Mobile Ad-Hoc Networks- Attack Detection

RAKESH KUMAR GIRI
Research Scholar, Department of Computer Science & Engineering, Sunrise University, Alwar, Rajasthan

Abstract— A Mobile Ad Hoc Network (MANET) is a system of mobile wireless nodes that dynamically self-organize into arbitrary, temporary network topologies. Security is essential for mobile ad hoc networks. Security comes from attack. Without attacks, there is no need for security. Among all the attacks against mobile ad-hoc networks, wormhole attacks are very difficult to detect because an attacker does not need to know the contents of a node's secrets to launch an attack. In a wormhole attack, a malicious node receives a packet from one location and routes it to another malicious node in another area of the network, disrupting the entire routing process. Therefore, all routes will be diverted through the wormhole created by the attacker. The entire routing system in a MANET can be brought down by a wormhole attack. We have studied several existing methods for detecting wormhole attacks in mobile ad-hoc networks. Our proposed method can effectively detect wormhole attacks in mobile ad-hoc networks. Our goal is to improve the detection rate compared to existing methods.

Index Terms- MANET, WORM HOLE, ROUTING

I. INTRODUCTION

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices, has impelled a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society. In this environment a route between two hosts may consist of hops through one or more nodes in the MANET. An important problem in a mobile ad hoc network is finding and maintaining routes since host mobility can cause topology changes. Several routing algorithms for MANETs have been proposed in the literature, and they differ in the way new routes are found and existing ones are modified. The mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

The most widely considered application of a MANET is battlefield communications. The other widely considered application for MANETs is interconnection of sensors in an industrial, commercial, or military setting. Another relevant application is that of emergency response. Following are the vulnerabilities of MANET.

(1) Lack of Secure Boundaries
(2) Threats from Compromised nodes Inside the Network
(3) Lack of Centralized Management Facility
(4) Restricted Power Supply
(5) Scalability

Security comes from attacks. If no attacks are there is no need for security. Karlof and Wagner[1] describes various attacks in ad hoc networks. Due to their open nature, mobile ad hoc networks are vulnerable to several attacks such as denial of service, black hole, gray hole, wormhole, Sybil etc. Among all the attacks, detecting wormhole attack is very difficult because to launch this type of attack, the attacker does not need any cryptographic break. One malicious node records traffic in one area of the network and tunnel them to another malicious node which is located far away in another location. So whole routing process is disturbed. Detecting such attack is very crucial in mobile ad hoc network.

The rest of the paper is organized as follows:
Section II describes various attacks on MANET and description of wormhole attack.
Section III describes various existing method to detect wormhole attack.
Section IV describes our proposed method.
Section V describes result and analysis.
Finally conclusion is presented in section VI.

II. VARIOUS ATTACK IN MOBILE AD HOC NETWORKS

Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their malicious behaviors. In the mobile ad hoc networks, attacks against routing are generally classified into two categories: attacks on routing protocols and attacks on packet forwarding/delivery. Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on packet forwarding try to disturb the packet delivery along a predefined path. The main influences brought by the attacks against routing protocols include network partition, routing loop, resource deprivation and route hijack. There are some attacks against routing that have been studied and well known:

- Impersonating another node to spoof route message.
- Advertising a false route metric to misrepresent the topology.
- Sending a route message with wrong sequence number to suppress other legitimate route messages.
- Flooding Route Discover excessively as a DoS attack.
- Modifying a Route Reply message to inject a false route.
- Generating bogus Route Error to disrupt a working route.
- Suppressing Route Error to mislead others.

Because of the mobility and constantly changing topology of the mobile ad hoc networks, it is very difficult to validate all the route messages. There are some more sophisticated routing attacks, which include Wormhole attacks, Rushing attacks and Sybil attacks. The second category of attacks against routing is attacks on packet forwarding/delivery, which are not easy to detect and prevented. There are two main attack strategies in this type: one is selfishness, in which the malicious node selectively drops route messages that are assumed to forward in order to save it own battery power; the other is denial-of-service, in which the adversary sends out overwhelming network traffic to the victim to exhaust its battery power.

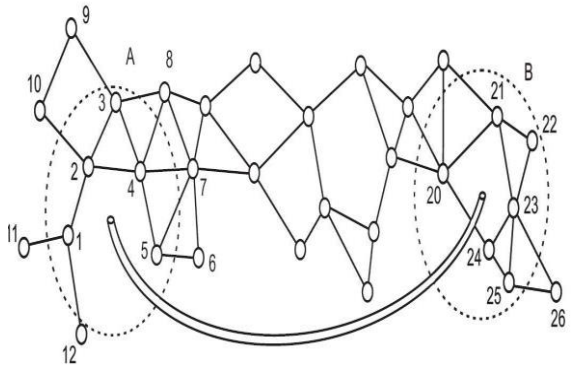


Fig.2.1 Demonstration of a wormhole attack.

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. 2.1

III. EXISTING METHODS

In an ad hoc network, several researchers have worked on pretending and detecting wormhole attacks specifically. To defend against them, some efforts have been put on hardware design and signal processing techniques. Some of the techniques we have studied are as follows:

3.1 Using Secure Localization

Lazos *et al.* [2] 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.

3.2 Using Two-hop Routing Information

Khalil et al [3] 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.

3.3 Wormhole Attack Prevention Algorithm

In [4] the author describes a method for preventing wormhole attack called as Wormhole Attack Prevention (WAP). All nodes monitor its neighbor's 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 author store the information of wormhole nodes at the source node to prevent them taking part in routing again. Moreover, the WAP has the ability of detecting both the hidden and exposed attacks without special hardware.

3.4 Distributed Algorithm using Graph Information

In [5] the author has described the distributed algorithm for wormhole detection based. The algorithm is based on unit disk graph assumption, but as mentioned it can also be extended to other cases. In a unit disk graph, two nodes in a network which are distance 1 apart cannot have more than two common neighbors which are also distance 1 apart from each other. In other words, two independent (non-neighboring) nodes cannot have more than two common neighbors which are they mutually independent. But in case of a wormhole attack, nodes in the neighborhood of one wormhole become neighbors of nodes in the neighborhood of the second wormhole and vice versa. Nodes in area *A* become neighbors of nodes in area *B* and vice versa.

3.5 Packet Leash Approach

Another approach to detect closed wormholes is *Packet Leash*, which was proposed by Hu, Perrig and Johnson [6]. 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.

3.6 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 [7]. 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.

3.7 Hop Count Analysis Method

The method of detecting wormhole using hop count analysis is presented by Shang, Laih and Kuo in [8]. 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.

3.8 Cluster Based Hierarchical Addressing Approach
The author [9] has presented cluster based Wormhole attack avoidance mechanism, where the receiver can identify whether there is a Wormhole in the routing path and avoid it during the route discovery phase. When receiver receives any packet, it checks the level-1 and level-2 cluster heads ids, and validates the route information stored in the packet. If the validation is successful then the receiver keeps the packet, otherwise it rejects it. Using hierarchical addressing, the receiver node can verify whether the packet has passed from the wormhole tunnel or not.

3.9 Trust Based Approach
Jain and Jain [10] 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.

3.10 Round Trip Time Based Approach
The proposed [11] detection is based on the RTT of the message between nodes. The consideration is that the adversary increases the number of neighbors of the nodes within the radius and shortens the path and longer the RTT value between successive nodes. Our propose mechanism consists of three phases. The first phase is to construct neighbor list for each node and the second phase is to find the route between sources to destination node. After that it finds the wormhole link to remove it.

3.11 Time and Trust Based Approach
Ozdemir *et al*. [12] 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

IV. PROPOSED SCHEME

We assume that any pair of nodes in the network shares at least one cryptographic key. Our proposed method to detect wormhole attacks on wireless ad-hoc networks is as follow:

Step 1: Node A wants to check whether node B is its genuine neighbor or not. We set a time constraint T to identify suspicious link. T is the value of standard time delay for one-hop wireless communication between two sensor nodes in neighbor.

Step 2: Node A sends a message to node B and starts to time. Node B makes a reply as soon as it receives the message. Suppose that after a time interval Δt the reply message reaches the node A.

Step 3: The sensor node A will compare Δt with T. If Δt is greater than T then the link is considered as suspicious link. Due to the existence of wormhole nodes the transmitting time delay between the two sensor nodes will be prolonged and the link is considered as suspicious link.

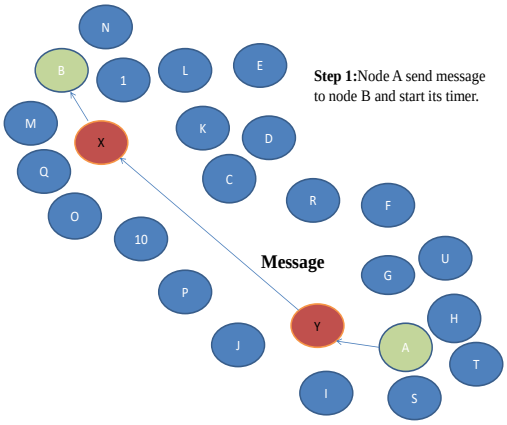
Step 4: Now node A sends RTS and a nonce N1 which is encrypted using K1 to B using a frequency f1 being used for communication between them.

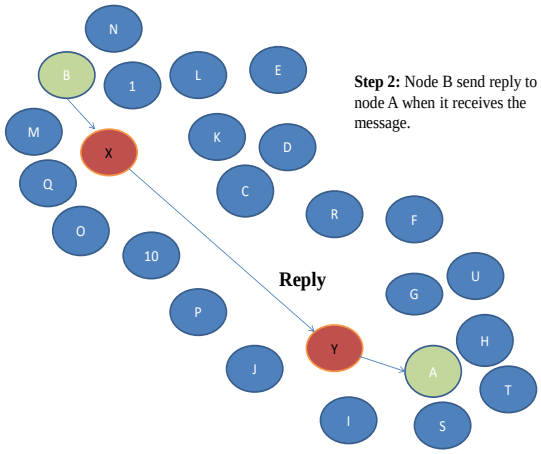
Step 5: B replies this message in frequency f1 with a CTS message that contains the frequency f2 common frequencies shared by A and B, the nonce N1 received previously and a new nonce N2, also encrypted with K1. Now B switches its receiver to frequency f2

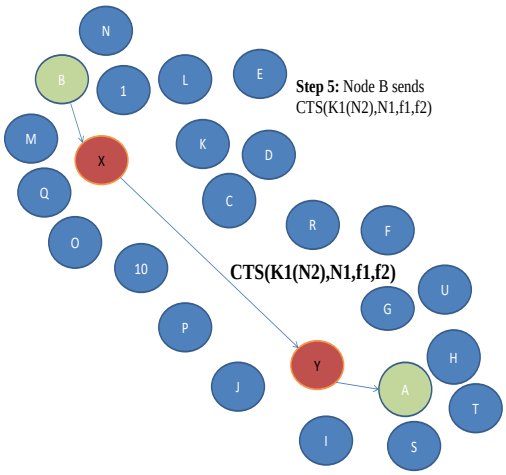
Step 6: After receiving CTS, A switches its transmitter to frequency f2 and sends a new RTS message to B.

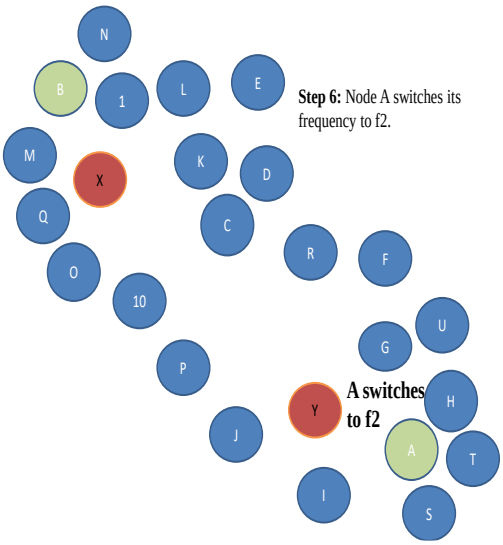
Step 7: If A does not receive an acknowledgment from B in frequency f2 within a specified time, then the link (A, B) is a confirm wormhole link.

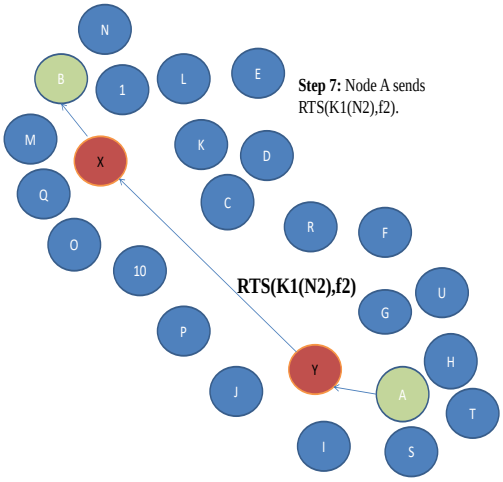
The example of the proposed method as follow:

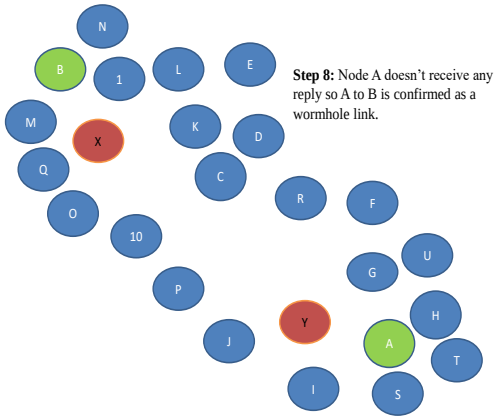












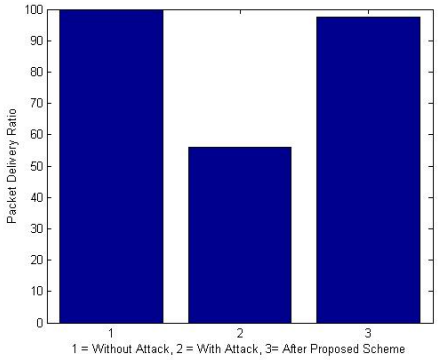
V. RESULT AND ANALYSIS

For simulation we have used NS-2.34. The simulation parameters are as follow:

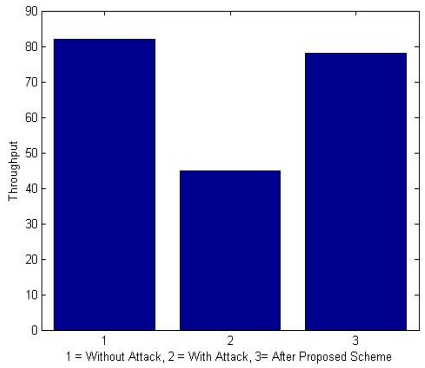
Parameter	Value
Simulator	NS2 (2.34)
Routing Protocol	AODV
Simulation Time	200s
No. of Nodes	30
Area	500 *500 m2

We have measured packet delivery ratio and throughput for normal scenario and attacking scenario.

(1) Packet Delivery Ratio:
The ratio between the total number of packets received by destination nodes and the total number of packets generated by source nodes. In normal scenario the packet delivery ratio is 99.80 percentages while in attacking scenario it decreases to 56 percentages. After applying proposed method it increase to 97.40 percentages.



(2) Throughput:
Throughput is the no. of data packets delivered from source to the destination per unit of time. In normal scenario the throughput is 82 kbps while in attacking scenario it decreases to 45 kbps. After applying proposed method it increases to 78.



We have measured the accurate detection ratio that is 90%. So we can say our method has good detection accuracy.

CONCLUSION

If there is no attack, there is no need for security.Security is very important for ad hoc networks because of their open nature.

Among all the attacks against mobile ad-hoc networks, wormhole attacks are very difficult to detect because they do not require breaking encryption to launch an attack.

The entire routing system of a MANET can also be destroyed by a wormhole attack.We reviewed several existing methods for detecting wormhole attacks in mobile ad hoc networks. Our proposed method can effectively detect wormhole attacks in mobile ad hoc networks. In the future, we hope to develop more sophisticated methods for detecting wormholes.

REFERENCES

[1] Chris Karlof *, David Wagner “Secure routing in wireless sensor networks: attacks and countermeasures”, Ad Hoc Networks 1 (2003) 293–315

[2] 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.

[3] 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.

[4] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks" 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing

[5] Ritesh Maheshwari, Jie Gao, Samir R Das, "Detecting Wormhole Attacks in Wireless Networks" IEEE International Conference on Ad Hoc Networks 2006

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

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

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

[9] Subhashis Banerjee1 and Koushik Majumder, "A Novel Custer Based Wormhole Avoidance Algorithm For Mobile Adhoc Networks" David C. Wyld (Eds) : ICCSEA, SPPR, CSIA, WimoA – 2013

[10] 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

[11] Zaw Tun and Ni Lar Thein "Round trip time based wormhole attack detection" *IEEE Wireless Communications andNetworking Conference - WCNC 2008*.

[12] 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.

[13] Radha Poovendran · Loukas Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks" Springer Science,Wireless Netw (2007)

[14] Dezun Dong, Mo Li, Yunhao Liu, Xiang-Yang Li, Xiangke Liao, "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks" IEEE 2009