Performance Analysis of Mobile Ad-Hoc Networks Protocols Under Black Hole Attack

Jaskiran Kaur

P.G. Dept. Computer Science & IT, Lyallpur Khalsa College, Jalandhar, India

Abstract-In MANET (Mobile Ad-hoc networks) wireless mobile nodes dynamically form an infrastructure less network. Due to security issues of its routing protocols, wireless ad hoc networks may be vulnerable to the malicious nodes. Black Hole Attack is one of these attacks against network integrity in which all data packets are absorbed in the network. Actually the traffic is redirected to such a node that actually does not exist in the network. The node advertises itself in such a way to the other node that it attracts other nodes and networks lying that it has the shortest path. So data packets do not reach the destination node hence, data loss occurs. Therefore to find a secure way for transmission and communication is quite challenging and vital issue in MANET. In this paper simulation study of network is done under black Hole attack. Comparisons are made with the network working with and without attack working on AODV protocol. Various performance metrics such as throughput, PDF and End to End delay are used for analysis.

Keywords- Ad hoc network; black Hole attack; AODV Routing protocol; PDR; RREQ; RRE; End to End Delay

I. INTRODUCTION

Mobile Ad-hoc network consists of dynamic nodes i.e. it is a multi-hop temporary communication network of mobile nodes with router functions equipped with wireless transmitters and receivers without the aid of any current network infrastructure. But, MANET due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation and constrained capability is vulnerable. Routing is thus an important sector in the security of the entire network as network topologies keep on changing according to the movement of active nodes [1]. Attacks in MANET can be divided into two classes: passive attacks and active attacks [2] [3]. In a passive attack, the attacker only attempts to discover valuable information by listening to the routing traffic and does not disturb the operation of a routing protocol. However, an active attack involves action performed by adversaries, modification and deletion of exchanged data. Black Hole is an active routing attack method where the attacker node, promotes itself as a best node path to arrive at the destination. The invader node is in waiting state till the neighboring nodes initiate the RREQ packet. When the invader node gets the request it sends a fake reply packet RREP along with a new sequence number. As the invader node presents itself as the active and best node to reach the destination so, the source node ignores the other nodes and sends all its data packets through invader node. The malicious node accepts the incoming data packets and does not forward them to other nodes instead it drops them. Since all the data packets are concentrated at a single invader node hence is called as 'Black Hole' and the region is called as 'Black region'. [4] [5] [6] Thus it is important to investigate the consequences of black Hole attack in order to know how much the MANET network is destabilized under normal operation as well as under the Black Hole attack.

II. AD-HOC ON DEMAND DISTANCE VECTOR (AODV) PROTOCOL

Routing and network management are most important in networking operations. Depending on the routing topology, routing protocols are proactive (typically table-driven), reactive (on demand) and hybrid in nature. In AODV routes are created on demand when they are needed. So basically it is reactive protocol in which when a node wishes to start transmission with another node in the network to which it has no route, AODV will provide topology information for the node. It creates symmetrical path between the nodes and has a routing table containing sequence number for the nodes. These sequence numbers are allocated by the destination node to obtain the originality of routing information [4] [5]. AODV uses Client-server method i.e. Request-reply method for finding a suitable path between sources and destination. To find a route to the destination node in the network AODV use three control messages. There are three types of control messages in AODV:

Route Request Message (RREQ):
Source node transmits RREQ message. Immediately AODV, using expanding ring technique, floods RREQ message. There is a TTL(time to live) value in every RREQ message, that states the number of hops the RREQ should be transmitted.

Route Reply Message (RREP):
Destination node or any intermediate node having a requested identity replies back with a route RREP message back to the originator node.

Route Error Message (RERR):
Each node keeps monitoring the link status to its neighbor's nodes during active routes. On detection of a link crack in an active route, RERR message is generated by the node in order to notify other nodes that the link is down.

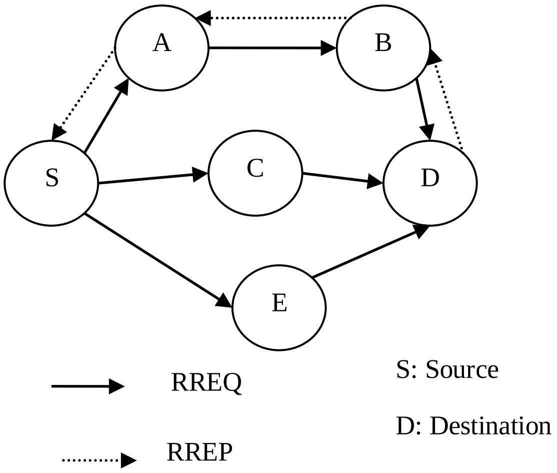

Fig.1: Propagation of RREQ and RREP from S to D

III. BLACK HOLE ATTACK

MANETs face different securities threats from the attack that are carried out to disrupt the normal performance of the networks.

Mobility is the main characteristics of MANET due to which it is very difficult to maintain the security in MANET [7]. Black Hole attack is one of the most common attacks that aim at modifying the routing protocol so that traffic flows through a specific node (which does not exist). In this attack, source node generates a RREQ message and passes it to its neighbors'. An invader node broadcast that it has the best path to the destination node during the process of route discovery. It immediately sends back a fake RREP message to the source node. The source node gets trapped and starts sending the packet to it. The invader node drops all packets instead of forwarding it i.e. "swallows" the data packet. And hence there is Denial of Service.

Black Hole are of two types: Internal Black Hole attack, External Black Hole attack. In **Internal** black Hole attack an internal invader node fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. Whereas in **External** attacks invader physically stay outside of the network and deny access to network traffic by creating congestion in network or disrupting the entire network.

In AODV protocol routing level black Hole can be classified into two categories: RREQ Black Hole attack and RREP Black Hole attack.

RREQ Black Hole attack

In RREQ Black Hole attack, the invader pretends to broadcast a RREQ message with a non-existent node address. Other nodes will update their route table for pass via the non-existent node to the destination node. So, the normal route will be broken down.

The invader can spawn Black Hole attack by false RREQ message as follows:

- Set the type field to RREQ (1)
- Set the originator IP address to the originating node's IP address
- Set the destination IP address to the destination node's IP address
- Set the source IP address, in the IP header, to a non-existent IP address (Black Hole)
- Either increase the source sequence number by at least one or decrease the hop count = 1

False information about source node is inserted to the routing table of nodes that get the fake RREQ, if any of these nodes will send data to the source; it all will be send to the malicious node.

Black Hole attack by RREP

In Black Hole attack caused by RREP a fake RREP messages is send after receiving RREQ from the source node. A malicious node can spawn black Hole attack by sending RREP as follow:

- Set the type field to RREP (2)
- Set the hop count field = 1
- Set the originator IP address as the initiate node of the route and the destination IP address as the destination node of the route
- Increase the destination series number by at least one
- Set the source IP address (IP header) to a non-existent IP address (Black Hole).

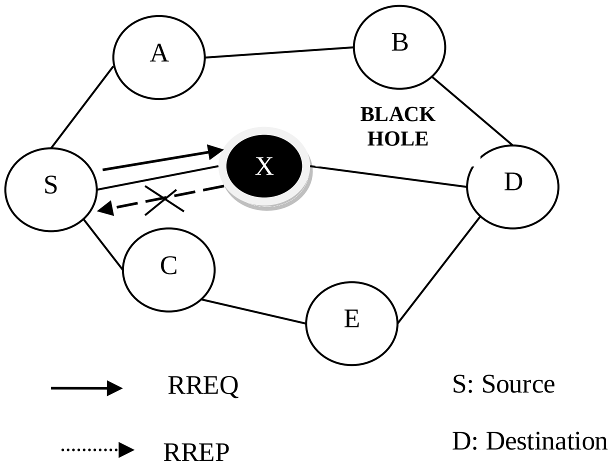

Fig.2: Black Hole attack

In the above figure 2, there are 7 nodes out of which node S is the source node which generates the RREQ message in order to find the fresh route to send a packet to the destination node i.e. D. The intermediate nodes of node S are node A, node C and node X. All the nodes get the RREQ message generated by the node S. Node X, being the malicious node, sends the RREP message back to the node S advertising that it has the best path to reach the destination node D. After receiving the RREP message from node X, node S started sending the packet to the node X. But node X will not forward it; it discards all the messages just making it the denial of service.

In black Hole attack, hostile node checks availability of fresh routes irrespective of its routing table. [8, 9] A path based detection method is planned, in which every node is not believed to watch every other node in their neighborhood. But in the current route path it observes the next hop. Many solutions have been proposed to battle on Black Hole attack. One of the solutions proposed by Deng [10] gives the loom of disabling the reply message by the intermediate. The resolution proposed in [11] focuses on the requirement of a source node to stay unless the arrival of RREP packet from more than two nodes. When source node receives numerous RREPs, then it checks that there is any share hops or not. But this solution has a drawback of time delay it has to wait for the arrival of multiple RREPs before it judges the authentication of node.

A. Detection Mechanism

Various approaches have been followed to detect Black hole in the network. Some are discussed below:

- A common approach for the detection of the black hole attack was given by Neighborhood-based and Routing Recovery Scheme Sun etal.[12] The method given by them is neighbor based in which the malicious node is detected and a routing recovery protocol is established for a correct path to the truthful destination. In this approach, nodes within the transmission range of a node forms neighboring node set. The control packets are used to share neighbor data set with the other nodes in the network. If two sets are received at the same time and contain different elements then they are taken as the set generated by two different nodes.
- Another approach was proposed by Gao et al [13], who anticipated a signature algorithm to trace packet dropping nodes. The approach consisted of algorithms to create proof, checkup algorithm and diagnosis algorithm. A Time-based Threshold Detection Scheme [14] was also proposed by Latha Tamilselvan et al. to get a solution based using timer approach. In this mechanism a timer is started when first request is received and remain active while the other request from other nodes are composed. It will store the packet's sequence number with its received time and count the timeout value based on incoming time of first route request. It also analyzes the route belong to valid path or not based on the threshold value.
- Ming-Yang Su proposed an Intrusion Detection System (IDS) based on Anti-black hole mechanism [15]. IDS scheme is used to remove the black hole attacks in MANET. The Anti-black hole mechanism employs two tables called RQ table and SN table. The IDS work on the irregular difference between routing information in these tables which are transmitted from a suspicious node. If the value goes beyond the threshold

IV. SIMULATION ENVIRONMENT

In this paper Black Hole Attack is implemented [16] using NS-2.34 in AODV protocol by modifying the original protocol and adding as a new protocol in NS2. NS-2.34 is an event driven simulation tool for networking. It consists of two types of languages: C++ and Otcl. In the back end C++, defines the internal mechanism of the simulation object; on the other hand at the front end Otcl sets up simulation by assembling, configuring objects and scheduling discrete events. On completing of each simulation two types of file are generated; one is trace (.tr) file, which is used for statically analysis and other one is nam (.nam) which is used for graphical animation. For plotting the result in form of graph, Xgraph, is used to create graphic representations of simulation results in NS2.

SIMULATIONS PARAMETERS

For the purpose of simulation these parameters are taken as common in each case:

Simulation Parameters Protocol	**AODV**
No. of Nodes	30
No. of malicious nodes	1-5
MAC	IEEE 802.11
Propagation	Two Way Ground
Traffic Connection	CBR over UDP on 5 nodes
Size of Packet	512 bytes
Mobility	Random Way Point
Speed	Minimum=10 to maximum=150 m/s
Simulation Area	1000 X 1000 (m x m)
Simulation Time	10sec
Pause time	1-6s
Maximum packets in IFQ	50

TABLE 1: Simulation Parameters

The performance metrics used for the performances analysis are defined as:

[1]. Throughput*:* Throughput is the average pace of successful message delivery over a communication channel in the network.

[2]. Packet Delivery Ratio: The ratio between the number of packets initiated by the application layer CBR sources and the number of packets received by the CBR hole at the final destination.

[3]. Packet End to End Delay: Refers to the average time taken by the packet to travel in the network from source to destination.

[4]. Network Load*:* It is basically the total traffic of the whole network from the top most layer of MAC that is received and chained for further

trans-mission.

We have divided my work in three scenarios: in the first scenario we keep the number of nodes variant and speed of packets constant; for judgment we add one malicious node in the network and compare the output on the basis of metrics: throughput, PDR, end to end delay.

In the second scenario total no. of nodes are constant and there is only one malicious node in the network but the speed of the nodes is variable. Results are compared again on basis of throughput, PDR, end to end delay with the original AODV protocol network.

In the third scenario the speed of nodes and total number of nodes are kept constant but pause time is varied for the nodes in the network are varied.

A. SCENARIO 1

In the first scenario *number of nodes is varied* and on each varied number of nodes, throughput, PDR and end to end delay is checked in the presence and in the absence of malicious node, while keeping the speed constant.

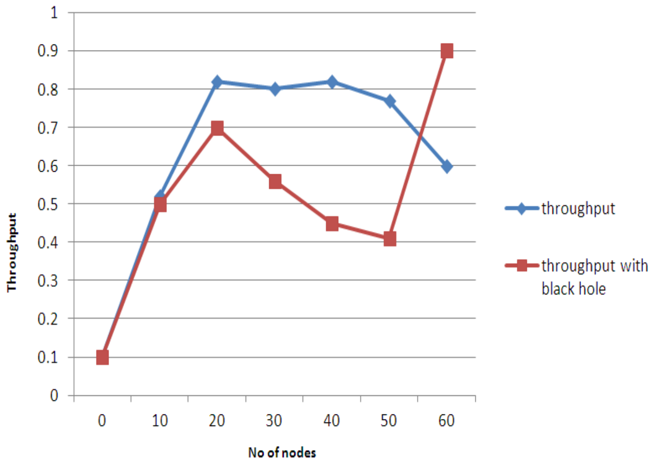

Fig.3: Throughput by varying number of nodes

In above figure 3 comparison of *throughput* is illustrated by varying the number of nodes in the network with and without attack.

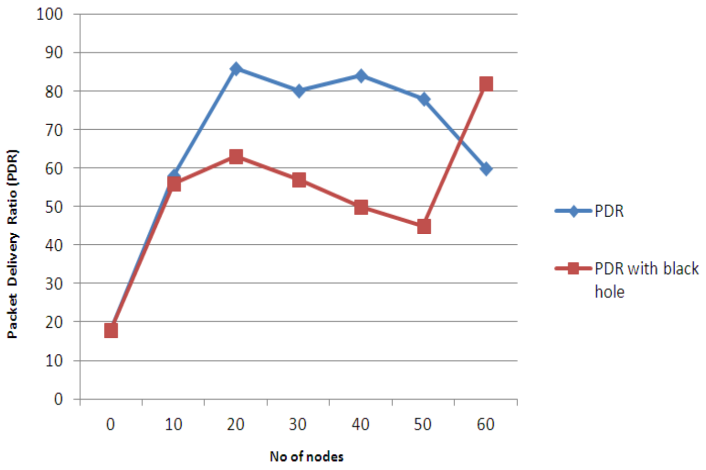

Fig.4: PDR by varying number of nodes

Figure 4 shows the comparison in *PDR* of the network with and without black hole attack. Variation in number of nodes is done first without intruding any black hole and after that by intruding the black hole in the network. Clearly in the graph it shows that first by varying the number of nodes the PDR also fluctuates but not with a high difference. But on comparing PDR with and without black hole, it is examined that PDR decreases with a noticeable difference with black hole in the network.

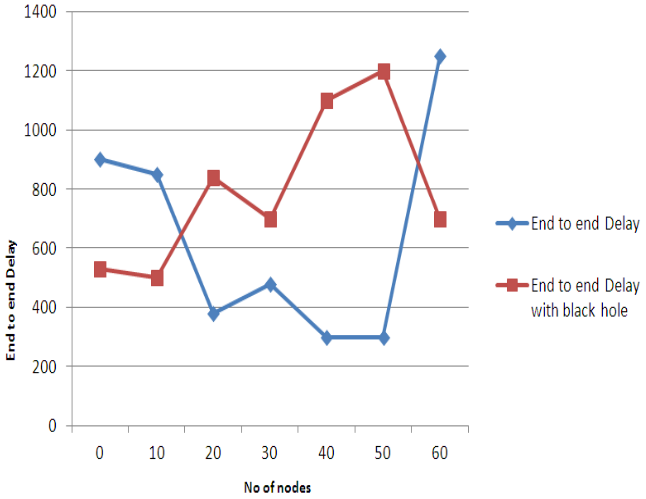

Fig.5: End to End Delay by varying number of nodes

In the above figure 5 it is observed that there is no similarity among the graphs without black hole and with black hole in the network. The graph clearly shows that at a point where the end to end delay increases (in the network without black hole), there is a decrement in delay when there is a black hole in the network. In both the cases with and without black hole some where the delay increase and somewhere it decreases.

B. SCENAREO 2

In this scenario total no. of nodes are kept constant and one malicious node is added but the speed of the nodes is varied. The performance of the network is analyzed with and without black hole.

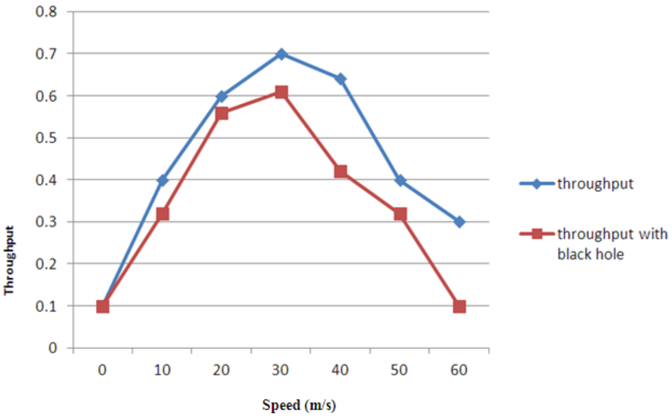

Fig.6: Throughput by varying the speed of nodes

Figure 6 shows the *throughput* with the varying speed of the nodes having one invader node in the network.

Graph clearly illustrates that the throughput of the network reduces drastically as the speed of the node increases. But there is a very minute difference in the working of the network protocol with and without invader node.

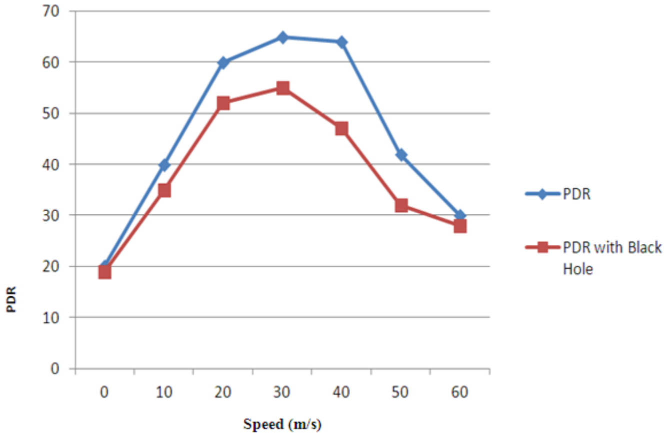

Fig.7: PDR by varying the speed of nodes

Figure 7 shows the comparison of packet delivery ratio with the increase in the speed of nodes. The PDR of network with no attack network is contrast with malicious attack, which shows lower packet delivery ratio when the speed of the node increases.

In both the cases PDR decreases with and without the black hole. But if the comparison is done between the performance when the black hole is present and it is absent, then a minute drop is visible in PDR graph with the black hole in the network. For instance the PDR in no attack network is 0.81 with node mobility speed 125 m/s and the PDF in the network with attack is 0.68 with the same speed.

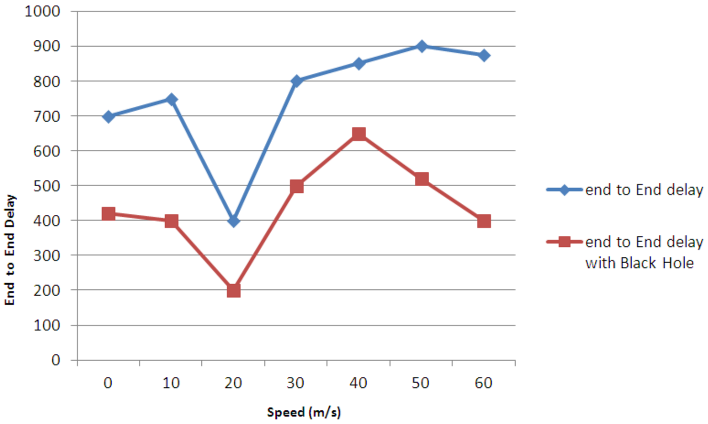

Fig.8: End to end Delay by varying Speed.

The graph shows that delay increases when the black hole is present in the network. In one case, when the speed is about 20m/s, the delay decreases in the network without the black hole and it increases when the black hole is present in the network.

C. SCENAREO 3

In the third scenario total no. of nodes and speed of these nodes is kept constant and one malicious node is added but the pause time of the nodes is varied. The performance of the network is analyzed both with and without black hole.

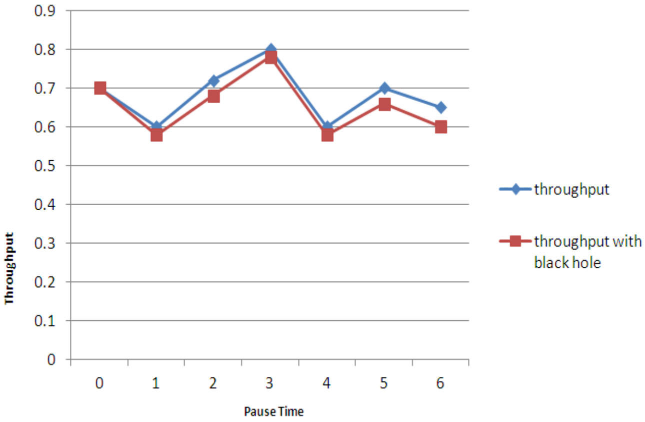

Fig.9: Throughput by varying the Pause Time

Throughput of the network is then evaluated by changing the pause time. Figure 9 clearly shows the graph in which throughput decreases in the presence of a black hole but the difference is negligible. Performance of the throughput is affected but not that much.

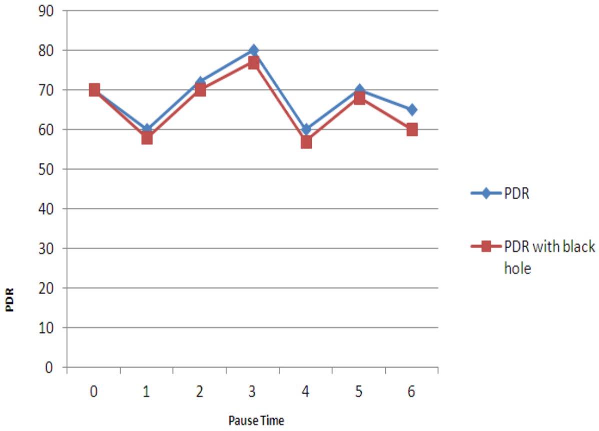

Fig.10: PDR by varying the Pause Time

The effect of variation in pause time is also an issue while comparing the PDR. It has been evaluated through the above graph that PDR in case of absence of black hole performs better than in the presence of black hole. However, the difference is not very large, but the performance of PDR is superior in the network with no black hole.

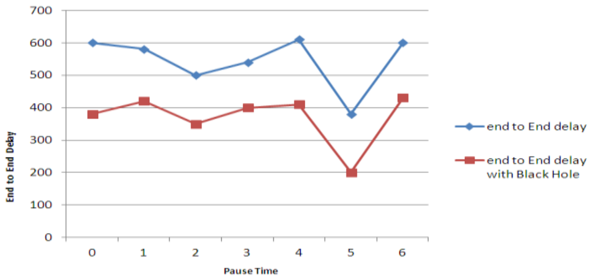

Fig.11: End to End Delay by varying the Pause Time

As seen in the figure11, the delay pattern goes in the same way in both the cases when black hole is present and when black hole is absent. But the delay value is slightly high when black hole is present in the network. Also there is no overlapping between the two values for any case.

V. CONCLUSION

In this paper we have analyzed the performance of ad hoc network working using AODV routing protocol under the black hole attack and compared its performance with the network without any attack. In all the three scenarios it can be seen that the performance of the network is decreased with the Black hole attack. All the three analysis is done by assessing certain parameters - varying the nodes, pause time and speed. The assessment is done two times: first when there is no black hole and second when there is a black hole in the network. During these implementations, a simple conclusion is made that the variation in speed, nodes and pause time has major effect on the performance of the protocol in the network with and without Black hole. But the difference is major in the case with Black hole in the network.

In future we would study on prevention from these parameters so that variations in nodes speed and pause time do not make much effect over the network. Also we will work on ways to improve the network, in order to prevent black hole attack from harming the network.

VI. REFERENCES

[1]. Harjeet Kaur , Manju Bala , Varsha Sahni Performance Evoluation of AODV ,OLSR ,ZRP Protocols under Blackhole attack in Manet IJAREEIE,vol 2 , issue 6, july 2013

[2]. Deng Hongmei, Li Wei and Agrawal D.P. (2002) IEEE Communications Magazine, 70-75.

[3]. Papadimitratos P. and Haas Z. Communication Networks and Distributed Systems Modeling and Simulation.

[4]. Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre. Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET (IJCSEA) Vol.2, No.1, February 2012

[5]. Ei Ei Khin1 and Thandar Phyu2 Impact Of Black Hole Attack On Aodv Routing Protocol (IJITMC) Vol. 2, No.2, May 2014

[6]. Deepali Virmani, Ankita Soni, Nikhil Batra, Reliability Analysis to Overcome Black Hole Attack wireless Sensor Network ICCIN-2K14 |January 03-04, 2014.

[7]. Prasant Mohapatra, Srikanth Krishnamurthy "Ad hoc Networks: Technoogies and Protocols" Springer, eBook ISBN: 0-387-22690-7 Print ISBN: 0-387-22689-3, 2005

[8]. Z.J.Hass, M.R.Pearlman, P.Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", 55th Proceeding of International task force, July, 2002.

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

[10]. M.Parsons, P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks", [Online]. Available: www.cse.buffalo.edu/srds2009/dncms2009_submission_person.pdf, [Accessed: April. 10, 2010].

[11]. D.B.Roy, R.Chaki and N.Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Networks", International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.

[12]. Sun; Y. Guan; J. Chen; U.W. Pooch, Detecting Black hole Attack In MANET

[13]. X.P. Gao; W. Chen; A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks; IFIP International Conference on Network and Parallel Computing Workshops, 2007

[14]. Tamilselvan L, Sankaranarayanan V (2007) Prevention of blackhole Attack in MANET. Wireless Broadband and Ultra ideband Communications, Sydney, Austral

[15]. F. J. Ros and P. M. Ruiz, "Implementing a New Manet Unicast Routing Protocol in NS2", December, 2004, http://masimum.dif.um.es/nsrt-howto/pdf/nsrt- howto.pdf, 25 July 2005.