Study and Performance Evaluation of AODV Protocols under Black Hole Attack in MANET

Arun Kumar Singh[1]
Pursuing M.Tech. Department of Information Technology,
S.I.T.M. Uttar Pradesh, India

Ravendra Ratan Singh[2]
Assistant Professor Department of Computer Science &
Engineering, S.I.T.M. Uttar Pradesh, India

Abstract: A Mobile ad-hoc network is a temporary network set up by wireless mobile computers moving arbitrary in the places that have no network infrastructure. Since the nodes communicate with each other, they cooperate by forwarding data packets to other nodes in the network. Thus the nodes find a path to the destination node using routing protocols. However, due to security vulnerabilities of the routing protocols, mobile ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. The data packets do not reach the destination node on account of this attack, data loss will occur. We simulated the black hole attack in various mobile ad-hoc network scenarios.

Keywords: MANET (Mobile ad hoc network), AODV (On-demand distance vector routing protocol), Blackhole attack.

I. INTRODUCTION

Mobile ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battle field or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To Support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector) [1], DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor nodes. Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the malicious node to the destination assuming it is a true path. Black Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface.

II. AODV ROUTING PROTOCOL

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. Additionally, AODV forms trees which connect multicast group members. AODV uses sequence numbers to ensure the freshness of routes. It is loop free, self- starting, and scales to large numbers of mobile nodes. 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. 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. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. 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.

III. BLACK HOLE ATTACK

A blackhole attack with highest destination sequence no and less hop count claiming a fresh route to the destination and then absorb all packet without forwarding them to the destination. In AODV routing protocol blackhole node absorb the network traffic and pretends to have fresh enough routes to all destinations requested by all the nodes. Blackhole node immediately responds with a fake RREP message that include highest dist. sequence no and less hop count. Source node found first RREP which come from blackhole node and start sending packet throw blackhole node and blackhole node dropped the entire packet.

Black hole algorithm

Step1: Set the black hole node highest destination sequence number.

Step2: Set black hole node Hop count with lowest value 1.

Step3: A source node broadcasts the RREQ message for any destination.

Step4: The black hole node immediately responds with an RREP message that includes the highest sequence number.

Step5: This message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination.

Step6: The source node then starts to send data packets throw black hole node.

Step7: If black hole node itself destination node then except the data packet otherwise drop the entire data packet.

IV. SIMULATION PARAMETERS

Simulator	Ns2(2.35)
Routing Protocol	AODV
Packet Size	512
Network Area	1180*500
Pause time	0,10,20,30,40
Traffic Generator	CBR
Speed	2.0m/s
Agent	UDP

These are simulation parameters which are used in this thesis.

V. RESULT

Simulation is performed with two conditions first condition are AODV without any attack and second conditions AODV under Blackhole Attack.

A) *Packet dropped*

The results for packet dropped are made for different number of pause time: 0, 10,20,30,40. The result of packet dropped for AODV and AODV with black hole node is show in following Figure 1.
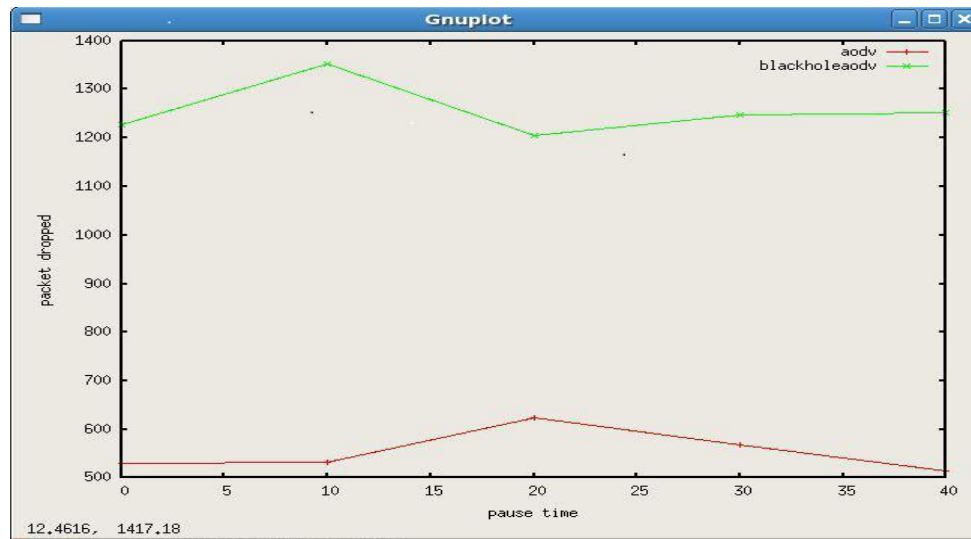

Figure 1

As shown in figure 1 Packet Dropped in AODV is less. AODV under blackhole attack packet dropped increases as compare to AODV.

B) End to End Delay

The results for end-to end delay are made for different number of pause time: 0, 10,20,30,40. The result of end-to-end delay for AODV, AODV with black hole node is show in following Figure 2.
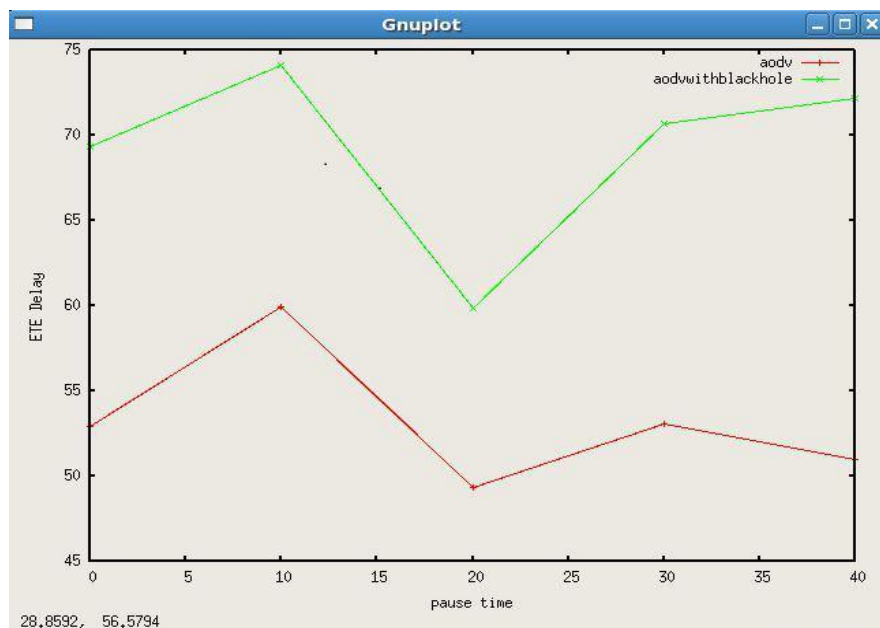

Figure 2

As shown in figure 2, end-to-end delay in AODV is varying for different pause tine. First it increases then decreases at a points sand again increases. It is not in consistent order.. The results show that end-to-end delay in AODV is minimum compared to AODV with blackhole node. It means that AODV is better in case of end-to-end delay.

VI. CONCLUSION

In this paper, we analyzed the effect of Black Hole in AODV routing protocols network in MANET. For this we implemented an AODV protocol that behaves as Black Hole in NS2. Simulations result show that in AODV without any attack it performed better No of packet loss is less but due to black hole attack in AODV it disturb hole network and dropped the packet.

VII. FUTURE WORK

In future work we created some IDS to overcome from blackhole attack and provide some security or authentication mechanism to Prevent blackhole attack. In this thesis we used UDP connection for data transfer but if we had used TCP connection between nodes due to ACK mechanism we overcome from black hole Attack.

References

1. W.Stallings, Cryptography and Network Security: Principles and Practices, 3rd edition, Prentice Hall, 2003.

2. Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir Das, "Ad Hoc On Demand Distance Vector (AODV) Routing", IETF Internet, Nov. 2002 (Work in Progress).

3. P. N. Raj, Prashant B. Swadas. "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV Based MANET", IJCSI International Journal of Computer Science Issues, 2:54-59, 2009

4. http://www.isi.edu/nsnam/ns/

5. NS by Example, http://nile.wpi.edu/NS/overview.html