International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 1 (February '2017)
Special Issue on 1st National Conference on Advanced Computing and Communication Technologies,
Conference held at Siri PSG Arts and Science College for Women, Sankari,Tamilnadu,India.

A DEFENSE MODEL FOR BLACK HOLE AND GRAY HOLE ATTACKS IN MANET USING CONTROL PACKETS

S.Radhika,
Research Scholar,
Department Of Computer Science,
Theivanai Ammal College for Women,
Villupuram,Tamilnadu,India.

N.Manohari,
Assistant Professor,
Department Of Computer Science,
Theivanai Ammal College for Women,
Villupuram,Tamilnadu,India.

Abstract: A Mobile Ad hoc Network (MANET) is a group of mobile nodes which cooperate in forwarding packets in a multi-hop fashion without any centralized administration. One of its key challenges is finding the malicious node in MANETs. In this paper we have proposed a scheme in which we are sending a control sequence to the neighbour nodes and we are expecting the nodes response. Based on the node response we can identify the malicious node.

Keywords: Control Sequence; MANET; Malicious node; Black hole; Network protocol; ABM

I. INTRODUCTION

Attacks in MANETs generally purpose and they are first is not to forward the packet or change the parameters of routing messages and to exhaust the battery of nodes by make them traversing the wrong packet in wrong direction and they also change the parameters of the packets such as sequence numbers and by using mechanism like authentication or cryptography as a preventive approach and can be used against attackers. By means of these mechanisms we can only prevent attacks from outside but not from inside any node inside by using this information can cause hazards in the network. This may lead to false positive detection of a non-malicious node. Another malicious behavior of the nodes is selfishness. Selfish nodes refrain from consuming its resources; such as battery, by not participating in network operations. Therefore failed and selfish nodes also affect the network performance as they do not correctly process network packets, such as in routing mechanism. We should, therefore ensure that everything is correctly working in the network to support overall security and know how an insider is able to attack the wireless ad-hoc network.The unique characteristics of ad hoc networks present a host of research areas related to security, such as secure routing protocols, instruction detection and trust based models. The most important concern for Mobile Ad-Hoc is the Security. Different types of attacks are applied in MANETs open medium, changing its topology dynamically and lack of central monitoring and management, no clear defense mechanism and cooperative algorithms. This

Mobile Ad-hoc Networks (MANETs) differ from existing networks by the fact that they depend on no fixed infrastructure. Nodes forming the network perform all functionality of the network with each node performs the functionality of both host and router.

Fig.1.1 A typical MANET

A MANET is introduced as an infrastructure less network simply because their mobile nodes in the network dynamically established routes along with them to transmit packets on a temporary basis. As a result of multihop routing and open working environment, MANETs are vulnerable and open to attacks by greedy or malicious nodes, these types of packet dropping (black-hole) attacks and exclusive forwarding (gray-hole) attacks. Yet another feature of a MANET is, moderate bandwidth, limited battery power. This attribute makes routing in a MANET an additionally more complicated task. Currently, several effective routing protocols have been projected. These types of protocols can be categorized into two classes: reactive routing protocols and proactive routing protocols. In reactive

routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol.

II. MOTIVATION

Today in communication world MANET is the very important part. MANET is also called Infrastructure less network. The information flow between source & destination. Currently wireless devices are achieved via infra-structure based fix service provider, or private networks. For example laptops are connected to Internet through access points. Infra-structure based network takes time and cost setup. In geographic area networking connection is not available. So in this condition connection and services becomes big problem. For all reason we capture all mobile devices which are connected to each other in the transmission radio wave range using automatic configuration in the ad hoc network that is both flexible and powerful.Applications of ad hoc network range from military operations and emergency disaster relief to interaction between attendees at a meeting and students during a lecture. These types of applications demand a secure and reliable communication. This type of networks is generally more vulnerable to information and physical security threats than fixed wired networks. Vulnerability of nodes and absence of infrastructure and dynamically changing topology make ad hoc networks security a difficult task. Broadcast wireless channels allows message eavesdropping. Nodes do not reside in physically protected places and they can easily fall under the attacker's control. The absence of infrastructure makes the classical security solutions based on certification authorities and on-line servers inapplicable. The security of routing protocols in the MANET dynamic environment is an additional challenge.

III.RELATED WORKS

Deng et. Al. [6] has recommended an algorithm in order to minimize black hole attacks in ad hoc networks. Based on to their algorithm, any kind of node on obtaining a RREP packet, cross examinations using the next hop on the route to the desired destination coming from a different path. If the next hop choose to doesn't come a link to the node that delivered the actual RREP or possibly doesn't come a route to the desired destination then this node that sent the RREP is viewed as malicious. This particular strategy is not effective when the malicious nodes collaborate with each other. S.Ramaswamy et. al. [7] introduced an algorithm to preclude the cooperative black hole attacks in ad hoc network. This algorithm is dependent holding a faith commitment regarding the nodes, so because of this it can't deal with gray hole attacks. Besides due to the fact intensive cross checking, the algorithm requires extra time in order to complete, even though the network is not under attack. S.Banerjee et. al. [8] has also projected an algorithm for discovery & elimination of Black/Gray Holes. In accordance with their algorithm on the other hand of transmitting the entire data traffic at one time, they break down it into moderate sized blocks, in the desire that the malicious nodes can be recognized& eliminated in the middle of transmission. Stream of traffic is evaluated and monitored by the neighbours of each and every single node. Source node makes use of the acknowledgment delivered by the destination to examine for the data loss & in turn examines the opportunity of a black hole. Nonetheless in this mechanism mendacious positive aspects could happen along with the algorithm may report that a node is behaving inappropriately, when in fact it is not.

In the end P.Agarwal et. al. [9] have projected an approach concerning implementing a backbone network of intense nodes. Together with the help of the central source network of intense nodes, source and destination nodes possess out an end to end verifying to discover in case any type of data packets arrived at the destination. If verifying produces a failure, then the anchor network leads to a protocol for detection the malicious nodes. We have used this principle of backbone nodes & organized an algorithm that is much simpler. We have also made use of the principle of state full method of IP addresses assignation in ad-hoc networks as talked about by S.Indrasinghe et. al.[10] and Mansoor Mohsin et. al.

A. Black and Gray hole attack

Black hole attack interrupts along with the routing protocol by confusing many other nodes regarding course-plotting information. A black hole node does work through the following pyramid scheme: as soon as obtaining RREQ and RREP messages, the assailant responses RREP messages exclusively and also claims that it is the getaway node. The source node is most likely to acquire a pseudo-RREP coming from the assailant just before the real RREP comes back. Underneath these types of ailments, this source node transmits info packets to the black hole as an alternative of the destination node. When the source node sends data packets by using the black hole, the assailant discards all of them without

sending back a RERR message. As for gray hole, its exercises are like a black hole.

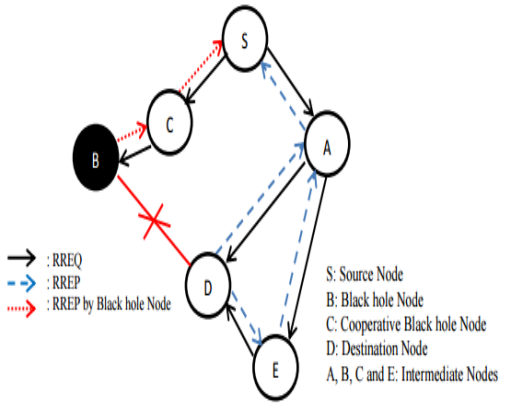

Fig. 2: Black hole Attacks in Mobile Ad hoc Network

A gray hole does not shed all the data packets except just simply part of packets. The Gray Magnitude is described once the proportion of the packets which are maliciously dumped by an assailant. For instance, a gray hole is gray magnitude of 60% will likely shed a data packet with a possibility of 60% and a classical black hole has a gray magnitude of 100%. The black and gray hole attack will bring great damage to the performance of Ad Hoc network. The malicious drop rate is defined by the ratio of dropped packet number and received packet number. Especially, the malicious drop rate of a black hole is 100%.

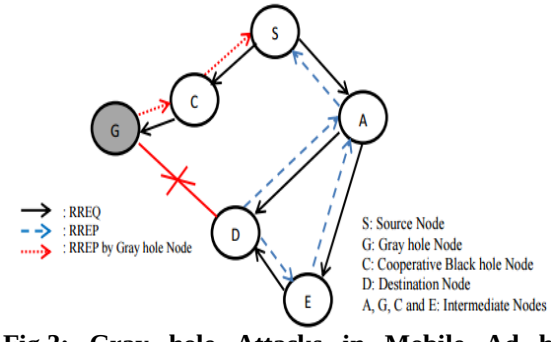

Fig.3: Gray hole Attacks in Mobile Ad hoc Network

IV. PROPOSED APPROACH

In the existing AODV Routing protocol we have beenintroducing two packets which are Response sequence (Rseq) packet and Code Sequence Packet (Cseq). These packets are transmitted in the AODV-MAC layer when a node wants to access the channel. Each intermediate node sends the Cseq to all its neighbours then neighbours intern send their Rseq to the intermediate node. If the Cseq and Rseq matches from the neighbour then the Intermediate node allow the connection to the network layer, Otherwise, it discard the node and send the information to all other nodes that particular node as malicious one.

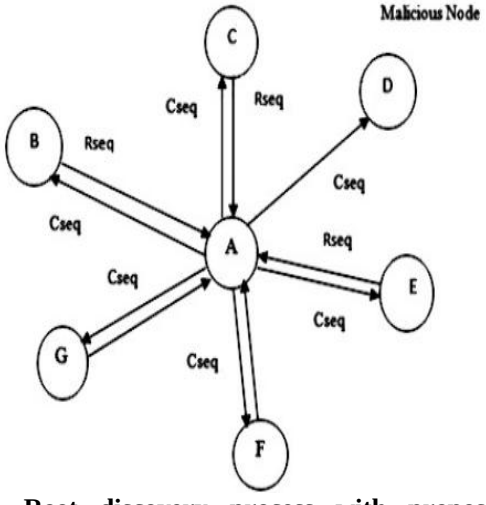

Fig.3. Root discovery process with proposed approach.

It checks the fix value of sequence packet in the Code sequence table. If seq packet is match with respective Cseq packet than the Rseq packet is accepted; otherwise it is discarded. Figure 1 shows the route discovery process in AODV in the presence of a malicious node D. Source node A broadcasts Code sequence packet (Cseq) within its communication range, B,C,E,F and G receive the Cseq packet and re-broadcasts Cseq to their neighbors until a node having a valid route. Each node sends Rseq packet to the source node on the reverse path of Cseq. The malicious node D sends Rseq to the source but source node check it with the Cseq packet then the result comes different.The Proposed method is used to prevent the malicious node and find the secured routes in the MANETs by using the criteria as follows. If there is large difference between the Cseq of source node and Rseq of neighbor or intermediate node who has sent back Rseq or not. Generally the first route reply will be from the malicious node with high destination sequence number. Which are stored in the first entry of Cseq-Table. Then compare the destination Rseq with the Cseq in the table.

4.1 Malicious node finding algorithm

Algorithm: Cseq and Rseq Method

Parameters: DS-ID – Destination Sequence ID, NID – Node ID, MN-ID – Malicious Node ID, SS-ID Sending Sequence ID.

Step 1: Initialization Process

Start the route discovery phase at source node A.

Step 2: Storing Process
Store all the Route Replies DS-ID and NID in Cseq Table.
Step 3: Identify and Remove Malicious Node.
Retrieve from Cseq Table
If DS-ID is much greater than SS-ID then discard entry from Cseq Table as Select DS-SID from table.
If (DS-SID>= SS-ID)
{
Malicious Node = Node Id
Discard entry from table
}
Step 4: Node Selection Process
Sort the contents of Cseq Table entries according to the DS-ID. Select the NID having highest DS-SID among RR-table entries.
Step 5: Continue default process.
Call Rseq method of default AODV Protocol. This is how malicious node is identified and removed from the network and the routing table for that node is not maintained.

4.2 Advantages of proposed algorithm

The malicious nodes are identified at the initial stage itself and immediately removed so that it cannot take part in further process. With no delay the malicious node is easily identified therefore we said before all the routes has unique sequence id. Normally the malicious node has the highest Destination Sequence id and it is the first Rseq to arrive. So the comparison is made only to the first entry in the table without checking other entries in the table.

V. PROPOSED DEFENSE MODEL

The proposed defense model for Black hole and Gray hole attacks provides the framework for developing a complete solution to combat against the different types of Black hole and Gray hole attacks possible in the MANET. The technique developed using this model not only addresses all these attacks but also provides reliable data transmission in the network. This model considers weaknesses of prominent reactive routing protocols and prevention and/or detection mechanisms for Black hole and Gray hole attacks and provides steps by step procedure to develop a robust solution. The proposed model comprises of four modules which are to be followed when developing the solution. The modules of the model are 1. Adversary Evasion 2. Adversary Recognition 3. Route Maintenance and 4. Data Restoration. Each of these modules is described below. A. Adversary Evasion B. Adversary Recognition C. Route Maintenance D. Data Restoration.

A. Adversary Evasion

This is the first module of the model in which an elimination mechanism is used to avoid the Black hole and Gray hole nodes from participating in the route discovery process. This is the first line of defense to the system. To prevent the malicious nodes from route discovery process the technique needs to have the knowledge of previous misbehaved nodes with certain rating value indicating its level of severity.

B. Adversary Recognition

This the second line of defense where a strong detection mechanism is used to find out the malicious node/nodes misbehaving during the data forwarding phase. The detection mechanism to find out the malicious node, it should not depend on the information collected from intermediate nodes adjacent to the malicious node because adjacent nodes collude to carry out a cooperative attack, which is hard to detect. It should confirm the data packet transmission by collecting the information from the destination node only. The detection mechanism requires continuous monitoring of malicious nodes because a gray hole toggles its behavior between honest and malicious. Once the malicious nodes are identified they must be blacklisted so that they will not be allowed to participate during the route discover process in the future. Therefore a detection mechanism must have two important processes i.e. first process is to identify the malicious nodes and second process is to blacklist the malicious nodes associating a rating value to them so that these rating values can be compared with a threshold value at the time route discovery process and decide whether to allow or reject the nodes in the routing process.

C. Route Maintenance

This is the next module which involves finding a new path for the remaining data transmission. After detecting the malicious node/nodes on the path, it is informed to the source node. Source node stops sending data packets and checks out its route cache for an alternative path with highest rating value if available otherwise finds a new path by initiating route discovery process. In this route discovery process previously detected malicious nodes are avoided so that the new path found will not contain suspected malicious nodes.

D. Data Restoration

The lost data packets are identified by source node with help of the destination node confirmations

received. In the case of Black hole attack, source node requires to start the data transmission from the first packet onwards and in the case of Gray hole attack, lost packets need to be identified and resend only the lost packets to the destination node. Next it continues with the remaining data transmission. Thereby all the packets from source node to destination node are transmitted reliably and securely.

VI. SIMULATION PARAMETERS AND MEASURED METRICS

The proposed scheme has been carried out using the network simulatorNS-2. The 802.11MAC layer implemented inNS-2is used for simulation. In the first scenario where there is not a Black Hole AODV Node, connection between Node 5 and Node 4 is correctly flawed when we look at the animation of the simulation, using NAM. Figure 4 shows the data flow from Node 2 to Node 5. When the Node 1 leaves the propagation range of the Node 2 while moving, the new connection is established via Node 3. The new connection path is shown in Fig. 5. Figure 6 shows how the Black Hole AODV Node absorbs the traffic. To figure out how the second packet came to source node, we created a simulation scenario with node positions shown in Fig. 7. In the scenario, Node 0 is the sending node, Node 1 is black hole node and Node 5 is the receiving node.To figure out how the second packet came to source node, we created a simulation scenario with node positions shown in Fig. 7. In the scenario, Node 0 is the sending node, Node 1 is black hole node and Node 5 is the receiving node.

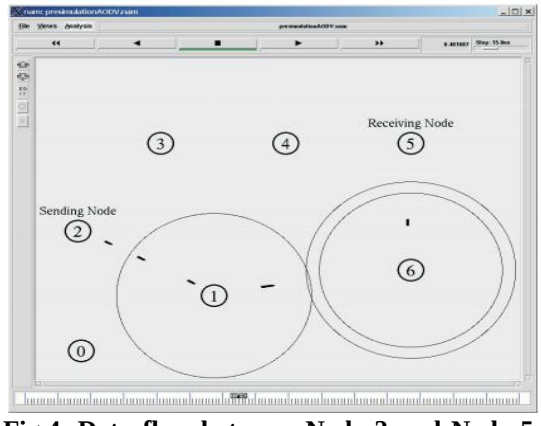

Fig.4. Data flow between Node 2 and Node 5 via Node 1 and Node 6.

An improved version of random way point 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. The scenarios developed to carry out the tests use one parameters i.e. the mobility of the nodes. 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. In Fig. 9 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. 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.

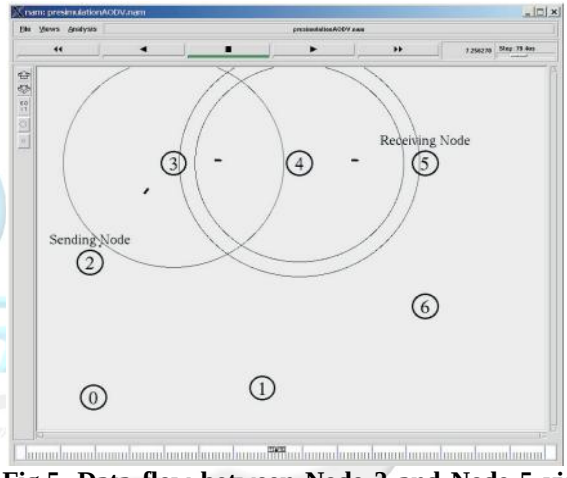

Fig.5. Data flow between Node 2 and Node 5 via Node 3 and Node4.

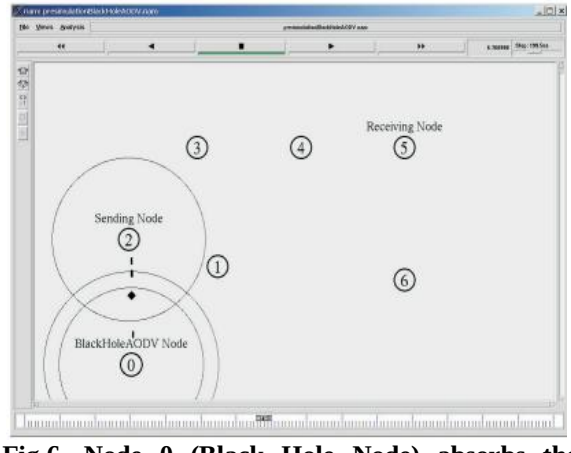

Fig.6. Node 0 (Black Hole Node) absorbs the connection Node 2 to Node 5.

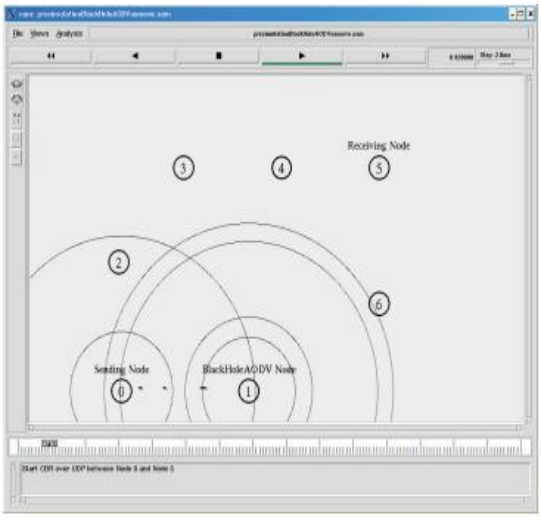

Fig.7. Test simulation to show two RREP message.

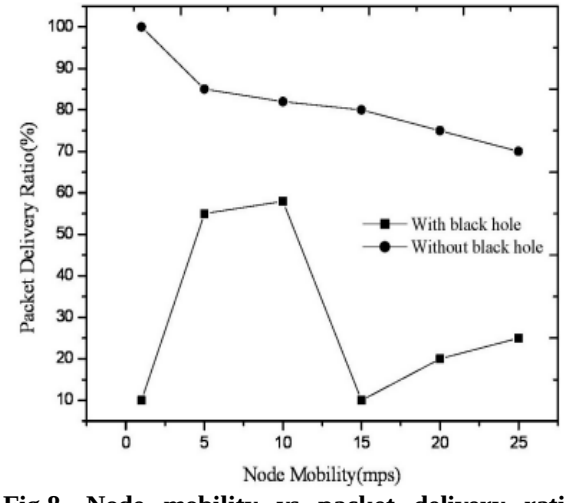

Fig.8. Node mobility vs packet delivery ratio (PDR).

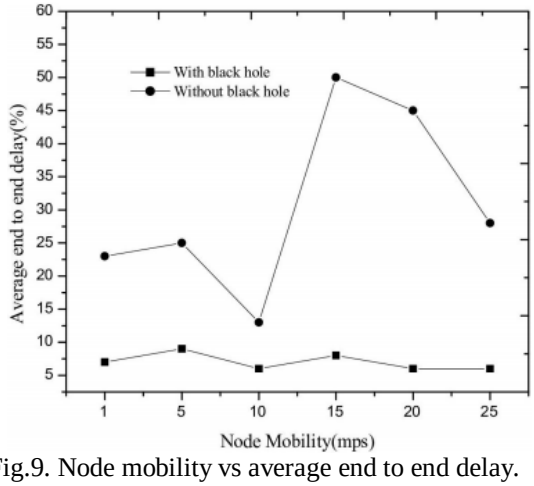

Fig.9. Node mobility vs average end to end delay.

VII CONCLUSION

Malicious behavior of the nodes effects network performance severely. Hence providing security in presence of these malicious nodes is the major constraint for deployment of the MANET. In this paper different types of Black hole and Gray hole attacks and various methods proposed to detect and/or prevent these attacks for most prominent routing protocols are discussed and proposed a novel approach to counter these attacks that efficiently finds short and secure route to the destination. The theoretical analysis shows that our approach would greatly increase PDR with negligible difference in routing overhead. The algorithm is equally applicable to other reactive protocols. There are various solutions proposed to address Black hole and Gray hole attacks but there is no one complete solution which addresses different varieties of Black hole and Gray hole attacks and provides a reliable, secure and efficient mechanism. The proposed model can be used to develop a technique that gives a complete solution to address these attacks and makes the data transmission reliable. Therefore the future work is to develop and implement a mechanism using this proposed defense model.

REFERENCES

[1]. C. Siva Ram Murthy and B. S Manoj, Ad Hoc Wireless Networks, Architecture and Protocols,Prentice Hall PTR, (2004).

[2]. Stefano Basagni, Macro Conti, Silvia Giordano and Ivan Stojmenovic, Mobile Ad Hoc Networks. IEEE Press: A John Wily & Sons INC.,(2003).

[3]. George Aggelou, Mobile Ad Hoc Networks, 2nd Edition:Mc GRAW Hill Professional Engineering, (2004).

[4]. ImrichChlamtac, Marco Conti and Jenifer J.-N. Liu, Mobile Ad Hoc Networking: Imperatives and Challenges,Elsevier Network Magazine, vol. 13, pp. 13–64, (2003).

[5]. E. M. Belding-Royer and C. K. Toh, A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks,IEEE Personal Communications Magazine, pp. 46–55, (1999).

[6]. Banerjee, S. Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks, In Proceedings of the World Congress on Engineering and Computer Science, (2008).

[7]. S. Jain, M. Jain and H. Kandwal, Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in

Mobile Ad Hoc Networks,J. Computer Applications, vol. 1(7), pp. 37–42, (2010).

[8]. Agrawal, P., Ghosh, R. K. and Das, S. K.. Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks,In Proceedings of the 2nd pp. 310–314, (2008).

[9]. Baadache and A. Belmehdi, Avoiding Black Hole and Cooperative Black Hole Attacks in Wireless Ad Hoc Networks, J.Comp.Sci.and Info. Security, vol. 7(1), pp. 10–16, (2010).

[10]. H. Weerasinghe and H. Fu, Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks, Int. J. of Soft. Eng. and Its App., vol. 2(3), pp. 39–54, (2008).

