IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 59-67
www.iosrjournals.org

Technique for Detection of Cooperative Black Hole Attack In MANET

Ms. Gayatri Wahane[1], Prof. Ashok Kanthe[2]
[1,2]Department of Computer Engineering, Sinhgad Institute of Technology, Lonavala, Pune, India

ABSTRACT : *Mobile Ad Hoc Network (MANET) is acollection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. 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. I am going to use a mechanism for detecting as well as defending against a cooperative black hole attack. This work suggest two new concepts, first one is Maintenance of Data Routing Information Table and second is cross checking of a node. This system also decreases the end to end delay and Routing overhead.*

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

I. INTRODUCTION

A mobile Ad hoc network (MANET) is a self –configuring network that does not require any fixed infrastructure, which minimizes their cost as well as deployment time. As each node in this network is free to move which makes the network to change its topology continuously. These infrastructure-less mobile nodes in ad hoc networks dynamically create routes among themselves to form own wireless network on the fly. Because of the dynamic nature, these networks are more vulnerable to attacks so security is an important as well as serious issue in mobile ad hoc network. One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. A set of nodes in a MANET may be compromised in such a way that it may not be possible to detect their malicious behavior easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic.

One of the most widely used routing protocols in MANETs is the *adhoc on-demanddistance vector* (AODV) routing protocol. AODV isvulnerable 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.

This paper is organized as follows. In Section II related work for detecting Black Hole attack has been discussed. Section III provides Programmer Design in which discuss Performance metrics and overview of AODV protocol with the description of black hole attack characteristics. Section IV describes the proposed solution for detecting cooperative Black hole attacks in mobile ad hoc networks and shows the working of the algorithm with the help of an example. We conclude plan for future work in section V.

RELATED WORK

In this section we will discuss some research work has been done by various author. Sukla Banerjee [1] proposed a mechanism capable of detecting and removing the malicious nodes launching these two types of attacks. Their approach consists of an algorithm which works as follows. Instead of sending the total data traffic at a time we 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.Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamlipour, and Yoshiaki Nemoto [2] 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.

Shalini Jain [3] 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.

JaydipSen, SripadKoilakonda, ArijitUkil [4] 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.

HesiriWeerasinghe [5] 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 [6] 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.

II. 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 Data Routing Information Table (DRI).
2. Cross 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 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. 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.

III. PERFORMANCE METRICS

3.1.1. Throughput

The throughput is the number of bytes transmitted or received per second. The throughput is denoted by T,

Throughput= received node/simulation time

$$T = \frac{\sum_{i=1}^{n} N_i^r}{\sum_{i=1}^{n} N_i^s} \times 100\% \qquad \ldots.(1)$$

Where,N^r= average receiving node for the ith application, N^s= average sending node for the i^{th} application, and n = number of applications.

3.1.2. Average end-to-end delay (average E2E delay):

It represents the time required to move the packet from the source node to the destination node.

E-2-E delay [packet_ id] = received time [packet_ id]– sent time [packet_ id]

The average end-to-end delay can be calculated by summing the times taken by all received packets divided by its total numbers [13]

$$D = \frac{\sum_{i=1}^{n} d_i}{n} \qquad \ldots.(2)$$

Where, d_i= average end to end delay of node of ith application and n=number of application

3.1.3. Dropped Packets:

It represents the number of packets that sent by the source node and fail to reach to the destination node [13].

Dropped packets = sent packets– received packets.

$$L = \sum_{i=1}^{n}(N_i^s - N_i^r) - \sum_{i=1}^{n} N_i^s \qquad \ldots.(3)$$

N^s , N^rnode sent by the sender and the number of application data node received by the receiver, respectively for the *i*thapplication, and *n* is the number of applications.

3.1.4 Packets delivery fraction (PDF):

It can be measured as the ratio of the received packets by the destination nodes to the packets sent by the source node [14].

PDF = (number of received packets / number of sent packets) * 100

$$\text{PDF}=\frac{\sum_{i=1}^{n}(N_i^s - N_i^r)}{\sum_{i=1}^{n} N_i^s} \times 100\% \qquad \ldots.(4)$$

N^s , N^rnode sent by the sender and the number of application data node received by the receiver, respectively for the ithapplication, and n is the number of applications.

3.2. AODV and Black Hole Attack

3.2.1 Overview Of Aodv

AODV is a reactive [15] routing protocol that does not require maintenance of routes to destination nodes. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is demand from mobile node. In ad hoc network first route discovery takes place, which means if a mobile node that wishes to communicate with other node first broadcast a RREQ (Route Request) message to find a fresh route to a desired destination node. Every neighbor node that receives RREQ broadcast first saves the path the RREQ was transmitted along its routing table. It then checks its routing table to see if it has a fresh enough route to the destination node provided in RREQ message. Destination sequence number attached to it indicates the freshness. If a node finds a fresh enough route it uncast a RREP (route reply) message back along the saved path to the source node or it rebroadcast the RREQ message otherwise. The same process continues until an RREP message from the destination node or an intermediate node that has a fresh route to the destination node received by the source node.

3.2.2. Black Hole Attacks

A black hole attack is a kind of Denial of service attack in mobile ad hoc networks. In this attack, a malicious node sends [15] a fake RREP packet to the source node that has initiated a route discovery, in order to show itself as a destination node or an intermediate node to the actual destination node. In such a case the source node would send all of its data packets to the malicious node the malicious node then absorbs all the packets and drops them fully or sometimes partially. As a result source and destination node will not be able to communicate with each other.

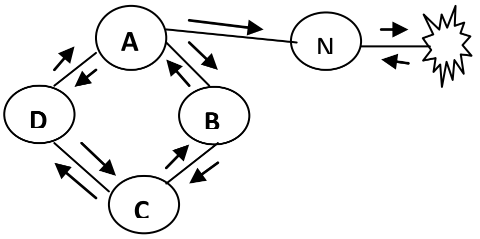


Fig 1. Route discovery with Black Hole attack by malicious node N

Consider the case in fig. 1 where A is the source node D is the destination node and N is the malicious node here node A starts with the route discovery process then the node N advertises itself as having a valid shortest route to the destination, even though the route is false with the purpose of intercepting packets. Moreover a malicious node does not need to check its routing table when sending a false message; its response is more likely to reach the source node first. This makes the source node think that the route discovery process is complete, ignore all other reply messages and begin to send data packets. As a result, all the packets through the malicious node are simply absorbed discarded and then lost. The malicious node could be said to form a black hole in the network. 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.*

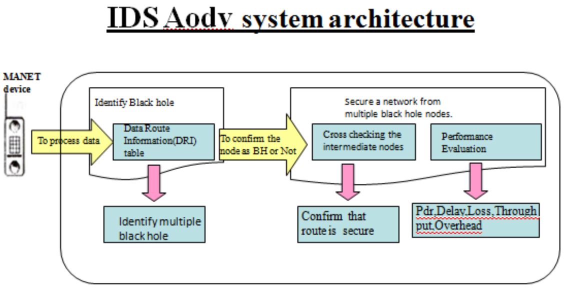
IV. THE PROPOSED ALGORITHM

In this, section the proposed algorithm for detection of a cooperative black hole attack is presented. The mechanism modifies the AODV protocol by introducing two concepts by using system architecture in fig. 2,

(i) Data routing information (DRI) table and
(ii)Cross checking.

4.1 Data Routing Information

In the proposed 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


IDS Aodv system architecture
MANET device
To process data
Identify Black hole
Data Route Information(DRI) table
Identify multiple black hole
To confirm the node as BH or Not
Secure a network from multiple black hole nodes.
Cross checking the intermediate nodes
Performance Evaluation
Confirm that route is secure
Pdr,Delay,Loss,Through put,Overhead

node (in the *Node* field). With reference to

Fig. 2 System Architecture

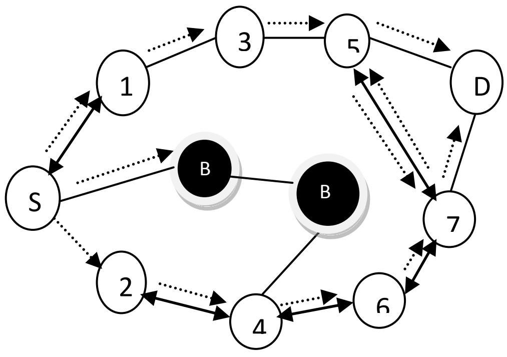


Fig. 3 AODV RREQ message

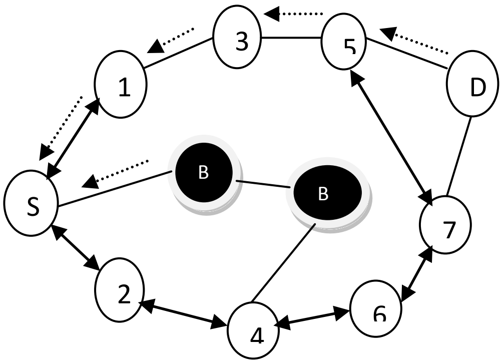


Fig. 4 AODV RREP message

the example depicted in Fig. 4, a sample database maintained by node *4* is shown in Table 1. The entry 1 0 for node *3* implies that node *4* has routed data packets from *3*, but has not routed any data packets through *3* (before node *3*moved away from *4*). The entry 1 1 for node *6* implies that, node *4* has successfully routed data packets from and through node *6*. The entry 0 0 for node *B2* implies that, node *4* has not routed any data packets from or through *B2*.

TABLE I: DRI table maintained of node 4

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

4.2 Cross Checking

The proposed scheme relies on reliable nodes (nodes through which source has routed data previously and knows them to be trustworthy) to transfer data packets. The modified AODV protocol and the algorithm for the proposed mechanism are depicted in Fig. 5 and Fig. 6 respectively. In the modified protocol, the source node (SN) broadcasts a RREQ message to discover a secure route to the destination node. The intermediate node (IN) that generates the RREP has to provide information regarding its next hop node (NHN) and its DRI entry for that NHN. Upon receiving the RREP message from IN, SN will check its own DRI table to see whether IN is its reliable node. If SN has used IN before for routing data packets, then IN is a reliable node for SN and SN starts routing data through IN. Otherwise, IN is unreliable and thus SN sends FRq message to NHN to check the identity of the IN, and asks NHN about the following information: (i) if IN has routed data packets through NHN, (ii) who is the current NHN's next hop to destination, and (iii) has the current NHN routed data through its own next hop. The NHN, in turn, responds with FRp message including the following responses: (i) DRI entry for IN, (ii) the information about its (NHN's) next hop node, and (iii) the DRI entry for its (NHN's) next hop. Based on the FRp message from NHN, SN checks whether NHN is reliable or not. If SN has routed data through NHN before, NHN is reliable; otherwise, NHN is unreliable for SN. If NHN is reliable, then SN will check whether IN is a blackhole or not. If the second bit of the DRI entry from the IN is equal to 1,i.e. IN has routed data *through* NHN, and the first bit of the DRI entry from the NHN is equal to 0 i.e. NHN has not routed data from IN, then IN is a blackhole. If IN is not a blackhole and NHN is a reliable node, then the route is secure, and SN will update its DRI entry for IN with 0 1, and starts routing data via IN. If IN is a blackhole, then SN identifies all the nodes along the reverse path from IN to the node that generated the RREP as blackhole nodes. Subsequently SN ignores any other RREP from the blackholes and broadcasts the list of cooperative blackholes in the network. If NHN is an unreliable node, SN treats current NHN as IN and sends FRq to the updated IN's next hop node and goes on in a loop from steps 7 through 24 in the algorithm depicted in Fig.6

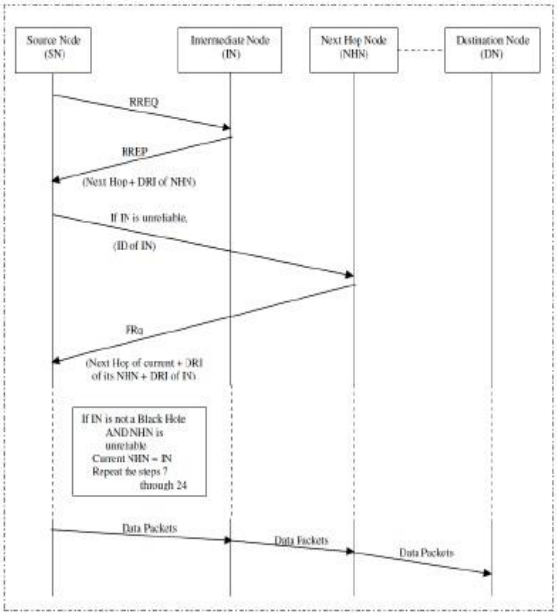


Fig. 5 Modified AODV protocol

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 node to share the DRI table of their trusted nodes with each other.

```
SN Source Node  IN Intermediate Node  DN Destination Node
NHN:Next Hop Node   ARq Additional Request ARp Additional Reply
DRI Data  Routing Information   ID  Identity of the node
 Relaible Node: The node through which the SN has routed data
SN broadcast RREQ
SN Receives RREP
IF(RREP is from DN or a reliable node) {
Route data packets(Secure Route)
}
ELSE {
    Do {
        Send FRq, and ID of IN to NHN
        Receive FRp, NHN of current NHN,
        DRI entry for NHN's next hop, DRI entry for current IN
        IF(NHN is a reliable node) {
            Check IN  for black hole using DRI entry
        IF(IN is not a black hole)
            Route data packets(Secure Route)
        ELSE {
            Insecure Route
            IN is a black hole
            All the nodes along the reverse path
            from IN to the node that generated RREP are black holes
            }
        }
        ELSE
            Current IN=NHN
    } While(IN is NOT a reliable node)
}
```

Fig. 6 Modified AODV algorithm

V. SIMULATION

The proposed scheme have been carried out using the network simulator *ns-2*. The 802.11 MAC layer implemented in ns-2 is used for simulation. An improved version of random waypoint model is used as the model of node mobility.Performances of the three protocols are evaluated: (i) Standard AODV protocol, (ii) AODV with two malicious nodes cooperating in a blackhole attack, and (iii) AODV with the proposed algorithm.

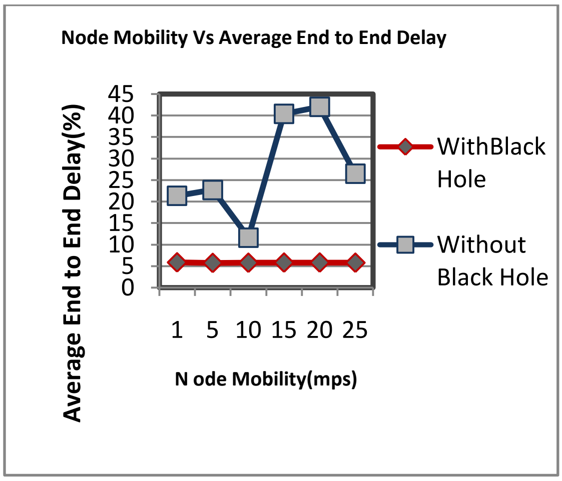


Fig.7 Average end to end delay Vs Node mobility

The scenarios developed to carry out the tests use one parameters ie. the mobility of the nodes.In Fig. 7 End to end delay is plotted against the mobility of the nodes. As compared to other solution this proposed work produce decreases end to end delay.In Fig. 8, packet delivery ratio is plotted against the mobility of the nodes. It is observed that AODV performs better for lower node mobility rates. The delivery rate starts dropping with increasing mobility of the nodes. The performance of the network significantly reduces when AODV is under the cooperative blackhole attack, and when the mobility of the nodes in the network increases.

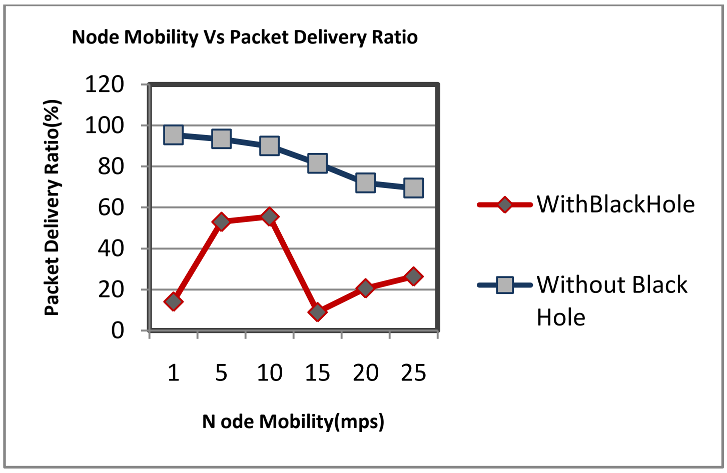


Fig.8 PDR Vs Node mobility

VI. CONCLUSION

In this paper, routing security issues in MANETs are discussed in general, and in particular the cooperative blackhole attack has been described in detail. A security protocol has been proposed that can be utilized to identify multiple blackhole nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the blackhole nodes. The proposed scheme has been evaluated by implementing it in the network simulator *ns-2*, and the results demonstrate the effectiveness of the mechanism. As a future scope of work, the proposed security mechanism may be extended so that it can defend against other attacks like resource consumption attack and packet dropping attack.

REFERENCES

[1] Sukla Banerjee(2008). Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks. The World Congress on Engineering and Computer Science.

[2]Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto(2007).Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. International Journal of Network Security, volume 5,Number 3,pp 338-346.

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

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

[5]Hesiri Weerasinghe (2007). Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, Volume 2, pp 362-367.

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

[7]Ravi Kumar Bansal and Anil Kumar Verma(2006). Performance Analysis of Cluster Based Routing Protocol in MANETs. MSc. thesis, Computer Science and Engineering Department Thapar Institute of Engineering and Technology (Deemend University), Patiala – 147004.

[8]AiffUmairSalleh, ZulkifliIshak, Norashidah Md. Din, and MdZainiJamaludin(2006). Trace Analyzer for NS-2, IEEE, Student Conference on Research and Development (SCOReD), Malaysia, pp. 29-32.

[9]Imran Khan and Professor Dr. Amir Qayyum(2009). Performance Evaluation of Ad Hoc Routing Protocol for Vehicular Ad Hoc Networks. MSc. Thesis, Mohammad Ali Jinnah University, Computer Science.

[10]N.Mistry,D.C.Jinwala and M.Zaveri(2010). Improving AODV protocol against black hole attacks. International multiconference of engineers and computer scientists, Hong Kong, vol 2.