Volume 3, Issue 3, March 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detection and Prevention of Wormhole Attack in MANET: A Review

Poonam Dabas[1], Prateek Thakral[2]
[1]Assistant Professor, U.I.E.T, KurukshetraUniversity Kurukshetra, Haryana, INDIA
[2]Research Scholar, U.I.E.T, Kurukshetra University Kurukshetra, Haryana, INDIA

Abstract: **Ad hoc networks are vulnerable due to their structure less property. A Mobile Ad-Hoc Network (MANET) is an infrastructure less self-configured collection of mobile nodes that can arbitrarily change their geographic locations such that these networks have dynamic topologies and random mobility with constrained resources. Security has become a primary concern in order to provide protected communication between mobile nodes in an aggressive environment. The absence of any central coordination mechanism and shared wireless medium makes MANETs more vulnerable to cyber attacks than wired networks. Different mechanisms have been proposed using various cryptographic techniques to countermeasures these attacks against MANET. The Wormhole attack at network layer is the most attention seeking attack in ad hoc networks. This attack is hard to detect and easy to implement. This paper presents a review of various techniques used to detect and prevent the Wormhole attack.**

Keywords: MANET, Security, Wormhole Attack, Detection and Prevention Techniques

I. INTRODUCTION

Mobile ad hoc networks (MANET) can be defined as a collection of large number of mobile nodes that form temporary network without help of any existing network infrastructure or central access point. Each node participating in the network acts both as host and as router. It provides high mobility and device portability's that enable to node connect network and communicate to each other. It allows the devices to maintain connections to the network as well as easily adding and removing devices in the network [1]. Security in MANET is the most important concern for the basic functionality of network. The provision of security services in the MANET context faces a set of challenges specific to this new technology. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. The Wormhole attack is one of the most severe security attacks which can significantly disrupt the communications across the network [2]. This paper presents various methods to detect and prevent Wormhole attack. The rest of the paper is organized as follows. Section 2 discusses the Wormhole attack in MANETs and its classification & various modes. Section 3 presents the various techniques used for the detection and prevention of Wormhole attack and finally Section 4 presents our conclusions.

Wormhole Attack In Manet

In physics, a wormhole is a hypothetical shortcut through space and time that connects two distant regions. The Wormhole attack at network layer is the most attention seeking attack in ad hoc networks [2][3]. Wormhole attack is also known as tunneling attack. In a wormhole attack, the attacker receives packets at one location in the network, tunnels them to another location and replays them there. This tunnel between two colluding attackers is referred to as a Wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. This attack is hard to detect and easy to implement [3]. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel. In the fig. below, 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.

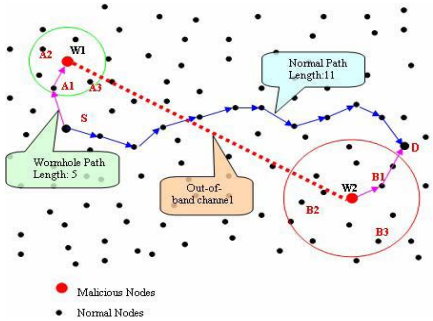

Fig1. Wormhole Attack in an ad-hoc network

The Wormhole attack can be classified into two categories: Hidden attacks and Exposed attacks, depending on whether wormhole nodes put there identity into packet's headers when tunneling & replaying packets [2][3].

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

S → A1 → B1 → D

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 in the figure above via wormhole will be:

S → A1 → W1 → W2 → B1 → D

Wormhole Attack Modes

Wormhole attacks can be launched using several methods, among these modes [3], we mention:

Wormhole using Encapsulation: When a malicious node at one part of the network hears the route request packet, it tunnels it to a second colluding party at a distant location near the destination. The second party then rebroadcasts the route request. The neighbors of the second colluding party receive the route request and drop any further legitimate requests that may arrive later on legitimate multi-hop paths. The result is that the routes between the source and the destination go through the two colluding nodes that will be said to have formed a wormhole between them. This prevents nodes from discovering legitimate paths that are more than two hops away. One way for two colluding malicious nodes can involve themselves in a route is by simply giving the false illusion that the route through them is the shortest, even though they may be many hops away.

Wormhole using Out-of-Band channel: This mode of the wormhole attack is launched by having an out-of-band high-bandwidth channel between the malicious nodes. This channel can be achieved, for example, by using a long-range directional wireless link or a direct wired link. This mode of attack is more difficult to launch than the previous one since it needs specialized hardware capability.

Wormhole using Packet Relay: In this mode of the wormhole attack, a malicious node relays packets between two distant nodes to convince them that they are neighbors. It can be launched by even one malicious node. Cooperation by a greater number of malicious nodes serves to expand the neighbor list of a victim node to several hops.

Wormhole with High Power Transmission: In this mode, when a single malicious node gets a route request, it broadcasts the request at a high power level, a capability which is not available to other nodes in the network. Any node that hears the high-power broadcast rebroadcasts it towards the destination. By this method, the malicious node increases its chance to be in the routes established between the source and the destination even without the participation of a colluding node. A simple method to mitigate this attack is possible if each node can accurately measure the received signal strength and has models for signal propagation with distance.

II. DETECTION AND PREVENTION TECHNIQUES

The various techniques or protocols used for the detection and prevention of Wormhole attack in MANET are described below:

Packet Leashes: The concept of Geographical and Temporal packet leashes were introduced first for the detection and prevention of wormholes [4]. A leash is defined as any added information to the packet for the purpose of protecting against the wormhole. The geographical leashes ensure that the recipient of the packet is within a certain distance from the sender. The temporal leashes ensure that the packet has an upper bound on its lifetime, which restricts the maximum travel distance. They require that all nodes have tightly synchronized clocks. Both geographical and temporal leashes need to add authentication data to each packet to protect the leash, which add processing and communication overhead.

Round Trip Time: A technique called Round Trip Time (RTT) was used to detect wormhole between two nodes in order to avoid use of any special hardware. A node, say A, calculates the RTT [5] 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 compute 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 recognize 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 can not detect exposed attacks because no fake neighbor is created in exposed attacks.

Directional Antennas: Directional antennas [6] were also used to prevent the Wormhole attack. To ruin the wormhole, each node shares a secret key with every other node and maintains an updated list of its neighbors. To discover its neighbors, a node, called the announcer, uses its directional antenna to broadcast a HELLO message in every direction. Each node that hears the HELLO message sends its identity and an encrypted message, containing the identity of the announcer and a random challenge nonce, back to the announcer. Before the announcer adds the responder to its neighbor list, it verifies the message authentication using the shared key, and that it heard the message in the opposite

directional antenna to that reported by the neighbor. This approach is suitable for secure dynamic neighbor detection. However, it only partially mitigates the wormhole problem.

LITEWORP: A lightweight countermeasure for the wormhole attack, called LITEWORP [7] was introduced. The basic method used is local monitoring whereby a node monitors traffic in and out of its neighboring nodes and uses a data structure of first and second hop neighbors. LITEWORP isolates the malicious node and removes its ability to cause future smash up. The guard node is a common neighbor of two nodes to detect a legitimate link between them. The guard node can detect the wormhole if one of its neighbors is behaving maliciously. LITEWORP does not require any specialized hardware, such as directional antennas or fine granularity clocks. In a sparse network, however, it is not always possible to find a guard node for a particular link.

***Time Based Mechanism*:** A transmission time based mechanism (TTM) was used to detect wormhole attacks [8]. TTM detects wormhole attacks during route setup procedure by computing transmission time between every two consecutive nodes along the recognized path. Wormhole is identified based on the fact that transmission time between two bogus neighbors created by wormhole is considerably higher than that between two authentic neighbors which are with in radio range of each other. TTM has good performance, little overhead and no special hardware required. TTM is designed specifically for Ad Hoc On-Demand Vector Routing Protocol (AODV) but it can be extended to work with other routing protocols.

***Wormhole Attack Prevention*:** An efficient method called Wormhole Attack Prevention (WAP) was developed without using specialized hardware [9]. The WAP not only detects the fake route but also adopts preventive measures against action wormhole nodes from re-appearing during the route detection phase. All nodes examine its neighbor's performance when they send RREQ messages to the destination by using a special list called Neighbor List. When a source node receives some RREP messages, it can detect a route under wormhole attack among the routes. Once wormhole node is detected, source node records them in the Wormhole Node List. The WAP has the ability of detecting both the hidden and exposed attacks without any special hardware. A special timer is used to detect wormholes.

***Topological Comparison Based Method*:** A new detection mechanism called RTT-TC, which is based on round trip time measurements and topological comparisons, was also introduced for the detection of wormhole attack [10]. The scheme is based on the following two observations of wormhole attacks: Two fake neighbors with a wormhole tunnel in between has longer RTT, compared to the RTT with true neighbors and Two true neighbors usually share other true neighbors between them, and two fake neighbors do not share common true neighbors. The first rely is on RTT measurements to identify suspected wormhole attacks and then use of topological comparison to exclude genuine neighbors from the suspected list.

***Using Wireless Protocol*:** A new protocol was designed and developed that prevents wormhole attacks on wireless networks. The design of this protocol is based on the use of asymmetric and symmetric key cryptography and a Global Positioning System (GPS). Nodes are distinguished here as GPS node and non-GPS node [11]. The most significant difference between GPS and non- GPS nodes is that non-GPS nodes do not know their location directly. Both types of nodes make use of asymmetric and symmetric key cryptography. Since non-GPS nodes refer to GPS nodes to determine relative location, asymmetric key cryptography plays a vital role to providing integrity and trust that only reports of location come from GPS nodes.

Packet Travel Time: An efficient algorithm was proposed which was an improvement on another algorithm which was based on transmission time-based mechanism (TTM). Moreover, this algorithm introduces a new mechanism called Packet Travel Time (PTT) [12]. This mechanism allows each device to monitor its neighbor's behavior. This mechanism initially uses the same procedure, which has been introduced in TTM mechanism, to calculate the RTTs. However, some alterations are added to it when it is required. The proposed mechanism is called Packet Travel Time (PTT) to examine all transmitted packets in the network. According to this method, nodes should have their network interfaces in the promiscuous reception mode, and network links function bi-directionally.

***Using Honeypots*:** Recently a method of providing security against wormhole attacks to a MANET by learning about the environment dynamically and adapting itself to avoid malicious nodes was introduced with the assistance of Honeypot [13,14]. The principle scope of a honeypot is to discover and learn the actions of the intruders and that to improve the network security. Honeypot is a trap to detect, capture, and misguide the intruders who try to attack the system or gain unauthorized access to it. Honeypots can be used to know the methodology used by the intruder, detect the threats, tools used and vulnerabilities the attackers are looking for, know the motives of an attacker and distract the attacker and provide early warning to the system about the attack [14].

III. CONCLUSION

Wormhole attacks are severe attacks that can easily be launched even in networks with confidentiality and authenticity. Malicious nodes usually targets the routing control messages related to topology or routing information. In this paper, we introduced the Wormhole attack along with its classification that can have serious consequences on many proposed ad hoc network routing protocols. Various methods and techniques used for the detection and prevention of wormhole attacks such as packet leashes, directional antennas, time-based mechanisms and many other protocols along with their advantages and drawbacks are also discussed.

REFERENCES

[1] C. Siva Ram Murthy & B.S Manoj, "Mobile Ad Hoc Networks- Architectures & Protocols" Pearson Education, New Delhi, 2004.

[2] I. Guler, M. Meghdadi, and S. Ozdemir, "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks," *IETE Technical Review*, vol. 28, no. 2, pp. 89–102, 2011.

[3] M. Jain, H. Kandwa1**,** "A Survey on Complex Wormhole Attack in Wireless Ad-Hoc Network," in Advances in Computing, Control & Telecommunication Technologies, pp. 555-558, 2009.

[4] Y. C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in Proceedings of the 22nd INFOCOM, pp. 1976-1986, 2003.

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

[6] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole attacks," in Network and Distributed System Security Symposium, 2004.

[7] I. Khalil, S. Bagchi, N. B. Shroff. *LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks*. In International Conference on Dependable System and Networks (DSN), Jul. 2005.

[8] Phuong, T. V., N. T. Canh, and Young-Koo. Lee, S. Lee, and H. Lee, "Transmission Time-based Mechanism to Detect Wormhole Attacks", IEEE Computer society, (2007), pp. 172-178.

[9] Sun Choi, Doo-Young Kim, Do-Hyeon Lee and Jae-Il Jung (2008), 'WAP: Wormhole Attack Prevention Algorithm in Mobile Ad hoc Networks', In Proc. of IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, pp. 343-348.

[10] Mohammad Alam and King-Sun Chan, "RTTTC: A Topological Comparison Based Method to Detect Wormhole Attacks in MANET", in 12th IEEE International Conference in Communication.

[11] S. Keer and A. Suryavanshi , To prevent wormhole attacks using wireless protocol in manets, In *Int'lConference on computer science and technology |ICCCT'2010.*

[12] A. Alshamrani, "PTT: Packet travel time algorithm in mobile ad hoc networks," in *Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference*, march 2011, pp. 561 –568.

[13] Mokube and M. Adams, "Honeypots: concepts, approaches, and challenges," in *Proceedings of the 45th annual southeast regional conference*. New York, USA: ACM, 2007

[14] T. H. project, "Know your enemy," July 2000.Available:http://project.honeynet.org/papers.

