Analysis of Black Hole Attack on MANET

Monika Agrawal
M.Tech.-CSE, Dept of CSE, IET
Mangalayatan University, Aligarh (U.P)

Rohit Kumar
Assistant Professor, Dept of CSE, IET
Mangalayatan University, Aligarh (U.P)

Abstract- Wireless network enables users to communicate and transfer data to each other without any physical link between them and MANET is a kind of wireless network. MANET has three types of routing protocols which allow the mobile nodes to connect and leave the network at any instance of time. MANET has the high possibility of attack because of its wireless connectivity some characteristics such as open medium and distributed cooperation. In this paper we simulate the effect of blackhole attack on AODV which is one of the attacks on MANET using Network Simulator (NS-2). The simulation results show the packet loss, throughput, and end-to-end delay without blackhole attack and with blackhole on AODV in MANET. We find that the packet loss in the presence of blackhole attack increases in the network and we also analyzed that the end–to-end delay and throughput decreases when blackhole node attacks on the network.

Keywords: AODV, MANET, Blackhole

I. INTRODUCTION

Wireless systems became pretty famous because of its wireless connectivity every time and everywhere irrespective to the user's geographic area. It sends data and information with the help of radio frequencies instead of any physical medium. Wireless networks are formed by hosts and routers. Wireless network has two modes of operations i.e. in the presence of Control Module (CM) which is known as base station and second is Ad-hoc connectivity. In Ad-hoc network, we use multi hop links to provide connectivity between two mobile nodes. Networks that are autonomous and decentralized in wireless systems typically called mobile ad hoc networks (MANET). In mobile ad hoc network (MANET) there is no fixed infrastructure or central module to communicate with mobile nodes in the network. There is no centralized module so the communication in MANET based on the mutual trust between the mobile nodes. As in [2] Nodes help each other in share the responsibilities of managing network and transfer the information about the topology which used in the network. As in [1] MANET works as autonomous system in which each mobile node work as a host and routers at the same time when required.

As in [3] Based routing security in wireless network, in this routing protocols of MANET can be classified into three categories: Reactive protocols (On Demand), Proactive protocols (Table Driven) and Hybrid protocol. These three protocols are further divide in to sub parts. As in [9] security in ad hoc network is very important issue for the basic functionality of the network. The attacks on routing protocols re vulnerable and these attacks can be classified in to five categories: Denial of Service attack, Fabrication attack, Modification attack, Replay attack and Impersonation attack. In this paper, we analyze the effect of black hole attack which belongs to the category of fabrication attack.

As in [4] analyzed the effect of black hole attack on routing protocols of MANET. In this mainly two protocols have been considered, AODV and Improved AODV. In this paper, simulations has been based on a no. of parameters and analyzes the effect of attack by adding the black hole node and then computes and compare the results of both routing protocols and analyzed the performance of both protocols.
The rest of the paper is organized as follow: In section 2 we discuss the AODV routing protocol in detail. Section 3 describes the blackhole attack on AODV. Section 4 provides the simulation environment and results. Finally we conclude in section 5.

II. AODV ROUTING PROTOCOL

As in [5] Ad-Hoc On-Demand Distance Vector (AODV) is an on demand routing protocol in which source initiate the route discovery to the destination node. As in [7] , [10] the Ad Hoc On-Demand Distance Vector (AODV) routing

protocol described in builds on the DSDV algorithm. AODV minimizes the number of broadcasts by creating routes on a demand basis.

AODV use the control messages to find a route between the source and the destination. It uses three types of control messages. It builds a route between two nodes by using the route request and route reply messages. When a source node wants to create a path to the destination, it broadcasts a RREQ (route request) message across the network. All active nodes in the network receive this request message and update the information for the source node and set the back pointer for the source node in the tables. Routing table contains source node's IP address, broadcast ID, and sequence number. A node which receives the RREQ may sends a RREP (route replay) message if it contains active route to the destination with corresponding to the sequence number which is greater than or equal to the number that contained in the RREQ or if it is a destination node in the network. If any route breaks in the network then it sends the RERR (route error) message to the source. After getting the RERR message it sends RREQ message again in the network to find another route to the destination once it maintains a route from source to the destination and then it may send data through this path or route. If the source node later receives a RREP containing a smaller sequence number with smaller hop count or greater sequence number, then it updates its routing information for that route to the destination and begins use the better route.

III. BLACKHOLE ATTACK IN AODV

As in [5] in blackhole attack, a malicious node uses the routing protocols to advertise itself to the destination or interrupt the transmission from source the destination. As in [1] blackhole attack in AODV has two properties**:**

1) Internal black hole attack, in this type of attack a malicious node fits itself between the routes from source to destination. When this malicious node gets chance make itself an active node for the destination and at this step this node is now capable to interrupt the packets to the destination.

2) External of internal attack, in this type of attack node stay outside the network and it deny access the traffic. It can become a kind of internal attack by taking the control of internal malicious node and control it to attack the node in the network. To explain the blackhole attack here we add a malicious node that exhibits blackhole behavior in the Fig.

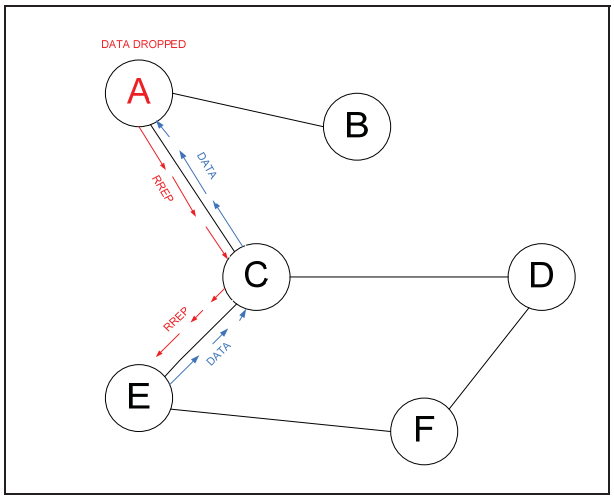

Figure 1: blackhole attack on AODV

In Fig. 1, we take node A as a malicious node. Suppose node E is the source node and wants to send data packets to node D, and it initiates the route discovery process by sending the RREQ message. We assumed node A, a malicious node

Which has no fresh enough route to the destination node D.? However, node A claims that it has the route to the destination by receiving RREQ message from the active node and sends the RREP message to the source node (E). First this malicious node analyzes the network then detects the active node and then notes the destination node's address. Other active nodes that have the route to the destination and the destination node also send the RREP message. If an active node

replay to the source node first everything goes well but the RREP message could reach the source node first from the malicious node A, if it is nearer to the source node E. Malicious node sends the RREP with destination address field spoofed with the false address that's why the source node thinks that the route discovery process is complete and ignores all other replay and start to send data to that route. As a result malicious node A now begins to drop all data packets.

IV. SIMULATION ENVIRONMENT AND RESULT

In this section we present the information about the simulator and the result of blackhole attack on AODV by performing the set of simulation experiments. We used Network Simulator NS2 to carry the MANET system. NS2 uses the discrete event for the network simulation and it provides collaborative environment for simulation. NS2 is the object oriented simulator and written in C++ ant OTCL. It supports most UNIX and UNIX like system and LINUX based operating systems. In this paper, we run two simulations, one with blackhole attack and other without blackhole attack. Figure 2 shows the network of 20 nodes. In this figure, network has created by the 19 active nodes and one blackhole attack node.

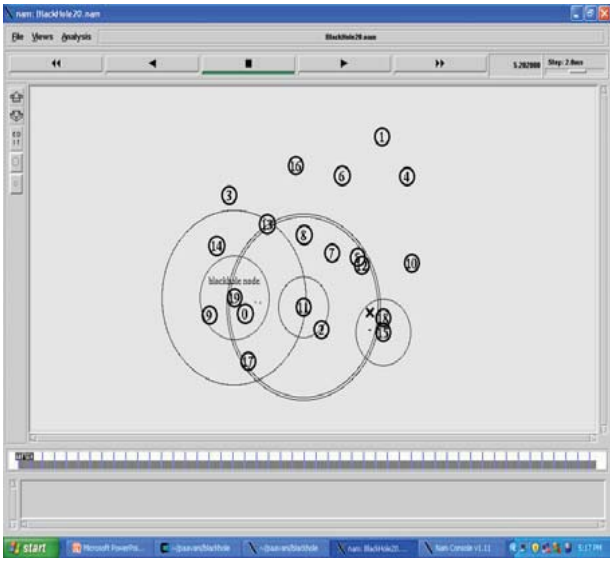

Figure 2: Network with Blackhole Attack

We have done the simulation study carried out the performance evaluation of MANET in the presence of black hole attack using the parameter metrics such as throughput, packet loss and end-to-end delay in the network. We use these simulations results to analyze the effect of blackhole attack in the network. We set the parameters as shown in the table1.

Parameter	Definition	Parameter	Definition	Parameter	Definition	Parameter	Definition
Routing Protocol	AODV	Number of Blackhole Nodes	1	Simulation Time	500s	Packet Size	512bytes
Data Rate	10kb	Traffic Source	CBR	MAC Layer	802.11	Connections	9
Simulator	NS-2(ver. 2.3.1))	Simulation Area	750m*750m	Number of Mobile Nodes	20	Connection Range	250m

Table 1: Definition and parameter

4.1 THROUGHPUT

Throughput is the rate of data transferred from sender to receiver in a given amount of time. It is measured in the packet per sec. or bit per sec. We calculated throughput in the presence of blackhole attack and in the absence of blackhole attack. We calculated throughput value for the nodes at the pause time 20s, 40s, 60s, 80s. These values are listed in table 2

and we use these values to plot the graph as shown in figure3. After performing the simulation we analyzed that, the throughput values decreases in the presence of blackhole attack when compared to the normal AODV condition.

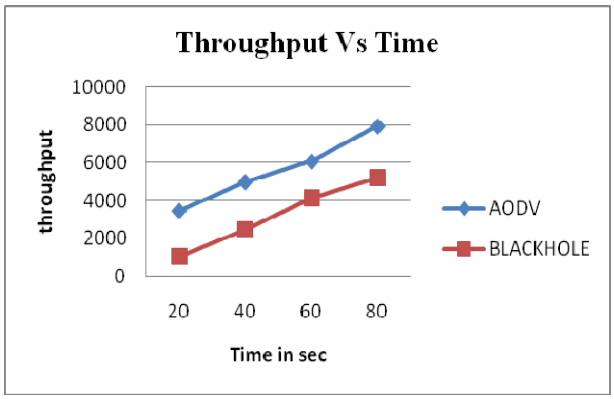

Figure 3: Shows the Throughput values of AODV and blackhole AODV

Pause time in sec	AODV	Blackhole
20	3436	1042
40	4966	2468
60	6058	4129
80	7925	5218

Table 2: Throughput values of AODV and blackhole AODV

4.2 PACKET LOSS

Packet loss can be calculated by subtracting the received packets by the no. of send packets. These values of packet loss calculated for the number of nodes 20, 40, 60, 80. These values are listed in table 3 and plotted in the graph as shown in figure 4.

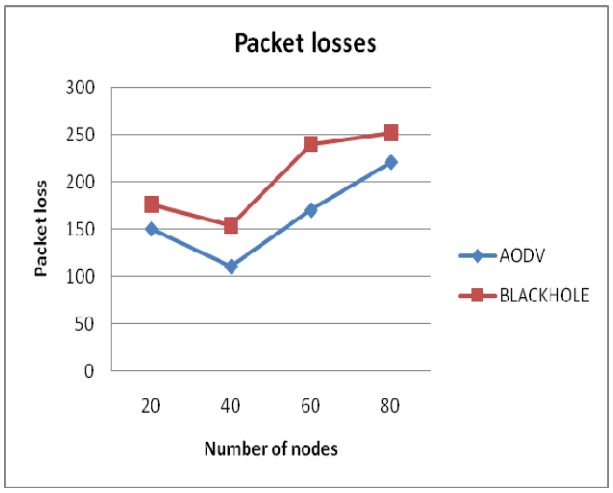

Figure 4: Shows the Packet losses of AODV and blackhole AODV

After the simulations we analyzed that the packet loss is high in the presence of blackhole attack in compared to normal condition of AODV.

Nodes	AODV	Blackhole
20	150	176.08
40	110	154.02
60	170.01	240.25
80	221.02	252.05

Table 3: Packet loss values of AODV and blackhole AODV

4.3 END -TO-END DELAY

End –to- end delay is the time taken for packet to be transmitted across a network from source to destination. It is measured in sec. We have calculated end-to-end delay with varying the mobility speeds 20m/s, 40m/s, 60m/s, 80m/s. These values are listed in the table 4 and are plotted in the graph as shown in figure 5.

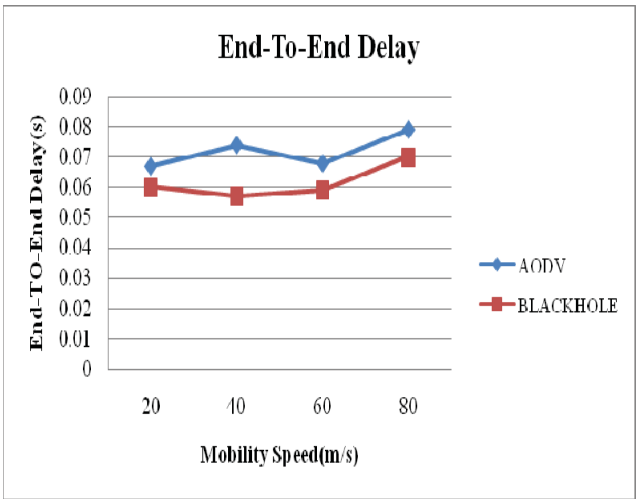

Figure 5: Shows the End-to-End delay of AODV and blackhole AODV

It is observed from the simulation that End-to-End delay of network decreases in the presence of black hole attack in the network. This is due to the immediate replay from the malicious node because it does not check its routing table.

Mobility Speed(m/s)	AODV	Blackhole
20	0.067	0.06
40	0.077	0.057
60	0.068	0.059
80	0.079	0.07

Table 4: End-to-End delay in AODV and blackhole AODV

V. CONCLUSION

In this paper, We have proposed blackhole attack in the network against AODV with the help of Network Simulator ns-2.We have also evaluated the effect of blackhole nodes on AODV routing protocol using parameter metrics in ad hoc network. We compared the simulation result of black hole attack in AODV with the original AODV. We observed that the packet loss in the network increases as the black hole nodes increases. After the simulation we also analyzed that the throughput decreases when a black hole enters in the network as compared to original AODV. We observed End-to-End delay in the presence of black hole attack is slightly decreases as compared to AODV without blackhole attack. After the completion of simulation we analyzed that the detection of black hole attack in ad hoc network is still a challenging task.

REFERENCES

[1] Latha Tamilselvan, Dr.V Sankaranarayanan, *"Prevention of Blackhole Attack in MANET"* The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) India, 2007 IEEE.
[2] Latha Tamilselvan and Dr. V. Sankaranarayanan *" Solution to Prevent Rushing Attack in Wireless Mobile Ad hoc Networks".*
[3] Mohammad Pervaiz, Mihaela Cardei, and Jie Wu, *"Routing Security in Ad Hoc wireless Networks"* Network Security, 2005 Springer.
[4] Jaspal Kumar, M. Kulkarni, Daya Gupta, *"Security within Ad-Hoc Networks,"* Position Paper, PAMPAS Workshop, Sept. 16/17 2002.

[5] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. *"Detecting Blackhole Attack on AODV based Mobile Ad hoc networks by Dynamic Learning Method"*.
[6] ns-2: http://www.isi.edu/nsnam/ns/
[7] C. E. Perkins and E. M. Royer*, "Ad Hoc On-Demand Distance Vector Routing"* Proc. 2nd IEEE Workshop. Mobile Computing System And Apps. New Orleans, LA, Feb. 1999, pp. 90–100.
[8] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network
[9] H. Deng, W. Li, and D. P. Agrawal, "Routing security in ad hoc networks," IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002
[10] V.K. Taksande and Dr.K.D.Kulat -Performance Comparison of DSDV, DSR, AODV Protocol with IEEE 802.11 MAC for Chain Topology for Mobile Ad-hoc Network using NS-2 , *IJCA Special Issue on "2nd National Conference- Computing, Communication and Sensor Network" CCSN, 2011.*