Performance Analysis of Aodv Protocol under Black Hole Attack

Monika Roopak , Dr. Bvr Reddy

ABSTRACT- Mobile Ad-hoc networks are a collection of mobile hosts that communicate with each other without any infrastructure. Due to security vulnerabilities of the routing protocols, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. In this paper are doing simulation study of network under black hole attack and do comparison with the network without attack working on AODV protocol using various performance metrics such as throughput, PDF and End to End delay in three different scenarios.

Keywords- Ad hoc network, black hole , AODV, MANET, PDR, RREQ, RREP

1. 1 INTRODUCTION

Wireless network is the network of mobile computer nodes or stations that are not physically wired. The main advantage of this is communicating with rest of the world while being mobile. The disadvantages are their limited bandwidth, memory, processing capabilities and open medium. Two basic system models are fixed backbone wireless system and Wireless Mobile Ad hoc Network (MANET). An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. So the functioning of ad hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes [1].In these networks, besides acting as a host, each node also acts as a router and forwards packets to the correct node in the network once a route is established. In this paper we will study the ad hoc network with and without the black hole attack using performance metrics PDF, Throughput and End to End delay.

2. AODV

The AODV [2,3] routing protocol is a reactive routing protocol therefore, routes are determined only when needed. Figure 1 shows the message exchanges of the AODV protocol. Hello messages may be used to detect and monitor links to neighbors. If Hello messages are used, each active node periodically broadcasts a Hello message that all its neighbors receive. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected.

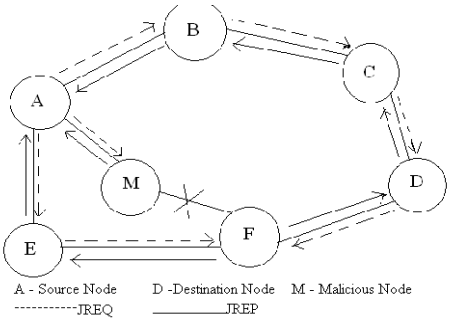


Figure 1 Black Hole Attack

source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen. As data flow from the source to the destination, each node along the route updates the timers associated with the routes to the source and destination, maintaining the routes in the routing table. If a route is not used for some period of time, a node cannot be sure whether the route is still valid; consequently, the node removes the route from its routing table. If data is flowing and a link break is detected, a Route Error (RERR) is sent to the source of the data in a hop-by- hop fashion. As the RERR propagates towards the source, each intermediate node invalidates routes to any unreachable destinations. When the source of the data receives the RERR, it invalidates the route and reinitiates route discovery if necessary.

3. BLACK HOLE ATTACK

Routing protocols are exposed to a variety of attacks. Black hole attack is one such attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [4]. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the route discovery process, the source node sends route discovery packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other route reply messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires. Malicious nodes take over all routes by attacking all route request messages. Therefore the quantity of routing information available to other nodes is reduced. The malicious nodes are called black hole nodes. For example, source A wants to send packets to destination D, in figure1, source A initiates the route discovery process. Let M be the malicious node which has no fresh route to destination D. M claims to have the route to destination and sends join reply JREP packet to S. The reply from the malicious node reaches the source node earlier than the reply from the legitimate node, as the malicious node does not have to check its routing table as the other legitimate nodes. The source chooses the path provided by the malicious node and the data packets are dropped. The malicious node forms a black hole in the network and this problem is called black hole problem.

4. SIMULATION ENVIRONMENT

We have implemented [5] Black Hole Attack using NS-2.34 in AODV protocol by modifying the original protocol and adding as a new protocol in NS2. Xgraph is used for plotting the result in form of graph in NS2. The simulation parameters are shown below.

Simulation Area	700x700
No. of Nodes	30
No. of Malicius Nodes	1,2...5
Communication Traffic	CBR
Simulation Duration	10
Speed of the Node	20,50.....150 m/s
Packet Size	512

We divide our work in three scenarios, in the first scenario we keep the number of nodes and speed constant, for comparison we add one malicious node in the network and compare the out put as throughput, Pdf, end to end delay with the original AODV protocol network.

In the second scenario we keep the speed of nodes and total number of nodes constant and we vary the no of malicious nodes in the network.

In the third scenario we keep the total no. of nodes constant and one malicious node in the network and vary the speed of the nodes and then compare the result again as throughput, pdf, end to end delay with the original AODV protocol network.

The performance metrics stated above are defined as

1) Throughput: Throughput is the average rate of successful message delivery over a communication channel.

2) Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.

3) End to End Delay: Refers to the time taken for a packets to be transmitted across a network from source to destination.

4.1 SCENARIO 1

For first scenario we keep 30 number of node with random movement and 1 out of 30 node is malicious and then we compare the black hole attacked network with the network with AODV routing protocol.

Figure 2 shows the comparison in throughput of network with and without black hole attack.

Throughput in case of network with no attack

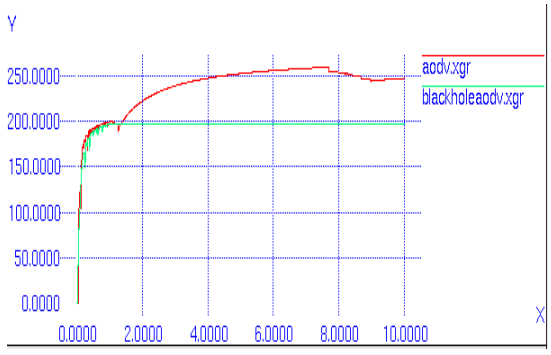


Figure -2 X-axis : Time Y-axis: Throughput ■ with

Blackhole ■ With no attack

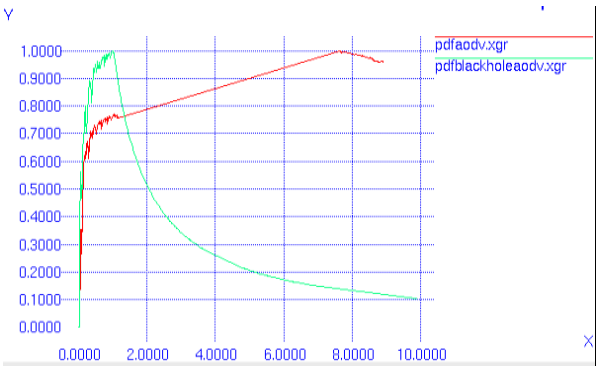


Figure -3 X-axis : Time Y-axis: PDF ■ with Blackhole ■ With no attack

increases with time whereas in case of black hole attacked network the throughput become constant when the malicious node comes into action in the network.

Figure 3 shows the comparison in PDF of network ith and without black hole attack. The PDF ratio decreased drastically in case of network with black hole attack

The End to End Delay with black hole attacked network measured is 179.85ms and the End to End Delay with no attack is 46.27 ms.

4.2 SCENARIO 2

In the second scenario we keep the total number of nodes constant with random movement with speed of 20 ms and vary the number of malicious nodes in the network and then compare the network with black hole attack with network without any attack.
Figure 4 shows the throughput with varying number of malicious nodes. Graph shows the decline in the throughput with the increase in the number of malicious nodes.

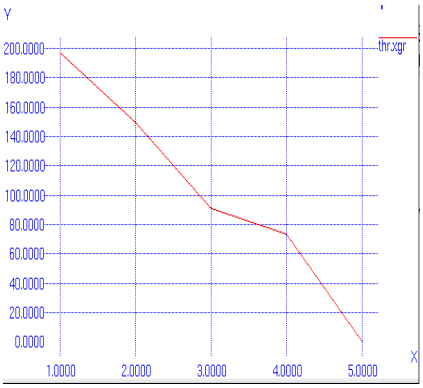
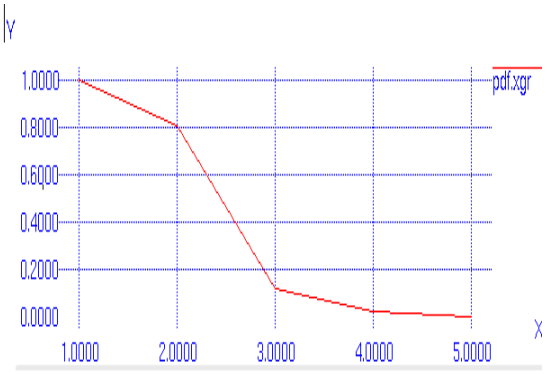


Figure -4 X-axis : Speed Y-axis: Throughput ■ with Blackhole

Figure 5 shows the packet delivery ratio with the number of malicious nodes. We can clearly conclude that the PDF of the network is reduced to zero in our case hence the PDF is decreasing with the increase in no of malicious nodes.

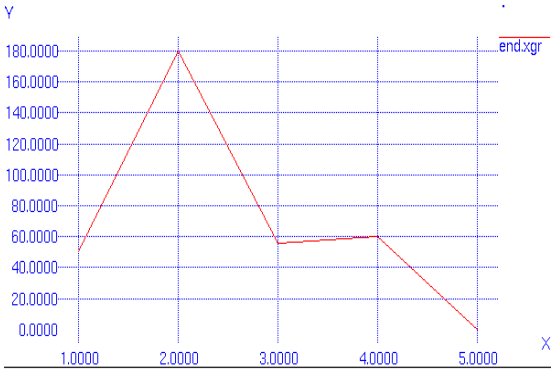
Figure -5 X-axis : Speed Y-axis: PDF ■ with Blackhole

Figure 6 shows the relation between increases in the



number of malicious nodes with end to end delay.

It can be seen from the graph that end to end fluctuates with increase in no. of malicious nodes.



4.3 SCENAREO 3

In the third scenario for the calculation of the performance of the network with and without black hole attack we keep to total no. of nodes constant and one malicious node and vary the speed of the nodes.

We keep no of nodes malicious node constant and vary the speed of the nodes

Figure 7 shows the throughput with the speed of the nodes having one malicious node in the network.

Graph indicates that the throughput of the network reduces drastically as the speed of the node increases.

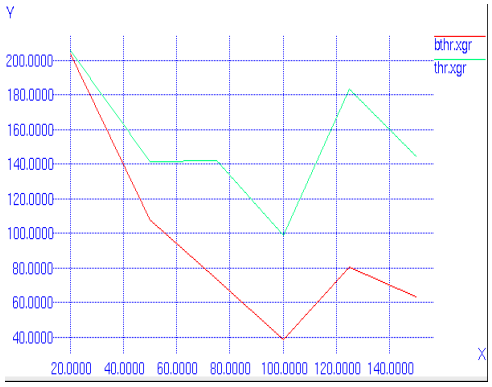


Figure-7 X-axis : Speed Y-axis: Throughput ■ with Blackhole ■ With no attack

Figure 8 shows the packet delivery ratio with the increase in the speed of nodes. With the comparison with the PDF of network with no attack network with malicious attack have much lower packet delivery ratio when the speed of the node increases. For eg. The PDF in no attack network is 0.8 with node mobility speed 125 m/s and the PDF in the network with attack is 0.67 with the same speed.

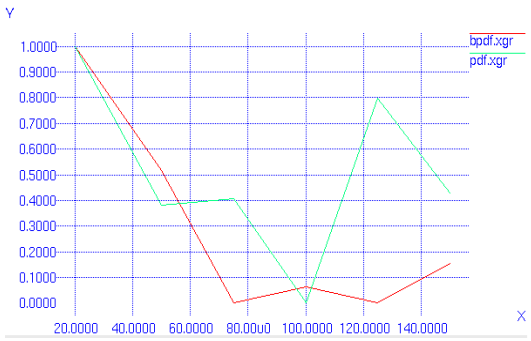


Figure -8 X-axis : Speed Y-axis: PDF ■ with Blackhole ■ With no attack

Figure 9 shows the end to end delay with the increase in the speed of the nodes. It can be seen from the graph that end to end delay is totally opposite when considering case of network with and without blackhole attack.

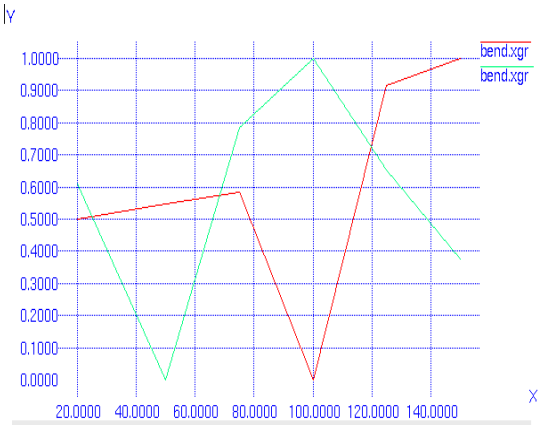


Figure -9 X-axis : Speed Y-axis: End to End Delay ■ with Blackhole ■ With no attack

5. CONCLUSION

In this paper we have analyzed the performance of ad hoc network under the black hole attack and compared that with the network without any attack working using AODV routing protocol in three scenarios . As we can see from Figure 2-9 the performance of the network is decreased under the attack in each scenario . The PDF and Throughput of the network has decreased drastically in all the three scenarios and the End to End delay has increased again in all the scenarios.

6. REFERENCES

[1] Tamilselvan, L.; and Sankaranarayanan, V. (2007). Prevention of blackhole attack in MANET. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications. AusWireless, 21-21.

[2] C. E. Perkins, E. M. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561, July 2003.

[3] C. E. Perkins and E. M. Royer. The Ad hoc On-Demand Distance Vector Protocol. In C. E. Perkins, editor, Ad hoc Networking, pages 173–219. Addison-Wesley, 2000.

[4].E. A. Mary Anita and V. Vasudevan, Black Hole attack on multicast routing protocols, JCIT, Vol.4, No.2, pp. 64–68,

2009
[5] 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.

Monika Roopak is pursuing M.Tech in IT from USIT, GGS Indraprastha University, Delhi

Dr. BVR Reddy is serving as DEAN of USIT, GGS Indraprastha University Delhi