Survey on Wormhole Attack Detection Method in MANET

Rajanikant Patel 1 Mr. Chandresh Parekh 2
1 PG-WIMC Student, Department of Computer Engineering, Gujarat Technological University, Gujarat
2 Head of Department & Assistant Professor at Govt. Eng. College, Gandhinagar, Gujarat, India

Abstract— In Mobile Adhoc Network applications are deployed, security emerges as a central requirement. There are many attacker attacks on the MANET. In this paper we introduce avoid wormhole attack. The wormhole attack is possible even if the attacker has not compromised any hosts, and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. Security in mobile ad hoc networks is difficult to achieve, because of the dynamic topologies, limited resources, the absence of a certification authority and the lack of a centralized monitoring point [1]. Most of the attacks in MANETs are routing protocol attacks. The wormhole effect is caused by attempts to draw all network traffic to malicious nodes that broadcast fake shortest path routing information. The wormhole nodes should be detected and detached as early as possible. Incremental Flexible Frequency Discretization (IFFD) is a recently proposed discretization approach for Naïve Bayes (NB). IFFD performs satisfactory by setting the minimal interval frequency for discretized intervals as a fixed number. In this paper, we first argue that this setting cannot guarantee that the selecting MinBinSize is on always optimal for all the different datasets. So the performance of Naïve Bayes is not good in terms of classification error. We thus proposed a sequential search method for NB: named Flexible IFFD. Experiments were conducted on 4 datasets from UCI machine learning repository and performance was compared between NB trained on the data discretized by FIFFD, IFFD, and PKID.

Keywords: Discretization, incremental, Naïve Bayes.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) face different levels of challenges due to its varying mobile characteristics. The major goal of these networks is to bring the idea of mobility into real-life networks. Even though there are multitudes of applications offered by MANETs, there are certain challenges that we need to overcome. These networks are known for their infrastructure less characteristics. The nodes are free to move anywhere and hence the communications links may be broken at any moment.

MANETs do not have any controlling point to regulate the traffic. Each node in the MANET has to take care of the routing aspect as well. There are many routing protocols available for routing in ad-hoc networks. The routing protocols for MANETs are broadly classified into two types proactive and reactive. The protocols like DSDV, OLSR, OSPF, TBRPF, FSR and FSLS are proactive protocols which will use periodic messages in order to know the network topology. The reactive protocols include AODV, DSR. The hierarchical routing contains the protocols like HSR, CGSR, ZRP, and LANMAR. In the geographic position assisted protocols we have GEOCAST, LAR, DREAM and GPSR [8]. MANETs are infra-structure-less and will have dynamically changing topologies which make them vulnerable to many kinds of failures and at-tacks. Most of the attacks in MANETs target the routing protocols. The mobility of nodes makes it more vulnerable to routing protocol attacks. By attacking the routing protocols, the attackers can absorb network traffic or inject themselves into the path between the source and destination. Some latest attacks on the routing protocol in MANETs are, wormhole attack, black hole attack, grey-hole attack, byzantine attack, rushing attack. Sinkhole attacks, if carried out successfully, can cause all of the above mentioned attacks possible. So it is important to detect the sinkhole nodes and prune them from the MANET. The nodes in the MANET should cooperate with each other to make the communication possible. Here comes the mutual understanding. We are going to use this property to detect the sinkhole nodes in the network.

II. WORMHOLE ATTACK

Tunneling of packets from one point to another location by an attacker is termed as wormhole attack in MANETs. Initially the attacker records the targeted packets at a specific location and then it is tunneled to another location in the network. If the control packets are captured and tunneled, it would result in the failure of routing mechanism. It is considered as a serious threat and the tunnel created between two conspiring attackers is termed as “wormhole”.

Tunneling attack is also called wormhole attack. In a tunneling attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point. It is called tunneling attack because the colluding malicious nodes are linked through a private network connection which is invisible at higher layers.

A. PROPOSED DETECTION METHOD

The different methods of wormhole detection in MANET.
1) Distance and location based solution
2) Special Hardware Based Approaches
3) Topology Based Solution
4) Hop Count and Delay Based Solutions
5) Synchronized Clock Based Solution
6) Key based solution
7) Neighbor-Based solutions

1) Distance and Location Based Techniques:
Most of the proposed wormhole solutions in the literature are based on location or time. Packet leashes have been proposed and specifically two types of packet leashes: geographical and temporal were considered in. The main idea is that by authenticating either an extremely precise timestamp or location information combined with a loose timestamp, a receiver can determine if the packet has traversed an unrealistic distance for the specific network technology used. Packet leashing was added to each packet on each link to restrict the transmission distance of the packet[4]. Two types of packet leashes could be added into the packet.

One is geographical leash in which the sender inserts its own position and sending time into the packet, the receiver will estimate the maximum distance between the sender and itself based on its own position and receiving time [5]. If the distance exceeds the transmission range, the packet will be discarded. The other type is temporal leash. This mechanism assumes that the maximum transmission speed of radio signal is the speed of light, thus the expiration time of a packet can be estimated using the maximum transmission range and the speed of light. The expiration time of the packet is inserted into the packet, and then the receiver can check whether the received packet has expired or not based on its receiving time [5]. A drawback of packet leashes is that it requires extremely tight time synchronization and GPS.

2) Special Hardware Based Techniques:
The Secure Tracking of Node Encounters in Multi-hop Wireless Networks (SECTOR) is a wormhole detection technique that does not depend on time synchronization.

SECTOR 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 extra hardware called transceiver. It accepts a single bit, carry out 2 bit XOR process over it and broadcast it[7]. Directional antenna detects the existence of wormhole nodes. In this scheme, directional information are 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.

3) Topology Based Solution:
The impact of wormhole attack is analyzed in two. In the first circumstance, an attacker aims to disrupt the communication to maximum extent. In the second circumstance, two malevolent nodes target a particular node. In this scenario, an attacker may have almost entire communication control over the network. The first scenario is strictly based on timing constraints while the second scenario is not so. In this approach, the nodes do not want to communicate with all its adjacent nodes and no need to compute the signature instead it stamps the data packet with the transmission time. The effects and symptoms of wormhole attacks are analyzed using topological techniques in.

4) Hop Count and Delay Based Solutions:
An algorithm for the distributed detection of wormhole attack is provided in 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[7]. DelPhi is an effective technique to detect wormhole attacks that uses delays of various paths for detection. It classifies the wormhole attacks as two divisions such as hidden and exposed[2]. DelPhi provides a solution to the exposed wormhole attacks. 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. EDWA is an End to End Detection of Wormhole Attack in Ad-hoc network.[5] The EDWA mechanism first estimates the shortest hop count among sender and receiver. When the hop count is less than the estimated hop value, it can be concluded the existence of wormhole. [3]

5) Synchronized Clock Based Solution:
TrueLink is a wormhole detection technique that depends on time based mechanisms. TrueLink verifies whether there is a direct link for a node to its adjacent neighbor [7]. 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 nonces. The major disadvantage is that TrueLink works only on IEEE 802.11 devices that are backward compatible with a firmware update.[4] 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. In this way, the source can identify its genuine and misbehaving neighbors. This detection technique is efficient only in the case of hidden attacks.

6) Key Based Solutions:
For the key based solutions, a scheme was proposed in, and depending on location-based keys, a node-to-node authentication scheme, which is not only able to localize the impact of compromised nodes within their vicinity, but also to facilitate the establishment of pairwise keys between neighboring nodes was developed. These schemes only accept messages from authenticated neighbors and discard
those messages tunneled from multi-hop-away locations preventing thus the wormhole attack.

7) **Neighbor-Based solutions:**
A wormhole attack prevention algorithm that depends on neighbor monitoring was suggested in [1]. In this method, all nodes monitor their neighbors’ behavior 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. Even though malicious nodes have been excluded from routing in the past, the nodes have a chance of attack once more. Therefore, the information of wormhole nodes is stored at the source nodes to prevent them taking part in routing again. In [2], another method was suggested. Whenever routing takes place in the network, analysis of the frequencies of links in different routes is done. If any of the links are suspicious, then the available trust information is used to check if the link is that of a wormhole. Following the neighbor monitoring phase, a trust vector of a node containing the trust values to each of its neighbors is calculated. In the trust model used, nodes monitor neighbors based on their packet drop pattern and not on the measure of number of drops. Finally, the algorithm for detection of Wormhole is run during the routing phase. A wormhole attack detection approach based on the probability distribution of the neighboring-node-number, WAPN, which helps the nodes to judge whether a wormhole attack is taking place and whether they are in the influencing area of the attack was proposed in [3]. In worms, wormhole attack defense method was proposed. In the proposed method, each node maintains its neighbors’ information. According to the information, each node can identify replayed packets that forwarded by two attackers.

### III. CONCLUSION

Wormhole attacks in MANET can significantly degrade network performance. In wormhole attacks, as adversaries usually relay the legitimate data packets, detection of these attacks is quite complicated. In this paper, we presented the detection technique of wormhole attack. It is shown that, while a number of wormhole detection techniques have been proposed each technique has its own weakness and there is no wormhole detection technique that can detect wormhole attacks completely. Finally, by analyzing pros and cons of the existing techniques, we presented the open research issues in the wormhole detection area.

### REFERENCES


[8] Zaw Tun and Ni Lar Thein, “Round Trip Time based Wormhole Attacks Detection”, University of Computer Studies, Yangon