



Prevention and Detection of Worm Hole Attack in Wireless Networks

Meenu Vijarana

Assistant Professor

Department of Computer Science Engineering,
Amity University, Haryana, INDIA.

Abstract: Security of deployed wireless sensor networks (WSNs) has become a crucial task as the deployment of WSN'S grows. In these environments, security issues are extremely important since a successful attack can cause great damage, even threatening human life. However, due to the open nature of wireless communication, WSNs are liable to be threatened by various attacks, especially destructive wormhole attack, in which the network topology is completely destroyed. In this paper the various aspects have been covered regarding security provisioning in wireless sensor networks. Also some light has been thrown on the various types of attacks and its classification. The wormhole attack is possible even if the attacker has not comprised any hosts, and all communication provides authenticity and confidentiality. By using the various approaches for finding the solution over wormhole attack, the dynamic information of the packets could still be modified. So in order to give more robust protection in some special scenario like battlefields, which requires highly secured information, there is need of developing some secured mechanism for wormhole detection and prevention. Even though an attack is inevitable on a live node network using a simulator, this paper has shown how the network nodes can be rerouted to avoid the attacked nodes.

Keywords: wormhole, wireless network, attack, nodes

I. INTRODUCTION

The promise of mobile ad hoc networks to solve challenging real-world problems continues to attract attention from industrial and academic research projects. Most previous ad hoc networking research has focused on problems such as routing and communication, assuming a trusted environment. However, many applications run in un-trusted environments and require secure communication and routing. Applications that may require secure communications include emergency response operations, military or police networks, and safety-critical business operations such as oil drilling platforms or mining operations. However, security issues are a major concern when WSNs are deployed in untrusted environments. An adversary may disable a WSN by interfering with intra-network packet transmission via wormhole attacks, sybil attacks [6], jamming or packet injection attacks [7]. The wormhole link can be established by a variety of means, e.g., by using a network cable and any form of "wired" link technology or a long-range wireless transmission in a different band. The end-points of this link (wormhole nodes) are equipped with radio transceivers compatible with the ad hoc or sensor network to be attacked. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end.

II. WORM HOLE 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. If the wormhole is placed carefully by the attacker and is long enough, it is easy to see that this link can attract a lot of routes. Note that if the wormhole link is short, it may not attract much traffic, and hence will not be of much use to the adversary.

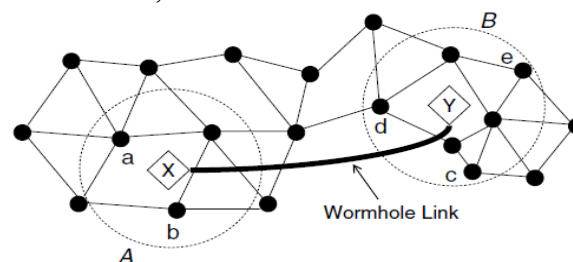


Figure 1: Demonstration of a wormhole attack. X and Y denote the wormhole nodes connected through a long wormhole link.

A Types of Wormhole Attack

Number of nodes involved in establishing wormhole and the way to establish it classifies wormhole into the following types. Wormhole using Out-of-Band Channel and in this two-ended wormhole, a dedicated out-of-band high bandwidth channel is placed between end points to create a wormhole link.

1. Wormhole using Packet Encapsulation

Each packet is routed via the legitimate path only, when received by the wormhole end, gets encapsulated to prevent nodes on way from incrementing hop counts. The packet is brought into original form by the second end point.

2. Wormhole using High Power Transmission

This kind of wormhole approach has only one malicious node with much high transmission capability that attracts the packets to follow path passing from it.

3. Wormhole using Packet Relay

Like the previous approach, only one malicious node is required that replays packets between two far nodes and this way fake neighbors are created.

4. Wormhole using Protocol Deviation

The malicious node creates wormhole by forwarding packets without backing off unlike a legitimate node and thus, increases the possibility of wormhole path getting selected. [5]

B. Models of Wormhole Attacks

The wormhole attack can classify in various ways. Here some of classifications are given below

- In bound wormhole attack
- Out of bound wormhole attack
- Open wormhole attack
- Half open wormhole attack
- Closed wormhole attack

In band and out of band are two other types of classification of wormhole. In this way the attacker builds an overlay tunnel over the existing wireless medium so that it is known as the in band wormhole attack. This attack is potentially very much harmful and is the most preferred choice for the attacker. On other hand the out of band uses the different wireless network in order to perform the attack in the network. In open wormhole attack, attacker node keep an eye on the RREQ packets of the network, in the presence of malicious node in the network other node on the network suppose that malicious node are present on path and they are their direct neighbours. It means the both nodes show their identity in the network. The Figure 2 shows the open wormhole attack of wireless sensor network.

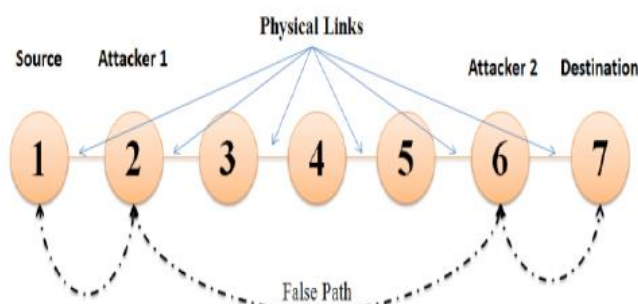


Figure 2 Open Wormhole Attack

The Half open Wormhole attack is just like the open wormhole but here only one node shows its identity another one hide itself from the network. So the packet modification will do on one side. The Figure 3 shows the Half Open wormhole attack of wireless sensor network.

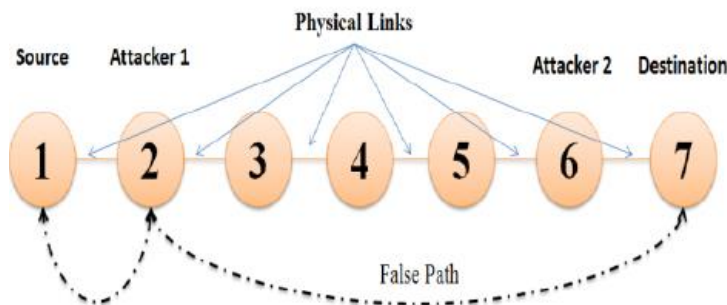


Figure 3 Half Open Wormhole Attack

This is third types of wormhole where the attacker node doesn't temper the data packet. The both node are hidden from the node. They listen to the network activity and always show the shortest path. When sender finds its path

using some algorithm, then hidden node reply and sender trap in this scenario. The Figure 4 shows the closed wormhole attack on wireless sensor network.

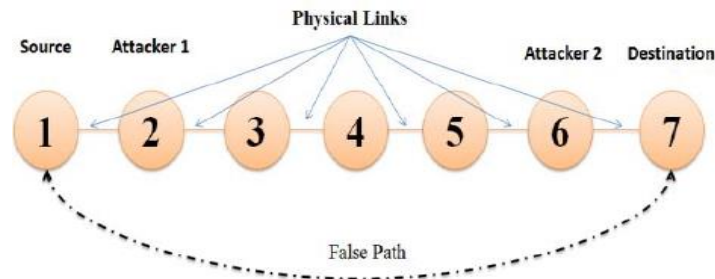


Figure 4 Closed Wormhole Attack

III. DETECTION TECHNIQUE

Based on the principle of detecting wormholes, detailed detection procedure will be presented in this section. Two neighbor nodes such as node A and B are to be checked which has its neighbor list $N(A)$ and $N(B)$ separately. The neighbor list information can be exchanged between neighbors through periodic beacon messages. After nodes A and B exchange the neighbor list information, the detection procedure will begin. Node A notifies all its neighbors in $N(A)$ through its beacon messages that will increase its transmission radius. The neighbor nodes receiving this notification will not change their transmission radius in the next beacon time. Then node A increases its transmission range to $2r$ and updates its neighbor list $N(A)$. Finally, node A compares $N(A)$ and $N(B)$: 1. If the neighbor lists $N(A)$ and $N(B)$ satisfy $N(B) \subseteq N(A)$, then there is no wormhole link between node A and B. 2. If the neighbor lists $N(A)$ and $N(B)$ satisfy $N(B) \subset N(A)$, then there is a wormhole link between node A and B.

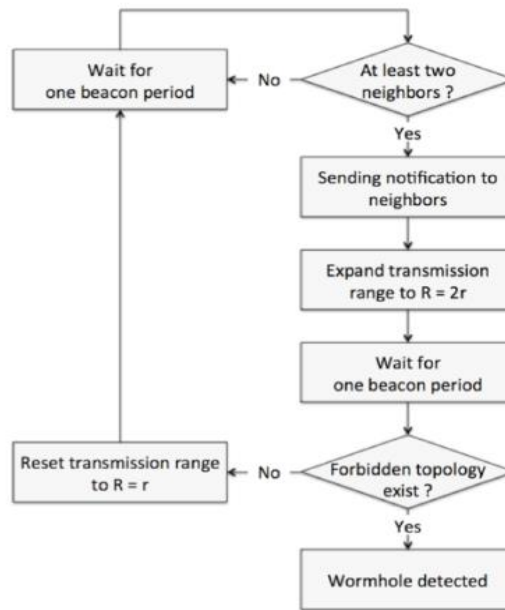


Figure 5 Wormhole Detection Process

IV Conclusion

In this paper, we have introduced the wormhole attack, a powerful attack that can have serious consequences on many proposed ad hoc network routing protocols; the wormhole attack may also be exploited in other types of networks and applications, such as wireless access control systems based on physical proximity. 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 studied 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.

References

- [1] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNSDS 2002), 2002.
- [2] Y. C. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in INFOCOM, 2003.

- [3] K. Sanzgiri, B. Dahill, B. Levine, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," in International Conference on Network Protocols (ICNP), November 2002.
- [4] B. Dahill, B. N. Levine, E. Royer, and C. Shields,, "A secure routing protocol for ad hoc networks," In Proc.of the 10th Conference on Network Protocols (ICNP), 2002.
- [5] I. Khalil, S. Bagchi, and N. B. Shroff, "LITEWOP: A lightweight countermeasure for the wormhole attack in multihop," In Proc.of the International Conference on Dependable Systems and Networks, 2005.
- [6] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," ACM WiSe, 2002.
- [7] 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.
- [8] W. Wang and B. Bhargava., "Visualization of wormholes in sensor networks", Proceedings of the ACM workshop on Wireless Security, 2004, pp. 51-60.