iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** V **Month of publication:** May 2021

DOI: https://doi.org/10.22214/ijraset.2021.34156

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue V May 2021- Available at www.ijraset.com

Analyzing AODV Protocol towards Blackhole Attack in MANET

Syed Abbas Mahdi Razvi[1], Faiz Mohiuddin[2], Afreen Sultana[3], Surayya Jabeen[4]
[1, 2, 3] *UG Student,* [4]*Assistant Professor, Department of Computer Science & Engineering, ISL Engineering College, Hyderabad, Telangana, India*

Abstract: ***MANETs (Mobile Ad Hoc Networks) are widespread today and are becoming a popular research topic. The wireless ad hoc network is another name for it. MANET is a portable multi-hop network with no infrastructure. In a MANET, data is transmitted to victims of mobile devices. These mobile nodes have no restrictions on their movement within a network. When a source node in a MANET needs to send or transfer data to a destination node, it first initializes the route to the destination node and then forwards the packets along this route. The intermediate nodes help transfer data packets from the source to the destination. However, due to the presence of malicious or misbehaving nodes such as black holes (BH), MANET data transmission is vulnerable to both internal and external attacks. MANET routing protection becomes a major problem as malicious or misbehaving nodes disrupt routing and result in significant loss of sensitive and confidential data. The main attack on MANET is the attack on the black hole. The aim of this document is to target the black hole attack using the SETRP (Secure and Efficient Transmission Routing Protocol) to identify and eliminate faulty nodes and to evaluate the efficiency of the network based on parameters such as average power consumption and service life of the network and the residual energy. In addition, we measured the effect and appearance of a black hole attack on the network based on the number of mobile nodes and the cumulative number of black nodes. Further investigation can be done by removing network parameters and applying a prevention strategy to avoid black hole attacks.***

Keywords: MANET, Blackhole Attack, Secure and Efficient Transmission Routing Protocol (SETRP), NS-2, Performance Metrics.

I. INTRODUCTION

Communication is the act of exchanging information from one peer to another. There are many and several approaches to achieve switching between interactive groups. However, information agencies favor efficient and reliable communication. Furthermore, the quality and efficacy of communication vary depending on the form of communication, environment, and entity specifications [1]. Initially, information sharing was conducted over a wired network, although this was later replaced by wireless communication. The current prerequisite of collaboration is to be able to communicate anywhere and at any time without interruption. This condition is met with the development of a wireless infrastructure-free network. The network was dubbed Mobile Ad Hoc Network or MANET for short [2]. The MANET infrastructure is depicted in the figure below.

As seen in Figure 1, a mobile ad hoc network (MANET) is an infrastructure-less wireless network composed of wireless mobile nodes spread in the wireless radio networking region with constrained and heterogeneous resources.

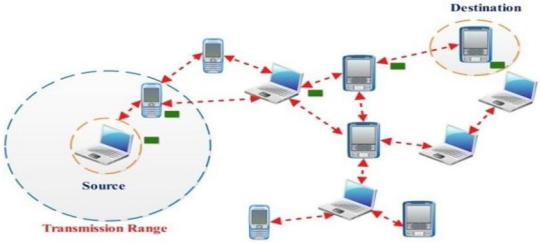


Fig 1: Infrastructure of MANET

Nodes in the network are able to move from one location to another. Because of versatility, the network topology of a MANET network is complex and unstable. Furthermore, nodes in the MANET network must serve as routers to forward other nodes' packets to ensure successful connectivity from source to destination [3]. In contrast to wired and wireless infrastructure-based networks, MANETs have distinct features, implementations, problems, and concerns. The following sections go into the different features, applications, problems, and concerns.

A. Characteristics of MANET

The key characteristics of a MANET are the absence of a centralized control node that controls its neighbours nodes, i.e., cluster formation with a cluster head. There is no effective cooperation or collaboration between nodes. A network topology that changes dynamically, There is no protection for the operating system world, there are few resources, and so on [4]. In this article, we addressed a variety of characteristics.

1) *Decentralized Control:* There is no power for the core node in a MANET, so contact occurs across all nodes. Without any centralized power, the nodes can communicate with one another and exchange data packets from one node to the next. Both network nodes have access to the whole power.
2) *Dynamic Topology: Remote nodes are the nodes in the MANET. They are able to arbitrarily drive about at various speeds in any direction. Via continuous change of links and topology at any moment, they could be in and out of the network. They set up their own path and dynamically form a network. Between nodes of the network, bidirectional or unidirectional links can be created.*
3) *Multi-hop Communication: If the source node in the network wishes to transmit the data to a target node that is beyond the contact range, multi-hop communication is conducted inside the network. Medium nodes help transfer data by creating multi-Hop networks from sources node to destination node. There might be one or more nodes in the intermediate nodes for multi-hop connectivity.*
4) *Infrastructure-less: MANET communicates between nodes by single-ho or multi-hop communication. Each network node can act simultaneously as the router and host. In the network, all nodes play various functions. Thus the nodes are behaviorally autonomous.*
5) *Scalability: Due to the computing capacity and small memory of mobile nodes, as we consider the big network sizes, scalability is the main concern.*

B. Applications of MANET

MANET programs have emerged as specialized networks which are controlled with the aid of using one authority and tailor-made to resolve precise problems in numerous areas, for instance in army networks, vehicular networks, or sensor networks. Additionally, MANETs are expected to turn out to be a key detail in the 4G structure and use maximum of the important features of typical next-technology Wi-Fi community technologies [5]. We at the moment are discussing traditional software conditions and a few of the most illustrative use instances in recent times that incorporate specific programs of MANETs through army-civilian and commercial programs.

1) *Mobile Conferencing:* MANETs are used for mobile conferencing by allowing business users to work outside of the office where no office network is available. MANET supports various business members in collaborating with any external office infrastructure by sharing documents, files and brainstorming for their projects, etc.
2) *Personal Area Network:* MANETs can also be used as personal networks or as a home network for various uses. We can connect any device through internet connectivity at personal area or home. Therefore, MANET's usability eases the work and allows users to use applications. It also allows the proximal electronic devices with specific functions, such as cameras, storage devices, televisions, mobile phones or laptops, to dynamically share data through as associate autonomous home network.
3) *Emergency Services:* When the occurrence of some natural disaster occurs like earth fire, earth quake, hurricanes, and so forth, they damage the existing infrastructure network. At this time, MANETs can be used to provide necessary solutions. They can also be used to remotely retrieve some specific information about the patients; this can be helpful to rescue team for search operations.
4) *Military Applications:* It supports communication and coordination between soldiers, military vehicles, and information headquarters. These MANETs are also used where there is absence of virtual network for communications.
5) *Vehicular Network:* The main goal is to avoid vehicle crash so that we can keep passengers as safe as possible. This can notify the drivers about the upcoming event on the road side. This also enables the drivers to communicate between each other to avoid accidents. Hence, MANETs plays a crucial task in Vehicular Networks
6) *Education and Entertainment:* MANETs now-a-days are used for education and entertainment purpose. It serves the user to access the applications such as gaming. It is also used in Universities and Campus settings, for Virtual Classrooms, Ad hoc communication during meetings and lectures and Multi-User game, Wireless P2P networking, Robotic pets and Theme parks.

C. Blackhole Attack in MANET

The attackers attack the network either in starting phase or in later phase. In MANET, there are many vulnerable attacks present. One of them is black hole attack. Black hole node drops the packets intentionally without notifying the source node. They can be 'n' number of black hole nodes present in the network.

The black hole attack in the MANET appeal the traffic towards it by forwarding the fake route reply to the source node. Upon receiving the route reply, the source node forward the data packets, which is then dropped by the black hole node. The other types of malicious nodes firstly cooperate with the routing functionalities and then in the later stage they selectively drop the data packets. These types of malicious nodes make use of neighbor nodes but they don't allow the neighbor nodes to use them [6]. However the malicious nodes don't forward the data packet to its neighbor node instead it drops the data packet to conserve energy. As in MANET during data transmission maximum energy is consumed by the nodes. Due to these types of attacks the network performance is degraded at the network layer. The network layer attackers only deal with the packet dropping attack.

There is another type of black-hole attack known as cooperative black hole attack. This type of attack initially cooperates during the establishment of route. Once the route is established then during the data transmission phase they drop the packets [7]. We should provide the secure routing protocols in MANET against these types of attacks. So that, this protocol can mitigates the behavior of routing during data transmission. In MANET there may also be chances that the packet may drop not only because the malicious nodes but also due to some characteristics i.e., due to dynamic network topology, due to non-centralized control, due to distributed network, etc.

D. Secure and Efficient Transmission Routing Protocol

The SETR protocol is the type of on-demand routing protocol. It establishes the route only when the source node wants to transmit the data towards the destination node. This protocol works on the basis of three different messages i.e., Route Request, Route Reply and Route Error. The route request message is sent by the source node to establish the route before data transmission. This route request works as hello message to initialize the communication between two different agents. The route request messages have an extra value field known as time to live (TTL) which notifies us that till how many hops this message should be forwarded. This value can be increased when there is no reply from the node i.e., the request message will be retransmitted to other node. The other type of message is route reply message. This message is send by the destination node only when it receives the route request message. Thus, upon receiving the route request message with destination address, the destination replies to the source node as an acknowledgement message. The last type of message is route error message. This message is forwarded only when the route or links are damaged or broken before reaching the destination node.

The remainder of the paper is organized as follows, Section 2 describes the related work, Section 3 describes the System architecture, Section 4 represents the proposed system and simulation results, and last section concludes the work.

II. RELATED WORK

In MANET, it is challenging to establish a secure and efficient route or path in order to communicate between nodes to send data from source to destination, due to dynamic topology, heterogeneity, mobility of nodes it becomes a challenging task to establish a secure route.

Sushil et al.[8] have evaluated the performance of AODV protocol and Blackhole AODV protocol (bhAODV). Also they have introduced the solution for black hole AODV protocol and given a name as Solution for Black Hole AODV (sbhAODV). They have evaluated the performance by using Network Simulator 2 (NS-2.35). In normal AODV as the number of nodes increases the throughput also increases but when black hole attack is occurred in the AODV protocol then the throughput decreases. Due to increases in number of nodes, the data packets are dropped in normal AODV. Whereas, during black hole attack, the packet drop is more than that of normal AODV. In case of PDR, in normal AODV PDR is maximum and during black hole attacks PDR is minimum. Sharma et al. [9]in this paper the performance of this AODV protocol is calculated based on the metrics such as Packet delivery ratio, Throughput and Node mobility. The simulations are carried out using the Qualnet Simulator. Constant Bit Rate (CBR) application is used in simulation. The simulation is calculated by varying the nodes in network. The network is designed with 40 nodes covering the area of 1500/1500 m^2. All the 40 nodes are normal nodes except the 28^{th} node. This node 28 is considered as black hole node. The evaluated results were the throughput, Packet delivery rate and End-to-End delay is higher than compare to that off black hole node attack. The throughput, packet delivery ratio is decreased and end-to-end delay is increased due to the increase in node moving speed. Hence, final result is that, due to the effect of black hole attack the network performance is reduced by 26%.

Neelam and Khushboo [10], in this survey we have studied that the black hole nodes are analyzed by using Network Simulator 3 (NS-3.26). The performance parameters are analyzed under different rate of black hole nodes present in the AODV protocol. The network scenario was considered of about 25 nodes from which 0, 1, 3 and 5 are considered as black hole nodes. The simulations were calculated only by taking some performance metrics i.e., Throughput, Average End-to-End Delay and Packet loss. By considering Normal AODV and AODV with 0, 1, 3 and 5 Black hole nodes. We have noticed the performance of AODV protocol changes or degraded when it is attacked by black hole nodes.

Thus, we have examined the activities such as route misbehavior in MANET and their mechanisms. Route misbehavior activities are divided in two types such as intentional misbehaving nodes and unintentional misbehaving nodes. Intentional misbehave nodes occur due to some malicious activity in the network, whereas unintentional misbehave nodes occur due to resource constraints of network. We have seen distinct methods for detecting and removing the misbehaving nodes or malicious nodes from the routing path of the network. We can solve the unintentional misbehaving nodes problem by studying the network performance in detail.

III. ROUTE DISCOVERY AND BLACK HOLE DETECTION

The MANET is developed with ties and nodes. Two or more nodes are connected to each other dynamically to communicate. We used a routing protocol called the SETR protocol for establishing the path. This protocol operates on the message sharing principle between the nodes. In the SER protocol, Route Request (RREQ), Route Response (RREP), and Route Error there are trois types of messages (RERR).

The message for the route request shall be sent to start or set up the route through the source node. This letter is connected to the destination such that the message will not be forwarded until it reaches the destination. Therefore, the destination address is checked for each intermediate node. The address does not match the address of the node. But once the message is met, the target transfers the response message to the source node. This message of the route response functions as a message of recognition. This is considered a method of road exploration. The below figure shows the RREQ and RREP process from source to destination.

Following the route find procedure, the data packets will be transmitted by the source node to the destination by choosing the shortest route. This method is called the process of transfer of data. We may observe the black hole assault during this process.

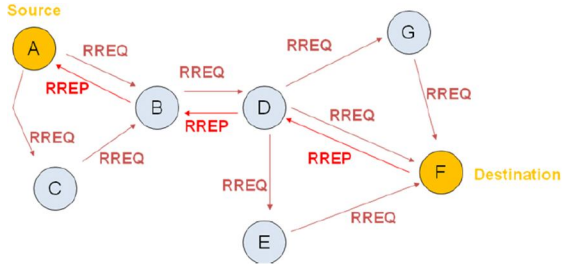


Fig 2: Route Discovery in SETR Protocol

The following figure shows the black hole attack in the commission model. Here 'M' Node acts as a black hole intruder node, attracting traffic by sending the message for the wrong path replay to the source node and then loses all contact data packets.

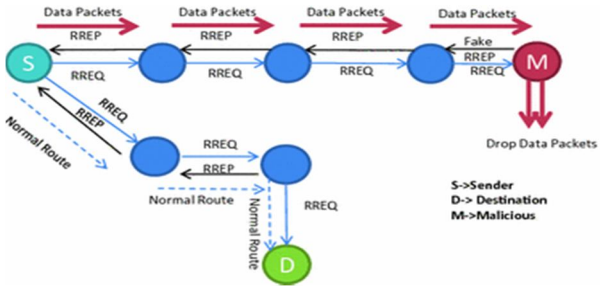


Fig 3: Blackhole Attack in SETR protocol

In fact, this correspondence is between S and D, the source generates and broadcasts the RREQ packet, the attacker Node now receives the RREQ packet with efficient routing information, crates the routing packet and attracts traffic to the REQ packet. Then the final contact data packets are dropped.

IV. PERFORMANCE ANALYSIS RESULTS

The main objective of the project is to examine the achievement of the proposed network routing protocol containing and reputable nodes and malicious odes. Thus we compares the suggested efficiency of the routing protocol with the SET protocol with reputable nodes and the SET routing protocol with reputable nodes. The assessment of success takes the following simulation case into consideration. In this network, accidental and deliberate nodes and reputable nodes are present. Unintentional malfunctioning nodes lose the packet either because of a buffer overload or because of restricted resources or both. Both packets received are discarded from the deliberate incorrect nodes and the wrong message is sent to the source. The scenario aims to test current systems' vulnerability and to determine how the planned work is performed. The situation is designed to assess the efficiency of the planned work against the deliberate misbehavior nodes.

Then the performance evaluation is calculated by below three conditions.

A. The number of multihop nodes between contact organizations varies.
B. Simulation time for different node numbers.
C. Various nodes of energy consumption.

In this simulation, the random mobility point model and 20 m/s pause time are considered as a variable amount of nodes. Initially, the battery is fitted with 20 joules of power per knot, and the 250m fixed radio transmission is equipped with a 2 Mbps data rate IEEE 802.11 MAC card. The power supply is 300mW and the drive capacity 600mW. Finally, the source nodes create 512 byte CBR traffic. The simulation lasts 1000 seconds, and we averaged the results of three scenarios. The simulation takes into account three groups of nodes: simulated nodes that adhere to the routing protocol parameters, simulated nodes that do not, simulated nodes that do not, simulated nodes that do not, simulated nodes that do not, simulated nodes that do not, simulated nodes Intentional misbehaving nodes lose packets due to malicious operations, while unintentional misbehaving nodes drop packets due to buffer overload and limited resources. The following are the threshold values for the region set in performance assessment.
ACK initialization counter tome is 0.8 seconds and

1) ACK packet timeout set to be 0.15 seconds,
2) $TTL = 200\ ms$.

Performance evaluation metrics of the proposed work are throughput, packet delivery fraction, and overhead, energy efficiency.

a) *Throughput:* It is a network efficiency measure that calculates how many packets of data are transmitted in a certain period of time from source to destination.
b) *Packet Delivery Fraction:* The transport ratio for packets is the share of the amount of parcels received by the target hub to the quantity of packages that the source hub transmits. The parcel transport component is the proportion of one hundred bundles.
c) *Overhead:* It is the amount of control packs that are distributed for transmission to actual data transmission in the system (counting direction finding, maintaining the path of transmission).
d) *Energy Efficiency:* This work measures the node's reaming power after simulation period has been completed. In addition, it measures how much energy is used to produce a given quantity of distribution and packages. Ultimately, this reaming power contains details about the node loss caused by battery fatigue.

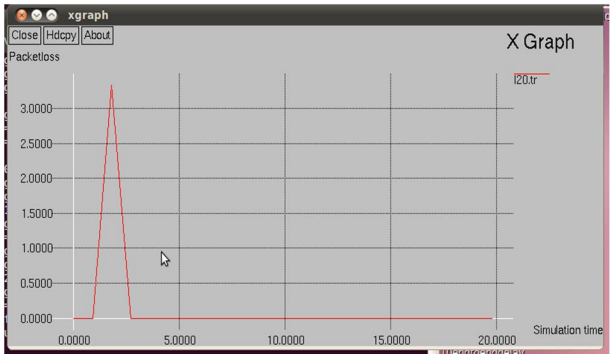


Fig 4: Delay proposed work, number of node with malicious nodes

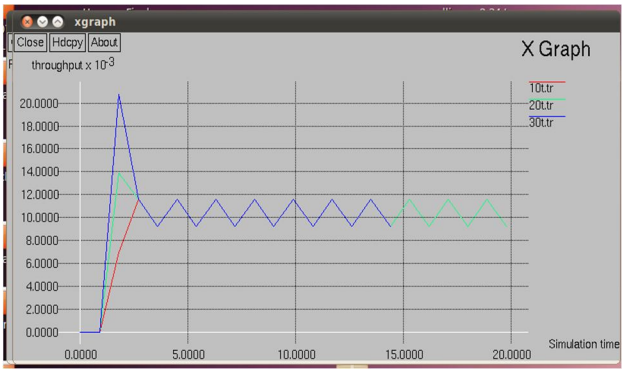


Fig 5: Throughput comparison of number of node with malicious node (Existing and proposed work)

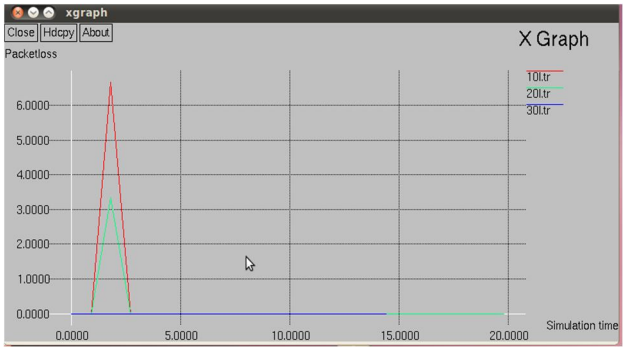


Fig 6: Pack loss comparison of number of node with malicious node (Existing and proposed work)

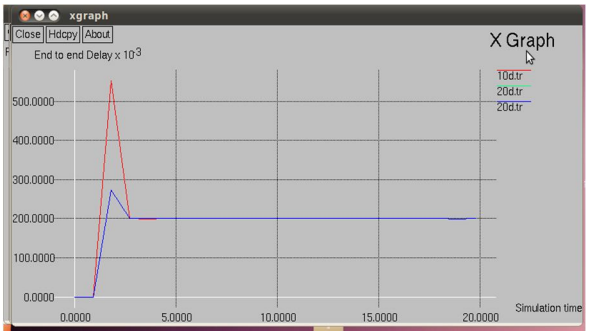


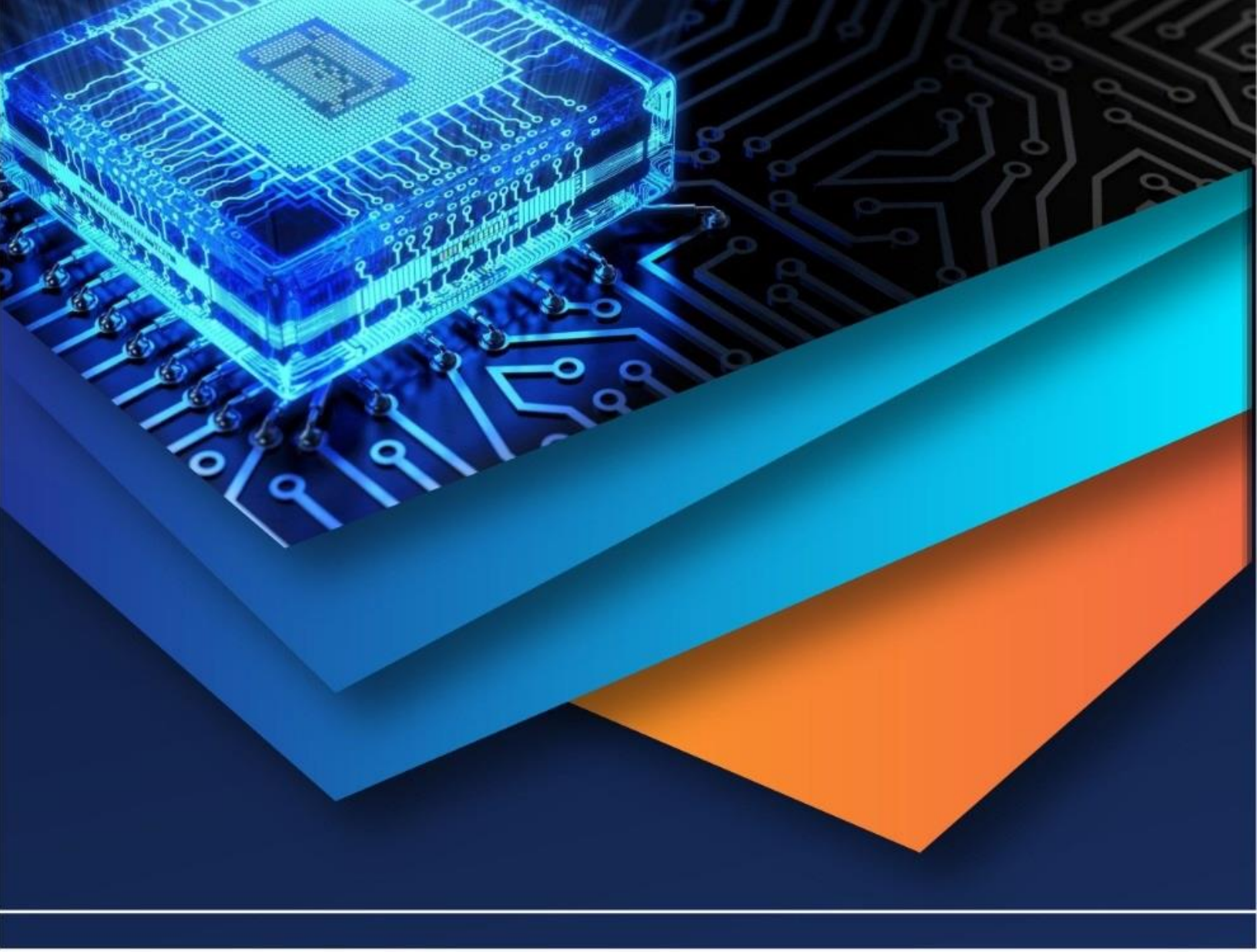
Fig 7: End to End Delay comparison of number of node with malicious node (Existing and proposed work)

V. CONCLUSION & FUTURE SCOPE

We addressed MANETs and security attacks in the SETR protocol i.e. Blackhole attack. Network efficiency decreases since the blackhole nodes present on the network. So, we have simulated SETR's output using Network Simulator 2, to find the solution. Based on the current scenario, we have increased network capacity through the simulation of the energy efficiency of network nodes during transmission on the basis of the various NS-2 scenarios. A standard SETRP without black hole attack is one of the scenarios we considered and the second scenario we considered was the black-hole SETRP attack. In the second example, we calculated the energy consumption output effect of a black hole attack. The results of my project are average energy consumption, lifetime network and residual energy. Other forms of attacks, such as greyhole attacks, may be further allowed in future for the present job. The efficiency parameter can then be measured using various simulators. The mitigation function can also be applied to the nodes in the network. The misbehaving nodes can be identified and disabled quickly by means of a mitigation system. You will extend the network by adding more nodes than the current network. In other ways, clusters are formed to prevent insecure network attacks and prevent failure of data or packets. Thus, various techniques like the examination of multiple attacks, application of the prevention mechanism, formation of clusters, etc, will further enhance the current work.

REFERENCES

[1] Kumar, Sunil, Kamlesh Dutta, and Girisha Sharma. "A detailed survey on selfish node detection techniques for mobile ad hoc networks." Parallel, Distributed and Grid Computing (PDGC), 2016 Fourth International Conference on. IEEE, 2019.
[2] Taneja, Sunil, and Ashwani Kush. "A survey of routing protocols in mobile ad hoc networks." International Journal of innovation, Management and technology 1.3 (2018): 279.
[3] Siddiqua, A., Sridevi, K., & Mohammed, A. K. (2019, January). Preventing black hole attacks in MANETs using secure knowledge algorithm. In Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on (pp. 421-425). IEEE.
[4] Sonu Kumar Aditya, Soni, Ravi Kumar, "Remote Patient Monitoring and MANET: Applications and Challenges, "International Journal on recent and innovation trends in computing and communication, Vol. 3, pp.4275-4283, 2017.
[5] K. S. Ali and U. Kulkarni, "Characteristics, Applications and Challenges in Mobile Ad- Hoc Networks (MANET): Overview," Wireless Networks, vol. 3, 2018.
[6] M. M. Y. Dangore and M. S. S. Sambare, "A Survey on Detection of Blackhole Attack using AODV Protocol in MANET,".
[7] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. E. Nygard, "Prevention of Cooperative Blackhole Attack in Wireless Ad Hoc Networks," in International Conference on Wireless Networks, Icwn '03, June 23 - 26, 2014, Las Vegas, Nevada, Usa, 2003, pp. 570-575.
[8] S. Kumar, D. Singh and S. Chandra, "Analysis and Implementation of AODV Routing Protocol against Blackhole Attack in MANET," International Journal of Computer Applications, vol. 124, pp. 975- 8887, 2015.
[9] S. Sharma and R. Gupta, "Simulation Study Of Blackhole Attack In The Mobile Ad Hoc Networks," Journal of Engineering Science & Technology, vol. 4, 2016.
[10] N. J. K. Patel and K. Tripathi, "Analysis of Blackhole Attack in MANET Based on Simulation through NS3.26".



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY