International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.321-330
http://dx.doi.org/10.14257/ijsia.2016.10.10.28

Detection and Performance Analysis of Wormhole Attack in MANET using DELPHI Technique

Sandeep Kumar Arora* and Ayushree

[1]*Discipline of Electronics and Communication Engineering,*
Lovely Professional University, Jalandhar, Punjab, India-144411
[2]*Discipline of Electronics and Communication Engineering,*
K.L. University, Andhra Pradesh, India.
Email:sandeep.16930@lpu.co.in, ayushrees@gmail.com

Abstract

Security is one of the primary issue in the Mobile Adhoc Network (MANET) particularly as for the size and complex nature of the system. The principle reason of security issues in MANET is that there is no physical connection between the nodes. This paper gives the impact of wormhole attack and discloses how to provide security to the packets with the help of Delphi technique. By applying Delay Per Hop Indicator (DELPHI), nodes which are the responsible for wormhole attack can be removed with the support of hop count method and AODV routing The metrics used for calculating network presentation are packet loss, throughput and end to end delay, which gives the better Quality of Services.

Keywords*: MANET, Blackhole attack, AODV, Detection, Routing*

1. Introduction

Mobile ad hoc network has reached outstanding success due to its self-maintenance and self-configuration nature. Mobile Ad-Hoc Networks are self-directed and without any centralized network in wireless systems. Nodes are the gadgets *i.e.*, cell telephone, tablet, individual computerized help, MP3 player and PC that are input in the system and these nodes can execute as host/switch or both at the one time. They can shape arbitrary topologies depend upon their availability with one another in the system. These nodes have the capacity to design them and as a result of their self-arrangement skill, they can be sent quickly without the need of any settled structure. Numerous routing protocols have been presented for MANET, *i.e.*, AODV, OLSR, DSR and so forth [1]. Security in Mobile Ad-Hoc Network is the most essential issue for the fundamental usefulness of the system. MANET frequently experiences security attacks in open medium, changing its topology consistently, no unified observing and administration, helpful calculations and absence of protection system. The MANET has no brought together organization where the nodes interconnect with one another on the premise of regular trust. This trademark makes MANET more powerless to be broken by an attacker inside the system. Remote connections likewise make the MANET more sensitive to attacks, which make simple to attacker for attack. A MANET is more open to these sorts of attacks since correspondence depends on shared trust between the hubs, there is no unified system, no authorization office, powerfully changing topology and restricted properties [2].

* Corresponding Author

ISSN: 1738-9976 IJSIA

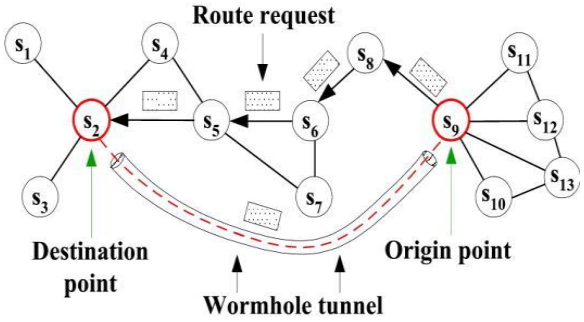

Figure 1. Representation of Wormhole Attack

In Figure 1., a tunnel is made between two nodes that can be utilized to secretly transmit packet. In a wormhole attack, an attacker gets packet at one point in the structure, hole them to another point in the structure and after that replays them into the structure beginning there. [3] If the attacker performs this tunnel genuinely and constantly, no harm will be there. Firstly, the packet leashes technique is suggested by HU *et. al.*, which is based on distance and location packet leashes method with aim to limit the separation of packet in the system. This technique has two ways for implementation: (i) Space based technology (ii) Time based technology. But there is some problem with both the techniques. The main problem is that it required extremely synchronized timekeeper. This problem is overcome by DELPHI (Delay per hop indicator). It can be implemented for both hidden and exposed wormhole attack. In this method, the detection of the wormhole attack, delay time and length of each route is measured and the average delay time per hop route is calculated. According to this method the wormhole attack route is having greater delay as compared to other. This method also has some disadvantage. It can detect both hidden and exposed attack but cannot pin point the location of wormhole attack.

2. Related Work

Under the communication of wormhole attack in the remote system utilizing NS2.35 test system and system parameters are throughput proportion. For such systems active directing conventions, receptive navigation conventions and half directing conventions [1] are considered.

The examination of the execution of AODV before and under Wormhole attack on various AODV parameters. The complete investigation of AODV convention under wormhole nodes which will help analysts to discover more precise or better Wormhole avoidance or hope systems. [2]

The investigation of wormhole attack driven in AODV directing convention in MANET as far as parameters prefer system throughput, normal end to end delay, packet transport proportion, drop rate utilizing NS2 system test system. In future, a novel multi-layer way to deal with recognize wormhole attack in MANET would be proposed and the reproduction results for same would be caught to demonstrate the capability of the proposed discovery component. [3]

The calculation of various measurements of the proposed convention from repair on NS2 on various situations *i.e.*, with worm opening attack and without worm gap attack is done [4] and there has been a recognizable change in the throughput and strength utilization is additionally decreased. System parameters that are considered for correspondence are throughput and energy examination. The proposed work [4] is free of number of equipment which expands the expense as well as quite mixed up to execute.

In [5] a robust, secure MANET on interest directing convention that is equipped for conveying packets to the destination even in the nearness of huge extents of dynamic

harmful or uncomplicated specialists that specifically drop packets they complied to advances simulated in OPNET Modeler.

The study of Black hole attack as for various execution parameters, for example, end-to-end delay, overhead and packets transport proportion is finished and broke down the powerlessness of two conventions AODV and Improved AODV under changing interval time. The Simulation results demonstrated that Improved Adhoc on Demand Distance Vector (IAODV) performs superior to anything AODV. The overhead of AODV is affected by twice as look at of IAODV. In this way, IAODV is weaker against Black hole attack than AODV. Yet at the same time the recognition of Black hole attacks in specially appointed systems is considered as a testing task [6]. The proposed work suggests a method where header node in each network is selected and the path with highest average sum of header number is elected as the optimal path. [7]

3. Research Methodology

Step-I: Start of simulation.

During the start of the process all the nodes send request packets so that the best path can be selected for transmission of information.

Step-II: Node deployment for requested WSN.

The nodes in the network communicate with each other.

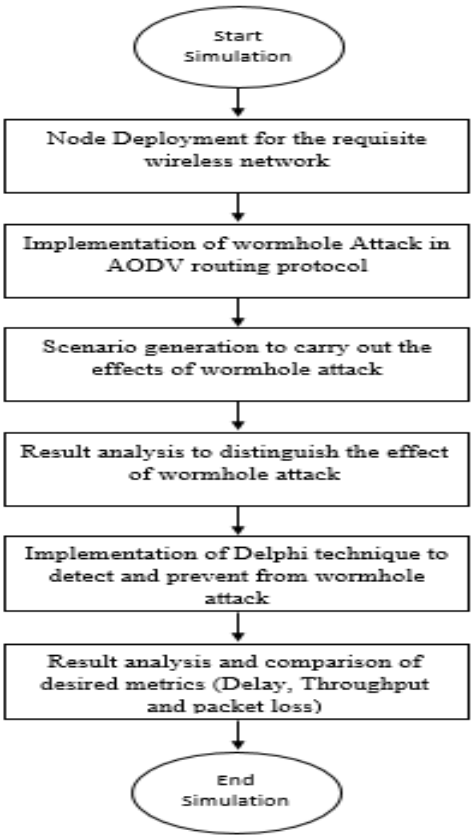

Figure 2. Representation of Proposed Technique

Step-III: Implementation of wormhole attack in routing protocol AODV.

AODV protocol and the worm hole attack. The worm hole attack is implemented in two malicious node of the network.

Step-IV: scenario generation to carry out the effect to wormhole attack.

When the attacker triggers the worm hole attack, all the packets are dropped by worm hole node.

Step-V: Result analysis to distinguish the wormhole attack.

The algorithm is used to differentiate between the attacker and the legitimate users of the network.

Step-VI: Implementation of Delphi to detect and prevent wormhole attack.

In this step, we implemented the DELPHI and also performs the detection and prevention of worm hole attack.

Step-VII: Result analysis and compression for the desired matrix like end to end delay.

After the whole process we analysis and the comparison of our result like throughput, end to end delay and energy. The whole process is shown in Figure 2.

4. Result and Analysis

The Table 1. shown gives the idea about the NS2 simulation parameters. The total number of nodes are 22. and total time taken for simulation is 650 seconds.

Table 1. Simulation Parameters

Parameter	Value	Description
Simulation time	650Sec	Highest performance time
Terrain Dimensions	800, 800	Physical region in which the hubs are set in meters
Number of Nodes	22	Hubs contributing in the network
Traffic Model	CBR	Constant Bit Rate link used
Network Model	Two ray ground	Hubs location policy
Routing protocol	AODV	Routing protocol used
Transport	UDP / TCP	For transportation of the Packet
Mobility	100 (m/s)	Pace of hub with which they are moving

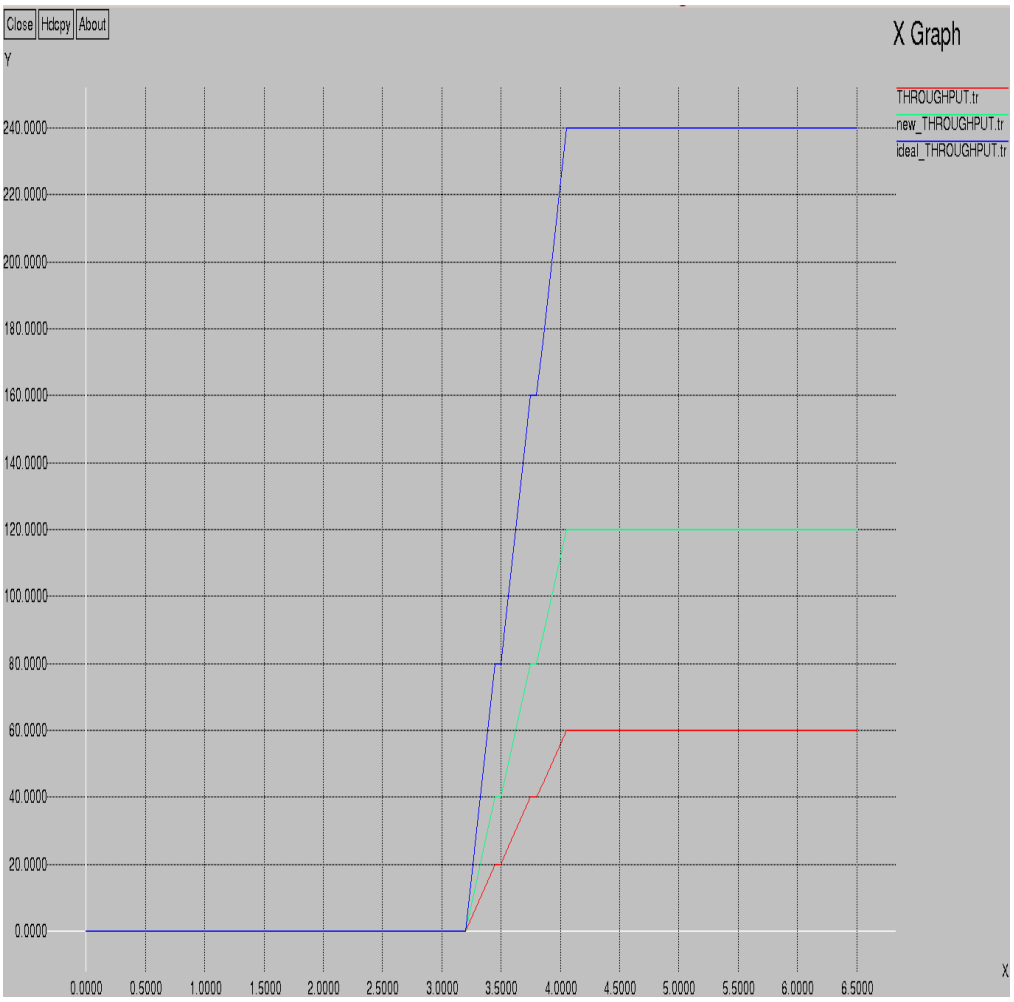

Figure 3. Throughput Graph (For Low Traffic – 20 Nodes)

The graph is plotted between the no. of packets vs time on x axis and y axis respectively, as shown in Figure 3. When the wormhole attack is executed, the efficiency of AODV protocol decreased. The throughput of the network is measured according to the number of received packets over time. When the attack will be removed from the network throughput will be increased by 33%.

The delay increases as the number of nodes in the network increases. The delay graph is shown in Figure 4. When the attack will be removed from the network, delay will be reduced by 37%.

The packet loss ratio between the transmitter and the receiver is shown in the Figure 5. As the no. of packets between the source and destination are dropped, the packet loss is increased by 31%. When the attack will be removed from the network packet loss will be reduced.

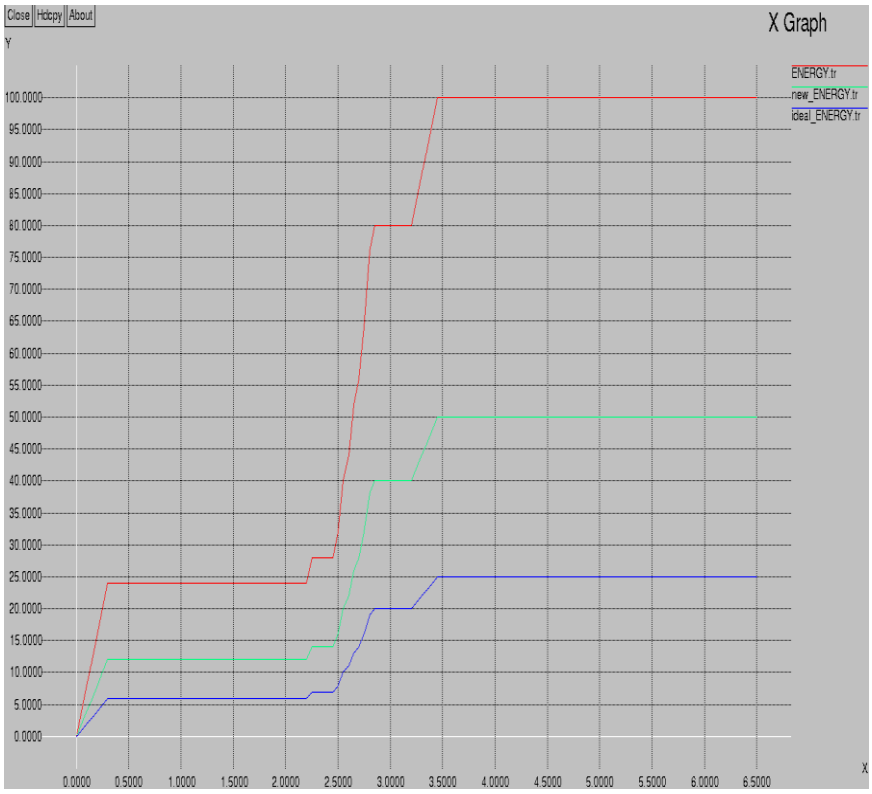

Figure 4. Delay Graph (For 20 Nodes)

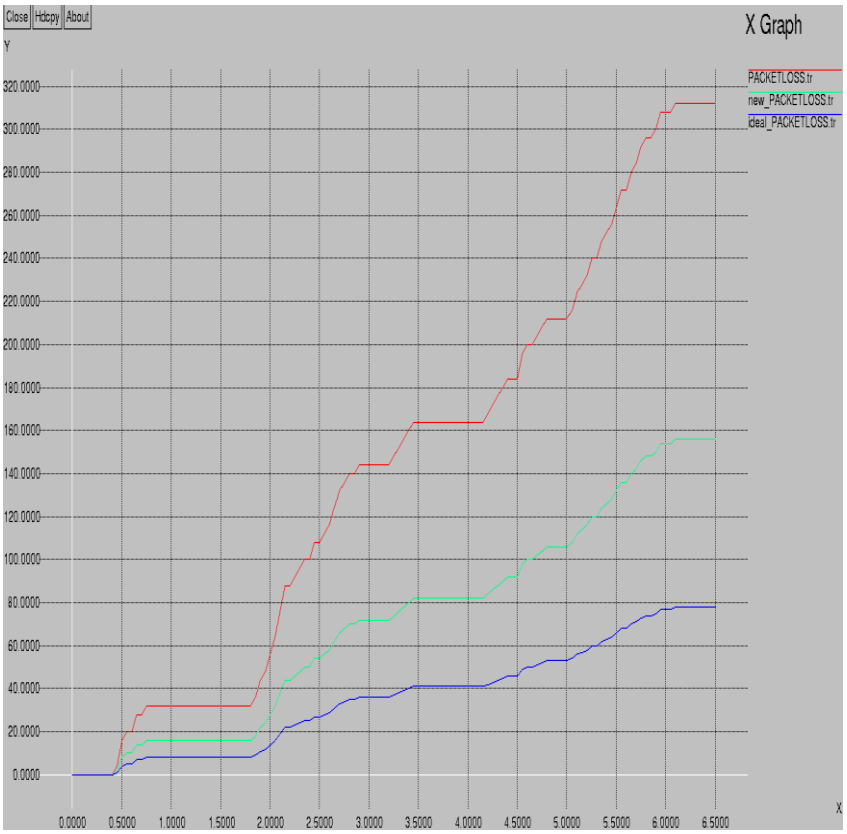

Figure 5. Packet Loss Graph (For 20 Nodes)

The graph is plotted between the no of packets vs time on x axis and y axis respectively, as shown in Figure 6. For High traffic *i.e.*, for 40 nodes. When the wormhole attack is launched, the efficiency of AODV protocol decreased. The throughput of the network is measured according to the number of received packets over time. When the attack will be removed from the network throughput will be increased by 33%.

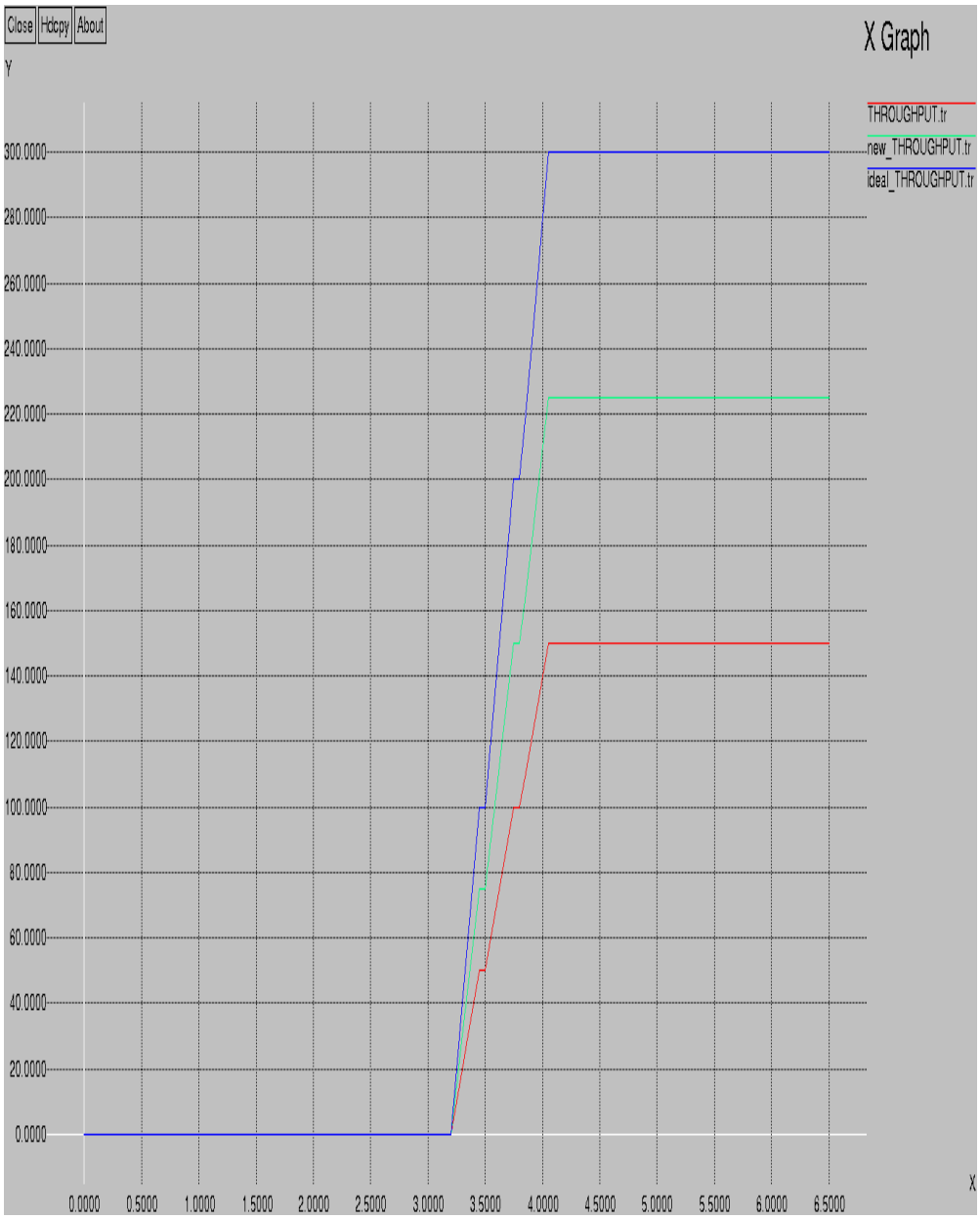

Figure 6. Throughput Graph (For 40 Nodes)

The packet loss ratio between the transmitter and the receiver is shown in the Figure 7. As the no. of packets between the source and destination are dropped, the graph is increased by 31%. When the attack will be removed from the network packet loss will be reduced.

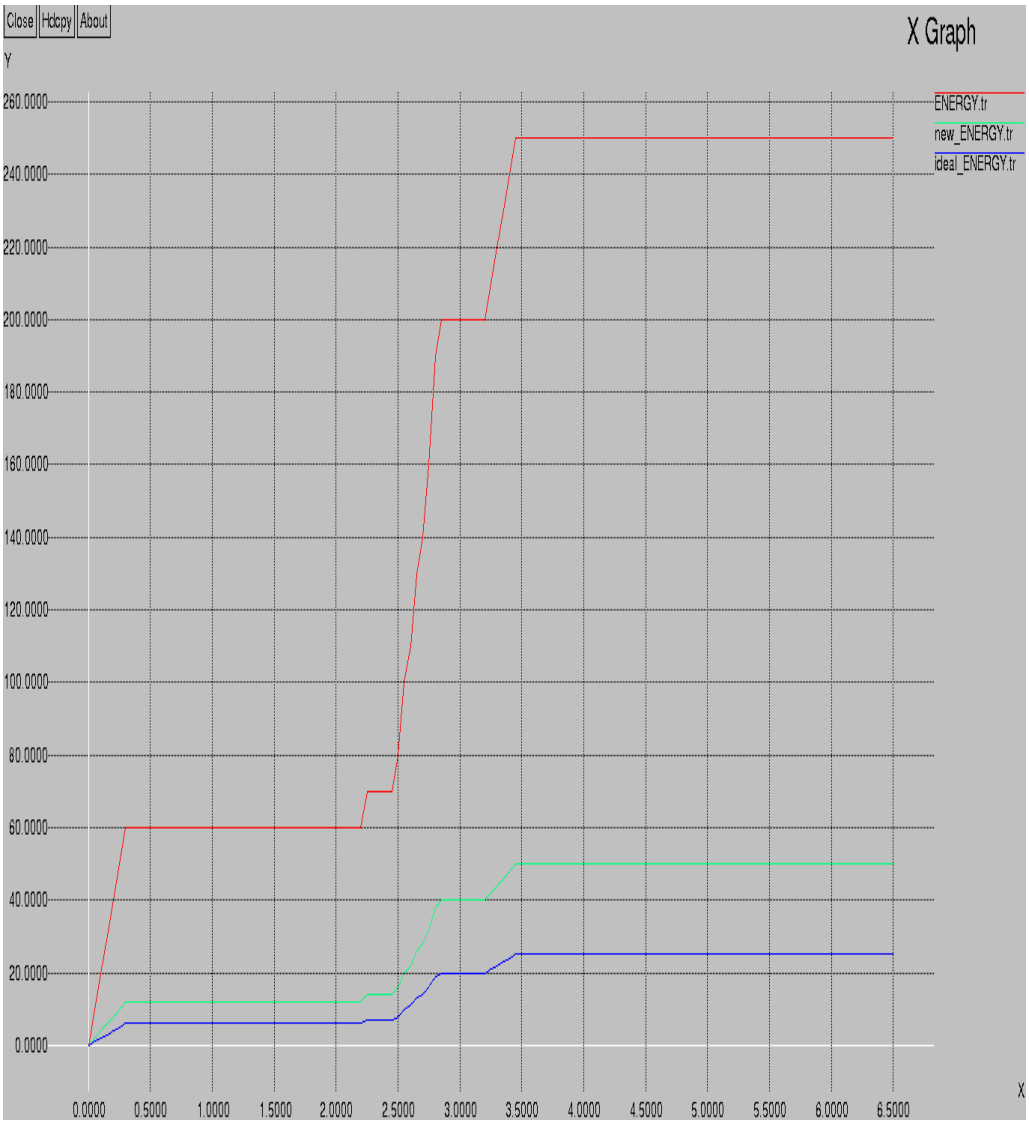

Figure 7. Delay Graph (For 40 Nodes)

The packet loss ratio between the transmitter and the receiver is shown in the Figure 8. As the no. of packets between the source and destination are dropped, the packet loss is increased by 31%. When the attack will be removed from the network packet loss will be reduced.

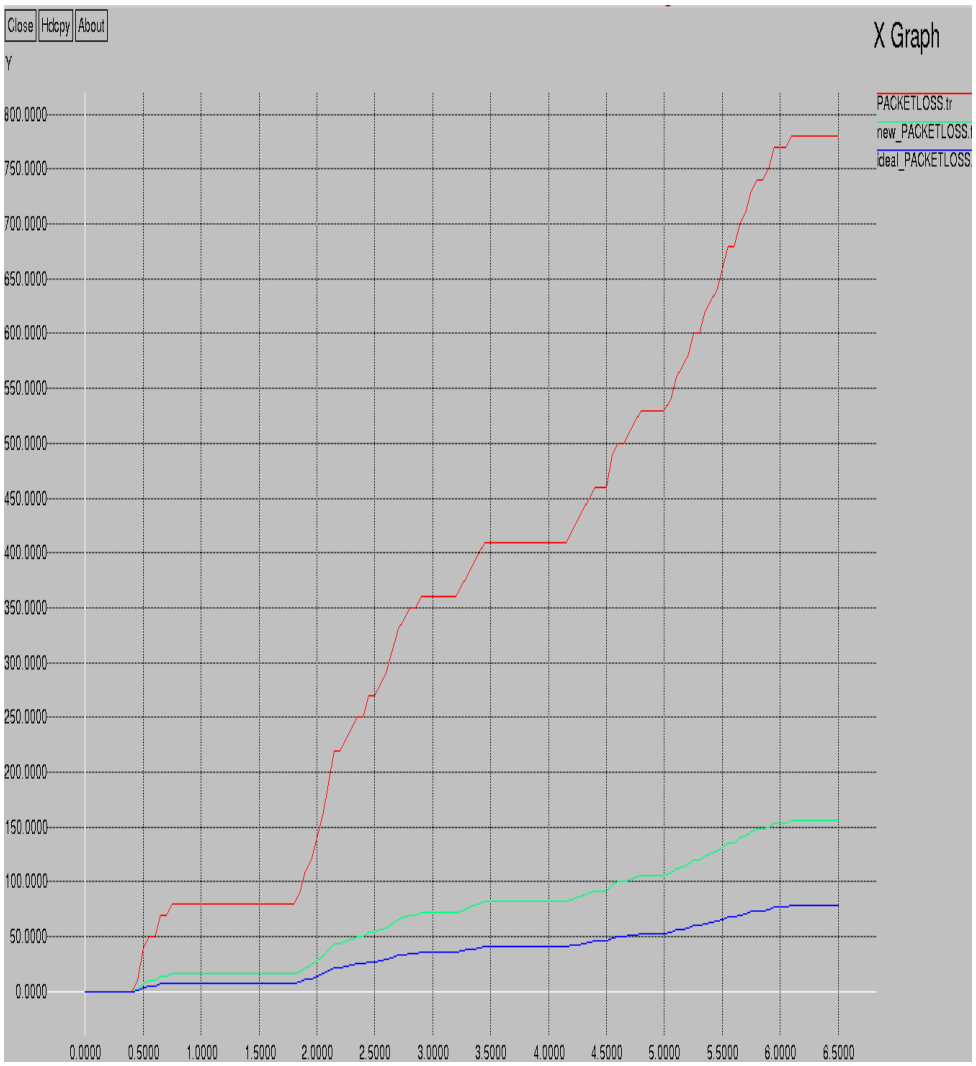

Figure 8. Packet Loss Graph (For 40 Nodes)

5. Conclusion

It is found that wormhole attack can be detected and removed by the DELPHI technique. This paper is focused on delay per hop and reliable packet transmission from source node to the destination node. This technique is helpful in the reduction of packet loss and improvement of the throughput. In future, we can pin point the location of wormhole node and execute more attacks to analyze the effect on the network which is the future scope of this work.

References

[1] Singh Y., "Wormhole Attack Avoidance Technique in Mobile Ad hoc Networks", Third International Conference on Advanced Computing & Communication Technologies, **(2013)**, pp. 283-287.
[2] Donatas S., "Mobile Adhoc Networks", IEEE Personal Communications Magazine., **(2003)**, pp. 46-55.
[3] Bhatiya S. A. and Rupinder K. C., "Analysing and Implementing the Mobility over MANETS using Random Way Point Model", International Journal of Computer Applications, vol. 68, no. 3, **(2013)**, pp. 888-975.
[4] Goyal P. and R. R. Vintra, "MANET: Vulnerabilities, Challenges, Attacks, Application", International Journal of Computational Engineering & Management, vol. 11, no. 16, **(2013)**, pp. 156-162.
[5] Manju O., "Impact and Performance Analysis of Wormhole Attack on AODV in MANET using NS2", International Journal Science and Research, vol. 8, no. 3, **(2013)**, pp. 1-6.

[6] Richa G., "Implementing Security algorithm to worm hole attack using AOMDV protocol & comparison using NS2 simulator", IOSR Journal of Computer Engineering., vol. 16, no. 5, **(2016)**, pp. 1-5.
[7] Arora K. S. and Gaba S. G., "Improvement in Data Packet Routing on the basis of stability", Indian Journal of Science and Technology, vol. 9, no. 3, **(2016)**, pp. 1-6.

Authors

Sandeep Kumar Arora, he is currently pursuing Ph. D. in Electronics & Electrical Engineering with Spl. in *Design of Secure Initiation Protocol in VANET*. He is working as an Asst. Prof. in Lovely Professional University since 2011. His research interest includes Wireless Sensor Networks, Computer Networks, Adhoc Networks Communications and Cryptography. He is a member of IEEE and also the author of more than one dozen research papers indexed in Scopus.

Ayushree, she is working as an Assistant Professor in K L University, Vijayawada (Andhra Pradesh). She has completed her B. Tech and M. Tech in the domain of wireless communication from Lovely Professional University, Punjab in 2015. Her research activities are directed towards computer networks (MANET).

