Detection of Malicious Nodes in MANET

Vandana Tripathi
M.TECH Scholar
SIIT GORAKHPUR
Vandana2905@gmail.com

***ABSTRACT*- Manet is a cluster of wireless mobile computer where node shift in self directed manner in any way. The purpose of this paper is to provide a framework for understanding the Black Hole attack in ad hoc networks and evaluate its damage in the association. We made our simulations using NS-2 (Network Simulator version 2) simulation plan that consists of the set of all network protocols to replicate many of the offered network topologies. Having implemented a fresh routing protocol which simulates the black hole we performed tests on diverse topologies to evaluate the network performance without and with black holes in the network. As expected, the throughput in the network was deteriorating considerably in the existence of a black hole. Afterwards, proposed a solution to remove the Black hole effects in the AODV network in terms of packet delivery ratio, end-to-end delay, and throughput and routing overhead.**

***KEYWORDS*-** *MANET (mobile ad-hoc network), DSR (Dynamic Source Routing), CBR (Constant Bit Rate),NS-2 (Network Simulator version 2) , Packet Delivery Ratio (PDR*).

1. INTRODUCTION

A MANET(mobile ad-hoc network) is a self-configuring infrastructure-less network

Chitrangada Choubey
Asst. professor
SIIT GORAKHPUR
chitrangada111@gmail.com

of mobile nodes connected by wireless links.

MANET is a type of multi-hop system, communications less and the most significant self-organizing. Due to wireless and spread nature there is an immense challenge for system protection designers.

A Black hole is a spiteful node that wrongly replies for route requirements without having an active route to the destination and exploit the Routing Protocol to announce itself as having a fine and valid path to a destination node.

2. Black Hole Attack

In AODV networks black hole node absorb the network traffic and drop all packets. A black hole is a node that forever responds positively with a RREP message to every RREQ, even though it does not really have a suitable route to the destination node. Since a black hole node does not have to check its routing table, it is the first to respond to the RREQ in most cases. Then the source routes data through the black hole node, which will drop all the data packets it received rather than forwarding them to the destination.

In this way the malicious node can easily misroute lot of network traffic to itself and could cause an attack to the network with very little effort on it.

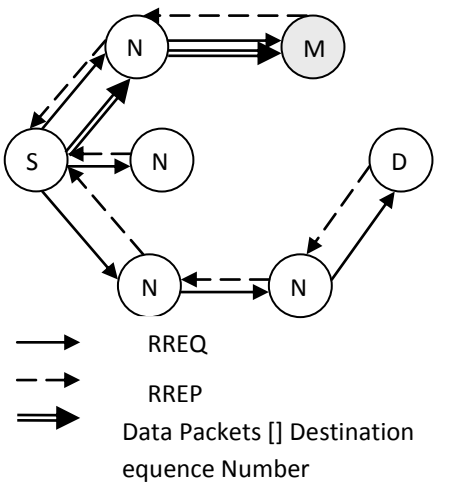


Figure 1 Black Hole Attack

In figure 1 Destination Sequence Number is a 32-bit integer associated with every route and is

used to decide the freshness of a particular route. The larger the sequence number, the fresher is the route. Node N3 will now send it to node. Since node N1 and node N2 do not have a route to node D, they would again broadcast the RREQ control message. RREQ control message broadcasted by node N3 is also expected to be received by node M (assumed to be a malicious node). Thus, node M being malicious node, would generate a false RREP control message and send it to node N3 with a very high destination sequence number, that subsequently would be sent to the node S. However, in simple AODV, as the destination sequence number is high, the route from node N3 will be considered to be fresher and hence node S would start sending data packets to node N3. But in our proposed AODV before sending data packets firstly source node will check the difference between sequence numbers. If it is too large, obviously the node will be a malicious one, and it will be isolated from the network. Otherwise it simply transfers the data packets to the destination node. In a Black Hole Attack, after a while, the sending node understands that there is a link error because the receiving node does not send TCP ACK packets. If it sends out new TCP data packets and discovers a new route for the destination, the malicious node still manages to deceive the sending node. If the sending node sends out UDP data packets the problem is not detected because the UDP data connections do not wait for the ACK packets.

3. ALGORITHM

Algorithm: ReceiveReply (RREP) Method

Notation: **SN:** Source Node, **IN:** Intermediate Node, **FRqI:** Further Request Information, **DN:** Destination Node, **NHN:** Next Hop Node **FRpI:** Further Reply Information, **Reliable Node:** The node through which the SN has routed data, **DRI:** Data Routing Information

Step 1: (Initialization Process)

SN broadcasts RREQ

Step 2: (Storing Process)

1. SN receives RREP
2. IF (RREP is from DN or a reliable node) then
3. {
4. Route data packets (Secure Route)
5. }
6. else {
7. Do {

Step 3: (Identify and Remove Malicious Node)

1. SN Send FRqI and ID of NHN that send RREP
2. SN Receive FRpI, NHN of IN, DRI entry for IN
3. IF (IN is a reliable node and send FRpI) then {
4. Check IN using DRI entry
5. And Route data packets (Secure Route or Reliable Node)
6. else {
7. Insecure Route
8. IN is a black hole

Step 4: (Node Selection Process)

1. Node from IN that generated RREP is black hole node
2. }}else
3. Current IN = NHN
4. } While (IN is NOT a reliable node) }
5. **Step 5: (Continue default process)**
1. Repeat step 3 and 4 until the intermediate node is not reliable node.
2. Call FRpI method of default AODV Protocol.

4. EXAMPLE

As an example from figure 2 node M responds to source node *S* with RREP message. Here the black hole node (M)

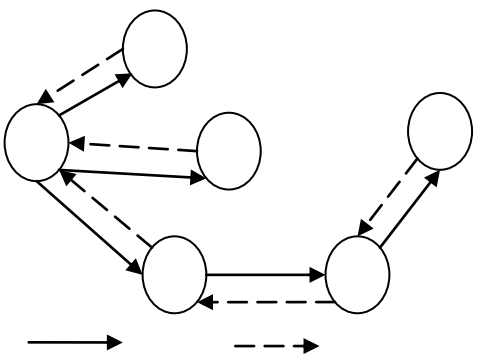


Figure 2 Detection of Malicious node in the Network

lies about using the path by replying with the DRI value. Upon receiving RREP message from M, the source node *S* checks its own DRI table to see whether M is a reliable node. Since *S* has never sent any data through M before, M is not a reliable node to *S*. Therefore, *S* sends FRqI to M and asks *a*bout three things: (i) whether M has routed any data (ii) who is M's next hop, and (iii) whether M has routed before. When the source node contacts node 3 via alternative path S-2- 3 to cross check the validity of the claims of node M, node 3 responds negatively. Since node 3 has neither a route to node M nor it has received data packets from node M. Based on this information, node *S* can infer that M is a black hole node. Then S discards any further responses from M and looks from a valid alternative route to *D*. This process is a one-time procedure which should be affordable for the purpose of security.

5. RESULTS AND SIMULATION

Simulation is done using the NS-2 (network simulator). The numbers of nodes we have considered for simulation are 10 to 70 mobile nodes in the terrain area of 800m * 800m. And also use some CBR (Constant Bit Rate) associations with packet length of 512 bytes to follow traffic over the network. All nodes independently repeat this behavior and mobility is varied by assembly each node motionless for a period of pause time.

Table 1: Simulation Parameters

Parameters	Values
Network size	800m * 800m
Number of nodes	10 to 70
Max speed/mobility	50 m/s
Wait/Pause time	10 sec
Traffic model	CBR
Routing protocol	AODV
Simulation time	900 sec
Number of sources	5

6. PERFORMANCE EVALUATION

The metrics used in evaluating the performance are:

A-Packet Delivery Ratio (PDR): It is the percentage of the number of data packets received by the destination to the number of data packets sent by the sources. These evaluate the skill of the protocol to carry data packets to the destination in the presence of spiteful nodes .It is clear from figure 3 that PDR of AODV is a lot affected by the spiteful nodes where as the PDR of future AODV is protected to it. It is represent by P and considered as:

$$P = \frac{number\ of\ data\ packets\ received}{numberof\ data\ packets\ sent} * 100$$

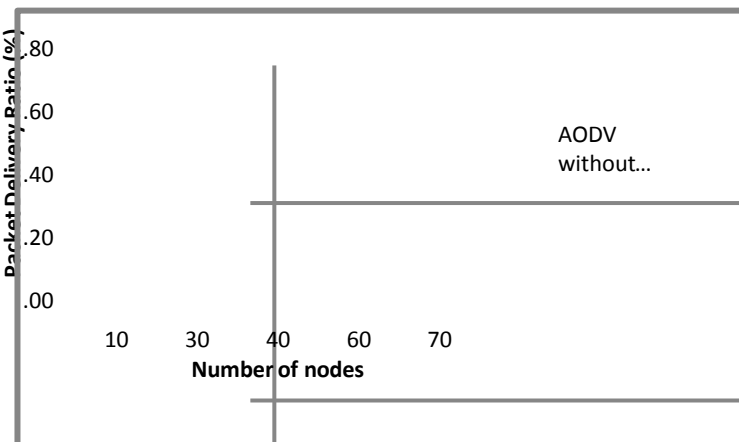


Figure 3 Packet Delivery Ratio vs. number of Nodes

Figure 3 confirms that while proposed AODV is safe agaThis finst black holes, AODV is not. This is mostly due to the reality that our protocol detects the attacker and allows the source nodes to keep away from it. The PDR decrease when there is spiteful node (black hole) in AODV since some packets is drop due to attack. This way the number of properly received packet is very less than the number of transmitted packets.

***B*- End-to-End Delay:** This is average delay between the sending of packets by the source and its receipt by the receiver. It means it is divergence between the receiving time and sending time. This include all probable delays caused by buffer during data gaining, route discovery, queuing, processing at middle nodes, retransmission delays, broadcast time, etc. It is measured in milliseconds or sec and denoted by D and calculated as:

$$D = \frac{\sum_{i=1}^{n} d_i}{n}$$

Where d_i is a time for end-to-end delay of data packets at i^{th} position.

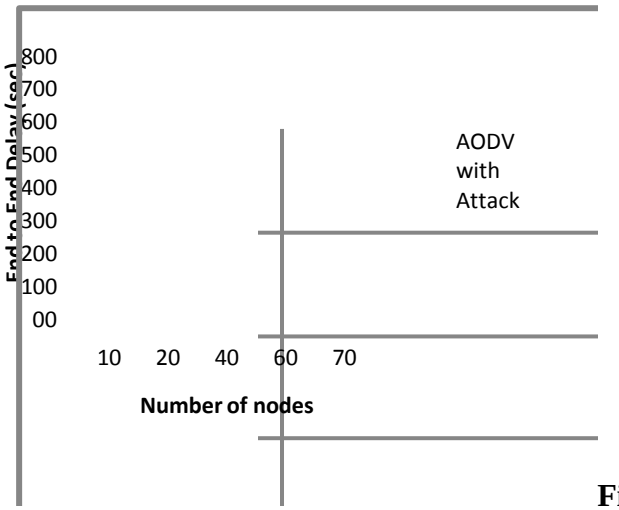


Figure 4 End-to-End delays vs. number of Nodes

The figure 4 shows the contact of the Black hole attack to the Networks end-to-end delay. The end-to-end delay of the network also decreases due to black hole effect as compare to without the effect of black hole attack.

***C- Throughput*:** A network throughput is the average rate at which communication is effectively delivered between a receiver (destination node) and its sender (source node). It is also referred to as the proportion of the amount of data received from its sender to the time the last packet reach its destination. Throughput can be calculated as bits per second (bps), packets per second or packet per time slot. In other words throughput is the number of data packets delivered from source node to destination node per unit of time. Throughput for the case with no attack is higher than the throughput of AODV under attack because of the packets discarded by the spiteful node. This is because of the fewer routing forwarding and routing traffic. Here the spiteful node discards the data rather than forwarding it to the destination, thus effecting throughput.

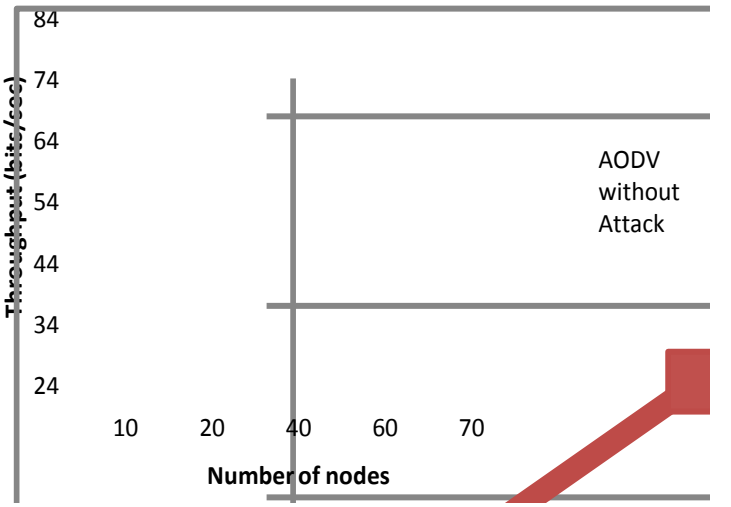
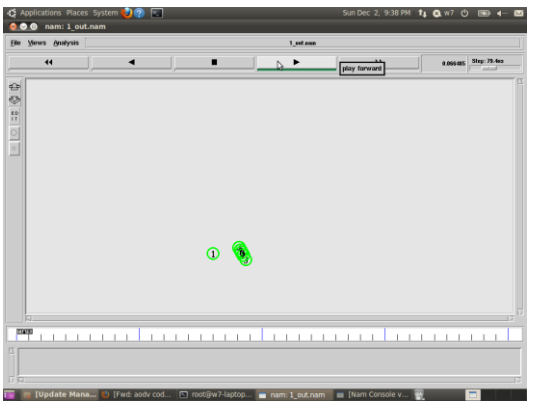
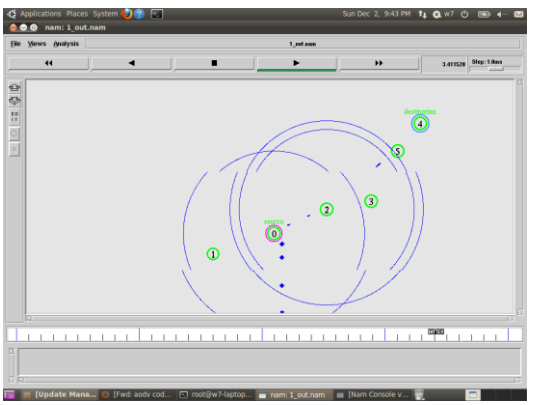


Figure 5 Throughput vs. number of Nodes

Figure 5 shows that the throughput of AODV in the occurrence of malicious node. We have experiential that the higher number of sources give less dissimilarity in throughput as compare to less number of sources. This is because the higher numbers of sources have more jamming. Over all, AODV ensures consistent routing paths with in the network, helping in lowering the delay. As throughput is the ratio of the total data received from source to the time it takes till the receiver receives the last packet. A lower delay translates into higher throughput. The overall low throughput of AODV is due to route reply. As the malicious node immediately sends its route reply and the data is sent to the malicious node which discard all the data. The network throughput is much lower.

7. SNAPSHOT





8. REFERENCES

[1] Y. R. Tsai and S. J. Wang, "Two-tier authentication for cluster and individual sets in mobile ad-hoc networks," *Comput. Netw.*, vol. 51, no. 3, pp. 883–900, 2007.

[2] H. Deng, W. Li and D. P. Agrawal, "Routing Security inWireless Ad Hoc Networks". University of Cincinnati, IEEE Communication Magazine, October 2002.

[3] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks 38 (2002) 393–422.

[4] E. Royer and C. E. Perkins, "Multicast Operation of the Ad-hoc On-Demand Distance Vector Routing Protocol", in Proceedings of MobiCom '99, Seattle, WA, Aug. 1999, pp. 207-218.

[5] B. Johnson, A. Maltz, "The Dynamic Source Routing Protocol for MANETs", Oct. 1999, IETF Draft, pp.1- 49.

[6] W., L. Olariu, S., A two-zone hybrid routing protocol for mobile ad hoc networks, Parallel and Distributed Systems, IEEE Transactions on Vol.15(12):1105–1116, Dec. 2004.

[7] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.

[8] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional 2004.