A SURVEY PAPER ON WORMHOLE ATTACKS IN MANET

Amandeep Kaur Grewal
MTech, Department of Information Technology, Adesh Institute of Engineering & Technology, Faridkot

ABSTRACT

Unlike, traditional wireless networks which rely on fixed infrastructure for the communication, ad-hoc networks do not have any fixed infrastructure rather it is the collection of the autonomous and self-organized mobile nodes. These mobile nodes are free to move in and out of the network. MANET is more vulnerable to security attacks of the malicious nodes because it has no clear mechanism of defense. The openness, dynamic and infrastructure-less nature makes it prone to the security threats. As the presence of malicious nodes is one of the greatest security threats in the MANET, so it has become necessary to implement a robust solution for its security. MANET can be attacked by two kinds of attacks active and passive attacks. Active attacks are wormhole attack, black hole attack, gray hole attack, flooding, spoofing etc. and eavesdropping, traffic analysis comes in the category of passive attacks. In this review paper, I have introduced a wormhole attacks, representing what the wormhole attacks are in actual, how they attack the network and the consequences caused by these attacks. Wormhole attack aims disguise itself as the shortest route than the original shortest route in the network, thereby, confusing the routing mechanisms of the mobile ad-hoc network. It can be easily launched without having any prior knowledge of the network and its security mechanisms implemented within the network. This paper focuses on the MANET and the consequences of wormhole attack by describing the related research of previous years.

Keywords: MANET, Ad-Hoc Network, Wormhole Attack, Wireless Network.

1. INTRODUCTION

Wireless networks have become the most prevalent areas of research in the networking. Wireless networks are the most convenient and probable solution of communication over the internet. Wireless Networks are categorized as Infrastructure Networks and Ad-Hoc Networks. Infrastructure Wireless Networks are those in which the devices in the network communicate with each other through an access point, that is, the wireless router. For example, say the two laptops are sitting close to each other and are connected to the same wireless network. But, these laptops cannot directly communicate with each other instead, they are communicating indirectly through the wireless access point. They can transmit the packets to the access point (wireless router) and
the access point in turn, transmits to the destined laptop. So, necessity of a central access point is
the basic requirement of the infrastructure mode.
Ad-Hoc Networks do not require any centralized medium like access points for communication.
But, the devices in the network can directly communicate with each other. It provides convenience
in terms of mobility, scalability, cost and easy setup but, vulnerable to attacks due to the
decentralized deployment scenario.
A MANET is infrastructure less dynamic network consisting of a collection of wireless mobile
nodes that communicate with each other without the use of any centralized network [1].
It is decentralized IP based network of mobile machine nodes. MANET is the new emerging
technology which enables users to communicate without any physical infrastructure regardless of
their geographical location, that’s why it is sometimes referred to as — infrastructure less network
[2].
As the network is decentralized, all the routing activities are carried out by the nodes only. All
the nodes can enter connected to each other in a dynamic topology where each node can enter or
leave the network freely. The openness of the network and lack of an infra-structured medium
for communication makes it prone to many security threats that result in the severe consequences.
The nature of MANET allows the attacker nodes to become part of the network easily and carry
out its malicious activities.
There are number of applications where MANET has become an indispensable part for the
purpose of communication. These applications are given below:
- Military communications and operations
- Automated battlefields
- Emergency services
- Search and rescue operations
- E-commerce and E-Payments
- Personal Area Networks (PAN)
- Commercial Sector
- Sensor Network
- Medical Service

![Decentralized & Infrastructure-less MANET](image)

Figure 1. MANET
2. ISSUES IN MANET

a. Decentralized Mechanism
MANET does not have any centralized medium for the communication like access point in case of infrastructure wireless networks. It basically depends on the network nodes only for the transmission of the packets from source to destination. So, this deployment scenario makes it easy for the attackers to become part of the network and disrupt the communication.

b. Scalability
Mobile Ad-Hoc networks are highly non-scalable in nature because of the mobility of the nodes. As the nodes are freely allowed to enter or leave the network, the security concern becomes an important issue in the network communication.

c. Cooperativeness:
Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.[3]

d. Dynamic Topology
Being infrastructure less and decentralized, nodes can leave or join the network unpredictably over the time. The topology is dynamic and thereby, creating mistrust relationship among the nodes.

e. Limited power supply
The nodes in mobile ad-hoc network start behaving in a selfish manner when the network is restricted with the limited power supply.

f. Resource availability
Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism [4].

3. WORMHOLE ATTACK
A Wormhole Attack is the most severe among the security threats in the MANET because it does not exploit any node of the network. It has the most devastating impact on the network as it halts the overall performance of the network by decreasing the throughput by dropping the packets. In Wormhole Attack nodes disguise themselves as the shortest route in the network than the original routing path. This leads to false conception regarding the routing paths that are to be selected based on the distance of the routes in the network. The attacking node does not need to have any prior knowledge of the network and the security mechanisms implemented on it.

In this type attack, the two attacking nodes are connected to each other through a link known as tunnel. The malicious node present on either side captures the packet from the legitimate node and by encapsulating the packet, transmits it to another malicious node in the network.

In given figure, wormhole attack is depicted. The nodes 2 and 9 are the malicious nodes in the network. These nodes will try to receive the RREQ message packets. Node 9 will send a packet which carries the false route of node 9 to node 2. But, in actual it is not the original path. The original path follows from node 9-8-6-5-4-2.
The path from node 9 to node 2 is the wormhole link / tunnel created by the malicious nodes.

Figure 2. Wormhole Attack

4. WORMHOLE MODES
The tunnel formed between the attacking nodes can be of two types:

In-Band Channel or Packet Encapsulation
In this mode, the attacking nodes are present within the network. The attacking node at one end captures the packets from the source node, encapsulates the packet header and transmits it to the other malicious nodes. After receiving the packet by the other end attacking node, it may either drop the packet or forward it to the other nodes in the network.

Out-of Band Channel
In this mode, an outer link is present between the two malicious nodes. A bandwidth channel is required so that the wormhole tunnel can be created.

High Power Transmission
In this type of mode, the packet captured from the source node is transmitted to the destination node with high power in such a way that it forces the nodes to follow the wormhole path.

5. TYPES OF WORMHOLE ATTACKS
Classification of Wormhole Attack Recent studies has classified the wormhole attack on various ways; these attacks are classified on the basis of these ways they are listed below [5].

- Implementation of these nodes
- The medium chosen by these nodes
- Way of attack
- On the basis of visibility of attacks

On the basis of visibility these are classified as given below:

- Open wormhole attack/ exposed
- Half open wormhole attack
- Closed wormhole attack/hidden

**Open Wormhole Attack / Exposed**
The two wormhole nodes are visible in the network. In this the attacking nodes includes themselves (their identity) in the packet header and then follows the normal route discovery mechanism. All the nodes in the network are aware of the presence of malicious nodes but they would behave as if the malicious nodes are their direct neighbors.

**Closed Wormhole Attack / Hidden**
Here the source and destination nodes are not aware of the presence of the malicious nodes. The packet headers are not updated in the route discovery mechanism. The malicious node at one end captures the packet from the legitimate node and tunnels it into another malicious node. So, the other end attacking node will either discard the packet or selectively discarding the packets or modifying the packets.

**Half Open Wormhole Attack**
In this type of attack the malicious node at one side of the network update its identity in the packet header at the time of route discovery process. Here one malicious node is visible and other is invisible to the legitimate nodes in the network. [6]

![Figure 3 Types of Wormhole Attacks](image)

6. RELATED WORK
Various Detection and Prevention Techniques have been proposed in order to gain security against the wormhole attacks.

a) **Packet Leashes**
Yhi-Chun et. al. [7] proposed a mechanism for detecting the wormhole attacks, based on the temporal and geographical leashes. In Temporal leashes, all nodes require a synchronized clock and these are used as sending and receiving methods. While in case of geographical leashes, there is no need of any synchronized clock. It uses the GPS hardware.

b) **Directional Antennas**
L. Hu et al. [8] used the mechanism in which the directional antennas are used for communication between the nodes. It is the hardware based approach. But, this method fails if an attacker intentionally places the wormhole link between the communicating nodes.

c) Digital Signatures

Pallavi Sharma et al. [9] proposed a method to detect and prevent the wormhole attack by using the technique of digital signatures. According to this method, every node has digital signatures of every other node. In this way, a verification mechanism is carried out when the receiving node can verify the sending node through its digital signatures.

So, a trusted path is created between the source and the destination and the attacking node can be easily identified.

d) Neighbor Node Analysis

Sweety Goyal et al. [10] presented a way of analyzing the neighbor nodes for the purpose of authentication. Every node will analyze all the other neighbor nodes. In this method, a node will send a request message (RREQ) to the neighbor nodes. All the nodes after receiving the request message will send the reply message (RREP) to the sending node.

This approach is based on the comparison between the response time of RREP sent and the actual RREP time. If response time of actual RREP is more than the RREP sent plus the threshold value, it can be said that the wormhole link is present in the network.

e) DelPHI Technique Delay Per Hop Indication

Lui K.S et al. [11] calculates the delay per hop of the disjoint paths. The delay per hop is calculated for every path. It has been proven that delay per hop value for a legitimate path is always shorter than the wormhole path.

So, if the value of delay per hop is extremely high, then it can be concluded that it is the wormhole path present in the network.

7. CONCLUSION

MANET is a wide area in which security concern is the major challenge because it lacks the centralized administration. This paper presents focus on the MANET, issues in the MANET and the wormhole attack is described. It represents that what exactly the wormhole attack is and how it affects the network. Various detection and prevention techniques have been studied and presented in the form of literature survey. Still the research in this field is going on and a lot improved techniques can be discovered with the research in the related area.

8. REFERENCES


