Investigation of Blackhole Attack on AODV in MANET

Anu Bala
University Institute of Engg. & Tech Deptt, Panjab University, Chandigarh,India
Email: anubala22@gmail.com

Raj Kumari and Jagpreet Singh
University Institute of Engg. & Tech Deptt, Panjab University, Chandigarh,India
Guru Teg Bahadur Khalsa Institute of Engineering and Technology, Malout, India
Email:rajkumari_bhatia5@yahoo.com and drjagz@gmail.com

***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.**

***Index Terms*—introduction, AODV routing protocol, blackhole attack in AODV, simulation environment and results, conclusion, acknowledgement, references**

I. 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. Ref. [1] Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Ref. [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.

Ref. [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. Ref. [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.

Ref. [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.

II. AODV Routing Protocol

Ref. [5] Ad-Hoc On-Demand Distance Vector (AODV) is a reactive routing protocol in which the network generates routes at the start of communication. Ref. [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. Ref. [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

doi:10.4304/jetwi.2.2.96-100

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 error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

The rest of this paper is organized as follows. In section II, we discuss the AODV routing protocol in detail. Section III describes the characteristics of the blackhole attack on AODV. Section IV provides the simulation environment and results. Finally we conclude in section V.

III. BLACKHOLE ATTACK in AODV

Ref. [5] In a blackhole attack, a malicious node can impersonates a destination node by sending a spoofed route packet to a source node that initiates a route discovery. Ref. [2] A blackhole has 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.

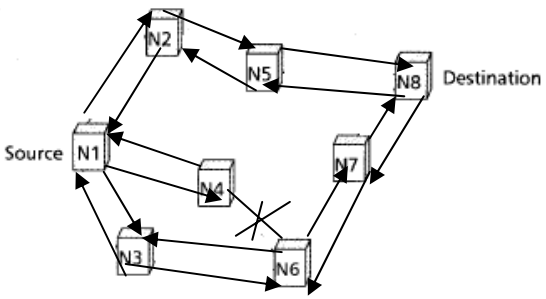

Figure 1: Blackhole attack in AODV

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.

IV. 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.

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.

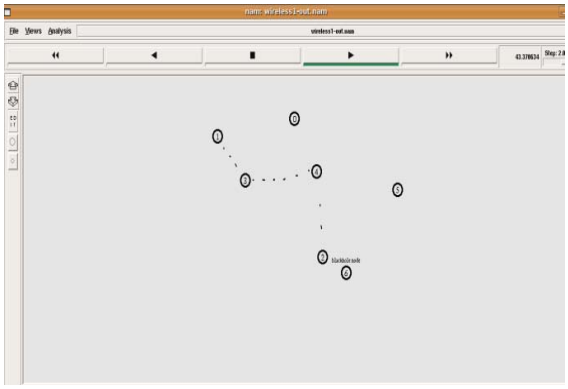

Figure 2 : Data flow between Node 1 to Node 2 via Node 3 and Node 4

Figure 3 : Link breakage and Data Loss

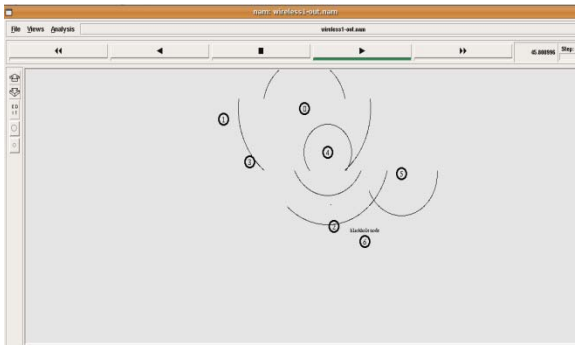

Figure 4 : Route Discovery Process

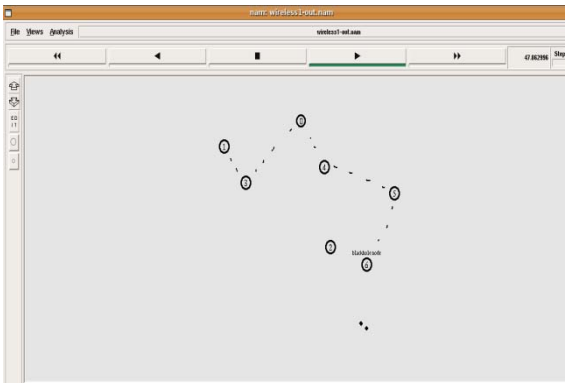

Figure 5 : Node 1 found new route and Node 6(Blackhole Node) absorbs the Data

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.

Table 2 shows the packet loss percentage on AODV with the presence and absence of blackhole nodes for four scenarios.

Table 2: Simulation Results with blackhole effect and without blackhole effect

Scenarios	**Total Loss of AODV**	**Total Loss of Black Hole AODV**	**Increase**
Scenario1	3.37	90.54	87.17
Scenario2	2.53	90.42	87.89
Scenario3	2.35	98.54	96.19
Scenario4	1.74	88.01	86.27

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).

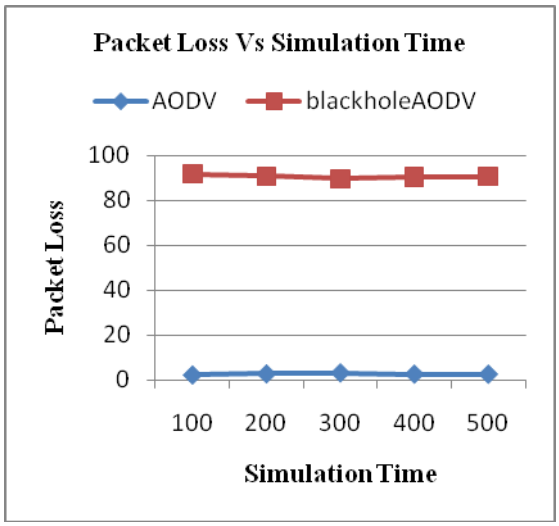

Figure 6 : Shows the Packet Loss of AODV and blackholeAODV

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 analysed 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.

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.

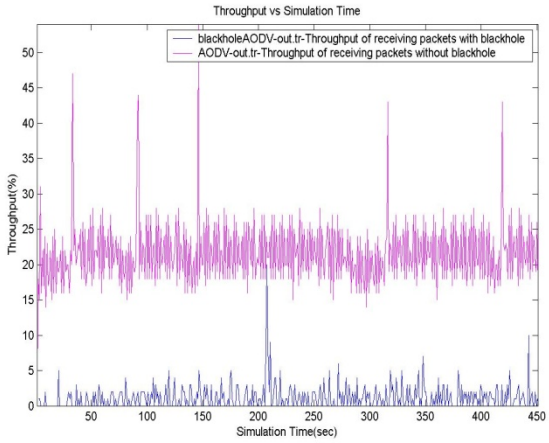

Figure 7: Impact of Blackhole Node on Throughput of Received Packets

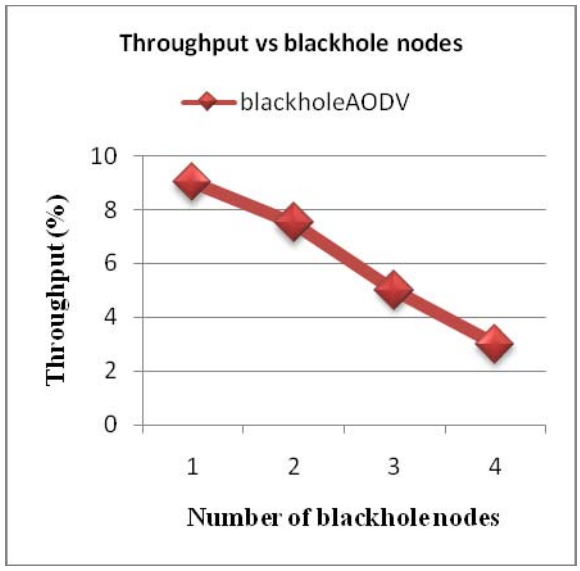

Figure 8: Impack of Number of Blackhole Nodes on Throughput

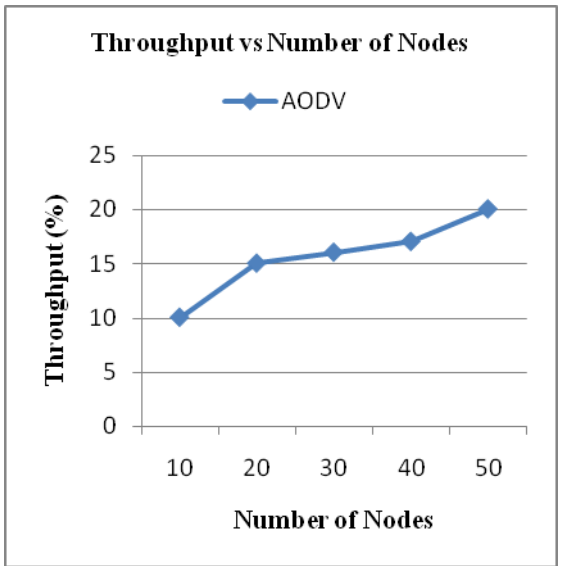

Figure 9: Impact of Number of Nodes on Throughput

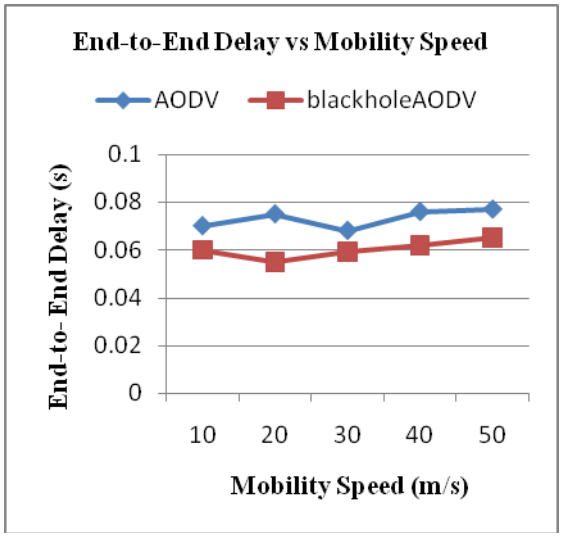

Figure 10: Impact of blackhole attack on End-to-End Delay

V. CONCLUSION

In this paper, we studied AODV in detail and the blackhole attack in AODV. We evaluate the effects of blackhole nodes on AODV in ad hoc networks. We simulate the blackhole behavior with the help of Network Simulator 2 and compared the performance of blackholeAODV with the original AODV in terms of packet loss percentage. The simulation results show that the packet loss increases in the network with a blackhole node. Simulation results also show that the throughput of the network is decreased with blackhole attack as compared to without blackhole attack.. When the number of blackhole nodes increases the throughput decreases. We observed that the End-to-end Delay without blackhole attack is slightly increased as compared to the effect of blackhole attack. The detection of blackhole in ad hoc networks is still to be a challenging task

ACKNOWLEDGEMENT

I would like to take the opportunity to thank people who guided and supported me during this process. Without their contributions, this project would not have been possible. I have a great pleasure in expressing my deep sense of gratitude and indebtedness to Mr. Jagpreet Singh, Lecturer, Teg Bahadur Khalsa Institute of Engineering and Technology, Malout and Ms. Rajkumari, lecturer, University Institute of Engineering and Technology, Panjab University, Chandigarh, my supervisor for their continuous guidance and invaluable suggestions at all the time during the research work. My special thanks to all my friends for being supportive in my hours of need. Finally, I would not forget to thank my parents for their love and blessings that support and encouraged me at every moment I need. They were the first ones that introduced the amazing world to me and encouraged me to explore the wonderful nature.

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 Wireles 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.

Anu Bala from Bhogpur (Jalandhar, India) and her date of birth is 22nd August 1985. She is a ME (IT) student in Information Technology at the University Institute of Engineering and Technology, Panjab University, Chandigarh, India. She received her B.Tech (CSE) degree from Panjab Technical University, jalandhar, India in 2006. Her research interests in the area of mobile ad hoc networks, especially ad hoc network security. Her recent work has focused on ad hoc routing protocol attacks.

She has worked as Lecturer for one year at IITT college of engg., Pojewal, Punjab, India.

Raj Kumari from chandigarh (India) and his date of birth is 6th June 1981. she received her M.Tech (IT) degree from GNDU, Amritsar, India in 2006 and her B.Tech from Panjab Technical University, Jalandhar, India in 2003.

She has works as Lecture for one year at college of Engg. Tangori, India. She has been working in UIET, Chandigarh, India since 2007

Jagpreet Singh from Malout (India) and his date of birth is 5th March 1983. He received his MS (Software System) degree from BITS Pilani, India and his B.Tech from Panjab Technical University, Jalandhar, India. He has been engaged in research on mobile adhoc network and he has enhanced algorithm of AODV protocol. He has been working in GTBIET, Malout, India since 2003. Two of his papers has been published in National Conferences.

1) Communication technology on UBI Quietest computing

2) Successful implementation of recruisite implementation of e-governance