ISSN:0975-9646

A Review - Prevention and Detection of Black Hole Attack in AODV based on MANET

Bhoomika Patel
Department of Information Technology,
Parul Institute of Engineering & Technology, Limda,
Vadodara, India.

Khushboo Trivedi
Department of Computer Science And Engineering,
Parul Institute of Engineering & Technology,Limda,
Vadodara, India.

***Abstract*- In recent years mobile ad hoc network has a great impact on wireless networks. In MANET ,each node acts as a router to establish a route and transfer data by means of multiple hops. MANET are more vulnerable to security problem. When a node wants to transfer data to another node, packets are transferred through the intermediate nodes, thus, searching and establishing a route from a source node to a destination node is an important task in MANETs. Routing is an important component in MANET and it has several routing protocols. Ad hoc On-demand Distance Vector (AODV) is one of the most suitable routing protocol for the MANETs and it is more vulnerable to black hole attack by the malicious nodes. A malicious node that incorrectly sends the RREP (route reply) that it has a latest route with minimum hop count to destination and then it drops all the receiving packets. This is called as black hole attack. In the case of multiple malicious nodes that work together with cooperatively, the effect will be more. This type of attack is known as cooperative black hole attack. There are lots of efforts have been made to defend against black hole attack, but none of the solution looks most promising to defend against black hole attack. So in this paper, We have surveyed and compared the existing solutions to black hole attacks on AODV protocol**.

Keywords— MANET, AODV, Black hole attack

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a set of mobile nodes that perform basic networking functions like packet forwarding, routing, and service discovery without the need of an established 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 ad 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. As nodes wish, they should be able to enter and leave the network. Multiple intermediate hops are generally needed to reach other nodes, 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. This way, every node performs role of both, a host and a router. The topology of ad hoc networks is dynamic and changes with time as nodes move, join or leave the ad hoc network. This unsteadiness of 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 rapidly deployed to support emergency requirements, short-term needs, and coverage in undeveloped areas. So there is a plethora of applications for wireless ad-hoc networks. ‘’

II.ROUTING PROTOCOLS

MANET routing protocols are categorized into three main categories:

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

In this paper, We are focusing on AODV Routing protocol which is Reactive protocol. AODV is one of the most common ad-hoc routing protocols used for mobile ad-hoc networks. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is a demand from mobile nodes in the network. In an ad-hoc network that uses AODV as a routing protocol, a mobile node that wishes to communicate with other node first broadcasts an RREQ (Route Request) message to find a fresh route to a desired destination node. This process is called route discovery. Every neighboring node that receives RREQ broadcast first saves the path the RREQ was transmitted along to its routing table. It subsequently checks its routing table to see if it has a fresh enough route to the destination node provided in the RREQ message. The freshness of a route is indicated by a destination sequence number that is attached to it. If a node finds a fresh enough 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 same process continues until an RREP message from the destination node or an intermediate node that has fresh route to the destination node is received by the source node. [1]

III. BLACKHOLE ATTACK

In an ad-hoc network that uses the AODV protocol, a blackhole node pretends to have fresh enough routes to all destinations requested by all the nodes and absorbs the network traffic. When a source node broadcasts the RREQ message for any destination, the blackhole 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 node then starts to send out its data packets to the blackhole trusting that these packets will reach the destination.

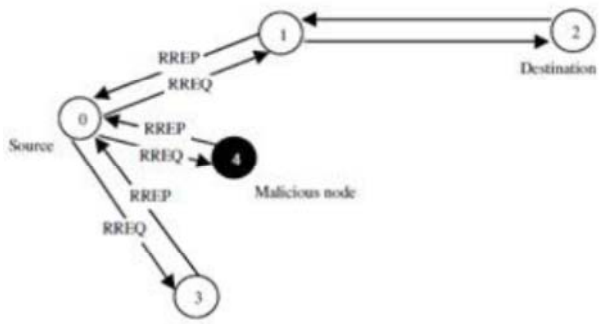

Fig.1 RREQ Broadcast

A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. As shown in fig.1, source node 0 broadcasts an RREQ message to discover a route for sending packets to destination node 2. An RREQ broadcast from node 0 is received by neighboring nodes 1,3 and 4. However, malicious node 4 sends an RREP message immediately without even having a route to destination node 2. An RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighboring nodes even from an actual destination node. Once a source node saves a route,it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. A malicious node drops all data packets rather than forwarding them on. [2]

IV. LITERATURE SURVEY

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

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

In this paper authors proposed have proposed the method DPRAODV[15] (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[15].

Results:
The packet delivery ratio is improved from 80 to 85% than AODV under black hole and 60% when traffic load increases.
Drawbacks:
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.

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

This paper attempts 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-Blackhole 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.[9]
Drawbacks:
IDS nodes are specially located within each others 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.

C. *Honeypot based detection scheme*

Athors 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[9]
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. *ERDA (Enhance Route Discovery for AODV) scheme*

Have designed an ERDA solution to improve AODV protocol with minimum modification to the existing route discovery mechanism recvReply() function. a method called ERDA (Enhance Route Discovery for AODV).
The proposed method is able to mitigate the a foresaid problem by introducing new conditions in the routing table update process and also by adding simple maliciousnode detection and isolation process to the AODV route discovery mechanism. The proposed method does not

introduce any additional control message and moreover, it does not change the existing protocol scheme.

There are three new elements introduced in modified recvReply() function namely: table rrep_table to store incoming RREP packet parameter mali_list to keep the detected malicious nodes identity and parameter rt_upd to control the process of updating the routing table. When RREQ packet is sent out by the source node S to find a fresh route to the destination node D. RREP packet received by node S will be captured into rrep_tab table. Since the malicious node M is the first node to response, the routing table of node S is updated with RREP information from node M Since the value of parameter rt_upd is true, node S accepts the next RREP packet from other node to update the routing table although it arrives later and with a lower destination sequence number than the one in the routing table.

The current route entry in 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.[7]

Drawbacks:

It cannot detect cooperative black hole attack.

E. *Cryptographic based technique*

This paper focuse 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.[8]

Drawbacks:

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.

V. CONCLUSION

Blackhole 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 blackhole problem. There are different security mechanisums are introduced to prevent blackhole attack.

REFERENCES

Papers:

[1] 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.

[2] Ranjeet Suryawanshi,Sunil Tamhankar," Performance Analysis and Minimization of Blackhole Attack in MANET" IJERA, july-August 2012

[3] 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.

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

[5] Mehdi Medadian, Khossro Fardad," Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol", European Journal of Scientific Research ISSN 1450-216X Vol.69 No.1 (2012), pp.91-101

[6] Priyanka Goyal, Vinti Parmar, Rahu Rishi"MANET:Vulnerabilities, Challenges, Attacks, Application" IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[7] Kamarularifin Abd. 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.

[8] Soufiene Djahel, Farid Na¨ıt-abdesselam, and Zonghua Zhang ,"Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 13, NO. 4, FOURTH QUARTER 2011.

[9] 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

[10] Adnan Nadeem · Michael Howarth," Protection of MANETs from a range of attacks usingan intrusion detection and prevention system" ,Springer Science+Business Media, LLC 2011

[11] Anoosha Prathapani,Lakshmi Santhanam,Dharma P. Agrawal," Detection of blackhole attack in aWireless MeshNetwork using intelligent honeypot agents" Springer Science+Business Media, LLC 2011

[12] Lalit Himral, Vishal Vig, Nagesh Chand, "Preventing AODV Routing Protocol from Black Hole Attack" International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[13] Sreedhar. C, Dr. S. Madhusudhana Verma and Dr. N. Kasiviswanath, "POTENTIAL SECURITY ATTACKS ON WIRELESS NETWORKS AN THEIR COUNTERMEASURE", International journal of computer science & information Technology (IJCSIT) Vol.2, No.5, October 2010

[14] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", proceedings of the International Multi Conference of Engineers and Computer Scientists 2010 Vol II, IMECS 2010.

[15] Payal N. Raj, Prashant B. Swadas" DPRAODV: A Dyanamic Learning System Against Blackhole Attack In AODV Based Manet." arXiv:0909.2371,2009.

[16] H. Deng, W. Li and D. P. Agrawal, Routing security in wireless ad hoc networks, IEEE Commun. Mag., 40(10): 70-75, October 2002.

[17] Lidong Zhou, and Zygmunt J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no.6, November/December 1999.

[18] http://www.faqs.org/rfcs/rfc3561.html