



A Novel Technique for the Prevention of Wormhole Attack

Poonam Dabas, Prateek Thakral

Department of Computer Science & Engineering
U.I.E.T Kurukshetra University, Kurukshetra
Haryana, India

Abstract- 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 network. 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 novel technique to prevent wormhole attack using clustering.

Keywords: MANET, Security, Wormhole Attack, Clustering and Digital Signatures

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 a novel technique to prevent Wormhole attack. The rest of the paper is organized as follows. Section II discusses the Wormhole attack in MANETs and its classification. Section III presents the various techniques used for the detection and prevention of Wormhole attack. Section IV presents our novel technique for the prevention of wormhole attack and finally Section V presents our conclusions.

II. 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.

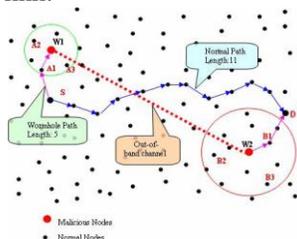


Fig1. Wormhole Attack in an ad-hoc network

The Wormhole attack can be classified into two categories: Hidden attacks and Exposed attacks, depending on whether wormhole nodes put their 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: $S \rightarrow A1 \rightarrow B1 \rightarrow D$

Exposed Attack: In exposed attack, 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:

$S \rightarrow A1 \rightarrow W1 \rightarrow W2 \rightarrow B1 \rightarrow D$

III. Related Work

Various techniques and protocols have been used for the detection and prevention of Wormhole attack in MANET. The concept of Geographical and Temporal packet leashes was 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. 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 [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.

A lightweight countermeasure for the wormhole attack, called LITEWOP [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. LITEWOP 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. LITEWOP 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. 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 within 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. 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 [9]. 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.

An efficient algorithm was proposed which was an improvement on another algorithm which was based on transmission time-based mechanism (TTM) [8]. Moreover, this algorithm introduces a new mechanism called Packet Travel Time (PTT) [10]. 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. 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 [11][12]. 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 [11].

IV. Proposed Technique

The Wormhole attack at network layer is the most attention seeking attack in ad hoc networks; it consists of two malicious nodes and a tunnel between malicious nodes. Several methods have been proposed for detecting wormhole attacks in ad-hoc network. However, these methods usually require that some nodes in the network be equipped with special hardware. Our proposed model consists of building such a mechanism which would be helpful in prevention of wormhole attack in a clustered ad hoc network using digital signatures.

The complete network is divided into small clusters based on proximity of nodes. Each cluster has a Cluster Head (CH) which helps in maintaining the cluster and one or more Gateway (GW) nodes that form the communication links to different clusters. A node is selected to be a Cluster Head based on the number of nodes in its proximity (transmission range). Thus, every node in a cluster is one hop away from the CH. A Gateway Node can belong to only one cluster. Thus, for every interface between two clusters, two GW nodes participate, one from each cluster. For a node to communicate with a node of another cluster, it must send the Route Request (RREQ) Packet to its CH which further sends the RREQ to other clusters (if needed) through GW nodes until the RREQ reaches the CH of the cluster to which the destination node belongs. The destination node then sends a Route Reply (RREP) packet to the source via the path that was discovered the earliest. Additionally, every CH broadcasts its Public Key to all the nodes within its cluster. GW nodes belonging to the two different clusters exchange the public keys of their respective CHs. Thus each GW node has two (or more) sets of Public Keys (one of its own CH and others of its neighbor's CH). The proposed algorithm will prevent nodes from routing data through the wormhole path as all communications take place through the CH and GW nodes, thereby, preventing a wormhole attack.

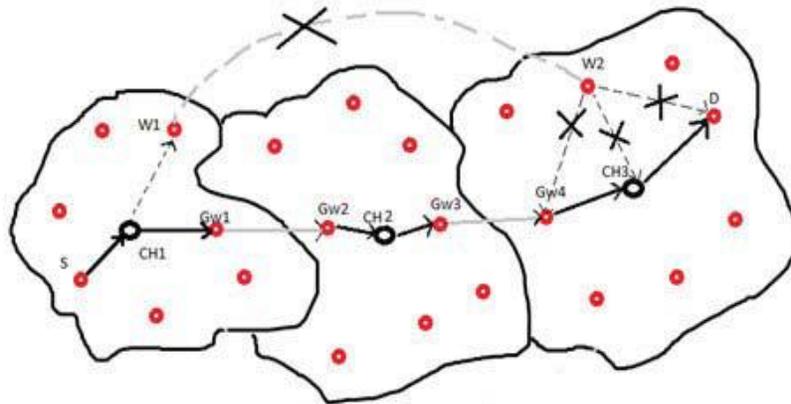


Fig. 2 Selection of Route

When a source has to send a RREQ, it sends it to its CH. The CH uses its private key to digitally sign the packet. The CH checks if the destination is a member node. If yes, it sends the signed packet to the destination node. If not, it forwards the RREQ to all of its GW nodes (multicast). The GW node checks if the packet has come from its own CH by using the public key of the CH to verify the digital sign. The GW node then forwards the RREQ to its corresponding GW node. The communication is done through Gateway and Cluster Head further until the packet is reached to Destination as shown in the fig 2 above. The performance of the proposed scheme is evaluated with and without the presence of a wormhole and is compared against traditional routing protocol in MANETs, AODV. We choose not to compare our proposed technique with any of the techniques. On the other hand, our proposed technique works efficiently in all the scenarios (including high speed links, sparse density, colluding nodes separated by very few hops without using additional hardware like GPS, directional antennas etc.). We use Java Simulation for simulating the network. The protocol succeeds in preventing a wormhole attack as the wormhole path cannot successfully satisfy the security conditions imposed by the unique digital sign of each CH node.

V. 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 attack along with their advantages and drawbacks are also discussed. Finally we introduced a novel technique for the prevention of Wormhole attack. Compared to traditional routing protocol, our proposed technique improves data security via robustness against the wormhole attack. It integrates principles of clustering and digital signatures during discovery and establishment of routes in reactive routing protocols. Moreover this technique is independent of any special hardware, time synchronization or density requirements.

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. Kandwal, "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] S. Keer and A. Suryavanshi , To prevent wormhole attacks using wireless protocol in manets, In *Int'l Conference on computer science and technology |ICCCT'2010*.
- [10] 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.
- [11] Mokube and M. Adams, "Honeypots: concepts, approaches, and challenges," in *Proceedings of the 45th annual southeast regional conference*. New York, USA: ACM, 2007.
- [12] T. H. project, "Know your enemy," July 2000. [Online]. Available: <http://project.honeynet.org/papers>.