A Review On: Detection and Prevention of Wormhole Attacks in MANET

Yashpalsinh Gohil, Sumegha Sakhreliya, Sumitra Menaria

(Information Technology, Parul Institutes/Gujarat Technological University, India)
(Information Technology, Parul Institutes/Gujarat Technological University, India)
(Computer Science & Engineering, Parul Institutes/Gujarat Technological University, India)

Abstract- Wireless ad-hoc network is a set of independent mobile nodes that communicates through a wireless link. Due to open medium and lack of centralized authority, ad-hoc networks are susceptible to numerous routing attacks. Wormhole Attack is one of the most severe attacks on routing protocols in which two or more malicious nodes receive packets at one point of the network and transmit them to another location by a wired or wireless tunnel. This attack is so powerful that the detection of it is difficult. This attack can form a serious threat in wireless networks, especially against many wireless ad-hoc networks and location-based wireless security systems. There is several wormhole detection and Prevention methods in the wireless ad-hoc networks which some of them are reviewed in this paper.

Index Terms- Ad-hoc Network, MANET attacks, Wormhole Attack.

I. INTRODUCTION

An *ad-hoc* network is inherently a self-organized network system without any infrastructure. Typically, the nodes act as both host and router at the same time i.e. each node participates in routing by forwarding data for other nodes and deciding to which nodes forward data next based on the network connectivity.

Most previous ad hoc networks research has focused on problems such as routing and communication, assuming a trusted environment. However, many applications run in untrusted environments and require secure communication and routing such as military or police networks, emergency response operations like a flood, tornado, hurricane or earthquake. However, the open nature of the wireless communication channels, the lack of infrastructure, the fast deployment, and the environment where they may be deployed, make them vulnerable to a wide range of security attacks.

The various holes that threaten the security of sensor networks are consist of sink/black hole, worm hole, Sybil attack and etc. They can form in sensor networks and create variations into the network topology which trouble the upper layer applications [1].In the selective forwarding attack, a malicious node firstly tries to be trusted by sender for next forwarding packet, and finally, intercepts a transmission by selecting an arbitrary packet or dropping it completely. Sinkhole attacks happen when the attacker can attract the large part of traffic to a region but if the attackers are able to forge the identities of the other nodes, the Sybil attack is occurred.

Among all attacks, the wormhole is more dangerous than the others; because this type of attack does not need to compromise a sensor in the network and it can create the other type of attack easily. On the other hand, using a cryptographic technic cannot prevent wormhole attack [2]. The remaining parts of this paper are arranged as follows. Section II gives a basic definition of Wormhole attack. Section III consists of reviewing on several wormhole detection methods. Section IV depicts a summary of wormhole detection methods that are discussed in the previous section. Section V consists of reviewing on several wormhole prevention methods finally, a conclusion is presented in Section VI.

II. WORMHOLE ATTACK

A particularly severe security attack, called *the wormhole attack*, has been introduced in the context of ad hoc networks. During this attack, a malicious node captures packets from one location in the network and "tunnels" them to another malicious node at a distant point which replays them locally. The tunnel can be established in many ways e.g. in-band and out-of-band channel. This makes the tunnelled packet arrive either sooner or with a lesser number of hops compared to the packets transmitted over normal multi hop routes. This creates the illusion that the two end points of the tunnel are very close to each other. However, it is used by malicious nodes to disrupt the correct operation of ad hoc routing protocols. They can then launch a variety of attacks against the data traffic flow such as selective dropping, replay attack, eavesdropping etc. Wormhole can be formed using, first, *in-band channel* where malicious node m1 tunnels the received route request packet to another malicious node m2 using encapsulation even though there is one or more nodes between two malicious nodes, the nodes following m2 nodes believe that there is no node between m1 and m2. Second, *out-of-band channel* where two malicious nodes m1 and m2 employ a physical channel between them by either dedicated wired link or long range wireless link shown in Fig. 1

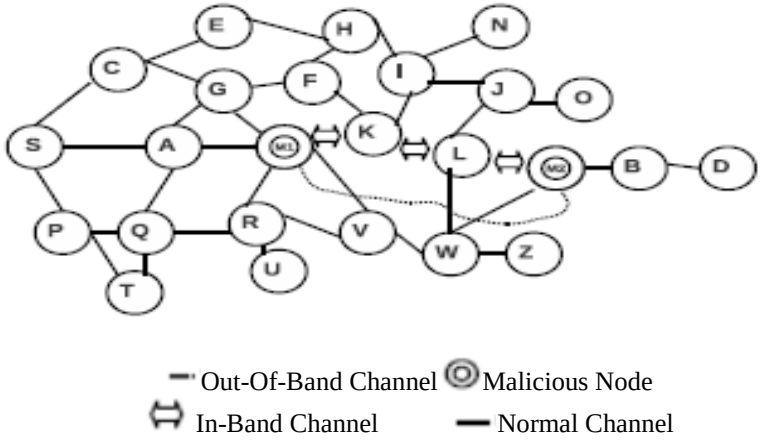

Figure 1. Wormhole Attack

When malicious nodes form a wormhole they can reveal themselves or hide themselves in a routing path. The former is an *exposed* or *open* wormhole attack, while the latter is a *hidden* or *close* one. In Fig. 1, the destination *D* notice that a packet from the source *S* is transferred through node *A* and *B* under hidden wormhole attack, while it believes that the packet is delivered via node *A,m1,m2,* and *B* under exposed wormhole attack.

III. WORMHOLE DETECTION TECHNIQUES

A. Distance and location Based: Packet Leash Technique.

Numerous methods were proposed using a packet leash technique for the detection of the wormhole attack. The packet leash (Yih-Chun Hu et.al, 2003) is the method that defends against the wormhole attack. The leashes can be grouped either into geographical or temporal. In geographical leashes, all nodes should have knowledge of its own location in the network and secure synchronized clock. Whenever a sender sends the data packet, it includes its own recent location and transmission time in header. Therefore, the receiver is capable of predicting the neighbour relation by calculating the distance between itself and source. In temporal leashes, all nodes calculate the expiration time of each packet by using light's velocity and append this expiration time in the packet's header. Destination compares its own arrival time and expiration time in the packet to detect the wormhole attack. Geographical leashes are more advantageous than temporal leashes as they do not require a tightly synchronized clock. It has the limitations of GPS technology.

B. Special Hardware Based Approaches

The Secure Tracking of Node Encounters in Multi-hop Wireless Networks (SECTOR) is a wormhole detection technique that does not depend on time synchronization (Srdjan Capkun et.al, 2003) [3].In this SECTOR method we uses Mutual Authentication with Distance-bounding (MAD) protocol for the estimation of distance between 2 nodes or users. MAD operates in the assumption that every node is appended with transceiver as extra Hardware. It accepts a single bit, carry out 2 bit XOR process over it and broadcast it which is shown in Fig 2.

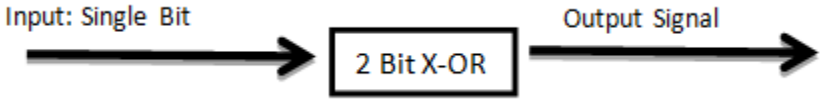

Figure 2. Process in Transceiver

Directional antenna detects the existence of wormhole nodes (Lingxuan Hu and David Evans, 2004). In this method, directional information is shared between source and destination. The destination can detect the wormhole by comparing the received signal from the malicious nodes and directional information from the source. If the both the signals from the source and intermediate nodes are different, then the wormhole link is detected.

C. Localized Encryption and Authentication Protocol (LEAP)

Localized Encryption and Authentication Protocol (LEAP) is a method which is suggested by Zhu[4].This model is based on clustering and it requires defining 4 type key for each sensor node such as,

a. Individual key that is shared with the base Station.
b. Pair wise key that is shared with another sensor node.
c. Cluster key that is shared with multiple neighbouring nodes.
d. Group key that is shared by all the nodes in the network.

This method is implemented for static or immobile sensor networks.

D. Topological Technique

Normally, a wireless multi hop network is deployed on the surface of a geometric environment, such as a plane or a rough

terrain [5]. In this method we develop principles in continuous domain, assuming continuous deployment of nodes over the geometric surface with one-to-one mapping to the points on the surface to detect wormhole nodes. A new topology space is formed after the wormhole is glued on the original surface. We subsequently analysehow the different topology spaces are generated after gluing different types of wormholes. We classify wormholes into four categories, according to their topological impacts. Fig. 3 shows the four types of wormholes.

- Class I wormhole, both of its two endpoints locate inside the surface (Fig. 3(a)).
- Class II wormhole has one endpoint inside the surface and the other on the boundary of the surface (Fig. 3(a)).
- Class III wormhole has its endpoints on two different boundaries (Fig. 3(b)).
- Class IV wormhole has both of its endpoints on the same boundary (Fig. 3(c)).

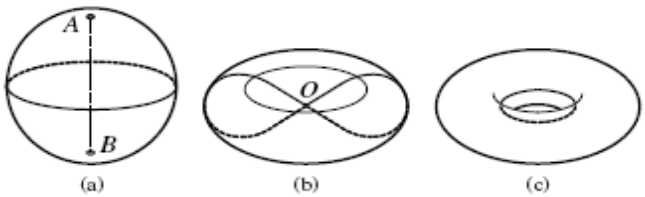

Figure 3. Classification of wormholes effect on topology

The four types of wormholes have different topological impacts on the original surface, and the complex wormhole attack can be considered as a finite combination of them. Base on their effect on topology we can detect wormhole in the topology.

E. ***Multipath Hop-count Analysis Technique***

This model is developed by Jen which is called Multipath Hop count Analysis to prevent wormhole attack for MANETs. MHA is a method based on hop-count analysis in order to avoid this attack in MANETs from the standpoint of users without any special environment assumptions [6]. In the MHA method first, the hop-count values of all routes are calculated and in the next step, a safe set of routes are chosen for data transmission. Ultimately, the packet is transmitted to destination through the safe routes due to decreasing the rate of packet that is sent by wormhole. One of the features of this method is that it does not require any specific hardware to well-done. It utilizes control packets as in RFC3561 and tries to modify it. Therefore, it used the RREQ packet is used for route discovery and the RREP packet is used for route.

F. ***Watchdog Technique***

To identifies misbehaving nodes and avoids routing through theses nodes, watchdog and pathrater. In this technique, watchdog identifies misbehaviour of nodes by copying packets and maintained a buffer for recently sent packets. The overheard packet is compared with the sent packet, if there is a match then discards that packet. If the packet is timeout, increment the failure tally for the node. And if the tally exceeds the thresholds, then node will misbehave. The implementation of watchdog technique is shown in Fig. 4.

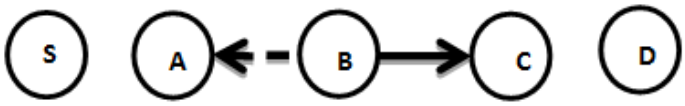

Figure 4. Watchdog Implementation

In this Fig. 4, it is assumed that bidirectional communication symmetry on every link between nodes that want to communicate. If a node can receive a message from a node at time, then node could instead have received a message from node at the time will implement the watchdog. It maintain a buffer of recently sent packets and compares each overheard packet with the packet in the buffer, when forwards a packet from to with the help of , can overhear transmission and capable of verifying that has attempted to pass the packet towards . But this approach has some limitations and it is not detect the misbehaving node during ambiguous collisions, receiver collisions, false misbehaviour and collusion. The approach is used directional antenna to detect and prevent the wormhole attack. The technique is assumed that nodes maintain accurate sets of their neighbours. So, an attacker cannot execute a wormhole attack if the wormhole transmitter is recognized as a false neighbour and its messages are ignored.

G. ***DelPHI Technique***

DelPHI provides a solution to the exposed wormhole attacks [7]. In this mechanism, delay per hop is determined in every path and it is proved that delay per hop for the genuine path is shorter than the wormhole path. If the path has noticeably high delay per hop, then the corresponding path is affected by wormhole.

H. ***Wormhole Geographic Distributed Detection***

An algorithm for the distributed detection of wormhole attack is provided by YurongXu in 2007 [8] called wormhole geographic distributed detection (WGDD). WGDD algorithm detects the wormhole attack based on the damage caused by them and the parameter used for wormhole detection is hop count. According to the hop count measured, it reconstructs the mapping details in each node and finally it exploits diameter feature to detect distortions caused by malicious nodes. WGDD algorithm is effective in finding the exact location of the wormholes.

I. ***TrueLink: A Time Base Mechanism.***

TrueLink developed by Jakob Eriksson in 2006 is a wormhole detection technique [9] that depends on time based mechanisms. TrueLink verifies whether there is a direct link for a node to its adjacent neighbour. Wormhole detection using TrueLink involves 2 phases namely rendezvous and validation. The first phase is performed with firm timing factors in which nonce exchange between two nodes takes place. In the second phase, both the nodes authenticate each other to prove that they are the originator of corresponding nonce. The major disadvantage is that TrueLink works only on IEEE 802.11 devices that are backward compatible with a firmware update. A round trip time (RTT) approach is emerged to overcome the problems in using additional hardware. The RTT is the time taken for a source node to send RREQ and receive RREP from destination. A node must calculate the RTT between itself and its neighbouring nodes. The malicious nodes have higher RTT value than other nodes. In this way, the source can identify its genuine and misbehaving neighbours. This detection technique is efficient only in the case of hidden attacks.

J. Secure Neighbour Discovery and Monitoring Based Approach

This is provided by Issa Khalil in 2008 [10] which uses local observation schemes to prevent malevolent nodes in the vicinity. The position of each node in the network is traced by central authority and it is capable of even isolating the malicious nodes globally. The detection rate of this method decreases as the network mobility increases.

IV. SUMMARY OF VARIOUS WORMHOLE DETECTION METHODS

In the following Table 1 [11], contains all wormholedetection methods that are explained previously andalso contains the requirements of each method.

Table 1: Qualitative Comparison of Wormhole Detection Methods

Method	**Localization Information**	**Checking the Authentication**	**Hop Count Analysis**	**Others**
Distance and location Based: Packet Leash Technique.	Yes	Geographical Leashes: RSA Temporal Leashes: TIK Protocol based on TESLA	N/A	Loosely Synchronized clocks
Special Hardware Based Approaches	N/A	Mutual Authentication with Distance-bounding (MAD) protocol	N/A	Transceiver, Directional Antenna
Localized Encryption and Authentication Protocol (LEAP)	N/A	Four Type Keys	N/A	N/A
Topological Technique	Yes	N/A	N/A	Topology of Network Information
Multipath Hop-count Technique	N/A	N/A	Yes	N/A
Watchdog Technique	N/A	N/A	N/A	Maintains Buffer
DelPHI Technique	N/A	N/A	Yes	N/A
Wormhole Geographic Distributed Detection	Yes	N/A	Yes	Local Map
TrueLink : A Time Base Mechanism.	N/A	Yes	N/A	Synchronized Clocks
Secure Neighbour Discovery and Monitoring Based Approach	N/A	N/A	N/A	Central Authority

V. WORMHOLE PREVENTION TECHNIQUES

A. Path Tracing Approach

There are two phases in Path tracing approach as described below.

Phase I

The source node floods the route request (RREQ) packets through immediate neighbours towards destination. When it reaches the destination, it sends back route reply (RREP) in the reverse path. The path details are stored in the DSR routing cache. In order to detect the wormhole, we optimize the general DSR header by adding extra fields. Prior per hop distance field, per hop distance field and timestamp fields are added to the header of each packet. We consider both prior per hop distance and per hop distance so as to compare the difference between the two distances. If the difference is too large that exceeds the maximum threshold value, then wormhole is detected. All nodes that participate in the routing mechanism perform this operation.

Phase II

Each node in the network has to perform four major operations to detect the wormhole attack.

1. Compute per hop distance and compare it with the prior per hop distance.
2. Check whether the difference between prior per hop distance and per hop distance is larger than the maximum threshold value.
3. If it is larger, then the wormhole is detected and it is informed to all other nodes in the networks to provide wormhole alertness.
4. For the confirmation of wormhole attack, the number of time a link is used in a path is also checked in addition to comparison of per hop distance.
5. If DBC - DAB > RTh and FAcount > FATh then it is a wormhole link.

Path Tracing Algorithm

In this algorithm the following steps are performed to detect the wormhole attackswhich are also shown in flowchart [12] in Fig. 5.

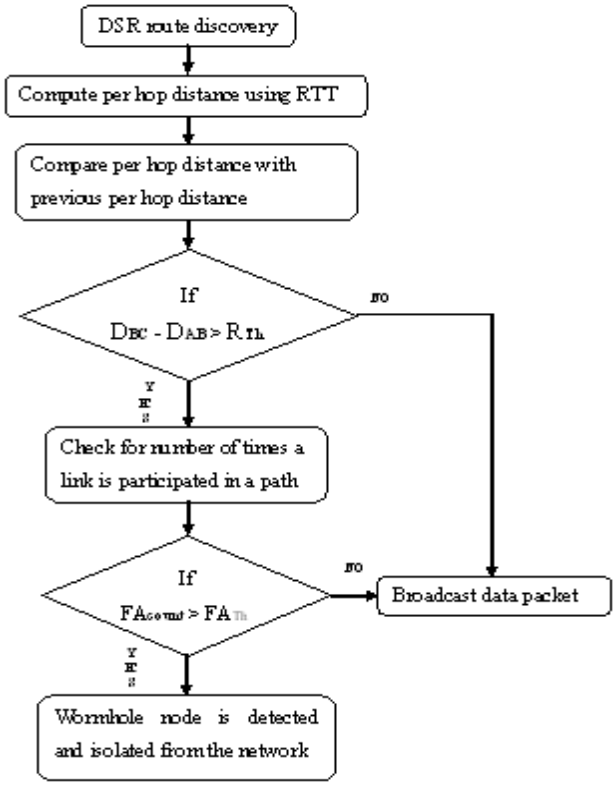

Figure 5. Flowchart Representation

Step 1: In that step RTT (based on its own clock) values are computed by Nodes in a path based on the time between the RREQ sent and RREP received.

Step 2: Compute per hop distance value using RTT value. The computed per hop distance value and timestamp are stored in each packet header.

Step 3: To identify wormhole link this information are stored. Every node in a path computes per hop distance with its neighbour and compares it with the prior per hop distance. If the per hop distance exceeds the maximum threshold range, RTh, go to step 4.

Step 4: Now check for the maximum count a link takes part in the path. If FAcount > FATh, then the link is wormhole.

Step 5: Mark the link as wormhole and the corresponding node informs other nodes to alert the network. These wormhole nodes are then isolated from the network.

B. Defence Mechanism against Wormhole Attacks in Wireless Sensor Networks

DAWWSEN is method [11] that is designed to prevent wormhole attack in WSNs withconstructing a hierarchical tree by base station – via transmitting a request packet due to find its children nodes - in which the base station is the root of tree, and the rest of sensor nodes are located in the intermediate or the leaf nodes of the tree.

This method consists of three major components such as request packet, replay packet and hopcount.When the request packet is originated by the source node, the hop-count and IDs is determined by the source node then this packet is transmitted. Each intermediate node that receives this packet should not replay it immediately. So, this packet is entered in the waiting list based on its hop-count. Once a replay timer is expired, the replay packet is prepared and sent through source node. This packet includes these fields like: The id address of the generator the replay packet (IDs), The id address of the source node that is equal to IDs request packet (IDd), The number of hop-count, The number of replayed packets (Num_Rep), The acceptance flag (Recv_Accept). Upon the replay packet is received by any nodes, each node firstly runs a timer that is called accept timer and before this timer expire, it checks its replay wait-list that is contain the id address of sender, hop-count and number of reply (Num_reply). If an entry is discovered that its ID is similar to the ID of received packet, its num_reply field will be enhanced by one else a new entry willbe created and insert to the list (Num_reply=1).

When the timer expires, this node prepares a packet (accept packet) that is contained its id (IDs), destination id that is equal to IDs of replay waitlist, and the Num_reply field and then it sends this packet to each entry in its reply list. Once a node receives an accept packet, it checks its replay list to find an entry that its id is similar to the received packet id. If this node finds a related entry, its feature in the list should update (Num_reply = Num_Rep + 1) otherwise the wormhole attack is detected and the following steps should be performed:

1. The received accept packet should be deleted.
2. Add the ID of the sender of the accept packet should be inserted into its (Not Accepted Packets (NAP) list.
3. Update its replay wait-list by resetting all values to zero.
4. In last step, the node should wait for another request packet or it can send another reply that is similar to the second item in its request list.

As a consequence, based on this method a hierarchical 3- way handshake routing tree can be made easily in order to detect wormhole attack for a multi-hop wireless sensor networks.

VI. CONCLUSION

In this paper, we reviewed the various detection and prevention mechanisms against wormhole attacks in wireless Ad-hoc networks. Along with the explanation of these methods we had done qualitative comparison of all the wormhole detection

techniques and give a brief view of all the techniques in Table 1. Overall, a significant amount of work has been done on solving wormhole attack problem. We can't say one solution is applicable to all situations. So there is choice of solutions available based on cost, need of security, type of network. Implementing more hardware for increasing security may lead better result, but can be costly, which may affect other networks need.

REFERENCES

[1] Fonseca, R., & Merino, A. S. (2004). Receiver Based Forwarding: Improving the security of Geographic Routing in Wireless Sensor Networks. Berkeley: Berkeley University.

[2] Loo, C., Ng, M., Leckie, C., &Palaniswami, M. (2006).Intrusion Detection for Routing Attacks in Sensor Networks.International Journal of Distributed Sensor Networks, pp.313–332.

[3] SrdjanCapkun, LeventeButtyan and Jean-Pierre Hubaux, 2003 "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks" SASN'03 Proceedings of 1st ACMWorkshop on Security of Ad Hoc and Sensor Networks, pp. 21-32.

[4] Zhu, S., Setia, S., &Jajodia, S. (2003). LEAP: efficient security mechanisms for large-scale distributed sensor networks. Proceedings of the 10th ACM conference on Computer and communications security (pp. 62 - 72). New York: ACM.

[5] MajidKhabbazian, Hugues Mercier, and Vijay K. Bhargava, 2009 "Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks" IEEE Transactionson Wireless Communications, Volume 8, Issue 2, pp. 736-744.

[6] Jen, S.-M., Laih, C.-S., &Kuo, W.-C. (2009). A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET. sensors, 5022-5039.

[7] Chiu, HS; Wong Lui, KS, 2006 "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks" 1st International Symposium on Wireless Pervasive Computing.

[8] YurongXu, Guanling Chen, James Ford and FilliaMakedon, 2007 "Detecting wormhole attacks in wireless sensor networks" International Federation for Information Processingproceedings on critical infrastructure protection, volume 253, pp. 267-279

[9] Jakob Eriksson, Srikanth V. Krishnamurthy, and MichalisFaloutsos, 2006 "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks" 14th IEEEInternational Conference on Network Protocols, pp. 75-84

[10] Issa Khalil, SaurabhBagchi, and Ness B. Shroff, 2008 "MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks" A*d Hoc Networks*, Volume 6, Issue 3, pp. 344-362

[11] AnkitaGupta , Sanjay Prakash Ranga,2012 "WORMHOLE DETECTION METHODS IN MANET" Internal Journalof Enterprise computing and Business System.

[12] T. Sakthivel, R. M. Chandrasekaran, 2012 "Detection and Prevention of Wormhole Attacks inMANETs using Path Tracing Approach" European Journal of Scientific ResearchISSN 1450-216X Vol.76 No.2 (2012), pp.240-252