International Journal of Computer Networks and Communications Security

VOL.2, NO.1, JANUARY 2014, 22–26
Available online at: www.ijcncs.org
ISSN 2308-9830

Wormhole Attack in Wireless Sensor Network

RAJ SHREE[1] and R. A. KHAN[2]

[1, 2] Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow

E-mail: [1]rajshree_shukla2001@rediffmail.com, [2]khanraees@yahoo.com

ABSTRACT

In multi hop wireless systems, such as wireless sensor networks, mobile ad hoc network, security is an important factor. It becomes more critical issue when we transmit important data between nodes. There are a lot of attacks available in wireless sensor network or mobile ad hoc network. In our paper we are going to discuss about a particularly devastating attack, known as the wormhole attack. In wormhole attack, an attacker forms two or more malicious nodes in the network at different locations. These nodes are connected with the help of low latency link. As a result of this way two or more malicious nodes create a higher level virtual tunnel in the network. This virtual tunnel is used for sending the packets between the end points of tunnel. Whenever transmission starts between a source to destination, adversary try to record transmitted packets at one location in the network and tunnels all captured packets to another location. The wormhole attack is possible even if the attacker has not compromised with any hosts and even if all communication provides authenticity and confidentiality. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. In this paper, we analyze the nature of wormhole attack in ad hoc and wireless sensor networks and existing methods of the defending mechanism to detect wormhole attacks without require any specialized hardware.

Keywords: *Ad hoc Network, Wireless Sensor Network, Wormhole Attack, Defending Mechanism.*

1 INTRODUCTION

In wormhole attack, the attacker receives packets at one point in the network, forwards them through a wireless or wired link with low latency in the network [1]. In this way, a default link is used by the attacker in the network. With the help of this link, attacker relays packet to another location in the network. In this paper, we assume that a wormhole tunnel can transmit packet in both the direction with two end points. This is called bidirectional approach. Apart from this, multi end wormholes are possible in theory. We can understa-nd wormhole attack with the help of example. Suppose that, we have two networks A and B. These two networks, A and B, have one malicious node X and Y. These two nodes X and Y are malicious nodes, called as wormhole nodes that are connected through a wormhole link. Due to this link, nodes X and Y consider as neighbors for sending routing messages. This has been pointed out by Korkmaz [2]. The attacker can disrupt communications between the network A and B. During transmission, the routes in the network can be rearranged when the attack occurs during protocol discovery phase. We can also observe that packets from protocol discovery phase will get from node A to node B fastest if going through the wormhole link since it has the smallest number of hops. This causes the disruption of the routing protocol and brings severe damage to the network. Therefore, in the section 2, we are presenting working of wormhole attack. In section 3, we are taking into consideration of techniques to mitigate wormhole attack. In section 4, we are simplifying techniques in tabular form. Section 5 and 6 cover conclusion and references.

2 WORMHOLE ATTACK

Wormhole attack is a severe type of attack for Wireless networks. Where two or more attackers are connected by high speed off-channel link called wormhole link [3], [4]. In wormhole attack, a pair

of attackers forms 'tunnels' to transfer the data packets and replays them into the network. This attack has a tremendous effect on wireless networks, especially against routing protocols. Routing mechanisms can be confused and disrupted when routing control messages are tunneled to wrong direction. The tunnel formed between the two colluding attackers is referred as wormhole link. Figure 1 shows the working of wormhole attack. Packets received by node X is replayed through node Y and vice versa. Normally it take several hops for a packet to traverse from a location near X to a location near Y. Packets transmitted near X travelling through the wormhole will arrive at Y before packets travelling through multiple hops in the network. The attacker can make A and B believe that they are neighbors by forwarding routing messages, and then selectively drop data messages to disrupt communication between A and B [5].

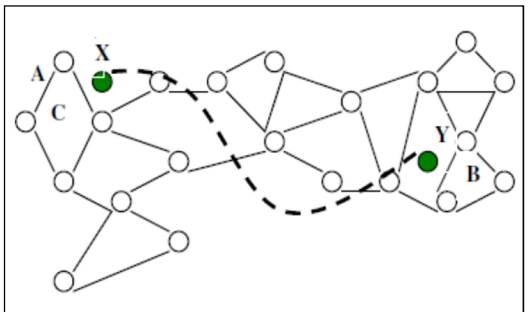

Fig. 1. Wormhole Attack

A wormhole receives a message at its "origin end" and transmits it at its "destination end". Note that the designation of wormhole ends as origin and destination are dependent on the context. We also assume a wormhole is passive i.e. it does not send a message without receiving a message and static i.e. it does not move. The wormhole attack can be occurred in an infrastructure based wireless network. In an infrastructure based wireless network, the two nodes that form the wormhole link can be two rogue access points. A rogue access point is an access point that is not authorized in the network. These access points are established by the attacker for capturing data or important information.

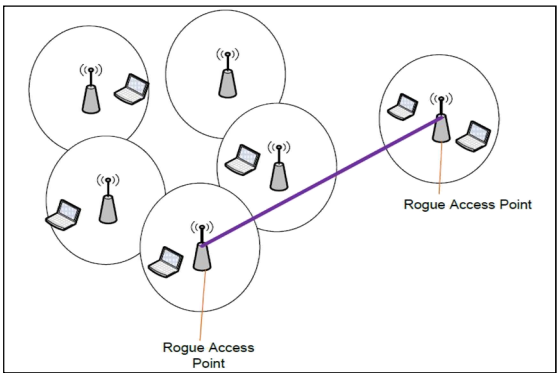

Fig. 2. Wormhole Attack in Infrastructure Based Network

As shown in figure 2 and described by Sriram [6], the attacker has two rogue access points in the infrastructure based wireless network. The essential point remains the same and that is packets from one rogue access point will be getting to the other rogue access point faster than other routes. The attacker has the control over the rogue access points so an attacker can launch wormhole attacks without the knowledge of cryptographic technique and keys. Wireless networks are widely used in private sectors, governments, and different parts of the world. The impact of the attacks can be severe. Therefore, it is not something that should be ignored.

3 TECHNIQUES TO MITIGATE WORMHOLE ATTACK

In an ad hoc network, several researchers have worked on pretending and detecting wormhole attacks specifically. In section A we discuss a technique called 'packet leashes'. In section B we discuss wormhole detection or prevention techniques suitable for only particular kinds of networks.

3.1 Packet Leashes

There are many methods for detecting and protecting the ad hoc or sensor wireless networks to the wormhole attack. One method or idea is of packet leashes for detecting wormhole attacks. This method was developed for ad hoc networks but also works for the other types of networks as well. A Packet leash is any information that is added to the

sending packets. Packet Leash in [7], [8], [9] is a mechanism to detect and defend against wormhole attacks. The mechanism proposes two types of leashes for this purpose: Geographic and Temporal.

In Geographic Leashes, each node knows its precise position and all nodes have a loosely synchronized clock. Each node, before sending a packet, appends own current position and transmission time to the sending packet. The receiving node, on receipt of the packet, computes the distance to the sender and the time which was taken by packet for travelling the path. The receiver can use this distance and time information to check the packet whether the received packet passed through a wormhole or not. In Temporal Leashes, all nodes are required to maintain a tightly synchronized clock but do not rely on GPS information. When temporal leashes are used, the sending node appends the time of transmission to each sending packet ts in a packet leash, and the receiving node uses its own packet reception time tr for verification. The sending node calculates an expiration time te after which a packet should not be accepted, and puts that information in the leash. To prevent a packet from traveling farther than distance L, the expiration time is set to:

$$te = ts + (L/c) - \Delta \quad (1)$$

In the formula (1) c is the speed of light and is the maximum clock synchronization error. All sending nodes append the time of transmission to each sent packet. The receiver compares the time to its locally maintained time and assuming that the transmission propagation speed is equal to the speed of light, computes the distance to the sender. The receiver is thus able to detect, whether the packet has travelled on additional number of hops before reaching the receiver. Both types of leashes require that all nodes can obtain an authenticated symmetric key of every other node in the network. These keys enable a receiver to authenticate the location and time information in a received packet.

3.2 Specialized Techniques

A wide variety of wormhole attack mitigation techniques have been proposed for specific kinds of networks: sensor networks, static networks, or networks where nodes use directional antennas. In this section, we describe and discuss such techniques, commenting on their usability and the possibility of their use in general mobile ad hoc networks. Hu and vans propose a solution to wormhole attacks for ad hoc networks in which all nodes are equipped with directional antennas in [3].

In this technique nodes use specific 'sectors' of their antennas to communicate with each other. Each couple of nodes has to examine the direction of received signals from its neighbor. Hence, the neighbor relation is set only if the directions of both pairs match. This extra bit of information makes wormhole discovery and introduces substantial inconsistencies in the network, and can easily be detected. Wang and Bhargava [10] introduce an approach in which network visualization is used for discovery of wormhole attacks in stationary sensor networks. In their approach, each sensor estimates the distance to its neighbors using the received signal strength. All sensors send this distance information to the central controller, which calculates the network's physical topology based on individual sensor distance measurements. With no wormholes present, the network topology should be more or less flat, while a wormhole would be seen as a 'string' pulling different ends of the network together. Lazos et al [5] proposed a 'graph-theoretical' approach to wormhole attack prevention based on the use of Location- Aware 'Guard' Nodes (LAGNs). Lazos uses 'local broadcast keys'. These keys will valid only between one-hop neighbors to defy wormhole attackers. In this, a message encrypted with a local key at one end of the network cannot be decrypted at another end. Lazos proposes to use hashed messages from LAGNs to detect wormholes during the key establishment. A node can detect certain inconsistencies in messages from different LAGNs if a wormhole is present. Without a wormhole, a node should not be able to hear two LAGNs that are far from each other, and should not be able to hear the same message from one guard twice. Khalil et al [11] proposed a protocol for wormhole attack discovery in static networks. This technique is called as Lite Worp. In Lite Worp, nodes obtain full two-hop routing information from their neighbors. While in a standard ad hoc routing protocol nodes usually keep track of their neighbors. In Lite Worp, they can take advantage of two-hop, rather than one-hop. This information can be exploited to detect wormhole attacks. These nodes also observe their neighbors' behavior to determine whether data packets are being properly forwarded by the neighbor. Song et al [12] proposed a wormhole discovery mechanism based on statistical analysis of multipath routing. Song observed that a link created by a wormhole is very attractive in routing sense, and will be selected and requested with unnaturally high frequency as it only uses routing protocols that are both on-demand and multipath.

4 SUMMARY OF WORMHOLE ATTACK DISCOVERY METHODS IN TEBULAR FORM

As per the above discussion, it is clear that there are various techniques available. These techniques can be categorized in tabular form as below:

Table 1: Summary of Wormhole Discovery Methods.

Method	Requirements	Commentary
Packet leashes, geographical	GPS coordinates of Every node; Loosely synchronized clocks (ms)	Robust, Straight forward solution; inherits general limitations of GPS technology
Packet leashes, temporal [7], [9]	Tightly synchronized clocks (ns)	Impractical; required time synchronization level not currently achievable in to sensor networks
Packet leashes, end-to-end [13]	GPS coordinates; Loosely synchronized clocks (ms)	Inherits limitations of GPS technology
Time of flight [14]	Hardware enabling one- bit message and immediate replies without CPU involvement [14]	Impractical; likely to require MAC-layer modifications
Directional antennas [3]	Directional antennas on all nodes [3] with both GPS and directional antennas [15]	solutions for networks relying on directional antennas, but not directly applicable to other networks
Network visualization [10]	Centralized controller	Seems promising; Works best on dense networks; Mobility not studied

5 CONCLUSION

Wormhole attacks have been identified as attacks that can be powerful and can be cause of severe damage to the network even if communications require authentication and encryption. It is not something that we should take lightly. Methodologies for detecting and protecting against these attacks have been proposed mainly for ad-hoc and sensor networks as we have mentioned a few of them in this paper. It is new for infrastructure based networks. However, it is not less significant. Therefore we have mentioned a possible strategy in detecting and protecting against wormhole attacks and may be other attacks in infrastructure based wireless networks by focusing on identifying rogue access pints in infrastructure based wireless networks.

6 REFERENCES

[1] R.E.Kassi, A.Chehab, and Z. Dway, "DAWWSEN: A Defense Mechanism against Wormhole Attacks in Wireless Sensor Networks", in proceeding of the second International conference on innovations in information Technology (ITT' 05), UAE, September 2005.

[2] Turgay Korkmaz, "Verifying Physical Presence of Neighbors against Replay-based Attacks in Wireless Networks", IEEE, 2005.

[3] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 14 Proceedings of the 11th Network and Distributed System Security Symposium, 2003.

[4] Y.-C. Hu, A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing", Security and Privacy Magazine, IEEE, vol. 2, issue 3, pp. 28-39, May 2004.

[5] L. Lazos and R. Poovendran, "Serloc: Secure Range- Independent Localization for Wireless Sensor Networks", Proceedings of the ACM Workshop on Wireless Security, October 2004, pp. 21- 30.

[6] V. S. Shankar Sriram, Ashish Praptap Singh and G. Sahoo, "Methodology for Securing Wireless LANs against Wormhole Attack", IJRTE, Vol. 1, May 2009, p.p. 148-152.

[7] Y.-C. Hu, A. Perrig, D. B. Johnson, "Wormhole Attacks in Wireless Networks", Selected Areas of Communications, IEEE Journal on, vol. 24, 2006, pp. 370- 380.

[8] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", in proceedings of INFOCOM, 2004.

[9] W. Weichao, B. Bharat, Y. Lu, X. Wu, Wiley Inter science, "Defending against Wormhole Attacks in Mobile Ad Hoc Networks", Wireless Communication and Mobile Computing, January 2006.

[10] W. Wang and B. Bhargava., "Visualization of wormholes in sensor networks", Proceedings of the ACM workshop on Wireless Security, 2004, pp. 51-60.

[11] Issa Khalil, Saurabh Bagchi and Ness B. Shroff, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", in International

Conference on Dependable Systems and Networks (DSN), 2005.

[12] N. Song, L. Qian and X. Li, "Wormhole Attack Detection in Wireless Ad Hoc Networks: a Statistical Analysis Approach", Parallel and Distributed Processing Symposium, 2005, Proceedings of, 19th IEEE International IPDPS'05, 04-08 April 2005.

[13] S. Capkun, L. Buttyan, J.-P. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks", October 2003, Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks.

[14] A. Baruch, R. Curmola, C. Nita- Rotaru, D. Holmer and H. Rubens, " On the Survivability of Routing Protocols in Ad Hoc Wireless Networks", Convergence on Security and Privacy for Emerging Areas Communications, SecureComm 2005, September 2005.

[15] L. Lazos, R. Poovendram, C. Meadows, P. Syverson and L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC 2005.