International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2017, pp. 202-205
e-ISSN:2278-621X

SECURING AODV PROTOCOL IN MANET

Mani Bushan Dsouza[1], Ajin Sanu[2], Manjaiha D.H[3] & Jeevan Pinto[4]

Abstract-Mobile Ad-hoc Networks or MANET is an infrastructure-less network formed by mobile devices that communicate among themselves without any centralized control. In such a dynamic environment, every transmission along the network becomes vulnerable to many attacks and security plays a major role in such networks.This paper focuses onvulnerabilities and various kinds of security attacks in MANET. The study is carried out for Ad hoc On-demand Distance Vector routing (AODV) protocol, which is a widely adopted network routing protocol for MANET. Black hole attack, is the one in which a malicious node,instead of forwarding the packets,drops all packets that it receives it. This attack causes degrade in the performance of AODV Protocol and hence affect the performance parameters. The paper also focuses on identifying the malicious node in AODV protocol suffering from black holeattack.
Keywords: Wireless system, Protocol, AdHoc, Network, Nodes, AODV,Blackhole, DPRAODV, ABM, ERDA

1. INTRODUCTION

A Mobile Ad Hoc Network (MANET), a set of mobile nodes that perform basic networking functions like packet forwarding, routing, and service discovery without the need of an infrastructure. All the nodes of an ad-hoc network depend on each another in forwarding a packet from source to its destination, due to the limited transmission range of each mobile node's wireless transmissions. There is no centralized administration in anad-hoc network. It guarantees that the network will not stop functioning just because one of the mobile nodes moves out of the range of the others[1].

A node should be able to enter and leave the network at any point of time. Multiple intermediate hops are generally needed to reach other nodes and due to the limited range of the nodes each and every node in an ad hoc network must be keen to forward packets for other nodes. In This way, each and every node performs therole of both a host and router. The topology of ad-hoc networks is dynamic and changes with time as nodes move or join or leave the ad hoc network. This unstable topology needs a routing protocol to run on each node to create and maintain routes among the nodes. Wireless ad-hoc networks can be used in special areas where a wired network infrastructure may be unsuitable due to reasons such as cost or convenience. It can be readily deployed to support emergency requirements, short-term needs, and coverage in developing and underdeveloped areas. So there are a plethora of applications for wireless ad-hoc networks.

2. AODV ROUTING PROTOCOL

MANET routing protocols are categorized mainly into three categories:

- Table-driven/ proactive
- Demand-driven/ Reactive
- Hybrid

Herewe are focusing on the AODV Routing protocol which is a Reactive protocol. AODV which is one of the most common ad-hoc routing protocols used in mobile ad-hoc networks. As given by their name, is an on-demand routing protocol that discovers a data transfer route only when there is a demand request from the mobile nodes in the given network. In an ad-hoc network that uses AODV as a routing protocol, a mobile node that wants to communicate with an adjacent or neighbouring node first, an RREQ (Route Request) message is broadcasted to find a fresh route to the desired destination node. This process is known as route discovery. All theadjcent node who receives the RREQ broadcast first saves the path that was followed by the RREQ during it's transmission.

The protocol checks its routing tableat periodic intervals to knowif a fresh enough route to the destination node was provided or not within the RREQ message. The novelty of a route is indicated by a destination sequence number that is attached to it. If a node discovers a freshnew route, it unicasts an RREP(Route Reply) message back along the saved path to the source node or it re-broadcasts the RREQ message otherwise. The process repeatsitself until an RREP message from the destination node or to an intermediate node that has afresh route to the destination node which was received by the source node.

3. BLACKHOLE ATTACK

[1] *Department of Computer Application & Bio Informatics, AIMIT, St Aloysius College,Mangaluru, Karnataka, India*
[2] *Department of Computer Application & Bio Informatics, AIMIT, St Aloysius College,Mangaluru, Karnataka, India*
[3] *Department of Computer Science, Mangalore University Mangaluru, Karnataka, India*
[4] *Department of Computer Science, Yenepoya Institute of Technology, Mangaluru, India*

In an ad-hoc network that uses the AODV protocol, a blackhole node makes its neighbouring node to believe that there is a fresh enough routes to the destination that was requested by the node. Thus the malicious node absorbs all the network traffic. When a source node broadcasts the RREQ message for any destination, the blackhole node immediately sends an RREP message which includes the highest sequence number and the message is perceived as if it has been dispatched from the destination or from a node which has a fresh enough route to the destination. The source node then starts to send out its data packets to the blackhole trusting that these packets will reach the destination. A malicious node sends RREP messages without looking up its routing table for a fresh route to a destination[2].The figure given below shows an example of a black hole attack(fig 1), where an attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than all the other nodes.

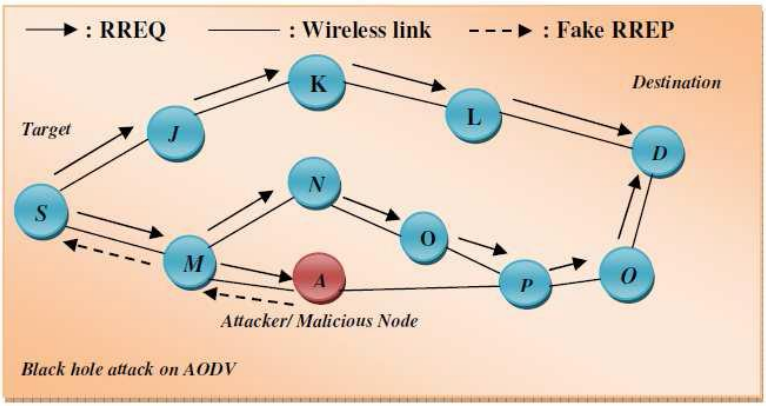

Fig. 1:Blackhole attack on AODV

Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A. However, a malicious node (performing a black hole attack) drops all the received data packets instead of forwarding them on.

4. METHODS FOR DETECTION & PREVENTION

In this section, we deal with five different methods for the detection and prevention of blackhole attacks in AODV based mobile ad-hoc networks.

4.1 DPRAODV(Detection,Prevention and Reactive AODV) scheme-

In this paper authors proposed have proposed the method DPRAODV[3]which tries to prevent blackholeattack by informing other nodes in the network. In normal AODV, the node which receives the RREP packet first checks for the sequencing value in the routing table. If its sequence number is higher than the one in the routing table, this RREP packet is accepted. In this proposed 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 forwarded to the other nodes nor is it updated into the routing table. The threshold value is dynamically updated using the data collected in the time interval. The threshold value is calculated as the average of difference of destination sequence number in each time slot between the sequence number in the routing table with that of the one received from the RREP packet. The main advantage of this protocol is that the source node notifies about the blackhole to its neighbours, so that it will be ignored and eliminated[3].

Drawback:

Threshold value is updated at every time interval along with the generation of an ALARM packet, this will considerably increase the routing overhead. Also This method does not support cooperative black hole nodes.

4.2 B.ABM (Anti-Blackhole Mechanism) scheme -

This paper [4]attempts in detection and removal of the malicious nodes, which selectively perform black hole attacks by deploying IDSs in MANETs (mobile ad hoc networks). All IDS nodes perform an ABM(Anti-Blackhole Mechanism), which estimates the suspicion value of a selected node, comparing itwith the amount of abnormal difference between RREQs and RREPs transmitted from the particular node, With the prerequisite that intermediate nodes are forbidden to reply to RREQs.If an intermediate node, which is not among the destination and those which never broadcasts a RREQ for a specific route but forwards a RREP for the route, then the nodes suspicious value will be incremented by 1 in the nearby IDS's SN (suspicious node) table. When the suspicious value of a node exceeds by a given threshold, a Block message is broadcasted by the detected IDS to all nodes so that the suspicious node could be isolated.

Drawbacks:

IDS nodes are specially located within their transmission range, which is not always feasible in normal case special security mechanism needed to safe communication between special IDS nodes. role of special IDS nodes became very confusing.

4.3. Honeypot based detection scheme :-

The author proposes a novel strategy that works by exploitingthe use of mobile honeypot agents that utilize their topological knowledge, which in turn usesthis knowledge to detect spurious route advertisements. They are setup as roaming software agents that tour the network and lure out the attackers by sending route request advertisements to the targeted nodes. The data collected is the valuable information on as attacker's strategy from the intrusion logs thatare gathered at a given honeypot[4]

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.

4.4. ERDA (Enhance Route Discovery for AODV) scheme:

An ERDA [5]solution to improve AODV protocol with minimalmodifications to the existant route discovery mechanism by employing anrecvReply() function. A method called ERDA (Enhance Route Discovery for AODV) where it is able to modify the problem by introducing new set of constraintsto the routing table update process and introducing simple maliciousnode detection & isolation process to the AODV route discovery mechanism. The proposed method won't deliver any additional control message and moreover, it won't change the existing protocol schemes. There are three new elements introduced to therecvReply() function namely: table rrep_table to store incoming RREP packet parameter, amali_list to keep the detected malicious nodes identity and a parameter rt_upd to control the routing tables updating process. When RREQ packet is sent out from source node S to find a fresh route to the given destination node D. The RREP packet received by the node S will updated into anrrep_tab table. Since the malicious node M is the first node to respond, the routing table of node S will be updated with the RREP information from node M. Since the parameter value of rt_upd is true, node S accepts the next RREP packet from the other node to update the routing table even though it arrives later and with a lower destination sequencing number than the one found in the current routing table. The present route entry within the routing table will be overwritten by the later RREP coming from other node. ERDA method offers a simple solution by eliminating the false route entry and replaced the entry with later RREP.

Drawbacks:

It cannot detect cooperative black hole attack.

4.5. Cryptographic Based Technique:

This paper[6]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 data integrity and availability. These techniques fail to prevent a malicious node from dropping packets that is supposed to be relayed. There basically are three defence lines devised here to protect MANETs against the packet dropping attack. The first defence line (for prevention purposes) aims at forbidding the malicious nodes from participating in packet forwarding. 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.

Drawbacks:

Most of the proposed solutions are built on a number of assumptions which were either hard to realize in a hostile and energy constrained environment like MANETs or not always available due to the network deployment constraints. These solutions are generally unable to launch a global response system whenever a malicious node is identified. In contrast to this, they either punish the malicious node locally without informing the rest of the network or reveal its identity to the network through cryptographic methods which have a considerable overhead. 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. CONCLUSION

Blackhole attack is a major security risk on MANET with AODV protocol and detection of the same is a matter of concern. Many researchers have conducted several techniques that proposes different techniques of prevention mechanisms against theblackholevulnerability. There are various security mechanisms which have been introduced to prevent it. Methods discussed in this paper not only prevent blackholeattacks but also helps in detecting them. The information about the malicious nodes are broadcasted to all other nodes, which intern delete the entries from their routing table. Thus all future communications with the malicious node can be avoided. By detecting and eliminating Blackhole nodes, Packet Delivery Ratio and Throughputcan be increased. Also, by detecting and preventing Blackhole security of AODV can be increased.

6. REFERENCES

[1] BhoomikaPatel, "Improving AODV Routing Protocol against Black Hole Attack based on MANET", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3586-3589

[2] Dr. S. Tamilarasan, "Securing AODV Routing Protocol from Black Hole Attack", International Journal of Computer Science and Telecommunications [Volume 3, Issue 7, July 2012]
[3] Payal N. Raj, Prashant B. Swadas" DPRAODV: A Dyanamic Learning System Against Blackhole Attack In AODV Based Manet." arXiv:0909.2371,2009.
[4] Ming-Yang Su," Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Elsevier, Computer Communications 34 (2011) 107–117
[5] KamarularifinAbd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan,"Mitigation of Black Hole Attacks for AODV Routing Protocol", Society of Digital Information and Wireless Communications (SDIWC) Vol01_No02_30, 2011.
[6] SoufieneDjahel, FaridNa¨ıt-abdesselam, and ZonghuaZhang ,"Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 13, NO. 4, FOURTH QUARTER 2011.