RESEARCH ARTICLE OPEN ACCESS

A Survey on Detecting Wormhole Attack in Manet

Bipin N. Patel[1], Prof. Tushar S. Patel[2]
[1]M. Tech.(CSE-Student), Comp. Engg. Dept., SPBP Engg. College, Linch, Gujarat, India
[2]Information Tech. Dept., SPBP Engg. College, Linch, Gujarat, India

Abstract
A Mobile Ad Hoc Network (MANET) is a self organizing, infrastructure less, multi-hop network. The wireless and distributed nature of MANETs poses a great challenge to system security designers. Ad hoc networks are by nature very open to anyone. Anyone with the proper hardware and knowledge of the network topology and protocols can connect to the network. This allows potential attackers to infiltrate the network and carry out attacks on its participants with the purpose of stealing or altering information. A specific type of attack, the *Wormhole attack* does not require exploiting any nodes in the network and can interfere with the route establishment process. It does not require any cryptographic primitives. This attack targets specifically routing control packets, the nodes that are close to the attackers are shielded from any alternative routes with more than one or two hops to the remote location. All routes are thus directed to the wormhole established by the attackers. The entire routing system in MANET can even be brought down using the wormhole attack. We have presented several existing techniques to detect wormhole attack in mobile ad hoc networks.

Keyword:-Wormhole attack, Tunneling, Security, Malicious Node

I. Introduction

A mobile ad hoc network is comprised of mobile hosts that can communicate with each other using wireless links. It is also possible to have access to some hosts in a fixed infrastructure, depending on the kind of mobile ad hoc network available. Some scenarios where an ad hoc network can be used are business associates sharing information during a meeting, emergency disaster relief personnel coordinating efforts after a natural disaster such as a hurricane, earthquake, or flooding, and military personnel relaying tactical and other types of information in a battlefield. MANETs are originally motivated by military applications such as border surveillance and battlefield monitoring. Today MANET can be used in many civilian applications, including home automation, healthcare, traffic control and habitat/environment monitoring.

In wireless network many types of attacks can be initiated but most of them are relatively easy to detect because of their property of dramatically altering the network statistics but one different type of attack we have consider is very important when considering security issues of network, is wormhole attack, which is difficult to detect & can harm by directing important data to unauthorized nodes. During the route discovery process, a wormhole can relay route request and response messages between distant nodes, creating the appearance of shorter routes to destinations. Since the wormhole can be anywhere along a route, a source will have to detect its existence somewhere along the route when a node sets up the route (on-demand). Security comes from attacks. If no attacks are there, there is no need for security. Section II describes various possible attacks in MANET. Section III describes wormhole attack and its modes. Section IV describes various possible countermeasures for wormhole attack in MANET. Finally, conclusion is presented in section V.

II. Various Attacks in MANET

Below are some examples of attacks that can be launched against MANET routing protocols.

(1) Black Hole Attack

In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. The attacker will then receive the traffic destined for other nodes and can then choose to drop the packets to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack by redirecting the packets to nodes pretending to be the destination.

(2) Spoofing

A node may attempt to take over the identity of another node. It then attempts to receive all the packets destined for the legitimate node, may advertise fake routes, and so on. This attack can be prevented simply by requiring each node to sign each routing message (assuming there is a key management infrastructure). Signing each message may increase the bandwidth overhead and the CPU utilization on each node.

(3) Modifying Routing Packets in Transit

A node may modify a routing message sent by another node. Such modifications can be done with the intention of misleading other nodes. For example, sequence numbers in routing protocols such as AODV are used for indicating the freshness of routes. Nodes can launch attacks by modifying the sequence numbers so that recent route advertisements are ignored.

(4) Packet Dropping

A node may advertise routes through it to many other nodes and may start dropping the received packets rather than forwarding them to the next hop based on the routes advertised. Another variation of this attack is when a node drops packets containing routing messages. These types of attacks are a specific case of the more general packet dropping attacks.

(5) Wormhole Attack

In this attack adversaries can collude to transport routing and other packets out of band (using different channels). This will interfere with the operation of the routing protocols.

(6) Rushing Attack

In this case, an adversary can rush some routing packets towards the destination, leading to problems with routing.

Among all this attack, wormhole attack is very hard to detect because it does not require any cryptographic break. Without knowing any security material am attacker can launch the attack.

III. Demonstration of a Wormhole Attack

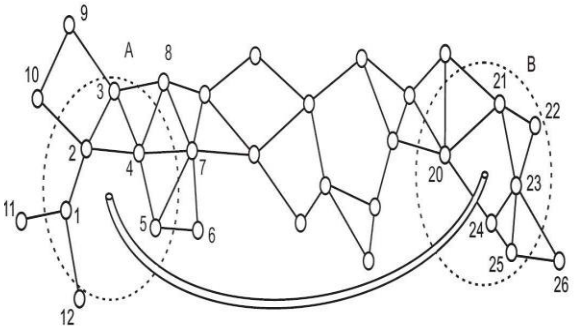

Figure.:-1 Demonstration of a wormhole attack.

A typical Tunneling attack requires two or more attackers - malicious nodes - who have better communication resources than regular sensor nodes. The attacker creates a low-latency link (i.e. high-bandwidth tunnel) between two or more attackers in the network. Attackers promote these tunnels as high-quality routes to the base station. Hence, neighboring sensor nodes adopt these tunnels into their communication paths, rendering their data under the scrutiny of the adversaries. Once the tunnel is established, the attacker collect data packets on one end of the tunnel, sends them using the tunnel (wired or wireless link) and replays them at the other end as shown in fig. 3.1

Wormholes are hard to detect because the path that is used to pass on information is usually not a part of the actual network. Interestingly, a wormhole itself does not have to be harmful; for it usually lowers the time it takes for a package to reach its destination. But even this behavior could already damage the operation, since wormholes fake a route that is shorter than the original one within the network; this can confuse routing mechanisms which rely on the knowledge about distance between nodes. Wormholes are especially dangerous because they can cause damage without even knowing the protocols used or the services offered in the network. In a wireless network, it is relatively easy to eavesdrop on the communication and forward the packets to other known nodes before the packet sent within the network arrives. This, for example, might be harmful if the data within the packet is altered to contain different information than the original.

The wormhole attack can be launched in two different modes. In the hidden mode, the attackers do not use their identities so they remain hidden from the legitimate nodes. In fact, the attackers act as two simple transceivers which capture messages at one end of the wormhole and replicate them at the other end. In this way, they can make a *virtual link* between two far-off nodes called “tunnelling” of the messages. The main characteristic of this attack is attacker does not require any cryptographic keys to launch the wormhole attack in the hidden mode.

In participation mode, the attackers can launch a more powerful attack by using valid cryptographic keys. In this mode, the attackers make no virtual links between the legitimate nodes. In fact, they participate in the routing as legitimate nodes and use the wormhole to deliver the packets sooner or with smaller number of hops. As in the hidden mode, the attackers can drop data packets after being included in the route between the source and the destination. The wormhole attack can affect network routing, data aggregation and clustering protocols, and location-based wireless security systems.

IV. Related Work

4.1 Using Secure Localization

Lazos *et al*. [1] has used a *Local Broadcast Key* (LBK) based method to set up a secure *adhoc* network against wormhole attacks. In other words, there are two kinds of nodes in their network: guards and regular nodes. Guards access the location information through GPS or some other localization method and continuously broadcast location data. Regular nodes must calculate their location relative to the guards' beacons, thus they can distinguish abnormal transmission due to beacon retransmission by the wormhole attackers. All transmissions between node pairs have to be encrypted by the local broadcast key of the sending end and decrypted at the receiving end. In addition, special localization equipment has to be applied to guard nodes for detecting positions.

4.2 Using Two-hop Routing Information

Khalil et al [2] propose a protocol for wormhole attack discovery in static networks. In this approach, once deployed, 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 are, in this approach they also know who the neighbors' neighbors are, they can take advantage of two hop, rather than one-hop, neighbors' information. This information can be exploited to detect wormhole attacks. Also, nodes observe their neighbors' behavior to determine whether data packets are being properly forwarder by the neighbor.

4.3 Packet Leash Approach

Another approach to detect closed wormholes is *Packet Leash*, which was proposed by Hu, Perrig and Johnson [3]. The leash is the information added into a packet to restrict its transmission distance. In the geographical leashes, the location information and loosely synchronized clocks together verify the neighbor relation. Each node, before sending a packet, appends its current position and transmission time to it. The receiving node, on receipt of the packet, computes the distance to the sender and the time it took the packet to traverse the path. The receiver can use this distance anytime information to deduce whether the received packet passed through a wormhole or not. In temporal leashes, the packet transmission distance is calculated as the product of signal propagation time and the speed of light. In Temporal Leashes, all nodes are required to maintain a tightly synchronized clock but do not rely on GPS information.

4.4 Using Directional Antenna

Hu and Vans propose a solution to wormhole attacks for ad hoc networks in which all nodes are equipped with directional antennas in [4]. 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. The adoption of directional antenna by mobile devices can raise the security levels.

4.5 Hop Count Analysis Method

The method of detecting wormhole using hop count analysis is presented by Shang, Laih and Kuo in [5]. This method selects routes and avoids the wormhole resulting in low cost and overhead. It does not identify the wormhole, but simply avoids it. Author has proposed multipath routing protocol to avoid wormhole attacks based on a *hop-count analysis* scheme. It is a highly efficient protocol which does not require any special supporting hardware. The protocol is designed to use split multipath routes, so the transmitted data is naturally split into separate route. An attacker on a particular route cannot completely intercept (and subvert) the content. The proposed scheme has high efficiency and very good performance with low overhead. In addition, this scheme does not require additional hardware or impractical assumptions of the networks. Hence, it can be directly used in MANET.

4.6 Trust Based Approach

Jain and Jain [6] present a novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network. This scheme does not require any cryptographic means**.** In this method, trust levels are derived in neighboring nodes based upon their sincerity in execution of the routing protocol. This derived trust is then used to influence the routing decisions. If the trust level is below threshold level then the node is declared as compromised node. All the nodes stop communication with this node.

4.7 Time and Trust Based Approach

Ozdemir *et al*. [7] proposed a time and trust-based wormhole detection mechanism. The proposed technique combines a time-based module with a trust-based module to detect compromised nodes that send false information. These two systems run in parallel. Time-based module acts in three steps: in the first step, neighboring nodes are specified for each node. In the second step each node finds the most appropriate path to the base station. Finally, in the third step, the algorithm investigates whether there is wormhole in the network. Malicious nodes on the path can mislead the time-based module by providing incorrect information. To prevent this problem, trust-based module constantly observes the first module and calculates trust values of neighbor nodes. These values are used to modify the path next time.

Following table shows comparison of various existing methods.

Table -1: comparison of various existing methods.

Method	**Comments**
Using Secure Localization [1]	Require GPS
Using two-hop routing information [2]	Every node has information about two hop neighbor
Geographical Packet Leash [3]	Require GPS Coordinates of every node.
Temporal Packet Leashes [3]	Require tightly synchronized clocks.
Using Directional Antenna [4]	Require directional antenna on all nodes
Hop count analysis [5]	Can detect wormhole attack but can not pinpoint the location of a wormhole.
Trust Based Method [6]	It does not require any extra hardware
Time and Trust Based Approach [7]	Both the modules run in parallel.

V. Conclusion

Security is very crucial for MANET. Wormhole is very dangerous compared to all the possible attacks on MANET because it does not require any cryptographic secret and completely disturb the routing process. We have presented several existing methods to detect wormhole attack in mobile ad hoc networks. Many solutions have been proposed to detect the wormhole attack but still it is an active research area.

References

[1] Lazos, L.; Poovendran, R.; Meadows, C.; Syverson, P.; Chang, L.W. Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. In *IEEE WCNC 2005*, Seattle, WA, USA, 2005; pp. 1193–1199.

[2] Khalil, S. Bagchi, and N. B. Shroff. LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks. In *Dependable Systems and Networks (DSN)*, pages 612–621, Jun 2005.

[3] Hu, Y.C.; Perrig, A.; Johnson, D.B. Wormhole Attacks in Wireless Networks. *IEEE J. Sel. Area Comm*. 2006, *24*, 370–380.

[4] L. Hu and D. Evans. Using directional antennas to prevent wormhole attacks. In Proceedings of the *Network and Distributed System Security Symposium*. 2004

[5] Jen S.-M.; Laih C.-S.; Kuo W.-C. A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET. *Sensors*. 2009.

[6] Shalini Jain and Dr.Satbir Jain. Detection and prevention of wormhole attack in mobile adhoc networks. *International Journal of Computer Theory and Engineering*, Vol. 2, No. 1 February, 2010

[7] S. Özdemir, M. Meghdadi, and Ý. Güler. "A time and trust based wormhole detection algorithm for wireless sensor networks," (manuscript in Turkish), in 3rd Information Security and Cryptology Conference (ISC'08), pp. 139−4, 2008.