total overheard packet number}}{\text{total forwarded packet number}}$$

If the forwarding rate is lower than the threshold, the detecting node will consider the next hop as a black or gray hole. Latter, the detecting node would avoid forwarding packets through this suspect node.

B. *Advantage of the Algorithm*

Our method has several advantages:

- In this scheme, each node only depends on itself to detect a black or gray hole. The algorithm does not send out extra control packets so that Routing Packet Overhead (the ratio of total number of routing related transmissions and the total number of packet transmissions) remains the same as the standard DSR routing protocol.
- Not like other collaborative detecting architectures, our proposal requires no encryption on the control packets to avoid further attacks on detection information sharing.
- There is no need to watch all neighbors' behavior. Only the next hop in the route path should be observed.

As a result, the system performance waste on detection algorithm is lowered.

C. *Analysis of False Positive Probability*

One problem of this detection method is that it suffers from a high false positive probability under high network overload if a constant threshold is used. The cause of high false positive probability is hidden node problem in carrier-sensing multiple access with collision avoidance (CSMA/CA) protocol. A hidden node is a node which is beyond range of a packet sender (node S in Figure 6) but in the range of a packet receiver (Node A in Figure 6). In Figure 6, Node B does not hear the data from Node S to Node A, and it is a hidden node. When Node B transmits to node C, the transmission collides with that from Node A to node B. Therefore, the hidden nodes lead to higher collision probability.

As for path based detection, black node problem will greatly increase the false positive probability. In Figure 6, Node S is source node and Node C is destination node. Packet 1 is transmitted from Node B to Node C. At the same time, Packet 2 is transmitted from Node S to Node A. Consequently, Packet 1 and Packet 2 will collide at Node A. Then Node S will retransmit Packet 2; but Packet 1 will not be sent again because Packet 1 has been received by Node C successfully. As a result, Node A misses Packet 1 and treats it being dropped by Node B deliberately. In summary, a high network overload leads to a high collision rate caused by hidden node problem, so that the probability that a detecting node fails to overhear its next hop increases accordingly. Thus, the false positive probability rises in the end.

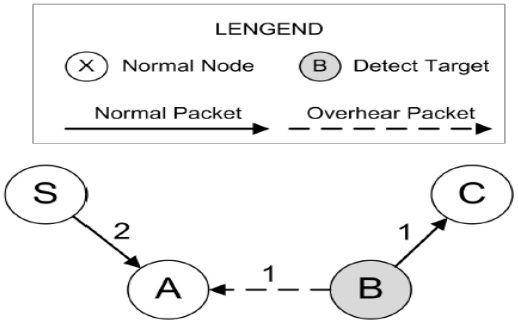

Fig. 6: A collision problem with the path based detection scheme

V. SOLUTION

In this section, we propose a methodology for identifying multiple black hole nodes cooperating as a group with slightly modified AODV protocol by introducing Data Routing Information (DRI) Table and Cross Checking.

A. Data Routing Information Table

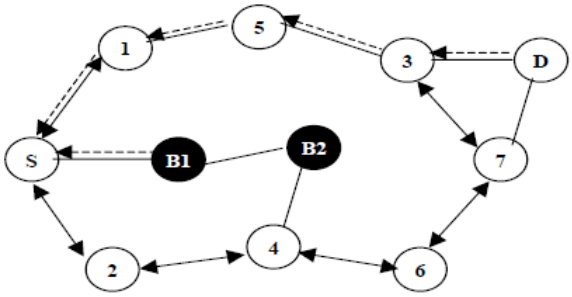

Fig. 7: Solution to avoid cooperative black hole attack

The solution to identify multiple black hole nodes acting in cooperation involves two bits of additional information from the nodes responding to the RREQ of source node S. Each node maintains an additional Data Routing Information (DRI) table. In the DRI table, 1 stands for 'true' and 0 for 'false'. The first bit "From" stands for information on routing data packet *from* the node (in the Node field) while the second bit "Through" stands for information on routing data packet *through* the node (in the Node field). In reference to the example of Figure 7, a sample of the database maintained by node 4 is shown in Table 1. The entry 1 0 for node 3 implies that node 4 has routed data packets from 3, but has not routed any data packets through 3 (before node 3 moved away from 4). The entry 1 1 for node 6 implies that, node 4 has successfully routed data packets from and through node 6. The entry 0 0 for node B2 implies that, node 4 has NOT routed any data packets from or through B2.

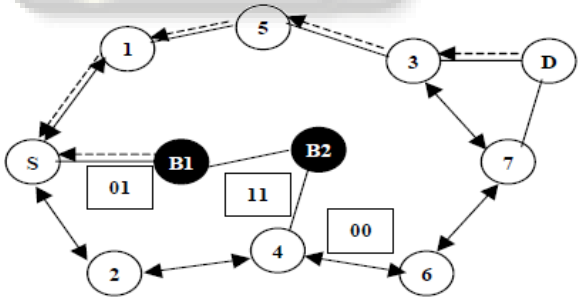

Fig. 8: Solution to identify multiple black hole nodes in one-time check

Node #	Data Routing Information	
	From	Through
3	1	0
6	1	1
B2	0	0
2	1	1

Table. 1: Additional table of data routed from, and routed to nodes maintained by node 4.

B. Cross Checking

In our techniques we rely on reliable nodes (nodes through which the source node has routed data) to transfer data packets. The modified AODV protocol, and the algorithm for our proposed methodology are illustrated in Figure 9. In the protocol, the source node (SN) broadcasts a RREQ message to discover a secure route to the destination node. The Intermediate Node (IN) generating the RREP has to provide its Next Hop Node (NHN), and its DRI entry for the NHN. Upon receiving RREP message from IN, the source node will check its own DRI table to see whether IN is a reliable node. If source node has used IN before to route data, then IN is a reliable node and source node starts routing data through IN. Otherwise, IN is unreliable and the source node sends FRq message to NHN to check the identity of the IN, and asks NHN: 1) if IN has routed data packets through NHN, 2) who is the current NHN's next hop to destination, and 3) has the current NHN routed data through its own next hop. The NHN in turn responds with FRp message including 1) DRI entry for IN, 2) the next hop node of current NHN, and 3) the DRI entry for the current NHN's next hop. Based on the FRp message from NHN, source node checks whether NHN is a reliable node or not. If source node has routed data through NHN before, NHN is reliable; otherwise, unreliable. If NHN is reliable, source node will check whether IN is a black hole or not. If the second bit (ie. IN has routed data *through* NHN) of the DRI entry from the IN is equal to 1, and the first bit (ie. NHN has routed data *from* IN) of the DRI entry from the NHN is equal to 0, IN is a black hole. If IN is not a black-hole and NHN is a reliable node, the route is secure, and source node will update its DRI entry for IN with 01, and starts routing data via IN. If IN is a black-hole, the source node identifies all the nodes along the reverse path from IN to the node that generated the RREP as black hole nodes. Source node ignores any other RREP from the black holes and broadcasts the list of cooperative black holes. If NHN is an unreliable node, source node treats current NHN as IN and sends FRq to the updated IN's next hop node and goes on in a loop from steps 7 through 24 in the algorithm.

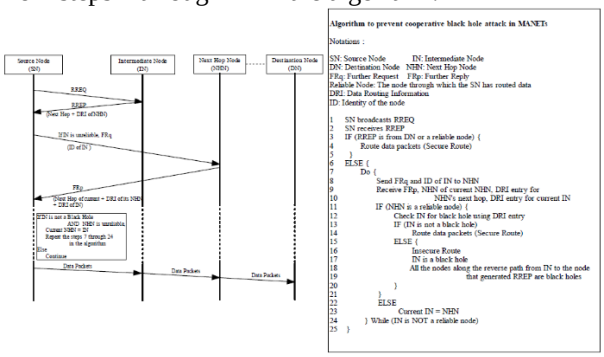

Fig. 9: Modified AODV protocol and algorithm to prevent cooperative black hole attack

As an example, let's consider the network in Figure 8. When node B1 responds to source node S with RREP message, it provides its next hop node B2 and DRI for the next hop (i.e. if B1 has routed data packets through B2). Here the black hole node lies about using the path by replying with the DRI value equal to 0 1. Upon receiving RREP message from B1, the source node S will check its own DRI table to see whether B1 is a reliable node. Since S has never sent any data through B1 before, B1 is not a reliable node to S. Then S sends FRq to B2 via alternative path S-2-4-B2 and asks if B2 has routed any data from B1, who is B2's next hop, and if B2 has routed data packets through B2's next hop. Since B2 is collaborating with B1, it

replies positively to all the three requests and gives node 6 (randomly) as its next hop. When the source node contacts node 6 via alternative path S-2-4-6 to cross check the claims of node B2, node 6 responds negatively. Since node 6 has neither a route to node B2 nor has received data packets from node B2, the DRI value corresponding to B2 is equal to 0 0 as shown in Figure 4. Based on this information, node S can infer that B2 is a black hole node. If node B1 was supposed to have routed data packets through node B2, it should have validated the node before sending it. Now, since node B2 is invalidated through node 6, node B1 must cooperate with node B2. Hence both nodes B1 and B2 are marked as black hole nodes and this information is propagated through the network leading to their listing as black holes, and revocation of their certificates. Further, S discards any further responses from B1 or B2 and looks for a valid alternative route to D. The process of cross checking the intermediate nodes is a one time procedure which we believe is affordable to secure a network from multiple black hole nodes. The cost of cross checking the nodes can be minimized by letting nodes sharing their trusted nodes list (DPI table) with each other.

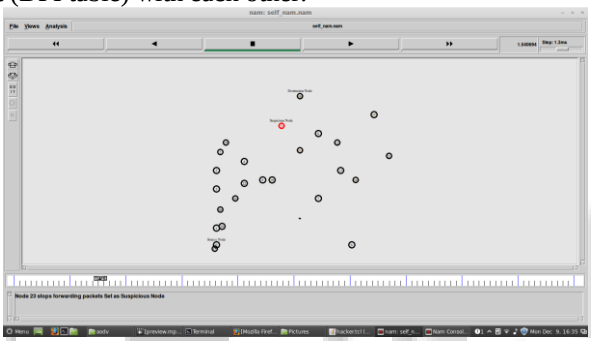

Fig. 10: Snapshot

VI. Conclusion

Wireless Ad Hoc network is likely to be attacked by the black and gray hole attack. To solve this problem, we presented a path based method to detect black and gray hole attack. After theoretically analyzing advantages and disadvantages of this method, we proposed an adaptive algorithm to enhance the detection performance. The simulation results reveal that attacks with gray magnitude above 60% would bring about magnificent damage to the network. We compare our method to other strategy, and confirm our proposal as successful to provide better detection. The proposed solution can be applied to 1.) Identify multiple black hole nodes cooperating with each other in a MANET; and 2.) Discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation. As future work, we intend to develop simulations to analyze the performance of the proposed solution. We also plan to study the impact of GRAY hole nodes (nodes which switch from good nodes to black hole nodes) and techniques for their identification.

References

[1] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, “Video transmission enhancement in presence of misbehaving nodes in MANETs,” Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009

[2] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami,” EAACK—A Secure Intrusion-Detection System for MANETs” IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013

[3] Yi Ping, Jiang Xinghao, Wu Yue & Liu Ning, Distributed intrusion detection for mobile ad hoc networks, Journal of Systems Engineering and Electronics Vol. 19, No. 4, 2008, pp.851–859.

[4] S. Zhong, J. Chen, and Y. R. Yang, .Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks,. In Proc. of Infocom'03, San Francisco, CA, USA, March 30 - April 3 2003.

[5] D.B. Johnson; D.A. Maltz; J. Broch; “DSR: The dynamic source routing protocol for multiple wireless ad hoc networks”. In: Perkins C, Ed, Ad Hoc Networking. Addison-Wesley, 2001. 139-172

[6] J.W. Cai; P. Yi, Y. Tian, Y.K. Zhou, N. Liu, The Simulation and Comparison of Routing Attacks on DSR Protocol[C], WiCOM 2009, in press.

[7] B. Sun; Y. Guan; J. Chen; U.W. Pooch, Detecting Black-hole Attack in Mobile Ad Hoc Networks[C]; 5th European Personal Mobile Communications Conference, 2003, 490-495.

[8] A. Patcha; A. Mishra; Collaborative security architecture for black hole attack prevention in mobile ad hoc networks[C]; Radio and Wireless Conference, 2003, 75-78.

[9] X.P. Gao; W. Chen; A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks[C]; IFIP International Conference on Network and Parallel Computing Workshops, 2007, 209-214.

[10] D. Boneh; C. Gentry; B. Lynn; H. Shacham. “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps”. Advances in Cryptology-EUROCRYPT’03: LNCS 2656. Berlin: Springer-Veralg, 2003. 416-432.

[11] D.M. Shila; T. Anjali; Defending selective forwarding attacks in WMNs, IEEE International Conference on Electro/Information Technology, 2008, 96-101.

[12] I.F. Akyildiz; X. Wang (2005). A Survey on Wireless Mesh Networks[J]. IEEE Communications Magazine , 43 (9), 23-30.

[13] D.S.J.D. Couto; D. Aguayo; J. Bicket; R. Morris, “A High-Throughput Path Metric for Multi-Hop Wireless routing,” in ACM Mobicom, 2003.

[14] K. Fall; K. Varadhan, NS notes and documentation, The VINT Project, UC Berkely, LBL, USC/ISI, and Xerox PARC, 1997.

[15] J. Broch; D. A. Maltz; D. B. Johnson; Y. C. Hu; J. Jetcheva. "A performance comparison of multi-hop wireless ad hoc network routing protocols." Proc. ACM Mobicom, 1998

[16] M. Just; E. Kranakis; T. Wan. “Resisting Malicious Packet Dropping In Wireless Ad Hoc Networks.” In Proc. ADHOC-NOW, Oct. 2003

