Indian J.Sci.Res. 17(2): 442-447, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

PREVENTION AND DETECTION OF BLACK HOLE ATTACK IN MANET

[1]P.Sree Rathna Malathi,[2]V. Harsha Shastri,[3]K.Anitha
[1,2,3] Department of Computer Science and Engineering, Loyola Academy Degree and P.G College, Secunderabad, TS.

Abstract: Mobile Adhoc network is an infrastructure-less network used for wireless communication. MANET can be built with the mobile nodes which can move anywhere at any time. This results into the dynamic topology of MANET. Each node is responsible for routing the message from one node to the other like a router, causes network more vulnerable to the different attacks.Security is a key feature in mobile ad-hoc network (MANET) but they are prone to various types of attacks such as network layer attacks. Black hole is one the network layer attacks. It is a prominent security threat in MANET. In Black hole attack, malicious node falsely claims that having shortest path to destination and eventually captures all data packets from source which are intended to forward further to destination. This results into the performance degradation of network and also causes battery problem. In this paper, some of the detection techniques are discussed which are put forward by various researchers. Since, in AODV, route to destination is looked for adaptively, this loophole is used to carry out malicious hacking practices. A lot of work has been done to overcome the above stated problem. In this paper, the already present solutions have been analyzed, comparisons has been done on the basis of various parameters.

keywords-MANET, Black hole attack, AODV, SAODV, Malicious Node, Routing Protocol

I.Introduction

MANETs is an autonomous system in which different mobile nodes are connected to each other by wireless links. Nodes in the network can be either fixed or mobile. In MANET, communication occurs between nodes directly or through intermediate nodes which act as routers. AODV (Ad-hoc on Demand Distance Vector) routing protocol is used as it minimizes the routing overhead. AODV provides loop free routes and repair broken links. AODV is an on demand routing protocol, this means that routes are only established when needed to reduce traffic overhead. The black hole attack is one of the most severe security attacks which can significantly disrupt the communications across the network. In this attack, without checking routing table, the malicious node sends the dummy reply to the destination node. Then, malicious node absorbs all data packets that are intended to forward to the destination. Due to loss of data packets, the hole is created in the network. Hence, the network faces data loss and its performance reduces [6]. This paper presents how black hole attack occurs in AODV routing protocol and various methods to detect and prevent Black hole attack in AODV.

II.Security Attacks in MANET

A MANET can be subjected to active attacks and passive attacks [11].

A. Passive Attacks

Passive attacks are the attacks in which attacker does not directly participate in bringing the network down. In this attacker simply looks on the network and observers the traffic of the network that which node is trying to routes to which node. And which node is vulnerable and a good candidate for the Denial of service (Dos) attack. The attacker can then give this information to a partner which can use this information to bring the network down.

B. Active Attacks

In Active attacks and attacker actively participates in inhibiting the normal operation of the network. The attacker can drop some packets, can modify the packets or can even fabricate the message. And in this the attacker can even tunnel them over a high speed private network to a partner in other part of the network. Black hole attack is active in nature.

III.AODV Protocol in MANET

Ad Hoc On-Demand Vector Routing [2] (AODV) protocol is a reactive routing protocol for ad hoc and mobile networks that maintain routes only between nodes which need to communicate. The AODV routing protocol builds on the DSDV algorithm. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on an on-demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The authors of AODV classify it as a pure on-demand route acquisition system, as nodes that are not on a selected path do not maintain routing information. That means, the routing messages do not contain information about the whole route path, but only about the source and the destination. Therefore, routing

[1]Corresponding Author

messages do not have an increasing size. It uses destination sequence numbers to specify how fresh a route is (in relation to another) which is used to grant loop freedom.

Whenever a node needs to send a packet to a destination for which it has no "fresh enough" route (i.e., a valid route entry for the destination whose associated sequence number is at least as great as the ones contained in any RREQ that the node has received for that destination) it broadcasts a route request (RREQ) message to its neighbors. Each node that receives the broadcast sets up a reverse route towards the originator of the RREQ (unless it has a "fresher" one).When the intended destination (or an intermediate node that has a "fresh enough" route to the destination) receives the RREQ, it replies by sending a Route Reply (RREP). It is important to note that the only mutable information in a RREQ and in a RREP is the hop count (which is being monotonically increased at each hop). The RREP travels back to the originator of the RREQ (this time as a unicast). At each intermediate node, a route to the destination is set (again, unless the node has a "fresher" route than the one specified in the RREP). In the case that the RREQ is replied to by an intermediate node (and if the RREQ had set this option), the intermediate node also sends a RREP to the destination. In this way, it can be granted that the route path is being set up bi-directionally. In the case that a node receives a new route (by a RREQ or by a RREP) and the node already has a route as fresh as the received one, the shortest one will be up dated. The source node starts routing the data packet to the destination node through the neighboring node that first responded with an RREP. The AODV protocol is vulnerable to the well-known black hole attack. This is illustrated in figure 1.

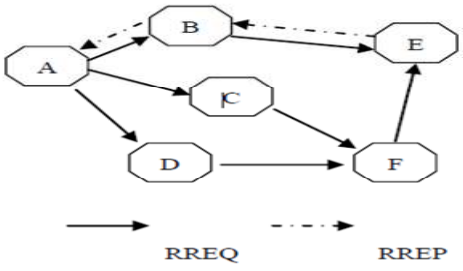

Figure 1: RREQ & RREP message exchange between A & E

IV.Black Hole Problem in AODV

Routing protocols [1] are exposed to a variety of attacks. Black hole attack is one such attack and a kind of Denial Of Service (DoS) in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the *Route Discovery process*, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received message instead of relaying them as the protocol requires.

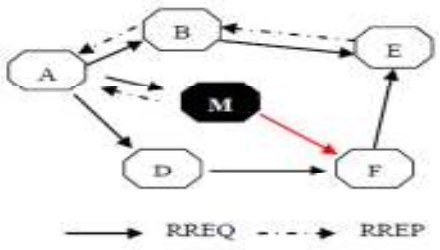

Figure 2: Black hole Attack in AODV

In the above figure 2, imagine a malicious node M. When node A broadcasts a RREQ packet, nodes B, D and M receive it. Node M, being a malicious node, does not check up with its routing table for the requested route to node E. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node A receives the RREP from M ahead of the RREP from B and D. Node A assumes that the route through M is the shortest route and sends any packet to the destination through it. When the node A sends data to M, it absorbs all the data and thus behaves like a Black hole.

In AODV, the sequence number is used to determine the freshness of routing information contained in the message from the originating node. When generating RREP message, a destination node compares its current sequence number, and the sequence number in the RREQ packet plus one, and then selects the larger one as RREPs sequence number. Upon receiving a number of RREP, the source node selects the one with greatest sequence number in order to construct a route. But, in the presence of black hole when a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from the other nodes. The source then starts to send out its packets to the black hole trusting that these packets will reach the destination. Thus the black hole will attract all the packets from the source and instead of forwarding those packets to the destination

it will simply discard those. Thus the packets attracted by the black hole node will not reach the destination.

V.Proposed Solution

We propose an additional route to the intermediate node that replies the RREQ message to check whether the route from the intermediate node to the destination node exists or not. When the source node receives the Further Reply (FRp) from the next hop, it extracts the check result from the reply packets. If the result is yes, we establish a route to the destination and begin to send out data packets. If the next hop has no route to the inquired intermediate node, but has a route to the destination node, we discard the reply packets from the inquired intermediate node, and use the new route through the next hop to the destination. At the same time, send out the alarm message to whole network to isolate the malicious node. If the next hop has no route to the requested intermediate node, and it also has no route to the destination node, the source node initiates another routing discovery process, and also sends out an alarm message to isolate the malicious node. Thus we avoid the black hole problem, and also prevent the network from further malicious behavior. But here we assume the black hole nodes do not work as a group and propose a solution to identify a single black hole. However, the proposed method cannot be applied to identifying a cooperative black hole attack involving multiple nodes. We may also develop a methodology to identify multiple black hole nodes cooperating as a group. The technique works with slightly modified AODV protocol and makes use of the Data Routing Information (DRI) table in addition to the cached and current routing tables. A black hole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets.

VI.Detection and Prevention techniques of Black Hole attack in AODV

A. DPRAODV (Detection, Prevention and Reactive AODV) scheme

We have proposed the method DPRAODV (A dynamic learning system against black hole attack in AODV based MANET) to prevent security of black hole by informing other nodes in the network. In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. If its sequence number is higher than the one in routing table, this RREP packet is accepted. In this solution, it has an addition check whether the RREP sequence number is higher than the threshold value. If it is higher than the threshold value, then the node is considered to be malicious node and it adds to the black list. As the node detected as anomaly, it sends ALARM packet to its neighbors. The routing table for that malicious node is not updated, nor is the packet forwarded to another node. The threshold value is dynamically updated using the data collected in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The main advantage of this protocol is that the source node announces the black hole to its neighbors in order to be ignored and eliminated.

B. ABM (Anti-Black hole Mechanism) scheme

We attempt to detect and separate malicious nodes, which selectively perform black hole attacks by deploying IDSs in MANETs (mobile ad hoc networks). All IDS nodes perform an ABM (Anti-Black hole Mechanism), which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. With the prerequisite that intermediate nodes are forbidden to reply to RREQs, if an intermediate node, which is not the destination and never broadcasts a RREQ for a specific route, forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS's SN (suspicious node) table. When the suspicious value of a node exceeds a threshold, a Block message is broadcasted by the detected IDS to all nodes on the network in order to cooperatively isolate the suspicious node.

C. Honeypot based detection scheme

We propose a novel strategy by employing mobile honeypot [9] agents that utilize their topological knowledge and detect such spurious route advertisements. They are deployed as roaming software agents that tour the network and lure attackers by sending route request advertisements.

We collect valuable information on attacker's strategy from the intrusion logs gathered at a given honeypot. Drawbacks: proposed algorithm is for WMN not for MANET. As it is proactive mechanism, it will generate lots of traffic. Honey pot has lack of centralized authority control.

D. Cryptographic based technique

This research focuses that many investigations have been done in order to improve the security in MANETs, most of which are relied on cryptographic based techniques in order to guarantee some properties such as data integrity and availability.

These techniques cannot prevent a malicious node from dropping packets supposed to be relayed, There are basically three defense lines devised here to protect MANETs against the packet dropping attack. The first defense line (for prevention purposes) aims to forbid the malicious nodes from participating in packet forwarding

function. Whenever the malicious node exceeds this barrier, a second defense line (for incentive purposes) is launched, which seeks to stimulate the cooperation among the router nodes via an economic model. Finally, once the two previous defense lines have been broken, a third on (for detection/reaction purposes) is launched aiming to reveal the identity of the malicious node and excludes it from the network.

E. Neighborhood-based and Routing Recovery Scheme

This detection scheme is based on a neighborhood-based method to recognize the black hole attack, and a routing recovery protocol to build the correct path. This method is employed to identify the nodes which are unconfirmed .In this method, source node sends a Modify Route Entry control packet to destination node to renew routing path in the recovery protocol. In this scheme, not only a lower detection time and higher throughput are acquired, but the accurate detection probability is also achieved. The main limitation of this scheme is that it becomes useless when the attacker agrees to forge the fake reply packets.

F. Redundant Route Method and Unique Sequence Number Scheme

In this scheme there are two techniques to prevent the black hole attack. The first technique is to find a true path to the destination. A method based on neighbor set information is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure, two steps are: 1- Collect neighbor set information. 2-Determine whether there exists a black hole attack. In Response procedure, Source node sends a modify Route Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination. This scheme effectively detects black hole attack without introducing much routing control overhead to the network find at least two routes from the source to the destination node. The working of this scheme is as follow: Firstly the source node sends a ping packet (a RREQ packet) to the destination. The receiver node with the route to the destination will reply to this RREQ packet and then the acknowledge examination is started at source node. Then the sender node will buffer the RREP packet sent by different nodes until there are it represents that there are at least two routing paths existing at the same time. After that, the source node identifies the safe route by counting the number of hops or nodes and thus prevents black hole attacks. In the second technique, unique sequence number is used. The sequence value is aggregated; hence it's ever higher than the current sequence number. In this technique, two values are recorded in two additional tables. These two values are last-packet-sequence-numbers which is used identify the last packet sent to every node and the second one is for the last packet received. Whenever a packet are transmitted or received, these two table values are updated automatically. Using these two table values, the sender can analyze whether there is malicious nodes in network or not. Simulation result shows that these techniques have less numbers of RREQ and RREP when compared to existing AODV. Second technique is considered to be good as compared to first technique because of the sequence number which is included to every packet contained in the original routing protocol.

VII.Related Works in Detecting Black Hole Attack

There have been quite a number of works done in securing the routing protocol in MANET from the black hole attack.

M.A. Shurman [16] in his work has proposed for the source node to verify the authenticity of the node that initiates the RREP messages by finding more than one route to the destination, so that it can recognize the safe route to the destination. This method can cause routing delay, since a node has to wait for a RREP packet to arrive from more than two nodes.

S. Yi [17] proposed a solution which looked at the Security-Aware Ad hoc Routing (SAR) using the security attributes such as trust values and relationships.

N.H. Mistry [18] has proposed for the source node to verify the RREP destination sequence number by analyzing the RREP messages which arrived within the predefined waiting period by using the heuristic method. If the sequence number is found to be exceptionally high, the sender of the respective RREP will be marked as malicious node. The major issue in this method is the latency time during the route discovery process since the source node has to wait until the waiting time period expired before the routing table can be updated. In the event where there is no attack in the network, the node still suffers with the latency time.

Satoshi Kurosawa [5], Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto's, proposed an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals.

S. Ramaswamy [4], H. Fu, M. Sreekantaradhya, J. Dixon, K. Nygard proposed a solution that contain a data routing information table where 1 stands for 'true' and 0 for 'false'. Whenever a RREP is received a cross check is done to verify whether the reply is from a legitimate node or not.

According to V Sankaranarayanan and LathaTamilselvan, they projected a technique that source will verify the reply packet coming from various nearest nodes to wait and check the replies from all the neighboring nodes to discover best possible and secure route.

VIII.Conclusion

We have gone through various routing security attacks of MANETs, described the black hole attack that can be mounted against a MANET and proposed a feasible solution for it in the AODV protocol. The proposed solution can be applied to identify black hole nodes cooperating with each other in a MANET

Black hole attack is a main security threat. Its detection is the main matter of concern. Many researchers have conducted many techniques to propose different types of prevention mechanisms for black hole problem. There are different security mechanisms are introduced to prevent black hole attack. Various techniques used for the detection and prevention of Black hole attacks such as DPRAODV,DRI Table and cross checking scheme and DCM are listed.

We intend to perform the solution for the black hole attack and apply this for with different routing protocols like DSR, TORA.

IX.Acknowledgment

The authors would like to thank the management of the college for their continual support in publishing papers. We would like to thank our colleagues who continually supported us.

References

[1] M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," *Proc. 2002 ACM Wksp. Wireless Sec.*, Sept. 2002, pp. 1-10.

[2] Elizabeth M. Royer et. al. "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communication, April 1999.

[3] Mohammad Al-Shurman and Seong-Moo YooSeungjin Park, "Black hole Attack in Mobile Ad Hoc Networks" Proceedings of the 42nd annual Southeast regional conference ACM-SE 42, APRIL 2004, pp. 96-97.

[4] Sanjay Ramaswamy, Huirong Fu, ManoharSreekantaradhya, John Dixon and Kendall Nygard.**"**Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".Department of Computer Science, IACC 258 North Dakota State Universities, Fargo, ND 58105.

[5] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. "Detecting Black hole Attack on AODV based Mobile Ad-hoc networks by Dynamic Learning Method". International Journal of Network Security, Vol.5, No.3, PP.338- 346, Nov. 2007.

[6] Nisha P John, Ashly Thomas," Prevention and Detection of Black hole Attack in AODV based Mobile Ad-hoc Networks- A Review " International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012

[7] Gagandeep, Aashima, Pawan Kumar," Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 - 8958, Volume-1, Issue-5, June 2012

[8] Rajesh J. Nagar, Kajal S. Patel " Securing AODV Protocol against Blackhole Attacks" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1, Jan-Feb 2012, pp.1116-1120.

[9] AnooshaPrathapani, Lakshmi Santhanam, Dharma P. Agrawal," Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents" Springer Science+Business Media, LLC 2011.

[10] Jaspal Kumar, M. Kulkarni, Daya Gupta," Effect of Black Hole Attack on MANET Routing Protocols", I. J. Computer Network and Information Security, Volume 5, pp-64-72, April 2013.

[11] Lidong Zhou, Zygmunt J. Haas "Securing Ad Hoc Networks," Cornell University Ithaca, NY 14853.

[12] Bing Wu, Jianmin Chen, Jie Wu, MihaelaCardei, A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ,‖ Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D. Z. Du (Eds.) pp, @ 2006 Springer.

[13] Baadache, and Belmehdi, Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks, J. Comp. Sci. and Info. Security, 2010, Vol. 7, No. 1, pp. 10-16.

[14] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard, Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks.

[15] Adrian Perrig, John Stankovic, and David Wagner, (2004) "Security in wireless sensor networks", Commun. ACM, 47(6):53-57.

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

[17] P. Yi et al., "A New Routing Attack in Mobile Ad Hoc Networks," Int'l. J. Info. Tech., vol. 11, no. 2, 2005.

[18] Mistry, N.H., Jinwala, D.C., Zaveri, M.A.(December 2009): MOSAODV: Solution to Secure AODV against Blackhole Attack, International Journal of Computer and Network Security.