AN ENHANCED APPROACH FOR WORMHOLE DETECTION & PREVENTION IN MANETS

Deepika Sharma[1], Kanta[2], Gaurav Banga[3]

[1,2,3]*Electronics and Communication Engineering Department ,*

Institute of Science and Technology, Klawad/Kurukshetra,(India)

ABSTRACT

In communication wireless technology achieve popularity in both home and business networking communication. A popular wireless technique is mobile ad-hoc network. In ad-hoc networks, communications are done over wireless media between stations directly in a peer to peer fashion without the help of wired base station or access points. Securing wireless ad hoc networks is a highly challenging issue. In this paper we suggest a new method to detect and prevent the network from wormhole attack in on demand routing protocol. This particular algorithm facilitates a digital Signature to communicate between sender & receiver. Malicious node whose Digital Signature value does not match with the defined Digital Signature, cannot impersonate and use another node authentication.

Keywords: Digital signature Manet, Wormhole Attack

I. INTRODUCTION

Wireless communication is a technology that is growing at a very fast pace and has replaced approximately all wired network due to its heavy advantages. Wireless Networks are classified in two classes - infrastructure network and infrastructure less (ad-hoc) networks. In these, the ad-hoc networks works without any pre-existing infrastructure [1]. Mobile ad hoc networks consist of mobile devices which communicate over wireless links without any support from a fixed infrastructure. Mobile ad hoc networks are applicable to a wide variety of applications that includes disaster recovery or tactical communication and connection of multiple mobile users in an area at low cost with the use of portable devices such as PDAs (Personal Digital Assistants), laptops, cell phones, media players, etc. Users of these devices can exchange photos, music files etc, within proximity without connecting to a fixed or Internet infrastructure. Below is a typical MANET architecture shown in figure 1.1.

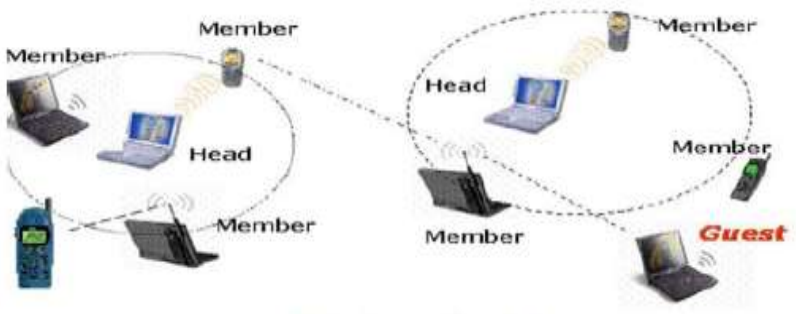

Figure 1.1: Manet Architecture

II. WORMHOLE ATTACK

A wormhole attack is a particularly severe attack on MANET routing where say two attackers who are connected by a link which is high-speed off-channel, and who are strategically placed at different ends of a network. These attackers then overhear the wireless data and record. Then they replay the packets at the other end of the network. Attackers replay these valid network messages at some other places, which can make far apart nodes believe that they are immediate neighbours, thus forcing all communications between affected nodes to go through them [2].

Usually, ad hoc routing protocols fall into two categories: proactive routing protocols that rely on periodic transmission of routing updates, and on-demand routing.

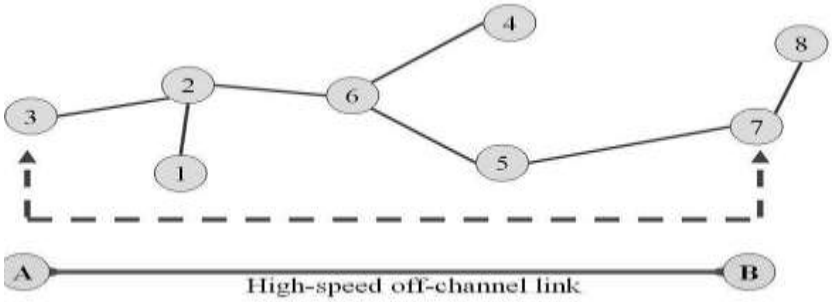

Figure 2.1: A Network Under a Wormhole Attack [38]

A wormhole attack is equally dangerous for both proactive and on-demand protocols. When a proactive routing protocol as Optimized Link-State Routing (OLSR) is used then ad hoc network nodes send periodic HELLO messages to each other indicating their participation in the network. In Figure 2.1, when node 3 forwards a HELLO message then the intruder A forwards it to the other end of the network where node 7 hears this HELLO message .Now Since 7 can hear a HELLO message from 3, it assumes itself and node 3 to be direct neighbours. Thus, if 7 want to forward anything to 3 then it will do so through the wormhole link, giving the wormhole attackers full control of the communication link and in on demand routing protocol when one node have to communicate with other node it sends a request to other nodes so that it can found shortest path as shown in above diagram there are two possible routes one 3, 4, 7 and is 2, 6, 5 and node will communicate from shortest path and there are chances of worm hole attack.

III. PROBLEM FORMULATION AND OBJECTIVE

The wormhole attack is principally dangerous against many ad hoc network routing protocols in which the nodes that listen a packet transmission directly from some node[4] The central research dilemma is how to provide security protection to the network topology and the routing process in a wireless network communication and detect the attacker(s) by verifying their digital signatures within routing path in MANETS and protect the network from the unwanted nodes present in the network by isolating them from the whole network

IV. SIMULATION PARAMETERS AND RESULTS

Table 4.1: Simulation Parameters

Parameters	Value
Simulator	NS 2.34
Simulation Area	1000X1000
Number of Mobile Nodes	40
Channel	Wireless
Routing Protocols	AODV
Simulation Time	500 Sec
Traffic Class	TCP
MAC Layer	802.11

To fulfil the research objective, simulation is performed. Following figures show the simulation result with or without wormhole attacks.

Transfer of packets for 40 Nodes using AODV protocol is shown in figure 4.1 in which no node is detected as wormhole attacker.

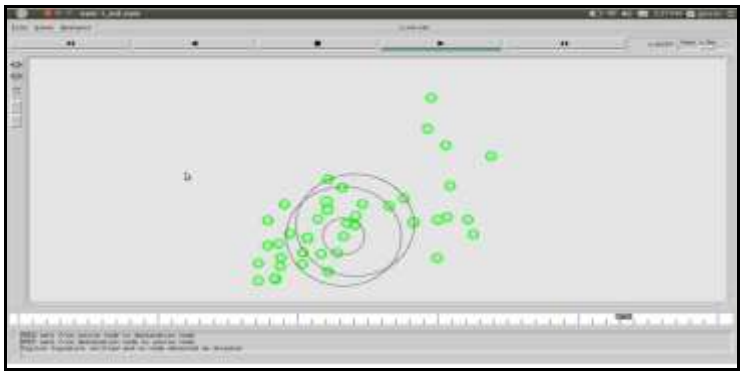

Figure 4.1: Transfer of Packets for 40 Nodes Using AODV

Transfer of packets for 40 Nodes using AODV protocol is shown in figure below, in which one node is detected as wormhole attacker. In figure 4.2 the node having red color is the wormhole attacker after verification of digital signature.

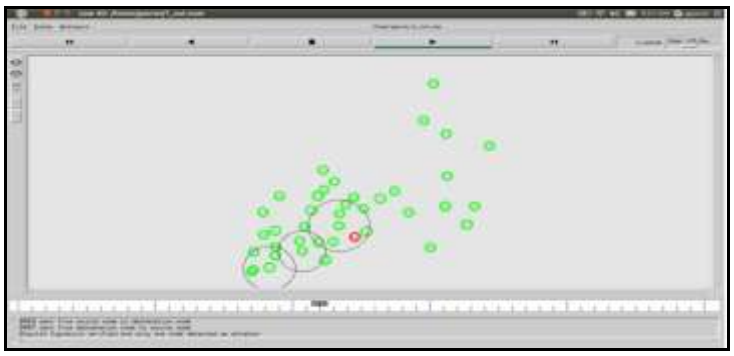

Figure 4.2: Transfer of Packets for 40 Nodes with One Node Detected as Wormhole

Transfer of packets for 40 Nodes using AODV protocol is shown in figure 4.3 in which two nodes is detected as wormhole attacker. In figure 4.3, nodes having red color are the wormhole attacker after verification of digital signature.

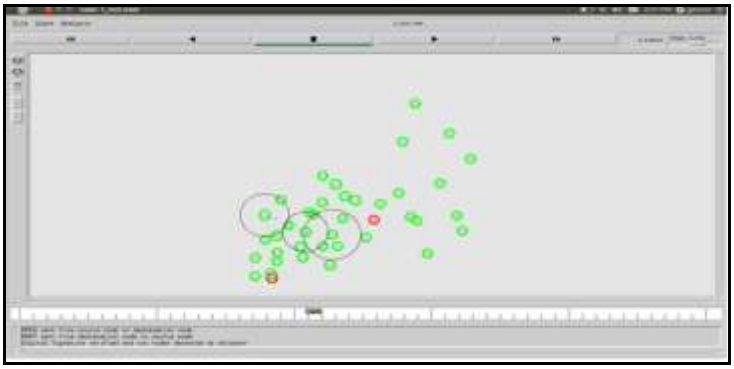

Figure 4.3: Transfer of Packets for 40 Nodes with Two Nodes Detected as Wormhole

Transfer of packets for 40 Nodes using AODV protocol is shown in figure 4.4 in which one node is detected and isolated as wormhole attacker. The node in figure 4.4, having red color is the wormhole attacker after verification of digital signature and moved away from the network.

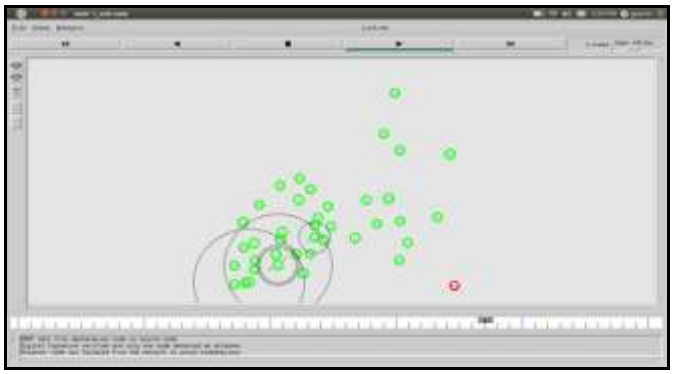

Figure 4.4: Transfer of Packets for 40 Nodes with one Node Isolated as Wormhole Attacker

Transfer of packets for 40 Nodes using AODV protocol is shown in figure 4.5 in which two nodes are detected as wormhole attacker. Figure 4.5 shows the nodes having red color is the wormhole attacker after verification of digital signature and moved away from the network.

Figure 4.5: Transfer of Packets for 40 Nodes with Two Nodes Isolated as Wormhole Attacker

Graph representation of packet received over packet drop for 40 Nodes using AODV approach is shown in figures given below.

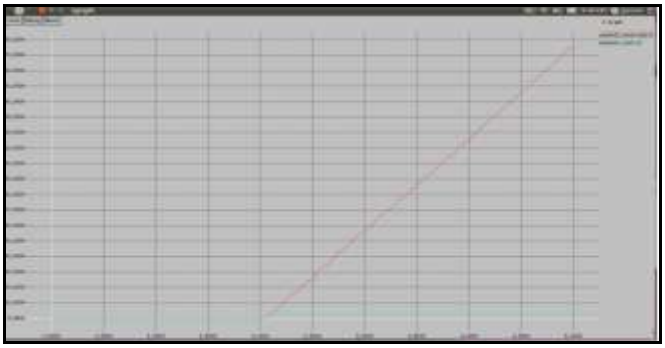

Figure 4.6: Graphical Representation of Transfer of Packets for 40 Nodes with One Node as Wormhole

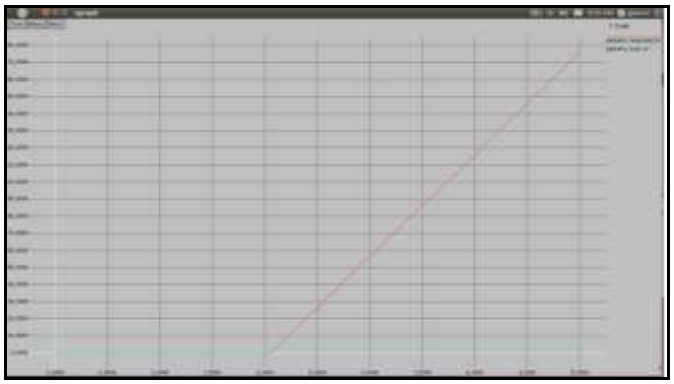

Figure 4.7: Graphical Representation of Transfer of Packets for 40 Nodes with Two Nodes as Wormhole

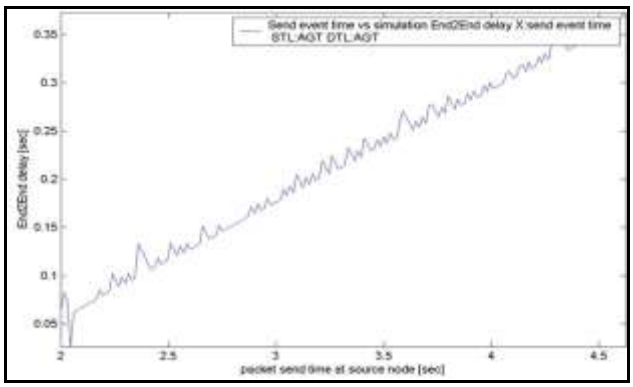

Figure 4.8: End to End Delay for 40 Nodes Using AODV one Node as Wormhole

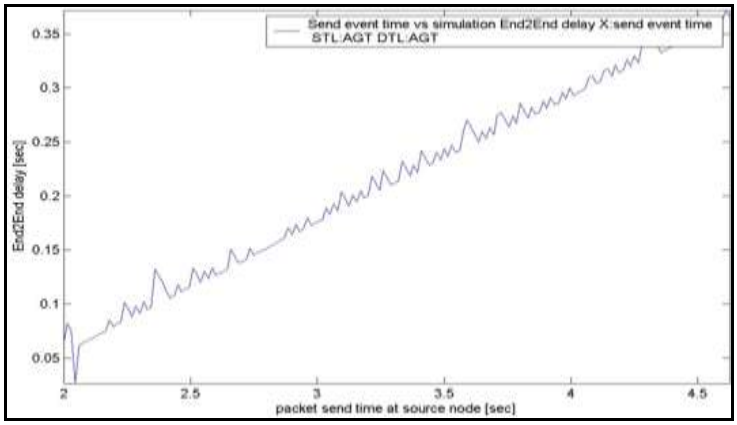

Figure 4.9: End to End Delay for 40 Nodes Using AODV two Node as Wormhole

We implement the random way point movement model for simulation in which nodes start at random position. With simulation time 500 seconds and 1000*1000 simulation area. A maximum speed of 20m/s. Pause time is 10 seconds. Traffic type is TCP. Payload size 512 bytes and a malicious node with a tunnel.

Figure 4.6 & 4.7 shows that when there is the malicious node in the network then number of packet received by receiver is less than the packet sends by sender. When we apply digital signature scheme then packet received by receiver is equal to the packet send by sender.

Figure 4.8 & 4.9 shows the comparison of end to end delay, The end to end delay is increased as we increase the number of nodes because it increases the packets in the network due to broadcast of route request RREQ again and again. All nodes contain the digital signature of every other node due to which end to end delay is increased.

V. CONCLUSION

A wormhole is one of regularly occurring attack which is formed by two malicious nodes and a tunnel. To protect from wormhole attack we used the scheme called detection & prevention approach with verification of legitimate nodes in network through its digital signature.

REFERENCES

[1]. Gaurav Banga, Shakti Kumar and Amar Singh, "e-EPSAR : Enhanced Efficient Power Saving Adaptive Routing Algorithm for Mobile Ad-hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue. 8, August 2013.

[2]. Ajay Prakash Rai et. al.(2012), "Wormhole Attack Detection in Mobile Ad Hoc Networks", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 2, August 2012.

[3]. Jacquet et. Al.(2003), "Optimized Link State Routing Protocolfor Ad hoc Networks", The Internet Society, 2003.

[4]. W. Wang, B. Bhargava(2004), "Visualization of wormholes in sensor networks", Proceedings of the 2004 ACM workshop on Wireless Security, pp. 51-60, 2004.

[5]. Hu, A. Perrig, D. Johnson(2003), "Rushing Attacks and Defence in Wireless Ad Hoc Network Routing Protocols", Wise 2003, September 19, 2003, San Diego, California, USA.

[6]. Y.-C. Hu, A. Perrig, D. B. Johnson(2006), "Wormhole Attacks in Wireless Networks, Selected Areas of Communications", IEEE Journal on, vol. 24, numb. 2, pp. 370-380, 2006.

[7]. Y.-C. Hu, A. Perrig, D. B. Johnson(2003), "Packet leashes: a defence against wormhole attacks in wireless networks", INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, Vol. 3, March 30 -April 3rd 2003, pp. 1976-1986.