A Review on: Various Methods of Detecting and Preventing Wormhole Attack

Deepinder Kaur Punia, Er Sukhpreet Kaur

Abstract— Mobile Ad Hoc Network are based on wireless networks composed of set of nodes that can communicate and are capable of moving. In this paper we present a survey on different wormhole detection technique. These issues are very important to secure the network .wormhole attacks are dangerous attacks we also studied about the different properties of the attack. Also briefly discussed bout the techniques used to detect the wormhole attacks occurring in the network and then compared the all the methods to one another so that a new effective method is formed. This study aims to combine some method to modify the existing method

Keywords— MANETs, Wormhole attack, Wormhole detection techniques.

1 Introduction

1.1 MANETS

Mobile ad hoc network are the ad hoc network that are used for the communication between two entities. MANETs consist of peer to peer, self-forming, self healing networks. MANETs are continuous self-configuring, infrastructure less network of mobile device connected without the wires. MANETs are a type of ad hoc network that can change their locations and can configure itself accordingly. They are mobile therefore uses wireless connections to connect with the various networks. The connections can be through Wi-Fi connection, or with the help of other mediums that can range from cellular to satellite transmission. Some of them are connected with the help of local area networks and some are connected on the basis of internet according to the application. The MANETs do not have a centralized administration machine.

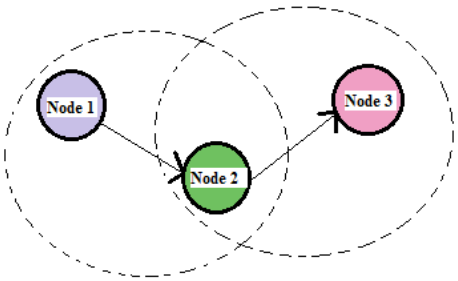


Fig 1: Example of Mobile Ad-hoc Network [1]

Fig1: Shows a simple ad-hoc network with 3 nodes. Node 1 and node 3 are not within range of each other; however the node 2 can be used to forward packets between node1 and node2.

- *Deepinder Kaur Punia* CSE Department *Shri Guru Granth Sahib World University, India, E-mail: deepinder.punia321@gmail.com*
- *Sukhpreet Kaur* CSE Department *Shri Guru Granth Sahib World University, India,E-mail: preetsukh@gmail.com*

The node 2 will act as a router and these three nodes together and these three nodes together form an ad-hoc network [1].

1.2 Characteristics of MANETs

1. No centralized infrastructure, they don't have any centralized server due to lack of centralized management mutual trust for nodes is needed.
2. Provides high mobility and device portability that enables to connect the nodes with the network and helps in communicating.
3. Each node act as autonomous terminal, which indicates that each node can function both as a host and a router.
4. Light weight terminals, MANETs have less CPU capability, low power storage and small memory storage.
5. Communication between the nodes is via wireless means generally through radio waves
6. .MANETs does not need any kind of infrastructure. They are infrastructure less networks.
7. Dynamic topology, nodes in the network are free to move with different speeds can also update routing frequently.
8. Can communicate through other intermediate nodes when data is to send to farther node, Multi-hop routing

1.3 Merits OF MANETs

1. These networks can be setup at anywhere at any place and at any time.
2. Network works without pre existing infrastructure.
3. They provide access to information and services headless of geographical locations.

4. Vigorous in nature due to decentralized administration.
5. Are Self-configuring network node.
6. Less expensive then the wired network.
7. Congruous towards adding more nodes to the network.

1.4 Demerits of MANETs

1. Security; security protocols for wired network cannot work for ad-hoc network.
2. Limited battery life; devices used in these networks have limited power supply to maintain the size and weight of the devices.
3. Bandwidth; wireless links have lower capacity than the networks that are based upon some infrastructure.
4. Dynamic topology; nodes can join and leave the network and can move dynamically the trust may not be disturbed.
5. Authorized facilities; mutual trust is vulnerable to attacks.
6. Fewer resources; Limited resources to mention the problem of limited security.
7. Route challenges, network topology is dynamic in nature; hence the running session can suffer from path breakage.

1.5 Application of MANETs

With the increase of portable devices as well as progress in wireless communication, ad hoc networking is gaining importance with the increasing number of widespread application. Ad hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is inconvenient to use ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to from the network. The set of applications for MANETs is diverse, ranging from large scale, mobile, highly dynamic networks to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services will be generating for the new environment [11]. The application of the MANETs includes:

1. Military or police exercises
2. Business meetings
3. Local levels
4. Commercial sectors
5. Medical services
6. Personal area network and Bluetooth
7. Robust data acquisition.
8. Education.

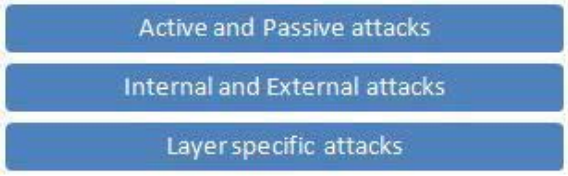
2. Security Attacks

Keeping in mind various demerits of MANETs the mobile ad hoc networks are insecure, as a result we need find the solutions for securing the MANETs. In this we studied some of schemes that are useful to protect the nodes from attacks.

1. Authentication
2. Confidentially
3. Integrity
4. Non repudiation
5. Authorization
6. Anonymity
7. Resilience to attacks.

2.1. Types of Security Attacks

There are many kinds of attack that occurs in MANETs. These attacks are differentiated on the basis of their behavior.



Active Attacks and Passive Attacks

Active are very harsh attacks for the network that fore stall the message flow in the network. Main goal of this attack is to attract all the data packets to attacker node to incapacitate network. Passive attacks are those attacks that do not alter the message flowing in the network but tries to decode the important information from it. This type of attacks does not also show any kind of effect on the routing protocols as a result they are hard to detect.

Internal and External Attacks

External attacks are the simple attacks that are carried out by the external nodes not trusted by the network. The external attacks are responsible for interrupting the nodes form their services, cause of congestion in the network and making false routing information. On the other hand internal attacks are caused by nodes that resist in the domain of the network. Internal attacks are more dangerous than the external attacks as the nodes that are the part of the network knows all the valuable information have authorized access as a sincere node.

Layer Specific Attacks

The attacks are further classified on the basis of layers of the Internet model.

1. Application Layer Attacks: Data Corruption and Repudiation.
2. Transport Layer Attacks: Session Hijacking and SYN Flooding Attacks
3. Network Layer Attacks: Wormhole Attack, Black-hole Attack, Rushing Attacks and Sinkhole Attack.

4. Data-Link Layer Attacks: Traffic Analysis and Location Disclosure Attacks, Denial of Service Attacks
5. Physical Layer Attacks: Eavesdropping and Active Interference.

3. Wormhole Attack

Network layer is third layer of the OSI reference model. Main function of this layer is to provide the service of exchanging the data over the network between the nodes/devices. Securing the network layer is an important issue so that the data used for the communication process is also secured. Wormhole attacks comes under the category of attacks occurring at the network layer Wormhole attacks is one of the most dangerous attacks, is executed in MANETs. In this attack the attacker records the data packet at the one end of the network and tunnels them to another end of the network. The tunnel can be made ether by wired links or through a wireless transmission.

Wormhole attack takes place when the packets are forwarded between the nodes through the communication links. Their exist one malicious node in between the existing path which forwards the packet to the destination by making a tunnel which creates a illusion that the path is shorter than the existing. Due to wormhole attack a loss of more data packets in the network and increase in the hop count is noticed.

3.1 Classification of Wormhole Attacks

Wormhole attack is classified into different categories based upon their tunneling mechanism they are:

1) In-band wormhole
2) Out-of-band wormhole

In-band Wormhole

These attacks can be launched very easily by any node in the network. The attacker forms a link between the two end points using the other external nodes for communication. The In-band attacks are simple to be implemented they also take place in real life.

Out of band Wormhole

These are those kind of attacks which forms the direct link between the two end points, these type of attacks can are more difficult to launch as they require external hardware to support the communication between the end points.

3.2 Types of Wormhole Attacks

The wormhole attack is divided into three types.

Open Wormhole Attack

In this mode the attacker includes themselves into the packet header. Nodes present in the network are aware of the attacker's node presence in their pat but they would think that they are direct neighbors.

Closed Wormhole Attack

In this mode no modification is done to data packets but they are simply broadcasts the packets.

Half- open Wormhole Attack

In this mode the attacks they do modifies the data packet at one end but not on the other and broadcast the packets from one end to another. Both source and destination feels them one hop away, thus fake neighbors are created.

3.3 Methods to Prevent Wormhole Attack

1. Location and Time based Approaches

Hu et al. in 2003 [7] proposed a mechanism, called packet leashes, They describe two approaches to achieve this goal, one is a space based approach, called as Geographical Leashes which establishes an upper bound on the distance that a packet can travel. Before sending a packet, node appends its current position and transmission time to it. On receiving packet, receiving node computes the distance with respect to the sender and the time required by the packet to traverse the path. The receiver can use this distance information to deduce whether the received packet passed through a wormhole or not. The drawback of this scheme is that, each node must know its own location and all nodes must have loosely synchronized clocks. In Time based approach called as Temporal Leashes the sending node includes in the packet the time at which it sent the packet, ts ; when receiving a packet, the receiving node compares this value to the time at which it received the packet, tr. The receiver is thus able to detect if the packet traveled too far, based on the claimed transmission time and the speed of light. Alternatively, a temporal leash can be constructed by instead including in the packet an expiration time, after which the receiver should not accept the packet; based on the allowed maximum transmission distance and the speed of light, the sender sets this expiration time in the packet as an offset from the time at which it sends the packet. The drawback of this is that they need highly synchronized clocks.

2. Delphi

The hop count is the minimum number of node-to-node transmissions. This method uses protocol Delay per Hop Indicator (Delphi) [5] proposed by Hon Sun Chiu and King-Shan Lui, can detect both hidden and exposed wormhole attacks. In DelPHI, attempts are made to determine every available disjoint route between a source and a destination. To identify wormhole, delay time and length of each route are measured and the average delay time per hop along each route is computed. According to this, the route containing a wormhole link will have a greater Delay per Hop (DPH) value. This mechanism can detect both modes of wormhole attack; however, pinpoint the location of a wormhole cannot be determined.

3. 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.

4. True link: A Time Based Mechanism

Jakob Eriksson in 2006 introduced the time based mechanism [6] 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. 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 neighboring nodes. The malicious nodes have higher RTT value than other nodes. This detection technique is efficient only in the case of hidden attacks.

5. Wormhole Geographical Distributed Detection

An algorithm for the distributed detection of wormhole attack is given by Yurong Xu [8] in 2007 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.

6. Special Hardware 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 3.

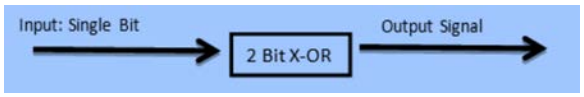


Fig 4: Processes in Transceiver

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.

7. Multi Hop-count Technique

This model is introduced 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 [4]. 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. Therefore, it used the RREQ packet is used for route discovery and the RREP packet is used for route.

8. Graph Theory

L. Lazos [12] designed a method to characterize wormhole attack in ad hoc network that called " a graph theoretic approach". According to this method, to secure an ad hoc network from wormhole attacks a Local Broadcast Key (LBK) was considered and provided a distributed mechanism for establishing them in random deployed networks. To succeed these approach its need to use a GPS and special localization equipment. This method is not readily applicable to mobile network.

3.4 Comparison of Various Detection Methods

In the following table 1 contains all the methods that are discussed above for handling the wormhole attack and their requirements are also listed.

TABLE.1. Comparison of Various Wormhole Detection Methods

Technique	Localization Information	Synchronization	Hop Count	Others
Geographical Leash	Yes	Low	N\A	Based upon Protocol RSA
Temporal Leash	Yes	High	N\A	TIK Protocol based upon TESLA
Delphi	N\A	N\A	Yes	Delay
Watchdog	N\A	Yes	N\A	Maintain Buffers
True Link: a time based approach	N\A	Yes	N\A	Synchronized Clocks are required
Wormhole Geographical Distribution Detection	Yes	N\A	Yes	Local Maps
Special Hardware	N\A	N\A	N\A	Direct Antenna
Multihop-count Technique	N\A	N\A	Yes	N\A
Graph Theory	N\A	N\A	N\A	Protocol LBK is used

REFERENCES

[1] Aarti and Dr. S.S Tyagi "Study of MANETS: "Characterstics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering.

[2] Kuldeep Sharma, Neha Khandelwal, Prabhakar.M "An Overview of Security Problem in MANET",International Journal of Advanced Research in Computer Science and mobile computing.

[3] SrdjanCapkun, LeventeButtyan and Jean-Pierre Hubaux SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks‖ *SASN'03, in 1st ACM Workshops*,pp.21-32.

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

[5] Chiu, HS; Wong Lui, KS, 2006 —DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks in IEEE.

[6] Jakob Eriksson, Srikanth V. Krishnamurthy, and MichalisFaloutsos, 2006 —TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks in IEEE, pp. 75-84 ,2006

[7] Y. C. Hu, A. Perrig and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", *(INFOCOM)*,2003, pp. 1976-1986.

[8]Y.C. Hu, A. Perrig, and D.B. Johnson. "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas of Communications*, Vol. 24, No. 2, pp. 370–80, 2006.

[9] Samiksha Suri"Different methods and approaches for the detection and removal of Wormhole Attack in MANETS ", IJETR, ISSN:2321-0869, VOLUME-1, Issue-5,July 2013

[10] Rashmi Vijaywargiya , Prof. Kamlesh Chopra "Comparative Study of Various Method of Detection of Wormhole Attack in MANETS, IJETR, ISSN 2347-7539

[11] A.Vani, D.Sreenivasa Rao, "Simple Algorithm For Detection and Removal OF Wormhole Attack for Secure Routing in Ad hoc Wireless Network", 2011.

[12]Lazos,L, R,Syverson,& Chang,L(2005). Preventing wormhole attack on wireless ad hoc comm: a graph approach. wireless. And networking network Washington: IEEE Confrence,pp:1193-1199.