Defending MANET against Blackhole Attackusing Modified AODV

Devang S. Patel
P.G. Student
Electronics & Communication Engineering
Dr. S. & S.S. Ghandhy Engineering College, Surat

Nita D. Maheta
Associate Professor
Electronics & Communication Engineering
Dr. S. & S.S. Ghandhy Engineering College, Surat

Abstract

A Mobile Ad-Hoc Network (MANET) is an autonomous network that consists of mobile nodes that communicate with each other over wireless links. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality. MANET is particularly vulnerable to security threats due to its fundamental characteristics such as open medium, dynamic topology, distributed cooperation and constrained capability. Due to the inherent characteristics, MANET is unprotected to various types of security attacks. Black hole is one of these attacks in which a malicious node announces the fresh and shortest path to a destination node and then drops/discards all data packets that subsequently go through it. Many researchers have proposed different techniques for preventing and detecting this attack. In this paper, we have presented a technique which can mitigate blackhole attack in Adhoc networks with minimal increase in end-to-end delay and routing overhead.

Keywords: AODV, Blackhole attack, MANET, Network security, Secure routing protocols

I. INTRODUCTION

A mobile ad hoc network (MANET) [1] is a self-configuring infrastructure-less network of mobile devices connected by wireless. MANETs have remained a challenging research area for the last few years because of its dynamic topology, limited range of each mobile host's wireless transmissions, power constraints and security issues etc. MANETs are suffering from a wide range of security threats and attacks, not only the same attacks their infrastructure counterparts are facing, but also new ones particularly targeting MANETs. Among various possible threats and attacks, MANETs are particularly susceptible to the DoS (Denial of Service) attacks. Blackhole attack is a denial of service attack [3] which disrupts the normal routing mechanism in MANET. Black hole problem in MANET is a serious security problem to be solved. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In flooding based protocol, if the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. This malicious node then can choose whether to drop the packets to perform a denial-of-service attack or to use its place on the route to exploit a man-in-the-middle attack. This paper presents the solution to black hole attack and improves the performance of the network. The paper is organized like section 2 describes blackhole attack in ad hoc networks, section 3 discusses our proposed approach, section 4 includes simulation and finally section 5 concludes the paper.

II. BLACKHOLE ATTACK

Black hole attack [1] [2] [4] is a kind of Denial of Service (DoS) attacks in MANET. In this attack, a malicious node waits the Route Request message (RREQ) from the neighbor nodes. When it receives the RREQ message, it sends immediately a false RREP with high sequence number to the source node. The source node assumes that the route is fresh route. However, when the source node sends the data packet to the destination node by using this route, the malicious node does not relay the packet and absorbs all data packets. Black hole attack can be classified into two categories:

A. Single Black Hole Attack:

Single black hole attack means the malicious node individually acts as a black hole node. It is called black hole attack with single malicious node.

B. Cooperative Black Hole Attack:

Cooperative black hole attack means the malicious nodes act in a group. It is called black hole attack with multiple malicious nodes.

As an example, consider the following scenario in Fig 1. In this scenario, the node 'S' is the source node and 'D' is the destination node. 'M' is assumed malicious node. When the source node 'S' want to send the data packet to the destination node

'D', it first broadcasts the RREQ message with destination sequence number 10 to the neighboring nodes. So, the neighboring node 'C', 'E' and 'F' receive this message.

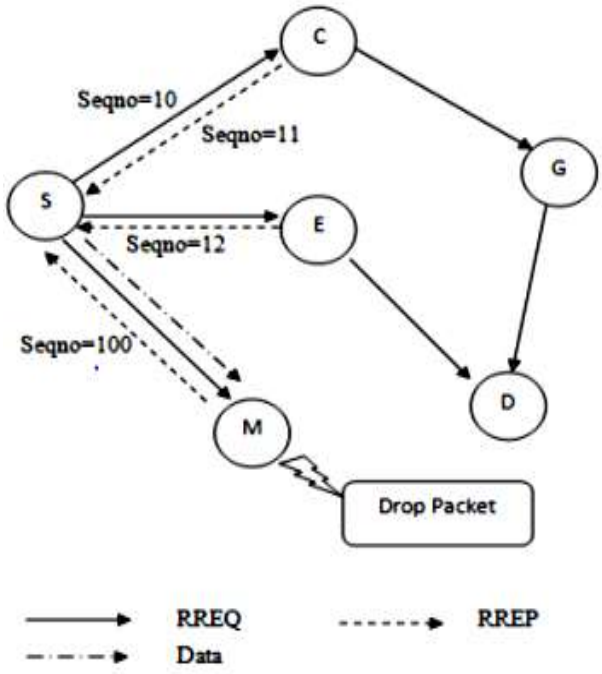

Fig. 1. Single blackhole attack

So if the node M is a malicious node, it immediately sends back a RREP message to node 'S' with highest sequence number that it has an active route to the destination. The node 'S' assumes that this is the freshest route. So, the node 'S' ignores all other replies and sends the data packets to the destination through it. However, node "M" absorbs all data and behaves like a *blackhole*.

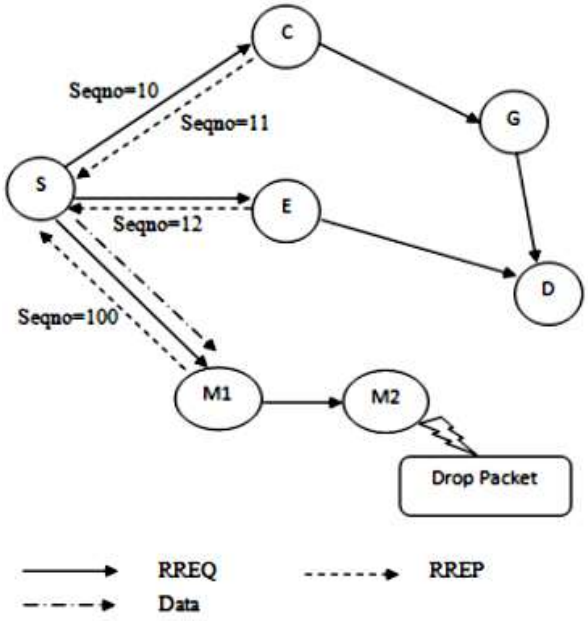

Fig. 2. Cooperative blackhole attack

Cooperative black hole attack is shown in Fig 2; on the receipt of data packets, M1 simply drops them or M1 forwards all the data to M2. M2 simply drops them instead of forwarding to the destination. Thus the data packets get lost and hence never reach the intended destination.

III. PROPOSED APPROACH

To protect network-layer reactive protocols from Blackhole attacks, it is necessary to discover malicious nodes during route discovery process when they pass fabricated routing information to attract the source node to send data through itself. Our

proposed approach does exactly the same. In AODV protocol, when a node receives a route reply packet (RREP), it checks the sequence number value in routing table; if it is greater than the one in the RREP, the RREP packet is accepted; otherwise it is discarded [10]. Fig. 1 (above) shows the route discovery process in AODV in the presence of a malicious node M. Source node S broadcasts route request packet (RREQ); nodes within its communication range, A and C, receive the RREQ and re-broadcasts RREQ to their neighbors until a node having a valid route to the destination or destination D itself receives RREQ [16]. This node sends RREP to the source node on the reverse path of RREQ. The malicious node M sends RREP with higher, but fabricated, sequence number to the source; another RREP is sent by D having genuinely higher sequence number. As malicious node sends RREP with higher sequence number than the normal node, S chooses path through M to transfer data packets and therefore, malicious node can drop some or all received packets which causes disruption in network operations.

In our proposed approach, an intermediate node dynamically calculates a PEAK value after every time interval [8] that uses three parameters for calculation: RREP sequence number, routing table sequence number and number of replies received during the time interval. The PEAK value is the maximum possible value of sequence number that any RREP can have in the current state.

The proposed algorithm detects and removes malicious nodes during the route discovery phase. Nodes receiving RREP verify the correctness of routing information; source node broadcasts a list of malicious nodes when sending RREQ. Nodes update route tables when they get any information of malicious nodes from received routing packets. As there is no extra control packets added in the proposed algorithm, there would be negligible difference in Routing Overhead which is the ratio of the number of routing related transmissions to the number of data related transmissions. Moreover, as the malicious nodes would be isolated, Packet Delivery Ratio (PDR) would be improved greatly; PDR is the ratio of number of received data packets to the number of sent data packets. If the node receiving RREP from a malicious node doesn't have the node marked as malicious in the routing table, the proposed algorithm adds a little computational overhead to that node as it has to calculate the PEAK value.

IV. SIMULATION AND RESULTS

The simulation is performed on Linux Ubuntu 10.04 installed on VMware Workstation 10.0.1. The experiments are implemented and run in the network simulator ns-2 (version 2.35). The performance metrics chosen for the evaluation of black hole attack are packet end to end delay, network throughput and network load.

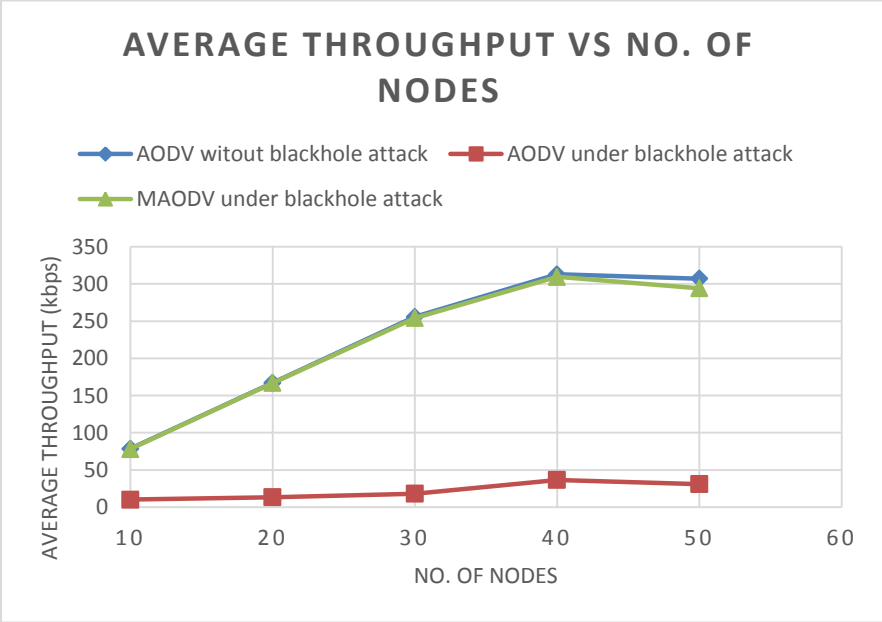

Fig. 3. Average throughput vs no. of nodes

Simulation results for average throughput with and without blackhole attack is plotted against no. of nodes. There is a drastic reduction in the average throughput when the network is under blackhole attack. This is because the blackhole node attracts the data packets and drops them. While Modified AODV (MAODV) is operating blackhole node is avoided. Hence throughput increases.

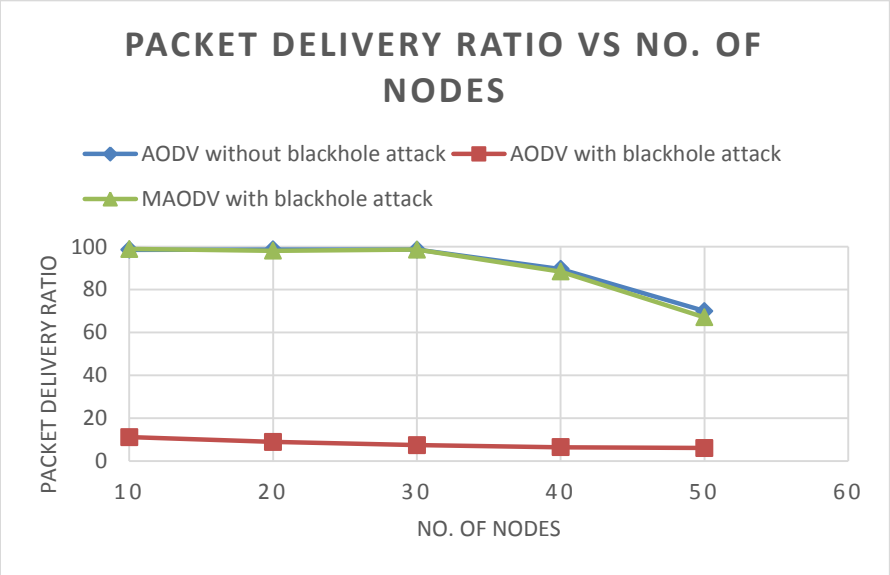

Fig. 4. Packet delivery ratio vs no. of nodes

Simulation results for packet delivery ratio with and without blackhole attack is plotted against no. of nodes. The reduction in the PDR is attributed to the blackhole node. Our modified AODV (MAODV) protocol helps improving packet delivery ratio significantly. Blackhole node is avoided in the initial stage & hence packet delivery ratio is improved.

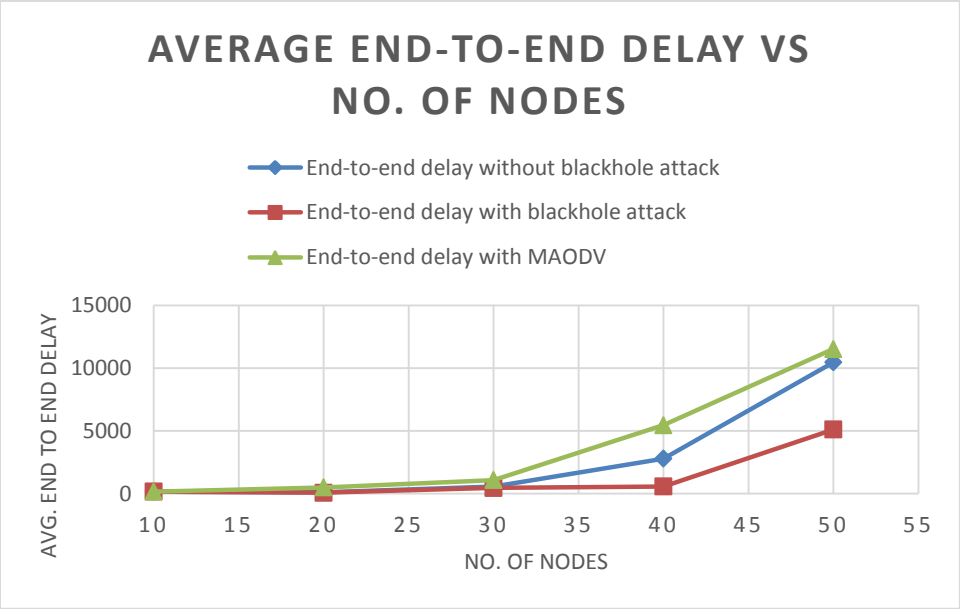

Fig. 5. Average end-to-end delay vs no. of nodes

Simulation results show that average end-to-end delay for AODV under blackhole attack is less that is because blackhole node responds with RREP message immediately without wasting time as in case with normal nodes. Our new MAODV protocol exhibits increased end-to-end delay as compared to original AODV.

V. Conclusion

Having simulated the Black Hole Attack, we saw that the packet loss is increased in the ad hoc network. Results show the difference between the average throughput in the network with and without a Black Hole Attack. From results it is also evident that average end-to-end delay is less when blackhole node is acting. 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. Our mitigation technique modified AODV (MAODV) increases packet delivery significantly. At the same time it also increases average end to end delay.

References

[1] H. Deng, W. Li, and D. P. Agrawal, "Routing Security in Ad Hoc Networks," IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol. 40, No. 10, October 2002, pp. 70-75.

[2] Md. Al-Shurman and S. Yoo, S. Park, "Black hole Attack in Mobile Ad Hoc Networks", Proceedings of the 42nd Annual Southeast regional conference ACM-SE 42, pp. 96-97, April 2004
[3] H. Yadav, R. Kuma, "Identification and Removal of Black Hole Attack for Secure Communication in MANETS", International Journal of Computer Science and Telecommunications, vol. 3, issue 9, September 2012.
[4] Md. Obaida, S. A. Faisal, Md. Horaira, T. Roy, "AODV Robust (AODVR): An Analytic Approach to Shield Ad-hoc Networks from Black Holes", International Journal of Advanced Computer Sciences and Applications, vol. 2, issue 8, pp. 97-102, 2011
[5] S. Gupta, S. Kar, S Dharmaraja, "BAAP: Blackhole Attack Avoidance Protocol for Wireless Network", Second International Conference on Computer & Communication Technology (ICCCT), pp. 468-473, 15-17 Sept 2011
[6] C. Sreedhar, S. M. Verma, N. Kasiviswanath, "A Novel Approach for Secure Routing in MANETs", IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498, vol.2, no. 5, October 2012.
[7] Sen, J.; Koilakonda S.; Ukil, A.; "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", Intelligent Systems, Modeling and Simulation (ISMS), 2011 Second International Conference, pp.338-343, 25-27 Jan. 2011.
[8] L. Himral, V. Vig, and N. Chand., "Preventing aodv routing protocol from black hole attack", International Journal of Engineering Science and Technology (IJEST), vol 3, No. 5, May 2011.
[9] L. Tamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, vol. 3, no. 5, pp. 13-20, May 2008
[10] P. N. Raj and Prashant B. Swadas, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", International Journal of Computer Science Issues, vol. 2, issue 3, 2009, pp. 54-59.
[11] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", proceedings of the International Multi Conference of Engineers and Computer Scientists, vol II, IMECS, 2010