Identifying, Avoidance and Performance Assessment of Black Hole Attack on AODV Protocol in MANET

Sonika Malik
Department of CSE, Manav Rachna International University
Faridabad, India

Indu Kashyap, Ph.D
Department of CSE, Manav Rachna International University
Faridabad, India

ABSTRACT
Composition of mobile devices communicating with each other deprived of any infrastructure is a Mobile Adhoc Network (MANET). A mobile node in MANET has dynamic topology and they may move expeditiously that means stability is very less. The intruders take advantage of such individualities of MANET to carry out different varieties of attacks. Out of all these attacks, black hole attack is the most severe one. The routing protocol used by a malicious node is to proclaim itself as having the shortest route to the target node. Black hole node discards all the packets that finally go through it. In this paper, we simulated the Black Hole Attack on AODV protocol using NS-2.34 simulator and compare the parameters like Packet Delivery Fraction, Network Overhead and Average throughput and also proposed a solution to prevent and figure out this black hole attack on AODV protocol.

General Terms
Sequence numbers in AODV protocol, Black Hole attack Prevention.

Keywords
MANET, AODV, Black Hole Attack, Security, NS-2.34

1. INTRODUCTION
MANETs (Mobile Ad-hoc Network) are composition of individual mobile devices without the need of any network infrastructure. In MANET nodes play dual role of host as well as router. Nodes can join and leave the network at any time. Basically the communication takes place in a decentralized manner i.e. without a centralized authority control, where each node independently passion the packets by evaluating the nearest proximity of next available node.
This type of wireless and infrastructure less network is useful in areas like battlefield, military and other emergency and calamity situations. In these areas, safety is a serious issue.
There are different routing protocols in MANET. When a mobile node wants to transfer data to a target node, it checks the present status of the neighbours because current routing information is unfamiliar or expired. According to information acquisition, the routing protocols can be categorized into proactive, reactive and hybrid routing.
The proactive routing is also entitled as table-driven routing protocol. In this routing protocol, mobile nodes from time to time send their routing information to the neighbours. The reactive routing is well-found with another designation named on-demand routing protocol. The hybrid routing protocol combines the benefits of proactive routing and reactive routing. AODV protocol is a reactive protocol. It is based on on-demand route discovery only when source wants to send data. It uses hop-by-hop routing, concept of sequence numbers and periodic beacons to check link with their neighbours.
Latest research in wireless specifies that the wireless MANET is presents larger security problems than the conventional wired and wireless networks. In MANET, all the signals go through the bandwidth-constrained links, which makes it more prone to physical security threats than fixed landline networks. As there is not any centralised control or support, authentication from public key cryptography and certification authorities may be difficult to accomplish in MANET.
In MANET, mobile nodes are portable and able to move independently in any direction. Therefore, any security solution with a static configuration would not be adequate for this. The in effect security solutions for wired networks cannot be applied directly in wireless MANETs.
We proposed a solution to prevent black hole attack in AODV protocol. In the proposed solution, we use a data routing table [1] to store the routing information of neighbour nodes. When initiator node gets replies from different nodes, it stores all the replies instead of forwarding data packets to the first replied node. It analyse the data routing table of the nodes and send check packet to the neighbour nodes of the replying nodes. Information about the neighbour nodes gets from the reply which source node receives. Source node initiates the process to examine the DRI table to detect suspected node. As we all know that in the routing process every node that comes in the path of source and destination has to take part in the routing process. Through data routing information table, source node detect which of the node did not take part in the communication process or did not interact with their neighbours to transmit packets will be treated as a suspicious node.
This DRI table is updated when any node received data packet from one of its neighbours or any node that sent data packets through one of its neighbours.

2. RELATED WORK
Researchers have proposed various techniques to prevent and detect black hole attack in MANET. Ankur, S.Sanjay et. al. [1] proposed a solution to detect, eliminate cooperative black hole nodes. They use the concept of DRI table in which one more field is added check bit that tells about the malicious node and it is updated only by source node. Local anomaly detection, finding trusted node to destination and generating alarm for malicious node are the techniques that the authors used in their paper [1]. Their solution is extended version of the solution in paper[2]. But the main drawback is they increase time delay and routing overhead too much. Storage space is also increased as one more field is added. When source node send probe message to the cooperative node (node that is active and take part in communication), there is

the chance that malicious node takes the probe message and reply on behalf of the cooperative nodes.

Mohammad Al-Shurman, Park et. al.[3] proposed two different approaches to solve the black hole attack. In the first solution the sender node needs to validate the truthfulness of the node that pledges the RREP packet by exploiting the redundancy of the network. The notion of this elucidation is to find more than one route for the target. The Source Node unicast the ping packet using dissimilar routes. The Intermediate Node or destination node or malicious node will ping requests. The Source Node checks the response and routes them to check which one is benign or having malicious node. In the intervening time the Source Node buffered its packet until it found the safe route. When the route is identified the buffered packets will be communicated to it. The second solution is to store the last sent packet sequence number and the last received packet sequence number in the table. It is updated when any packet is attained or conveyed. When node gets reply from another node it checks the last sent and received sequence number. If there is any discrepancy then an ALARM shows the presence of a black hole node. This method is faster and more trustworthy and has no overhead. According to the simulation done by authors, the solutions had less requests and reply than a normal AODV protocol. As sequence numbers are used in second solution, it is better than first one. The message overhead can be eradicated by this solution because of the inward bound cryptography method. Main disadvantage is that none of the solution can detect cooperative black hole attacks and increase in time delay, since source node has to wait for other route replies.

Hongmei Deng, Wei Li and Dharma P. Agarwal [8], proposed two solutions to the black hole problem. First solution is to confine the ability of an intermediate node to reply in a message, so all reply should be lead out only by the destination node. Using this method the intermediate node cannot reply. Disadvantage of these solutions is increased time delay of message and malicious node can fabricate a reply message on behalf of destination node.

Another solution proposed by Hongmei Deng, Wei Li and Dharma P. Agarwal, is to use one more route to the intermediate node to check whether the route from the intermediate node to the destination node exists or not. If it exists, they can trust the intermediate node and send out the data packets. If not, just discard the reply message from the intermediate node and send out alarm message to the network and segregate the node from the network.

Disadvantage of this solution is time delay and it did not prevent cooperative black hole attack.

Djenouri D [13] proposed a solution in which three phases- Monitor, Detect and Remove are performed to remove the black hole attack. In the monitor phase, an well-organized procedure of random two-hop acknowledgement is used. The aim of this methodology is to deliberate and dodge false allegation attacks vulnerability, as well as diminishing false positives that might be caused by nodes movement. This solution detects black hole attack node whenever it drops packets.

Collaborate black hole attack is difficult to prevent using this method.

3. BLACK HOLE ATTACK PROBLEM IN AODV PROTOCOL

AODV protocol is a significant reactive protocol that generates path only when demanded by the source node. When a node wants to transmit data packets, it requires a route to the destination, for this it initiate a route discovery process with in the network. It broadcast a route request (RREQ) message in the network. It sends this RREQ message to its neighbours, which then forwards the message to their neighbours, and so on, until destination node is not found. In this process the intermediate node can reply to the RREQ packet only if it has a fresh route to the destination. Once the RREQ reaches the target node or an intermediate node, the target node (destination) responds by unicasting the route reply (RREP) packet.

According to the AODV protocol, any intermediate node gives reply to the RREQ message, only if it has fresh route, and that is checked by the sequence number of destination contained in the RREQ packet. The malicious node easily disrupts the routing process.

Fig. 1 shows how black hole attack happen, here node "S" wants to communicate with node "D" and send data packets to "D". For this, it initiate route discovery process. Here "M" is a malicious node, it will claim that it has active and shortest route to the indicated destination as soon as it receives RREQ packets. It will send its reply to node "S" with highest sequence number. When reply reaches to node "S", it thinks that route discovery process is complete. Node "S" will disregard all other replies that came after the malicious node reply and then it will start routing data packets to node "M". Malicious node "M" drop all the packets, due to which the packet loss increased and destination node never knows get packet and source node never get to know about this. The malicious node formed a black hole in the network, and it is called black hole problem.

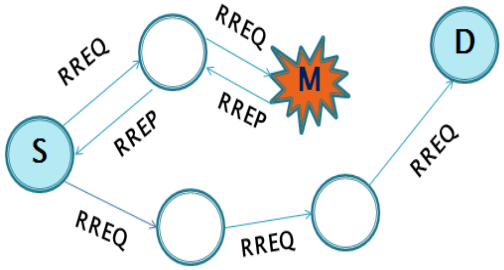

Figure 1: Black Hole Attack

4. OTHER ATTACKS ON MANET

4.1 Flooding attack

The flooding attack aims to exhaust the network resources like bandwidth and resources of node, such as battery and computational power or to interrupt the routing process to cause extreme degradation of performance of network. For instance, a malicious node can send multiple numbers of Route Requests (RREQs) in a short span of time to a hypothetical destination node which does not exist in the network. The network will be flooded with the RREQs sent by the malicious node as no node reply to route requests. This, results in draining of battery power of nodes and consuming bandwidth of the network. It could lead to the DoS attack.

4.2 Routing Loop

In this attack, attacker creates fake/ forged routing packets to consume both bandwidth and power on the network. This type of attack can be considered a type of denial of service attack. By sending packets that did not have any destination, attacker can create a routing loop.

4.3 Grey Hole

It is the type of black hole attack. In this attack, the attacker drops some of the packets. For instance, drops data packets and forwards routing packets.

4.4 Partitioning

In this type of attack, attacker creates a network partition in which some nodes are split up to not being able to communicate with another set of nodes. Attacker analyse the network topology to choose the partition between the set of nodes that makes the most harm into the system.

4.5 Blackmail

Some Ad Hoc routing protocols tries to handle the security problems by keeping lists of possibly malicious nodes. Each node has a blacklist of, what it thinks, bad nodes and thereby avoiding using them when setting up routing paths. An attacker might try to blackmail a good node causing other good nodes to add this node to their blacklists and so avoid it.

4.6 Wormhole

In the wormhole attack an attacker uses a pair of nodes connected in some way. It can be a special private connection or the packets are tunnelled over the Ad Hoc network. Every packet that one of the nodes sees are forwarded to the other node which in turn broadcast them out. This might create short circuits for the actual routing in the Ad Hoc network and thereby create some routing problems.
Also, all the data can be selectively forwarded or not using this attack thereby controlling the Ad Hoc network to a large extent. This kind of attack together with a partitioning attack can gain almost complete control over the network traffic.

4.7 Rushing Attack

Reactive routing protocols use sequence number for dominance of duplication at every node. An attacker can send multiple route requests with increasing sequence number so that it appear to be from different nodes. Due to which when actual request is sent out many nodes think it as a duplicate and interrupt actual route discovery process.

4.8 Resource Consumption

By injecting extra data packets into the Ad Hoc network limited resources such as bandwidth and maybe battery power are consumed for no reason. Even more resources might be consumed by injecting extra control packets since these might lead to additional computation. Also, the other nodes might forward control information as it comes in resulting in even more resource consumption [2].
For devices that try to conserve battery power by only occasionally enabling their communication device a malicious attacker might communicate in an ordinary way but with the only intent to drain battery power.

4.9 Dropping Routing Traffic

It is important that in Ad Hoc network all nodes participate in the process of routing. However, in order to conserve energy, a node may act selfishly and process only routing information that are related to it. This behaviour of the selfish node can instable the network and even /attack can create network instability or even part the network.

4.10 Location disclosure

Using Location disclosure attack, the malicious node knows the exact location or address of the node and can also get the information about the structure of the network. Due to which nodes which are neighbour to the destination node is also known by the attacker.

5. COMPUTER SIMULATION AND ANALYSIS IN NS-2.34 SIMULATOR.

- For the simulations, we use NS-2 (v-2.34) network simulator. NS-2 provides truthful implementations of the different network protocols.
- The size of the packet is 512 bytes.
- All the data packets are CBR packets.
- We use cbrgen to generate the connection pattern and the movement of the nodes is generated using *setdest utility.*
- *Setdest* generates random positions of the nodes in the network with stated mobility and pause time.
- The terrain area is 500m X 500m with number of nodes varying from minimum 10 to maximum 50 in first scenario.
- In another scenario, pause time vary from 20sec to 120 sec.

Table1: Simulation Parameters for Scenario1

Parameter	**Value**
Simulator	Ns-2(ver. 2.34)
Simulation Time	100s
Number of Nodes	10,20,30,40,50
Max. no. of Connections	8,16,24,32,40
Pause time	20s
Terrain Area	750 x 750
Max. speed	20s
Routing Protocol	AODV
No. of Malicious Node	1

5.1 Simulation Results and Evaluation Results

To evaluate the packet delivery ratio, Average Throughput and Normalized Routing Overhead; simulation is done with nodes with the source node transmitting maximum 100 packets to the destination node. Fig. 2, shows the graphs when network size (number of nodes) is varying. It can be seen from the Fig. 2,4, In AODV throughput is higher than the throughput of AODV under attack. As the number of nodes increase throughput for normal AODV is increase but in the case of AODV under black hole attack, throughput decrease. Here the mischievous and selfish node abandons all the data packets rather than sending it to the destination, thus effecting throughput. In Fig. 3 In AODV, packet delivery ratio is very near to 100% but in the case of AODV under black hole attack, PDF is very less and affect the total delivery of packets.

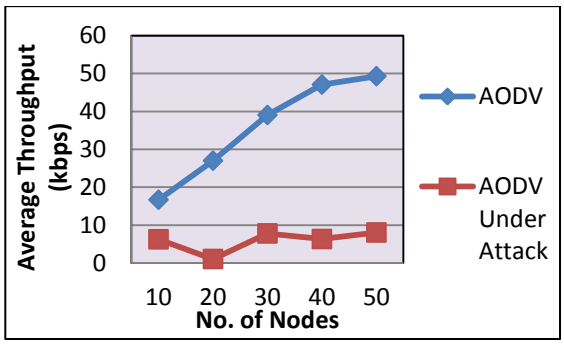

Figure 2: Effect of Black Hole Attack on Average Throughput

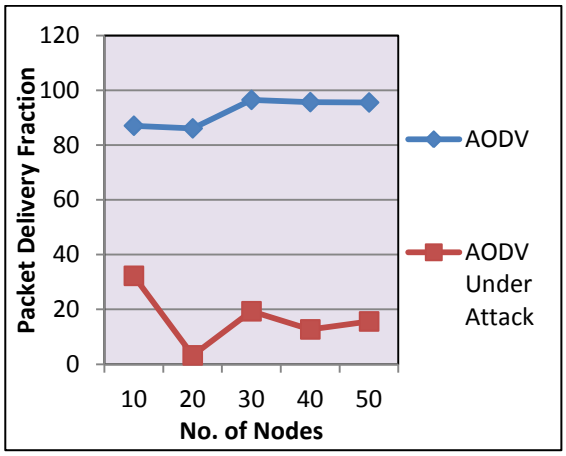

Figure 3: Effect of Black Hole Attack on Packet Delivery Fraction

Table 2: Simulation Parameters for Scenario II

Parameter	Value
Simulator	Ns-2(ver. 2.34)
Simulation Time	200s
Number of Nodes	25
Pause time	20,40,60,80,100,120
Terrain Area	500 x 500
Routing Protocol	AODV
Malicious node	1

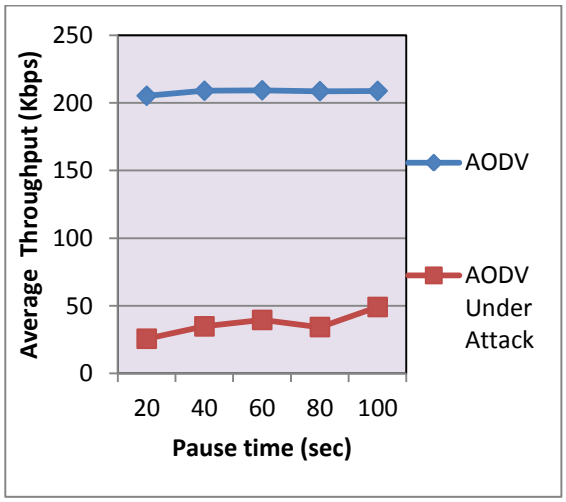

Figure 4: Average Throughput Vs Pause Time

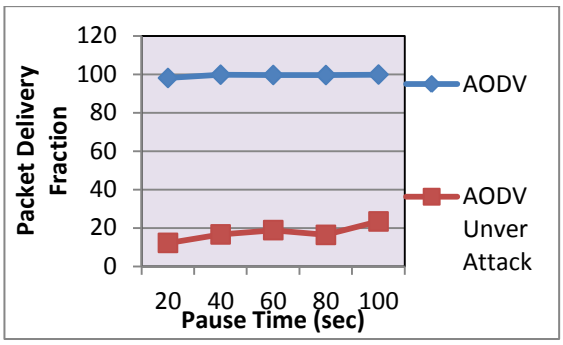

Figure 5: Packet Delivery Fraction Vs Pause Time

Table 3: Simulation Parameters for Scenario III

Parameter	Value
Simulation Time	100sec
Number of Nodes	25
Terrain Area	500 X 500
Number of Malicious Nodes	1,2,3,4,5
Routing Protocol	AODV

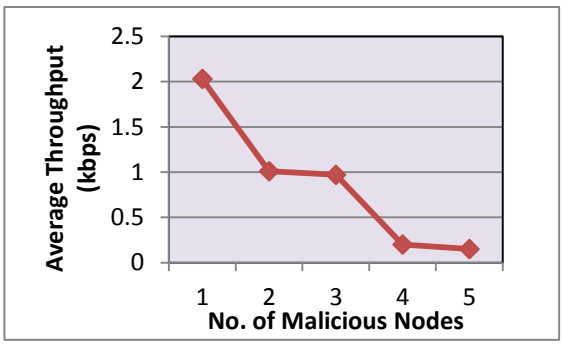

Figure 6: Effect on Average Throughput when malicious nodes increase in number.

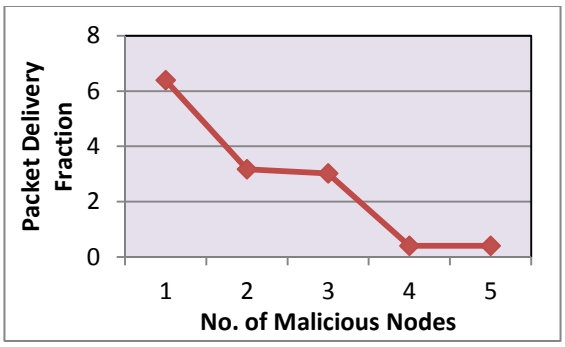

Figure 7: effect on Packet Delivery Fraction

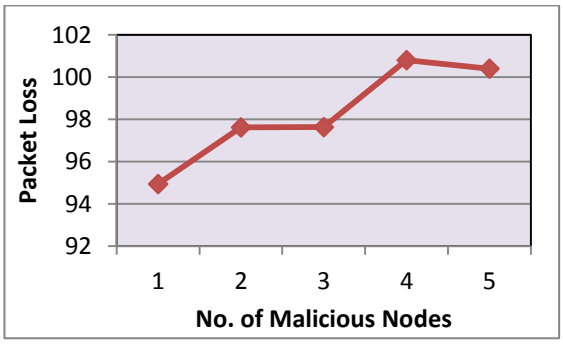

Figure 8: Packet Loss

6. PROPOSED SOLUTION

In the proposed solution, we use a data routing table[1] to store the routing information of neighbour nodes. When initiator node gets replies from different nodes, it stores all the replies instead of forwarding data packets to the first replied node. It analyse the data routing table of the nodes and send check packet to the neighbour nodes of the replying nodes. Information about the neighbour nodes gets from the reply which source node receives. In our proposed method, 3 techniques are used:

1. Collection of routing data of the Neighbours and analyses of data to detect malicious node.
2. Finding node that is trust worthy and reliable and elimination of malicious black hole nodes.
3. Global alarm rising to exclude malicious nodes.

a. Collection of routing data of the Neighbours and analyses of data to detect malicious node.

Each node stores the data routing information of their neighbours in the table called data routing table (DRI). This table keeps track of the data transfer history of its neighbours. This table contains three columns, first that specify its neighbour node, second column indicates whether the node received data from this neighbour to forward it and third column indicates whether the node sent data through this neighbour.

Source node initiates the process to examine the DRI table to detect suspected node. As we all know that in the routing process every node that comes in the path of source and destination has to take part in the routing process. Through data routing information table, source node detect which of the node did not take part in the communication process or did not interact with their neighbours to transmit packets will be treated as a suspicious node.

In the Route request discovery process, when source node wants to transmit data to destination and demand a route to destination, it broadcast the request message to its neighbours. Malicious node will reply first to get the packets from source node. Other nodes will also reply if they have fresh route to the destination and if request packet reaches to destination, destination node will also respond. Instead of sending data packets to the first node that replies, source node will wait and store all the replies received.

b. Finding node that is trust worthy and reliable and elimination of malicious black hole nodes.

To know whether the replying nodes are reliable and trust worthy, Source node sends a check packet to the neighbours. Neighbour checks their Data Routing information table, if they find 1 in the 'through' column and 0 in the 'from' column and 0 in both the column, that means the node is suspicious one. If they find '1' in both the columns that means node is most reliable and the route is safe and sound to transmit data. In [1] source node gets the data routing information of the replying as well as neighbouring nodes , it will increase routing overhead and time delay. And in [1] source node send the probe messages to the neighbours to check the reliability, it will increase overhead and these probe message can also capture by the malicious node. Instead of sending full DRI table of the replying node, source node will request to the neighbours of the replied node to check their DRI table and this check request will be sent to only the neighbours by setting the Destination only flag so that malicious node could not try to capture the check packets, (the neighbours are previous and next hop node of the node). Source node analyse the results and get to know about the suspected node and most reliable node.

c. Global alarm rising to exclude malicious nodes.

Source node get to know about the malicious node by its neighbour's DRI table and then it raise the alarm to exclude malicious black hole node from their routing table and add it in black list. Source node broadcast the IP address and node ID of the Malicious node to all other nodes, that this is a black hole node, don't take reply from this node and also update their routing table and remove this node from their forwarding table.

This DRI table is updated when any node received data packet from one of its neighbours or any node that sent data packets through one of its neighbours.

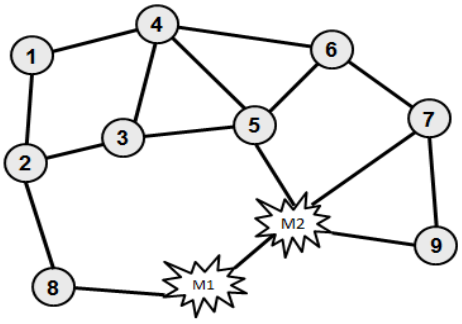

Figure 9: Cooperative black hole attack example

Table 4: Data Routing Table for Node 6

Node	From	Through
4	1	1
5	1	0
7	1	1

In the above figure, Source node is the node 2 and destination node is node 7. Node 2 broadcast Route Request Message to its neighbour nodes to get the route path. Malicious node M1 also get the request and it replies to the node 2 that it has the fresh route to the destination with less number of hops. Node 6 also replies to the source that it has the route to the destination node 7.

Table 5: Data Routing Table for Node M1

Node	From	Through
8	1	0
M2	0	0

As we see from table 5, that M1 node did not send any packet further to its neighbour nodes. It is the suspected node.

Table 6: Data Routing Table for node 8

Node	From	Through
2	1	1
M1	0	0

In the table 6, Node 2 is the most reliable, but it is the source node.

From Table 4 it is clear that, Node 4 is the most reliable one, and the route to the destination is safe. Source node takes this

route and generates alarm for node M1 and M2 who have '0' entry in both of the columns of DRI table.

7. CONCLUSION

Attack on MANET from Black Hole Nodes is very serious attack and we proposed a feasible solution to detect and eliminate single, multiple and Cooperative black hole nodes from network. We simulate the black hole attack on AODV protocol and show that a single and multiple black hole nodes has diverse effect on the throughput, packet delivery fraction and routing overhead. Throughput and Delivery fraction declines drastically and network overhead increases. All network traffic directed towards Black Hole nodes and they drop all the packets creating a denial of service attack on the network. The proposed solution can be used to detect other type of attacks like gray hole attack, worm hole attack and even selfish nodes.

8. REFERENCES

[1] Ankur Mishra, J. Ranjeet, Sharma S.," A Novel Approack for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network",3rd IEEE International Advanced Computing Conference (IACC), 2013.

[2] 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*

[3] Al-Shurman Mohammad and Yoo Seong-Moo," Black Hole Attack in Mobile Ad Hoc Networks", Huntsville, AL, USA. April 2-3, 2004.

[4] P.V.Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 16/17 2002.

[5] V.Mahajan, M.Natue and A.Sethi, " Analysis of Wormhole Intrusion attacks in MANETs," IEEE Military Communications Conference, pp. 1-7, Nov, 2008.

[6] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007

[7] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.

[8] Deng Hongmei, Li Wei and P. Agarwal Dharma ,"Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE, October 2009

[9] P. Yietaal., " A Routing Attack in Mobile AdHoc Networks", Int'l. J. Info. Tech., vol.11, no.2, 2005.

[10] Junhai Luo, Mingyu Fan, and Danxia Ye," Black Hole Attack Prevention Based on Authentication Mechanism", University of Electronic Science and Technology of China, Chengdu, China, 610054, IEEE, 2008

[11] Kozma W, Lazos L "REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits", Second ACM Conference, Zurich, Switzerland, 16-March 2009

[12] Su M-Y,"Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems", IEEE Computer Communications:107–117, August 2010

[13] Djenouri D, Badache N, "Struggling Against Selfishness and Black Hole Attacks in MANETs", *Wireless Communications & Mobile Computing* Vol. 8, Issue 6, pp 689-704, August 2008.

[14] H.Weerasinge and H.Fu(2008) "Preventing Black Hole Attack in Mobile Ad hoc Networks: simulation, implimentation and evaluation"*international journal of software engg. and its applications,vol2,no3*