A STUDY ON NETWORKING ATTACKS IN MANET

[1] S.Geetha Priya, Assistant Professor,Department of IT & CT, VLB Janakiammal College of Arts and Science,TamilNadu, India
[2] S.Joy Jeba Merline, Assistant Professor,Department of IT & CT, VLB Janakiammal College of Arts and Science,TamilNadu, India

ABSTRACT

This paper discusses about the networking attack that takes on a wireless network. There are a broad classification of network attacks, but here we discuss only about black hole attack and grey hole attack. The network topology is dynamic each and every node communicates from difficult network, so there arise a problem of security issues. It is very difficult to identify the intruder. So here we have discussed about the detection and the prevention techniques of both grey hole and black hole attack.

Keyword: - *MANET, Black hole attack, Grey hole attack, RREQ, RREP, intruder*

1. INTRODUCTION

The network is applied in fields such as wars, education, natural disasters etc. Manet is an adhoc network which is constructed without any infrastructure. A node acts as a router as well as a transmitter. The nodes transmit data from source to destination through frequency signals. Ad-Hoc network face the greatest challenge. Many researchers have proposed solutions for identifying the single black hole node. The packet delivery ratio will reduced if some malicious node is in the path of destination node. To overcome from this problem, identification of malicious node is necessary.

The performance of network is enhanced by adding a trust for each node and its behavior is monitored. A node with a low trust value in a network is considered as a misbehaving node in the network. A single node or multiple nodes collectively can perform the black hole attack. When a Source node want to establish a route to Destination node, the source node S will broad cast the RREQ message to all the nodes in the network until it reaches to Destination node. This process happens when their is no networking attacks

2. Black hole Attack

.

Two nodes communicate on their active participation in data exchange process. The source node transfers or sends data to the destination node by checking its routing table. If it does not have the destination node in the list, then it performs route discovery process A node X needs to transmit a data to node Z. So it broadcasts a RREQ packet to all of its neighborhood nodes. The intruder node W replies with a RREP packet that it has the route to the destination node Z. The destination node have also send the RREP packet . If the RREP packet of the destination node reaches before the intruder node packet delivers, then it works well. If not then the intruder node misbehaves as it wish.

Hence if the source node receives the intruder node packet first, it accepts the packet and completes the route discovery process and discards all the incoming packets thereafter. Now it gets ready to send data to the intruder node. The data packets are transmitted through hacked routing. Now the intruder node receives all data packets and drops it by occupied the data transmission route. The Node W is known as the black hole in the network and it is said to be as the black hole attack.

A. Types of Black hole attack

Black hole attacks are of two types: Single Black hole Attack and Collaborative Black hole Attack

1) **Single Black hole Attack**

The Single black hole attack has a single intruder node and it acknowledges with a fake packet RREP of the shortest path to the destination node when it receives a RREQ packet for a particular destination . Then this node drops all the packets passing through it.

2) **Collaborative Black hole attack:**

In collaborative Black hole attack has multiple intruder nodes . These intruders combines and coordinates all hacking operations against a targeted node. Here the initial intruder node sends the packet to the next intruder node. All the intruder nodes have the complete data about other intruder node. This type of attack is very tedious to detect.

B. Black hole detection

In this approach [10]each node maintains a secret protocol. Each node monitors its neighborhood node continuously. If their is any discrepancy on the transaction of that node it informs by sending an ALERT message to its neighbor nodes.

If the process of that node is intolerable its informs to the manager if that network about the trustworthy issue about a particular node. The manager then disconnects the path to that intruder node. This mechanism fails to work on grey hole attack that is dropping partial bits of data.

A proposed simple Black hole detection technique is sequence number generation. Each and every node in the network is allotted a number and it is stored in the routing table. When a source node receives a RREP packet it finds the difference between its id with that of the destination nodes id. If their arise a major difference then it is considered as the intruder node. It removes the nodes information from RREP table and the intruder node is permanently removed from the network.

Next Black hole detection approach is to identify individual nodes. For example, a node A sends a data packet to node C via node B. hence A ,the sender sends a RREQ packet to its neighboring node B. Now node B replies with a RREP packet saying that node C is its neighborhood node. To ensure a trustworthy communication node A communicates with node C and confirms whether node B is its neighbor node. This method even though it is better, but it fails to support in collaborative GREY hole attack.

C. Black hole Prevention

The black hole attack can be prevented by buffering mechanism . The sender sends a REQ packet to all its neighborhood nodes. While receiving the RREP packet, the sender buffers at least three RREP packets and decides the safest path to send the data packets. In this approach the sender after sending RREQ packet receives RREP packet from its neighbor nodes. It discards the first RREP packet because it may be a Black hole node. Hence it accepts the next shortest path to transmit the data to the destination node. There is a possibility for the Black hole node to be available in the next network. To resolve this issue hashing function is incorporated. RREP node holds the hash message along with it , even though it's quite costly to implement. Hashing technique is the best authentication mechanism. But Hash function is cost effective than other authentication technique.

3. GREY HOLE ATTACK

Grey Hole Attack can't be easily detected and can't identify how many packets will be lost. In GREY hole Attack , the intruder node aims at a specific or a group of IP address and selectively discards certain packets and forwards the rest of the packets intruder node acts as a genuine node and performs dropping random data . A packet contains data and a link to its neighboring node. Every node in the network maintains the routing table .Each and every time a packet arrives it checks whether the destination node is in its list. If it contains the data it transmits the packet to the destination path, if not it performs route discovery process to identify the path.

The neighboring node process its routing table to identify the path to the destination node. It then sends the path in reverse order to the source node as a RREP packet. GREY hole nodes in MANET is very effective. It is very

difficult to identify such type of attacks because packet loss may happen not only by the intruder node , it can occur due to network traffic , overload etc. Greyhole attack is very tedious task because a node acts both as an intruder node and as a normal node.

GREY hole attack consist of two phases:

Phase 1: The intruder node updates source routing table with the information about the destination node as its shortest path.

Phase 2: The intruder node now receives all the packets from the sender. It uses certain algorithm to randomly drop packets. It sends some data exactly and drops certain packets to the destination node to pretend itself as a normal node.

C. Grey hole detection

In this proposed approach ,each and every node allots a value for its neighbor node known as credit value. This credit value added on sending a request through RREQ packet protocol and subtracted on receiving a RREP packet protocol. When the sender node receives a garbage value from a node as its credit value it is called as the intruder node.

D. G. Kariya et al proposed an algorithm which is based on a course based scheme. In this scheme, a node observes only the next hop in current route path but does not observe every node in the neighbor. In this scheme FwdPacketBuffer is maintained by every node, it is also known as a packet digest buffer. The algorithm is divided into three steps: A) when a packet is forwarded out, its digest is stored into the FwdPacketBuffer and the detecting node overhears. B) Once the action that the next hop forwards the packet is overheard, the digest will be freed from the FwdPacketBuffer. C) The detecting node should calculate the overhear rate of its next hop node and compare it with a threshold in a fixed period of time. The overhear rate of the Nth period of time is defined as OR (N), the percentage of the data packets which are actually received by the destination.

P. Agrawal et al proposed a technique for detecting gray hole nodes in ad hoc network. In this technique the strong nodes are connected to the ad hoc network. These strong nodes identify other nodes with low power antenna , whether they act maliciously. Now the source and destination nodes makes an end to end checking to identify whether the packets have reached the destination or not. If their arise any failure, the network takes some measures to identify the intruder node. In order to detect the malicious node, the source node broadcast a find a chain message to all its neighboring nodes. All strong nodes votes for the next node and then forwards the packet, if the node id is null, it is considered to be as the malicious node. The process gets terminated immediately and the network alerts all the strong nodes about the malicious node in the network.

D. Grey hole Prevention

Pradeep Kumar Sharma et al, proposed a centralized system with MANET to prevent the attacks. All nodes s gets connected to a server as a mediator for all sending and receiving information's. The server stores information about t users and all the communications between the nodes as a centralized server-structure. The packet drop ratio is more in black Hole attacks than Gray Hole attacks. The routing load increases in the presence of Black Hole attacks compared to Gray Hole attacks.

4. CONCLUSION

In this paper I have discussed different techniques for detection and prevention of gray hole and black hole attacks in MANET. A lot of efforts have been done for the detection and prevention of gray hole attack which are still computational intensive. There is also need to explore new types of coordinated attacks that can be launched on mobile ad hoc networks, design and implement an efficient algorithm to detect and prevent them, because these attacks can greatly reduce the system performance in a small amount of time and result in a larger damage. In our

future work we are going to propose a new algorithm based on trace gray and course based algorithm which can improve the gray hole

5. REFERENCES

[01]. J. K. Author, "Title of chapter in the book," in Title of His Published Book, xth ed. City of Publisher, Country if not USA: Abbrev. of Publisher, year, ch.x, sec. x, pp. xxx–xxx.

[02]. W.- G.O.Young,"Syntheticstructureofindustrial plastics,"in Plastics, 2nded., vol. 3, J. Peters, Ed. New York: McGraw-Hill,1964,pp.15–64.

[03]. K.Chen,LinearNetworksandSystems.Belmont, CA:Wadsworth, 1993, pp. 123–135.

[04]. J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility," IEEE Trans. Electron Devices, vol. ED-11, no. 1, pp. 34–39, Jan. 1959.

[05]. E. P. Wigner, "Theory of traveling-wave optical laser,"Phys. Rev., vol. 134, pp. A635–A646, Dec. 1965.

[06]. E. H. Miller, "A note on reflector arrays," IEEE Trans.Antennas Propagat., to be published.

[07]. L. Junhai, X. Liu, and Y. Danxia, "Research on multicast routing protocols for mobile ad-hoc networks", Cmput Netw., vol. 52, no.5, pp. 988-997, 2008.

[08]. K. Lakshmi, S.Manju Priya, A. Jeevarathinam K.Rama, K.Thilagam, "Modified AODV Protocol Here Blackhole Attacks in MANET", In- ternational Journal of Engineering and Technology

[09]. S. Buchegger and J. Y. Le Boudec. A robust reputation system for mobile adhoc networks. Technical Report IC/2003/50, EPFL-DI-ICA, July 2003

[010]. Yibeltal Fantahum Alem & Zhao Hheng Xaun, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection ", from Tainjin 300222, China 2010, IEEE Vol.2 (6), 2010.

[011]. Lalit Himral, Vishal Vig, Nagesh Chand," Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology (IJEST).

[012]. M. Amaresh and G. Usha, "Efficient malicious detection for AODV in mobile ad-hoc network," in Recent Trends in Information Technology (ICRTIT), 2013 International Conference on, 2013, pp. 263-269.

[013]. Al-Shurman M, Yoo S-M, Park S, "Black Hole Attack in Mobile AdHoc Networks," 42nd Annual ACM Southeast Regional Confer- ence (ACMSE"42), Huntsville, Alabama, 2-3 April 2004.

[014]. K. Vishnu, A. J. Paul, "Detection and removal of cooperative black/gray hole attack in mobile adhoc networks", IJCA(0975-8887), Vol. 1 No. 22, pp. 38-42, 2010

[015]. Sukla Banerjee, "Detection/Removal of Coperative Black and Gray Hole Attack in Mobile Ad-hoc Networks", Proceedings of the World Congress on Engineering and Computer Science 2008, October 22-24, 2008

[016]. Deepali A. Lokare, A.M Kanthe, Dina Simunic, "Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in MANET", International Journal of Computer Applications (0975- 8887), Volume 88-No.15, pp. 13-22, February 2014

[017]. J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility," IEEE Trans. Electron Devices, vol. ED-11, no. 1, pp. 34–39, Jan. 1959. E. P. Wigner, "Theory of traveling-wave optical laser,"Phys. Rev., vol. 134, pp. A635–A646, Dec. 1965.

[018]. J. K. Author, "Title of report," Abbrev. Name of Co., City of Co., Abbrev. State, Rep. xxx, year.

[019]. E. E. Reber, R. L. Michell, and C. J. Carter, "Oxygen absorption in the earth's atmosphere," Aerospace Corp., LosAngeles, CA, Tech. Rep. TR-0200 (4230-46)-3, Nov. 1988.

[020]. J. H. Davis and J. R. Cogdell, "Calibration program for the 16-foot antenna," Elect. Eng. Res. Lab., Univ. Texas, Austin, Tech. Memo. NGL-006-69-3, Nov. 15, 1987.

[021]. Transmission Systems for Communications, 3rd ed., Western Electric Co., Winston-Salem, NC, 1985, pp. 44–60.

[022]. Motorola Semiconductor Data Manual, Motorola Semiconductor Products Inc., Phoenix, AZ, 1989.