A Review on Detection of Wormhole Attack in Mobile Ad-hoc Networks

[1]Jayrajsinh K. Jadeja, [2]Naren Tada
[1]ME Scholar, [2]Assistant Professor
Computer Engineering Department
V.V.P. Engineering College, Rajkot, Gujarat, India, Gujarat Technological University (GTU)
[1]jayrajsinh.jadeja90@gmail.com, [2]naren.tada@gmail.com

Abstract— **The ad-hoc networks are the temporarily established wireless networks which do not require fixed Infrastructure. It is also called as Infrastructure less network. Each mobile node functions as base station and as router forwarding packets for other mobile nodes in network. Among all attacks wormhole attack is most dangerous attack. In this attack an attacker capture the packets at one node in the network and send it to the another attacker node at a distant location through tunnels which is established through different ways like packet encapsulation, using high power transmission or by using direct antennas. Wormhole attack is so strong and detection of this attack is hard. Also, the wormhole attack may cause another type of attacks like Sinkhole or Select forwarding. Using a cryptographic technique is not enough to prevent wormhole attack. In this paper we are going to review some methods in wormhole detection and investigate the weaknesses and strengths of the methods.**

Index Terms— **Wormhole Detection Techniques, Intrusion Detection, Wormhole attack, Mobile Ad-Hoc Networks**

I. Introduction

“Ad-hoc” is a Latin term that means “for this purpose”. This kind of network often used to define solutions that are expanded on-the-fly for a specific aim. Ad-hoc Networks are autonomous and decentralized wireless systems. The nodes in Ad-hoc can be consisting of the systems or devices i.e. Mobile phone, laptop, Personal Digital Assistance (PDA), and a personal computer that is participating in the network. These nodes can act as host/router or both at the same time. Dynamic topology is the most important characteristics of Ad-hoc network caused by this nodes feature, flexibility and self-configuration feature also provided by this kind of behavior. By this ability, Ad hoc network topology can be deployed urgently without any infrastructure.

Ad-Hoc networks are so flexible and every kind of communication between two and more nodes can be applied on it. For example if you want to send a file to your laptop friends, you can create a single session by an Ad-hoc network between your computer and your laptop’s friend to transmit the file. This work may be done using network cable or the wireless card to link with each other. If you need to transmit or share files with more than one workstation, you can launch a multi-hop ad hoc network, which could carry data over multiple nodes. Ad hoc network is a provisional network connection established for a specific object, such as sending data from one node to another node or one computer to one another.

Wireless Ad-hoc networks are involved three sub networks. Figure 1 shows the classification of wireless ad hoc network.

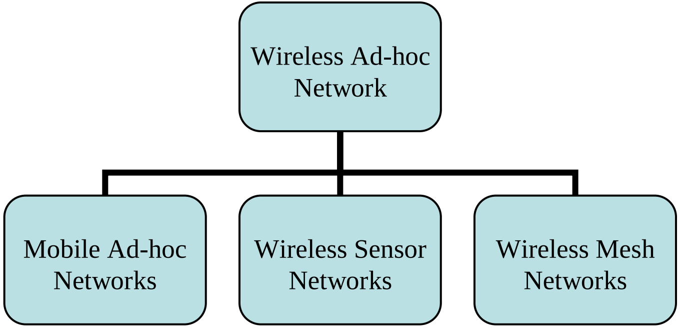

Figure 1 Classification of Wireless Ad-hoc networks

Mobile ad hoc networks (MANET) is the first category which are consist of some auto configuring nodes that can move freely and utilize wireless equipment to communicate with each other. These kinds of network do not need a concentrate entity and are infrastructure-less. MANET can be a standard Wi-Fi connection, like a cellular or satellite broadcast. Some MANETs are limited to a local area of wireless system, such as a group of laptops.

Wireless sensor network (WSN) is the second category. WSNs were firstly designed to facilitate military operations but today it's used for monitoring and recording the physical conditions of the environment and organizing, such as health, pollution levels, humidity, wind speed and direction, traffic, and many other consumer and industrial areas of collecting data at a central location.

The third category is Wireless Mesh Network (WMN). Mesh network made up through the link of wireless access points, which set at each local user's network. Every network user provides and forward data to the next node. Wireless mesh networking can let people living in faraway areas to connect their networks together for reasonable Internet links. Wireless mesh networks often involve gateways, mesh clients and mesh routers. In mesh network clients are often cell phone, laptops and other wireless devices, while the mesh network sends traffic to and from the gateways, do not need to connect to the internet.

Wireless sensor nodes usually suffered from some limitation such as low power radios, short lifetime and limited memory; also the most secure algorithms that proposed for this issue are not perfect. Generally, wireless sensor nodes are developed in an untrusted environment. For this reason security becomes one of the most important major in these small devices. Because of WSN limitation, providing the secure communication in an unreliable environment still is in challenging factor. Node characteristics, dynamic topology without central monitoring system, provided different security threat on WSN routing protocol. Between all attacks, the wormhole is more dangerous than the other attack such as Sinkhole, Sybil attack, Selective forwarding attack, etc. because this type of attack does not need to compromise a sensor in the network and it can create the other type of attack easily.

II. Wormhole Attack

A wormhole is a kind of attack that typically happens with two or more malicious nodes in which the first malicious node eavesdrop or listen in packets at one location and then send them by tunnel to second malicious node in another area. Transferring the packets between these attackers can be done by using direct tunnel in wire/ wireless connection.

For example in Fig. 2 X and Y are two different areas which are out of the wireless communication link. Due to the wormhole link between the two nodes A and B, the nodes *d,e,f* will be one-hop neighbours to *a,b,c* respectively. The attacker at one end records the incoming traffic and tunnels them to the other end. If routing control messages like RREQ are tunneled, this will lead to distorted routing tables in the network. If a fast transmission path exists between the two ends of the wormhole, they may tunnel the data faster than the normal mode of wireless multihop communication. Thus, they attract more traffic from their neighbours. This is termed as rushing attack. These wormholes by themselves are harmless. But, in many circumstances they act as the first stage attackers wherein they indulge themselves in denial-of-service attacks in their second stage. This can compromise the security of

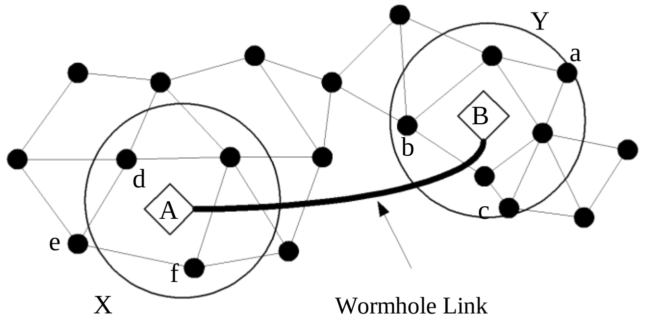

Figure 2 Wommhole Attack

The entire network. In the absence of security mechanisms, the existing routing protocols may not be able to find a legitimate path to forward their data resulting in isolation of a single or a set of mobile nodes. Hence, a reliable and efficient defense mechanism is required to detect the wormholes in an ad hoc network.

One of the main classifications of wireless networks that are usually vulnerable against wormhole attack is wireless ad hoc network in which the malicious nodes prevent to discover any routes to destination except through the wormhole. Therefore, in recent years, a wormhole attack attracts more consideration and some studies are performed on this issue. Detection of wormholes is difficult because the packets are transmitted by the malicious nodes to a far location from the received point by utilizing just a single hop out-of-band channel. This channel cannot be listened to by the network. Also, when this attack combine with the other attacks like selective forwarding, it becomes more dangerous for security of the network. It is important to mention that wormhole can cause to create Sybil and sinkhole attack. The common method for wormhole mitigation can be handed out in two main diversity; end to end detection by considering in extra devices on nodes as well as GPS (Geographic Position System), direct antenna and those methods which submitted on specific reading protocol. In the following some defense methods against wormhole attack are reviewed.

III. Wormhole Detection Methods

A. Distance & location Based: Packet Leash Technique

Numerous methods were proposed using a packet leash technique for the detection of the wormhole attack. The packet leash (Yih-Chun Hu et.al, 2003) is the method that defends against the wormhole attack. The leashes can be combined either into geographical or temporal. In geographical leashes, all nodes should have knowledge of its own location in the network and secure synchronized clock. Whenever a sender sends the data packet to receiver, it includes transmission time and its own recent location in header. Therefore, the receiver is capable of assuming the neighbour relation by calculating the distance between itself and source. In temporal leashes, all nodes calculate the expiration time of each packet by using light's velocity and append this expiration time in the packet's header. Destination compares its own arrival time and expiration time in the packet to detect the wormhole attack. Geographical leashes are more advantageous than temporal leashes as they do not require a tightly synchronized clock. It has the limitations of GPS technology.

B. Special Hardware Based Approaches

The Secure Tracking of Node Encounters in Multi-hop Wireless Networks (SECTOR) is a wormhole detection technique that does not depend on time synchronization (Srdjan Capkun et.al, 2003) [3]. In this SECTOR method we uses Mutual Authentication with Distance-bounding (MAD) protocol for the estimation of distance between 2 nodes or users. MAD operates in the assumption that every node is appended with transceiver as extra Hardware. It accepts a single bit, carry out 2 bit XOR process over it and broadcast it which is shown in Fig 3.

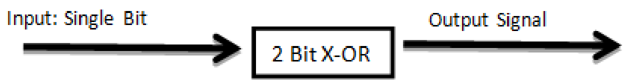

Figure 3 Processes in Transceiver

Directional antenna detects the existence of wormhole nodes (Lingxuan Hu and David Evans, 2004). In this method, directional information is shared between source and destination. The destination can detect the wormhole by comparing the received signal from the malicious nodes and directional information from the source. If the both the signals from the source and intermediate nodes are different, then the wormhole link is detected.

C. Localized Encryption and Authentication Protocol (LEAP)

Localized Encryption and Authentication Protocol (LEAP) is a method which is suggested by Zhu[4]. This model is based on clustering and it requires defining 4 type key for each sensor node such as,

a. Individual key that is shared with the base Station.
b. Pair wise key that is shared with another sensor node.
c. Cluster key that is shared with multiple neighbouring nodes.
d. Group key is shared by all the nodes in the network.

This method is implemented for static or immobile sensor networks.

D. Topological Technique

Normally, a wireless multi hop network is deployed on the surface of a geometric environment, such as a plane or a rough terrain [5]. In this method we develop principles in continuous domain, assuming continuous deployment of nodes over the geometric surface with one-to-one mapping to the points on the surface to detect wormhole nodes. A new topology space is formed after the wormhole is glued on the original surface. We subsequently analyse how the different topology spaces are generated after gluing different types of wormholes. We classify wormholes into four categories, according to their topological impacts. Fig. 4 shows the four types of wormholes.

- Class I wormhole, both of its two endpoints locate inside the surface (Fig. 4(a)).
- Class II wormhole has one endpoint inside the surface and the other on the boundary of the surface (Fig. 4(a)).
- Class III wormhole has its endpoints on two different boundaries (Fig. 4(b)).
- Class IV wormhole has both of its endpoints on the same boundary (Fig. 4(c)).

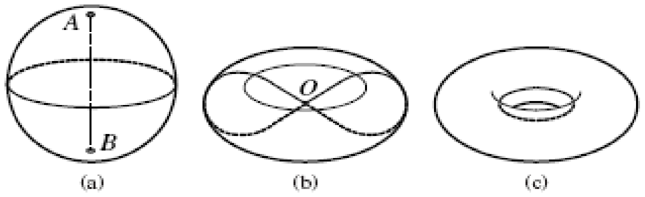

Figure 4 Classification of wormholes effect on topology

The four types of wormholes have different topological impacts on the original surface, and the complex wormhole attack can be considered as a finite combination of them. Base on their effect on topology we can detect wormhole in the topology.

E. Multipath Hop-count Analysis Technique

This model is developed by Jen which is called Multipath Hop count Analysis to prevent wormhole attack for MANETs. MHA is a method based on hop-count analysis in order to avoid this attack in MANETs from the standpoint of users without any special environment assumptions [6]. In the MHA method first, the hop-count values of all routes are calculated and in the next step, a safe set of routes are chosen for data transmission. Ultimately, the packet is transmitted to destination through the safe routes due to decreasing the rate of packet that is sent by wormhole. One of the features of this method is that it does not require any specific hardware to well-done. It utilizes control packets as in RFC3561 and tries to modify it. Therefore, it used the RREQ packet is used for route discovery and the RREP packet is used for route.

F. Watchdog Technique

To identifies misbehaving nodes and avoids routing through theses nodes, watchdog and pathrater. In this technique, watchdog identifies misbehaviour of nodes by copying packets and maintained a buffer for recently sent packets. The overheard packet is compared with the sent packet, if there is a match then discards that packet. If the packet is timeout, increment the failure tally for the node. And if the tally exceeds the thresholds, then node will misbehave. The implementation of watchdog technique is shown in Fig. 4.

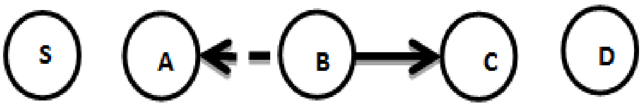

Figure 4 Watchdog Implementation

In this Fig. 4, it is assumed that bidirectional communication symmetry on every link between nodes that want to communicate. If a node can receive a message from a node at time, then node could instead have received a message from node at the time will implement the watchdog. It maintain a buffer of recently sent packets and compares each overheard packet with the packet in the buffer, when forwards a packet from to with the help of , can overhear transmission and capable of verifying that has attempted to pass the packet towards . But this approach has some limitations and it is not detect the misbehaving node during ambiguous collisions, receiver collisions, false misbehavior and collusion. The approach is used directional antenna to detect and prevent the wormhole attack. The technique is assumed that nodes maintain accurate sets of their neighbours. So, an attacker cannot execute a wormhole attack if the wormhole transmitter is recognized as a false neighbour and its messages are ignored.

G. DelPHI Technique

DelPHI provides a solution to the exposed wormhole attacks[7]. In this mechanism, delay per hop is determined in every path and it is proved that delay per hop for the genuine path is shorter than the wormhole path. If the path has noticeably high delay per hop, then the corresponding path is affected by wormhole.

H. Wormhole Geographic Distributed Detection

An algorithm for the distributed detection of wormhole attack is provided by Yurong Xu in 2007 called wormhole geographic distributed detection (WGDD). WGDD algorithm detects the wormhole attack based on the damage caused by them and the parameter used for wormhole detection is hop count. According to the hop count measured, it reconstructs the mapping details in each node and finally it exploits diameter feature to detect distortions caused by malicious nodes. WGDD algorithm is effective in finding the exact location of the wormholes.

I. TrueLink: A Time Base Mechanism.

TrueLink developed by Jakob Eriksson in 2006 is a wormhole detection technique [9] that depends on time based mechanisms. TrueLink verifies whether there is a direct link for a node to its adjacent neighbour. Wormhole detection using TrueLink involves 2 phases namely rendezvous and validation. The first phase is performed with firm timing factors in which nonce exchange between two nodes takes place. In the second phase, both the nodes authenticate each other to prove that they are the originator of corresponding nonce. The major disadvantage is that TrueLink works only on IEEE 802.11 devices that are backward compatible with a firmware update. A round trip time (RTT) approach is emerged to overcome the problems in using additional hardware. The RTT is the time taken for a source node to send RREQ and receive RREP from destination. A node must calculate the RTT between itself and its neighbouring nodes. The malicious nodes have higher RTT value than other nodes. In this way, the source can identify its genuine and misbehaving neighbours. This detection technique is efficient only in the case of hidden attacks.

J. Secure Neighbour Discovery and Monitoring Based Approach

This is provided by Issa Khalil in 2008 [10] which uses local observation schemes to prevent malevolent nodes in the vicinity. The position of each node in the network is traced by central authority and it is capable of even isolating the malicious nodes globally. The detection rate of this method decreases as the network mobility increases.

IV. Summary Of Various Wormhole Detection Methods

In the following Table 1 [11], contains all wormhole detection methods that are explained previously and also contains the requirements of each method.

Table 1: Qualitative Comparison of Wormhole Detection Method

Method	Localization Information	Checking the Authentication	Hop Count Analysis	Others
Distance and location Based: Packet Leash Technique.	Yes	Geographical Leashes: RSA Temporal Leashes: TIK Protocol based on TESLA	N/A	Loosely Synchronized clocks
Special Hardware Based Approaches	N/A	Mutual Authentication with Distance-bounding (MAD)	N/A	Transceiver, Directional Antenna

		protocol		
Localized Encryption and Authentication Protocol (LEAP)	N/A	Four Type Keys	N/A	N/A
Topological Technique	Yes	N/A	N/A	Topology of Network Information
Multipath Hop-count Technique	N/A	N/A	Yes	N/A
Watchdog Technique	N/A	N/A	N/A	Maintains Buffer
DelPHI Technique	N/A	N/A	Yes	N/A
Wormhole Geographic Distributed Detection	Yes	N/A	Yes	Local Map
TrueLink : A Time Base Mechanism.	N/A	Yes	N/A	Synchronized Clocks
Secure Neighbour Discovery and Monitoring Based Approach	N/A	N/A	N/A	Central Authority

V. Conclusion

In this paper, we reviewed the various detection mechanisms against wormhole attacks in wireless Ad- hoc networks. Along with the explanation of these methods we had done qualitative comparison of all the wormhole detection techniques in Table 1. Overall, a significant amount of work has been done on solving wormhole attack problem. We can't say one solution is applicable to all situations. So there is choice of solutions available based on cost, need of security, type of network. Implementing more hardware for increasing security may lead better result, but can be costly, which may affect other networks need.

References

[1] Fonseca, R., & Merino, A. S. (2004). Receiver Based Forwarding: Improving the security of Geographic Routing in Wireless Sensor Networks. Berkeley: Berkeley University.

[2] Loo, C., Ng, M., Leckie, C., &Palaniswami, M. (2006).Intrusion Detection for Routing Attacks in Sensor Networks.International Journal of Distributed Sensor Networks, pp.313–332.

[3] SrdjanCapkun, LeventeButtyan and Jean-Pierre Hubaux, 2003 "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks" *SASN'03 Proceedings of 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 21-32.

[4] Zhu, S., Setia, S., &Jajodia, S. (2003). LEAP: efficient security mechanisms for large-scale distributed sensor networks. *Proceedings of the 10th ACM conference on Computer and communications security (pp. 62 - 72). New York: ACM.*

[5] MajidKhabbazian, Hugues Mercier, and Vijay K. Bhargava, 2009 "Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks" *IEEE Transactions on Wireless Communications, Volume 8*, Issue 2, pp. 736-744.

[6] Jen, S.-M., Laih, C.-S., & Kuo, W.-C. (2009). A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET. sensors, 5022-5039.

[7] Chiu, HS; Wong Lui, KS, 2006 "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks" *1st International Symposium on Wireless Pervasive Computing.*

[8] Sanaei, Mojtaba Ghanaatpisheh, et al. "An Overview on Wormhole Attack Detection in Ad-hoc Networks." *Journal of Theoretical and Applied Information Technology* 52.3 (2013).

[9] Jakob Eriksson, Srikanth V. Krishnamurthy, and MichalisFaloutsos, 2006 "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks" *14th IEEE International Conference on Network Protocols*, pp. 75-84

[10] Issa Khalil, Saurabh Bagchi, and Ness B. Shroff, 2008 "MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks" A*d Hoc Networks*, Volume 6, Issue 3, pp. 344-362

[11] Ankita Gupta , Sanjay Prakash Ranga,2012 "WORMHOLE DETECTION METHODS IN MANET" *Internal Journal of Enterprise computing and Business System.*

[12] T. Sakthivel, R. M. Chandrasekaran, 2012 "Detection and Prevention of Wormhole Attacks in MANETs using Path Tracing Approach" *European Journal of Scientific Research ISSN 1450-216X Vol.76 No.2 (2012)*, pp.240-252

[13] Yashpalsinh Gohil, Sumegha, Sumitra. "A Review On: Detection and Prevention of Wormhole Attacks in MANET." International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013