International Journal of Computer Applications Technology and Research
Volume 4– Issue 5, 377 - 379, 2015, ISSN:- 2319–8656

A Survey on Different Modes of Wormhole Attack and it's Countermeasures in MANET

Shahapur Farhat Kauser Iqbal
Dept of CSE
SECAB Engineering College
Bijapur, India

Syeda Sheema
Dept of CSE
SECAB Engineering College
Bijapur, India

Asha Guddadavar
Dept of CSE
SECAB Engineering College
Bijapur, India

Abstract: One of the most popular areas of research is wireless communication. Mobile Ad Hoc network (MANET) is a network with wireless mobile nodes, infrastructure less and self organizing. With its wireless and distributed nature it is exposed to several security threats. One of the threats in MANET is the wormhole attack. In this attack a pair of attacker forms a virtual link thereby recording and replaying the wireless transmission. This paper presents types of wormhole attack and also includes different technique for detecting wormhole attack in MANET..

Keywords: Mobile Ad Hoc Network; Packet encapsulation; Out of Band; Security; Wormhole

1. INTRODUCTION

Mobile devices for example laptops mobile, PDA's and many other are increasingly becoming common, making wireless technology popular. With the wireless technology users are provided with the ease to move freely while they are connected to a network. Wireless network can be classified as infrastructure based and Ad Hoc network. Infrastructure based requires a central access point or base station for communication. Ad Hoc in Latin means "for this" or "for this purpose only". This Ad Hoc network can be set up without the need for any external infrastructure (like central access point or a base station

Since the devices are mobile that's why the term "Mobile Ad Hoc network MANET)". Mobile Ah Hoc network consist of independent mobile nodes and communication between them is done via radio waves [1]. If the nodes are within the radio range of each other then they communicate directly else need intermediate node for routing the packets. Hence it is also called multihop network. Here Figure1 shows example of MANET where there is no central access point or base station is required for communication. Each node can communicate directly with the node which lies within its radio range.

There are many application of MANET. Some of the applications of MANET include disaster relief operations, military or police operations, business meetings, site operations (such as mines), Robot data acquisition.

Few characteristic of MANET can be summarized as follows:

- Communication is done via wireless means.
- Nodes act as both host as well as routers.
- No centralized access point or base station is needed.
- Network topology is dynamic and multihop.
- Set up can be done anywhere
- Limited security.
- No infrastructure required.

Due to the open and dynamically changing network topology, MANET is much more susceptible to attack then wired network.

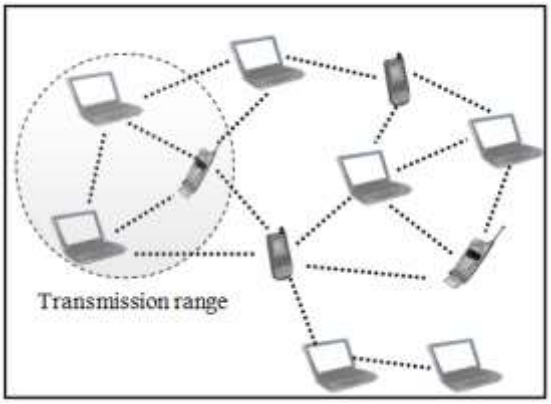

Figure 1. Example of MANET consisting of mobile nodes

2. WORMHOLE ATTACK

Wormhole attack is one of the severe attacks on MANET. In wormhole attack wormhole nodes are introduced which form a virtual link and make other nodes belief that there is a route between them and make all communication to go through this link. In the first phase the wormhole node will broadcast about the false route. In the second phase the attacker can do whatever they want to with the data passing through this link [2], [3].

3. DIFFERENT MODES OF WORMHOLE ATTACK

Wormhole attack is particularly severe against routing protocol such as DSR [11] and AODV [12]. In such routing protocol if a node, say S needs to discover route to destination, say D, then S floods the network with rote request

message. The node that receives the request packet processes the packet, adds its own identity and rebroadcast it. In order to limit the amount of flooding each node only broadcast the first packet it receives and drops further copies of same request. When destination node D receives the request it generates a route reply and sends back to S. The sender node then selects the best route from all the route reply it has received. Best route is selected on basis of shortest route. In case of wormhole attack the node at one end hears the route request and tunnels it to the wormhole node at the other end of tunnel. The wormhole nodes give false illusion that the route passing through them is the shortest, even though they are not.

Wormhole can be classified into four modes-packet encapsulation, packet relay, high power transmission and out-of-B-band [13].

3.1 Packet Encapsulation

In packet encapsulation the wormhole node on one end encapsulates the packet to prevent nodes on the way from incrementing node count. When the wormhole node at the other end receives this packet it will bring the packet to its original form. Figure 2 below shows an example of packet encapsulation where node C and node J are wormhole nodes.

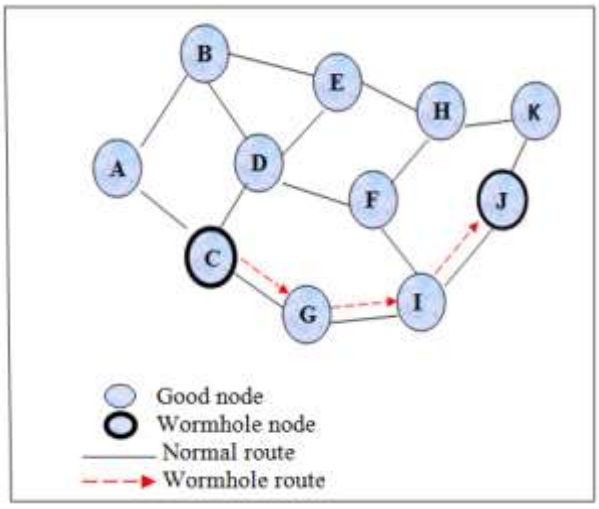

Figure 2. Example of packet encapsulation in wormhole attack

3.2 Packet Relay

In this type of attack two malicious nodes relay the packets between them which are far apar but make illution of being neighbor.

3.3 High Power Transmission

In this kind of attack there exist only one malicious node which has high transmission power used to attract packets to pass through it.

3.4 Out Of Band

In Out-of-band wormhole attack the attacked node form an external link between the two nodes to form a tunnel. The wormhole node then advertises about the shortest path and makes all the communication pass through it. This can be further classified as High power transmission. In high power transmission the attacked node has much higher capability that lures other nodes to send packets to go through this path.

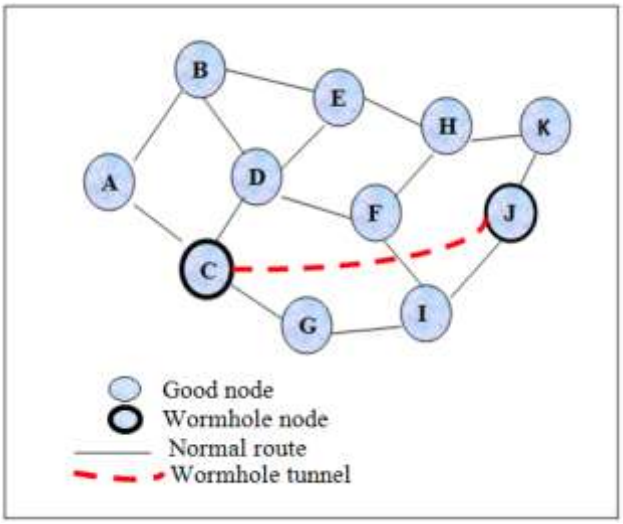

Figure 3. Out-Of-Band Wormhole Attack

Here figure 3 shows Out-Of-Band wormhole attack in which node C and node J forms an external link or in other words a tunnel through which all communication can be captured. The wormhole node will advertise that there is a shortest path between node C and node J and make all communication go through this link.

4. DIFFERENT DETECTION METHODS

Several researchers have worked on detection of wormhole attack in MANET. Some of the detection methods discussed in next section.

4.1 Hop Count Analysis Method

Shang, Laih and Kau[4] introduced a method called hop count analysis for detection of wormhole. This method does not really identify the wormhole but simply avoids the route that is suspected to have wormhole and selects a different route. The author introduced a multipath routing protocol that is based on hop count analysis method. The idea is to use split multipath route and so the data is also split. With this the attacker cannot completely seize the data.

4.2 Location Based Approach

Location based approach is useful where the location of neighboring nodes and transmission range are known. In this technique the nodes share their location information with each other. Author of [5] proposed a special method called the geographical leash to detect wormhole. A leash is some information which is attached to a packet designed to control the maximum allowed transmission distance. This geographic leash ensures that the receiver of the packet is within the range of sender. Initially all nodes know their own location. The node while sending a packet includes time when the packet was sent, time when packet was received and its

location. The recipient node now compares this information with its own location and time when the packet was received.

In location based approach special hardware is used. Location based is equipped with either GPS or some positioning technology. This technology fails in the absence of GPS system.

4.3 Time Based Approach

Time pased approach proposed by Hu et al [5][6] is based on accurate time measurement. This technique requires the nodes to maintain tightly synchonized clock. The author has proposed a technique called temporal leash. In this method extremly accurate clock synchonization is needed to bound propogation time of packet. In [7], the author has proposed a methode called transmission time based mechanism(TTM). Thia method detects wormhole during early stage of route set up by calculating the time of transmission between two successive nodes. If the transmission time betweenn two nodes is high then wormhole is detected. It doesa not require any special harware like GPS system.

4.4 Digital Signature Based Approach

In **[**8**]** author has proposed a method using digital signature. All nodes in network contains digital signature of every other nodes in the same network. A trusted path is created between the sender and the receiver using digital signature. If a node does not have legal digital signature, it is identified a malicious node.

4.4 Neighbor Node Monitoring

Author of [9] has proposed a method based on a response time of reply message. This response time is used for authentication purpose. All nodes maintain table for storing the reply time. If the reply time is not accurate then there is a malicious node in the network. Comparison is done on response time and repeated until destination is reached.

4.5 Round Trip Time Based Approach

The Round Trip Time (RTT) based approach proposed by Zaw Tun and Thein [10] considers the round trip time (RTT) between two successive nodes. Based on transmission time between two nodes wormhole is detected. Here the transmission time between two false nodes is considered to be higher than others. This technique does not require any kind of special hardware for its detection process.

5. CONCLUSION

Due to the open nature and dynamic network topology of MANET, it is much more vulnerable to attacks. This paper discusses a particularly severe attack that is the wormhole attack and its different types in detail. Wormhole attack has different modes through which it can capture and disrupt the packets. It can either hide the route information by packet encapsulation or form a tunnel between the attacked nodes to pass all packets through this tunnel. Various countermeasures are also discussed here which are used to detect the wormhole attack in MANET.

6. REFERENCES

[1] C. Siva Ram Murthy and B.S.Manoj, “Ad hoc Wireless Networks” (Chapter 7), 2014.

[2] Jyoti Thalor, Ms. Monika “Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review”, International Journal of Advanced Research in Computer Science and Software Engineering - Volume 3, Issue 2, February 2013.

[3] Reshmi Maulik and Nanbendu Chaki: “A Study on Wormhole Attacks in MANET” International Journal of Computer Information System and Industrial Management Applications (IJCISIM),Vol.3 (2011), pp. 271-279.

[4] Jen S.-M.; Laih C.-S.; Kuo W.-C. A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET. *Sensors*. 2009.

[5] Yih-Chun Hu, Adrian Perig, David B. Johnson: “Wormhole Attack on Wireless Network” IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Vol. 24- No 2, 2006.

[6] Y.C.Hu, A.Perrig and D.Johnson: “Packet leashes: a defense against wormhole attacks in wireless networks,” in INFOCOM, 2003.

[7] Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Sungyoung Lee and Heejo Lee: “TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks” IEEE CCNC, 2007.

[8] Pallavi Sharma, Prof. Aditya Trivedi, "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature”, *IEEE*, 2011.

[9] sweety goyai, harish rohil, “Securing MANET against Wormhole Attacl using Neighbour Node Analysis” *IJCA* volume 81,November 2013.

[10] Zaw Tun and Ni Lar Thein “Round Trip Time Based Wormhole Attack Detection” ICCA 2009

[11] D. Johnson, D. Maltz, and J. Broch, The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks, in Ad Hoc Networking, Addison-Wesley, 2001.

[12] C. E. Perkins and E. M. Royer, Ad-Hoc On-Demand Distance Vector Routing, in Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’99), pp. 90-100, February 1990.

[13] Himanshu Prajapati “Techniques for Detection & Avoidance of Wormhole Attack in Wireless Ad Hoc Networks” Vol. 3 Issue 3, March-2014, pp: (21-27)