Volume 2, Issue 2 ISSN: 2320-5288

International Journal of Engineering Technology & Management Research
Journal homepage: www.ijetmr.org

A Review on Detection of Gray Hole Attack in MANET AODV Routing Protocol

Dr. Mamta Lambert
Associate Professor
Department of Computer Applications
Jabalpur Engineering College
Jabalpur , India
Email: lambert_mamta@yahoo.co.in

Mr. Sharda Prasad Patel
Email :- sharda21patel@gmail.com

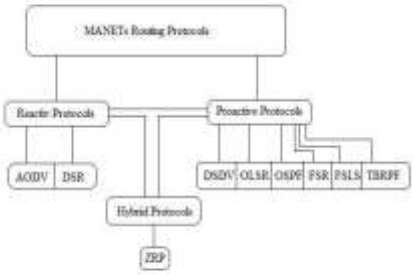
***Abstract*—**Mobile ad-hoc network is mobile, multihop wireless network which is capable of autonomous operation. A Gray hole is a node that selectively drops and forwards data packets after advertises itself as having the shortest path to the destination node in response to a route request message. Information exchange in a network of mobile and wireless nodes without any infrastructure support such networks are called as ad-hoc networks. Many researchers have given different solutions for preventing and detecting this attack. We have discussed some of the proposed solution in this survey.

Keywords:— MANET, AODV, Routing Protocols, gray hole node, malicious node.

1. INTRODUCTION

A Mobile Ad-hoc Network (MANET) can be defined as collection of mobile nodes. It does not rely on any fixed infrastructure. Since it is an infrastructure less network, the mobile nodes in the network dynamically setup paths among themselves to transmit packets from the source to destination and it is a self-configuring network. Gray hole attack is one of the attack in network layer which comes under security attacks. MANET can be used in different applications such as battlefield communication, emergency relief scenario etc. The nature of MANET is a dynamically changing process, due to its dynamically changing process its vulnerable for wide range of attack. [11]

For example, routing messages are an essential component of mobile network communications, as each packet needs to be passed quickly through intermediate nodes, which the packet must traverse from a source to the destination. Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols. There are also attacks that target some particular routing protocols, such as DSR, or AODV.



2. SECURITY ATTACKS

The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks, according to the attack means. A passive attack obtains data exchanged in the network without disrupting the operation of

the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Table 1 shows the general taxonomy of security attacks against MANET. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay. The attacks can also be classified into two categories, namely external attacks and internal attacks, according the domain of the attacks. Some papers refer to outsider and insider attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

TABLE 1: Security Attacks Classification

Passive Attacks	Eavesdropping, traffic analysis, monitoring
Active Attacks	Jamming, spoofing, modification, replaying, DoS

3. PROTOCOLS USED IN MANET

In MANETs nodes communicate with each other by using some routing protocols. According the dynamic topology and characteristic there are three main routing protocol used in MANETs. These all are discussed below.

Proactive (table driven) routing protocol:
This protocol is also called as table driven protocol because in this protocol each node in the network maintains its detailed routing table. These all are discussed below.

In the routing table each node maintain complete path to the reachable node with its hop count. In this, each node periodically broadcast their routing information to the neighbors. Periodically update and large routing table generate large amount of overhead in the network which makes this protocol unusable. There are two main kind of this protocol optimized link state routing (OLSR) protocol and destination sequenced distance vector routing (DSDV) protocol.

Reactive (On-Demand) routing protocol:
This protocol starts functioning whenever any node wants to transmit data to other node. In this protocol network bandwidth is not wasted and network is less congested. This protocol is less secure than the proactive protocols. Two kinds of protocols are there in it Ad-hoc On Demand Distance Vector (AODV) protocol, Dynamic Source Routing (DSR) protocol.

Hybrid Routing Protocol:
This protocol combines advantages of both proactive and reactive routing protocol. Two types are: Zone routing protocol (ZRP) and temporally ordered Routing protocol (TORA). At the initialization phase this follows proactive characteristic after that in between when network topology has changed it follows reactive characteristic

4. OVERVIEW OF AODV ROUTING PROTOCOL

AODV is an ad-hoc on demand distance vector routing protocol that establishes route to the destination when it is desired by the source node. It maintains this routes as and when needed by the source node. It offers quick adaptation to dynamic link conditions, low processing, memory overhead, low network utilization, and determines unicast routes to destinations within the Ad-hoc network. The format of

RREQ and RREP packets are in Figure 1.1 and 1.2 respectively. [14]

Src_ad-dres	Src_se-quence	Broad_Cast_id	Dest_ad-dres	Dest_se-quence	Hop count

Figure 1.1 : AODV RREQ Field

Src_ad-dres	Dest_ addres	Dest_se-quence	Hop count	Life time

Figure 1.2 : AODV RREP Field

One of the distinguishing feature of AODV protocol is its use of destination sequence number associated with every route. Destination sequence number is created by the destination to include route information about it send to the requesting node. In order to communicate among the mobile nodes, Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. When a source node wants to connect to a destination node, first it checks in the existing route table, as to whether a fresh route to that destination is available or not. Fresh enough route means a valid route entry whose sequence number is greater than it in the RREQ. Larger the sequence number, fresher is the route. If a fresh enough route is available, it uses the same. Otherwise the node initiates a Route Discovery by broadcasting a RREQ control message to all of its neighbors. This RREQ message will further be forwarded by the intermediate nodes to their neighbors having a fresh route to the destination.

5. GRAY HOLE ATTACK

Gray Hole attack is an active type of attack in which attacking node first agrees to forward packets and then fails to do so, which leads to dropping of messages. In Gray Hole attack we can't predict the probability of losing data. In Gray Hole Attack a malicious node refuses to forward certain packets and merely drops them.

Gray Hole nodes in MANETs are very dominant. Every node maintains a routing table that stores the next hop node information. When a source node wants to route a packet to the target node, it uses a specific route if such a route is available in its routing table. Otherwise, nodes start a route discovery process by broadcasting Route Request (RREQ) message to its neighbors. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node. A Route Reply (RREP) message is sent back to the source node when the RREQ query Reaches either the destination node itself or any other node that has a current route to destination .

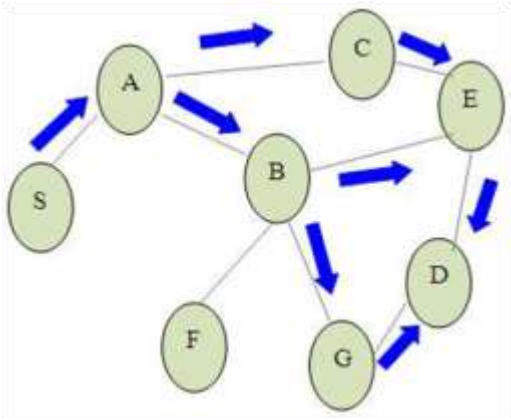


Figure. 2. AODV route discovery using RREQ Packet

6. REVIEW OF THE METHODS

6.1. First Method

Detection process for gray hole attack by source node:

- Dividing data packets into *k* equal parts.
- Sending a message to destination containing number of messages.
- Broadcasting messages to all neighbors of route.
- After ensuring that destination node knows count of messages, source begins sending of data.

Setting up a timer until getting number of data packets that destination receives.

If number of announced data packets from destination is less than a limit, initiates removing process of gray hole attack.
Also if after terminating of timer, did not get any message from destination, starts removing process of gray hole attack.

Advantages
Using a limit for identifying malicious nodes, decreases number of mistakes in identifying gray hole attack. This threshold is the probability of packet dropped by a node through no fault of its own. Packet dropping may occur due to overhead, lack of CPU cycles, buffer space or bandwidth, congestion or collusion to forward packets.
This method can detect both black and gray hole attacks and also can detect selfish node.

Disadvantages
In this method, all nodes should always monitor each other; in this case, the network has a high overhead and also each node consumes a lot of energy for monitoring.
Detection speed for malicious nodes is low, a lot of data lost until malicious node can be detected.

6.2. Second Method
Another algorithm is considering a limit for sequence number. When source node receives RREP packets, it checks them with a threshold for sequence number of that route and if the received RREP sequence number is higher than that, source enters that node ID in a blocked list and announces that node as malicious to all nodes by broadcasting its ID; because in Gray hole, attacker starts dropping packets by announcing itself as a node has the freshest route to destination. This sequence number threshold is calculated by average of table's entries sequence numbers in a certain period of time.

Advantages
Main benefit of this method is simplicity.
On the contrary of other methods, no energy is consumed for monitoring.

Disadvantages
This algorithm does not detect any grayhole attacks.

This method may also make mistake when a node is not malicious, but according to its higher sequence number may be entered into blocked list.

6.3. Third Method
By using watchdog timer, malicious node can be detected. Each node monitors its next node in the route. If it finds any packet forwarding misbehavior or any packet dropping in a predefined period of time for its next node, it will introduce the next node as a malicious node to the source.

Advantages
This is a simple method, so that one node should just listen to its next node in the route.

Disadvantages
In watchdog, each node should always monitor its next neighbors.

Source node should trust the other node's information about one node's misbehavior.

It does not use predefined limit to distinguish malicious nodes and as previously mentioned it increases numbers of mistakes to find gray hole attacks.

6.4. Fourth Method
This method is an extension similar to watchdog design. It categorizes nodes into two groups called trusted and ordinary. Trusted nodes are previously proved their trustfulness to other nodes. Watchdog nodes that monitor the network are selected from these trusted nodes. Watchdog nodes are selected according to some other criteria such as: energy of each node, enough storage memory and node

calculating power. Watchdog tasks exchange between trusted nodes after a period of time. In each watchdog two limit values and counters are considered, ACCEPTANCE threshold and SUSPECT threshold. ACCEPTANCE threshold is a limit that once correct packet sending of one node exceeds it, that node enters in trusted nodes. SUSPECT threshold is used to count maliciousness of one node for packet dropping and after exceeding that limit, that node enters in malicious nodes and announces that as a Gray hole node to the network.

Advantages

Selecting some trusted nodes for monitoring decreases monitoring overhead on all the 0nodes and also just some special trusted nodes monitor other nodes in network.

Assuming a limit for maliciousness of a node and entering that node in gray hole list, is a reason of decreasing detection mistakes in this method.

This method also can distinguish cooperative gray hole attacks.

Disadvantages

In this method, if trusted nodes start maliciousness treat and drop packets, like gray hole attack, security of the network is missed and this attack cannot be detected.

7. CONCLUSION

Based on the above survey Gray hole attacks are the most important security problems in MANET. Detection of gray hole is difficult, because the attacker works as normal node then starts dropping of data. In this paper, the approaches proposed by different authors to eliminate the gray hole attack are discussed. In this paper we have discussed different techniques for detection and prevention of gray hole attack in MANET.

REFERENCE

[1] Banerjee, S. 2008. "Detection/ removal of cooperative black and gray hole attack in mobile ad-hoc networks", In Proceedings of the World Congress on Engineering and Computer Science.

[2] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., and Nemoto, Y. 2007. "Detecting black hole attack on aodv-based mobile Ad-hoc networks by dynamic learning method". J. Network Security. Vol. 5, No. 3 (Nov. 2007), 338–346.

[3] Marti, S., Giuli, T. J., Lai, K., and Baker, M. 2000. "Mitigating routing misbehavior in mobile ad hoc networks", In Proceedings of the 6th Annual International Conference on MOBICOM, Boston, Massachusetts, United States, 255-265.

[4] Patcha, A., and Mishra, A., 2003. Collaborative security architecture for black hole attack prevention in mobile ad hoc networks. In Proceedings of the Radio and Wireless Conference (RWCON), VA, USA, 75-78.

[5] "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad- Hoc Networks", Sukla Banerjee, Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 – 24, 2008, San Francisco, USA.

[6] "A Literature Survey of Black Hole Attack on AODV Routing Protocol**"** Chandni Garg1, Preeti Sharma2, Prashant Rewagad3 International Journal of advancement in electronics and computer engineering (IJAECE) Volume 1, Issue 6, Sep 2012.

[7] "Advanced Algorithm for Detection and Prevention of

Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks”**,** Shalini Jain, ©2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 7.

[8] “Detection and Removal of Cooperative Black/Gray hole attack in Mobile AD-HOC Networks”, Amos J Paul, ©2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 22.

[9] “Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol” Onkar V.Chandure International Journal of Computer Applications (0975 – 8887) Volume 41– No.5, March 2012.

[10] “Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol” Nishu kalia, Kundan Munjal, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-3, February 2013.

[11] “A Survey on Gray Hole Attack in MANET” V. SHANMUGANATHAN, Master of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, India.

[12] “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei Department of Computer Science and Engineering Florida Atlantic University Wireless Mobile Network SECURITY Y. Xiao, X. Shen, and D.-Z. Du (Eds.) 2006 Springer.

[13] “Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET: A Survey”

[14] Nitesh A. Funde1, P. R. Pardhi2 M Tech Scholar, Department of Computer Science, RCOEM, Nagpur, India 1 Professor, Department of Computer Science, RCOEM, Nagpur, India. IJARCCE Vol. 2, Issue 10, October 2013.