A Survey on Wormhole Attack Prevention: ASWAP

Prof.Smita Pawar[1] Steffi Saldanha[2] Silviya Mouris[3] Leena Mariaselvam[4]

Abstract— An ad-hoc network has a dynamic topology. The network is self-organizing and adaptive which repeatedly changes its topology. Nodes can be easily added into the network and hence security issues are a major concern in such networks. It's broadcasting character and transmission medium helps the attacker to interrupt the network. In this paper, we have elaborated on a severe attack called as wormhole attack, its causes and the techniques that are available to detect and prevent the attack. Also a comparative study of the techniques is done and their pros and cons have been stated.

Key words: ASWAP, Wormhole Attack Prevention

I. INTRODUCTION

Security is an essential factor that is taken into consideration for the creation of ad-hoc networks. Ad-hoc networks most striking feature is that it does not require any infrastructure. The ad-hoc network is generally a decentralized network in which nodes are free to move, hence it is said to have a dynamic topology. The adding or extraction of nodes in ad-hoc networks is not a difficult task. This raises the issue of security in them. Various attacks can be launched on ad-hoc networks such as a black hole attack, sinkhole attack, eavesdrop attack, rushing attack etc. The attack that we are going to take into consideration is the wormhole attack.

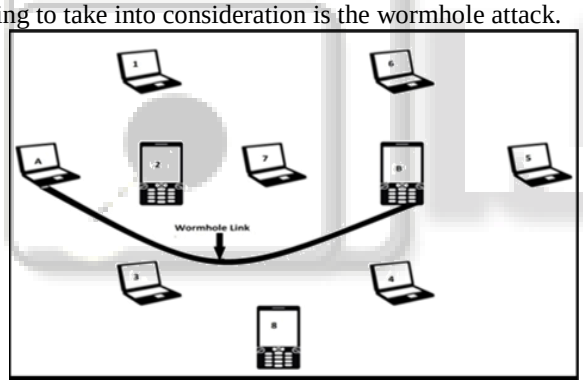

Fig. 1: Wormhole tunnel

It is considered to be a severe attack on security. This is a type of denial of service attack. DOS attack is an active attack on a network in which an attacker can disrupt the normal operation of the network. Here Fig.1 shows an example of a wormhole attack. In this attack, an attacker captures packets at one location, tunnels them to another location of the network, where it is retransmitted into the network [1]. A wormhole attack comprises one or more guileful node, if the network is large the two or more colluding nodes can be present. Out of these nodes, one lies at the source end while the other lies near the destination node. Recent studies have classified the wormhole attack in various ways, these attacks are classified as stated below [5,6]. In the way these nodes are implemented; The medium chosen by these nodes; In the way they attack, on the bases of their visibility[3].The wormhole attack can be classified based on the medium as [2]: 1) In-band channel attack. 2) Out-of-band channel attack

Wormhole can be formed using, in-band channel where a malicious node tunnels the received route request packet to another malicious node that is near to the destination node using encapsulation even though there is one or more nodes between two colluding nodes, the nodes following the colluding node believe that there is no node between the two malicious nodes. Out-of-band channel where two malicious nodes employ a physical channel between them by either dedicated wired link or long range wireless link [2].The wormhole attack can also be classified based on the modes of the attack [3]. There are two main attack modes for a wormhole attack, these are mainly the hidden mode and the participation or active mode. The following is a list of the wormhole attacks based on the hidden mode.

A. Packet Encapsulation or In-band:

Here the packets are transmitted via the legitimate path only, the packet when reaches a colluding node is encapsulated so that the nodes on the way are not able to increase the hop count. When the packet reaches the other colluding node at the receiving end, this node, then decides whether to drop the packet or retransmit it in the network. The attacker nodes are within the network.

B. Packet Relay:

In packet relay the colluding nodes relay packets between two nodes which are far apart from each other and convince these nodes that they are neighbours.

Here is a list of wormhole attacks based on the on the active mode of participation:

1) Out-of Band:

In this type of mode the colluding nodes are connected to each other via an external link. A channel with a high bandwidth is used for creation of the external.

2) High Power Transmission:

In this type of mode when the source node forward the packet the attacker node captures it and transmits it to the destination node with a high power, it enforces the nodes to follow the wormhole link and so that all traffic passes to this path. The detection and prevention of the wormhole are the two main ideas that are being focused on. For the detection and prevention of wormhole there are various techniques available such as liteworp, packet leash, cluster based, and many more.The remainder of this paper is set as follows. We first give a brief explanation of the wormhole detection and prevention techniques that are available. Then we give a comparative study of the methods.

II. METHODS OF WORMHOLE DETECTION

Localized algorithm [6] method is used for detection of wormhole attack in this method the detection is mainly based on the connectivity information. In this method the no additional hardware and overhead is required. It can also be used to detect the attacks at the physical layer. This method can be used to detect the attack of wormhole that are launched even before the network is set up, that may influence localization.

The most commonly cited wormhole prevention mechanism is 'Packet Leash' by Hu et al [7].Packet leash

can be classified broadly as geographical leash and temporal leash. Geographical leash should work fine when GPS coordinates are practical and available [8]. As opposed to geographical leash, temporal leash requires much tighter clock synchronization (in the order of nanoseconds), but does not rely on GPS information [8]. A leash using a timestamp requires accurate time synchronization, so that the receiver can detect if the packet traveled past the distance restricted by the leash; this approach is similar to TIK [9].

In Graph Theoretic[10] technique a local broadcast key is used which satisfies the condition for graph theoretic method. This method does not require time synchronization, or highly accurate clocks, and only a small fraction of nodes need to know their location. This method uses encryption techniques.

Delphi [11] introduced by Hon Sun Chiu et al and King-Shan Liu et al. As mentioned earlier the wormhole attack could be of two types mainly a hidden attack or a participation attack. Delphi provides a method to detect both types of wormhole attack. Delphi stands for Delay Per Hop Indication. In this method the delay of various paths to the receiver is observed, the sender is hence able to detect a wormhole attack. this technique does not need synchronized clocks or external hardware. In Delphi both delay and hop count information is required and this information is obtained by the sender in a way similar to that used by ad-hoc on demand distance vector routing protocol [12].

HMTI (Hello Message Timing Interval Procedure) proposed by M.A. Gorlatva et al. [13] In this technique the main aim is to detect the wormhole based on Hello control messages. Consider an HMTI is in this range R,where R is a range surrounded by the amount of jitter, it is considered to be legitimate; otherwise it is out-of-protocol. An inferior evaluation test is done whenever the Hello Message Timing Interval packet behavior is doubtful.

Trust based models are a significant method proposed for the detection of wormhole attack by Jain and Jain [14]. In this model a trust level is derived and then based on this trust the nodes make routing path selections such that these paths do not contain any wormhole nodes. By using Trust Based Model Packet Dropping is reduced by 15% without using any cryptography mechanism and throughput is increased up to 7-8% [15].

LiteWorp [16] is considered to be a lightweight countermeasure for wormhole attack. It is used for multi-hop ad-hoc networks. LiteWorp is a protocol that detects a wormhole and then eliminates it from a network, thus taking the network to the climax of its performance. In this technique the guard nodes are used to analyse the network performance, it keeps track of the traffic going in and out of its neighbours. The guard node also maintains a list of the malicious nodes that it encounters. It then avoids the use of such node for data transfer. Liteworp does not require any time synchronization or external hardware eg. Directional antenna.

III. COMPARISON OF THE ABOVE STATED TECHNIQUES

Method	Requirement	Benefits	Drawbacks
Localized algorithm	Connectivity information.	Detects attacks at physical layer. No overhead. No special hardware. No false alarms.	Only one -hop detection does not perform well in non-UDG cases. Detection probability drops for sparse networks.
Packet leash	Synchronized time. Location information(GPS). Tik protocol for temporal leash.	Geographical leash- loose time sync . Non- repudiation. Temporal leash- highly efficient.	Geographical leash- more network overhead and computation. Temporal leash- tight time synchronization.
Graph theoretic	Encryption techniques. Local Broadcast key	No time synchronising required. No special hardware. Low overhead.	Guard node requires GPS access. Local broadcast keys only available to one hop neighbours.
Delphi	Delay and hop count information	Can detect hidden and open wormhole attack. Time synchronisation not required. High power efficiency.	In presence of background traffic the rate of detection decreases. False alarm is not detected.
Trust based models	Trust Based Model Packet Dropping	Trust values are used for modification of the path next time	This system is robust only when time and trust based modules are combined together
Liteworp	Guard node. Storage and computational requirement Overhead bandwidth.	Does not require synchronization, specialized hardware. Overhead bandwidth requirement is very small.	Cannot detect protocol deviation mode of attack. Increase in network density increases the false detection probability.

Table 1: Comparative Study of Techniques

IV. CONCLUSION

In conclusion of this paper, we would like to believe that we meticulously explained the notion of a wormhole attack in an ad-hoc network and also stated a majority of the techniques that are available for the detection and prevention of the wormhole attack in ad-hoc networks.

REFERENCES

[1] Karthik Pai B.H1, Dr.Nagesh H.R2, Dr.Niranjan, N.Chiplunkar3, Sharath Kumar4"A Study of Behaviour And Performance Analysis Of Wormhole Attack In Mobile Ad-Hoc Networks" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 4, April 2014.
[2] Chandraprabha Rawat Master's in Software system,Department of computer application, Samrat Ashok Technological Institute, Vidisha, India 1"A Review: Wormhole attack In Mobile Ad Hoc Network. "International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2013.
[3] Akansha Shrivastava and Rajni Dubey Department of Computer Science Engineering SRCEM, "Wormhole Attack in Mobile Ad-hoc Network: A Survey" .International Journal of Security and Its Applications Vol.9, No.7 (2015), pp.293-298
[4] S. Upadhyay and B. K. Chaurasia, "Impact of wormhole attacks on MANETs", International Journal of computer science & Emerging Technologies (E-ISSN: 2044-6004) vol. 2, no. 1, (2011) February.
[5] R. Maulik and N. Chaki," A comprehensive Review on Wormhole Attacks in MANET", in proceeding of 9th International Conference on Computer Information Systems and Industrial Management Applications, (2010), pp. 233-238.
[6] Ritesh Maheshwari, Jie Gao and Samir R Das Department of Computer Science, Stony Brook University Stony Brook, NY 11794-4400, USA. "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information".
[7] Y.-C. Hu, A. Perrig, D. B. Johnson; "Packet leash: a defense against wormhole attacks in wireless networks"; INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, Vol. 3, pp. 1976-1986, 2003.
[8] D. Barman Roy, R. Chaki, N. Chaki, "A new cluster-Based Wormhole Intrusion Prevention Algorithm for Mobile Ad-Hoc Networks", International journal of network security and its application, vol.1, pp-44-52, 2009.
[9] Y. Chun- Hu, A. Perrig, B. Johnson David, "Wormhole Detectionin Wireless Ad Hoc Networks", In Ninth International Conference on Network protocol (ICNP), vol.1, 2002.
[10] L. Lazos1, R. Poovendran1, C. Meadows2, P. Syverson2, L. W.Chang2. "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach". IEEE Communications Society / WCNC 2005.
[11] Hon Sun Chiu and King-Shan Lui Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong, PRC. "Delphi: Wormhole Detection Mechanism for Ad Hoc Wireless Networks". O-7803-9410-O/06/$20.OO ©2006 IEEE.
[12] C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector VI. CONCLUSION Routing," Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, Feb. 1999, pp. 90 - 100.
[13] M.A. Gorlatva, P. C. Mason, M. Wang, L. Lamont, R. Liscano, "Detecting Wormhole attacks in Mobile A d Hoc Networks through Protocol Breaking and Packet Timing Analysis", In IEEE Military Communications Conference, pp. 1-7 ,2000.
[14] Preeti Nagrath,Bhawna Gupta, "Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A survey", pp 245-250, IEEE 2011.
[15] Priya Maidamwar and Nekita Chavhan, "A SURVEY ON SECURITY ISSUES TO DETECT WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK" International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012.
[16] Issa Khalil, Saurabh Bagchi, Ness B. Shroff. "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks" Dependable Computing Systems Lab and Center for Wireless Systems and Applications (CWSA).

