ISSN : 2455-9679
Impact Factor : 2.015

ijrtsm

IJRTSM

INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"WORMHOLE ATTACK IN MANET: A STUDY"

Margi Patel [1], *Nitin Rathore* [2]
[1,2] *Department of Computer Science and Engineering, IIST, Indore*

ABSTRACT

MANET (Mobile Ad-hoc Network) refers to a multi-hop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. MANET'S are actually self-organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. It generally works by broadcasting the information and used air as medium. Its broadcasting nature and transmission medium also help attacker to disrupt network. The emphasis of this paper to study wormhole attack. Wormhole attack is a severe attack in wireless ad-hoc networks, to establish a wormhole attack; attackers create a direct link, referred to as a wormhole tunnel, between them. Wormhole tunnel can be occurring by means of a wired link, a high-quality wireless out-of-band link or a logical link via packet encapsulation.

KEYWORD: *- MANET, Worm hole, Attack, Packets, Mobile nodes***.**

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) is a self-configuring network of wireless mobile nodes that formed network capable of dynamic changing topology. Each node in the network acts as a router, forwarding data packets to other nodes. MANET has many potential applications such as military services in battlefield, disaster relief operations and in commercial environments.

MANET has several challenges. They include-

1) Multicast Routing: - Designing of multicast routing protocol for a constantly changing MANET environment.

2) Power Consumption: - Since the nodes in MANET network typically run on batteries and are deployed in hostile terrains, they have stringent power requirements

.

3) Dynamic Topology: - The nodes are mobile and hence the network is self-organizing. Because of this, the topology of the network keeps changing over time.

4) Quality of service (QOS):- Providing constant QOS for different multimedia services in frequently changing environment.

5) Security: - The ultimate goal of the security solutions for MANET is to provide a framework covering availability, confidentially, integrity, and authentication to insure the services to the mobile user.

The following are five major security goals which require preventing from attacks

1) Authentication: Authentication ensures that the communication or transmission of data is done only by the authorized nodes. Without authentication any malicious node can pretend to be a trusted node in the network and can adversely affect the data transfer between the nodes.

2) Availability: Availability ensures the services should be available even in the presence of the attacks. Systems should be able to take care of Various attacks such as denial of services, energy starvation attacks, and node misbehavior.

3) Confidentiality: Confidentiality ensures that data should be accessible only to the intended party. No other node except sender and receiver node can read the information. This is implemented through data encryption technique.

4) Integrity: Integrity ensures transmitted data is not being altered by any other malicious node.

5) Non Repudiation: Non-repudiation ensures that neither a sender nor a receiver should not deny a transmitted message.

Attacks on MANET:-

1) Active Attacks:-

Performed by attackers for replicating, modifying and deletion of exchanged data. They try to change the behavior of the protocol. These attacks are meant to degrade or prevent message flow among the nodes. Such attacks collectively can be called as DOS attacks that either degrade or completely block the communication between the nodes.

2) Passive Attacks: -

This type of attack involves unauthorized listening of the routing packets. Attacker may eavesdrop on all the routing updates. In this case an attacker does not disrupt the operation of a routing protocol rather it only listens to it to discover the valuable information about the routing.

Physical Layer Attacks: -

1)Eavesdropping: In eavesdropping attack, attacker tries to get the secret information during communication.

2) Jamming: Jamming attack will be implemented by knowing the frequency. Malicious nodes send jam signal to disturb the communication.

3) Active interference: An active interference is a type of denial of service attack which distorts the communication.

Link Layer Attacks:

1) Selfish Misbehavior of nodes: in the selfish misbehavior nodes will act as selfish and will not be willing to participate in forwarding process.

2) DOS attack: This attack prevents authorized access of resources to the legitimate node.

3) Resource Exhaustion: Malicious nodes make repeated collision to drain the battery power.

4) Malicious Behavior: The main task of malicious node is to disrupt normal operation of routing protocol. The impact of such attack is increased when the communication takes place between neighboring nodes.

Wormhole Attack

The wormhole attack in wireless networks was independently introduced by Dahill, Papadimitratos, and Hu. In, authors have described different types of wormholes depending upon the techniques used to tunnel the packets between the colluding nodes:

wormhole using encapsulation, wormhole using out-of-band channel, wormhole with high power transmission, and wormhole using packet relay.

Wormhole using encapsulation
Wormhole using out-of-band channel
Wormhole using high power transmission
Wormhole using packet relay

1)Wormhole using encapsulation: The source node broadcasts a route request packet, received by the malicious node M1, which encapsulates it and forwards it to M2 via legitimate nodes. M2 demarches the packet and broadcasts it further to the destination. Note that due to the packet encapsulation, the hop count does not increase during the traversal through the good nodes.

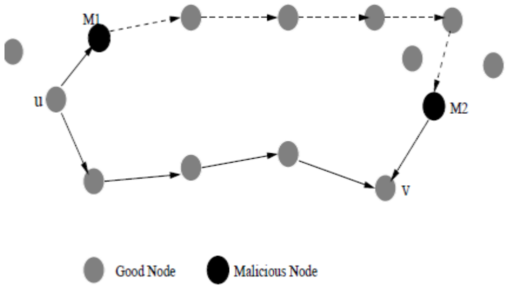

Figure 1. wormhole using encapsulation

2) Wormhole using out-of-band channel: The two colluding nodes communicate directly via an out-of-band high-bandwidth channel using a long-range directional wireless link or a direct wired link.

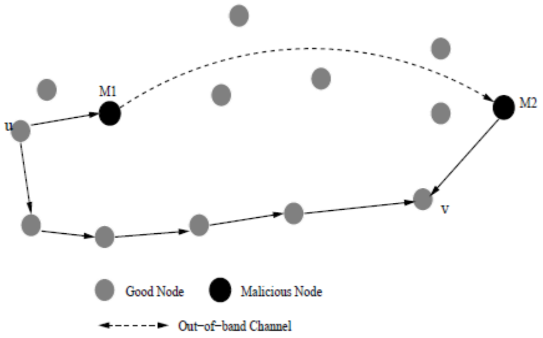

Figure 2. wormhole using out-of-band channel

3)Wormhole using high power transmission: Malicious nodes have a high power antenna and hence distant nodes receive the route request packet faster from the malicious nodes than through the normal multi-hop route increasing the chance of malicious node to get inserted in the route.

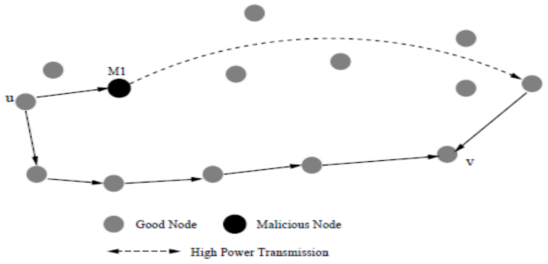

Figure 3. wormhole using high power transmission

4) Wormhole using packet relay:

A malicious node relays packets between two non-neighbor nodes creating an illusion that they are neighbors. We have classified worm holes depending upon whether one, both or none of the two colluding nodes at the end of the tunnel are visible to the good nodes (we will call them the victim nodes). See Figure 4. They describe the wormhole as closed if none of them is visible; u and v get the illusion that they are direct neighbors of each other. It is called half-open, if the malicious node near u is visible to it but the other end is not visible to v; two hops path is established between u and v.

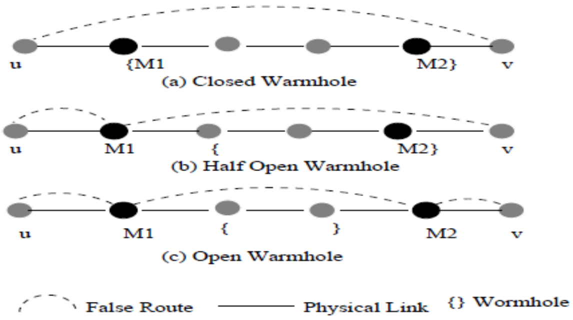

Figure 4. Types of wormhole

II. METHODOLOGY

1) Distance and location Based: Packet Leash Technique.

Numerous methods were proposed using a packet leash technique for the detection of the wormhole attack. The packet leash (Yih-Chun Hu et.al, 2003) is the method that defends against the wormhole attack. The leashes can be grouped either into geographical or temporal. In geographical leashes, all nodes should have knowledge of its own location in the network and secure synchronized clock. Whenever a sender sends the data packet, it includes its own recent location and transmission time in header. Therefore, the receiver is capable of predicting the neighbor relation by calculating the distance between itself and source. In temporal leashes, all nodes calculate the expiration time of each packet by using light's velocity and append this expiration time in the packet's header. Destination compares its own arrival time and expiration time in the packet to detect the wormhole attack.

2) Localized Encryption and Authentication Protocol (LEAP): -

It is a method which is suggested by Zhu . This model is based on clustering and it requires defining 4 type keys for each sensor node such as,

a. Individual key that is shared with the base Station.

b. Pair wise key that is shared with another sensor node.

c. Cluster key that is shared with multiple neighboring nodes.
d. Group key that is shared by all the nodes in the network.

3) **Multipath Hop-count Analysis Technique: -**

This model is developed 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.

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. It utilizes control packets as in RFC3561 and tries to modify it. Therefore, it used the RREQ packet is used for route discovery and the RREP packet is used for route.

Before we describe the mechanism, we first represent some definitions and then briefly describe our system requirements and assumptions. We define a cluster head node while a node wants connect more than two nodes. We displayed them with blue color. Each cluster head is connected with other cluster heads with one or more hops, and in each cluster head's routing table, moreover the distance until his cluster members, distance between neighbors cluster head's written.
An algorithm for Detecting and removal of Worm hole attack (tunnelling) with the help of truss computing. With the help of Proposed Algorithm, it Increases the threshold time of the data packets which avoids the attack. Reduce the Attacking Effect by introducing packet expiration time also for security.

III. CONCLUSION & FUTURE WORK

In this paper, we have introduced the wormhole attack, as a sever attack that can have serious consequences on many proposed ad hoc network routing protocols

REFERENCES

[1]Yahya Ghanbarzadeh, Ahmad Heidari, and Jaber Karimpour International Journal of Computer Theory and Engineering Vol. 4, No. 2, April 2012

[2] B. Dahill, B. Levine, E. Royer, and C. Shields. A secure routing protocol for ad hoc networks. In *Tech report 02-32. Dept. of Computer Science, University*of Massachusetts, Amherst, 2011.

[3] Jyoti Thalor, Ms.Monika Volume 3, Issue 2, February 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 6 – May 2014

[4] International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 6 – May 2014 ISSN: 2231-5381 *Nitesh Funde#1, P. R. Pardhi*2* M Tech Scholar, * Assistant Professor,Department Of Computer Science & Enggineeing Shri Ramdeobaba College Of Engg. & Management Nagpur, India

[5]FEEPVR:first end-to-end protocol to secure ad-hoc network with variable ranges worm hole attack Sandhya Khurana Department of CS University of Delhi

[6] B. Dahill, B. Levine, E. Royer, and C. Shields. A secure routing protocol for ad hoc networks. In Tech report 02-32. Dept. of Computer Science, University of Massachusetts, Amherst, 2001.