International Conference on New Era in Technologies, Science and Role of Management
Parvatibai Genba Moze College of Engineering, Wagholi, Pune NETSRM-18
9th-10th April 2018 www.conferenceworld.in ISBN: 978-93-87793-13-2

COMPARATIVE STUDY OF MANET UNDER NORMAL & SINKHOLE ATTACK

[1]Nikita Anil Deshmukh, [2] Prof.K.T.Jadhao

[1] M.E (EXTC) Sem - IV, ARMIET, Sapgaon,Thane.Dist.,M.H.

[2]M.E (EXTC), ARMIET, Sapgaon,Thane.Dist.,M.H.

ABSTRACT

Wireless ad hoc network are more vulnerable to the security attacks. The nature and structure of wireless ad hoc network makes it very attractive to attackers, because there is no fixed infrastructure and administrative approach in it. “Sinkhole attack” is one of the severe attacks in this type of network; this makes trustable nodes to malicious nodes that result in loss of secure information. This focuses on sinkhole attacks on routing protocols such as DSR, AODV. To overcome the problems occur due to sinkhole we discuss About Security-aware routing (SAR) which helps to reduce the impact of such attack. Due to security vulnerabilities of the routing protocols, however, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. In this paper we discuss the behaviour of DSR protocol under normal and sinkhole attack by analysing different parameters.

Keywords: AODV, DSR, IDS, MANET, PDR, SAR

1 INTRODUCTION

Mobile Ad-hoc Network (MANET) is a kind of wireless network which has no infrastructure and is a self configuring wireless network of mobile nodes, each node on the MANET will act like a router which forwards the packets. Due to these properties MANET is vulnerable to attacks. Mobile ad hoc networks are open to a wide range of attacks due to their unique characteristics like open medium, dynamically changing topology, absence of infrastructure, resource constraint (memory, bandwidth, computation power etc.) and trust among nodes. an ad hoc node in MANET operates as not only end terminal but also as an intermediate router. Data packets sent by a source node may be reached to destination node via a number of intermediate nodes. Thus, multi-hop scenario occurs. . In the absence of a security mechanism, it is easy for an attacker to insert, intercept or modify the messages.

This means that unprotected MANETs are vulnerable to many attacks such as wormhole attack, black hole attack including node impersonation, message injection, loss of confidentiality etc. Another issue in mobile ad hoc networks is that the nodes are resource constraint. Nodes are totally dependent on battery power and have limited memory and bandwidth. Therefore, security requirements such as authentication, integrity, availability, confidentiality, and non-reputation should be guaranteed during the communication between source and destination. Ad hoc network might consist of several home-computing devices, including laptops, cellular phones, and so on. Each node will be able to communicate directly with any other node that resides within its transmission range. For communication nodes are reley on other nodes.

II ANALYSIS DEFINITIONS

2.1 PDR: Packet Delivery Ratio (PDR): is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic sink. It measures the loss rate as seen by transport protocols and as such, it characterizes both the correctness and efficiency of ad hoc routing protocols. A high packet delivery ratio is desired in any network.

2.2 End To End Delay: The packet End-to-End delay is the average time that a packet takes to traverse the network. This is the time from the generation of the packet in the sender up to its reception at the destination's application layer and it is measured in seconds. It therefore includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities and MAC control exchanges.

2.3 DSR Overhead:

Routing Overhead is the number of routing packets required for network communication. Routing Overhead is calculated using awk script which processes the trace file and produces the result.

2.4 Throughput: It is the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet. When comparing the routing throughput by each of the protocols, DSR has the high throughput. It measures of effectiveness of a routing protocol.

III IMPLEMENTATION STRATEGIES

Implementation Strategy: Implementation Strategy is summarized as follow:

The DSR protocol uses the a) RREQ message to send request and uses the b) RREP message to reply, then when it has a valid route c) sends data to desired destination. In case of an error accurse d) RERR message will be sent. The arrows in a), b) and d) describe the sending of routing packets and their complexity related to the overhead on the network.

a) RREQ: Node [A] propagates a route request to Node [G]

Node [A] wants to send data to destination node [G], but it has no route yet! So it starts a route request discovery. Additionally, I assume that all intermediate nodes have no valid route - in their route cache table - to destination node [G]. Blue arrow represents the actual broadcast of RREQ packet, black arrow represents the old process of RREQ broadcast.

Step 1

Figure 3.1 DSR RREQ propagation In step 1, node [A] broadcasts a RREQ packet (blue arrow) to destination node [G] and appends its own address in the route record field on the packet header. The RREQ packet is received by all nodes within the transmission range of the initiator node (node [A]). The RREQ packets arrive at node[C] and node [B].

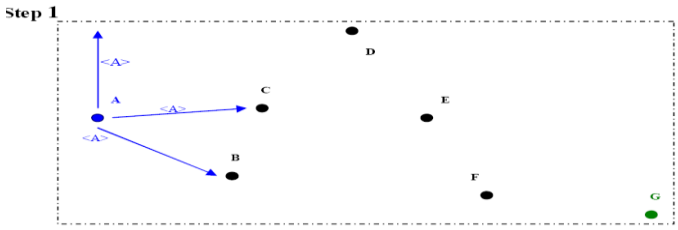


Fig 3.1 DSR RREQ propagation step

In step 1, node [A] broadcasts a RREQ packet (blue arrow) to destination node [G] and appends its own address in the route record field on the packet header. The RREQ packet is received by all nodes within the transmission range of the initiator node. The RREQ packets arrive at node[C] and node [B].

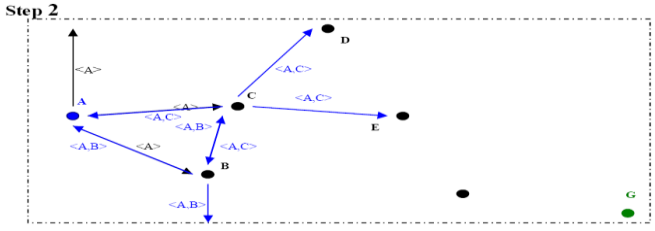


Fig 3.2 DSR RREQ propagation step2

In step 2, node [C] and node [B] rebroadcast the RREQ packet and appends their own addresses in the route record field. RREQ packet is received by all nodes within the transmission range of node [B] and node [C]. The RREQ packets from node [B] arrive at nodes [A and C] and from node [C] is received by nodes [A, B, D and E]. Node [A] ignores these RREQ packets, as it is the initiator of the packet respectively it finds its own address in the route record field. Node [B] and node [C] ignore the RREQ packets from each other as well. These RREQs have been already processed (i.e. old RREQ). Nodes [D and E] received the RREQ packet from node [C].

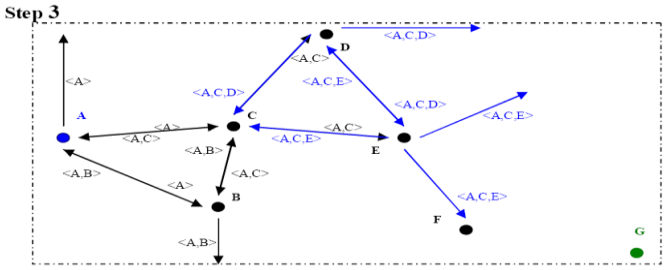


Fig 3.3 DSR RREQ propagation step3

The step 3 the RREQ packet is rebroadcast by node [D] and node [E] after they have appended their own address in the route record field. Duplicate and old RREQ packets are ignored by nodes [C, D and E]. Node [F] receives the RREQ packet from node [E].

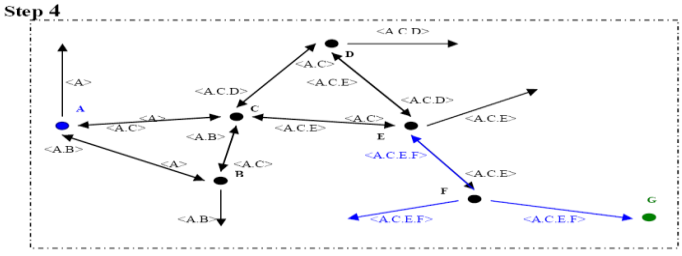


Fig 3.4 DSR RREQ propagation step4

In step 4, node [F] appends its own address in the route record field and rebroadcasts the RREQ packet. Node [E] ignored this RREQ packet from node [F] as it is an old one. Node [G] receives the RREQ packet from node [F].

Now, the RREQ packet arrives at the destination node [G]. Then node [G] replies with a RREP packet to the initiator node [A]. The RREQ packet arrives its destination via nodes [C, E and F]

b) RREP: Node [G] sends a route reply to Node [A]

I assume that destination node [G] has no other route in its route cache table. It sends the RREP packet via the reverse path as an unicast packet.

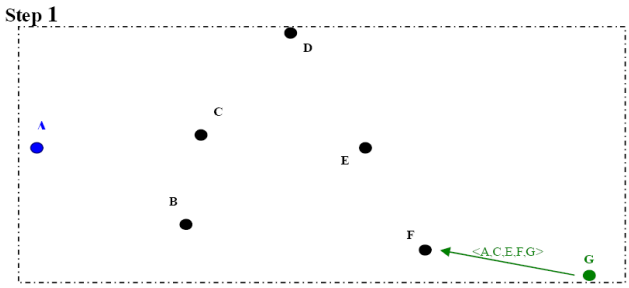


Fig 3.5 DSR RREP step1

In step 1, the node [G] sends the RREP packet to the node [F]. RREP packet includes the traversed path by RREQ packets.

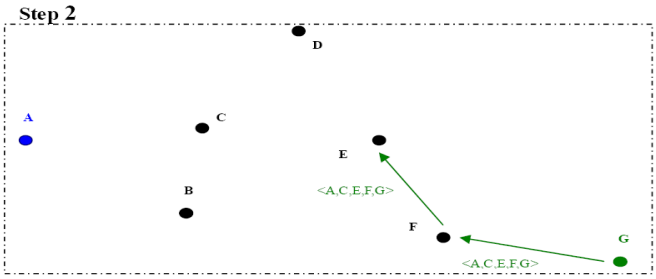


Fig 3.6 DSR RREP step2

In step 2, node [F] checks if it the destination for this RREP packet. Otherwise, it forwards the RREP to the next hop on the source route field (i.e. node [E]).

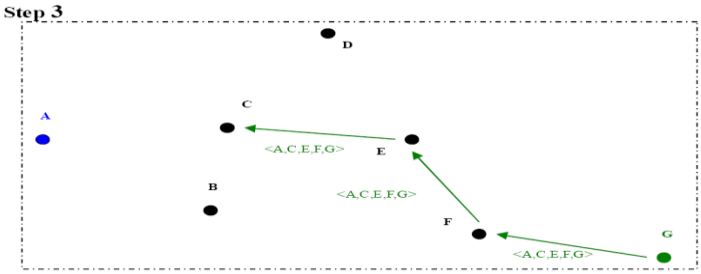


Fig 3.7 DSR RREP step3

In step 3, it is similar to step 2. Node [E] forwards the packet to node [C].

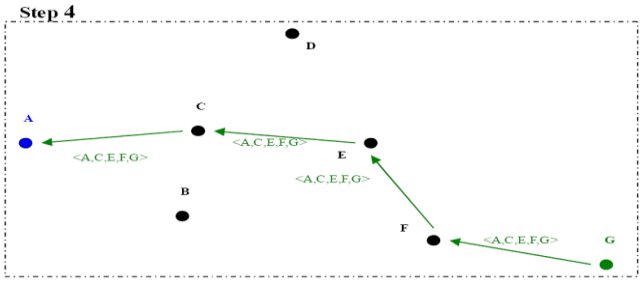


Fig 3.8 DSR RREP step 4

In step 4, the packets are processed as in step 2. Node [C] forwards the RREP packet to next node [A]. Whenever a node receives a RREQ or RREP packet, it adds all usable routing information from the packet in its route cache table.

Now, node [A] has a valid route to node [G] via: A □ C □ E □ F □ G, and can start to transmit its data packets.

c) Send data: node[A] sends data to node[G]

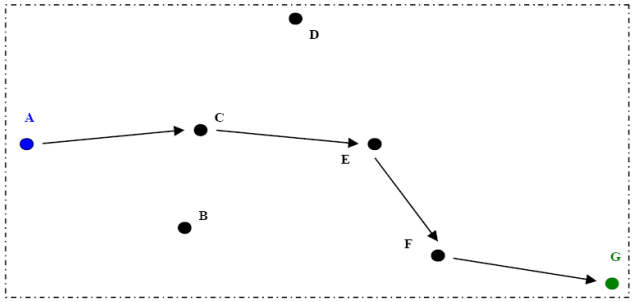


Fig 3.9 DSR send data

Whenever a node receives a data packet, it acknowledges the reception by sending an ACK to the source (previous) node. I assume that "at least" one of the nodes over this discovered path has moved out of the transmitting range of its previous node, during an active session. Now, I have a broken link between these two nodes. In such case, the previous node will send back a RERR packet to the source (initiator) node as unicast packet.

d) RERR: link between node [E] and node [F] is broken

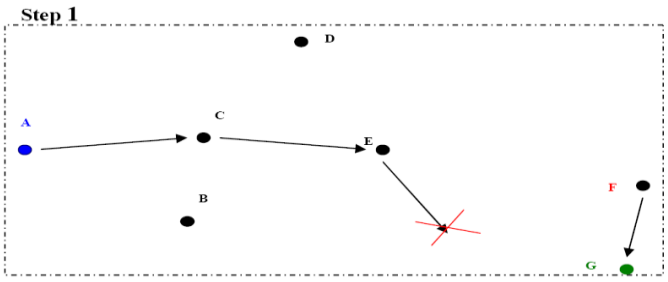


Fig 3.10 DSR link broken

In step 1, node [F] moves out of the transition range of node [E]. So, if node [E] forwards a data packet to node [F], it does not receive any ACK message. After some tries, it considers this link as a broken link and node [F] no more reachable through this path.

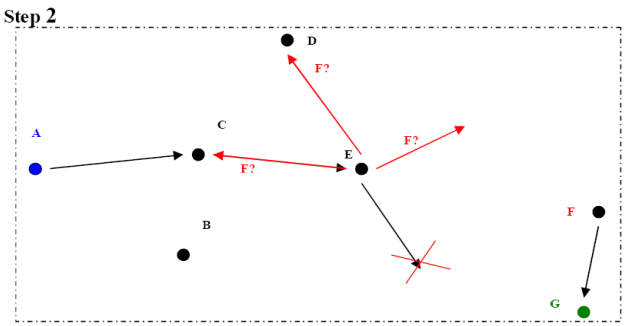


Fig. 3.11 DSR RERR

In step 2, node [E] generates an RERR, puts the previous node [C] as next hop and sends it back to the source node [A] as an unicast packet.

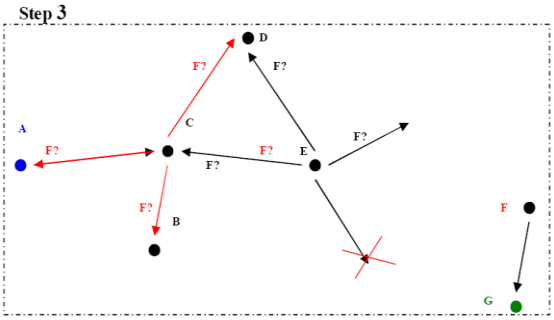


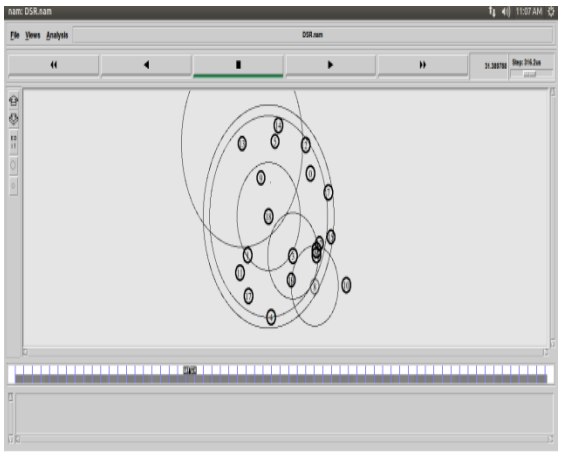
Fig 3.12 DSR RERR

In step 3, node [C] forwards the RERR to node [A]. Then, node [A] updates its route table, and if the session is still active and if there is another valid route to destination in its route table, node [A] uses this route, otherwise it starts a new route discovery process. If the nodes [D and B] receive the RERR packet, they update their route cache table, but they do not forward the packet, insofar it does not address them. Whenever a node receives an RERR packet, it deletes all route entries in its route cache table, which includes this broken link.

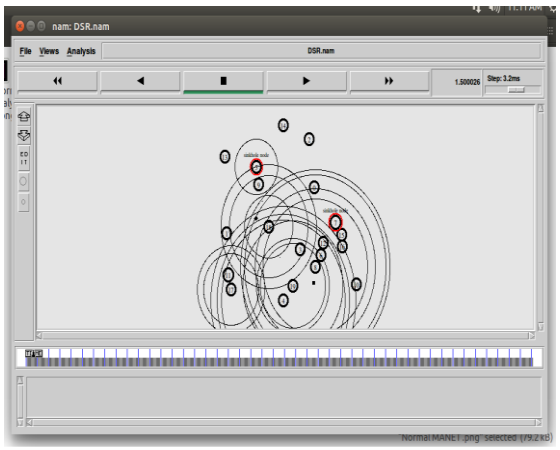
IV RESULTS

Simulation Parameters For DSR

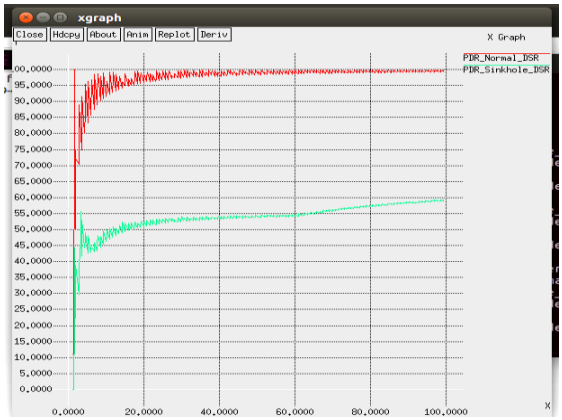
Simulator Ns-2 (Version 2.32)
Simulation Time 100 (s)
Number of mobile nodes 20
Topology 700 * 700 (m)
Routing Protocol DSR
Traffic CBR (constant bit rate)
Pause Time 10ms
Max Speed 0,1,2,3,4



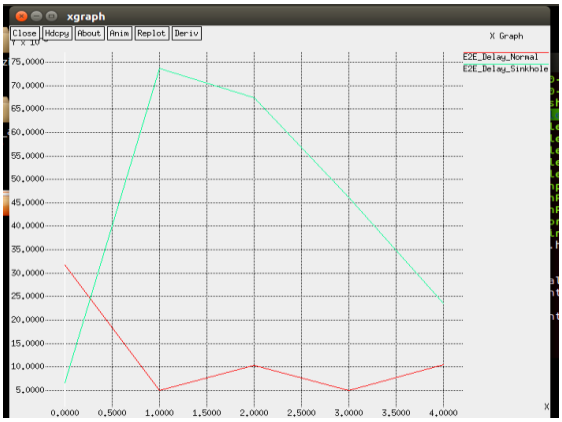
4.1 MANET Normal DSR



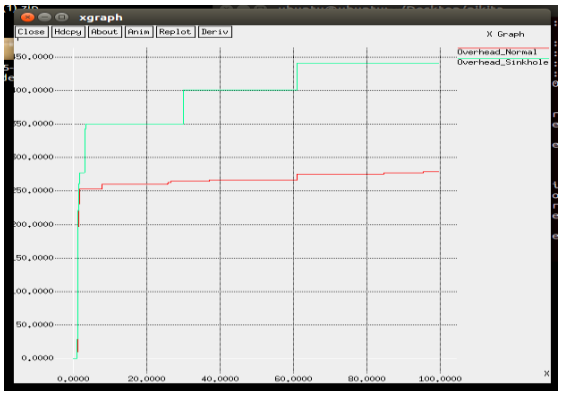
4.2 MANET with Sinkhole DSR



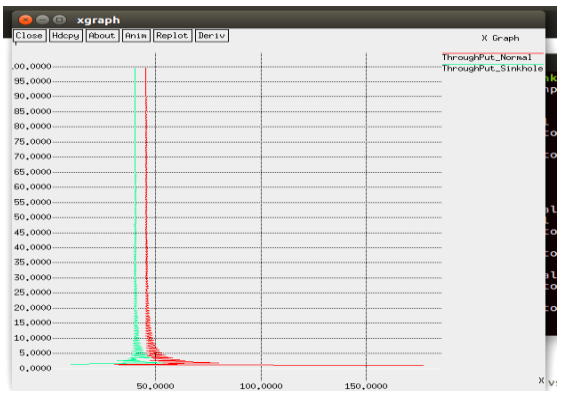
4.3 PDR Normal vs PDR Sinkhole



4.4 E2E Delay Normal vs E2E Dealy Sinkhole



4.5 DSR Overhead normal vs sinkhole Sinkhole



4.6 ThroughPut Normal vs ThroughPut

V CONCLUSION

According to post process simulation result we compare the effect on mobile adhoc network under normal and sinkhole attack with DSR protocol. And conclude that as per the comparison the performance of the MANET is degraded.

Parameter	Protocol	With Normal Condition	With Sinkhole Attack
Packet Delivery Ratio (PDR	DSR	High	Low
End To End Delay	DSR	Low	High
DSR Overhead:	DSR	Low	High
Throughput	DSR	High	Low

REFERENCES

[1] Shubh Lakshmi Agrwal The ICFAI University, Jaipur, India "Analysis of detection algorithm of Sinkhole attack & QoS on AODV for MANET" Next Generation Computing Technologies (NGCT), Pages: 839 - 842 ,Date Added to IEEE Xplore: 16 March 2017.

[2]Neelu Kumari "New Performance Analysis of AODV, DSDV and OLSR Routing Protocol for MANET",Page(s)33-38 978-9-3805-4421-2/16/$31.00_c2016 IEEE, 2016 International Conference on Computing for Sustainable Global Development (INDIA Com)

[3] Mohamed Guerroumi Dept. of Electron. & Comput. Sci., Univ. of USTHB Algiers, Algiers, Algeria "Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink" Information Technology - New Generations (ITNG), 2015 12th International Conference, Year: 2015, Page(s):307 - 313 Date Added to IEEE Xplore: 01 June 2015

[4] Aayushi Bhatiya "Detection And Prevention Of Sink Hole Attack In Aodv Protocol For Wireless Sensor Network" International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue: 05 May -2017

[5]David B. Johnson, David A. Maltz, and Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks," In Ad Hoc Networking, edited by Charles E. Perkins, chapter 5, pages 139-172, Addison-Wesley, 2001.

[6] Charles E. Perkins and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector Routing," Proceeding of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), New Orleans, LA, USA, February 1999, pages 90-100.

[7] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Communications Magazine, October 2002, pages 70-75.

[8]Douglas S. J. De Couto, Daniel Aguayo, John Bicket and Robert Morris, "A High-Throughput Path Metric for Multi-Hop Wireless Routing," in Proceedings of the Ninth Annual International Conference on Mobile Computing and Networking (MobiCom '03), San Diego, California, September 2003.

[8] NS-2 Network Simulator, http://www.isi.edu/nsnam/ns/.

[9] Benjamin J. Culpepper and H. Chris Tseng, "Sinkhole Attack Detection in DSR MANETs: A Fuzzy Logic Approach," Technical Report No.200303, Computational Intelligence Lab., SJSU, 2003.

[10] Yong guang Zhang and Wenke Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," In 6th International Conference on Mobile Computing and Networking (MOBICOM'00), pp275-283, June 2000.

[11] Elizabeth M. Royer and Chai KeongToh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," In IEEE Personal Communications, Volume 6, pp46-55, April 1999.

[12] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," In Proceedings of Mobicom2000, Boston, August 2000.

[13] Sonali Bhargava and Dharma P. Agrawal, "Security Enhancements in AODV protocol for Wireless Ad Hoc Networks," In Proceedings of Vehicular Technology Conference, 2001.

[14]S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad hoc Routing forWireless Networks," In the 2nd ACM Symposium on Mobile Ad HocNetworking& Computing (MobiHoc'01), 2001.