The Effects of Various Wormhole Detection Techniques

Amit Rawat[1], Radhika Manjusha[2]

[1]Student of Master of Computer Engineering, LDRP-ITR, Gandhinagar, India
[2]Assistant Professor, Dept. of Computer Engineering, LDRP-ITR, Gujarat, India

---***---

Abstract - *Mobile ad hoc networks (MANETs) are a set of mobile nodes which are auto-configuring and connected by wireless links automatically as per the defined routing protocol. In this type of network communication is done through multiple hops with dynamic topology. Mobile nodes send and receives data through wireless links, that makes it more vulnerable to various attacks. Wormhole is the most dangerous and most frequently occurred attack in MANET in which one malicious node tunnels the packets from one point of location to other malicious nodes to the other part of node. If the source node takes this fake route, the attacker has the alternative of delivering the packets or dropping them. In this paper we discuss the effect of various detecting and preventing techniques for wormhole attacks.*

***Key Words*: MANET, AODV, NAP, E2IW, HOUND PACKET, DelPHI, Wormhole Attack**

1. INTRODUCTION

In this age of wireless devices, Mobile Ad-hoc Network (MANET) has became an important part to establish communication between mobile devices. Hence, research in the field of Mobile Ad-hoc Network has been growing since last few years. A Mobile Ad hoc Network (MANET) is a cluster of mobile node connected through wireless links. In MANET all nodes are connected with the nodes near in communication range. So if a node wants to communicate to another node it sends the data to the destination node through the neighbour node. Now the neighbour node will act as router like wired network. In wired network security protocols will be implemented in router node, but implementing security in MANET is a challenging task, because here nodes itself will be acting as a router node. So identifying neighbour node as a legitimate node or malicious node is a difficult thing in MANET. As shown in Figure [1] Communication in the network depends upon the trust on each other also communication can work properly if each node co-operates for data transmission. As MANET has no fixed infrastructure, they have more security threats when compared to the infrastructure based wireless networks. Each communication layer has lots of attacks in MANET due to it dynamic nature, lack of centralized monitoring, and limited resources like bandwidth and battery power.

Figure1.1 MANET Model

Security problems in MANETS are:-

1) Open Medium – There is no authentication means in MANET. So eavesdropping is much easier than in wired network.
2) Dynamically Changing Network Topology – Mobile Nodes enters and exists from the network, which allows any malicious node to join the network without being detected.
3) Cooperative Algorithms - The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of Network Security.
4) Lack of Centralized Monitoring - Absence of any centralized infrastructure prohibits any monitoring agent in the system

2. Wormhole Attck

A wireless mobile ad hoc network consists of wireless nodes communicating without the need for a centralized admin. A collection of autonomous nodes that communicate with each other by forming a multiple hop radio network and maintaining connectivity in a decentralized manner is called an ad hoc network. There is not a static infrastructure for the network, such as a coordinator node or an administrator. The idea of such networking is to support robust and efficient operation in mobile wireless networks by the cooperation of the neighbor mobile node. Due to this characteristic of wireless network, they are more vulnerable to attacks. The wormhole attack is the most vulnerable attack to wireless network. During Routing process, at least one intermediate node within the network is encountered. Wormhole attack affects the routing activities with the help of malicious node and Wormhole tunnel. Malicious node is the deceitful node which acts as the part of the network. Malicious nodes downgrade the performance of the network or scrutinize the network traffic. These malicious nodes obtain the end points of the wormhole, which are connected using a high-speed link called as a wormhole tunnel. Figure [1.2] represents the wormhole tunnel which is formed by two malicious nodes S2 and S9. When malicious nodes form a wormhole they can expose or conceal themselves in a routing path.

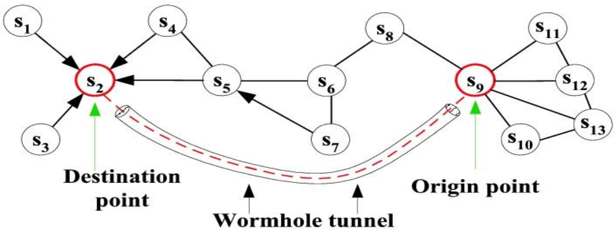

Figure1.2 Wormhole tunnel

There are two types of Wormhole attacks.

[1] Out of band wormhole attack:- In this type of attack only malicious nodes takes participation and none of the nodes are involved from the network. The figure 1.3[a] represents the out off band attack. It is also called as hidden attack

[2] In band wormhole attack:- In this attack malicious node involve the mobile nodes which are the part of a valid network. Figure1.3 [b] represents the in band attack in which all the network node are involved in the wormhole attack. Thus this attack is also called exposed attack.

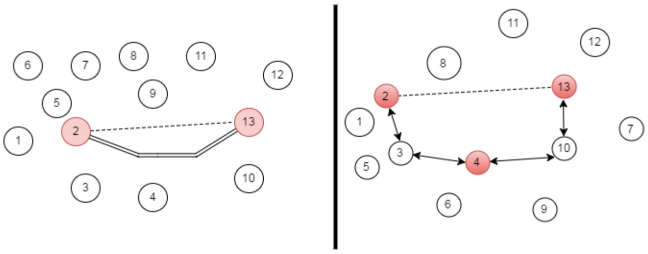

Figure1.3 [a] Out-of-band wormhole, [b] in-band wormhole

3. Detection and Prevention Techniques For Wormhole Attack

1. Neighbor- Probe-Acknowledge (NPA) was a new algorithm proposed Zhou et al[14] by for detection of wormhole attacks. It does not require time synchronization or any other special hardware. Moreover, it accomplishes higher detection rate and lower false alarm rate than the other methods using RTT under different traffic load conditions. From theoretical analysis and comprehensive experiments, wormhole attacks links are easy to identify, standard deviation of *RTT* (*stdev*(*RTT*)) is a more effective metric than per-hop *RTT* to detect wormhole attacks.
2. Energy efficient scheme to immune the wormhole attack (E2IW) is an energy efficient scheme to detect the wormhole proposed by Dhurandher et al[13]. This protocol use the location information of the mobile nodes to find the presence of a wormhole in MANET, and in case a wormhole exists in the path, it discovers alternate routes involving the nodes of the selected path so as to get a more secure route to accomplishment. The protocol is capable of detecting wormhole attacks employing both the hidden and participating malicious nodes. E2SIW finds the wormholes with a high detection ratio, less overheads, and consume less energy in less time. This protocol keep down the overhead related with the control packets.
3. WHOP (Wormhole Attack Detection Protocol using Hound Packet) approach proposed by S. Gupta et al [15] which is based on the AODV protocol and considered to detect wormhole attack with the help of hound packets. In this approach a hound packet is sent after the route has been discovered. This hound packet is processed by all the nodes apart from the nodes which are involved in the path setup process. Essentially the path discovery is done by the help of the two types of packet, called RREQ and RREP. When the sender gets the message, it creates a hound packet and computes its message digest and sign this message digest with its own private key and attached all the information with the hound packet. But processing delay of the packet becomes high.

4. Delay Per Hop Indication (DelPHI) is a method proposed by Hon Sun Chiu and King-Shan Lui[16]. Chiu had identified two types of attack (1) Malicious node does not involve in finding routes (Out of band wormhole attack) and (2) Authorized nodes aware of the existence of malicious nodes (In band wormhole attack). There are different paths to the destination node. Thus, by observing delays per hop the source node is capable of detecting both kinds of wormhole attacks. This method does not require any synchronized clocks or any special hardware for mobile nodes. Advantages of DelPHI are as below:

- DelPHI does not require clock synchronization and position information.
- Some special hardware's are not required in the DelPHI scheme, thus it provides higher power efficiency.

5. Summary of Different Wormhole Detection Techniques

Table -1: Summary of Different Techniques

NO.	Techniques	Method	Comments
1.	Neighbor-Probe-Acknowledge (NPA)[14]	RTT used as measure to detect the wormhole	- Efficient. -No additional hardware support and clock synchronization required.
2.	Energy efficient scheme to immune the wormhole attack (E2IW) [13]	uses the location information of the mobile nodes to find a wormhole	-Capable in detection of hidden and malicious node. -High detection rate.
3.	Wormhole Attack Detection Protocol using Hound Packet [15]	A hound packet is sent after the route discovery process	-Independent of physical medium of wireless network.
4.	Delay Per Hop Indication (DelPHI) [16]	Collects hop count and delay info. of disjoint and calculate the delay/hop value to serve as indicator	-Position information and clock synchronization are not required.

3. CONCLUSIONS

The Mobile Ad Hoc network is greatly influenced by wormhole attack. These attacks degrade the network performance and menace to network security. In this paper various techniques are presented for detection and prevention of wormhole attacks. In future these approaches will help to efficiently remove the malicious nodes from the Mobile Ad Hoc networks. All above techniques based on different factors like cost, need of security, Quality of Service may lead better result but can be costly. So we cannot say that one solution is perfectly deal with all conditions. One factor may have effect on the other factor. Like some networks need more security like whether forecasting and military area may increase the cost. From all above solutions we can find the efficient method to prevent the wormhole attacks by equating all factors.

4. Future Work

On the basis of present scenario and stepwise implementation we came to conclusion that by using DelPHI for MANET we can detect and prevent WORMHOLE attacks. So, I will try to implement an improved approach for WORMHOLE detection mechanism using DelPHI using MANET in terms of future extension of this work.

ACKNOWLEDGEMENT

We would like to express our gratitude towards our Project guide, Prof. Radhika Manjusha for providing me inspiration, encouragement, help and valuable guidance that I needed for the project.

REFERENCES

[1] JG Ponsam, DR Srinivasan, "A Survey on MANET Security Challenges, Attacks and its Countermeasures" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) ,pp. Volume 3, Issue 1, January – February 2014.

[2] Nishu Garg and R.P.Mahapatra, "MANET Security Issues", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[3] Sudhir Agrawal, Sanjeev Jain and Sanjeev Sharma,"A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks" JOURNAL OF COMPUTING, VOLUME 3, ISSUE 1, JANUARY 2011.

[4] Mamatha. T "Network Security for MANETS", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012.R.

[5] Kayarkar, Harshavardhan. "A survey on security issues in ad hoc routing protocols and their mitigation techniques." *arXiv preprint arXiv:1203.3729*(2012).

[6] Djenouri, Djamel, L. Khelladi, and N. Badache. "A survey of security issues in mobile ad hoc networks." *IEEE communications surveys* 7.4 (2005): 2-28.

[7] Kadam, Aakanksha, Niravkumar Patel, and Vaishali Gaikwad. "Detection and Prevention of Wormhole attack in MANET." (2016).

[8] Maulik, Reshmi, and Nabendu Chaki. "A comprehensive review on wormhole attacks in MANET." Computer Information Systems and Industrial Management Applications (CISIM), 2010 International Conference on. IEEE,2010.

[9] Sadeghi, Mohammad, and Saadiah Yahya. "Analysis of Wormhole attack on MANETs using different MANET routing protocols." *2012 Fourth International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 2012.

[10] Sahib, Fatehgarh. "Detection and Prevention Techniques for Wormhole Attacks".

[11] Zhou, Jie, et al. "Analysis and countermeasure for wormhole attacks in wireless mesh networks on a real testbed." *2012 IEEE 26th International Conference on Advanced Information Networking and Applications*. IEEE, 2012.

[12] Gupta, Saurabh, Subrat Kar, and S. Dharmaraja. "WHOP: Wormhole attack detection protocol using hound packet." *Innovations in information technology (IIT), 2011 international conference on*. IEEE, 2011.

[13] Chiu, Hon Sun, and King-Shan Lui. "DelPHI: wormhole detection mechanism for ad hoc wireless networks." *2006 1st International Symposium on Wireless Pervasive Computing*. IEEE, 2006.