An Advanced Wormhole Detection Approach for Securing MANETs

Vanita Sharma[1]Saurabh Mittal[2]
[1, 2] Computer Department
[1, 2]Galaxy Global Imperial Technical Campus, Ambala

Abstract—*Wireless networks are susceptible to many attacks, including an attack known as the wormhole attack. The wormhole attack is very powerful, and preventing the attack has proven to be very difficult. A strategic placement of the wormhole can result in a significant breakdown in communication across a wireless network. In such attacks two or more malicious colluding nodes create a higher-level virtual tunnel in the network, which is employed to transport packets between the tunnel endpoints. These tunnels emulate shorter links in the network and so act as benefit to unsuspecting network nodes which by default seek shorter routes .This project report presents the model to prevent the wormhole attack in MANET.*

Keyword:- *AODV, MANETs, Wormhole Attacks, Security.*

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is an independent collection of mobile nodes that form a short-term network without of any existing network organization or central access point. The popularity of these networks created security challenges as an important issue. The old routing protocols perform well with dynamically changing topology but are not designed to protection against security challenges. In this paper we discuss about current challenges in an ad hoc situation which includes the different types of potential attacks that are likely in the Mobile Ad hoc Networks that can harm its working and operation. We have found that there is no universal algorithm that suits well against the most commonly known attacks. But the whole security solution requires the prevention, detection and reaction mechanisms applied in MANET. To develop suitable security solutions for such environments, we must first understand how MANETs can be attacked. This paper provides a broad study of attacks against mobile ad hoc networks. We present a detailed taxonomy of the attacks against MANETs.

Wireless mobile ad-hoc network have many advantages [1] as fast & low cost of deployment, active configuration etc.

MANET has several possible applications. Some classic examples include emergency search-rescue operations, meeting events, dealings, conferences, and battleground communication between moving vehicles and/or soldiers. With the abilities to meet up the new claim of mobile calculation, the MANET has a very bright future. Even though security has long been an active research issue in wired networks, the individuality of Ad Hoc networks presents a new set of nontrivial challenges in the path of security design. These challenges include open network architecture, joint wireless medium, stringent resource constraints, and highly lively topology. Some of the main security attributes [1] [2], which are used to inspect the security status of the mobile ad-hoc network, are: Availability, Integrity, Confidentiality, Authenticity, Non repudiation, Autho-rization, Anonymity.

II. Wormhole Attack

The wormhole attack [3] is one of the most cultured and severe attacks in MANETs. The wormhole attack is possible even if the attacker has not negotiated any hosts and even if all statement provides authenticity and confidentiality. In this attack, a pair of conniving attackers record packets at one location and replay them at another location using a private network.

The figure 1 shows the Wormhole attack. It is also possible for the attacker to forward each bit by the wormhole directly, without waiting for a whole packet to be received before start to tunnel the bits of the packet, in order to lessen delay introduced by the wormhole.

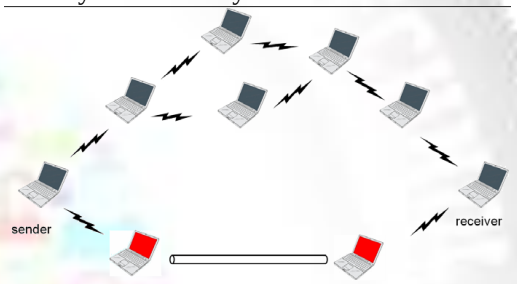

Fig. 1: Wormhole attack

The attacker is unseen at higher layers; unlike a nasty node in a routing protocol, which can often easily be named, the existence of the wormhole and the two planning attackers at either end- point of
the wormhole are not visible in the route.

III. PROBLEM

During 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 tunneled distances longer than the normal wireless transmission range of a single hop, it is easy for the attacker to make the tunneled packet than a normal multihop route. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to it, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole.

III. OBJECTIVE

The various objectives to formulate the problem can be outlined as follows:

1. In this research we study few of wormhole Detection & Prevention techniques to identify Worm hole attack in MANET.
2. The objective of our work is to find an efficient method for Detection of Worm hole in MANETs.

3. To examine the performance and the feasibility of more energy efficient protocol by considering a set of parameters.

IV. Present Work

A. *Proposed Work*

We suggest a new method to detect the wormhole attack in on demand routing protocol. Before each node transfers data, it is necessary to check node authentication that is important feature of security, to its nearest neighbor. For this purpose one approach is followed, which come to know wormhole node: Provide a Digital Signature between sender & receiver node. According to this approach, the malicious node whose Digital Signature value does not match with the defined Digital Signature, cannot impersonate and use another node authentication.

Above written Proposed scheme can be easily understand through the algorithm shown in below.

Algorithm: Detection of wormhole Node

1. Begin
2. Route discovery using AODV protocol by Sender node to the Fixed Destination.
3. Provide Digital Signature via sender node.
4. Compare the Digital Signature with Destination Node.
    a. If (satisfies criteria)
        i. then go to step 5.
    b. Else
        i. Wormhole Node Detected and infected node will be excluded from the transmission line and go to step 5.
5. Transmission starts.
6. These nodes are black listed by the nodes hence they are not involved in future routes in this particular network.
7. Whole process (from step1 to step 6) is repeated until we didn't get the specified goal. Goal can be:
    a. To get complete list of malicious nodes.
    b. To run for specified time.
    c. To run for specific number of packets etc.
8. End

B. *Simulation Model*

The simulations were performed using Network Simulator 2 (Ns-2.34), particularly popular in the ad hoc networking community.

The model parameters that have been used in the following experiments are summarized in Table 1.

Table 1: Simulation Parameters

Parameters	**Value**
Simulator	NS 2.34
Simulation Area	800X800
Number of Mobile Nodes	30
Channel	Wireless
Routing Protocols	AODV
Simulation Time	500 Sec
Traffic Class	TCP
MAC Layer	802.11

V. Results

Graph representation of packet received over packet drop for 30 Nodes using AODV approach is shown in figures given below.

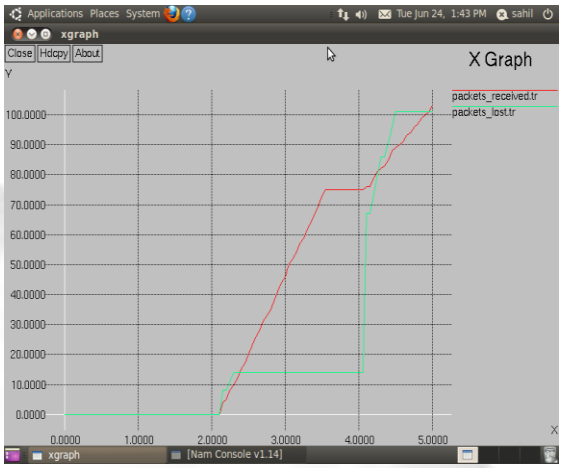

Fig. 2: Transfer of packets for 30 Nodes using AODV

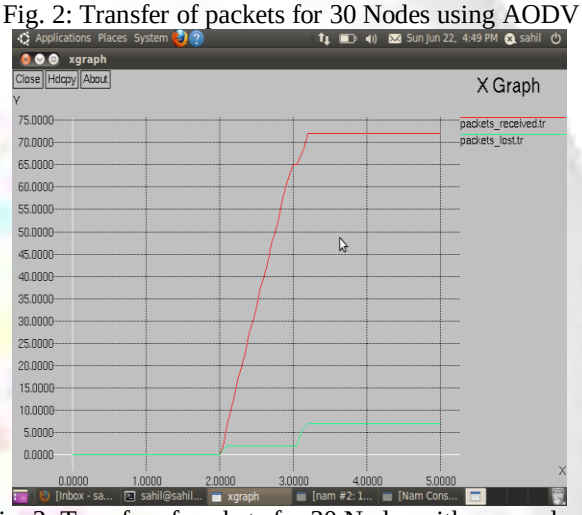

Fig. 3: Transfer of packets for 30 Nodes with one node as wormhole

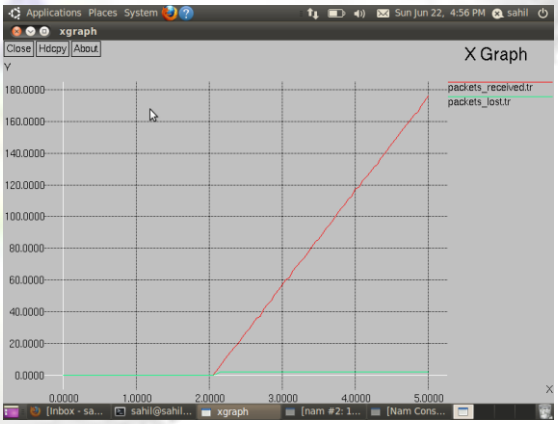

Fig. 4: Transfer of packets for 30 Nodes with two nodes as wormhole

Packet delivery ratio for 30 nodes has been depicted using figure 5 as function of Time. The previous approach is demonstrated with the help of blue color and purposed approach with red color. As time increases, there is slight variation in loss of packets .In previous approach, the variation in loss of packet is more than purposed approach.

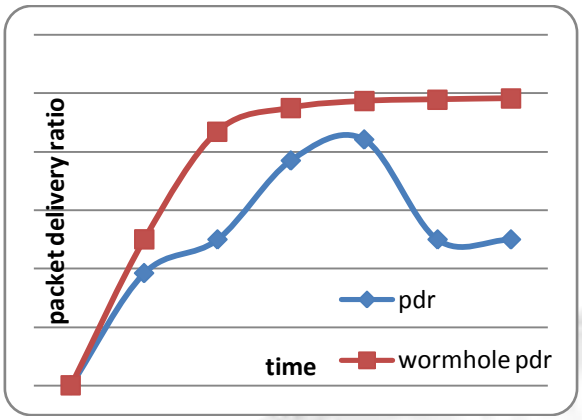

Fig. 5: PDR v/s time for 30 nodes using AODV & two nodes as wormhole

VI. Conclusion

A. *Conclusion*

A wormhole is one of noticeable attack which is formed by two malicious nodes and a tunnel. In order to defend from wormhole attack we used the scheme which verifies the legitimate nodes in network through its digital signature. For checking the authentication of selected path, we used verification of digital signature of all sending node by receiving node. If there is no malicious node between the paths from source to destination, then source node creates a path for secure data transfer. Also we have checked the wormhole attack for one and two nodes (acts as attacker).

B. *Future Scope*

As we are detecting wormhole in the given work, the future of the work can be as follows:

1. Wormhole prevention can be done.

References

[1] C. Siva Ram Murthy and B. S Manoj, Ad Hoc Wireless Networks, Architecture And Protocols(Prentice Hall PTR, 2004).

[2] Nguyen, D. Q., & Lamont, L, "A Simple and Efficient Detection of Wormhole Attacks". IEEE Conferences New Technologies, Mobility and Security (pp. 1-5). NTMS '08.

[3] G. Schäfer, "Research Challenge in Security for Next Generation Mobile Networks," Position Papers PAMPAS '02 - Workshop on Requirements for Mobile Privacy & Security, Sept. 16-17, 2002.