A Brief Analysis on Detection and Avoidance Techniques of Wormhole Attack in MANET

Dhruva Patel
M.E Student
GTU-PG-School
Ahmedabad

Parth Trivedi
Project Scientist
BISAG
Gandhinagar

M.B.Potdar,Ph.D
Project Director
BISAG
Gandhinagar

ABSTRACT

Mobile Ad-hoc Network (MANETs) is a temporary wireless network, which is self-configuring in which nodes moves freely and continuously. It consists of a collection of wireless mobile nodes which dynamically exchange data among themselves without the reliance on a fixed base station or a wired resolution network. Due to its mobility and self-routing effective nature, there are many deficiencies in its security. Various security threats show their impact at different layer. Wormhole attack is a network layer attack observed in MANET, which completely disrupts the communication channel. Among all of security thread worm hole is consider to be a very serious security thread over MANET. In wormhole two selfish node which is geographically very far away to each other, makes tunnel between each other to cover their actual location and try to believe that they are true neighbours and makes conversation through the wormhole tunnel. The goal of this paper to study wormhole attack, some detection methods and different techniques to prevent network from these attacks.

General Terms

Your general terms must be any term which can be used for general classification of the submitted material such as Pattern Recognition, Security, Algorithms et. al.

Keywords

MANET, wormhole attack

1. INTRODUCTION

A mobile ad hoc network or MANET [3] is a kind of wireless ad hoc network, which is the infrastructure wireless networks where each user directly communicates without an access point or base station. It is a self-configuring network of mobile routers connected by wireless links with no access point. Nature of mobile device in a network is autonomous. Due to these mobile devices are free to move. In other words, the mobile ad hoc network is infrastructure less wireless network. The Communication in MANET is take place by using multi-hop paths. Nodes in the MANET share the wireless medium and the network topology changes dynamically. In MANET, breaking of communication link is very frequent because the nodes are free to move to anywhere. The density of nodes and the number of nodes are depends on the applications in which we are using MANET.

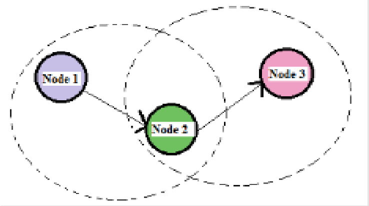

Fig-1 Ad-Hoc Network [2]

In figure a simple ad-hoc network shown 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 node 1and nodes 2. The node 2 will act as a router and these three nodes together form an ad-hoc network.

1.1 MANET Characteristics

Distributed operation: The control of the network is distributed among the nodes; there is no central background for the control of operations. The nodes should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security

Multi hop routing: When a node want to send information to other nodes which is out of its communication range, then the packet should be forwarded via one or more intermediate nodes.

Autonomous terminal: In MANET, each mobile node could function as both a host and a router because is an independent node.

Dynamic topology: The network topology may change randomly and at unpredictable time; nodes are free to move dynamically with different speeds.

Light-weight terminals: The nodes at MANET are mobile with less CPU capability, low power storage and small memory size.

Shared Physical Medium: The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. [2]

1.2 Advantages of MANET

The advantages of an Ad-Hoc network [2] include the following:

1. They provide access to information and services regardless of geographic position.

2. Self-configuring network, nodes are also act as routers. Independence from central network administration.

3. Less expensive as compared to wired network.

4. Scalable

5. Improved Flexibility.

6. Robust

7. The network can be easily set up at any place and time.

1.3 MANET Challenges

Limited bandwidth: Wireless link have significantly lower capacity than wired networks. The realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.

Dynamic topology: Due to this adaptive nature of MANET membership may disturb the trust relationship among nodes. Some nodes are detected as compromised, the trust may be disturbed.

Routing Overhead: In MANET, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

Hidden terminal problem: The hidden terminal problem refers that the collision of packets at a receiving node due to the simultaneous transmission of those nodes, that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

Packet losses due to transmission errors: MANET experiences a much higher packet loss due to, increased collisions, presence of interference, uni-directional links; frequent path breaks due to mobility of nodes.

Battery constraints: Devices used in MANET have restrictions on the power source in order to maintain portability, size and weight of the device.

Security threats: As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.[2]

1.3 MANET Routing Protocols

MANET routing protocols are categorized into three main categories depending upon the criteria when the source node possesses a route to the destination, as shown in figure 1.

1. Table driven/ Proactive
2. Source initiated (demand driven) / Reactive
3. Hybrid

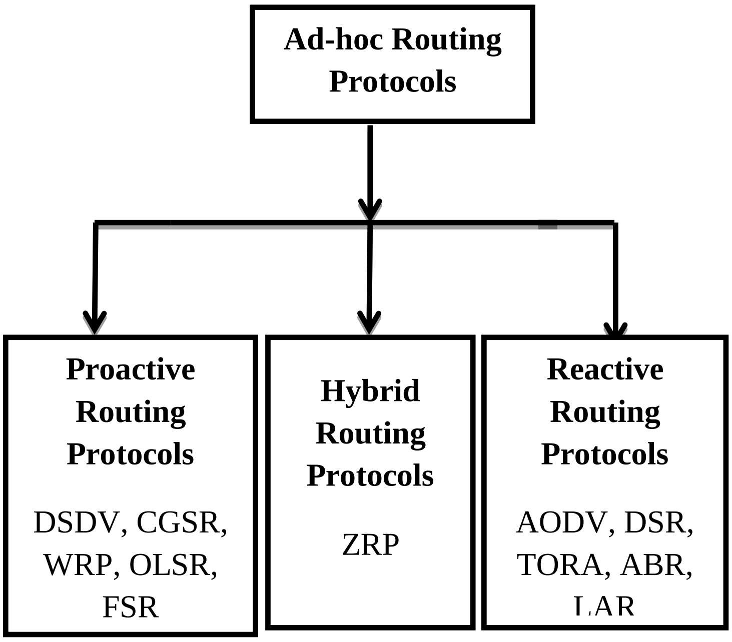
Ad-hoc Routing Protocols
Proactive Routing Protocols
DSDV, CGSR, WRP, OLSR, FSR
Hybrid Routing Protocols
ZRP
Reactive Routing Protocols
AODV, DSR, TORA, ABR, LAR

Fig-2 Classification of MANET Routing Protocols

2. ATTACKS IN MANET

The wireless Channel is accessible to both legitimate network users and malicious attackers. There is no well-defined boundary where traffic is monitoring. There are two types of security attacks in mobile ad hoc networks.

Passive Attacks: A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, thereby making it impossible for the attacker to get useful information from the data overhead.

Active Attacks: An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. *External attacks* are carried out by nodes that do not belong to the network. *Internal attacks* are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation, modification, fabrication and replication.

The security of MANET can be divided into 5 OSI layers: Application layer, Transport layer, Network layer, Data link layer and Physical layer. According to the specific layer there are various types of attacks which differ in their essence

Layer	**Types of Attack**
Application	Malicious code, Data corruption, viruses and worms
Transport	Session hijacking attack, SYN Flooding Attack

Network	Black hole, Worm Hole, sinkhole, link spoofing, rushing attack, replay attack, Sybil attack etc.
Data link	Selfish misbehaviour, malicious behaviour, traffic analysis
Physical	Eavesdropping, jamming, active interference

3. WORMHOLE ATTACK

The wormhole attack is one of the most efficient attacks, which can be executed within MANET. There are two collaborating attackers should establish the wormhole link (using private high speed network e.g. over Ethernet cable or optical link): connection via a direct low-latency communication link between two separated distant points within MANET. When this wormhole link is built up one of the attackers captures data exchange packets, sends them via the wormhole link to the second one and he replays them.

In wormhole attack, a tunnel is created between two nodes which is used to secretly transmit data packets. In a wormhole 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. For tunnelled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunnelled packet arrive sooner than other packets transmitted over a normal multi hop route. The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbor of) that node.[9]

Classification of Wormhole Attack:

In MANET it is difficult to detect such dangerous attacks and no one can predict what the wormhole nodes can do and where and when. At the higher layer wormhole attack is invisible; therefore two end points of the wormhole are not visible in the route in which detection becomes much more complex. Wormhole attack can be classified into five categories:

- Wormhole using Encapsulation.
- Wormhole using out of band channel.
- Open wormhole attack.
- Closed wormhole attack.
- Half open wormhole attack.
- Wormhole with high power transmission.

3.1.1 Wormhole Using Encapsulation In this mode of worm hole; a malicious node at one part of the network and hears the RREQ packet. It channels that packet to a second party at a distant location near the destination. The second party then rebroadcasts the RREQ packet; neighbours of the second party receive the RREQ and drop any further legitimate requests that may arrive later on legitimate multi hop paths.

3.1.2 Open wormhole attack In this attack malicious node keep examine the wireless medium to process the discovering RREQ packets, in the presence of malicious node in the network other node on the network suppose that malicious node are present on path and they are their direct neighbours.

3.1.3 Closed wormhole attack In this the attacker does not modify the capture packet nor did it modify the packet field head. The attacker take the advantage when the packets are in the process to find a route know as route discovery. At route discovery process attack tunnel the packet from one side of the network to another side of the network and re-broadcast packets.

3.1.4 Half open wormhole attack In this attack only one side of the packet is modify from the malicious node and the other side of the malicious node do not modify the packet subsequently route discovery procedure.

3.1.5 Wormhole with high power transmission In this attack malicious node use maximum level of energy transmission to broadcast a packet, When malicious node received a Route Request (RREQ) by using route discovery process, it broadcast the Route Request (RREQ) at a maximum level of energy of it power so the other node on the network which are on the normal power transmission and lack of high power capability hears the maximum energy power broadcast they rebroadcast the packet towards the destination. By doing this malicious node get more chances to create a route between source and destination without using colluding.[9]

4. RELATED WORK

For the detection and avoidance of wormhole attack in MANET recently many techniques introduced but this section discuss some technique that prevent the wormhole attack.

In [1], authors proposed a lightweight technique to prevent wormhole attack in AODV. In MANET, wormhole by itself does not represent a threat. The attackers are offering a valuable service, by providing a shortcut across the network. This technique can detect the wormhole attack using backbone network nodes which monitor other nodes in the network and maintain a monitoring trust value for each node. The backbone network is constructed from the regular nodes chosen based on their trust value. In this technique AODV HELLO messages are used to exchange all the control information of the proposed technique to reduce the overhead. The simulation results using NS2 show that, the proposed technique can highly detect and remove the wormhole attack and gives the lowest total packet loss rate compared with AODV under attack and the other techniques. In the proposed technique, only the backbone network can estimate the monitoring trust value which is more secure than the previous technique.

In [4], authors divide their work in to two phases; in phase 1 they describe the generation of wormhole attack and in phase 2 an efficient approach for analyzing and prevention of wormhole attack. In phase 1 they generate the wormhole attack on mobile nodes in the ad-hoc network. In that two nodes connected via tunnel. Illusive neighbors generated in network hence route request packet misled by those neighbors. Malicious nodes receive that route request and extract the network topology information. In phase 2 they described the neighbour list detection approach for preventing wormhole attack. In this approach the Source node neighbor list stored in NLs and Destination node neighbor list stored in NLd. Compare both neighbor list source node and destination node and calculate the number of common neighbor nodes present between sources to destination by if {NLs(i)==NLd(j)}. Number of common neighbors between source and destination exceeds the Threshold value then it will find out wormhole attacker nodes may present among the path. When it will find out wormhole attacker nodes present then Sender send worm announcement message to all nodes. All original nodes drop the wormhole attacker nodes.

In [5], authors proposed some modification on existing approach and designed secure and very efficient approach for the detection of the Wormhole nodes. This work is implemented DSR routing protocol. The algorithm always stores the table entries in the sorted form. The main thing of the algorithm is that the Hound packets are sent in the Fibonacci series pattern. So the numbers of packets are less than as in the previous approaches. This approach reduces the processing delay in comparison to the previous approaches.

In [6], authors proposed algorithm implemented on AODV routing protocol. First the algorithm randomly generate a number in between 0 to maximum number of nodes. After that they generate the route from selected transmitting node to any destination node with specified average route length. Then it send packet according to selected destination and start timer to count hops and delay. For the detection of malicious node; if the hop count for a particular route decreases abruptly for average hop count then at least one node in the route must be attacker. Now to find out exact malicious node, repeat the whole algorithm. If more than one node is misbehaving and that will take time and resource.

In [7], authors implemented their trust based model, TBAODV in the network simulator, NS2. The nodes communicated in this model across each other using five constant bit rate (CBR). In movement scenario, a node moves towards the destination at a uniform Speed. To analyse the performance of their TBAODV, they compared it with the performance of normal AODV. Based on the trust factor, routing takes place. This saves nodes transmission power by avoiding unnecessary transmission and also its bandwidth.

Authors of [8], suggested the use of geographical leashes to detect wormholes. A leash is any information that is added to a packet designed to restrict the packet’s maximum allowed transmission distance. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. To construct a geographical leash, in general, each node must know its own location, and all nodes must have loosely synchronized clocks. When sending a packet, the sending node includes in the packet its own location, and the time at which it sent the packet and when packet is received, the receiving node compares these values to its own location, and the time at which it received the packet. If the clocks of the sender and receiver are synchronized to within some threshold then the receiver can compute an upper bound on the distance between the sender and itself by using upper bound value of velocity of nodes.

5. CONCLUSION

This paper describes several detection and avoidance techniques of wormhole attack in MANET. In section 4 we describe many detection techniques which are proposed earlier. In that the detection was done almost AODV, DSR routing protocols. So for the future enhancements there is a need to detect the wormhole attack in other routing protocols like TORA, ZRP etc.

6. ACKNOWLEDGEMENT

This paper is carried out with the full support from Bhaskaracharya Institute for Space Applications and Geo-informatics and the director of institute Mr T. P. Singh. I am also thankful to all the members of the institute for supplying the precious data and resources.

7. REFERENCES

[1] Assiut, Egypt, Hosny M. Ibrahim, Nagwa M. Omar, Ebram K. William: “A Lightweight Technique to Prevent Wormhole Attacks in AODV” International Journal of Computer Applications ,Volume 104 – No.6, October 2014

[2] Aarti: “Study of MANET: Characteristics, Challenges, Application and Securiy Attacks” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013. R. Nicole, "The Last Word on Decision Theory," *J. Computer Vision*, submitted for publication. (Pending publication)

[3] P.Chandra Sekhar: “A SURVEY ON MANET SECURITY CHALLENGES AND ROUTING PROTOCOLS” Int.J.Computer Technology & Applications(IJCTA), Vol 4, Mar-Apr 2013.

[4] Shivangi Dwivedi, Priyanka Tripathi: “An Efficient Approach for Detection of Wormhole Attack in Mobile Ad-hoc Network” International Journal of Computer Applications, Volume 104 – No.7, October 2014

[5] Farman Ahmed, Ankit Jha ,Neeraj Kumar: “Efficient Approach for the Detection of Wormhole Attack Using Dynamic Source Routing Protocol in MANET” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 8, August 2014

[6] Ajit Singh, Lehra Gaga, O.S.Khanna: “Multipath Algorithm For Prevention Of Wormhole Attack In Manet”, Journal of Advanced Studies and Communication Research, Volume.1, Issue.3, March 2014

[7] Prof. Ramya S Pure, Prof. Gouri Patil, Prof. Mohammad Manzoor Hussain: “Trust based solutions using counter strategies for Routing attacks in MANET” International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue4,June2014.

[8] Yih-Chun Hu, Adrian Perig, David B. Johnson: “Wormhole Attack on Wireless Network” IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Vol. 24-No 2,2006.

[9] K. Sivakumar, Dr. G. Selvaraj: “Analysis of Worm Hole Attack In MANET And Avoidance Using Robust Secure Routing Method” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013.