Simulation of AODV under Black hole Attack in MANET

Vinay P.Viradia*, Vidhya P.Patel**
*(Department of Computer Engineering, Gujarat Technological University, India)
* (Department of Computer Engineering, Gujarat Technological University, India)

ABSTRACT

This paper analyzes the blackhole attack which is one of the possible attacks in ad hoc networks. In a blackhole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. By doing this, the malicious node can deprive the traffic from the source node. In this paper, we simulate the Ad hoc on Demand Vector Routing Protocol (AODV) under blackhole attack by considering different performance metric. The simulation results show the effectiveness of blackhole attack on AODV protocol.

***Keywords* -** AODV, Black Hole Attack, Security, MANET.

I. INTRODUCTION

Mobile ad hoc network (MANET) is a collection of mobile hosts without the required intervention of any existing infrastructure or centralized access point such as a base station. The applications of MANET range from a one-off meeting network, emergency operations such as disaster recovery to military applications due to their easy deployment. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks. These include passive eavesdropping, active interfering, impersonation, and denial-of-service Blackhole attack is one of many possible attacks in MANET. In this attack, a malicious node sends a forged Route REPLY (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node. By comparing the destination sequence number contained in RREP packets when a source node received multiple RREP, it judges the greatest one as the most recent routing information and selects the route contained in that RREP packet. In case the sequence numbers are equal it selects the route with the smallest hop count. If the attacker spoofed the identity to be the destination node and sends RREP with destination sequence number higher than the real destination node to the source node, the data traffic will flow toward the attacker. Therefore, source and destination nodes became unable to communicate with each other. In [14], the authors investigated the effect of blackhole attack when movement velocity and a number connection toward the victim node are changed, and proposed the detection technique at the destination node. In Section 2 of this paper, we discuss related work. In Section 3, we summarize the basic operation of AODV (Ad hoc On-Demand distance Vector Routing) protocol on which we base our work. In Section 4, we describe the effect of blackhole attack on AODV.

Section 5 presents the simulation of AODV under blackhole attack. Section 6 discusses the simulation result based on simulation experiments. Finally, Section 7 presents conclusion.

2. RELATED WORK

There indeed have been numerous attempts published in the literature that aim at countering the Black hole attacks. We survey them in the following. In [5], the authors discuss a protocol that requires the intermediate nodes to send RREP message along with the next hop information. When the source node gets this information, it sends a RREQ to the next hop to verify that the target node (i.e. the node that just sent back the RREP packet) indeed has a route to the intermediate node and to the destination. When the next hop receives a Further Request, it sends a Further Reply which includes the check result to thesource node. Based on information in Further Reply, the source node judges the validity of the route. In this protocol, the RREP control packet is modified to contain the information about next hop. After receiving RREP, the source node will again send RREQ to the node specified as next hop in the received RREP. Obviously, this increases the routing overhead and end-to-end delay. In addition, the intermediate node needs to send RREP message twice for a single route request. In [6], the authors describe a protocol in which the source node verifies the authenticity of a node that initiates RREP by finding more than one route to the destination. When source node receives RREPs, if routes to destination shared hops, source node can recognize a safe route to destination. Sanjay Ramaswamy, et al [7] proposed a method for identifying multiple black hole nodes. They are first to propose solution for cooperative black hole attack. They slightly modified AODV protocol by introducing data routing information table (DRI) and cross checking. Every entry of the node is maintained by the table. They rely on the reliable nodes to transfer the packets. In [8] proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. A technique is give to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. It was assumed in the solution that nodes are already authenticated and therefore can participate in the communication. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having 0 values is considered as malicious node and is eliminated.

In [9] proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the S.Ramaswamy to improve the accuracy. This algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperativeblack hole attacks.

3. THEORETICAL BACKGROUND OF AODV

AODV is a reactive routing protocol; that do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges. Further, the nodes do not have to discover and maintain a route to another node until the two needs to communicate, unless former node is offering its services as an intermediate forwarding station to maintain connectivity between other nodes [2]. AODV has borrowed the concept of destination sequence number from DSDV [5], to maintain the most recent routing information between odes.. Whenever a source node needs to communicate with another node for which it has no routing information, Route Discovery process is initiated by broadcasting a Route Request (RREQ) packet to its neighbors. Each neighboring node either responds the RREQ by sending a Route Reply (RREP) back to the source node or rebroadcasts the RREQ to its own neighbors after increasing the hop_count field. If a node cannot respond by RREP, it keeps track of the routing information in order to implement the reverse path setup or forward path setup. The destination sequence number specifies the freshness of a route to the destination before it can be accepted by the source node. Eventually, a RREQ will arrive to node that possesses a fresh route to the destination. If the intermediate node has a route entry for the desired destination, it determines whether the route is fresh by comparing the destination sequence number in its route table entry with the destination sequence number in the RREQ received. The intermediate node can use its recorded route to respond to the RREQ by a RREP packet, only if, the RREQ's sequence number for the destination is greater than the recorded by the intermediate node.

Instead, the intermediate node rebroadcasts the RREQ packet. If a node receives more than one RREPs, it updates its routing information and propagates the RREP only if RREP contains either a greater destination sequence number than the previous RREP, or same destination sequence number with a smaller hop count. It restrains all other RREPs it receives. The source node starts the data transmission as soon as it receives the first RREP, and then later updates its routing information of better route to the destination node. Each route table entry contains the following information:

- Destination node
- Next hop
- Number of hops
- Destination sequence number
- Active neighbors for the route
- Expiration timer for the route table entry

The route discovery process is reinitiated to establish a new route to the destination node, if the source node moves in an active session. As the link is broken and node receives a notification, and Route Error (RERR) control packet is being sent to all the nodes that uses this broken link for further communication. And then, the source node restarts the discovery process.

As the routing protocols typically assume that all nodes are cooperative in the coordination process, malicious attackers can easily disrupt network operations by violating protocol specification. This paper discusses about blackhole attack and providesrouting security in AODV by purging the threat of blackhole attacks

4. DESCRIPTION OF BLACKHOLE ATTACK

MANETs are vulnerable to various attacks. General attack types are the threats against Physical, MAC, and network layer which are the most important layers that function for the routing mechanism of the ad hoc network. Attacks in the network layer have generally two purposes: not forwarding the packets or adding and changing some parameters of routing messages; such as sequence number and hop count. A basic attack that an adversary can execute is to stop forwarding the data packets. As a result, when the adversary is selected as a route, it denies the communication to take place. In blackhole attack, the malicious node waits for the neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a blackhole as it swallows all objects; data packets. Fig. 1 Blackhole attacks in MANETs In figure 1, source node S wants to send data packets to a destination node D in the network. Node M is a malicious node which acts as a blackhole. The attacker replies with false reply RREP having higher modified sequence number. So, data communication initiates from S towards M instead of D.

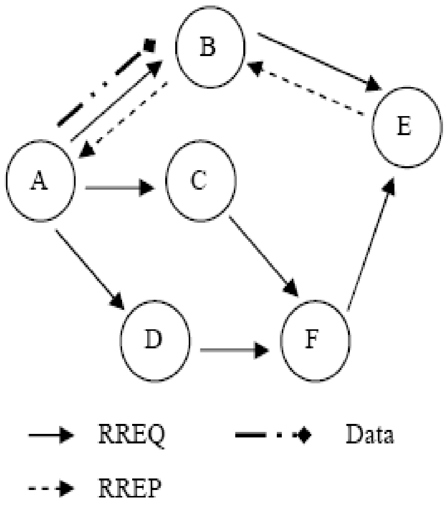

Fig: 1 Blackhole Attack

5. SIMULATION OF AODV UNDER BLACKHOLE ATTACK

For simulation, we set the parameter as shown in Table 1. Random Waypoint Model (RWP) [1] is used as the mobility model of each node. In this model, each node chooses a random destination within the simulation area and a node moves to this destinationwith a random velocity. The simulation is done using Network Simulator 2 to analyze the performance of the network by varying the nodes mobility. The metrics used to evaluate the performance are given below.

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.

Average End-to-End Delay: This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc. It is measured in milliseconds.

Table: 1 Simulation Parameters

Simulator	Ns-2(version 2.32)
Simulation Time	500 (s)
Number of Mobile Nodes	10, 15,20,25,30
Topology	750 * 750 (m)
Routing Protocol	AODV
Traffic	Constant Bit Rate (CBR)
Pause Time	10 (m/s)
Max Speed	20 (m/s)

Here, we assume that the blackhole attack take place after the attacking node received RREQ for the destination node that it is going to impersonate. We also assume that the communication started from a source node to a destination node and the node numbers of the source node, destination node and attacking node are 0, 1 and 9, respectively, as shown in Figure 5 (for 10 nodes). We have carried out the simulation by considering the different number of nodes 10, 15, 20, 25, and 30.

First, we investigate the packet delivery ratio of packet from source node 0 to destination node 1 in case there are connections from other nodes to the destination node. For the experiment, in Figure 2, nodes which are selected randomly from 2 to 8 (for 10 nodes), 2 to 18 (for 20 nodes) etc. (except the source node, destination node, and attacking node) generate traffic toward the destination node. Here, we perform experiment by changing the number of nodes generating the traffic from one to nine.

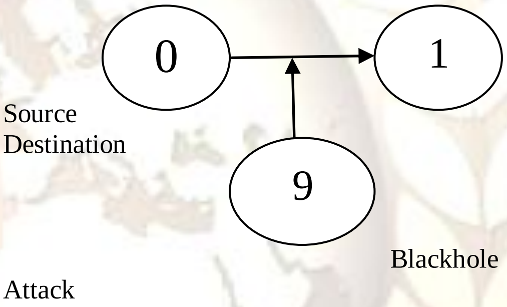

Fig: 2 Node Descriptions

From Figure 3, we can see that when the number of connection is 1, the more Dst Seq is increased in blackhole attack the more packet delivery ratio drops. However, when the number of connections increases, the packet ratio increases even when blackhole attack took place. This is because the destination node's Dst Seq tends to be higher than the attacker's Dst Seq, since attacker set the Dst Seq based on the Dst Seq contained in RREQ coming from the source node. We can see that the more the attacker increases the Dst Seq, the lower the packet delivery rate is.

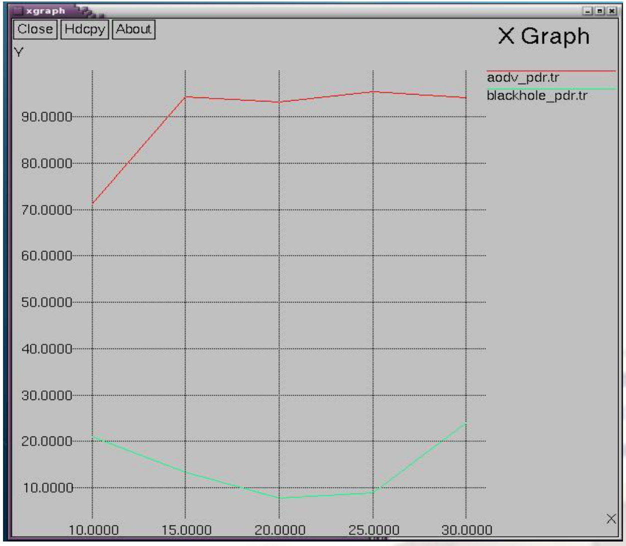

Fig: 3 Packet Delivery Ratios

6. SIMULATION RESULT AND DISCUSSION

Figure-3 shows the packet delivery ratio of normal AODV protocol and in the presence of blackhole attack. In AODV the packet delivery ratio is reduced to 80%. From this figure 3 it is clear that when the malicious node is present in the network, it reducethe packet delivery to destination. From the figure-4 it can be observed that, when blackhole attack initiates in network, there is nearly 21% increase in the average end-to-end delay.

7. CONCLUSION

Blackhole attack is one of the most important security problems in MANET. It is an attack that a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In this paper, we have analyzed the effect of blackhole attack on AODV protocol. The result shows significant degradation in performance of ad hoc on demand vector routing protocol (AODV) under blackhole attack.

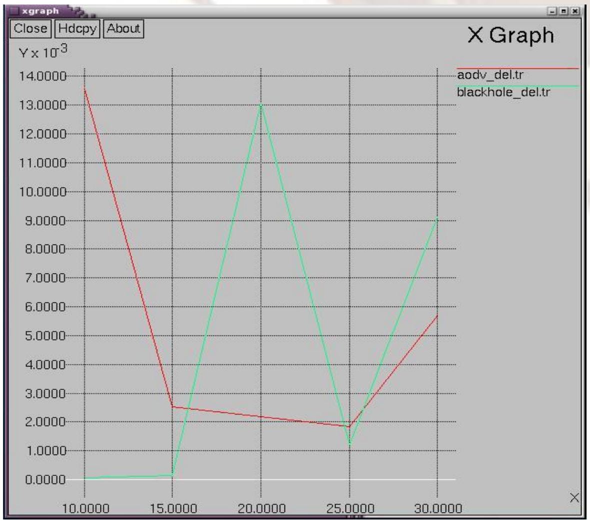

Fig: 4 Average End-to-End Delays

REFERENCES

[1] C. Bettstetter, G. Resta, and P. Santi, “The node distribution of the random waypoint mobility model for wireless ad hoc networks,” IEEE Transactions on Mobile Computing, vol. 2, no. 3, pp. 257-269, Jul./Sep. 2003.

[2] 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.

[3] Y. C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks,” in EigConference on Mobile Computing and Networking (Mobi- Com 2002), pp. 12-23, Sept. 2002.

[4] Y. C. Hu, D. B. Johnson, and A. Perrig, “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,” in The 4th IEEE Workshop on Mobile Computing Systems & Applications, pp. 3-13, June 2002.

[5] C. Perkins and P. Bhagwat. “Routing over multihop wireless network for mobile computers”. SIGCOMM ’94 : Computer Communications Review: 234-244, Oct. 1994.

[6] M. A. Shurman, S. M. Yoo, and S. Park, “Black hole attack in wireless ad hoc networks.” In: Proceedings of the ACM 42nd Southeast Conference (ACMSE’04), pp 96-97, Apr. 2004.

[7] Y. A. Huang and W. Lee, “Attack analysis and detection for ad hoc routing protocols,” in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID’04), pp. 125-145, French Riviera, Sept. 2004.

[8] Tamilselvan, L. Sankaranarayanan, V. “Prevention of Blackhole Attack in MANET”, Journal of Networks, Vol.3, No.5, May 2008.

[9] S. Lee, B. Han, and M. Shin, “Robust routing in wireless ad hoc networks,” in ICPP Workshops, pp. 73, 2002.

[10] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, “Performance comparison of two on-demand routing protocols for ad hoc networks,” IEEE Personal Communications, pp. 16-28, Feb. 2001.

[11] C. E. Perkins, E. M. B. Royer, and S. R. Das, Ad hoc On-Demand Distance Vector (AODV) routing, RFC 3561, July 2003.

[12] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. B. Royer, “Authenticated routing for ad hoc networks,”

IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598-610, Mar. 2005.

[13] M. A. Shurman, S. M. Yoo, and S. Park, “Black hole attack in wireless ad hoc networks,” in ACM 42nd Southeast Conference (ACMSE’04), pp. 96-97, Apr. 2004.

[14] W. Wang, Y. Lu, and B. K. Bhargava, “On vulnerability and protection of ad hoc on-demand distance vector protocol,” in The 10th International Conference on Telecommunications (ICT’03), vol. 1, pp. 375-382, French Polynesia, Feb. 2003.

[15] M. G. Zapata, Secure Ad Hoc on-demand Distance Vector (SAODV) Routing, IETF Internet Draft,draft-guerrero-manet-saodv-03, Mar. 2005