Wormhole Detection and Isolation Scheme Based on Threshold Mechanism in Mobile Ad Hoc Network

Syed Arbaaz Ali
Research Scholar
arbaazali3112@gmail.com
Sam Higginbottom University of Agriculture,
Technology and Sciences
Prayagraj (Allahabad)

Er. Prateek Singh
Assistant Professor Sr. Grade
prateek.singh@shiats.edu.in
Sam Higginbottom University of Agriculture,
Technology and Sciences
Prayagraj (Allahabad)

Abstract - The mobile nodes further transmit message to their neighbouring nodes after receiving any message. The message is sent by the intermediary nodes and act as a router in the condition when a node wishes to forward information to a movable node but it is out of coverage area of sender node. Due to the random movement of nodes, the fixed paths cannot be obtained for message forwarding. The wormhole intrusions are the kind of system layer intrusion. When the system passage is forwarded via the channel for increasing the network delay, then it is identified as worm hole. While the source nodule delivers the control memo for the trail organization towards the target, then the control memos go through via the channel. The respond memos go through the channel as well and source scrutinized that direct route occurs via the channel. The wormhole is the active type of attack which affects network performance. In this research work, technique is proposed for the detection and isolation of wormhole attack. The proposed technique is implemented in network simulation version 2. The performance of proposed technique is analyzed in terms of certain parameters and it give high performance as compared to existing technique for isolation of wormhole attack in MANET.

Keywords - MANET, Wormhole, Threshold Delay

I. INTRODUCTION

MANETs includes various movable sensor nodes. These sensor nodes interact with each other through the movement of data packets in multi-hops without having any centralized control. These networks involve numerous mobile hosts. These hosts use wireless links for communication purpose [1]. These nodes move randomly in any direction as these are infrastructure less network with no central control. Due to these attributes, all nodes in the network behave as router where data packets are transmitted by host. MANET provides optimum solutions in many cases for example wired or wireless network in which the issue of damage and congestion occurs abruptly. The security of route is the major issue of MANET. In past few years, various types of local link fixing techniques were proposed to minimize the issue of link failure. For instance, the interconnection of all devices coming from the same place such as business meeting at a place for the composition of Ad-Hoc network in presence of network services. The mobile nodes further transmit message to their neighbouring nodes after receiving any message [2]. The message is sent by the intermediary nodes and act as a router in the condition when a node wishes to forward information to a movable node but it is out of coverage area of sender node. Due to the random movement of nodes, the fixed paths cannot be obtained for message forwarding. The wireless network faces many issues due to its infrastructure-less configuration. An infrastructure is required for efficient functioning of these networks. The nodes within this network can behave both as router and host as it has the ability using which traffic can be routed from source to destination. Topology change, unreliable communication and inadequate energy of nodes are some factors which cause issue in the design of these networks. Therefore, the more attention should be given to the issues of MANET such as limited bandwidth and node mobility. The MANET faces various routing issues during the routing process due to some factors such as the nodes present in network are movable type. The nodes are distributed randomly. The movement of intermediated nodes in the path causes path failure. Therefore, an effective mobility management is required during routing process. The bandwidth limitation is the one more design issue present in MANETs. Thus, it is required to design a routing protocol for eliminating the issue of limited bandwidth to reduce network overhead. Collision and congestion are two major issues of wireless sensor network. The immediate mobility of nodes inside the system is the main cause of collision between data and control packets during communication in mobile ad hoc network. The issue of hidden terminal and exposed terminal also occurs in MANET [4]. The packet collision at the end point of receiving node is called hidden terminal issue. This issue occurs due to the concurrent transferring of nodes towards those which do not exist in straight coverage area of correspondent but occur in the receiver transferring area. Therefore, this is a main problem as it causes intrusion among nodes due to link variation. These issues destroy overall transmission. The situation in which nodes do not know each other and transfer packets at the same time due to which they come in the way of each other and cause collision and terminals damage. Thus the issues of hidden and exposed terminal should be minimized during the designing of protocols.

MANETs are extensively utilized in various areas for example financial, military and private sectors. This network allows users to send and exchange information without considering distance and hence avoids geographic locations [5]. Following are the various applications of MANETs.

a. Military Sector: In recent times, military technologies regularly include several types of processing tools. MANET networking allows military to get benefit from regular network machinery in order to maintain an information sharing network among military. The vital performance of MANET comes from this region.

b. Commercial Sector: These networks give effective results during disaster. Because of this reason, these networks are broadly used for rescue operations or urgent situations. The communication among nodes is essential during the security process in order to provide appropriate support. The communication device generates information system automatically using which rescue operations are implemented by the rescuers easily**.**

c. Sensor Networks: This network involves large numbers of small sensors for identifying large numbers of resources within a region. These sensors have limited potential and depend on each other for information transmission. The computing capability of single sensor is limited due to which more failure and information loss occur [11]. Thus, this can be used as a key to future homeland security.

d. Personal Area Networking: In order to simplify, communication among various movable devices, very small range MANET is utilized such as PDA, laptop, mobile phone etc. Wireless links are replaced by repetitive wired flex. In MANET, access can be provided to certain systems or internet with the help of some techniques such as WLAN, GPRS, as well as UMTS. PAN is considered a promising functional area of mobile ad hoc networks for the future determined computing scenario.

e. Emergency Services: This network is extensively used in such situation when entire communication structure is distorted or not working properly. These situations include Tsunamis, storms, volcanic activity etc. The lessening of disaster effects and rapid re-formation of infrastructure is very necessary [6]. With the help of this arrangement, a network can be established within few hours as this network does not need wired link.

II. LITERATURE REVIEW

Elbasher Elmahdi, et.al (2018) presented a new approach to provide trustworthy and safe data transferring in the occurrence of attacker nodes [7]. In this study, a routing protocol named AOMDV was modified for splitting message into numerous routes. This approach implemented a homomorphic encryption technique. The simulation outcomes depicted that proposed approach performed well in terms of higher packet delivery ratio and network throughput. Therefore, this approach was extremely advantageous for urgent functions of MANETs. Moreover, higher achievement rate and packet delivery assurance towards destination had been provided by the presence of numerous dynamic routes in each network cluster. As future work, end-to-end delay can be decreased by expanding this study for applying this approach within urgent situations.

Oussama Sbai, et.al (2018) presented a study relevant to single and numerous black hole intrusions in AODV and OLSR protocols [8]. In this simulation, the network density based on the quantity of nodes within the network was taken into account with the mobility scheme and nodes' velocity. For physical layer, a routing protocol named IEEE 802.11ac was selected to perform simulation. This routing protocol was able to manage more genuine and universal circumstances. Routing overhead, average end to end delay, throughput and packet delivery ratio were the factors on which performance of proposed approach was evaluated. In terms of these parameters, the proposed approach showed better performance in comparison with existing techniques.

Guoquan Li, et.al (2018) proposed a research study to detect the impact of blackhole intrusion within the network during the occurrence of AODV protocol [9]. Different performance parameters like packet loss, end-to-end delay and throughput were considered to estimate this effect. Overall nodes, the black hole nodes as well as the velocity of mobile nodes were modified to analyze the performance of network. The properties of blackhole intrusions were provided through the tested outcomes. These properties reflected the behaviors of blackhole intrusion and its effect on the network performance.

Amar Taggu, et.al (2018) proposed an easy and effective intrusion detection scheme for the detection of blackhole attack occurring in the application layer of MANETs [10]. The proposed algorithm utilized mobile agents (MA) and modified version of Trace route to detect manifold black holes in DSR protocol. In the proposed approach, the utilization of mobile agents eliminated the need of improvements in routing algorithms. The simulation outcomes depicted that the single and multiple blackhole nodes could be identified fruitfully athwart changeable mobility of sensor nodes.

Sayan Majumder, et.al (2018) projected a novel scheme named as Absolute Deviation (AD) for the impediment of wormhole intrusion [11]. The discovery of wormhole intrusion could be executed in extremely small amount of time because of the exploitation of absolute deviation covariance and correlation. The projected algorithm did not need any additional circumstances for its implementation. The wormhole malevolent generated a false channel from source to target. The frequency level of this connection was extremely elevated. In this study, it was supposed that the remoteness amid source and target was extremely small and the time period utilized for the transmission of message would be extremely fewer. Though, the large duration of time was utilized for the following of authentic route. Therefore, the time period utilized for the prevention of wormhole malevolent from coming to the network was computed significantly in this study. The tested outcomes demonstrated that absolute deviation approach provided superior outcomes than AODV. In addition, the Absolute Deviation Correlation Coefficient was used for the identification of the wormholes through determining the packet plunge prototype.

Nikhil G. Wakode, (2017) presented a new scheme with the help of cooperative bait detection approach (CBDA). The novel scheme was presented in conjunction with attacker node detection algorithm for the prevention of black hole intrusion. This intrusion caused a lot of damage to the network [12]. Due to the proposed approach, end-to-end delay, normalized routing overhead and packet delivery ratio were reduced significantly. On the other hand, the existence of attacker nodes within the network increased packet drop ratio. Nevertheless, overall performance parameters were enhanced due to the reduction in packet drop ratio and growth in normalized routing, end-to-end delay and packet delivery ratio. The tested results demonstrated that safe information sharing was executed by network simulator.

Pratik Gite, et.al (2017)stated that the expanding technique of Mobile Ad-hoc Network was utilized extensively in the wireless links. The proposed technique was dependent on some parameters such as mobility, wireless connectedness and self-configuration. The movement of the nodes and the shortage of the energy were the major issues of multi-hop Ad-Hoc network which occurred due to the link failure in the system. These losses could not be identified through the standard congestion system. Thus, in the system, the routing protocols were identified as the necessary part because of their benefits and drawbacks. Routing protocol was extremely important because it discovered and maintained all paths. A new routing protocol was presented in this study. With the help of this protocol, preference was provided to the available paths in accordance with their route robustness [13]. A link prediction approach was proposed based on the signal power. In this study, the proposed approach was applied on the AODV routing protocol. The tested outcomes indicated that performance of the proposed technique was better than the earlier approach. The proposed approach enhanced the performance of network in terms of some parameters.

Kavitha T, et.al (2017) stated that link failure inside mobile ad hoc network occurred to the nodes' movement. Till now, various approaches had been proposed for the speedy re-routing of data packets. In these techniques, hop count was utilized as the main factor but these techniques did not provide good results for end to end delay. Thus, in this study, an immediate Route Migration protocol was proposed for the creation of shortest path. This protocol considered route distance and hop count. A partial topology aware technique was applied to obtain shortest route immediately [14]. A technique was presented in this study for redirecting packets towards the target easily during link failure at every node. The experienced outcomes revealed that projected technique showed highest throughput, less end to end delay, and instant path transfer.

Roshani Verma, et.al (2017) stated that the main objective of this study was the recognition and removal of wormhole intrusion for the duration of the broadcasting and transmission procedures. The projected approach improved the safety of ad hoc arrangements. These types of intrusions were prohibited from entering the system [15].The packet delivery proportion was improved and the control overhead was diminished by the improvement of routing protocols in the systems. The table accesses at target node were enhanced in order to recognize the wormhole attack affected nodules at elevated speed. The new technique provided assistance in the exploitation of competent techniques by which the DoS intrusions and hybrid intrusions could also be prohibited from entering the systems and thereby enhanced the network safety.

III. RESEARCH METHODOLOGY

This research work is based on the detection and isolation of wormhole attack in mobile ad hoc network. The routing and security are the major issues of mobile ad hoc network. The routing protocols are broadly classified into reactive and proactive. In the reactive routing protocols path from source to destination is established when required. The source node flood route request packets in the network and nodes which are adjacent to destination will reply back with the route reply packets. The source node receives many replies and path from source to destination is established based on hop count and sequence number. The path which have least hop count and maximum sequence number will be considered as best path for the data transmission. In the established path malicious nodes exists which increase delay in the network. The methodology is proposed for the detection of malicious nodes from the network. The proposed methodology has various phases which are explained below in detail:-

Step 1: Path Establishment:- In the first phase, the path will be established from source to destination based on the hop count and sequence number. The path which have least hop count and maximum sequence number will be considered as the best path for the data transmission from source to destination

Step 2: Define maximum and minimum bandwidth:- The network, the data rate is defined according to network configuration. The mobile ad hoc network configuration is not so high, due to which bandwidth consumption is also low. The bandwidth consumption will decide the delay in the network.

Step 3: Malicious node Detection:- When the malicious node trigger wormhole attack in the network than delay start increasing at steady rate. The delay at every hop gets counted and if the over delay in the path get improved than threshold value then it possibility of malicious node. The hop at the which delay is maximum that hop node is considered as the malicious node which will be marked as red color

Step 4: Isolation of Malicious node:- The last phase is isolation phase in which malicious node get isolated from the network. In the isolation phase, the technique of multihop routing will be implemented in the network. The path in which malicious node exists can be further selected for the data transmission

IV. RESULT AND DISCUSSION

Network Simulator is an occasion relied simulator. The network simulator is a kind of distinct occasion packet level simulator. It covers huge amount of dissimilar types of protocols used in different kinds of applications and packets. In the network simulator, scripting language is utilized. It comprises “NAM” files using which animatronics proceeds. In this investigative study, the AODV routing protocol is utilized for the route formation from source to target. The AODV protocol is the reactive kind of routing protocol which attains data when it is mandatory for the establishment of path from source to target. The AODV protocol is relied on distinct source and a particular target method is utilized for the formation of a route which comprises slightest remoteness and highest consistency

Table 1: Simulation Parameters

Simulation parameters	**Values**
Channel – Type	Wireless channel
Propagation model	Two ray ground propagation
Mobility Model	Random way point
Antenna Type	Omi-directional
Number of nodes	100
Speed (s)	150 m/second
Traffic Type	CBR
Mac Type	IEEE 802.11 (b/g)
Routing Protocol	AODV
Area of simulation	800* 800
Time of simulation	100 seconds

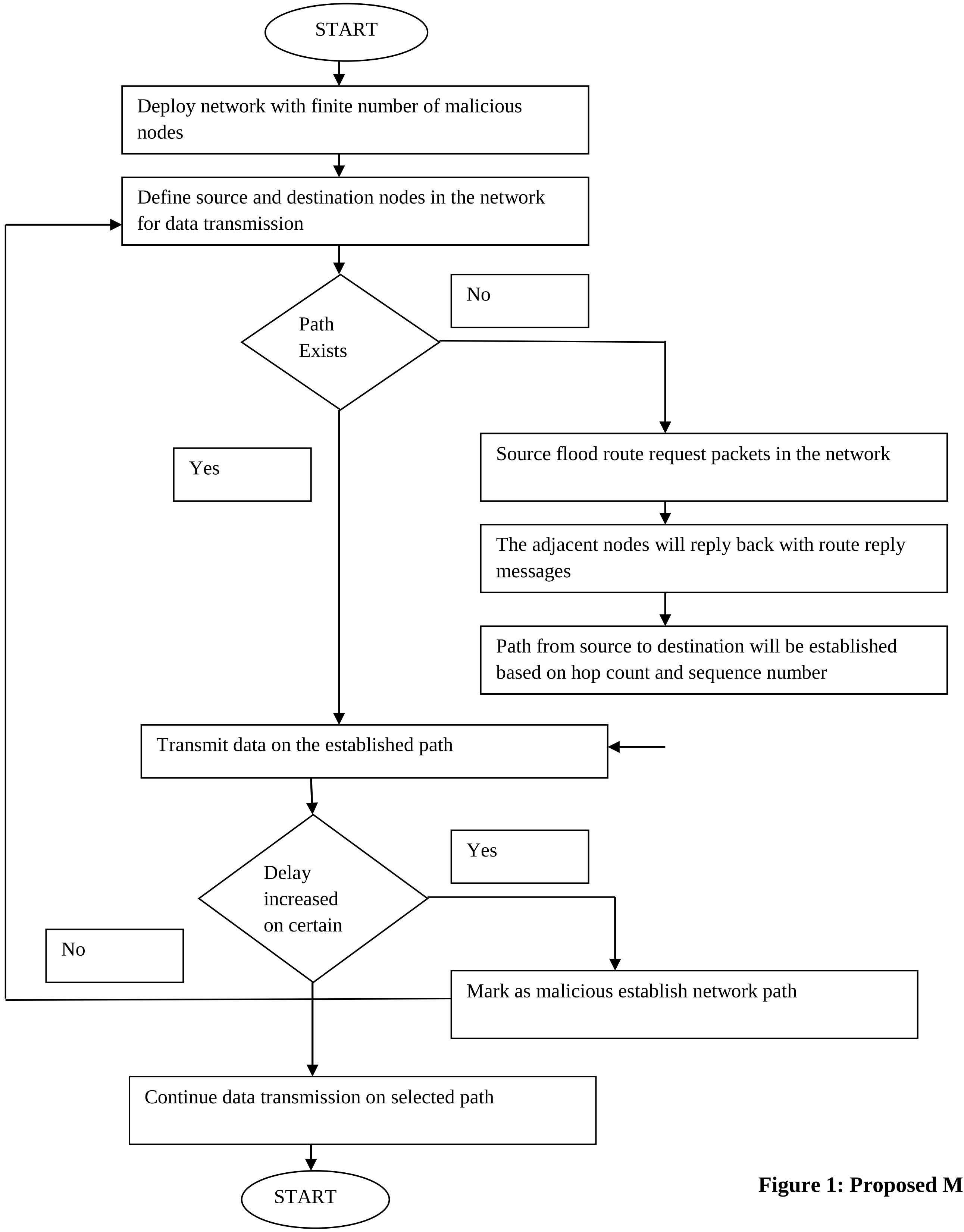
START
Deploy network with finite number of malicious nodes
Define source and destination nodes in the network for data transmission
Path Exists
No
Yes
Source flood route request packets in the network
The adjacent nodes will reply back with route reply messages
Path from source to destination will be established based on hop count and sequence number
Transmit data on the established path
Delay increased on certain
Yes
No
Mark as malicious establish network path
Continue data transmission on selected path
START

Figure 1: Proposed Methodology

The performance Matrix of the work is described below:-

a. Throughput: How many packets are effectively transmitted to the target in analyzed by the throughput

$$\text{Throughput} = \frac{No\ of\ packets\ Received}{Total\ number\ of\ packet\ send} * \text{time}$$

b. Power : The power utilization is the parameter which scrutinize the power utilization in the network

Power Consumption = Number of packets send * per unit power

c. Packet loss : The packet loss is the total amount of packets which are misplaced during information broadcasting in the network

Packet loss= No of packets send - No of packets received

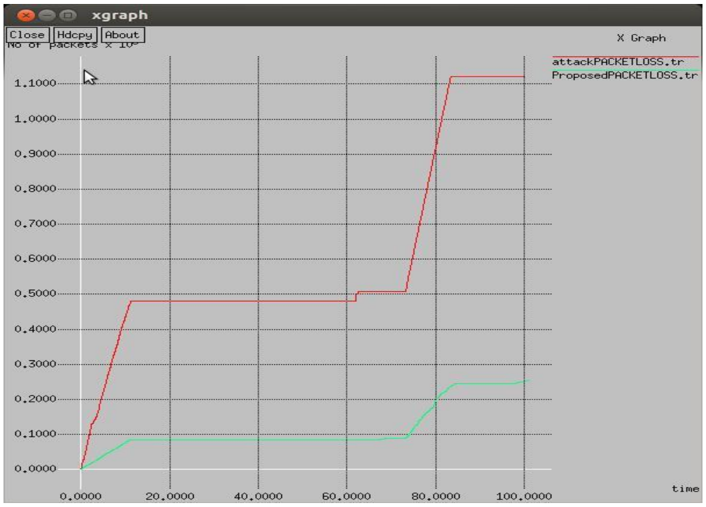

Figure 2: Packet loss Comparison

As shown in figure 2, the packet loss of the proposed technique and existing technique is compared for the performance analysis. It is analyzed that packet loss of proposed technique is low as compared to existing technique

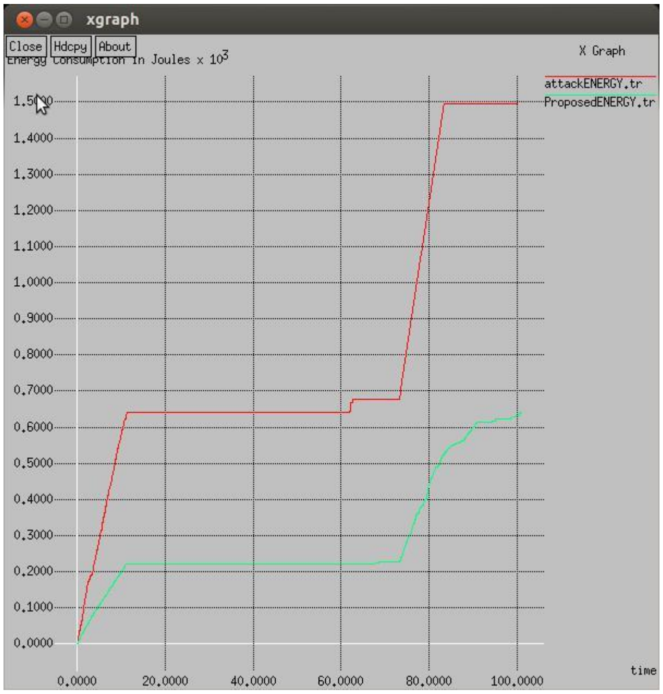

Figure 3: Energy Comparison

As shown in figure 3, the energy of the proposed technique and existing technique is compared for the performance analysis. It is analyzed that energy of proposed technique is low as compared to existing technique

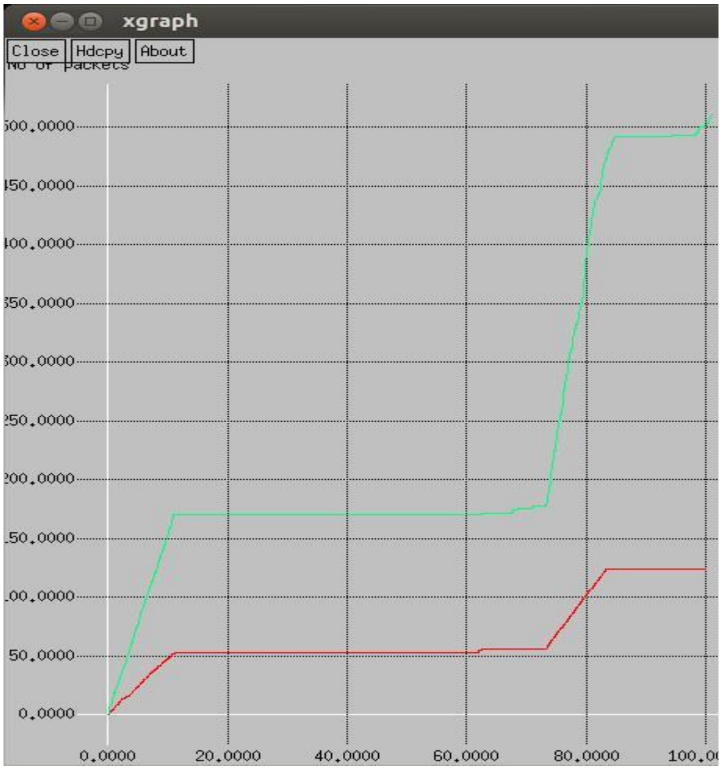

Figure 3.: Throughput Comparison

As shown in figure 3, the throughput of proposed technique is compared with the existing technique. It is analyzed that throughput of proposed technique is high as compared to existing technique

V. CONCLUSION

The wireless ad hoc network is the decentralized kind of network in which movable nodes can connect or depart from the network according to their requirement. This kind of network does not comprise any kind of middle manager or central controller. The network security, routing and quality of service are the major constraints of this arrangement because of the self arranging character of this network. An active kind of attack named wormhole intrusion may be the reason of the entering of attacker nodes in the system and because of this delay increases. In the presented research, two phase verification scheme is utilized. For the recognition of attacker mobile nodes, this scheme shows fewer precision and large implementation times. The projected and accessible approaches are applied in NS2 and the reproduction outcomes depict development in throughput, reduction in delay and packet loss.

VI. REFERENCES

[1] R C Poonia, D. Bhargava, and B.Suresh Kumar. "CDRA:Cluster-based dynamic routing approach as a development of the AODV in vehicular ad-hoc networks." In Signal Processing and Communication Engineering Systems (SPACES), International Conferenceon, vol. 6, issue 3, pp.397-401, IEEE, 2015.

[2] Sadiya Mirza, Sana ZebaBakshi, "INTRODUCTION TO MANET", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 1 | Jan-2018

[3] S.Umang, BVR Reddy, MN Hoda, "Enhanced intrusion Detection System for Malicious Node detection in ADHoc Routing Protocols using Minimal energy Consumption", IET Communications volume 4, issue 17, pp-2084-2094. 2010.

[4] B Wu, J Chen, J Wu, M Cardei, "A survey of attacks and counter measures in mobile adhoc networks", Wireless network security, volume 15, issue 7, pp-103-135, 2007.

[5] Sandeep Kumar, Suresh Kumar, "Study of MANET: Characteristics, Challenges, Application, Routing Protocol and Security Attacks", INTERNATIONAL JOURNAL OF R&D IN ENGINEERING, SCIENCE AND MANAGEMENT Vol.2, Issue 5, July 2015

[6] Sagar R Deshmukh, P N Chatur, Nikhil B Bhople, "AODV-based secure routing against blackhole attack in MANET", 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Pages: 1960 – 1964

[7] ElbasherElmahdi, Seong-Moo Yoo, Kumar Sharshembiev, "Securing data forwarding against blackhole attacks in mobile ad hoc networks", 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Pages: 463 – 467

[8] Oussama Sbai, Mohamed Elboukhari, "Simulation of MANET's Single and Multiple Blackhole Attack with NS-3", 2018 IEEE 5th International Congress on Information Science and Technology (CiSt), Pages: 612 – 617

[9] Guoquan Li, Zheng Yan, Yulong Fu, "A Study and Simulation Research of Blackhole Attack on Mobile AdHoc Network", 2018 IEEE Conference on Communications and Network Security (CNS), Pages: 1 – 6

[10] Amar Taggu, Abhishek Mungoli, Ani Taggu, "ReverseRoute: An Application-Layer Scheme for Detecting Blackholes in MANET Using Mobile Agents", 2018 3rd

Technology Innovation Management and Engineering Science International Conference (TIMES-iCON), Pages: 1 – 4

[11] Sayan Majumder, Prof. Dr. Debika Bhattacharyya, "Mitigating Wormhole Attack in MANET Using Absolute Deviation Statistical Approach", 2018, IEEE

[12] Nikhil G. Wakode, "Defending blackhole attack by using acknowledge based approach in MANETs", 2017 International Conference on IoT and Application (ICIOT), Pages: 1 – 6

[13] Pratik Gite, "Link Stability Prediction for Mobile Ad-hoc Network Route Stability", International Conference on Inventive Systems and Control, 2017.

[14] Kavitha T, Muthaiah R, " INSTANT ROUTE MIGRATION DURING LINK FAILURE IN MANETS", International Journal of Mechanical Engineering and Technology (IJMET) Volume 8, Issue 8, August 2017

[15] Roshani Verma, PROF. Roopesh Sharma, Upendra Singh, "New Approach through Detection and Prevention of Wormhole Attack in MANET", International Conference on Electronics, Communication and Aerospace Technology ICECA 2017