Impact J. Sci. Tech., Vol. 14, No. 1, 37 - 50, 2020
ISSN - 0973-8290

SIMULATION STUDY FOR DETECTION AND REMOVAL OF COOPERATIVE BLACK HOLE ATTACK IN AODV IN MANET

Rupali Goyal[1], Pinaki A. Ghosh[2]

doi:10.46598/impactjst.14.1.2020.293

URL:https://doi.org/10.46598.14.1.2020.293

Abstract

A mobile ad hoc network (MANET) is an autonomous network consisting of mobile nodes communicating with each other over wireless links. In the absence of a fixed infrastructure, nodes cooperate to provide the necessary network functionality. Routing protocol used in Ad hoc networks is AODV (Ad hoc on demand Distance Vector) protocol. The AODV protocol is prone to an attack called 'Black Hole' attack. Black Hole Attacks has become a serious threat to communication in MANETs.

In a black hole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. The malicious node deprives the traffic from the source node. When these malicious nodes work together as a group the damage is very serious. This type of attack is called cooperative black hole attack [16]. It is proposed to wait

[1]Bansal Institute of Science & Technology, BHOPAL (M.P.),INDIA.

[2]Deptt of CSE, Bansal Institute of Science & Technology, BHOPAL (M.P.), INDIA.

and check the replies from all the neighboring nodes to find a safe route. The Objective of this paper is to provide a simulation study illustrating the effects of cooperative Black hole attack. The Simulation environment is Qualnet Simulator from Scalable networks.

Keywords: Mobile ad hoc network, AODV, Cooperative Black Hole Attack, Qualnet Simulator

1. Introduction

Wireless networks can be basically either infrastructure based networks or infrastructure less networks. The infrastructure based networks uses fixed base stations, which are responsible for coordinating communication between the mobile hosts (nodes) [6]. Mobile ad hoc network (MANET) is a collection of mobile hosts without the required intervention of any existing infrastructure or centralized access point such as a base station [5]. In addition to freedom of mobility, a MANET can be constructed quickly at a low cost, as it does not rely on existing network infrastructure. Due to this flexibility, a MANET is attractive for applications such as disaster relief, emergency operations, military service, maritime communications, vehicle networks, casual meetings, campus networks, robot networks, and so on [2].

The Routing protocols can be divided into proactive, reactive protocols, depending on the routing topology. Proactive protocols are typically table-driven. Examples of this type include Destination Sequence Distance Vector (DSDV). Reactive or source-initiated on-demand protocols, in contrary, do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type includes Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV) [6].

Security is a major concern in all forms of communication networks, but due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks. Black hole attack is one of many possible attacks in MANET. In this attack, a malicious node

sends a forged Route Reply (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node [5].

2. Routing Protocols in MANET

The goal of routing in a MANET is to discover the most recent topology of a continuously changing network to find a correct route to a specific node. Routing protocols in a MANET can be classified into two categories: reactive routing protocols (e.g., AODV) and proactive routing protocols (e.g., OLSR). In reactive routing protocols, nodes find routes only when they must send data to the destination node whose route is unknown. On the other hand, in proactive Protocols, nodes periodically exchange topology information, and hence nodes can obtain route information any time they must send data. We describe two standard routing protocols that currently are being researched actively, that is, AODV and OLSR [2].

AODV:

AODV is a reactive routing protocol designed for a mobile ad hoc network. In AODV, when a source node S wants to send a data packet to a destination node D and does not have a route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination node. Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. The same RREQ that arrives later will be ignored by the destination node. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node [2].

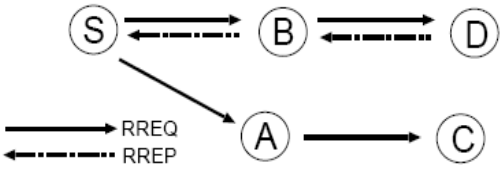


Figure 1: Route discovery process

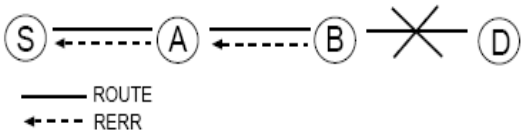


Figure 2: Transferring route error messages

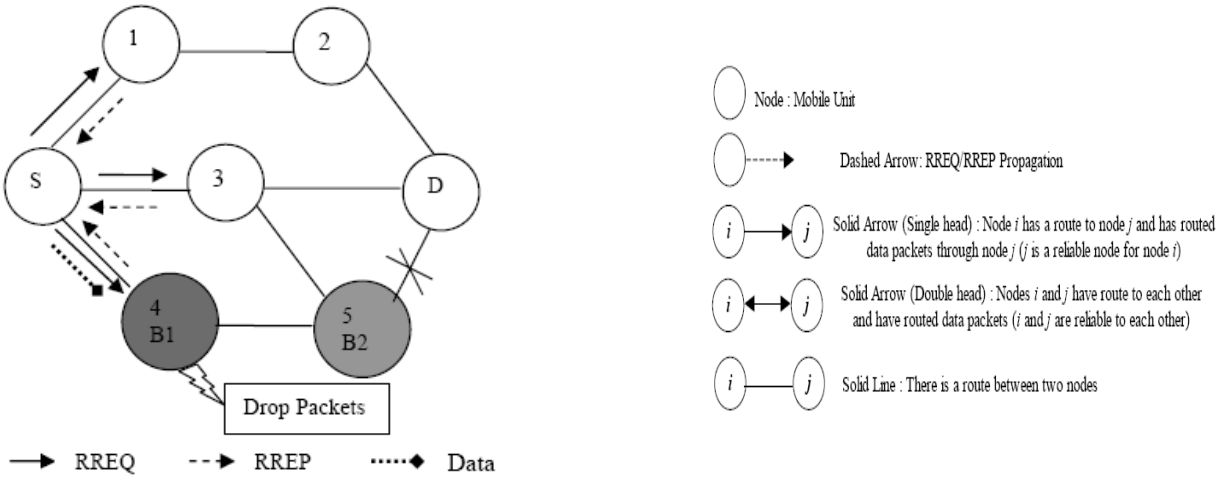
OLSR:

OLSR is a proactive routing protocol, that is, it is based on periodic exchange of topology information. The key concept of OLSR is the use of multipoint relay (MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required. In OLSR, each node selects its own MPR from its neighbors. Each MPR node maintains the list of nodes that were selected as an MPR; this list is called an MPR selector list. Only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs [2].

3. Black Hole Attack

In MANETs, every node participates in the routing process. Hence, it is possible for attackers to launch attacks against the routing protocol by sending false routing information. By sending false routing information, an attacker may try to dispose other nodes to make it a part of their routes. This is often referred to as 'route attraction'. If an attacker succeeds in attracting routes, he may perform several attacks, including-

- **Eavesdropping messages,**
- **Selectively dropping data,**
- **manipulating data, or**
- **launching a denial-of-service (DoS) attack [3].**



A black hole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets. We define the following conventions for protocol representation [17]

According to the original AODV protocol, when source node S wants to communicate with the destination node D, the source node S broadcasts the route request (RREQ) packet. The neighboring active nodes update their routing table with an entry for the source node S, and check if it is the destination node or has a fresh enough route to the destination node. If not, the intermediate node updates the RREQ (increasing the hop count) and floods the network with the RREQ to the destination node D until it reaches node D or any other intermediate node which has a fresh enough route to D, as depicted by example in Figure 4.

The destination node D or the intermediate node with a fresh enough route to D, initiates a route response (RREP) in the reverse direction, as depicted in Figure 5. Node S starts sending data packets to the neighboring node which responded first, and discards the other responses. This works fine when the network has no malicious nodes [17].

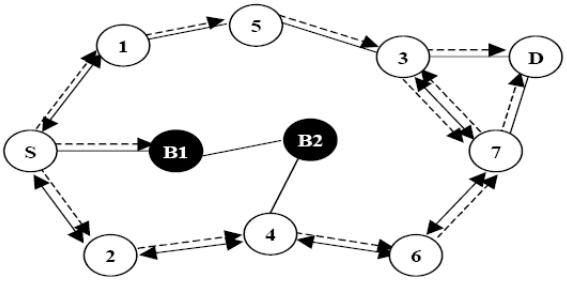


Figure 5: Network Flooding of RREQ messages

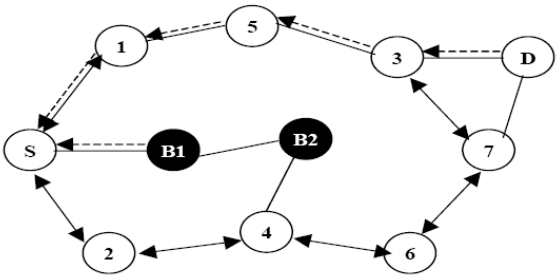


Figure 6: Propagation of RREP messages

When multiple black hole nodes are acting in coordination with each other, the first black hole node B1 refers to one of its teammates B2 as the next hop, as depicted in Figure 5. According to [3], the source node S sends a "Further Request (FRq)" to B2 through a different route (S-2-4-B2) other than via B1. Node S asks B2 if it has a route to node B1 and a route to destination node D. Because B2 is cooperating with B1, its "Further Reply (FRp)" will be "yes" to both the questions. Now per the solution proposed in [3], node S starts passing the data packets assuming that the route S-B1-B2 is secure. However, in reality, the packets are consumed by node B1 and the security of the network is compromised [17].

4. Proposed Algorithm

4.1 Algorithm for Detecting Black Hole

1. Action performed by Source Node S

Step 1: Divides the data packets to be sent in k equal parts. DATA [1, ..., K]. Initialize i=1.

Step 2: Send prelude message to the destination node D containing the no of data packets to be sent in current block.

Step 3: Broadcast monitor message to all its neighbors instructing neighbors to monitor next node in the route.

Step 4: Start transmitting data packets from the block DATA[i] to D.

Step 5: Sets timeout for the receipt of the postlude message containing no. of data packets received by D.

Step 6: If timeout is not expired and postlude message received, and no. of data packets received by D is equal to the no. of data packets sent by S then go to Step 7. Else Start Black hole removal process.

Step 7: Continues from Step 2 when i less than or equal to k.

Step 8: Terminates S's action.

2. Action performed by Destination Node D

Step 1 On receiving prelude message from S, extracts no. of data packets sent by S and Initialize no. of data packets received by D = 0.

Step 2: Sets timeout for the receipt of the current data sample and waits for the data packets.

Step 3: When Timeout is not expired and a data packet received, Increment no. of data packets received by 1.

Step 4: When Timeout expires, it sends postlude message to S containing the no. of data packets received by D.

Step 5: Terminates D's action.

3. Action performed by neighbors on receiving monitor message

Step 1 On receiving monitor message nodes extracts the id of the next node in the route from S to D.

Step 2: If the receiving node is neighbor of next node in the route then,

Step 2.1: Start monitoring the action of the node.

Step 2.2: Initialize to Count the no. of Data packets forwarded by the node.

Step 2.3: Find next node id to which it is forwarding the data packets.

Step 2.4: Start counting data packets.

Step 2.5.: If next node is not destination node D then

Step 2.5.1: Broadcast monitor message to all its neighbors containing the id of the next node.

Step 3: Else Rebroadcast monitor message to all its neighbors.

Step 4: Terminates its action.

4.2 Black Hole Removal process

1. Action performed by Source Node S

Step 1: Broadcasts query message to all its neighbors containing the id of the node sending route reply message to S.

Step 2: Sets timeout for the receipt of the result message from the monitoring node.

Step 3: When timeout is not expired and result message received or "The node is Malicious" message received then the node sending the route reply is added in the findMalicious Table.

Step 3.1 If node already exists in FindMalicious table

Step 3.1.1: Then increment voteCount for node sending route reply by 1.

Step 3.1.2: If votecount >= predefinedCount

Step 3.1.2.1: Remove node from FindMalicious table and append Node in BlackHole table.

Step 3.1.2.2: Broadcast "*The node is Malicious*" to the Network.

Step 3.1.2.3: Set findHoleStatus = true for that route in the routing table of S for the route to D.

Step 3.2: Else

Step3.2.1: Append Node in FindMalicious table.

Step 3.2.2: Initialize voteCount = 1 and Initialize j = 1.

Step 4: When j <= length of FindMalicious table

Step 4.1: Broadcast (vote request) VREQ message to the network requesting other nodes in the network to vote for node in findMalicious table if it is malicious.

Step 4.2: Sets timeout for the reply from the network VREP (vote reply) message containing the id of regular node.

Step 4.3: When timeout for vote reply not expired and VREP message received then

Step 4.3.1: increment voteCount for node in findMalicious table by 1.

Step 4.4: If voteCount >= PredefinedCount

Step 4.4.1: Remove Node from FindMalicious table and append that Node in BlackHole table.

Step 4.4.2: Broadcast "The node is Malicious" to the Network.

Step 4.4.3: Set findHoleStatus = true for that route in the routing table of S for the route to D.

Step 4.5: Increment j by 1.

Step 6: If findHoleStatus is True

Step 6.1: Terminate sending data. Find new route to D.

Step 7: Resume its normal action.

2. Action by Neighbors on receiving on receiving *query* message

Step 1: On receiving query message nodes extracts id of the node sending route reply message to D, S, D and no. of data packets sent to D.

Step 2: If the receiving node is neighbor of node sending route reply then,

Step 2.1: If no. of data packets forwarded by monitor node is equal to the no. of data packets sent.

Step 2.1.1: when Next node is not D

Step 2.1.1.1: Broadcast query message to all its neighbors replacing Node sending route reply by Next node to which monitor node is forwarding.

Step 2.2: Else

Step 2.2.1: If Next node to which the monitor node is forwarding the data packets is equal to NULL then Next node itself is dropping all the packets.

Step 2.2.1.1: Reply "The node sending route reply is Malicious" to S.

Step 2.2.2: Else

Step 2.2.2.1: Reply result message to S, which means node sending route reply, may be malicious.

Step 2.2.2.2: Broadcast query message to all its neighbors replacing Node sending route reply by next node and no. of data packets sent to next node by no. of data packets Count of the monitoring node.

Step 3: If the receiving node is not neighbor of Node sending route reply then broadcast query message to all its neighbors.

Step 4: Terminates its action.

3. Action by any regular nodes on receiving on VREQ message

Step 1 On receiving VREQ message nodes extracts id of the node.

Step 2: If Node exists in BlackHole table.

Step2.1: Reply VREP to S.

Step 3: Terminates its action.

4. Action by any regular nodes on receiving on receiving "The node is Malicious"

Step 1 On receiving "The node is Malicious" all regular nodes in the network check BlackHole table.

Step 2: If Node sending route reply not exists in BlackHole table, then

Step 2.1: If Node sending route reply not exists in FindMalicious table.

Step 2.1.1: Append Node sending route reply in FindMalicious table.

Step 2.2.2: Initialize voteCount = 1.

Step 3: Terminates its action.

5. Simulation Environment

We have implemented Cooperative Black hole attack in a Qualnet simulator [18]. For our simulations, we use CBR (Constant Bit Rate) application, UDP/IP, IEEE 802.11b MAC and physical channel based on statistical propagation model. The simulated network consists of 30 randomly allocated wireless nodes in a 1500 by 1500 square meter flat space. The node transmission range is 250- meter power range. Random waypoint model is used for scenarios with node mobility. The selected pause time is 30s and selected simulation time is 180s. A traffic generator was developed to simulate constant bit rate (CBR) sources. The size of data payload is 512 bytes. In our scenario we take 30 nodes in which nodes 1-5, 7-12, 14-17, 19-20, 22-26 and 28-29 are simple nodes, and node 6, 13,18,21,27 and 30 are a malicious nodes or Black hole nodes.

6. Result Analysis

The simulation is done using Qualnet [18], to analyze the performance of the network by varying the nodes mobility. The metrics used to evaluate the performance are given below.

i). Packet Loss Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets dropped between CBR source and the CBR sink.

ii). Throughput: Throughput is the average rate of successful message delivery over a communication channel.

iii). Node Mobility: Node mobility indicates the mobility speed of nodes.

The Fig.9 shows the effect to the packet loss ratio measured for the AODV protocol when the node mobility is increased. The result shows comparison of the cases, with the cooperative black hole attack, without the black hole attack and the proposed scheme. When we applied proposed scheme it is observed that the packet loss ratio decreases when there are malicious nodes in the network.

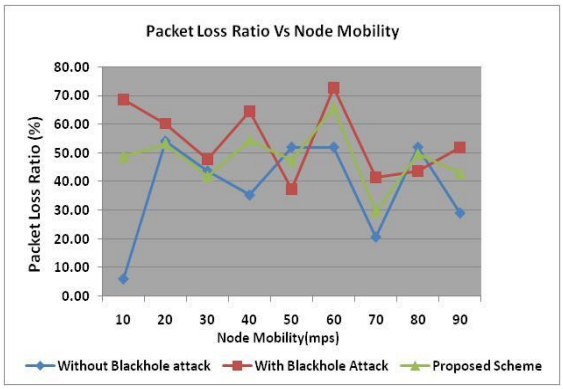


Fig. 9 Packet Loss Ratio Comparison

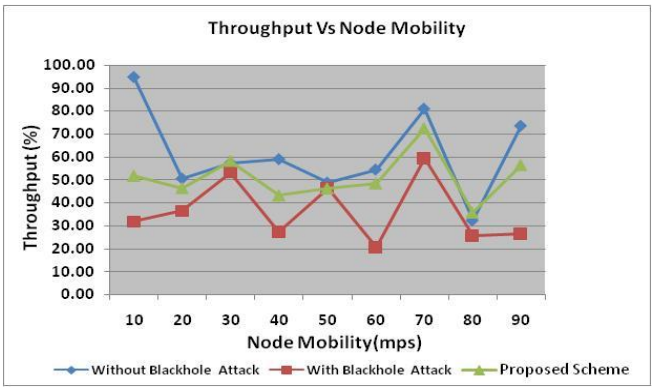


Fig. 10 Throughput Comparison

Same as the fig. 10 shows the impact of the cooperative Black hole attack to the Networks throughput .The throughput of the network increases when proposed scheme is applied when compared to with cooperative black hole attack. We vary the speed of the node and take the result to the different node speed.

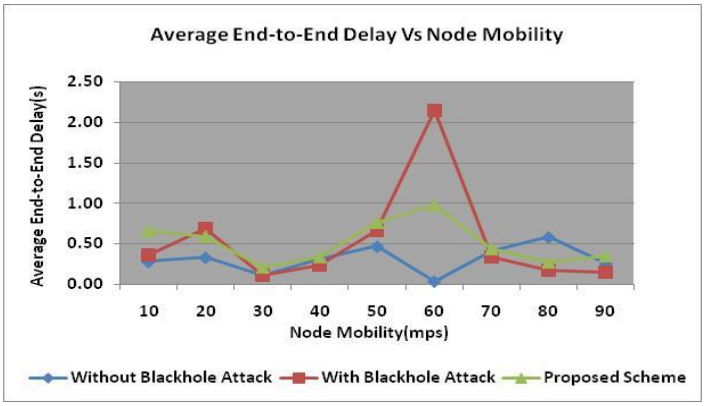


Fig. 11 Avg. End-to-End Delay Comparison

From the figure 11 it can be observed that, there is slight increase in the average end-to-end delay without the effect of black hole and the proposed scheme, as compared to the effect of cooperative black hole attack. This is due to the immediate reply from the malicious node i.e. the nature of malicious node here is it would not check its routing table.

7. Conclusion

Wireless Ad Hoc Networks are vulnerable to various attacks due to the physical characteristic of both the environment and the nodes. In this paper the effect of packet delivery ratio, Throughput, End-to-End Delay and Jitter has been detected with respect to the variable node mobility. There is reduction in Packet Delivery Ratio, Throughput, E-E Delay, and Jitter as shown in fig. 9-12. In cooperative Black hole attack all network traffics are redirected to some specific node or from the malicious nodes causing serious damage to networks and nodes as shown in the result of the simulation. The detection of Black holes in ad hoc networks is still considered to be a challenging task.

8. References

[1] Hoang Lan Nguyen, Uyen Trang Nguyen, A study of different types of attacks on multicast in mobile ad hoc networks in: Science Direct, Ad Hoc Networks 6 (2008) 32–46.

[2] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, A Survey Of Routing Attacks In Mobile Ad Hoc Networks, IEEE Wireless Communications, 1536-1284/07.

[3] Elmar Gerhards-Padilla, Nils Aschenbruck, Peter Martini, Marko Jahnke, Jens T¨olle, Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs, 32nd IEEE Conference on Local Computer Networks, 0742-1303/07.

[4] Benamar Kadri, Mohammed Feham and Abdallah M'hamed, Securing reactive routing protocols in MANETs using PKI (PKI-DSR), Security and Communication Networks, Security Comm. Networks, Published online in Wiley Inter Science, DOI: 10.1002/sec.63.

[5] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method, International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007 338.

[6] Latha Tamilselvan, Dr. V Sankaranarayanan, Prevention of Co-operative Black Hole Attack in MANET, Journal Of Networks, Vol. 3, NO. 5, MAY 2008.

[7] Bracha Hod, "Cooperative and Reliable Packet-Forwarding On top of AODV", www.cs.huji.ac.il/~dolev/pubs/reliable-aodv.pdf, 2005.

[8] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communications magazine, Vol.40, No.10, October 2002.

[9] S. Buchegger and J. Y. Le Boudec. A robust reputation system for mobile adhoc networks. Technical Report IC/2003/50, EPFL-DI-ICA, July 2003.

[10] S. Bansal and M. Baker. Observation-based cooperation enforcement in ad hoc networks, July 2003. Available on: http://arxiv.org/pdf/cs.NI/0307012.

[11] P. Michiardi and R. Molva. Preventing denial of service and selfishness in ad hoc networks. In Working Session on Security in Ad Hoc Networks, Lausanne, Switzerland, June 2002.

[12] P. Michiardi and R. Molva. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Proceedings of the 6th IFIP Communications and Multimedia Security Conference, pages 107–121, Portorosz, Slovenia, September 2002.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker Mitigating routing misbehavior in mobile ad hoc networks. In mobile Computing and Networking (MOBICOM), pages 255–265, 2000. Available on: citeseer.ist.psu.edu/marti00mitigating.html.

[14] S. Buchegger, C. Tissieres, and J. Y. Le Boudec. A testbed for misbehavior detection in mobile ad-hoc networks - how much can watchdogs really do. Technical Report IC/2003/72, EPFL-DI-ICA, November 2003. Available on:citeseer.ist.psu.edu/645200.html.

[15] Sheenu Sharma, Roopam Gupta Simulation Study Of Blackhole Attack in the Mobile Ad hoc Networks. International Conference on Network

Applications, Protocols and Services 2008, 21-22 November 2008, Executive Development Centre, Universiti Utara Malaysia

[16] Hesiri Weerasinghe and Huirong Fu, Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation. International Journal of Software Engineering and Its Applications, Vol. 2, No. 3, July 2008.

[17] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA.

[18] Scalable Network Technologies (SNT). Qualnet. http://www.qualnet.com/.

[19] Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad- hoc Networks", WCECS 2008, October 22-24, 2008, San Francisco, USA