AN EFFICIENT APPROACH FOR WORMHOLE DETECTION & EVADING IN DSR FOR MOBILE AD HOC NETWORK

Manju Saini[1], Rupal Satija[2]

[1,2] *Computer Science and Engineering Department*

World College of Technology and Management, Gurgaon (Haryana), India

ABSTRACT

Wireless networks are capable of being affected by many attacks, along with an attack known as the wormhole attack. A wormhole attack is very difficult to prevent because of its effectiveness. In wireless network wormhole can cause a meaningful breakdown in communication. 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. 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. Because of 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. If the attacker performs this tunnelling genuinely, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. Though, the wormhole brings the attacker in a very powerful position compare to other nodes in the network, and the attacker could handle this position in a variety of ways. In this paper, we determine wormhole attack nature in ad hoc networks and existing methods of the defending mechanism to detect & isolate wormhole attacks with DSR routing protocol using digital signature without require any particular hardware.

Keywords: Digital Signature, DSR, Manet, Wormhole Attack

I. INTRODUCTION

Wireless network refers to any type of computer network that uses wireless for network connections. Wireless telecommunications networks are usually implemented using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure. Wireless networks fetch necessary changes to data networking and makes combined networks valid. Wireless network offers a network without wires because by using wireless network we can connect our computer to a network using radio waves and can move our computer anywhere easily. In wireless network air is used as a medium. The rapid adoption of wireless networking technology in the commercial sector using IEEE 802.11- based WLAN specifications is an excellent example [1]. Wireless networks introduced by IT Consulting group with IEEE certified 802.11b technology. A wireless network provides us secrecy and private computer security more than before. A Wireless networks presenting flexibility, roaming, high standard and low cost. Different types of wireless network are wireless LAN, wireless MAN, and mobile devices network. Mobile ad hoc network nodes are furnished with

wireless transmitters and receivers using antennas, which may be highly directional (point-to-point), unidirectional (broadcast), probably steerable. At a given point in time, depending on positions of nodes, their transmitter and receiver coverage patterns, communication power levels and co-channel interference levels, a wireless connectivity in the form of a random, multichip graph or "ad hoc" network exists among the nodes. This ad hoc topology may modify with time as the nodes move or adjust their transmission and reception parameters.

A wormhole attack is a particularly severe attack on MANET routing where two attackers, connected by a high-speed off-channel link, are strategically placed at different ends of a network. These attackers then record the wireless data they overhear, forward it to each other, and replay the packets at the other end of the network. Replaying valid network messages at improper places, wormhole attackers can make far apart nodes believe they are immediate neighbors, and force all communications between affected nodes to go through them. In general, ad hoc routing protocols fall into two categories: proactive routing protocols that rely on periodic transmission of routing updates, and on-demand routing.

II. PROBLEM FORMULATION AND OBJECTIVE

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 tunnelled distances longer than the normal wireless transmission range of a single hop, it is easy for the attacker to make the tunnelled packet than a normal multihop route.

It is also possible for the attacker to forward every bit over the wormhole directly, without waiting for whole packet to be received before beginning to tunnel the bits of the packet, in order to reduce 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. If the attacker performs this tunnelling genuinely and accurately, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. However, the wormhole puts the attacker in a very powerful position compare to other nodes in the network, and the attacker could utilize this position in a variety of ways. Furthermore, the attacker is invisible at higher layers; unlike a malicious node in a routing protocol, which can often easily be named, the presence of the wormhole and the two colluding attackers at either endpoint of the wormhole are not visible in the route. The objective is to detect the node(s) which are having misbehavior characteristics by verifying their digital signatures within routing path in MANETS and to evaluate the performance and the feasibility of more secure network by considering a set of parameters.

III. SIMULATION MODEL

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	1200X1200
Number of Mobile Nodes	50
Channel	Wireless
Routing Protocols	DSR
Simulation Time	500 Sec
Traffic Class	TCP
MAC Layer	802.11

The simulation is performed to fulfill the research objective. The following figures show the simulation result with or without wormhole attacks.

Transfer of packets for 50 Nodes using DSR protocol is shown in Figure 3.1 in which no node is detected as wormhole attacker.

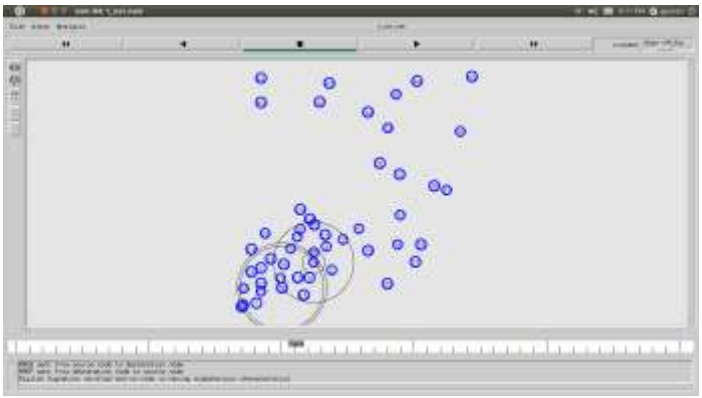

Figure 3.1: Transfer of Packets for50 Nodes Using DSR

Transfer of packets for 50 Nodes using DSR protocol is shown in Figure 3.2 in which one node is detected as wormhole attacker. In Figure 3.2 the node having yellow color is the wormhole attacker after verification of digital signature.

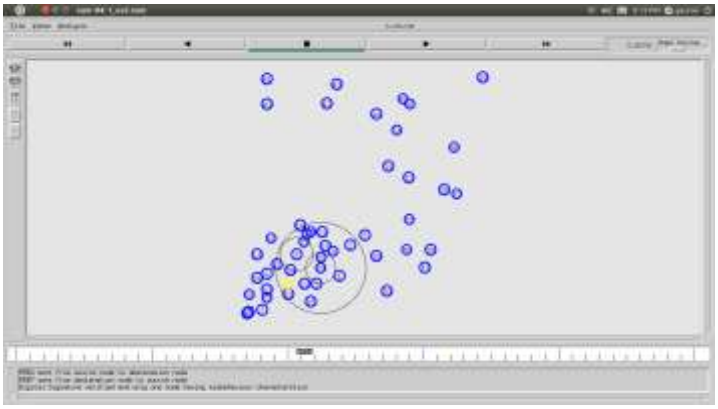

Figure 3.2: Transfer of Packets for 50 Nodes with one Node Detected as Wormhole

Transfer of packets for 50 Nodes using DSR protocol is shown in Figure 3.3 in which two nodes is detected as wormhole attacker. In Figure 3.3 the nodes having yellow color is the wormhole attacker after verification of digital signature.

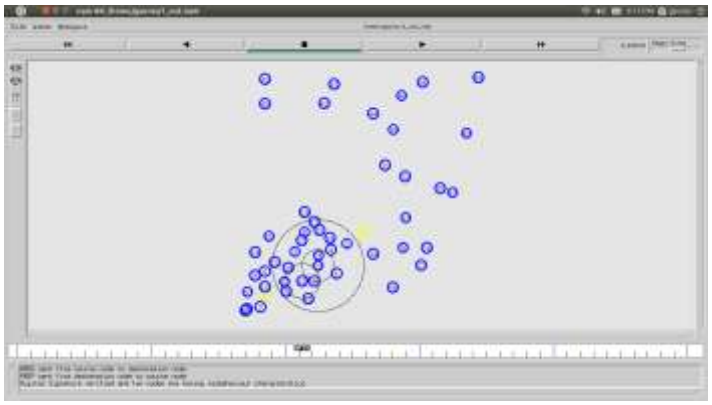

Figure 3.3: Transfer of Packets for 50 Nodes with two Nodes Detected as Wormhole

Transfer of packets for 50 Nodes using DSR protocol is shown in Figure 3.4 in which one node is detected and isolated as wormhole attacker. In Figure 3.4 the node having yellow color is the wormhole attacker after verification of digital signature and moved away from the network.

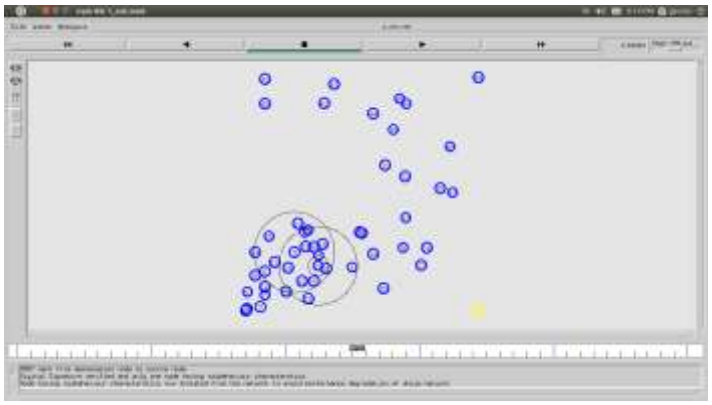

Figure 3.4: Transfer of Packets for 50 Nodes with One Node Isolated as Wormhole Attacker

Transfer of packets for 50 Nodes using DSR protocol is shown in Figure 3.5 in which two nodes is detected as wormhole attacker. In Figure 3.5 the nodes having yellow color is the wormhole attacker after verification of digital signature and moved away from the network.

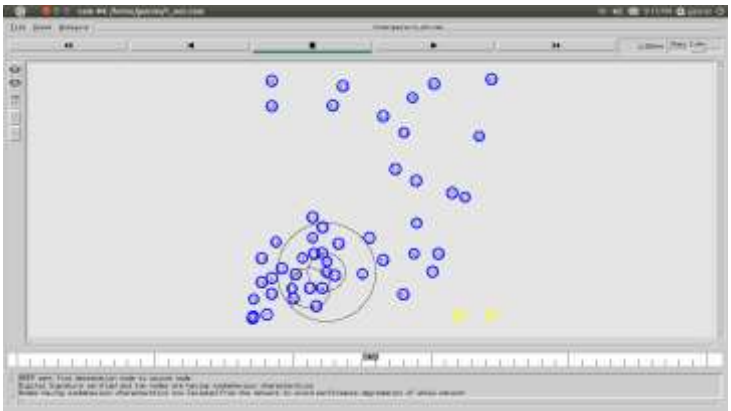

Figure 3.5: Transfer of Packets for 50 Nodes with Two Nodes Isolated as Wormhole Attacker

Graphical representation of packet received over packet drop for 50 Nodes using DSR approach is shown in graphs given below.

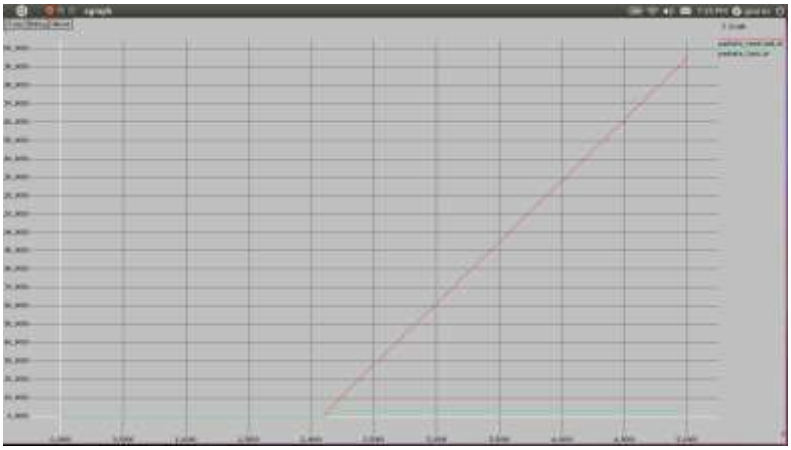

Figure 3.6: Graphical Representation of Transfer of Packets for 50 Nodes Using DSR

Figure 3.7: Graphical Representation of Transfer of Packets for 50 Nodes with One Node as Wormhole

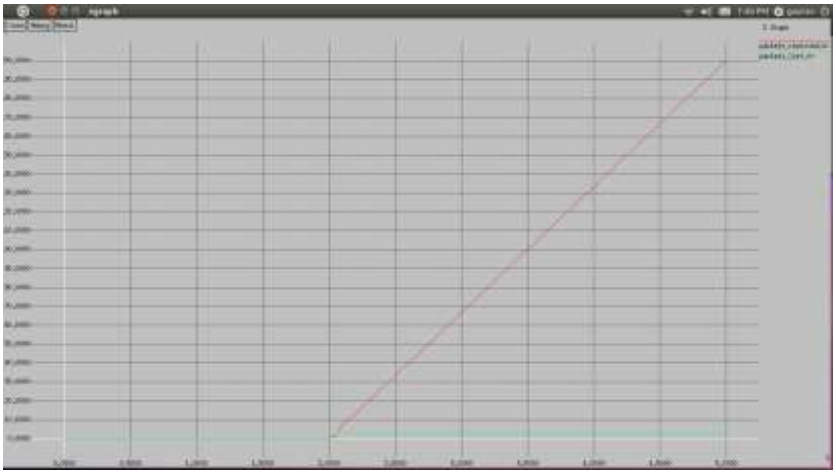

Figure 3.8: Graphical Representation of Transfer of Packets for 50 Nodes with Two Nodes as Wormhole

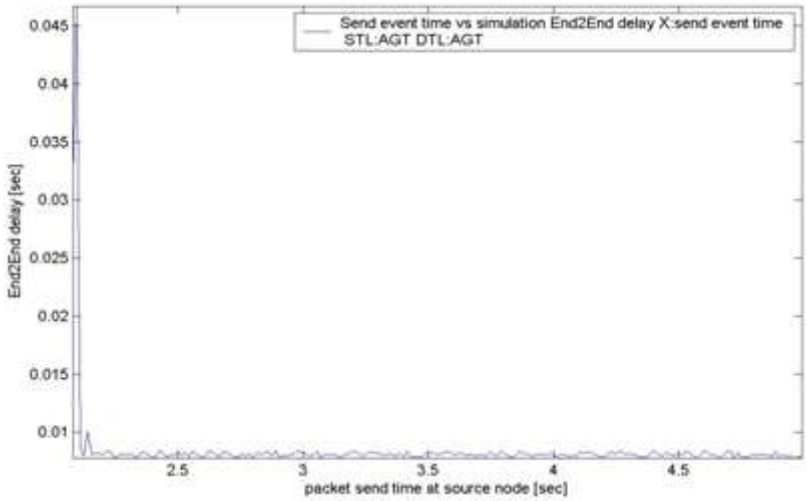

Figure 3.9: End to End Delay for 50 Nodes using DSR

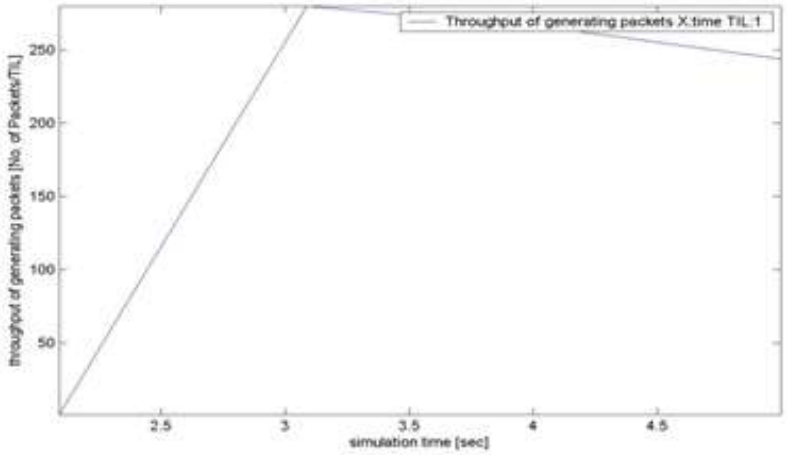

Figure 3.10: Throughput for 50 Nodes using DSR

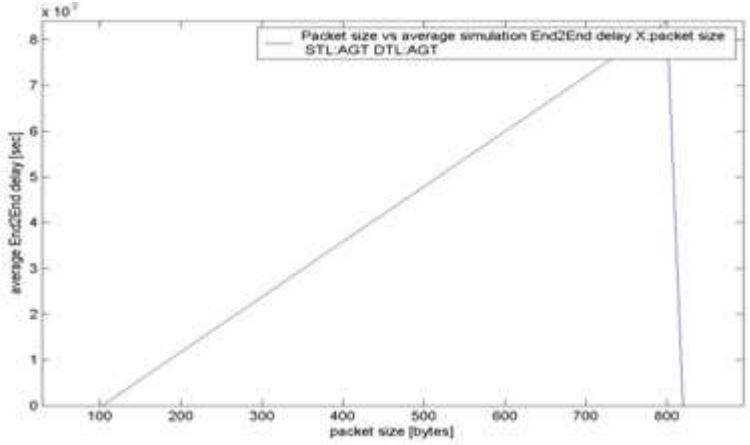

Figure 3.11: Packet Size vs. Average End to End delay for 50 Nodes using DSR

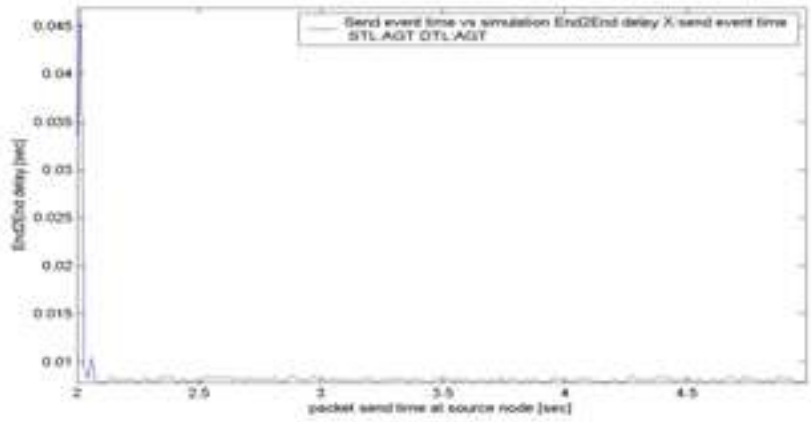

Figure 3.12: End to End Delay for 50 Nodes using DSR one node as wormhole

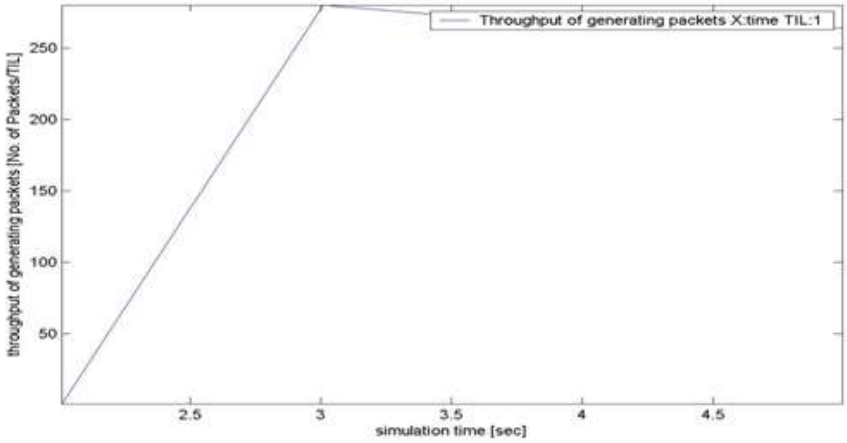

Figure 3.13: Throughput for 50 Nodes using DSR one node as wormhole

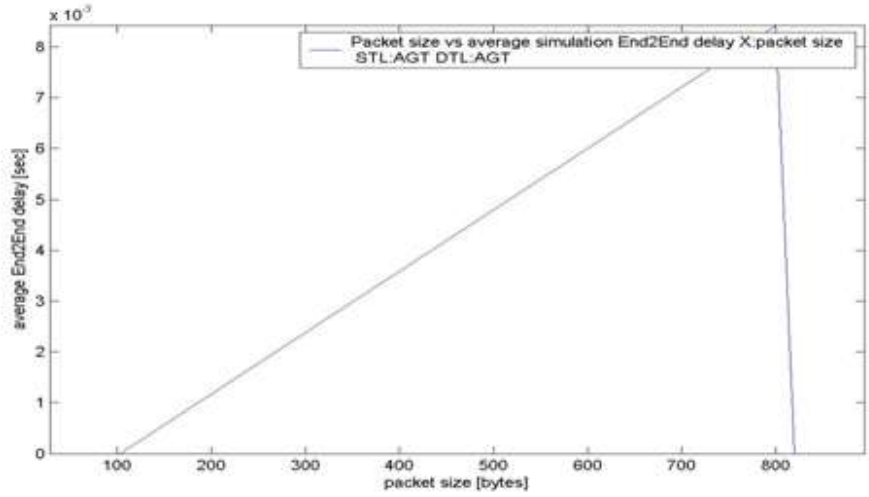

Figure 3.14: Packet Size Vs. Average End to End Delay for 50 Nodes Using DSR One Node as Wormhole

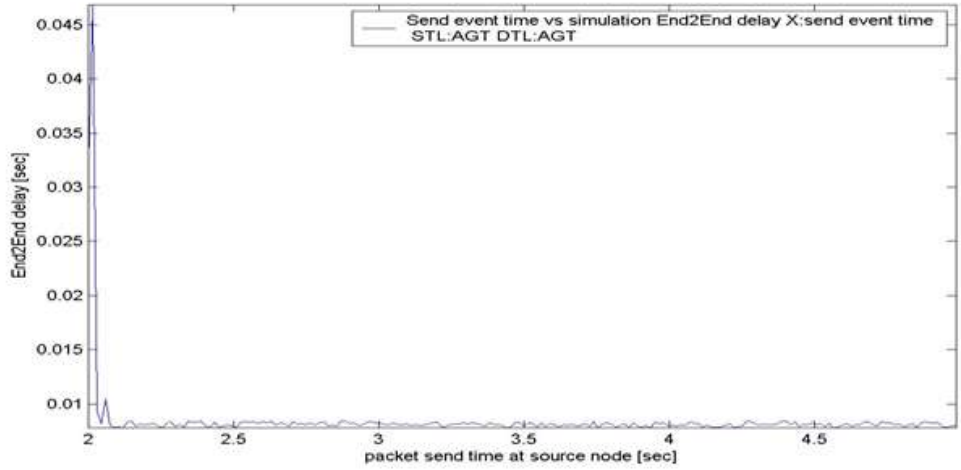

Figure 3.15: End to End Delay for 50 Nodes using DSR Two Node as Wormhole

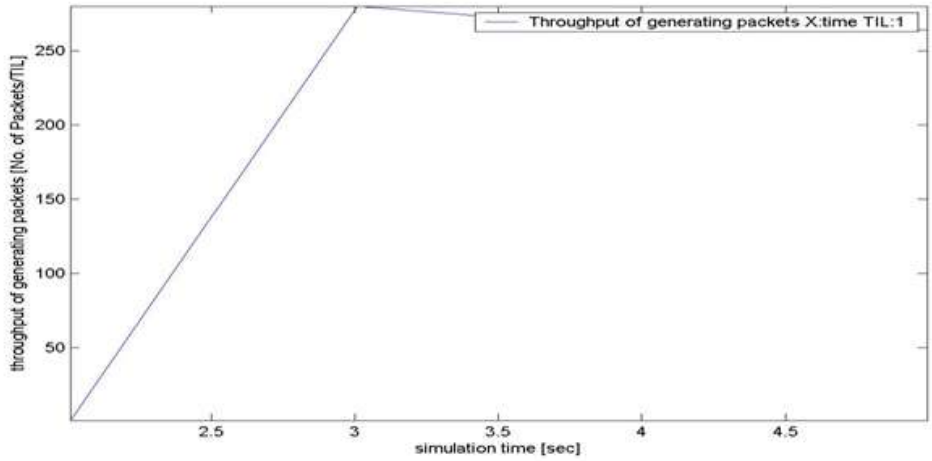

Figure 3.16: Throughput for 50 Nodes Using DSR Two Node as Wormhole

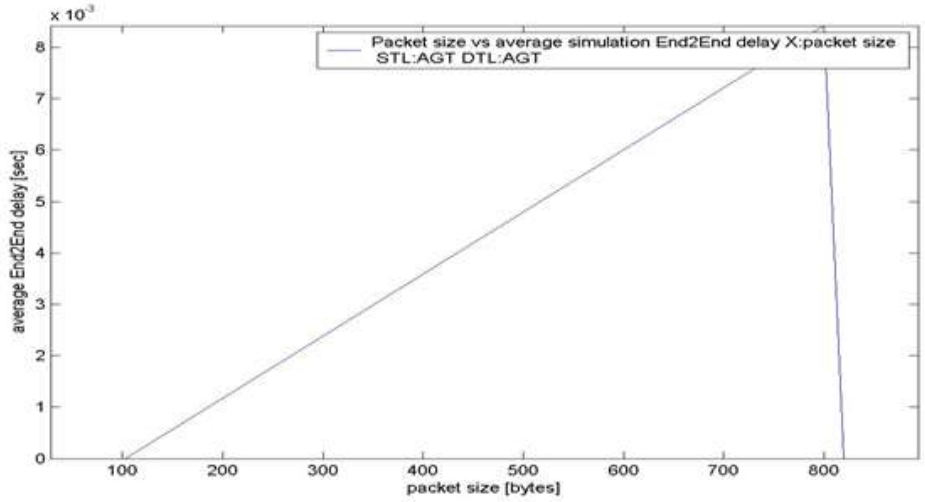

Figure 3.17: Packet Size vs. Average End to End Delay
for 50 Nodes Using DSR Two Node as Wormhole

We implement the random way point movement model for simulation in which nodes start at random position. with simulation time 500 seconds, 1200*1200 simulation area, maximum speed 20m/s, pause time is 10 seconds, traffic type is TCP, payload size 512 bytes, malicious node with a tunnel.

Figure 3.7 & 3.8 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 3.12 & 3.15 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.

Figure 3.13 & 3.16 shows the comparison of throughput, when we apply the digital signature scheme then the throughput level is increased than the previous scenario when there is no digital signature and presence of malicious node in the network. The throughput is increase with digital signature scheme because it does not allow any malicious node in between the path of data transfer.

Figure 3.14 & 3.17 shows the comparison of packet size & average end to end delay relationship, it can be seen that as packet size increases average end to end delay also increases linearly and it is maximum for packet size of 800 bytes.

IV. CONCLUSION

A wormhole is one of prominent attack which is formed by two malicious nodes and a tunnel. In order to protect from wormhole attack we used the scheme called detection & prevention approach with verification of legitimate nodes in network through its digital signature. Destination node analyzes the number of hop count of every path and selects the best path for replying. 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.

REFERENCES

[1] Pore Ghee Lay, John C. McEachen (2006), “A Comparison of Optimized Link State Routing with Traditional Ad-hoc Routing Protocols” U.S. Navy Research Paper 2.

[2] Singh Umang et al (2011), “Secure Routing Protocols in Mobile Adhoc Network-A Survey and Taxonomy” International Journal of Reviews in Computing. Vol. 7.

[3] LuoJunhai et al. (2007), “Research on multicast routing protocols for mobile ad-hoc networks” , School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, PR China School of Computer Science, McGill University, Montreal, Canada.

[4] Larry L. Peterson and Bruce S. Davie (2011), “Computer Networks - A Systems Approach”. San Francisco, Morgan Kaufmann Publishers Inc. ISBN 1-55860-368-9.

[5] Sharma M.L et al. (2008), “Performance Evaluation of MANET Routing Protocol under CBR and FTP traffic classes” Int. J. Comp. Tech. Appl., Vol 2 (3), 392-400 ISSN: 2229-6093.

[6] Stephen Kent and Randall Atkinson (1998), "Security Architecture for the Internet Protocol", Internet draft, draft-ietf-ipsec-arch-sec-07.txt.

[7] Singh Yudhvir et al.(2010), "Performance Evaluation of On-Demand Multicasting Routing Protocols in Mobile Adhoc Networks" International Conference on Recent Trends in Information, Telecommunication and Computing.

[8] Taneja Sunil and Kush Ashwani (2010), "A survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, ISSN: 2010-0248.

[9] Kumar D. Siva (2010), "Review: Swarm Intelligent based routing Protocols for Mobile Adhoc Networks" International Journal of Engineering Science and Technology Vol. 2 (12), 7225-7233.

[10] Liang Qin, Thomas Kunz, (2003), "Increasing Packet Delivery Ratio in DSR by Link Prediction" Proceedings of the 36th Hawaii International Conference on System Sciences.

[11] Mehran Abolhasan et al. (2003), "A review of routing protocols for mobile ad hoc networks", Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522, Australia b Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia.

[12] Elizabeth M. Royer (1999), "A Review of Current Routing protocols for Ad Hoc Mobile Wireless Networks ", IEEE Personal Communication.

[13] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang (2005), "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC.

[14] I. Khalil, S. Bagchi, N. B. Shroff (2005), "A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", Proceedings of the International Conference on Dependable Systems and Networks.

[15] L. Lazos, R. Poovendran (2004), "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks", Proceedings of the ACM Workshop on Wireless Security, pp. 21-30,.

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

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

[18] GULWADE M.P et. al. (2012), "Effectiveness of Wormhole Attack on DSR Protocol in Manet", World Research Journal of Telecommunications Systems, Volume 1, Issue 1, pp. 13-15.

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

[20] 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.