A Comparative Analysis of Detection and Prevention of Wormhole Attacks in Mobile Ad-hoc Networks

Sushant S. Bahekar[1], Prashant Panse[2]

[1]M. Tech Student, Departemnt of Computer Engineering, SVCE, Indore, India

[2]Guide & HOD, Department of Information Technology, SVCE, Indore, India

Abstract: ***In day to day life the Computer Networks Becomes more popular especially Mobile Ad hoc Networks. Its applicability and popularity attracts some miss users for malfunctioning and disturbing the network traffic. The ad-hoc networks are the temporarily established wireless networks for doing specific task, which do not require fixed Infrastructure. Each mobile node functions as base station and as router forwarding packets for other mobile nodes in network. There are various types of attacks in Mobile networks but 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. By Using a cryptographic technique is not enough to prevent wormhole attack. In this paper we are going to Comparative Analysis of Detection and prevention techniques of Wormhole attacks trying to find out their pros and cons.***

Keywords: Network Security, Tunnels, Packet Encapsulation, Sinkhole, Select forwarding

1. Introduction

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 friend's laptop, you can create a single session by an Ad-hoc network between your computer and your friend's laptop to transmit the file. 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. Following fig. shows the classification of wireless ad hoc network.

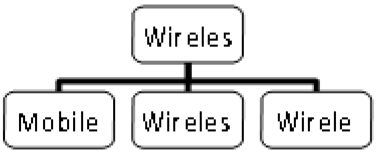


Figure 1: Types of Wireless Network

MANET: Mobile ad hoc network is the first categories 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 don't infrastructure. 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.

WSN: Wireless sensor network 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. Humidity, wind speed and direction, traffic and other industrial areas.

WMN: The third category is Wireless Mesh Network. 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 sensor networks have some limitation such as low power radios, short lifetime and limited memory and 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.

2. Wormhole Attack and Classification

Before discussing wormhole attack, first we try to understand types of attacks in Mobile Ad-hoc Networks. Following fig. shows the classification of Wireless Mobile Ad-hoc network attacks.

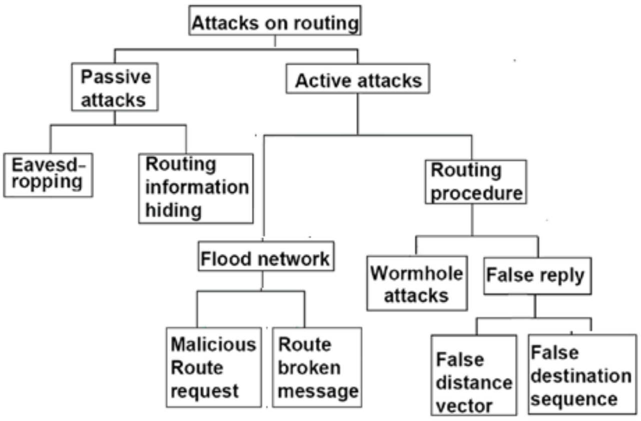
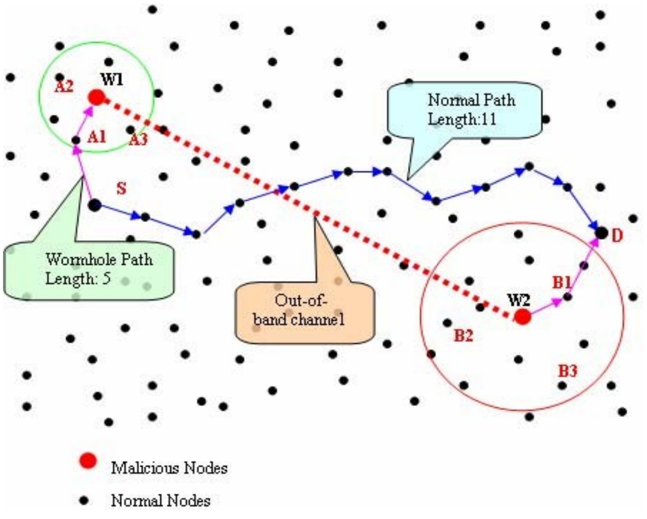


Figure 2: Classification of Wireless Mobile Adhoc network attacks

We can think of wormhole attack as a 2-phase process launched by one or several malicious nodes. In the first phase, these malicious nodes, called wormhole nodes, try to lure legitimate nodes to send data to other nodes via them. In the second phase, wormhole nodes could exploit the data in variety of ways such as trying to break the encryption key, modifying packets or simply dropping packets selectively to make some legitimate nodes unable to communicate with each others.

How to lure legitimate nodes to send data via wormhole nodes? This work can be done in many ways [1]. In the simplest case, wormhole attacks include two malicious nodes which are able to communicate directly with each other from far distance via an out-of-band channel. One node will overhear packets at its location and tunnel them to the second node which in turn replays tunneled packets into the network at its location. Because two wormhole nodes can communicate with each other directly from far distance so packets sent via wormhole link will be faster than those sent via normal nodes and paths containing the wormhole link are likely shorter than normal paths. Therefore, more nodes will send their data via wormhole nodes.



For example, in above fig, the path from S to D via wormhole link (W1, W2) has the length of 5 when the normal path has the length of 11. Therefore, in most routing protocols, S prefers sending data to D along the path with wormhole link.

However, the above method is difficult to deploy because it requires some special hardware to create an out-of-band channel. Another technique using encapsulation is more popular to launch wormhole attacks. Instead of using an out-of- band channel, the malicious node W1 encapsulates packets it overhears and sends them to the second malicious node W2 through the path exists between them. W2 decapsulates, gets the original packets and rebroadcasts them again. By this way, W2 seems to get the packet directly from W1 with the same hop count although they are several hops far from each other.

Wormhole attack is serious to ad-hoc networks because it is easy to launch. The nature of wireless communication is broadcasting so wormhole nodes do not have to authenticate or communicate with legitimate nodes. They just overhear packets; tunnel them to the other node and replay into the network without any modifying or creating packets. So no encryption or authentication mechanism can protect Ad-hoc networks from wormhole attacks.

There are several ways to classify wormhole attacks. Here we divide wormhole attacks into 2 categories: hidden attacks & exposed attacks, depending on whether wormhole nodes put their identity into packets' headers when tunneling & replaying packets [2].

A. Hidden Attacks

Before a node forwards a packet, it must update the packet by putting their identity (MAC address) into the packet's header to allow receivers know where the packet directly comes from. However, in hidden attacks, wormhole nodes do not update packets' headers as they should so other nodes do not realize the existence of them. As showed in figure 1, a packet P sent by node S is overheard by node W1. W1 transmits that packet to node W2 which in turn replay the packet into the network. Because W1 & W2 do not change thepacket header so D seems to get the packet directly from S. In this way, D& S are neighbors although they are out of radio range from each other (fake neighbors). General speaking, in hidden attacks nodes within W1's vicinity are "fake neighbors" of nodes within W2's vicinity and vice versa.

In this kind of attack, a path from S to D via wormhole link will be:

S → A1 → B1 → D

In the viewpoint of legitimate nodes, there is no existence of W1 & W2 in the path (hidden).

B. Exposed Attacks

In exposed attacks, wormhole nodes do not modify the content of packets but they include their identities in the packet header as legitimate nodes do. Therefore, other nodes are aware of wormhole nodes' existence but they do not know wormhole nodes are malicious. In case of exposed attacks, the path from S to D via wormhole will be:

S → A1 → W1 → W2 → B1 → D

In hidden attacks, there are many fake neighbors created by wormhole link but there's no fake neighbor except (W1, W2) in this case. This difference leads to differences in detection mechanisms. Some mechanisms which can do well in detecting hidden attacks cannot detect exposed attacks and vice versa.

3. Various Wormhole Detection Methods

Some work has been done to detect wormhole in Ad Hoc networks. Most of them based on the fact that transmission time between two wormhole nodes or between two fake neighbors is much longer than that between two real neighbors which are close together. Because two wormhole nodes (or two fake neighbors) are far from each other and packets sent between two wormhole nodes maybe go through several intermediate nodes so it takes a longer time to transmit a packet between two wormhole nodes (or two fake neighbors) than between two real neighbors which are close together. By detecting this difference, we can identify wormhole attacks.

1) Packet Leashesh

One of the first proposals for detecting wormhole is packet leashes [3][4]. Every time a node, say A, sends a packet to another node, say B, A has to put a time stamp (sending time) (temporal packet leashes) or the location of A and sending time (geographical packet leashes) into the packet. Based on this information, B can estimate the distance between A & B. If the estimated distance is longer than the possible radio range, B will reject the communication with A. These two mechanisms require tightly synchronized clocks (temporal packet leashes) or special hardware for location (geographical packet leashes) which is expensive to use widely. Therefore, we can say these two mechanisms are impractical with current technology.

2) RTT

In order to avoid using special hardware, Jane Zhen and Sampalli Srinivas try to detect wormhole using a so-called Round Trip Time (RTT) between two nodes [5]. A node, say A, calculates the RTT with another node, say B, by sending a message to node B requiring an immediate reply from B. The RTT between A and B is the time between A's sending the request message and receiving the reply message from B. In this mechanism each node (called N) will calculate the RTT between N and all N's neighbors. Because the RTT between two fake neighbors is higher than that between two real neighbors so by comparing these RTTs between A and A's neighbors, node A can identify which neighbors are fake neighbors and which neighbors are real neighbors. This mechanism do not require any special hardware and easy to implement but it cannot detect exposed attacks because no fake neighbor is created in exposed attacks.

3) Delphi

Another mechanism called DelPHI (Delay Per Hop Indicator), proposed by Hon Sun Chiu and King-Shan Lui [6], is able to detect both hidden and exposed wormhole attacks. In this mechanism, they try to find every available disjoint path between a sender and a receiver. Then, they calculate delay time & length of each path, computing Delay per Hop value (average delay time per hop along each path). Delay per Hop values of paths are used to identify wormhole: the path containing wormhole link will have greater Delay Per Hop value. This mechanism can detect both kind of wormhole but they cannot pinpoint the wormhole location. Moreover, because lengths of paths are changed by every node (including wormhole nodes) so wormhole nodes could change the path length in a certain way to make them unable to be detected.

4) Sector

In multi-hop wireless networks, keeping track of node encounters is a crucial function, to which the research community has devoted very little attention so far. This function can be used for the detection of wormhole attacks, to se- cure routing protocols based on the history of encounters, and for the detection of cheating attempts (e.g., in charging mechanisms).SECTOR can be used to prevent wormhole attacks [8, 9] in ad hoc networks, without requiring any clock synchronization or location information; it is therefore a valid alternative to the other solutions already proposed to this problem. SECTOR can also help to secure routing protocols in mobile ad hoc networks, which are based on the history of encounters; we illustrate this with FRESH [10], the last- encounter protocol that enables an efficient route discovery for large-scale ad hoc networks.

5) Neighbor Number Test

There are several other approaches which do not use transmission time to detect wormhole. In [10], the author proposed two statistical approaches to detect wormhole attack in Wireless Ad Hoc Networks. The first one called Neighbor Number Test bases on a simple assumption that a wormhole will increase the number of neighbors of the nodes (fake neighbors) in its radius. The base station will get neighborhood information from all sensor nodes, computes the hypothetical distribution of the number of neighbors and uses statistical test to decide if there is a wormhole or not. The second one calledAll Distance Test detects wormhole by computing the distribution of the length of the shortest paths between all pairs of nodes. In these two algorithms, most of the workload is done in the base station to save sensor nodes' resources. However, one of the major drawbacks is that they cannot pinpoint the location of wormhole which is necessary for a successful defense.

6) Truelink

True Link developed by Jakob Eriksson in 2006 is a wormhole detection technique [11] that depends on time based mechanisms. True Link verifies whether there is a direct link for a node to its adjacent neighbour. Wormhole detection using True Link 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 True Link 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 neighboring nodes. The malicious nodes have higher RTT value than other nodes. In this way, the source can identify its genuine and misbehaving neighbors. This detection technique is efficient only in the case of hidden attacks.

7) Secure Neighbor Discovery & monitor based system
This is provided by Issa Khalil in 2008 [12] 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.

8) TTM
TTM –Transmission Time Mechanism [12, 13] to detect wormhole in Wireless Ad Hoc Networks using AODV routing protocol by calculating & comparing the Round Trip Time between every two successive nodes along that route during route setup protocol. TTM is able to detect both hidden & exposed wormhole attacks, locating the wormhole, requiring no special hardware. The performance of TTM is also evaluated by simulation using network simulator The simulation shows that the mechanism can detect wormhole attack with 100% accuracy when the wormhole length is large enough. Some future work also needs to be done to extend our mechanism to work in other routing protocols such as DSDV and DSR.

Table: Comparative analysis of various wormhole detection techniques

Detection Technique	*Advantages*	*Disadvantages*
Packet Leashes	Can find Pinpoint location of wormhole	Can't Detect Exposed attacks Required special Hardware for location
RTT (Round Trip Time)	Don't required any Hardware Easy to implement	Can't detect Exposed Attacks
DeIPHI (Delay Per Hop Indicator)	Can detect Exposed attacks as well as Hidden attacks	Can't Pinpoint the wormhole location
SECTOR	No need to Time Synchronization	Can't find pinpoint location
Neighbor number Test	Can detect Hidden attacks No special Hardware required	Can't detect Exposed attacks
Truelink: A Time based Mechanism	Can detect Hidden attacks More efficient	Works only on IEEE 802.11 Devices Can't detect Exposed attacks
Secure Neighbor Discovery and Monitor based Approach	Central Authority It is capable of even isolating the malicious nodes globally	The Detection rate of this method decreases as the network mobility increases
Transmission Time Mechanism(TTM)	Can find Hidden as well as Exposed attacks Can find Pin point lacation of wormhole No special hardware required	Wormhole detection rate is high only when wormhole length is more than 6 (hop)

4. Conclusion

Wormhole attack is one of the prominent attack in Mobile Ad-hoc network it significantly degrade the performance and reliability of network security. Here we tried to do comparative analysis of various existing approaches which will help us in future to design a new approach for detecting wormhole attack in network. Here we are also doing the comparative analysis of various techniques so it will helpful for detecting various pros and cons of different techniques. So there is choice of solution available based on Cost, Requirements of hardware, security, etc. So there is lot of work still remaining for securing Wireless Mobile Ad-hoc networks from wormhole attacks.

5. Future Scope

In this paper, we done comparative study and analysis of various Wormhole detection techniques but techniques have some pros and cons, there is necessity to develop a such technique, that overcome all these disadvantages with a proper Wormhole detection and prevention also so that Network will more secure form miss users.

References

[1] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks, International Conference on Dependable Systems and Networks (DSN 2005): 612-621

[2] Hon Sun Chiu King-Shan Lui, DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks, International Symposium on Wireless Pervasive Computing ISWPC 2006.

[3] http://mnet.cs.nthu.edu.tw/paper/Fredy/030731.pdf

[4] Wormhole Attacks in Wireless Networks by Yih-chun Hu, IEEE, Adrian Perrig, Member, IEEE, and David B. Johnson, Member IEEE

[5] J. Zhen and S. Srinivas. Preventing replay attacks for secure routing in ad hoc networks. Proc. of 2nd Ad Hoc Networks & Wireless (ADHOC- NOW'03), pp. 140--150, 2003

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

[7] Balfanz, D. Smetters, P. Stewart, and H. Wong.

[8] Talking to strangers: Authentication in ad hoc wireless networks. In *Proceedings of NDSS*, 2002.

[9] N. Ben Salem, L. Butty´an, J.-P. Hubaux, and M. Jakobsson. A charging and rewarding scheme for packet forwarding in multi-hop cellular networks. In *Proceedings of MobiHoc*, 2003

[10] http://dc2.crysys.hit.bme.hu/publications/files/ButtyanDV05esas.pdf

[11] 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

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

[13] http://ieeexplore.ieee.org/Xplore/defdeny.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D4199210&denyReason=133&arnumber=4199210&productsMatched=null&userType=inst

[14] C.-K. Toh, Ad Hoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall, 2002.

[15] W. Wang and B. Bhargava. Visualization of wormholes in sensor networks. In Proceedings of the ACM Workshop on Wireless Security (WiSe), 2004.

[16] Anthony D. Wood and John A. Stankovic: Denial of Service in Sensor Networks, IEEE Computer, October 2002, pp. 61-62.

[17] Karlof and D. Wagner: Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, Ad Hoc Networks, vol. 1, pp. 293-315, 2003

Author Profile

Sushant S. Bahekar received the B.E. degrees in Computer Engineering from SSBT's College of Engineering & Technology, Jalgaon in 2011. Currently pursuing M. Tech in Computer Science & Engineering from SVCE, Indore. He published various Papers in International and National Journals. He also Publish 5 Books for Engineering students of North Maharashtra University. His area of interest is Network Security specially in Ad- Hoc Networks and currently working on Wormhole detection techniques.

Prashant Panse, Reader Department of Information Technology at SVCE, Indore. Received B.E. degree in Information Technology from MIT, Mandsaur in 2003. He also received M. Tech degree in Information Technology from MIT, Ujjain in 2010. Currently He Pursuing his PhD. He published various Papers in International and National Journals. His area of Interest is Mobile Ad-hoc network MANET and Vnet.