S Chaturya * et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.6, Issue No.2, February - March 2018, 7980-7987.

MBDS: Message Authentication Code (MAC) Based Black Hole Detection System Inmanet's

Ms. S.CHATURYA
Department of Computer Science Engineering,
Gudlavalleru Engineering college, Gudlavalleru,
India

Mrs.Y.ADILAKSHMI
Department of Computer Science Engineering,
Gudlavalleru Engineering College, Gudlavalleru,
India

***Abstract*---** Mobile ad hoc network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes can directly communicate to those nodes that are in radio range of each other, whereas others nodes need the help of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the aid of any infrastructure. This property makes these networks highly robust. Security is a major challenge for these networks due to their features of open medium, dynamically changing topologies. The black hole attack is a well known security threat in mobile ad hoc networks. However, it spuriously replies for any route request without having any active route to the specified destination. Sometimes the Black Hole Nodes cooperate with each other with the aim of dropping packets these are known as Cooperative Black Hole attack.

This research work suggests the modification of Ad Hoc on Demand Distance Vector Routing Protocol. we are going to use a mechanism for detecting as well as defending against a cooperative black hole attack. This work suggest Maintenance of Routing Information Table and Reliability checking of a node with MAC address and Sequence Number. This system also decreases the end to end delay and Routing overhead.

Keywords-Mobile ad hoc network (MANET), Blackhole, Malicious node, Routing, MAC, AODV.

I. INTRODUCTION

An Ad hoc network is a collection of mobile nodes which forms a temporary network without the aid of centralized administration or standard support devices regularly available as conventional networks. These nodes generally have a limited transmission range and, so, each node seeks the assistance of its neighbouring nodes in forwarding packets and hence the nodes in Ad hoc network can act as both routers and hosts. Thus a node may forward packets between other nodes as well as run user applications. By nature these types of networks are suitable for situations where either no fixed infrastructure exists or deploying network is not possible. Mobile Ad hoc networks have found many applications in various fields like military, emergency, conferencing and sensor networks. Each of these application areas has their specific requirements for routing protocols.

Since the network nodes are mobile, an Ad hoc network will typically have a dynamic topology which will have profound effects on network characteristics. Network nodes will often be battery powered, which limits the capacity of CPU, memory and bandwidth. This will require network functions that are resource effective. Furthermore, the wireless media will also affect the behaviour of the network due to fluctuating link bandwidths resulting from relatively high error rates. These unique desirable features pose several new challenges in the design of wireless Ad hoc networking protocols. Network functions such as routing, address location, authentication and authorisation must be designed to cope with a dynamic and volatile network topology. In order to establish the route between the nodes, which are farther than a single hop, specially configured routing protocols are engaged.

Because of the features like dynamically changing topologies and fixed infrastructure, mobile ad hoc networks are prone to suffer from malicious behaviour. Therefore we need to pay more attention to the security issues in mobile ad hoc networks.MANET suffers from disruption so that node not able to take part in path finding methods with a target to spoil the full network functioning. A number of protocols have been found for efficient routing.

One of the most widely used routing protocols in MANETs is the *Adhoc on-demand distance vector* (AODV) routing protocol.The mobile devices or nodes in the network exchange the routing packets between them when they want to communicate with each other and maintain only these established routes.AODV is vulnerable to the well-known black hole attack. Most author has assumed that the black hole in the MANET do not work in a group and have proposed a solution to identify single black hole attack .However in their proposed solution many of them found multiple black hole malicious node. Some author has suggested solution for detecting cooperative attack but due to multipath routing it require more end to end delay and more routing overhead .The proposed technique works with modified AODV protocol and routing information table for searching trustful node.

II. RELATED WORK

Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamlipour, and Yoshiaki Nemoto [1] use an anomaly detection scheme. It uses dynamic training method in which the training data is updated at regular time intervals. Multidimensional feature vector is identified to express state of the network at each node. Each dimension is counted on every time slot. It uses destination sequence number to detect attack. The feature vector include Number of sent out RREQ messages, number of received RREP messages, the average of difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. They calculate mean vector by calculating some mathematical calculation. They compare distance between the mean vector and input data sample. If distance is greater than some threshold value then there is an attack.

ShaliniJain [2] proposed a mechanism capable of detecting and removing the malicious nodes launching two types of attacks. Their approach consists of an algorithm which works as follows. Instead of sending the total data traffic at a time they divide the total traffic into some small sized blocks. So that malicious nodes can be detected and removed in between the transmission of two such blocks by ensuring an end-to-end checking. Source node sends a prelude message to the destination node before start of the sending any block to alert it about the incoming data block. Flow of the traffic is monitored by the neighbors of the each node in the route. After the end of the transmission destination node sends an acknowledgement via a postlude message containing the no of data packets received by destination node. Source node uses this information to check whether the data loss during transmission is within the tolerable range, if not then the source node initiate the process of detecting and removing malicious node by aggregating the response from the monitoring nodes and the network.

KundanMunjal, ShilpaVerma, AdityaBakshi [3] proposed an Algorithm to detect cooperative Black Hole Attack considering three different cases. In the first case there were no malicious node present in the network and the reply for route request was from the reliable node so based on this previous information of reliability of node the route is confirmed to be secured. In the second case there were two black hole nodes in the network mutually cooperating with each other as there was no previous information for these two nodes so they are checked for reliability and found malicious at the end and this information of malicious behavior was propagated throughout the network. In the third case a node is found to be reliable and this information is broadcasted throughout the network and 3rd bit with respect to that node is set to true which shows that the node in question is trustful node.

Payal N. Raj, Prashant B. Swades [4] proposed DPRAODV (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which a node receives the Route reply (RREP) packet which first checks the value of sequence number in its routing table.

The RREP is accepted if its sequence number is higher than that in the routing table. It also check whether the sequence number is higher than the threshold value, if it is higher than the threshold value than it is considered as the malicious node.

Mohammad Al-Shurman, Seong-Moo Yoo and SeungjinPark[5] proposed two different approaches to solve the black hole attack. The first solution the sender node needs to verify the authenticity of the nodes that initiates the RREP packet by utilizing the redundancy of the network. The idea of this solution is to find more than one route for the destination. The SN unicast the ping packet using different routes. The IN or destination node or malicious node will ping requests. The SN checks the acknowledgement and processes them to check which one is safe or having malicious node. In the meantime the SN buffered until it found the safe route.

JaydipSen,SripadKoilakonda, ArijitUkil [6] proposed mechanism for defending against a cooperative black hole attack is presented. The mechanism modifies the AODV protocol by introducing two concepts, (i) data routing information (DRI) table and (ii) cross checking.

In the DRI scheme, two bits of additional information are sent by the nodes that respond to the RREQ message of a source node during route discovery process. Each node maintains an additional data routing information (DRI) table. In the DRI table, the bit 1 stands for ‘true’ and the bit 0 stands for ‘false’. The first bit ‘From’ stands for the information on routing data packet *from* the node (in the *Node* filed), while the second bit ‘Through’ stands for information on routing data packet through the node.

The process of cross checking the intermediate nodes is a one-time procedure which should be affordable for the purpose of security. The cost of crosschecking the nodes can be minimized by allowing the nodes to share the DRI table of their trusted nodes with each other.

LathaTamilselvan, DR.V. Sankaranarayanan [7] proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. A technique is give to identify multipleblack holes cooperating with each other and discover the safe route by avoiding the attacks.

It was assumed in the solution that nodes already authenticated and therefore can participate in the communication. It uses Fidelity table where every node that is participating is given a fidelity level that will provide to that node. Any node having 0 value is considered as malicious node and is eliminated.

HesiriWeerasinghe [8] proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the Ramaswamy to improve the accuracy. This algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (RREP).

Chang Wu Yu, Tung-Kuang, Wu, ReiHeng, Cheng, and Shun Chao Chang [9] proposed a distributed and cooperative procedure to detect black hole node. In this each node detect local anomalies. It collects information to construct an estimation table which is maintained by each node containing information regarding nodes within power range. This scheme is initiated by the initial detection node which first broadcast and then it notifies all one-hop neighbors of the possible suspicious node. They cooperatively decide that the node is suspicious node.

Ms. GayatriWahane, Ms. Savita Lonare[10] proposed the detection of blackhole attack by modifying AODV routing protocol by introducing two techniques called Maintenance of Routing Information Table (RIT) and Reliability checking of a node. In the maintainance of routing information table the bit information is maintained. The bit information stored in from node, through node and through any trustful node states whether the node is reliable or not. In reliability checking of the node the intermediate node that generates RREP will provide the information about next hoping node and RIT entry of next hoping node.

III. PROGRAMMER'S DESIGN

In the proposed scheme, technique for detecting as well as defending against a cooperative black hole attack is identified and presented by an algorithm. In this proposed scheme the modification of Ad Hoc on Demand Distance Vector Routing Protocol takes with the introduction of two types of concepts:

1. Maintenance of Routing Information Table (RIT).

2. Reliability checking of a node.

In this, an Algorithm to detect cooperative Black Hole Attack has been proposed and examination has been done by considering three different cases. In the first case there were no malicious node present in the network and the reply for route request was from the reliable node so based on this previous information of reliability of node the route is confirmed to be secured. In the second case there were two black hole nodes in the network mutually cooperating with each other as there was no previous information for these two nodes so they are checked for reliability and found malicious at the end and this information of malicious behaviourwas propagated throughout the network. In the third case a node is found to be reliable and this information is broadcasted throughout the network and 3rd bit with respect to that node is set to true which shows that the node in question is trustful node. Finally it has been concluded that this algorithm works well in all the three cases with the aim of detecting Cooperating Black Hole Attack and ensuring a secure as well as reliable route from source to destination.

A. AODV and Black Hole Attack

1. Aodv Overview:

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in ad-hoc mobile networks. AODV is a reactive protocol. The routes are created only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is upto-date and to prevent routing loops. An important feature of AODV is the maintenance of time-based states in each node. A routing-entry not recently used is expired. In case of a route is broken the neighbours can be notified.

Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries. The following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbours.

2. Black Hole Attack

A Black Hole Attack is a malicious node waits forneighboring nodes to send RREQ messages.When it receives, it replies to them blindly RREQ as if it is the shortest route to the destination. When the data is actually start transferring it absorbs all the packets originally meant for the destination. Black Holes are difficult to find if they start using sequence number

comparable to the current sequence number ofnetworks.

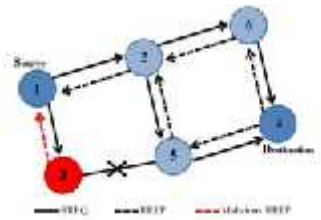

Figure 1: Black hole attack

Figure 1 is an example of single black hole attack in the mobile ad hoc networks. Node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehaviour node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. In the mobile ad hoc networks, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem.Sometimes these malicious nodes cooperate with each other with the same aim of dropping packets these are known as cooperative Black Hole nodes and the attack is known as *Cooperative Black Hole attack.*

IV. PROPOSED WORK

In this proposed scheme the Ad Hoc on Demand Distance Vector Routing Protocol is modified by introducing two types of concepts.

1. Routing Information Table (RIT) maintenance

2. Reliability checking.

1. Routing Information Table maintenance:

In the proposed scheme, each and every node maintains three bit information from which two bits of the information are sent by the nodes that respond with the RREP message to the source node during route discovery phase and third bit information is broadcasted by any node in the network. In the routing information table (RIT) the bit 1 stands for true and the bit 0 stands for false. The four types of information stored are:

1. from Node

2. through Node

3. through any Trustful Node

4. Message authentication code(MAC)

From Node : It stands for the information on routing data packet from the node in question.

Through Node : It stands for the information on routing data packet through the node in question.

Through any trustful node: This bit is set if any trustful node has routed data packet through the node in question.

Message Authentication Code: It is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographickey. It may be used to simultaneously verify both the *dataintegrity* and the *authentication* of a message, as with any MAC. Any cryptographic hash function, such as MD5 or SHA-1 may be used in the calculation of an HMAC.

Table 1: The routing information for node N5 is maintained.

SEQ NUMBER	MESSAGE AUTHENTICATION CODE	NODE ID	FROM NODE	THROUGH NODE	THROUGH ANY TRUSTFUL NODE
19	H1	N1	1	1	0
21	H2	N2	1	0	1
23	H3	N3	0	0	1
26	H4	N4	1	1	1
28	H6	N6	0	0	0

The entry 1 1 0 for node N1 shows that node N5 has routed data from node N1 before, node 5has also successfully routed data through node N1 before, but any other trustful node hasn't routed data through node N1.Similarly, node N2 entry is 1 0 1 which shows that node N5 has successfully routed data from node N2 but not through node N2 but the third entry shows that any other node (trustful node) has successfully routed data through node N2. The entry for node N3 is 0 0 1 which shows that node N4 has never routed data from or through node N3 but any other trustful node had successfully routed through it in the past. The route entry for node N6 is 0 0 0 which shows that no node in the network had routed data from or through node N6.

TRUSTFUL NODE:

Nodes through which source node or any trustful node has routed data previously then that nodes are considered as **reliable or trustful nodes**. Consider the table 1 in which: 1. Node N1 is trustful as node N5 had routed data through it previously. 2. Node N2 is trustful as any other trustful node had routed data through it previously. 3. Node N6 is not trustful as no node in the network had routed data through it.

2. Reliability Checking:

In the modification the source node (SN) broadcasts a RREQ message to discover a reliable route to the destination. The intermediate node(IN) that generates the RREP has to provide the information about the Next Hoping Node (NHN) and the table entry (RIT entry) for the NHN with MAC and sequence number. The original message authentication code is "de7c9b85b8b78aa6bc8a7a36f70a90701c9db4d9". The MAC code in the table is represented as H1 and so on. Along with the RREP the source node also checks whether the MAC is matched or not.Upon receiving the RREP message from the intermediate node the source will check its own routing information table to see whether IN is a trustful node or not. If SN has routed data through IN before, then IN is trustful and it starts routing data through IN but if it hasn't routed before then IN is unreliable. Along with the reliability checking of the node it also checks for MAC matching. If MAC does not matched then also the node is treated as malicious and SN sends Additional Request (ARq) message to next hop node about following information:

1. If IN has routed data through NHN

2. Who is the current NHN's next hop towards the destination?

3. The RIT entry for NHN's next hop.

4.What is the sequence number and Hash based message authentication code?

Based on the Additional reply message (ARp) from NHN, SN checks whether the MAC is matched or not and NHN is reliable or not. If SN has routed data through NHN before then NHN is reliable. Otherwise NHN is unreliable for SN. If NHN is unreliable then SN will check whether IN is Black Hole or not. If the second bit entry for the IN is 1 then it shows that IN has routed data through NHN before but if the first bit entry of the NHN is 0 then it shows that NHN hasn't routed data from IN before so this contradiction shows that IN is a Black Hole node. And, if IN is not a Black Hole and NHN is reliable node with MAC matched and sequence number difference is not more, then the route is reliable and SN will update its RIT entry with 0 1 0 and also broadcasts a B_REPLY message with the identity of the IN to show that this node is reliable. On the other hand the node receiving the B_REPLY message first checks whether the B_REPLY message is from the node through which it had routed data before or any trustful node had routed data before (i.e. trustful node).

This checking is made as cooperative Black Hole nodes can also broadcast a B_REPLY message for e.g. Consider two Cooperative Black Hole nodes B1 and B2. B1 can also broadcast a B_REPLY message with the ID of B2 to show that B2 is trustful. And, if the broadcasted B_REPLY message is from the trustful node then the node receiving the B_REPLY message will set the third bit in the RIT to true for the respective IN.

Consider Example to show the working of algorithm in different cases:

Case No 1: When there are no black hole nodes in the network and the reply is from reliable node.

Consider the case in the figure2 in which the source node S broadcasts a route request packet (RREQ) packet to the destination node D**,** node N2 replies with a RREP packet, node S check its RITentry for node N2 i.e. 1 1 1 which means that (Table 1) it has routed data through this node previously

Table 2: Routing information table for node S

SEQ NUMBER	MESSAGE AUTHENTICATION CODE	NODE ID	FROM NODE	THROUGH NODE	THROUGH ANY TRUSTFUL NODE
19	H1	N1	1	1	0
21	H2	N2	1	0	1
23	H3	N3	0	0	1
26	H4	N4	1	1	1
27	H5	N5	0	0	0
28	H6	N6	0	0	0

Consider the case in the below figure 2 in which and also some other trustful node had also routed data successfully through this node as second and third bit entry are set to true (1). Therefore, node N2 is reliable and the route is secure.

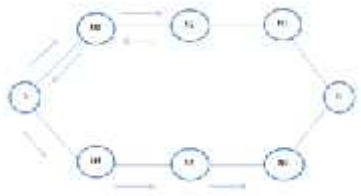

Figure 2: Reply from node N2

Case No.2 When there are Cooperative Black Hole Nodes in the network and the route reply is from one of the black hole node.

Consider the case in the figure 3 with two Black Hole nodes in the network cooperating with each other. Here, node S request for a route to the destination D by broadcasting a RREQ packet.

The node B1 immediately replies spuriously with RREP packet showing that it is having the shortest as well as fresh enough route to the destination. The SN according to the algorithm first checks whether the RREP is from the destination node or from the trustful node i.e. it checks the RIT entry for that node but it finds the node B1 unreliable and then it checks it for reliability. It asks B1 for its next hop and also the RIT entry for the next hop.

It provides its next hop B2 and it lies with the RIT entry with value 0 1 1. Since no node in the network has sent data through B1 before, B1 is not a trustful node to S. Therefore S sends additional request (ARq) to B2 via alternative path and ask B2 about four things: 1. Whether B2 had routed any data from B1. 2. Who is B2's next hop to the destination? 3. Whether B2 had routed data packets through B2's next hop. 4.What is the MAC and sequence number?

Since B2 is maliciously collaborating with B1 it replies positively to all the three queries and gives node N5 with its next hop. Since node 3 has neither a route to node B2 nor it has received data packets from B2 the RIT entry value with respect to B2 as in routing information table of node N5 is 0 0 0. Based on this information node S infers that B2 is a black hole and source node S also infers that node B1 is maliciously cooperating with node B2. Hence both nodes B1 and B2 are marked as Black Hole nodes and this information is propagated throughout the network.

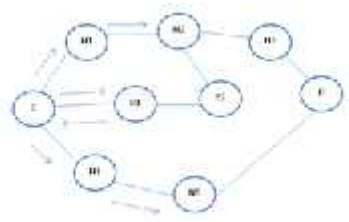

Figure 3: Cooperative Black Hole attack detection

Case No. 3: when a node broadcasts a B-REPLY message

Consider the case in the fig. 4, here node N3 starts a route discovery process by broadcasting a route request (RREQ) packet for node N7. Node N6 replies with a route reply (RREP) packet, now node N3 checks its routing information table (RIT) to see whether node N6 is reliable or not. It found node N6 unreliable and then checks it for reliability. Suppose node N6 found to be reliable at the end then node N3 will broadcast this message as B_REPLY message in the whole network with the id of node N6 to show that this node is trustful. This broadcast message is known as B_REPLY message.

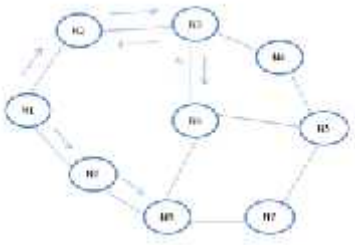

Figure 4: node N3 broadcasts B_Reply message with id of node N6.

Now consider the case when this B_REPLY message reaches node N1 then node N1 first checks that which node had broadcasted it whether it is trustful or not through its RIT table after checking the table (Table 4) node N2 found to be reliable and then it will set the third bit entry for node N6 to be true.

Table 4: Routing information table for node setting the 3rd bit entry true for node N6 by checking the reliability of node N3.

SEQ NUMBER	MESSAGE AUTHENTICATION CODE	NODE ID	FROM NODE	THROUGH NODE	THROUGH ANY TRUSTFUL NODE
22	H3	N2	1	1	1
23	H4	N3	1	1	1
25	H6	N8	0	0	1
27	H8	N6	1	1	1

Now consider the case in fig 4 when node N1 starts a route discovery process by broadcasting a route request packet for node N5 and node N6 replies with a route reply packet. As the third bit entry for node N6 is true in the routing information table for node N1 there is no need for reliability check i.e. node N6 is a trustful node.

Network Simulator: (NS2)

Ns is a discrete event simulator targeted at networking research. Ns provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless networks.

Output:

Figure 5: Simulation parameters setup.

The above figure describes the simulation parameters that are to be taken while doing simulation. The Mac type, network interface type, max packets in ifq, number of mobile nodes taken, the protocol that is used, and the dimensions of topography, time of simulation end are described.

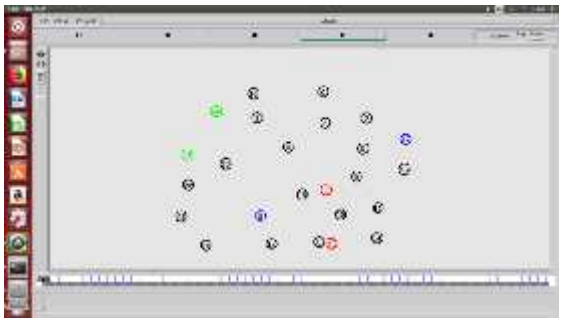

Figure 6: NAM set up for 25 nodes

Network animation tool (NAM) is set up for 25 nodes where the nodes which are coloured green are source nodes and the nodes which are coloured blue are destination nodes. The nodes which are in red colour are black hole nodes.

We have performed simulation by using NS2 with different simulation parameters. Here 25 nodes are taken to perform simulation. The observation is as follows:

Figure 7: Trace file execution before simulation.

The source node delivers data packets to the destination nodes. If there are any black hole nodes in the network, then they will be dropped. They will not be received by the destination nodes. Figure 6 shows the trace file execution with number of packets sent, number of packets received and number of packets dropped. This concludes that there are black hole nodes in the network.

So, to detect the black hole nodes and to ensure more security, the Message authentication code is provided to the nodes. After modifying the AODV protocol by maintenance of routing information table and reliability checking along with message authentication code (MAC) the simulation results are as follows.

By considering the trace file of the above program the result shows that the blackhole nodes dropped the data packets.

Figure 8: Trace file execution after simulation.

After the simulation of the trace file the results shows the detection of black hole nodes. Therefore the dropped packets are zero.

V CONCLUSION:

From the above discussion it is clear that security is the major concern in mobile ad hoc networks. Here we modified AODV routing protocol by adding message authentication code to the routing information table and reliability checking of the node we detected the black hole nodes. After detecting those nodes we prevented that route from forwarding packets to the destination nodes.

As a future work, the proposed algorithm is efficient for detection of black hole attacks and cooperative black hole attacks in the network. But more improvement can be done in end to end delay.

REFERENCES

[1] 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, volume 5, Number 3, 2007, pp 338-346.

[2] S halini Jain, ”Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks”, 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 7

[3] KundanMunjal, ShilpaVerma, AdityaBakshi “Cooperative Black Hole Node Detectio by Modifying AODV”,International Journal ofManagement, IT and Engineering, Volume 2, Issue 8, Aug 2012.

[4] Payal N. Raj and Prashant B. Swadas, “DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET”, International Journal of Computer Science Issues(IJCSI), Volume 2, Number 3, 2009, pp 54-59.

[5] Mohammad Al-shurman, Seong-Moo Yoon and Seungjin park, “Black Hole Attack in Mobile Ad Hoc Networks”, ACM Southeast Regional Conference, Proceedings of the 42nd annual southeast regional conference , 2004, pp 96-97.

[6] J. Sen, S.Koilakonda and A.Ukil, “A mechanism for detection of cooperative black hole attack in mobile ad hoc networks”, second international conference on intelligent system, modeling and simulation ,innovation lab, Tata consultancy services ltd. , Kolkata, 25-27 jan 2011.

[7] LathaTamilselvan and V Sankarnarayana, “Prevention of Black Hole Attack in MANET”, Journal of Networks, Volume 3, Number 5, 2008, pp 13-20.

[8] HesiriWeerasinghe“Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation”, Proceedings of the Future Generation Communication and Networking, Volume 2, 2007, pp 362-367.

[9] Chang Wu Yu, Tung-Kuang, Wu, ReiHeng, Cheng and Shun Chao Chang, “A distributed and Cooperative Black Hole Node Detection and Elimination mechanism for Ad Hoc Networks”, PAKDD 2007 International Workshop, May 2007, Nanjing, China, pp 538-549.

[10] Ms. GayatriWahane, Ms. Savita Lonare, “Technique for detection of Cooperative black hole attacks in MANET’S”,international conference on computing, communication and networking technologies, July 4-6, 2013.

