2013 27th International Conference on Advanced Information Networking and Applications Workshops

GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs

Sanjay K. Dhurandher[1], Isaac Woungang[2], Raveena Mathur[1] and Prashant Khurana[1]
[1]CAITFS,Division of Information Technology
Netaji Subhas Institute of Technology, University of Delhi, New Delhi, India
E-mail: dhurandher@rediffmail.com,raveenamathur91@gmail.com,
prashantkhurana145@gmail.com
[2]Department of Computer Science
Ryerson University
Toronto, Canada
E-mail: iwoungan@scs.ryerson.ca

Abstract— MANETs are best suited for emergency situations as they facilitate fully distributed, self maintainable dynamic topology networks that operate without the use of external infrastructure. But the proliferation of such MANET based applications is limited as its features though impart high applicability but also manifest unreliability. Another cause of unreliability is the mutual intrinsic trust during communication. One such attack exploiting this trustworthiness is called the Black Hole attack wherein the Black Hole in the network promises routing of the data packet to the destination while in actuality it drops them hence decreasing reliability.

In this paper we therefore analyse MANETs under single and collaborative Black Hole attack and prevent it by diverting traffic from the Black Hole. The MANETs so discussed employ the AODV routing protocol and the method so proposed is based on sending confirmation packets that are verified by the destination to check for Black Hole presence in the GAODV routing protocol so proposed. The GAODV algorithm was then simulated in both static as well as mobile node environment and it was observed that its data delivery ratio is significantly better than the conventional AODV.

Index Terms— Black Hole, Collaborative Black Hole, AODV, MANETs, security, routing.

I. INTRODUCTION

A MANET is a self-configuring, distributed, dynamic network in which the nodes are mobile and communication is not via fixed access points. Since they act as open medium any node in space can be a part. Manets have a huge applicability potential as they have the potential to be anywhere anytime.[1]

Although the features of MANETs attract huge applicability, they also manifest vulnerability. This vulnerability to attacks imposes unreliability, a condition that cannot be compromised especially in emergency situations. There are a variety of attacks that the MANETs are exposed to. These attacks can be classified as active and passive attacks. In active attacks the adversary breaks into the system and is able to insert and capture transmissions thus modifying or corrupting the data whereas in passive attacks the adversary merely listens to the traffic and extracts information from the transmissions.The increasing rate and extent of black hole attacks raise concerns for a defensive mechanism that has the properties of being preventive as well as curative. Therefore this paper is an attempt to defend against ”Black hole” attack that compromises reliability of the networks by dropping all data packets routed towards them.

The organization of this paper is as follows. Section II describes the AODV protocol and Black Hole attack, section III describes the various approaches proposed till date to handle this attack, section IV explains the proposed algorithm, section V provides the simulation results along with comparison to basic AODV protocol and section VI provides the conclusion and discusses the future research options.

II. AODV AND BLACK HOLE ATTACK

A. AODV: An overview

AODV[2] stands for Ad-Hoc on Demand distance Vector Routing algorithm. It is an algorithm that initiates the route discovery only on demand, that is, a route is discovered whenever a route is needed for communication. It uses the following control packets in the process of route discovery:

1) RREQ: Route Request
2) RREP: Route Reply
3) RRER: Route Error

B. Black Hole Attack: Single and Collaborative

Black Holes are malicious nodes that exploit the following features of AODV:

1) AODV does not perform authentication of a new node during it’s entry in a MANET.
2) It does not verify the route promised by any node.

Black Hole node’s motive is to divert all the data traffic in the network toward itself. In order to do so, Black Holes send RREP’s to the source node with the least hop count or highest sequence numbers. Since Black Holes do not search their routing tables before generating a reply, they usually are the quickest. Thus, the RREP packet so received from the black hole is usually the first and appears to bear the latest

978-0-7695-4952-1/13 $26.00 © 2013 IEEE
DOI 10.1109/WAINA.2013.168

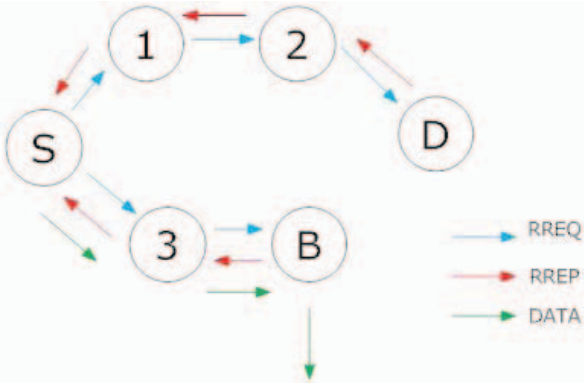

Fig. 1: Black Hole Attack. S(source) receives RREP from B(black hole) and starts sending data which is dropped by B and never reaches D(destination).

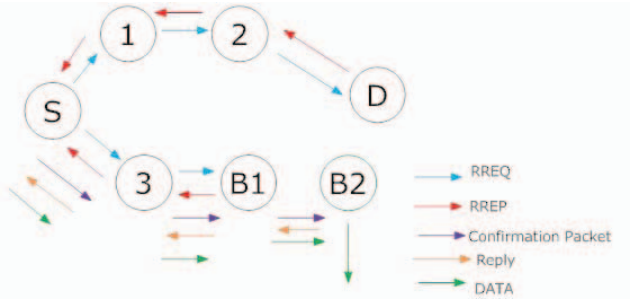

Fig. 2: Collaborative Black Hole Attack. S(source) recieves RREP from B1(black hole) along with the next hop(B2) information and sends a confirmation packet to B2(black hole) which replies in affirmation and hence S begins sending data which gets dropped by B2.

network configuration, causing the source to route towards the Black Hole. The Black Hole node finally drops these data packets.

Black Hole attacks can be independent, that is, performed by a single node or can be collaborative. In collaborative attack, when multiple Black Hole nodes are acting in coordination with each other, B1 sends the RREP and specifies the route through B2 as shown in Fig.2. When B2 is asked by the source for the verification of a route to the destination through it, it responds in conformity while in actuality it does not have the route. The packets are then routed by the source, just to be dropped by the node B1 or B2.

III. Related Work

A number of solutions to handle the black hole attack have been proposed in [3].In [4] Deng et al. proposed a method based on verifying the existence of a path from the next hop node (to the rrep sending node).The method was suitable for single black hole detection only.

In [5](S. Ramaswamy et al.) used the 'THROUGH' and 'FROM' bit in the DRI table to detect the collaborative Black Hole Chains. However, their approach uses redundant bit transmissions of 'THROUGH' bits.

Another method proposed by Al-Shurman et al. [6] utilised the network redundancies to find out the safe route (that is the one which is not black hole struck). The algorithm, however, suffered form a huge time delay, unnecessary when the path is not black hole struck.

Another significant algorithm was presented by Aggarwal et al. [7], where a backbone network was used to identify black hole chains. The back bone network was instructed by the source to do the black hole route discovery only when the destination is unable to receive the packets it transmitted.

IV. Proposed Algorithm:The GAODV Protocol

A. Terminology Used

1) *S*: Source Node
2) *D*: Destination node
3) *IN*: Intermediate Node
4) *RREPN*:The node that sends an RREP to source
5) Packets apart from the ones used in AODV are as follows:
   a) *CONFIRM*: Sent by RREPN to destination
   b) *CHCKCNFRM*: Sent by source to THE destination on receipt of RREP
   c) *REPLYCONFIRM*: Sent by destination to the source on receipt of CHCKCNFRM
6) Tables used apart from the ones used in AODV are as follows
   a) *Confirm Table*: For every CONFIRM packet received destination stores the following:
      i) Source Node Address
      ii) RREPN Node Address
   b) *ReplyConfirm Table*: For every CHCKCNFRM packet the source stores the following :
      i) The Destination Address from which it expects a reply confirm.
      ii) The RREPN Address of the node that sent the first RREP
   c) *BlackHole Table*: possessed by every node and it stores the following
      i) Node Address of the black hole nodes.
   d) *Collaborative BlackHole Table*: possessed by every node and it stores the following:
      i) Node Address of the collaborating black holes

B. Working Principle

The AODV protocol has a provision of sending a gratuitous RREP packet to the destination node. Whenever an intermediate node has a route towards destination, in addition to sending the RREP to the source, it also unicasts a gratuitous RREP to the destination node. In our protocol the gratuitous RREP is conceptualized and simulated as the CONFIRM packet. Thus, a CONFIRM packet is unicasted/routed by the RREPN to the destination. Note that it can be sent only if the RREPN has a route towards

1)S sends RREQ;
2)RREPN replies with RREP;
if *RREPN not a BlackHole* then
  RREPN Sends CONFIRM Packet to D via the route for D;
end
3)S receives RREP;
if *RREPN in BlackHole Table* then
  Discard RREP;
end
else if *RREP from IN* then
  Send CHCKCNFRM packet to D via route advertised by RREPN;
end
else
  route data;
end
4)IN recieves CONFIRM;
if *IN is not a BlackHole* then
  relay CONFIRM;
end
else
  drop CONFIRM;
end
5)D receives CONFIRM;
broadcast REPLYCONFIRM;
6)if *S receives receives REPLYCONFIRM before timeout* then
  route data;
end
else
  store RREPN in Black Hole table;
  retry RREQ;
end

Algorithm 1: Algorithm For Black Hole

destination. It is only after the receipt of CONFIRM will the destination await for packets from the source. In order to facilitate cross checking by the source (of the route claimed by the RREPN), the source unicasts a CHCKCNFRM to the destination. Upon CHCKCNFRMs receipt the destination replies by broadcasting a REPLYCONFIRM to the source, only if it received a CONFIRM and a CHCKCNFRM. Since a black hole does not possess a route towards the destination, it fails to send the CONFIRM, thus reply to the CHCKCNFRM is never generated by the destination. This leads the source to conclude that the RREP sending node was the black hole one.

The proposed algorithm will hereafter be called as the G-AODV protocol. It gets its name from the utilization of the gratuitous RREP.

C. Working with Single Black Hole Attack

1) Suppose S wants to send data to D and RREPN has a fresh route towards D.
2) So RREPN will generate a RREP with a new field as sender's address(that is, its own address) and unicast it to S .
3) Also RREPN sends a CONFIRM packet to the destination node containing the source address, destination address and its own address.
4) Now when S receives the RREP it will unicast a CHCKCNFRM(containing the RREPN address, destination address and its own address) packet to D via the route suggested by RREPN.
5) While doing so, it will activate a timer to wait for a reply by D.As CHCKCNFRM packet is forwarded the forwarding nodes also activate a timer to receive a reply from D.
6) When D gets the CONFIRM packet from RREPN, it stores its contents in a confirm table for REPLY-CONFIRM generation. When D receives the CHCK-CNFRM packet from S it looks up in the table to see if it got any CONFIRM packet with matching source ID and sender ID.
7) If yes, it sends a REPLYCONFRIM packet. Although a route existed from the destination to the source, yet the REPLYCONFIRM packet is not unicasted. This is so because unicasting will increase the REPLYCONFIRM packet size as it will now contain hop count, lifetime etc.
8) In case of a black hole no REPLYCONFRIM will reach the source as no CONFIRM packet was sent, also because CHCKCNFRM was not forwarded, hence the timer will go off and S will mark RREPN as a black hole. Otherwise, if REPLYCONFRIM is received the source begins routing data.

TABLE I: Check Table

Node ID	ID of the node
Relay Value	0 if it did not relay the CHCKCNFRM and CONFIRM 1 if it relayed the CHCKCNFRM and CONFIRM

D. Working with Collaborative Black Hole Attack

The working of this algorithm is similar to the algorithm presented before. The difference, however, starts to develop after step 5, after which each intermediate node that had received CONFIRM and now has received CHCKCNFRM replies back with a REPLYCONFIRM. A modified RE-PLYCONFIRM packet is used which contains the next hop address to which it is relaying CHCKCNFRM packet. In addition, this algorithm has an additional table called the check table maintained by the source node. This check table has 2 fields , i.e., Node id and Relay value.The Node id field contains the id's of all the nodes that act as intermediate nodes in the route claimed by the RREP sending node. The default value of the relay value field is 0, indicating no CHCKCNFRM and CONFIRM have been relayed by it. They are updated to a value 1 for the previous node id each time REPLYCONFIRM is received from the next intermediate node. Initially the table has the only entry of RREPN i.e RREP sending node, with relay value as 0. As

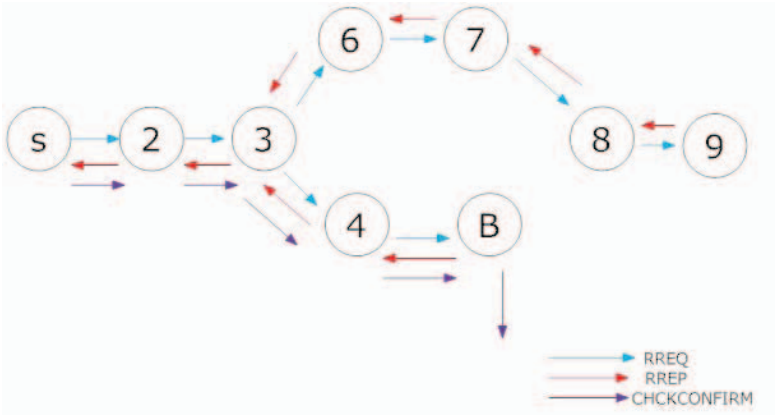

Fig. 3: Working with Single Black Hole Attack. As S receives RREP from B(black hole) it sends a CHCKCNFRM packet to which it gets no response and hence marks B as a black hole and next time will not consider the RREP from B.

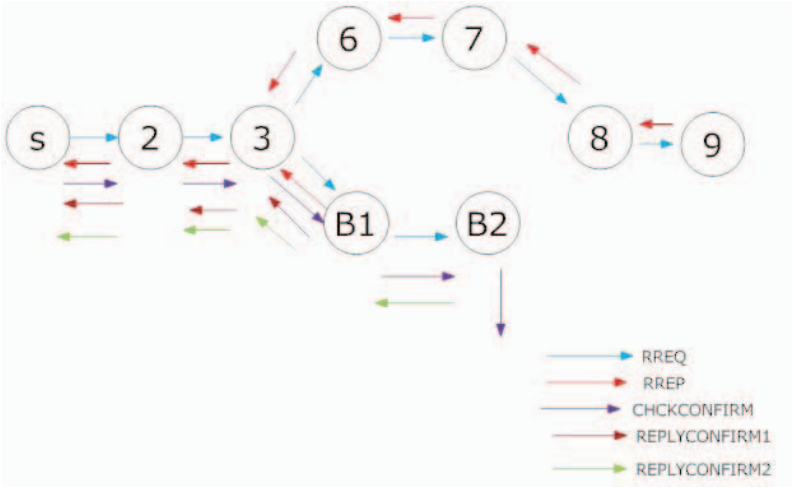

Fig. 4: Working with Collaborative Black Hole Attack. As we receive REPLYCONFRIM from only B1 and B2, it shows that they are acting in collaboration.

the source receives REPLYCONFRIM from the next hop of RREPN, it sets the relay value of RREPN as 1. This process is continued for other nodes that send REPLYCONFIRM. Now, the source expects REPLYCONFRIM from destination as well. After waiting for a specified time, if the source does not receive a REPLYCONFRIM from the destination, it adds to its Black hole Collaboration table all the nodes starting from the RREP sending node to the first node id with relay=0, to be working in collaboration with each other. This check table is deleted from time to time, i.e., before the beginning of a new routing.

E. Enhancements suggested over GAODV

1) Handling the gray hole attack: There is a trade off so as to whether broadcast the black hole table after detection or not. Broadcasting the Black Hole table has an advantage that since all the nodes know all the Black Hole node addresses discovered so far, any RREP packet so received from the Black Hole will be discarded, hence reducing the network traffic and computation time significantly. But this also has a disadvantage as if a Black Hole is node selective, that is, can alternate between a Black Hole and normal node, then for the other routes where it was not acting as a Black Hole there also it will not be used to send data packets.To detect such black holes,the black hole table should table should not be broadcasted. These node selective black hole nodes can are a type of gray hole nodes.
2) As mentioned in section 4 subsection C point 7 of the paper, we are broadcasting the REPLYCONFIRM. In cases where network traffic is an issue as against the increase of packet size, we unicast the REPLYCONFIRM by adding the necessary fields of hop count, next hop, etc.

V. Simulation Graphs and Analysis

A. Methodology of Evaluation

1) Simulation Environment: For the simulation, we use glomosim network simulator [8]. At the MAC layer, the

1)S sends RREQ;
2)RREPN replies with RREP;
if *RREPN not a BlackHole* then
  RREPN Sends CONFIRM Packet to D via the route for D;
end
3)S receives RREP;
if *RREPN in BlackHole Table* then
  Discard RREP;
end
else if *RREP from IN* then
  Send CHCKCNFRM packet to D via route advertised by RREPN;
end
else
  route data;
end
4 if *IN receives CHCKCNFRM and had received CONFIRM* then
  IN unicasts (on the same route as CHCKCNFRM) REPLYCONFIRM to the source;
end
5 if *S receives REPLYCONFIRM from IN* then
  checks in its checktable and updates checktable and Stores appropriate relay values ;
end
6 if *S receives REPLYCONFIRM from D and S doesnt time out* then
  Deletes check table;
  Routes the data;
end
else
  process checktable;
  stores in collaborative Black Hole list the IDs of nodes starting From RREPN uptil all the nodes until relay value 0 reached;
  Retry RREQ;
end

Algorithm 2: Algorithm For Collaborative Black Hole

IEEE 802.11[9] was implemented. The channel is Wireless Channel with Two Ray Ground radio propagation model. At the network layer, we use AODV as the routing algorithm. Finally, UDP is used at the transport layer. The packet traffic is CBR.

B. GRAPHS AND ANALYSIS

1) Static Topology: In this case the network topology of figure 3 is used In all the cases the source is 1 whereas the destination is 8. The simulation parameters are set to the values as shown table 2:

1) Average End to End Delay versus number of Black Holes(figure 5)-When there are more than 1 black holes in the route, the end to end delay rises because of an overhead of 3 packets.

TABLE II: Simulation Parameters

Number of Nodes	10
SIMULATION-TIME	15M
TERRAIN-DIMENSIONS	(2000, 2000)
PROPAGATION-LIMIT	-111.0
NOISE-FIGURE	10.0
TEMPARATURE	290.0
RADIO-FREQUENCY	2.4e9
RADIO-TYPE	RADIO-ACCNOISE
RADIO-BANDWIDTH	2000000
RADIO-TX-POWER	15.0
MAC-PROTOCOL	802.11
NETWORK-OUTPUT-QUEUE-SIZE-PER-PRIORITY	100

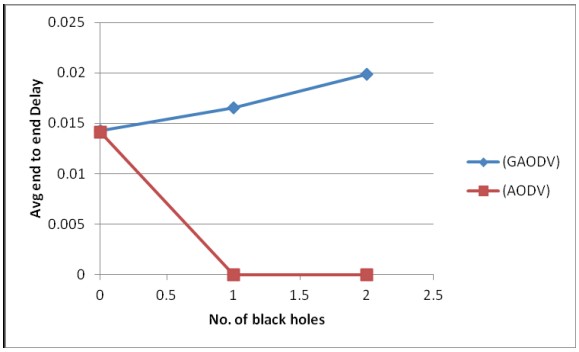

Fig. 5: Average End to End Delay versus number of Black Holes

2) Data Delivery Ratio(DDR) versus Inter packet delay(figure 6)-Inter packet Delay is the time difference between 2 consecutive packets sent by the source from the application layer. Our protocol is able to detect Black Holes and thereafter successfully divert all the traffic from it, hence a DDR of 1.With AODV, however, all data is routed through the Black Hole and hence no data reaches the destination giving a DDR of 0.

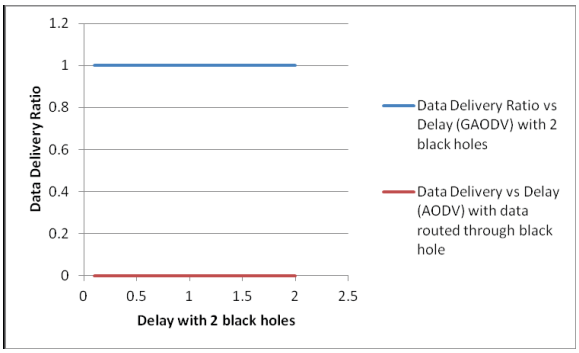

Fig. 6: Data Delivery Ratio(DDR) versus Inter packet delay

2) Mobile Topology: The simulation parameters which are changed are set to the values as shown in table 3:

1) Average End to End Delay with Max mobility Speed(figure 7)-In this case as we vary the maximum mobility speed of nodes(in m/s), we find the Average

TABLE III: Simulation Parameters

Number of Nodes	36
Node Placement	Grid

end to end delay increases. This is because, the links between nodes break as the nodes move with fast speed. At lower speed the delay of GAODV and AODV is similar(difference of 0.00004) and this difference increases as the speed increases.

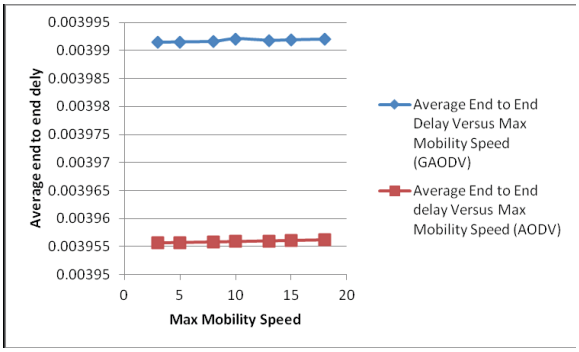

Fig. 7: Average End to End Delay with Max mobility Speed

2) Data delivery Ratio versus Number of Black Holes(figure 8)-The graph shows that the data delivery ratio of our protocol is very high(0.9 approximately) in presence of Black Holes, hence proving that we are successful in detecting the black hole and diverting all the data from it.

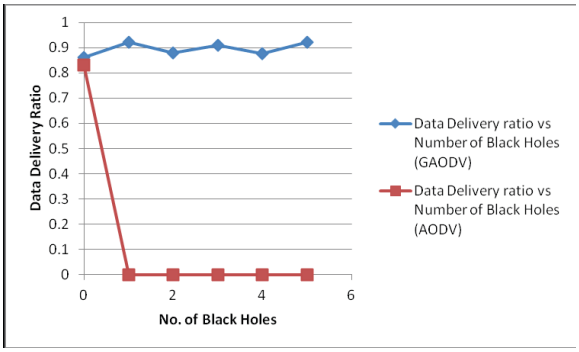

Fig. 8: Data delivery Ratio versus Number of Black Holes

3) Data delivery Ratio versus maximum mobility speed(figure 9)-Owing to the rapidly changing changing network topology the data delivery ratio decreases as maximum mobility speed(in m/s) increases. No significant difference in Data Delivery ratio is observed between the proposed protocol (in presence of 2 Black Holes) and AODV without any Black Hole.

VI. Conclusion and Future Work

In this paper, with the control packets called CONFIRM, CHCKCNFRM and REPLYCONFIRM, we have been able to detect the presence of Black Hole and hence successfully

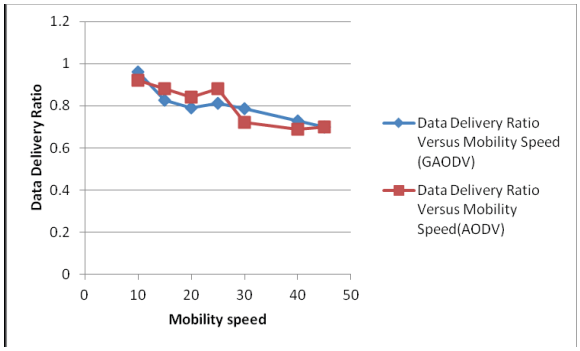

Fig. 9: Data delivery Ratio versus maximum mobility speed

diverted all the traffic from it. As explained, a slight modification in the protocol shows that a single run of the algorithm can detect the presence of collaborative Black Hole chains. Also with slight modifications in our method we are able to detect time varying and target varying Black Holes called the gray Holes. Simulation results also show that our algorithm is packet traffic efficient as well as time efficient as it produces 90 percent DDR for dynamic topology with an end to end delay, 0.9 times greater than that of conventional AODV.

As a part of our future endeavour we aim to study the processing time the Black Holes take, to analyse their behaviour further. Also we would work upon decreasing the number of packets transmitted per route in our algorithm. A simulation to detecting the Black Hole chains will also be done hereafter.

References

[1] I. Chlamtac, M. Conti, J. Liu, "Mobile ad hoc networking:imperatives and challenges, Ad Hoc Networks", pp. 13-64, 2003.

[2] C Perkins, E Belding-Royer and S Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", Internet RFCs Volume: 1, Issue: 3561, Publisher: IETF, Pages: 1-38,2000.

[3] Fan-Hsun Tseng, Li-Der Chou, Han-Chicj Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences, 2011.

[4] Deng H., Li W. and Agrawal, D.P., "Routing security in wireless ad hoc networks," Communications Magazine, IEEE , vol.40, no.10, pp. 70- 75, October, 2002.

[5] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, Proceedings of 2003 International Conference on Wireless Networks (ICWN03), Las Vegas, Nevada, USA, pp. 570-575.

[6] Al-Shurman, M., Yoo, S. and Park, S., "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004.

[7] Piyush Agrawal, R. K. Ghosh and Sajal K. Das, "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks", proceedings of the 2nd international conference on Ubiquitous information management and communication, pp. 310-314, Suwon, Korea, 2008.

[8] Xiang Zeng, RajiveBagrodia, Mario Gerla, GloMoSim: a Library for Parallel Simulation of Large-scale Wireless Networks, Proceedings of the 12th Workshop on Parallel and Distributed Simulations PADS 98, May 26-29, 1998.

[9] L. M. S. C. of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Standard 802.11, 1999.