IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

Study of Mobile Ad Hoc Network in the Presence of Wormhole Attack

F. Anne Jenefer[1], A. M. Merlin Ruby[2], D. Vidhya[3]

Assistant Professor, Electronics and Communication Engineering, Panimalar Engineering College, Chennai, India [1, 2, 3]

Abstract: A generic definition of security is "freedom from risk, danger or safety". Mobile Ad-Hoc Networks (MANETs) are a kind of wireless network that usually has a routable network environment above the link layer. It is a peer-peer self forming and self healing network. The nodes which are present in this network can move from one place to another in the network or may leave or join the network at any time. Due to this the topology of the network changes rapidly. Due to the absence of central administrator the MANETs are vulnerable to attacks. In this paper, performance comparison of MANET in the presence and absence of two types of wormhole attack such as replay and tunnelling has been carried out. The performance of the network is measured using metrics like Link Breakage and Delay in the network by varying the number of nodes and number of attackers. The study results prove that the network performance is severely affected in the presence of wormhole attack.

Keywords: Link Breakage, AODV, Mobile Ad-hoc Networks, Wormhole, Tunnelling, Replay.

I. INTRODUCTION

A wireless network ad hoc network is a decentralized type of wireless network. The network is defined as ad hoc because it doesn't rely on the previously existing infrastructure. An ad hoc network (Ad Hoc means "for this purpose") is a network you create on-the-fly, using direct Ethernet, FireWire, Wi-Fi, or even Bluetooth connections among your Macs. An ad hoc network does, of course, have its limits. If you're using the network to share Internet access, the number of people who can effectively join it will be limited by the amount of available bandwidth. And each connection method has its own limits. A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. To reach the destination node of a network, the other nodes in the network act as routers. MANETs have a wide range of applications, since it can be set up easily. Especially in military operations and disaster relief efforts MANETs plays a major role. However, MANETs are more vulnerable to security attacks both in wired and wireless networks.

MANETs are used in many applications like wireless sensor networks, rescue operations, sports events and conferences etc. because of its advantages like simple, cheap and fast setup of networks, more robust concerning failure of single component due to decentralized structure.

Features of Mobile Ad Hoc Networks: The Mobile Ad Hoc Networks has the following features,

- Dynamic network topology
- Fluctuating link capacity
- Autonomous terminal
- Multi-Hop routing
- Light-weight terminals
- Distributed operation

II. ABOUT WORMHOLE ATTACK

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. It is a severe type of attack, where two attackers are connected to each other through high speed off-channel link. A wormhole allows an attacker to create two attacker controlled choke points to which traffic is attracted and which can be utilized by the attacker to degrade or analyse traffic at a desired time. The covert communication channel used by the attackers could be a separate communication mechanism not generally used by the network, forming an out-of-band wormhole attack.

If the attacker performs this tunnelling honestly and reliably, no harm is done. The attacker actually provides a useful service in connecting the network more efficiently. However, the worm-hole puts the attacker in a very powerful position relative to other nodes in the network, and the attacker could exploit this position in a variety of ways. The wormhole node receives the packet at one location and sends it to other wormhole node through high speed off-channel link. Wormhole refers to an attack on MANET routing protocols in which colluding nodes create an illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbours but are actually distant from one another.

There are 6 types of wormhole attacks. They are shown below:

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

All Pass: The wormhole nodes will pass all the packets irrespective of their size.
All Drop: All the packets are dropped by wormhole nodes in the network.
Threshold: The Wormhole node drops all the packets size greater than or equal to the threshold value.
Replay: The Packets are replayed by the wormhole node after tunnelling in the network.
Tunnelling: The Wormhole node tunnels the packet from one point to another through the wormhole link in the network.
Propagation Delay: The propagation delay in the network is increased due to the wormhole nodes.

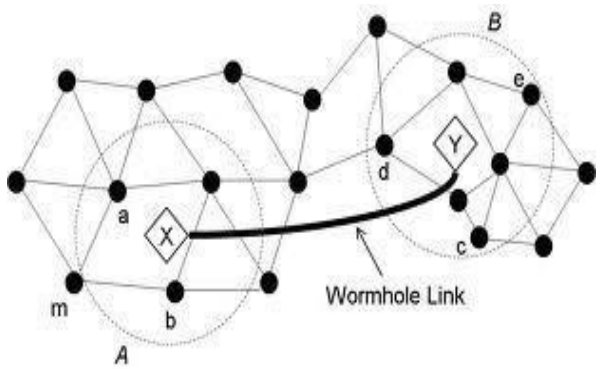

Fig.1: Wormhole Attack in a Network.

Fig.1 shows the wormhole attack in a Network. Here the nodes a, b, c, d and e are involved in communication with each other. The nodes X and Y are the wormhole nodes and they form a link between them called "Wormhole Link". Through this wormhole link the wormhole node tunnels the data packets from one end to another.

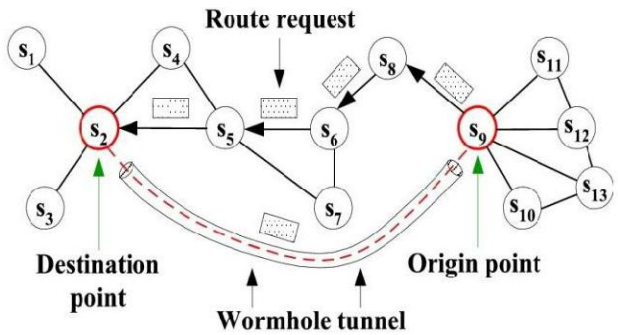

Fig.2: Wormhole-Tunnelling Attack in a Network.

Fig.2 shows the wormhole-tunnelling attack in a Network. As seen in the previous figure, figure2 also creates shows that the wormhole nodes creates a link between them called wormhole link and tunnels the packets from one end to another. In this figure there are several nodes from node S1 to node S13. The nodes S2 and S9 act as the wormhole nodes in the network. Here the tunnelling is caused due to a wired link or a high frequency link. This creates the illusion that the two end points of the tunnel are very close to each other. A direct link can be established via a wire line, a long-range wireless transmission, or an optical link.

There are certain attack modes in which the wormhole attacks can be launched. They are Hidden modes and Participation Modes. It is further divided as follows:

- Packet Encapsulation
- Packet Relay
- High Power Transmission
- Out of Band

III. FLOW CHART

In this section the flow diagram of the study of MANET and the associated parameters of the proposed system are discussed. The flow diagram for the proposed system is shown in fig.3.

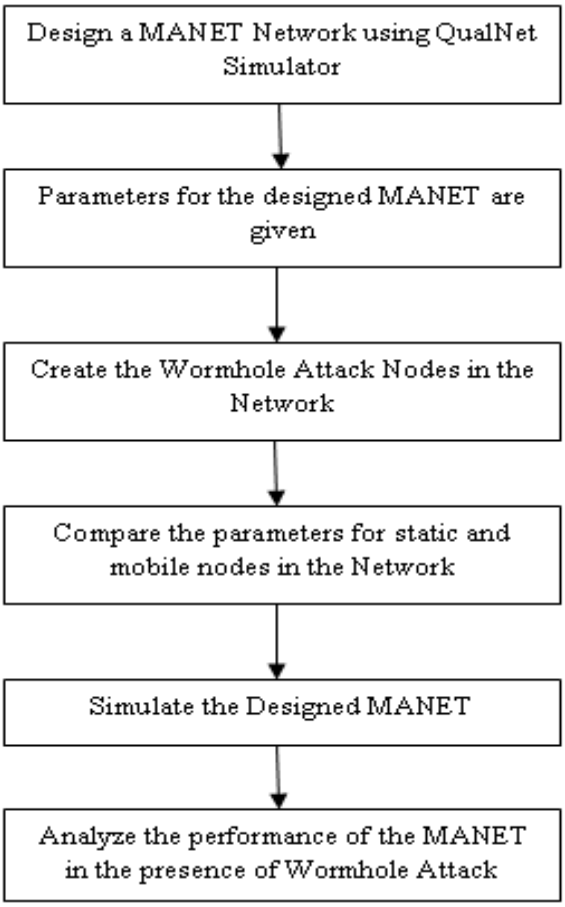

Fig.3: Flow diagram of proposed system.

As shown in the above flow diagram initially a MANET is designed using the QualNet simulator. Then the network parameters such as routing protocols, data rate, etc. are been set in the simulator for the designed network. The wormhole nodes are created by changing the properties of the node in the MAC layer. The MAC layer of the subnet is also changed for enabling the wormhole attack in the network. The simulation time and the mobility speed of the nodes are given in the scenario properties and the network which is designed is simulated using the Qual Net Network simulator.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

IV. MOBILE AD HOC NETWORK

A. Designing MANET

MANET which is designed for the analysis is been simulated using the Qual Net simulator, with different number of nodes such as 10, 20 and 30 nodes. For each network varying number of passive intruders were included. CBR traffic link was used for communicating between the nodes. Initially, MANETs without any attacks have been created for performance comparison. The network parameters such as throughput, end-to-end delay and jitter are used for analysis purpose. The nodes are grouped using the wireless subnet in the simulator.

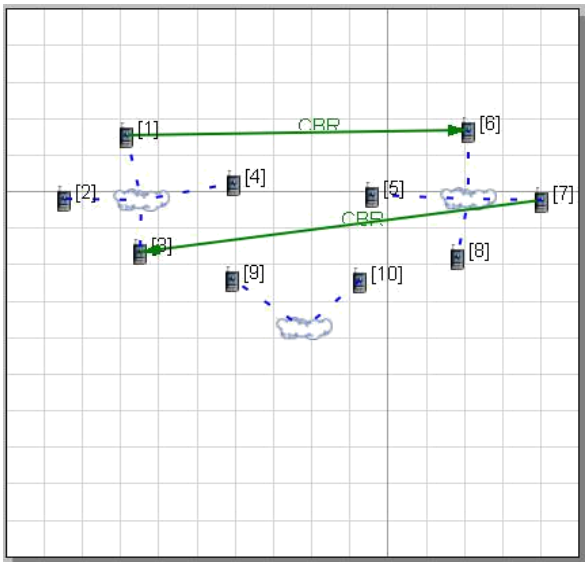

Fig.4: MANET designed using Qual Net Simulator.

Fig.4 shows the MANET which is design without the wormhole attack for the analysis. The network with 10 nodes and 2 CBR links is shown in the above figure. Here, nodes 1 and 7 represent the source nodes and the nodes 3 and 6 represent the destination nodes.

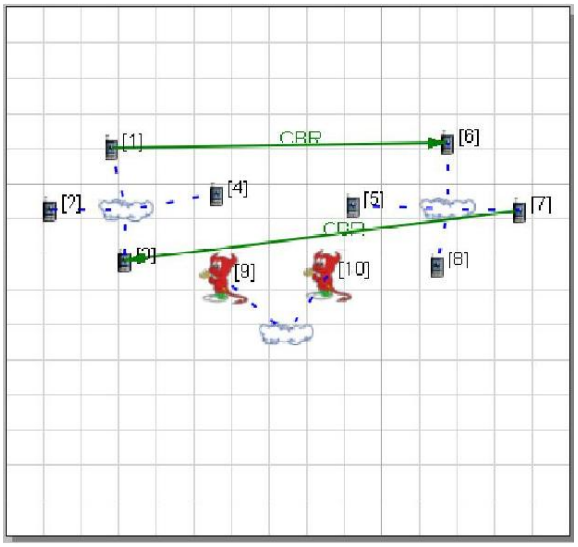

Fig.5: MANET designed with two Wormhole Attacks

The subnets in the network are shown in the form of cloud which indicates the wireless link in the MANET network. The CBR links are given with the data rate of 2 Mbps for the network with and without the wormhole attack.

Fig.5 shows the MANET which is designed with two wormhole attacks in the network. The network with 10 nodes and 2 CBR links is shown for example. Here also the nodes 1 and 7 represent the source nodes and the nodes 3 and 6 represent the destination nodes. The nodes 9 and 10 represent the wormhole nodes in the network which is shown in the form of daemon in the Mobile Ad Hoc Network.

B. Parameter for Simulations

The QualNet 5.2 simulator is used for simulation. The MAC protocol IEEE 802.11 was used with a data rate of 2 Mbps. The values of each parameter used in designing the network are shown in the Table 1.

TABLE 1 Simulation Parameters needed for designing MANET.

Parameter	**Value**
Terra in Size	1500m×1500m
Traffic Type	CBR
Mobility Model	Random way Point
Routing Protocol	AODV
MAC	802.11
Packet Size	512 Bytes
Speed	0-10 m/s
Simulation Time	300 sec
Attack Type	Wormhole

C. Performance Metrics

Performance metrics which are considered to analyse the performance of the MANET are explained below.

Link Breakage: When a link breaks, a RERR message is propagated to both the end nodes. This indicates that the AODV does not repair the link locally, but rather makes the end nodes to discover alternate routes to the source. Moreover link breakage caused by the movement of end nodes also results in initialization of route discovery process.

Average End-to-End Delay: Average end-to-end delay is the average time taken by a data packet to reach to destination in seconds. It is calculated by subtracting "time at which first packet was transmitted by source" from "time at which first data packet arrived to destination".

V. QUALNET SIMULATOR

The QUALNET communications simulation platform is a planning, testing and training tool that "mimics" the behavior of a real communications network. Simulation is a cost-effective method for developing, deploying and

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

managing network-centric systems throughout their entire lifecycle. Users can evaluate the basic behavior of a network, and test combinations of network features that are likely to work. Qual Net executes on all commonly used platforms including Windows NT/2000/XP Professional, Solaris, Linux, and most UNIX variants.

The Qual Net Simulator enables the users to:

- Design new protocol models.
- Optimize new and existing models.
- Design large wired and wireless networks using pre-configured or user-designed models.
- Analyse the performance of networks and perform what-if analysis to optimize them.

The key features of QualNet that enable creating a virtual network environment are speed, scalability, model fidelity, portability and extensibility. QualNet provides a comprehensive environment for designing protocols, creating and animating network scenarios, and analysing their performance. QualNet is a commercial version of GloMoSim used by Scalable Network Technologies for their defence projects. It is a commercial network simulator from Scalable Network Technologies, Inc in 2000-2001. This tool is an extension of GloMoSim which is being commercialized. It is ultra high fidelity network simulation software that predicts wireless, wired and mixed-platform network and networking device performance.

QualNet Developer is network evaluation software that analyses the performance of wired, wireless and hybrid network. QualNet supports thousands of nodes for simulation and also supports for 64 bit Operating system. It works on UNIX, Linux and MacOS and even can be deployed in live networks. They have separate licenses for Academics and others. QualNet is designed to simulate large-scale wired and wireless networks with thousands of mobile nodes, each of which may different communication capabilities via multi-hop ground, aircraft and satellite media. It uses the parallel simulation environment for complex systems (PARSEC) for basic operations, hence can run on distributed machines.

QualNet includes a graphical user interface for creating the model and its specification. So, it is very easy to specify small to medium networks by using the GUI. Since it uses primarily Java for the GUI, it is available for Linux as well as for Windows. It is a state-of-the-art simulator for large, heterogeneous networks and the distributed applications that execute on those networks. The features of QualNet provide a unique capability for accurate, efficient simulation of large-scale, heterogeneous networks. Robust set of wired and wireless network protocol and device models are useful for simulating diverse types of networks.
QualNet is a state-of-the-art simulator for large, heterogeneous networks and the distributed applications that execute on those networks. The following QualNet features provide a unique capability for accurate, efficient simulation of large-scale, heterogeneous networks:

- Robust set of wired and wireless network protocol and device models, useful for simulating diverse types of networks.
- A robust GUI interface covers all aspects of the simulation, from scenario creation and topology setup, integration of custom protocols, through real-time execution of network models from within the GUI, animation, to post-simulation statistical analysis.
- QualNet is used to simulate high-fidelity models of wireless networks with as many as 50,000 mobile nodes.
- Optimized for speed and scalability on one processor, QualNet executes equivalent scenarios 5-10x times faster than commercial alternatives.

VI. SIMULATION METHODS

This section presents the simulation methods and nodes mobility for the simulation purpose. The performance of the MANETs with and without the wormhole attacks analysing certain parameters is discussed in this paper. The network can be analysed by comparing the performances of both the static and mobile nodes. For the different number of nodes and passive intruders the Link Breakage and average end-to-end delay are used. As per the analysis the network performances degrades with the increase in number of nodes and passive intruders. The delay for the network increases with the increase in number of nodes and intruders.

A. Static Nodes

The performance of the network for different number of nodes and passive intruders are been analysed in this paper. The network for the static and mobile nodes of MANET are been analysed. In case of static nodes the throughput of the network increases with the decrease in number of nodes. The performances of the network with and without the passive intruders are been compared for analysis purpose.

The network with and without passive intruders are compared for the network parameter Link Breakage and Delay. The Delay increases for the network which includes the wormhole attack. And it is low for the network without any wormhole attack. As such for static nodes the analysis are been done for the network with mobile nodes.

B. Mobile Nodes

The network with and without passive intruders are compared for the analysis purpose. The network parameters such as Link Breakage and Delay are been analysed for the mobile nodes. As discussed for static nodes, mobile nodes also have increased throughput in-case of network without any attack. The end-to-end delay of the network is increased for the network with passive intruders.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

VII. CONCLUSION

In this paper, the performance of MANET with and without wormhole attack was analysed. The simulation methods have concluded that the performance of the MANET degrades due to wormhole attack. The throughput of the network decreases with the increase in the number of attackers. The end-to-end delay and Link Breakage increases with the increase in the number of attackers in the network.

A. References

The heading of the References section must not be numbered. All reference items must be in 8 pt font. Please use Regular and Italic styles to distinguish different fields as shown in the References section. Number the reference items consecutively in square brackets (e.g. [1]). When referring to a reference item, please simply use the reference number, as in [2].

VIII. FUTURE WORK

The future includes the detection of such wormhole attacks in the MANETs by simulating and analysing the various communication parameters such as Link Breakage and Average End-to-End delay in the MANETs.

REFERENCES

[1] R. Gilbert, K. Johnson, S. Wu, B. Y. Zhao, and H. Zheng, "Location Independent Compact Routing for Wireless Networks", In MobiShare '06: Proceedings of the 1st International Workshop on Decentralized Resource Sharing in Mobile Computing and Networking, July 2006.

[2] Pardeep Kaur and Deepak Aggarwal, "Performance Evaluation of Routing Protocols in MANETs under Wormhole Attack", International Journal of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 8, December 2012.

[3] Maitreya Natu and Adarshpal S. Sethi, "Intrusion Detection System to Detect Wormhole using Fault Localization Techniques" collaborative participation in the Communications and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011..

[4] Rajendra V. Boppana and Xu Su, "On the Effectiveness of Monitoring for Intrusion Detection in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol.10, no.8, pp. 1162-1174, August 2011.

[5] R.V. Boppana and X. Su, "An Analysis of Monitoring Based Intrusion Detection for Ad Hoc Networks," Proc. IEEE Globecom: Computer and Comm. Network Security Symp., Dec. 2008.

[6] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[7] L. Zhou, Z.J. Haas, "Securing ad hoc networks", IEEE Network Mag. 13 (6) (1999).

[8] Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, and David B. Johnson, Member, IEEE, "Worm Hole Attacks in Wireless Networks", 370 IEEE Journal on selected areas in Communications, Vol. 24, no.2, February 2006.

[9] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks", in Proc. of INFOCOM 2003, San Francisco, CA, USA, April 2003.