Original Research Paper Engineering

All About Wormhole Attack and its Remedies in Manet

Geetika Srivastava M.Tech. Scholar, Department of Electronics and Communication, IES College of Technology, Bhopal

Sonu Lal Assistant Professor, Department of Electronics and Communication, IES College of Technology, Bhopal

ABSTRACT

MANET stands for mobile Ad-Hoc network. This is a type of wireless network. Practically MANET suffers with various types of attacks. Some of them are easy to detect but some of them are very difficult. Due to this attack the packets may be tunneled to the unauthorized persons. This is not all desirable for any network. So security is a major challenge for MANET network designers. This paper is going to provide a method to make the MANET more secure. This paper deals with a special type of attack that is WORMHOLE attack and its type along with respective remedies will be cited.

KEYWORDS : MANET, Ad-Hoc, Wormhole Attack, Tunneling, OPNET modeler 14.0.

INTRODUCTION

Now a day wireless communication is playing a major role in our day to day life. Internet technology, cell phone services, satellite phones works on wireless technology. Mobile Ad-Hoc network (MANET) draws more attention towards wireless communication.

Fig-1: MANET Network

This network is very simple in nature because it has no fixed infrastructure. This means that any of the nodes can act as sender receiver or the router. This MANET is extremely helpful in case of rescue missions, military tactical operations and emergency law enforcement.

The special properties of MANET are robustness, easy deployment and dynamic topology.

PROBLEMS WITH MANET

Various researches have been carried out in increasing efficiency of MANET. During this the security of this network decreased. So, now a days lot of research are going on specially on security only.

Due to dynamic topology MANET is highly immune to attack. Still then there are various types of attack which affects MANET a lot.

ATTACKS ON MANET

Attack means the undesirable change in the functioning of designed MANET network. It is observed that sometimes MANET behaves completely against the desired function. This attack is broadly classified into two types:

Active Attacks: This attack hampers the proper functioning of the network. This is done by generally altering the route, altering data packets and so on. It is easy to detect this type of attack compared to others.

Passive Attacks: This attack do not alters the proper functioning of the network but silently draws the information from the packets. This is why it is difficult to detect this attack.

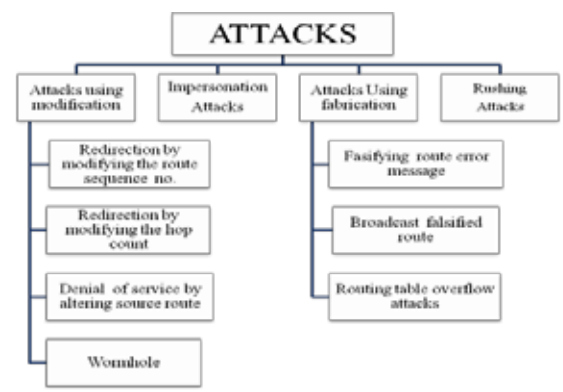

Fig 2: Types of Attack in MANET

This passive attack is further classified into four major categories as shown in figure 2.

WORMHOLE ATTACK

This is a type of passive attacks. In this attacker generally tunnels the packets to other area of network bypassing normal/desired routes as shown in fig 3 below.

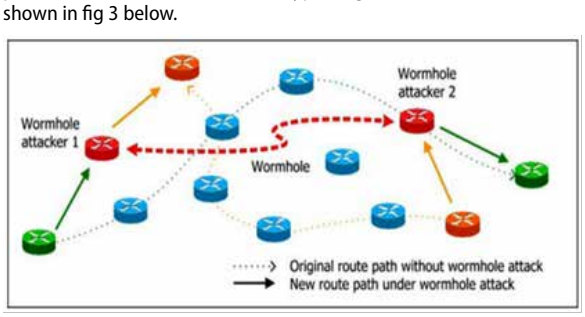

Fig 3: Wormhole attack in MANET

Here nodes appeared in black color are source and destination node. Nodes in blue color are authorized route nodes and node in orange color is attacker node. It is desired that packets will go from source to destination through desired path not the undesired path because authencity is a major issue.

In practice attackers may use high power antennas or wired links or some other devices. Whenever wormhole attack takes place the hope count and/or average time delay decreases abruptly.

When this attacks takes place attacker receives packet at one point and tunnels it to the other point of the network. If this attacker is dry honest then attack is advantage but should not be expected at all.

IMPACTS OF WORMHOLE ATTACK

Since the traffic is routed through the wormhole so the attacker gets full control over the traffic as well as data. After this attacker start malicious operations with the network. Tunneling means that every node gets few new routes. So, if these attacks take place the entire security of network vanishes completely. That's why it is highly desirable to detect this attack within timeframe and attacker must be black listed.

TYPES OF WORMHOLE ATTACK

In-band wormholes attackers are inside the network and they use the same radio channel and other gadgets that are made for other nodes. Attacker follows MAC protocol.

Out-of-band wormhole attackers use fast range connections. Like fast wired link or high gain transmitting antenna.

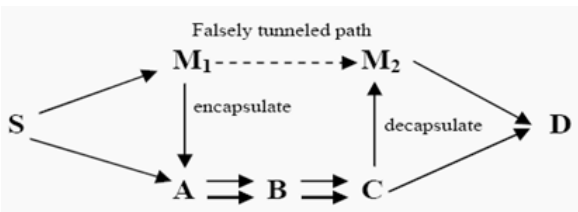

Fig 4: Tunneling

According to visibility of M1 and M2 wormhole attack can also be classified as **Closed Wormhole Attack**, **Half Open wormhole Attack** and **Open Wormhole Attack.**

In closed wormhole attack nodes M1 and M2 are not visible to adjacent nodes because they do not public their node id and MAC address. In half open either of M1 and M2 is visible to adjacent nodes. In open wormhole attack both of M1 and M2 are visible.

GOAL OF PROPOSED WORK

In the proposed research work the main aim is to detect the wormhole attack and to black list the attacker node so that in future packets could not be tunneled by this attacker node. Also, the effectiveness and efficiency of secure routing protocol of MANET will be evaluated.

PROPOSED RESEARCH METHODOLOGY

The proposed research is going to be executed as per flow chart shown below.

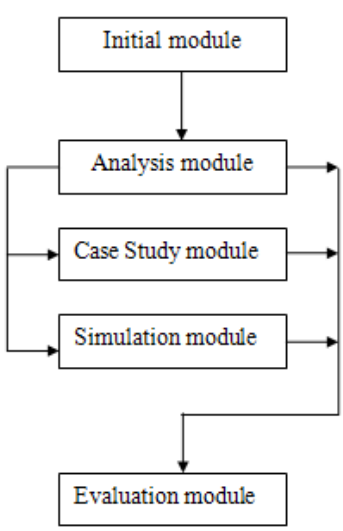

Fig 5: Steps of Research Methodology

INITIAL MODULE

Scope of research is mainly elaborated in this module. For this broad literature survey is carried out. Routing mechanism and MANET characteristic is studied out. Then information is gathered related to previous research. After this various secure routing protocols and attack patterns in Ad-Hoc pattern is studied

ANALYSIS MODULE

In this module detailed knowledge of Ad-Hoc routing protocols is obtained. Also they all are compared among themselves.

METHODOLOGY FOR CASE STUDY MODULE

For this purpose the attacks and their effect is considered. Number of attacker nodes is changed and their effect is observed and they are compared.

METHODOLOGY OF SIMULATION MODULE

Simulation is carried out with the help of OPNET Network Modeler 14.0. With this the practical efficiency of proposed scheme is found out.

To examine numerical and measurable characteristic of secure routing protocols quantitative approach is adopted.

METHODOLOGY FOR EVALUATION MODULE

Final conclusion of research will be found in this module. Data accumulated from previous modules are compared here.

CONCLUSION AND FUTURE WORK

This paper is for giving the idea about the research work which is going to be executed in the thesis. Step by step procedure of proposed research work is cited above.

REFERENCES

[1] N.Shanthi, Dr.Lganesan "Study Of Different Attacks On Multicast Mobile Ad Hoc Network," in Journal of Theoretical and Applied Information Technology, 2009, pp. 45– 51.

[2] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, "WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", In IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2008, pp. 343-348.

[3] Saurabh Upadhyay and Brijesh Kumar , " Impact of Wormhole Attacks on MANETs ", International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 77 Volume 2, Issue 1, February 201, pp.77-82

[4] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. *IEEE INFOCOM, Mar 2003.*

[5] Ali Ghaffari , " Vulnerability and Security of Mobile Ad hoc Networks ", in Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24, 2006, pp.124-129