ISSN : 2231-0711
IJCSET |September 2011 | Vol 1, Issue 8, 447-450

Modified AODV to Prevent Black Hole Attacks in MANET

S.Thirumal
Department of Computer Science,
Aringar Anna Govt. Arts College,Cheyyar, Tiruvannamalai District,Tamil Nadu, India

Abstract—Mobile Adhoc 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. So security in MANET is a complex issue. There are many routing protocols that establish the routes between the nodes in the network. The control towards the management of the nodes in the MANET is distributed. This features does not give assurance towards the security aspects of the network. There are many routing attacks caused due to lack of security. In this paper, therefore, we attempt to focus on analyzing and improving the security of one of the popular routing protocol for MANET viz. the Adhoc On Demand Distance Vector (AODV) routing protocol. Our focus specifically, is on ensuring the security against the Blackhole Attack. The proposed solution is capable of detecting black hole nodes in the MANET at the initial stage itself. The simulation study is performed using Network Simulator NS-2.34.

Keywords: ***Mobile Ad-hoc Network, Black Hole Attack, Simulation, Security, Network simulator***

INTRODUCTION

Wireless 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 battlefield 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), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector) [2]. Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network. 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, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped [3]. 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. In any case, nodes in the network will constantly try to find a route for the destination, which makes the node consume its battery in addition to losing packets.

In this study, I simulated the Black Hole attack in wireless ad-hoc networks and evaluated its damage in the network. I made our simulations using NS-2 (Network Simulator version 2) simulation program that consists of the collection of all network protocols to simulate many of the existing network topologies. Even though NS-2 contains wireless ad-hoc routing protocols, it does not have any modules to simulate malicious protocols. Thus, to simulate Black Hole attacks, we first added a new Black Hole protocol into the NS-2. We started our study by writing a new AODV protocol using C++, to simulate the Black Hole attack. Having implemented a new routing protocol which simulates the black hole we performed tests on different topologies to compare the network performance with and without black holes in the network. As expected, the throughput in the network was deteriorated considerably in the presence of a black hole. Afterwards, we proposed an IDS solution to eliminate the Black Hole effects in the AODV network. We implemented the solution into the NS-2. and evaluated the results as we did in Black Hole implementation. As a result, our solution is eliminated the Black Hole effect with %24.38 success.

AD-HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages [5]. Thanks to these control messages, AODV Routing Protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network bandwidth utilization with small size control messages. The most distinguishing feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination

when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes sure the route to the destination does not contain a loop and is the shortest path. Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are control messages used for establishing a path to the destination, sent using UDP/IP protocols. When the source node wants to make a connection with the destination node, it broadcasts an RREQ message. This RREQ message is propagated from the source, received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbors. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination. Figure 9 shows how the RREQ message is propagated in an ad-hoc network.

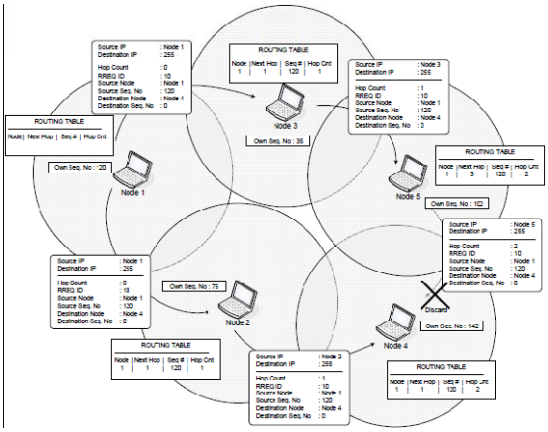

Fig 1. Propagation of RREP messages.

Fresh enough means that the intermediate node has a valid route to destination formed a period of time ago, lower than the threshold. While the RREQ packet travels through the network, every intermediate node increases the hop count by one. If an RREQ message with the same RREQ ID is received, the node silently discards the newly received RREQs, controlling the ID field of the RREQ message. When the destination node or intermediate node that has fresh enough route to the destination receive the RREQ message they create an RREP message and update their routing tables with accumulated hop count and the sequence number of the destination node. Afterwards the RREP message is unicasted to the source node. The difference between the broadcasting an RREQ and unicasting RREP can be seen from Figures 9 and 10. While the RREQ and the RREP messages are forwarded by intermediate nodes, intermediate nodes update their routing tables and save this route entry for 3 seconds, which is the ACTIVE_ROUTE_TIMEOUT constant value of AODV protocol.Thus the node knows over which neighbor to reach at the destination. In terminology, the neighbor list for destination is labeled as “Precursor List”.

SEQUENCE NUMBERS

Sequence Numbers serve as time stamps and allow nodes to compare how fresh their information on the other node is. However when a node sends any type of routing control message, RREQ, RREP, RERR etc., it increases its own sequence number [5]. Higher sequence number is more accurate information and whichever node sends the highest sequence number, its information is considered and route is established over this node by the other nodes. The sequence number is a 32-bit unsigned integer value (i.e., 4294967295). If the sequence number of the node reaches the possible highest sequence number, 4294967295, then it will be reset to zero (0). If the results of subtraction of the currently stored sequence number in a node and the sequence number of incoming AODV route control message is less than zero, the stored sequence number is changed with the sequence number of the incoming control message. In Figure 2, while Node 2 forwards the RREP message coming from Node 3, it compares its own previously stored sequence number with that of Node 3. If it notices that the sequence number is newer than its own, then it changes its route table entry as necessary.

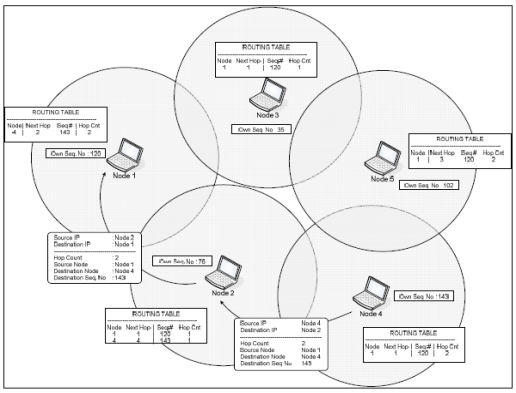

Fig 2. Updating the Sequence Number with fresh one

BLACK HOLE ATTACK

In an ad-hoc network that uses the AODV protocol, a Black Hole node absorbs the network traffic and drops all packets. To explain the Black Hole Attack we added a malicious node that exhibits Black Hole behavior in the scenario of the figures of the previous section.

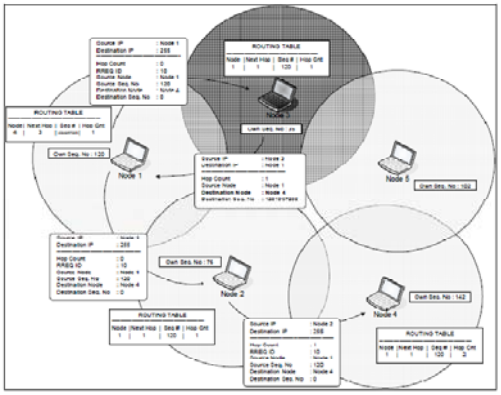

Fig 3. Illustration of Black Hole Attack

In this scenario shown in Figure 3, we assume that Node 3 is the malicious node. When Node 1 broadcasts the RREQ message for Node 4, Node 3 immediately responds to Node 1 with an RREP message that includes the highest sequence number of Node 4, as if it is coming from Node 4. Node 1

assumes that Node 4 is behind Node 3 with 1 hop and discards the newly received RREP packet come from Node 2. Afterwards Node 1 starts to send out its data packet to the node 3 trusting that these packets will reach Node 4 but Node 3 will drop all data packets. 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.

SOLUTION FOR BLACK HOLE ATTACK AND ITS EFFECTS

The proposed modifications to the AODV routing protocol includes addition of two new type of data packets (Test and Test_Ack) , a new parameter HopCount_dest is added to the RREP which gives the hop count between the destination node and the intermediate node which sends the route reply RREP to the source node and some changes to the SendReply and ReceiveReply methods. The threshold levels T1 is used to check whether a given node is malicious or not.

Algorithm :

Let us consider S is the source node , D is the destination node, I is an intermediate node and H is the Hop count between source and destination and the threshold value T1 = 4294967000. The source node S , broadcasts RREQ packets when it wants to send data packets to the destination node D.

i. After receiving the route request packet RREQ packets the intermediate nodes (may be a Black Hole node) can also send RREP packets to the source node .
ii. When the RREP packets are received by the source node from various intermediate nodes and destination node it selects the route based on the sequence number and the hop count.
iii. After selecting a route to find whether the reply is from a malicious intermediate node, it checks the sequence number. If it is greater than T1 it simply discards the RREP packet assuming that the RREP packet is from a malicious node.
iv. If it is less than T1 then it extracts the information from RREP packet and then sends a Test packet to the destination node in the selected route path. The data packet will reach the destination node through the intermediate node I.
v. When the destination node D, receives a Test packet it sends back a Test_Ack packet to the source node in the same route path.
vi. If the source node S, receives the Test_Ack packet from the destination node with in a prefixed time delay it verifies whether the Test_Ack is from the destination node D or from the intermediate node I (since if the node I is malicious node it impersonates the destination node D and sends Test_Ack packet to the source node S). This is accomplished by comparing the Hop Count in the RREP packet sent by the intermediate node I with the Hop Count in the Test_Ack packet.
vii. If the node I is not malicious then both the Hop counts will be same. If they are not same then it is clear that the malicious intermediate node I is a BlackHole node.
viii. If it is not a malicious node the source node forwards all the data packets waiting in the queue for the destination node in the selected route path or else starts fresh route discovery process.

Here in this process as a general solution we have used threshold value T1 to verify whether the RREP is from a malicious node or not. Even after the preliminary check as a secondary confirmation we have used the Test and Test_Ack packets. These packets are intentionally sent to check whether the destination node D is reachable in the selected path or not. The Hop count information available in the RREP is compared with Hop count in the Test_Ack to further confirm that the intermediate node I is not malicious node.

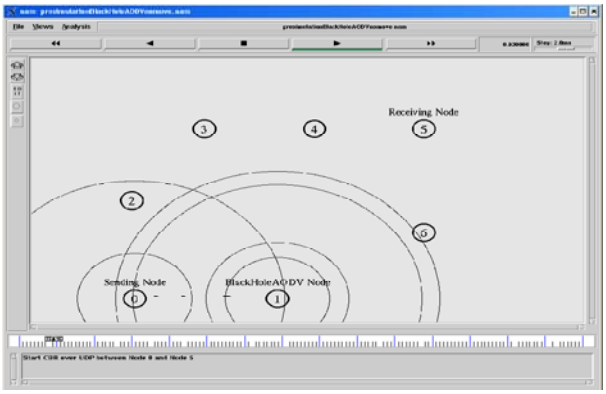

Fig 4.Test simulation screen shot

SIMULATIONS & RESULTS

To analyze the performance of BlackHole nodes in AODV and modified ADOV routing protocol we used NS-2.34. In our simulation scenarios the total number of mobile nodes is kept constant as 50. The routing protocol used in all the simulations for general node is AODV. In each scenario the number of BlackHole Node is increased to evaluate corresponding increase in Packet Loss percentage.

UDP connections are established between even numbered nodes (0 (zero) included) and odd numbered nodes and we used 50 nodes in the scenarios where Node 48 and Node 49 did not have a connection to any other node in the network. In the scenarios, even numbered nodes (Node 0 - Node 46) are the sending nodes and odd numbered nodes (Node 1 - Node 47) are the receiving nodes and the even numbered nodes send the packets to the next odd numbered nodes, for example Node 0 to Node 1, Node 2 to Node 3, Node 4 to Node 5 etc. Thus, we could count the sent and received packets between any 2 nodes. In the scenarios, UDP agents are attached to the even numbered nodes and NULL agents are attached to odd numbered nodes. In all the scenarios, we have a total of 24 connections between 48 nodes and all of these connections are always between the same nodes. But, in each scenario, every single node is placed in different coordinates and exhibits different movements. This helps us get different results with the same nodes and for scenario we increased the mobility speed of the nodes. We attach the CBR

(Constant Bit Rate) application that generates constant packets through the UDP connection. The total simulation time in all the scenarios is 200 Seconds In our scenarios CBR parameters are;

Packet Size : 512 bytes Data Rates : 10 Kbits and we did not use random packets in the simulation.

We first try to evaluate the packet loss. Therefore we counted how many packets are sent by the sending nodes and how many of them reached the receiving nodes. We noticed that the percentage of data loss in the presence of the Black Hole AODV is increased more than the normal AODV network simulations in all scenarios. After implementing proposed modifications in the AODV successfully then, we performed the same simulations on the scenarios we used for the BlackHole nodes to compare the performance of modified AODV.

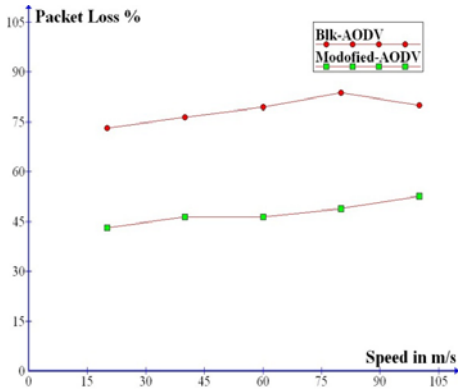

Fig 4. Packet Loss vs Speed

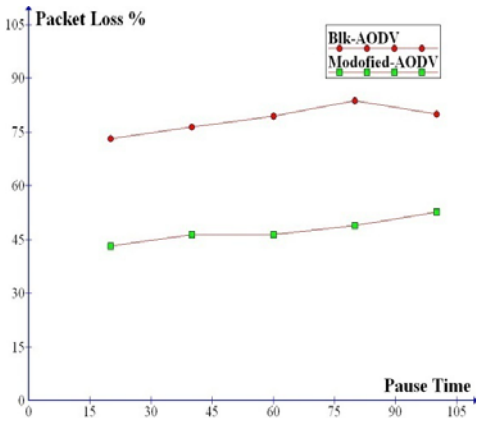

Fig 5. Packet Loss vs Pause Time

CONCLUSION

In this study, we analyzed effect of the Black Hole in an AODV Network. For this purpose, we implemented an AODV protocol that behaves as Black Hole in NS-2. We simulated five scenarios where each one has 50 nodes that use AODV protocol and also simulated the same scenarios after introducing one Black Hole Node into the network. Moreover, we also implemented a solution that attempted to reduce the Black Hole effects in NS-2 and simulated the solution using the same scenarios. Our simulation results are analyzed below:

Having simulated the Black Hole Attack, we saw that the packet loss is increased in the ad-hoc network. The graph results show the difference between the number of packets lost in the network with and without a Black Hole Attack. This also shows that Black Hole Attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack in the network. If the number of Black Hole Nodes is increased then the data loss would also be expected to increase.

On an average AODV network has normally 3.21 % data loss and if a Black Hole Node is introducing in this network data loss is increased to 82.59 %. As 3.21 % data loss already exists in this data traffic, Black Hole Node increases this data loss by 79.38 %. When we used modified AODV protocol in the same network, the data loss decreased to 48 % on an average. These two results show that our solution reduces the Black Hole effects by 31.8 % as packet loss in a network using modified AODV

REFERENCES

1.Mohammad Al-Shurman and Seong-Moo Yoo " Black Hole Attack in Mobile Ad Hoc Networks " April 2004 Proceedings of the 42nd SouthEast regional conference. ACM-SE 42.

2. P. Misra,. "Routing Protocols for Ad Hoc Mobile Wireless Networks", http://www.cse.wustl.edu/~jain/cis788-99/adhoc_routing/index.html, 14 May 2006.

3. Hao Yang et al., "Security in mobile ad hoc networks: challenges and solutions", IEEE Wireless Communications, Volume 11, Issue 1, Page(s): 38 – 47, Feb. 2004

4 .G. Vigna, S. Gwalani and K. Srinivasan, "An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks", Proc. of the 20th Annual Computer Security Applications Conference (ACSAC'04).

5. C. E. Perkins and E. M. Royer, "The Ad hoc On-Demand Distance Vector Protocol," in Ad hoc Networking, C. E. Perkins, Ed.Addison-Wesley, 2000, pp. 173–219.

6. S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Ad Hoc Networks", Proc. 6th Annual Int'l. Conf. Mobile Comp. and Net., Boston, MA. pp. 255-265. August 2000.

7. D. Johnson, D. Maltz and J. Broch, "DSR the Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks". Ad Hoc networking, Chapter 5, page 139-172. Addison-Wesley, 2001.

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

9. F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks", Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, 1999. University of Cambridge Computer Laboratory.

10. C.Perkins, "(RFC) Request for Comments – 3561", Category: Experimental,Network, Working Group, July 2003.

11. K Fall and K. Varadhan, The NS Manual, November 18, 2005, http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf. 25 July 2005.

12. Virtual InterNetwork Testbed, http://www.isi.edu/nsnam/vint, 14 May 2006.

13. NS by Example, http://nile.wpi.edu/NS/overview.html, 14 May 2006.

14. F. J. Ros and P. M. Ruiz, "Implementing a New Manet Unicast Routing Protocol in NS2", December, 2004, http://masimum.dif.um.es/nsrt-howto/pdf/nsrthowto.pdf, 25 July 2005.

15. Webopedia, An Internet Dictionary, 14 May 2006 http://www.webopedia.com/TERM/T/Tcl.html.