SURVEY OF BLACKHOLE ATTACKS ON AODV PROTOCOL IN MANET

Khushbu Patel
P. G. Student
Department of Computer Science Engineering
S.P.B. Patel Engineering College
Gujrat, India.

Abstract:* A mobile ad-hoc network (MANET) is an autonomous wireless network which consists of mobile nodes that communicate with each other over multi-hop wireless links. Due to the absence of any fixed infrastructure, MANETs are unprotected to various types of security attacks. Black hole is one of these attacks. Black hole is a type of routing attack where a malicious node advertise itself as having the shortest path to all nodes in the environment by sending fake route reply. By doing this, the malicious node can deprive the traffic from the source node. There are lots of detection and defense mechanisms to eliminate the intruder that carry out the black hole attack. Here, a mechanism is proposed for the nodes which are deployed in MANETs in order to detect and prevent black hole attacks In this paper, we have surveyed and compared the existing solutions to black hole attacks on AODV protocol.

***Keywords:* Routing Protocols, AODV, Black Hole Attack, MANET.**

I. INTRODUCTION

A Mobile ad hoc network is a collection of wireless nodes that can be dynamically set up ANYWHERE and ANYTIME, without using any pre-existing network infrastructure. There are no basic network devices, such as routers or access points to transfer data among nodes. Instead, each node acts as a router to establish a route and transfer data by means of multiple hops. Due to the mobility nature of nodes, the network topology changes rapidly and erratically over time. MANETs have many potential applications, like Sensor Networks, Medical Service, Personal Area Network, especially in military and rescue operations such as connecting soldiers in the battlefield or creating a temporary network in place of one, which collapsed after a disaster like tsunami [2]. Routing in ad-networks has been a challenging task ever since the wire- less networks came into existence. The major reason for this is the constant change in network topology because of high degree of node mobility [1].

The available routing protocols are mainly categorized into proactive routing protocols, reactive routing protocols and hybrid routing protocol. In proactive routing protocols, the routing information of nodes is exchanged, sporadically, such as DSDV. In reactive routing protocols, nodes exchange routing information when it is needed such as AODV and DSR. Some ad-hoc routing protocols are a combination of the above two categories which we called as hybrid routing protocols. The primary goal of such an ad hoc network routing protocols are correct and efficient route establishment between a pair of nodes so that messages can be delivered in a timely manner [3].

The remainder of the paper is structured as follows. In next section, we discuss Section 2 provides an overview of AODV protocol section 3 describes how the black hole attack is performed on AODV, Section 4 deals with several solutions to black hole attack, section 5 presents conclude the paper with plan for future work.

II. AODV ROUTING PROTOCOL

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is an adaptation of the DSDV protocol for dynamic link conditions. Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. RREQ (Route Request) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route Error) packet to all other nodes that uses this link for their communication to other nodes[4]. This is illustrated in figure 1.

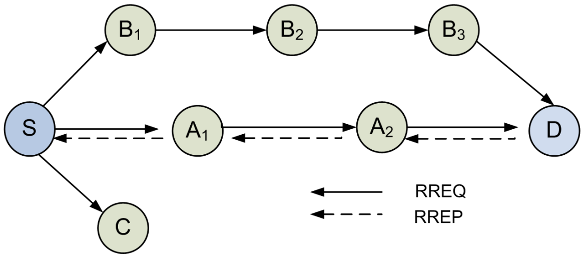

Figure 1: AODV Route Discovery [12]

III. BLACK HOLE ATTACK ON AODV PROTOCOL

Black hole attack] 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 packet.

For example As shown in Figure. 2, C is a malicious node whereas S and D are the source and destination nodes, respectively. First, the node S broadcasts RREQ packet to its one hop neighbors. Then, upon receiving this packet each neighbor node is supposed to rebroadcast it if a route cache towards the destination is unavailable. However, the node C disobeys this rule and claims that it has the shortest path to the destination and sends a RREP packet back to node S. Consequently, if the RREP packet sent by node D or any honest intermediate node, which has a fresh route to D, reaches the node S before the C's RREP then everything works well. Otherwise, the source node S deems that the route passing through the node C is the shortest path, and thus it starts transmitting data packets towards C which in its turn drops them.

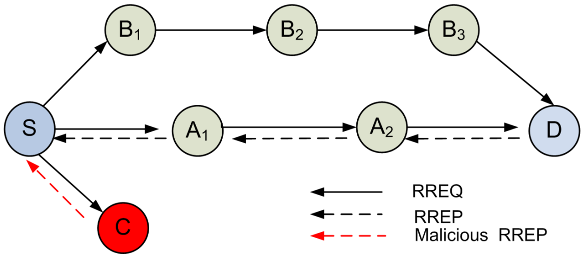

Figure 2: Black hole attack in AODV

IV. SOLUTIONS TO BLACK HOLE ATTACK IN MANET

In this section, we will review the several solutions to black hole attacks.

Soufiene Djahel, Farid NaÂÍÄśt-abdesselam, and Zonghua Zhang 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 defence lines devised here to protect MANETs against the packet dropping attack. The first defence line (for prevention purposes) aims to forbid the malicious nodes from participating in packet For-warding function. Whenever the malicious node exceeds this barrier, a second defence 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 defence 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. Most of the proposed solutions are built on a number of assumptions which are either hard to realize in a hostile and energy constrained environment like MANETs or not always available due to the network deployment constraints. Moreover, these solutions are generally unable to launch a global response system whenever a malicious node is identified. In contrast, they either punish the malicious node locally without informing the rest of the network or divulge its identity to the network through costly cryptographic computations. Moreover, even though the malicious node is punished in a part of the network it can move to another part and continues causing damage to the network until it is detected again [5].

In [6] solution the source node stores all the RREPs in the table called Cmg_RREP_Tab until receiving first RREP packet waits for MOS_WAIT_TIME. Meanwhile, the source node analyses all the stored RREPs from Cmg_RREP_Tab table, and discard the RREPs having a very high destination sequence number. Every node in the network maintains a table called Mali_node for storing the malicious node details to isolate the malicious node in the network. Moreover, in order to maintain freshness, the Cmg_RREP_Tab is flushed once an RREP is chosen from it. However, this solution fails to detect co-operative black hole attack and it has high processing delay.

In [7] authors proposed 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 neighbours. 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 neighbours in order to be ignored and eliminated. An overhead of updating threshold value at every time interval along with the generation of ALARM packet will considerably increase the routing overhead. This method is not support cooperative black hole nodes.

In [8] Authors Ming-Yang Su et.al discussed a mechanism, called an ABM (Anti-Black hole Mechanism), which is mainly used to estimate the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When a suspicious value exceeds a threshold level, the nearby IDS broadcasted a block message with id of IDS, the identified black hole node and the time of identification will place the malicious nodes on their blacklists to isolate the malicious node in the network cooperatively. The advantage of this method is that it can be able to detect cooperative black hole nodes in the MANETs. The main drawback of this technique is that mobile nodes have to maintain an extra database for training data and its updations, in addition to the maintenance of their routing table.

In[9] author propose a generalized intrusion detection and prevention mechanism. He use a combination of anomaly-based and knowledge based intrusion detection to secure MANETs from a wide variety of attacks. This approach also has the capability to detect new unforeseen attacks. In this paper monitors both network layer characteristics (NCM) and performance statistics (DM). GIDP uses a combination of anomaly-based and knowledge-based ID that can protect MANETs against a variety of attacks. In this paper suggested approach can protect MANETs from a wide variety of attacks with an affordable processing overhead. We also investigated the severity of various attacks and their impact on network performance along with the impact of the GIDP intrusion response on network performance. The results shows that in some cases isolating the attacker can cause more harm than good to network, hence an adaptive flexible intrusion response mechanism is required. But anomaly based and knowledge based IDS is proposed, which is very low and not appropriate concept for MANET. Because MANET does not have any kind of control management or centralized control. As proposed IDS is for various attacks very little attention is given to blockhole attack.

In [10] Authors propose a novel strategy by employing mobile honeypot 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. 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.

V. CONCLUSION

The various authors have given several proposals for detection and prevention of black hole attacks in MANET but every proposal has its own disadvantages in their respected solutions and we made a comparison among the existed solutions. We observe that the mechanisms detects black hole node, but no one is reliable procedure since most of the solutions are having more time delay, much network overhead because of newly introduced packets and some mathematical calculations. For future work, to find an effective solution to the black hole attack on AODV protocol.

References

[1] Kapang Lego. Comparative Study of Adhoc Routing Protocol AODV, DSR and DSDV in Mobile Adhoc Network. *Indian Journal of Computer Science and Engineering*, 1(4):364–371.

[2] Sheikh R., Singh Chande, M., and Kumar Mishra D. Security issues in MANET: A review. *Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference*, pages 1–4, 2010.

[3] Madhusudhananagakumar K.S., and G. Aghila. A Survey on Black Hole Attacks on AODV Protocol in MANET. *International Journal of Computer Applications*, 34(7), 2011.

[4] Mehdi Medadian, and Khossro Fardad. Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol. *European Journal of Scientific Research*, 69(1):91–101, 2011.

[5] Soufiene Djahel, Farid Naït-abdesselam, and Zonghua Zhang. Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges. *IEEE COMMUNICATIONS SURVEYS and TUTORIALS*, 13(4), 2011.

[6] Nital Mistry, Devesh C Jinwala, and Mukesh Zaveri. Improving AODV Protocol against Blackhole Attacks. *Proceedings of the International Multi Conference of Engineers and Computer Scientists - IMECS 2010*, 2, 2010.

[7] Payal N. Raj, and Prashant B. Swadas. DPRAODV: A Dyanamic Learning System Against Blackhole Attack In Bodv Based Manet. *International Journal of Computer Science Issues*, 2, 2009.

[8] Ming-Yang Su. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Department of Computer Science and Information Engineering, Ming Chuan University Computer Communications*, 34:107–117, 2011.

[9] Adnan Nadeem , and Michael Howarth. Protection of MANETs from a range of attacks using an intrusion detection and prevention system. *Springer Science Business Media, LLC*, 2011.

[10] Anoosha Prathapani, Lakshmi Santhanam, and Dharma P. Agrawal. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Springer Science Business Media, LLC*, 2011.