GLOBAL JOURNAL OF ENGINEERING, DESIGN & TECHNOLOGY
(Published By: Global Institute for Research & Education)
www.gifre.org

BLACK HOLE ATTACK- HAZARD TO AODV ROUTING PROTOCOL IN MANET

Ketan Sureshbhai Chavda
PG Student, Master of Computer Engineering, C.U.Shah College of Engineering and Technology, Wadhwan, India

Abstract

Mobile Ad Hoc Network (MANET) consists of a collection of wireless mobile hosts without the required intervention of any existing infrastructure or centralized access point such as base station. The dynamic topology of MANET allows nodes to join and leave the network at any point of time. Wireless MANET is particularly vulnerable due to its fundamental characteristics such as open medium, dynamic topology, distributed cooperation and constrained capability. In this paper we simulate the blackhole attack which is one of the possible attacks on AODV routing protocol in mobile ad hoc networks by the help of network simulator (NS-2).The simulation results show the packet loss, throughput, and end-to-end delay with blackhole and without blackhole on AODV in MANET. We analyzed that the packet loss increases in the network with a blackhole node. We also observed that the throughput and end-to-end delay decreases in the network with a blackhole node. We propose a solution that makes a modification in existing AODV routing protocol.

Keywords: Ad hoc Networks, Routing Protocols, AODV, Black Hole Attack, MANET

1. Introduction

Wireless networks use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. Wireless networks are formed by routers and hosts. Ad-hoc networks are wireless networks where nodes communicate with each other using multi-hop links. Networks that support mobile wireless ad hoc architecture are typically called mobile ad hoc networks (MANET). A mobile ad hoc network is formed by mobile hosts. There is no stationary infrastructure or base station for communication. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes. As in [1] Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. As in [2] each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network. As in [3] Based on the routing information update mechanism, routing protocols in ad hoc wireless networks can be classified into three broad categories: Proactive (or table-driven) protocols, Reactive (or on-demand) protocols, and Hybrid routing protocols. These are further divided into sub categories. As in [3] these are vulnerable to routing attacks. Routing attacks in ad hoc wireless networks can also be classified into five broad categories: Attacks using Impersonation, Modification, Fabrication, Replay, and Denial of Service (DoS). In this paper, we focus on blackhole attack that belongs to category of fabrication attacks. As in [4] there are three main routing protocols proposed for MANET: Ad hoc On-demand Distance Vector (AODV) routing, Dynamic Source Routing (DSDV), and Destination Sequence Distance Vector routing protocols. AODV and DSR belong to on-demand routing protocols and DSDV is a table-driven routing protocol. These protocols are vulnerable to different security attacks. In this paper, we use AODV routing protocol because the AODV protocol is vulnerable to the blackhole attack. So we have simulated the behavior of blackhole attack on AODV in MANET.

1.1 AODV Routing Protocol

As in [5] Ad-Hoc On-Demand Distance Vector (AODV) is a reactive routing protocol in which the network generates routes at the start of communication. As in [7] The Ad Hoc On-Demand Distance Vector (AODV) routing protocol described in builds on the DSDV algorithm. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. As [7] the authors of AODV classify it as a pure on-demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it. As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing

Information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained. If a link break occurs while the route is Active, the node upstream of the break propagates a route the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

1.2 Blackhole Attack in AODV

As in [5] in a blackhole attack, a malicious node can impersonate a destination node by sending a spoofed route packet to a source node that initiates a route discovery. As in [2] a blackhole have two properties:

1. The node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination, even though the route is spurious, with the intention of intercepting packets.
2. The node consumes the intercepted packets. In an ad hoc network that uses the AODV protocol, a blackhole node absorbs the network traffic and drops all packets. To explain the blackhole attack we add a malicious node that exhibits blackhole behavior in the Fig. 1

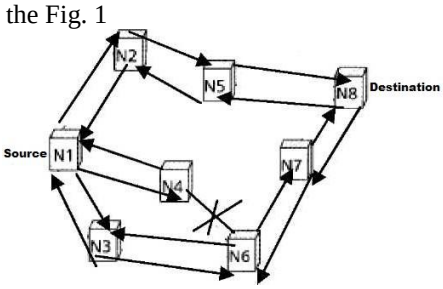

Figure 1: Blackhole attack in AODV

In Fig. 1, we assume that node N4 is the malicious node. Suppose node N1 wants to send data packets to node N8 in Fig. 1, and initiates the route discovery process. We assumed node N4 is a malicious node with no fresh enough route to destination node N8. However, node N4 claims that it has the route to the destination whenever it receives RREQ packets, and sends the response to source node N1. The destination node and any other normal intermediate nodes that have the fresh route to the destination may also give a reply. If the reply from a normal node reaches the source node of the RREQ. First, everything works well; but the reply from malicious node N4 could reach the source node first, if the malicious node is nearer to the source node. Moreover, a malicious node does not need to check its routing table when sending a false message; its response is more likely to reach the source node first. This makes the source node think that the route discovery process is complete, ignore all other reply messages, and begin to send data packets. As a result, all the packets through the malicious node are simply consumed or lost. The malicious node could be said to form a black hole in the network. In this way the malicious node can easily misroute a lot of network traffic to itself, and could cause an attack to the network with very little efforts on its part.

1.3 Simulation Environment and Result

In this section we present a set of simulation experiments to evaluate the effect of blackhole attack on AODV protocol in MANET. First I have explained blackhole attack in detail via simulation in NS-2.We have generated a small size network with7 nodes in a flat grid of 670m x 670m including blackhole node. We have generated a connection between nodes 1 and node 2. We have also introduced some movements in our scenario. Duration of the scenario is 60 seconds. Node 1 is the source node, node 2 is the destination node and node 6 is the blackhole node. Fig. 2 shows the data flow from node 1 to node 2 via intermediate nodes 3 and 4. For some seconds, the link breaks and all data that is send from node 1 get lost as shown in Fig.3. Now Fig. 4 shows that node 1 again sends the RREQ to all nodes to find route. Nodes further rebroadcast the request if they are not the destination nodes. Node 6 that is blackhole node claims that it has the route to destination whenever it receives RREQ packets and sends the response to source node 1. All other nodes that have the fresh route also send a reply. But the reply from node 6 reaches the source node first. Node 1 accepts it and ignores all other reply messages and begins to send data packets to node via node 3, 4, 5 and Node 6 being a blackhole node absorbs all the packets and traffic as shown in Fig. 5.

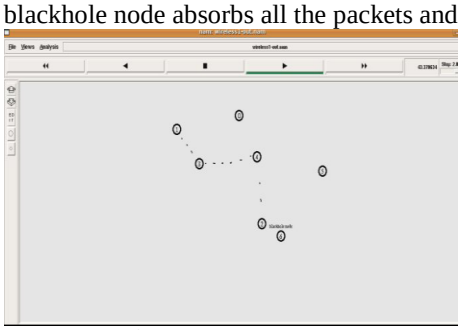

Figure 2: Data flow between Node 1 to Node 2 via Node 3 and Node 4

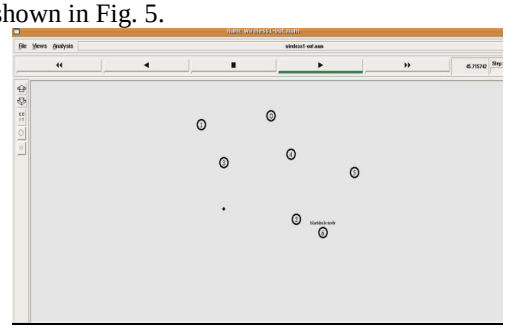

Figure 3: Link breakage and Data Loss

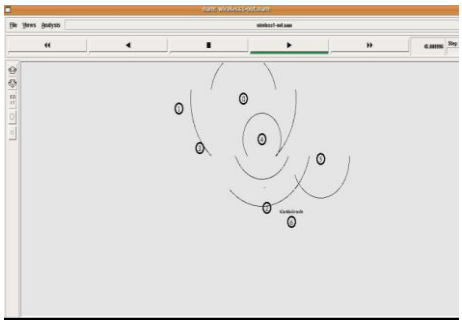

Figure 4: Route Discovery Process

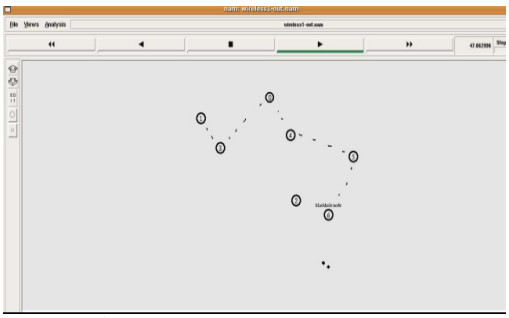

Figure 5: Node 1 found new route and Node 6(Blackhole Node) Absorbs the Data

Secondly, to calculate network performance, we simulate blackhole node behavior in AODV in large number of nodes and connections with the help of Network Simulator 2 Ref. [6]. We set the parameters for our simulation as shown in Table 1.

Table 1: Simulation Parameters

Simulator Ns-2	(ver.2.31)
Simulation Time	500(s)
Number of Mobile Nodes	20
Number of Blackhole Nodes	1
Topology	750m x750m
Transmission Range	250m
Routing Protocol	AODV
Traffic Constant Bit Rate	(CBR)
Pause Time	10(s)
Maximum Connections	9
Packet Size	512 bytes
Data Rates	10 Kbits

We have taken four scenarios of defined parameters for our simulation with or without blackhole node. We have taken different positions and movements of nodes for each scenario. Then we have varied the blackhole nodes and simple nodes to evaluate the performance. We have also varied the mobility speed of mobile nodes. The metrics are used to evaluate the performance are packet loss percentage, throughput and end-to-end delay. We calculate data loss percentage with blackhole and without blackhole node. Then we compare the results of these two simulations to understand the network and node behaviors. The results of the simulation show that the packet loss in the network with a blackhole increases beyond that dropped by the blackhole node. This is due to increased congestion in the routes toward the blackhole node.

Our simulation results show that AODV network has normally 2.50 % data loss and if a blackhole node is introducing in this network data loss is increased to 89.38 %. As 2.50 % data loss already exists in this data traffic, blackhole node increases this data loss by 86.88 %. We have also analyzed the throughput of received packets with the presence and absence of blackhole node with respect to the simulation time of 450(s). Fig. 6 illustrates the graphic representation of packet loss percentage with and without blackhole node with respect to simulation time (1=100seconds).

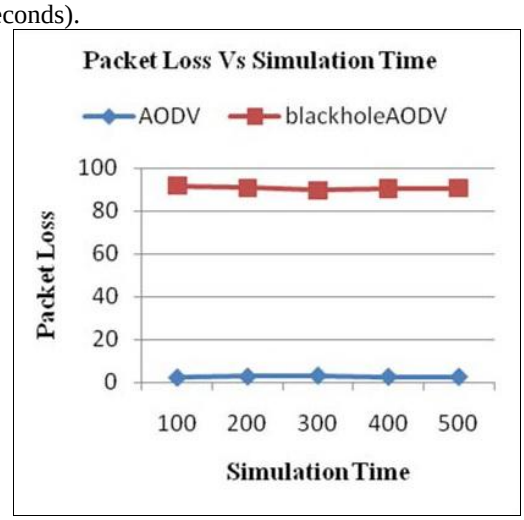

Figure 6: Shows the Packet Loss of AODV and blackholeAODV

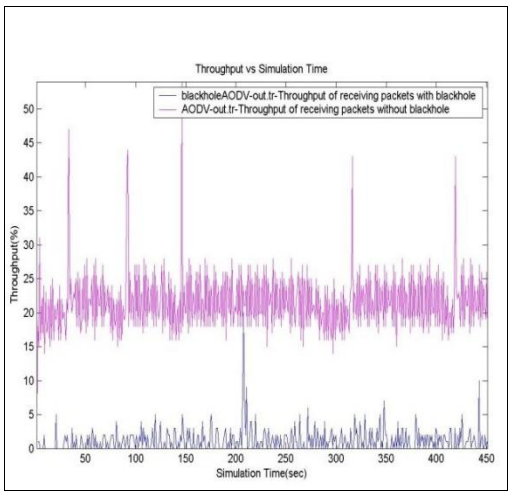

Figure 7: Impact of Blackhole Node on Throughput of Received Packets

Fig. 7 shows the effect of blackhole attack on throughput of received packets of network. The result shows both the cases with blackhole and without blackhole attack. With our simulation, we analyzed that the throughput of received

packets in AODV is very high than the throughput of received packets in blackholeAODV. Because the packet loss in blackholeAODV is higher than the AODV protocol.

We studied the performance with varying number of Blackhole Nodes. Number of Blackhole Nodes varies from 1 to 4 with the increment of 1. Fig. 8 shows the impact of number of Blackhole Nodes on throughput in the network. Simulation results show that the throughput decreases with the increase of number of Blackhole Nodes.

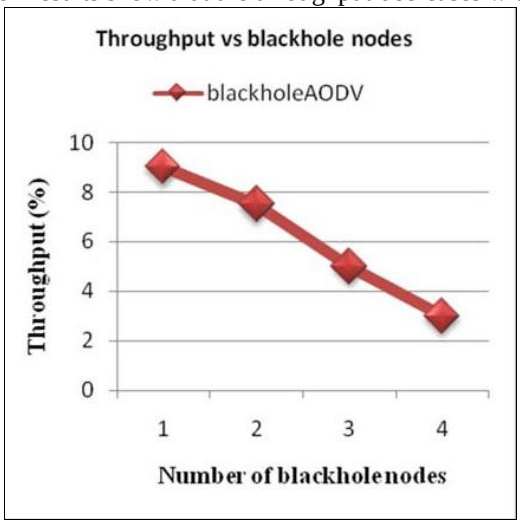

Figure 8: Impact of Number of Blackhole Nodes on Throughput

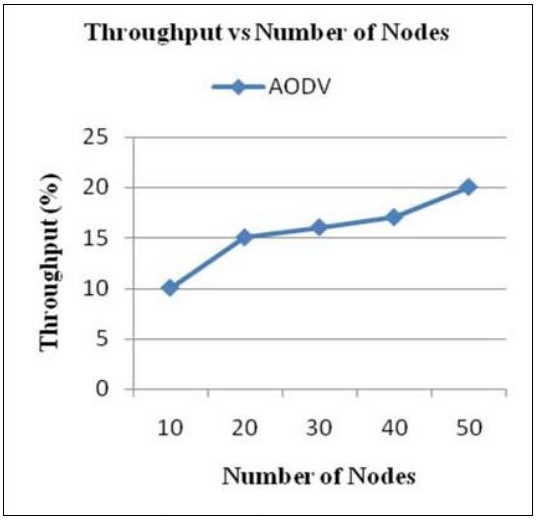

Figure 9: Impact of Number of Nodes on Throughput

We also studied the performance with varying the number of nodes. Fig. 9 shows the impact of number of nodes on throughput without blackhole attack. The number of nodes is varying from 10 to 50 with the step of 10. Simulation results show that when the number of nodes increases, the throughput increases for AODV protocol.

We have evaluated the End-to-End Delay with varying the mobility speed of nodes without blackhole node and with blackhole node. The mobility speed varies from 10m/s to 50m/s with the increase of 10. Fig. 10 illustrates the End-to-End Delay with blackhole attack and without blackhole attack. We observed that, there is increase in the average end-to-end delay without the effect of blackhole attack. This is due to the immediate reply from the malicious node because it doesn't check its routing table.

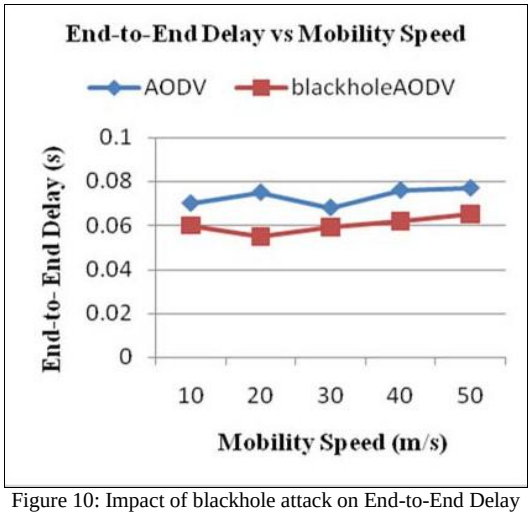

Figure 10: Impact of blackhole attack on End-to-End Delay

1.4 Related Work

There are a large number of methods or proposes have been authored to detect the black hole attack. In [8] *Hongmei Deng et al*. have been proposed a solution for single black hole node detection. In this method, each intermediate node send backs next hop information and RREP message. When the source node receives the reply message, it does not send the data packets immediately. The node takes out the next hop information from the reply packet and then sends a *Further-Request* to next hop for verification of route existence in between intermediate node who node who sends back the Further Reply (FRP) message, and that it has a route the destination node. In [9] *Luo Junhai et al*. proposed a method to prevent the black hole attack by authentication mechanism. The authentication mechanism, based on the hash function, the Message Authentication Code (MAC), and Pseudo Random Function (PRF), is proposed for black hole prevention on top of Ad-hoc On-demand Distance Vector (AODV). In [10] *M. Khalili shoja et al*. proposed a hash chain mechanism to prevent the black hole attack. Black hole attack is based on alteration of sequence number and hope count. In this mechanism, when an intermediate node receives RREQ or RREP, check an extra field to verify sequence number and hop count. The hash_RREQ and hash_RREP fields are add with RREQ and RREP field respectively. A seed value should be choosing randomly for calculating hash function.

1.5 Purpose of the work

Though there are many solutions proposed by various authors to deal with black hole attack, some of them are reviewed in this literature and found to exhibit the effect on performance in terms of increase in delay and overhead. In this literature considering the limitations (battery power, storage and processing power) of nomadic computing paradigm, we devise an algorithm that prevents from black hole attack at the cost of only marginal processing overhead.

2. Proposed Work

The proposed algorithm is simple and does not affect workings of either intermediate or destination node. It does not even modify the working of normal AODV but calls a preprocess called Pre_Process_RREP. The Process continues to accepts RREP packets and calls a process called Compare_Pkts(packet p1, packet p2) which actually compares the destination sequence number of two packets and selects the packet with higher destination sequence number if the difference between two numbers are not significantly high. Packet containing exceptionally high destination sequence number is suspected to be a malicious node and an ALERT message containing the node identification is generated which is broadcasted to neighbor nodes so that any message receive from such malicious node is discarded. A list of such malicious nodes can be maintained by the nodes participating in communication which can be used to prevent black hole attack. The algorithm is given in following fig 2.

```
Pre_Process_RREP(){
1 t=CURRENT_TIME+WAIT_TIME;
2 while (CURRENT_TIME < t){
3 packet Old_pkt=Cur_Pkt=Sel_Pkt=NULL;
4 Cur_Pkt=Compare_Pkts(packet New_Pkt, packet Old_Pkt};
5 If(Cur_Pkt!=NULL && Cur_Pkt!=Sel_Pkt){
6 Process_RREP(Cur_Pkt);
7 Sel_Pkt=Cur_Pkt;
8 }
9 f(Cur_pkt!=NULL && Cur_pkt =New_Pkt)
10 ld_Pkt= Cur_pkt;
11 ur_Pkt=NULL;
12 //End of while
13 //End of Pre Process RREP()
```

Fig.-2 Proposed Algorithm: at source node

```
1 Compare_Pkts(packet p1, packet p2){
2 Packet Selected_Pkt=NULL;
3 if(p1!=NULL && p1.dest_seq_no is exceptionally high){
4 generate ALERT message;
5 p1=NULL
6 }
7 if(p2!=NULL && p2.dest_seq_no is exceptionally high){
8 generate ALERT message;
9 p2=NULL
10 }
11 If(p1!=NULL && p2!=NULL)
12 Selected_Pkt=Packet containing higher
dest_seq_no.
13 else
14 If(p1!=NULL)
15 Selected_Pkt=p1;
16 else
17 Selected_Pkt=p2;
18 return Selected_Pkt;
```

Fig.-3 Proposed Algorithm calls Compare_Pkts.

3. Conclusions

Black hole attack is one of the major security challenges for MANETs. It is one of the active DoS in which a malicious node impersonates a destination node by sending a forged RREP to the source node. Although there exists many variants of black hole attack, in this paper we just studied the black hole attack by the existence of single malicious node in the network and its solution proposed by various authors. Review of the proposed solutions suggests that the

performance of the routing protocol is affected in terms of additional overheads, end-to-end delay and packet delivery ratio. In our future work, we would carry our research in optimizing the performance of a network having black hole attack.

4. References

[1] Latha Tamilselvan and Dr. V.Sankaranarayanan, "*Solution to Prevent Rushing Attack in Wireless Mobile Ad hoc Networks*".
[2] 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.
[3] Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu, "*Routing Security in Ad Hoc wireless Networks*", Network Security, 2005 Springer.
[4] Elizabeth M. Royer, and Chai-Keong Toh, "*A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks*," IEEE Personal Communications, pp. 46-55, April 1999.
[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*". International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov 2007.
[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 Wksp. Mobile Comp. Sys. And Apps. New Orleans, LA, Feb. 1999, pp. 90–100.
[8] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "*Routing Security in Wireless Ad-hoc Network*", IEEE Communications Magazine, Issue 40, pp 70-75, 2002.
[9] L. Junhai, X. Liu, and Y. Danxia, "*Research on multicast routing protocols for mobile ad-hoc networks*", Cmput Netw., vol. 52, no.5, pp. 988-997, 2008.
[10] M. Khalili, H. Taheri, S. Vakilinia, "*Preventing black hole attack in AODV through use of hash chain*", in Proc. of 19th Iranian Conference Electrical Engineering (ICEE), Iran, pp. 1- 6, 2011.