BIOINFO Sensor Networks
ISSN: 2249-944X & E-ISSN: 2249-9458 Volume 2, Issue 1, 2012, pp.-30-33.
Available online at http://www.bioinfo.in/contents.php?id=301

EXCLUSION OF BLACK HOLE ATTACK TO PROVIDE PRIVACY SECURITY SERVICE IN AD HOC WIRELESS NETWORKS

BOMPILWAR M.D., KARIYA D.G., HEDA S.R. AND HATWARE I.V.

Department of Computer Science and Engineering, J.D.I.E.T, Yavatmal, MS, India.
*Corresponding Author: Email- mahesh_bompilwar@yahoo.com

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- Ad hoc wireless networks are infrastructure less networks and contain mobile nodes. To give protected communication between mobile nodes security is the necessary requirement in ad hoc wireless networks. Safe communications among the mobile nodes are accomplished by substantial challenges. These challenges are overcome by building the multiple safety solutions that defend and improve the network performance. Ad hoc wireless networks are exaggerated by different attacks. Black hole attack is one of the rigorous attacks that come from misbehavior of the node. The mischievous node acts as selfish or malicious. Malicious node is called the black hole. The black hole intercepts the packet and privacy of the message is revealed. In this paper Black hole attack is detected using AODV (Ad hoc on demand distance vector routing) protocol. The simulation was carried on NS-2
Keywords- Ad hoc wireless networks, AODV, privacy, Black hole attack.

Citation: Bompilwar M.D., et al. (2012) Exclusion of Black Hole Attack to Provide Privacy Security Service in Ad Hoc Wireless Networks. BIOINFO Sensor Networks, ISSN: 2249-944X & E-ISSN: 2249-9458 Volume 2, Issue 1, pp.-30-33.

Introduction

The security of communication in ad hoc wireless networks is very essential, especially in military use. The lack of central management and shared wireless medium makes them exposed to attacks than wired networks [1].The attacks may be passive or active attacks. The passive attacks caused by malicious nodes without troubling the network operation. The active attacks disturb the operation. The attacks take place when routing the control information and data. In ad hoc wireless networks each node acts as host and router [2].

Different types of routing protocols are used in ad hoc wireless networks to update the routing information. Proactive (or table driven), reactive (on demand) and hybrid routing protocols are used for ad hoc wireless networks. The routing attacks that affect the ad hoc wireless networks are: Attacks using Modification, Fabrication, Interruption, and Interception. In this paper we focus on Interception of the message caused by black hole attacks [3].

Ad hoc on-demand distance vector (AODV) routing, dynamic source routing (DSR) and Destination sequence vector routing (DSDV) protocols are the important routing protocols for ad hoc wireless networks [4].These protocols are affected by different security attacks. In this paper Black hole attack is detected and removed using AODV protocol.

Ad hoc on-Demand Distance-Vector Routing Protocol.

Ad-hoc On-Demand Distance Vector (AODV) [5] 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. 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. Header information of these control messages are explained in [5]. 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.

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 1. 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. The default constant values of the AODV protocol are listed in appendix of RFC - 3561 [5]. Thus the node knows over which neighbor to reach at the destination. In terminology, the neighbor list for destination is labeled as “Precursor List”. Figure 1 shows how the RREP message is unicasted and how the route entries in the intermediate nodes are updated.

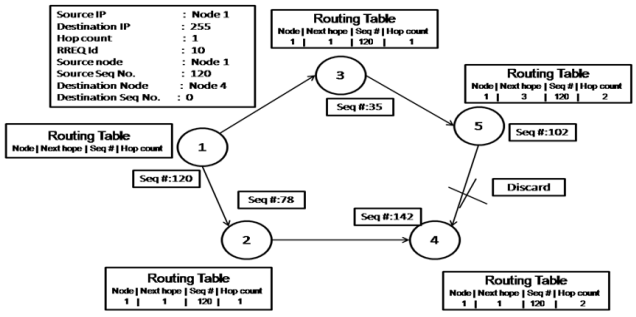

Fig. 1- Propagation of the RREQ message

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. 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.

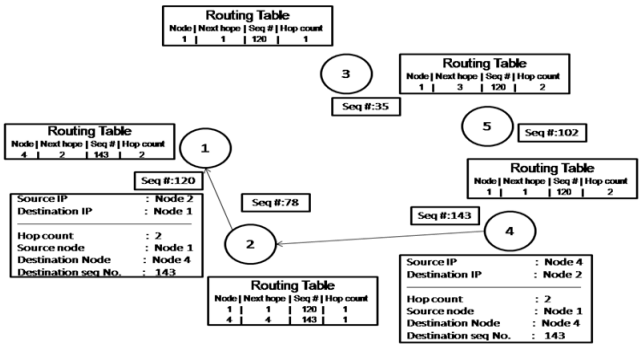

Fig. 2- Updating the Sequence Number with fresh one

Black hole Attack in AODV

In black hole attack malicious node initiate route discovery by impersonating a destination node by sending a spoofed route packet to a source node [6] [7].A black hole having two properties [2]:

i. The node exploits the ad hoc routing protocol, such as AODV to advertise itself as having a valid router to a destination, even though the route is spurious with the intention of intercepting packet.

ii. The node consumes the intercepted packet. The simulation of black hole attack in ad hoc wireless is carried out using AODV protocol; a black hole node absorbs the network traffic and drops all packets. In order to explain black hole attack a malicious node is added that excites the black hole behavior in fig.3.

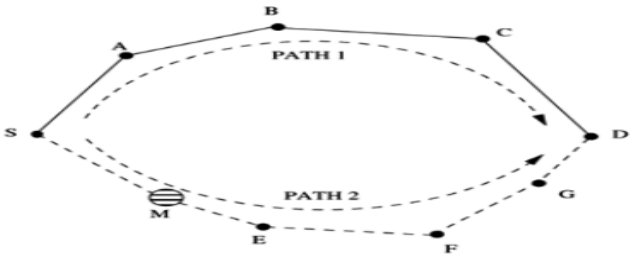

Fig. 3- Illustration of Black hole attack

It advertises that it has the shortest path to the destination node D when it receives the Route Request packets sent by node S. The attacker may not be able to succeed if node A, which also receives the Route Request packet from node S, replies earlier than node M. But a major advantage for the malicious node is that it does not have to search its routing table for a route to the destination. Also, the Route Reply packets originate directly from the malicious node and not from the destination node. Hence, the malicious node would be able to reply faster than node A, which

would have to search its routing table for a route to the destination node M, allowing node M to listen all packets meant for destination node.

After receiving the data packets the black hole may drop the packets selectively or intercept the packets (change destination seqNum, add its own information etc) and to destination. Hence confidentiality of the message is disclosed in the presence of the black hole attack.

Fig. 4- Shows the start of Animator

Simulation result and discussion

To evaluate the packet delivery fraction, End-to-End Delay and Normalized Routing Overhead; simulation is done with nodes with the source node transmitting maximum packets to the destination node. Fig. 5 shows the graphs when network size (number of nodes) is varying. It can be seen from the Fig. 5 (a), that PDF of AODV drops by near about 80% in presence of Black-hole attack. The same increases by near about 80 % when our solution is used in presence of Black-hole attack. At the same time, Fig. 6 (b) shows that the rise in End-to-End delay Fig. 6 shows the graphs when mobility of nodes is varying. It can be seen from the Fig. 7 (a), that routing overhead of S-AODV rises by some percent when solution is implemented in presence of attack. The same decreased by some percentage for AODV in presence of the attack as shown in fig. 7(b).

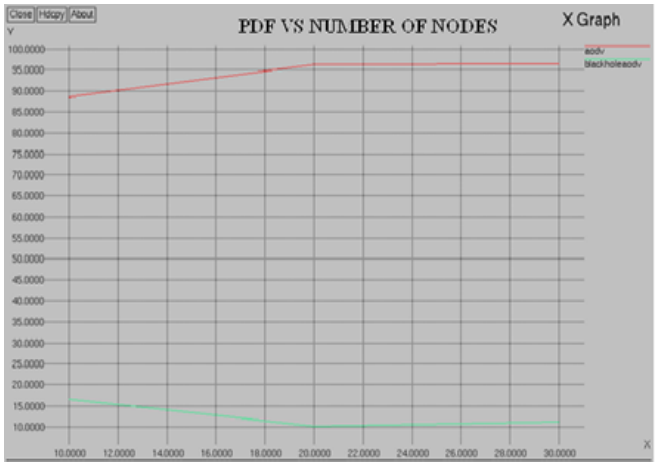

Fig. 5(a)- Packet Delivery Fraction of black-hole AODV and AODV

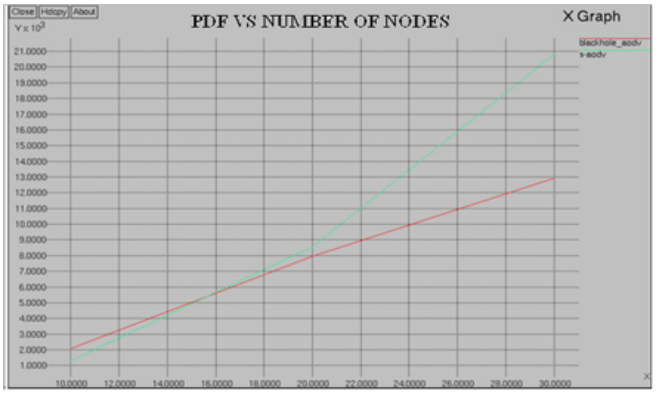

Fig. 5(b)- Packet Delivery Fraction of black-hole AODV and s-AODV

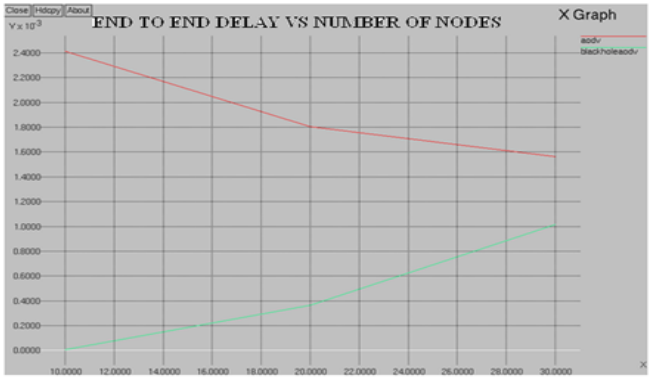

Fig. 6(a)- end to end delay of black-hole AODV and AODV

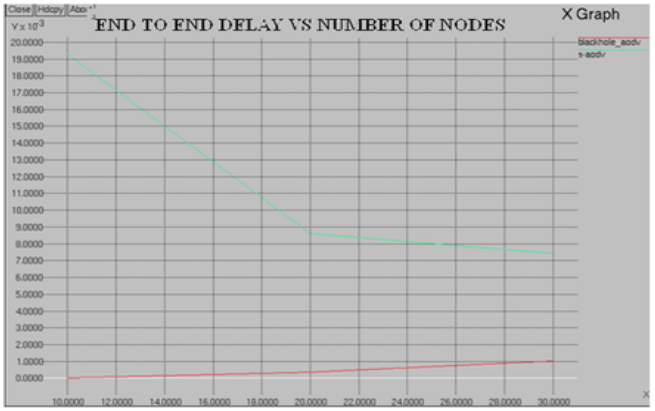

Fig. 6(b)- end to end delay of black-hole aodv and s-aodv

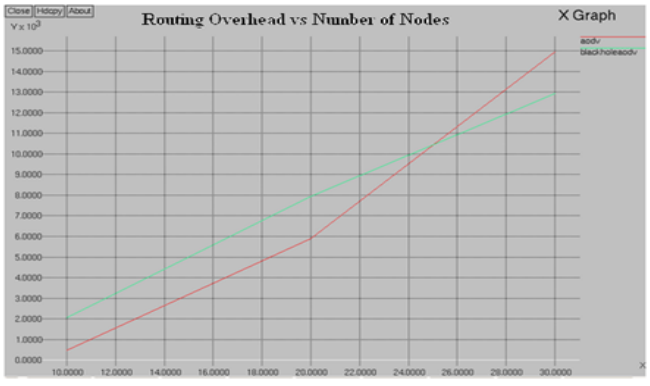

Fig. 7(a)- Routing Overhead of black-hole aodv and s-aodv

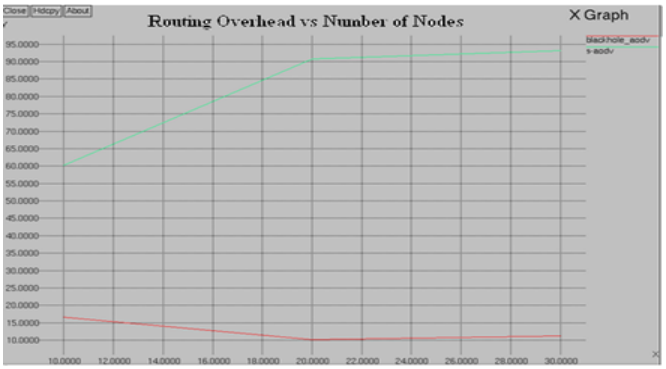

Fig. 7(b)- Routing Overhead of black-hole aodv and s-aodv

Conclusion

In this study we analyzed the effects of backhoes in ad hoc wireless networks. We implemented an AODV protocol that simulates the behavior of a black hole in NS-2.In this method we have used very simple and effective way of providing security in AODV against black hole attack that causes the interception and confidentiality of the ad hoc wireless networks. The solution detects the malicious nodes and isolates it from the active data forwarding. As from the graphs illustrated in results we can easily infer that the performance of the normal AODV drops under the presence of black hole attack. Our solution with sequence number detection increases the PDR with minimum increase in Average-End-to-End Delay and with little more routing overhead.

Though the algorithm is implemented and simulated with AODV routing algorithm, we believe that the solution can also be used by other routing algorithm as well.

References

[1] Vani A., D. Sreenivasa Rao. *International Journal Of Engineering Science And Technology (Ijest).*

[2] Siva Ram Murthy C. and Manoj B.S. *A text book on Ad Hoc Wireless Networks*.

[3] Tamilselvan L., Sankarayanan V. (2007) *International Conference on Wireless Broadband and Ultra Wideband Communications.*

[4] Pervaiz M.O., Mihaela Cardien Jie wu (2005) *Routing Security in Ad Hoc wireless Networks*.

[5] Perkins C. (2003) *Experimental, Network, Working Group*.

[6] Royer E.M. and Chai-Keong Toh (1999) *IEEE Personal Communications*, 46-55.

[7] Perkins C.E. and Royer E.M. (1999) *IEEE Workshop on Mobile Computing Systems and Applications*, 90-100.

[8] Dokurer S. "*Simulation of Black Hole Attack in Wireless Ad-Hoc Networks." A Thesis Submitted To the Graduate School Of Natural And Applied Sciences Of Atilim University.*