International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 3, ISSN No. 2455-2143, Pages 582-588
Published Online July 2020 in IJEAST (http://www.ijeast.com)

A WORM HOLE ATTACK DETECTION IN MOBILE AD-HOC NETWORK USING GA AND SVM

Rubi
J.C Bose University of Science and Technology
YMCA Faridabad, Haryana, India

Dr. Rashmi Popli
J.C Bose University of Science and Technology
YMCA Faridabad, Haryana, India

***Abstract*— Mobile Adhoc Network (MANET) - A MANET is a collecting of self-arranged node connected with wireless connections. Every node of a mobile ad hoc network goes about as a router and discovers an appropriate route to forward a packet from source to destination. This network is relevant in regions where establishment of framework is not possible, such as in the military condition. In a mobile ad-hoc network (MANET), there is a short-term network setup by boundless nodes, which move anywhere and communicate within the absence of centralized network. In Wormhole Attack, two or more malicious node discover a wormhole attack using a private channel called tunnel Wormhole tunnel will at that point begin gathering the data packets and transfer the same to some other area. Proposed work recommended the proficient and secure routing in MANET. We have chosen 20 significant features at that point make a dataset that labelled with the help of a one of a kind node address. Along these lines, apply two popular Machine Learning classifiers that group into two classifications to be specific normal and malicious data of test samples. We are using Genetic Algorithm for feature selection and SVM (Support Vector Machine) for classification. The exhibition of the system evaluated on various measurable parameters and compared and the recent methods.**

***Keywords*— MANET, Wormhole attack, Genetic Algorithm, SVM, RREQ, RREP**

I. INTRODUCTION

A MANET (**Mobile Adhoc Network**) is a collecting of self-arranged node connected with wireless connections. Every node of a mobile ad hoc network can act itself as a router to forward the packet from source node to goal node. Mobile ad hoc network are broadly used network and very vast. Each movable node is self-managing node and there is not any central node for managing the mobile network. The movable nodes have permission to shift anywhere according to its need. It allows that the nodes can easily join or leave the network.

The capability of nodes for communication is not limited. When the connection is established and the nodes lie outside from the radio range of network then it may cause loss of data. MANET has large application in different areas like research, rescue operations, military etc. Due to increase of communication over networks the cyber attacks are also increasing.

Wireless mobile ad-hoc networks are sensitive to many security attacks because light of shared channel, unconfident working environment, restricted resource accessibility, dynamically changing system topology, resource limited. The architecture of MANET is shown in figure 1.

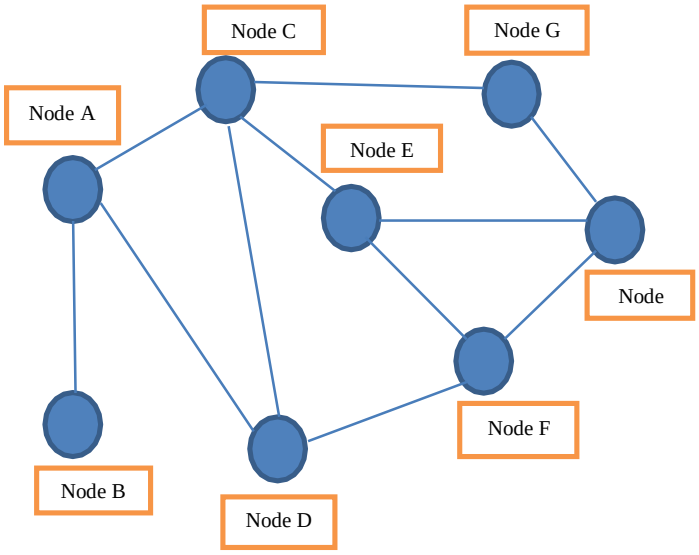


Fig 1: Mobile Ad-hoc Network

Wormhole attack is type of network layer attack and it represent the problem against routing protocols. Two or more malicious node discover a wormhole attack using a private channel called tunnel. Wormhole tunnel will then start gathering the data packets and relay the same to some other location. At one side of the tunnel, a malicious node gets a control packet and sends it to another fascinating node at the opposite end through a private channel, which rebroadcasts the packet locally. Route for correspondence among source and goal is chosen through the private channel because of having better estimation e.g., less number of hops or less time, when as compared to packets communicated over other ordinarily route. The main focus of this research is to propose a wormhole attack detection technique. In this paper, we proposed an effective wormhole attack detection technique.

The wormhole detection algorithm composed of two primary strategies to be specific Genetic Algorithm(GA) and Support Vector Machine (SVM). Genetic Algorithm technique is used for feature selection and SVM (Support Vector Machine) is used for classification.

Security Problems in MANETS:

- open media
- Routing protocol don't have any security component

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 3, ISSN No. 2455-2143, Pages 582-588
Published Online July 2020 in IJEAST (http://www.ijeast.com)

• inaccessibility of central organizer.

The rest of this paper is organized as follows. In section 2, we describe the wormhole attack. In section 3, the related work about the detection of wormhole attack using various approaches are presented. In section 4, the proposed wormhole attack detection method is presented. In Section 5, the simulation techniques used in detection are described. In Section 6, simulation results to evaluate the proposed method are presented, and we make concluding remarks in Section 7.

II. WORMHOLE ATTACK

Wormhole attack is one of most serious security attack in MANET. It can harm more MANET routing protocol (DSR), AODV, OLSR, DSDV etc. At least two malicious node find a wormhole attack using a private channel called tunnel. Wormhole tunnel will at that point then begin gathering the data packets and transfer the same to some other location.

Working: At one side of the tunnel, a malicious node gets a control packets and sends it to another interesting node at the opposite end through a private channel, which rebroadcasts the packet locally. Route for correspondence among source and goal is picked through the private channel because of having better measurements for example less number of hops or less time, when contrasted with packets transmitted over other normally route. The attack normally works in two phases.

In this Figure, MANET describe how to work MANET in the Wormhole Attack.

The architecture of wormhole attack is shown in figure 1.

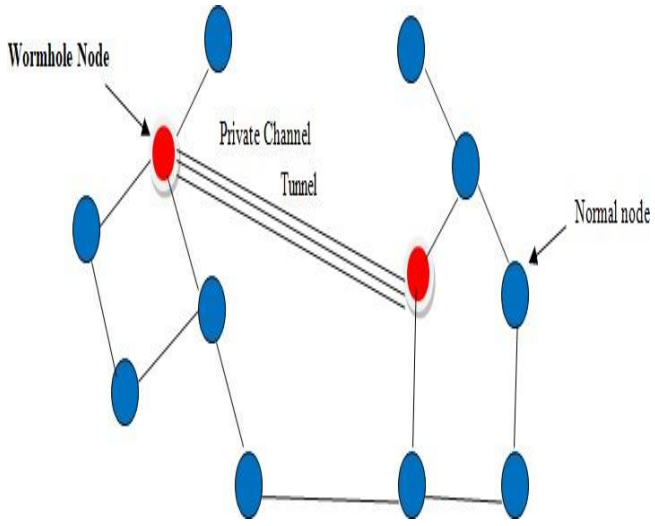


Fig 2: Wormhole Attack

In first stage, the wormhole nodes get themselves involved in many routes. In the second stage, these malicious nodes begin utilize the packets they receive. These nodes can confuse the network functionality in a number ways. Wormhole nodes can drop, modify, or send data to a outsider for malicious purpose. Different kind of attack, for example, DOS attack, Eavesdropping and creation can be performed with the utilization of this enable. Wormhole attack can cut down the entire routing network in MANET.

III. RELATED WORK

Wormhole attack is major threats to mobile Adhoc network. Wormhole attack is a type of network layer attack where the two or more malicious node discover a wormhole attack using a private channel called tunnel. Wormhole tunnel will then start gathering the data packets and relay the same to some other location. In wormhole attack, it is not required to target all the nodes in the network only its closed nodes are enough to target.

It is recognized that some recent works in wormhole attack detection in MANET use various techniques such as Machine Learning, Genetic algorithm, and Support vector machine (SVM) and many more techniques. This technique for wormhole detection the malicious nodes and stay away from the routes having wormhole nodes without affecting the exhibition of the network. The various techniques used to detect and prevent the wormhole attack are discussed as follows:

Jignesh Joshi et. al. propose a model to detect wormhole attack in MANET. In these methodology named "Hop Based Analysis" the wormholes noes are resolved when sudden decrement in the average hop count of a way from the source node to the goal node had been seen when contrasted with the another ways because the fact that the way with wormholes nodes has extremely littler hop count. This algorithm uses a few methods to be specific Time of Flight, Packet Leash, Trust Based Approach, RREQ Based Analysis. In this paper, we have basically analyzed the current mechanisms that will help us in future to develop another procedure for wormhole attack detection. One arrangement can't be applicable to all situations. According to need of systems, arrangements may very and decision is accessible dependent on cost and need of security. [2]

Richa Mudgal et. al. proposed an approach to detect wormhole attack in MANET using some approaches like Path tracing approach, A trust based approach, Improved Trustful Routing Protocol, RTT based approach etc. This paper focus around impact of this attack has been demonstrated to be adverse to network performance, lowering the packet delivery ratio and drastically expanding the end-to-end delay.

In spite of the fact that part of examination has been done to battle wormhole assault and numerous wormhole discovery methods proposed by scientist like Packet rope, SECTOR, SAW, DAW, Delphi, Multi-way Hop-Count and TTM. Utilizing this methodology of support length and RTT calculation, routing overhead minimizes [3]

T. Sakthivel and R.M. Chandrasekaran et. al. proposed a detect and prevent wormhole attack in MANET. It depends on "Path Tracing Approach" utilizing this methodology when wormhole is identified, it is eliminated of from the system and then new course is chosen for routing. At the point when wormhole is identified, warning message is passed to entire network. So all other node of network will remember the ID of attacker for the wormhole node list for additional avoidance of

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 3, ISSN No. 2455-2143, Pages 582-588
Published Online July 2020 in IJEAST (http://www.ijeast.com)

attack. This proposed scheme included two stages, Phase 1 figure for each hop distance of all sending node and in nodes 2 all nodes detect the wormhole node from data fetched from the stage 1.

K. Singh, G. Singh and A. Aggarwal et. al."A Trust based Approach" for Detection and Prevention of wormhole Attack in MANET. It is proposed another infrastructure developed for the avoidance of wormhole attack which can distinguish and prevent the wormhole attack. Nodes and device are composed utilizing a fixed foundation of MANET gadgets, where gadgets are classified in Mobile nodes, Cluster Heads, Monitoring worker. These nodes essentially take an interest in information communication.

D. S. Kushwaha, A. Khare and J.I. Rana et. al."Improved Trustful Routing Protocol" to detect wormhole attack in MANET. This technique works on the concept of finding the substitute path to the objective node T. These alternative path are not comparable long methods length of alternative path is more greater than wormhole path and just at this circumstance wormhole draws in huge rush hour gridlock. Threshold value is determined by checking normal number of nodes between node in the system. In this methodology Threshold is the primary part of this strategy. Wormhole tunnel is available or not, is chosen by threshold. In the event that the estimation of interchange way is more noteworthy than the threshold value, at that point wormhole is recognized.

Soo Y. Shin & Eddy H. Halim et. al. "RTT based approach", proposed detection scheme based on three combinational advances which are route repetition, route aggregation and Round-Trip-Time(RTT)calculation. Those mixes are required to get the receive most brief way and identify malicious node whose make wormhole tunnel. Routes redundancy beginnings when source sends RREQ utilizing every single imaginable approaches to goal. All routes that associate source to goal are recorded along with number of hops from each route of system. Attacker in wormhole attack may drop the information packets and mislead the transmission. To detect and prevent the system from attacker, numerous analysts had created wormhole discovery calculation dependent on various methods.

Muhammad Imran and Farrukh Aslam Khan et. al. In this paper introduced the features that could be utilized to identify the wormhole attack. These features are talked about in detail with their pros and cons. The potential restrictions of Intrusion Detection Systems(IDS) are additionally examined. This work gives a basis to build a productive IDS to identify wormhole attack in MANETs. According to our analysis, the methods dependent on route request (RREQ) or hop count would be better than different procedures to distinguish wormhole attacks. As future work, we intend to manufacture an IDS for MANETs dependent on RREQ.

Aakanksha Kadam and Niravkumar Patel et. al. "Adhoc Demand Distance Vector routing algorithm in Detection and Prevention of Wormhole Attack in MANET", proposed Wormhole attacks in MANET can fundamentally degrade systems execution and undermine arrange security. In wormhole attacks as the adversaries usually replay the authentic information packet, identification of these attacks is very complicated. In this paper we have discussed about what a wormhole really is and to recognize them in the MANET. All the recognition systems have their own advantages and drawbacks. Be that as it may, there is no recognition technique which recognizes wormhole attack perfectly. Here we have concentrated all the current methodologies and tried to suggest our methodology of utilizing brilliant packet so as to eliminate the disadvantages experienced in before proposed works.[4]

Table 1: Comparison of Wormhole Attack Detection Methods

AUTHORS	TECHNIQUES	TOOL	OBSERVATION	YEAR PUBLISH
1.Ashka Shastri et. al	Hop-Based Analysis Technique	NS2	Able to detect both hidden and exposed attack.	2016
2.Richa Mudgal et. al	AODV Technique	NS2	Approach is that the routing overhead is greatly reduced.	2016
3.Soo Y. Shin et. al	RTT based approach	NS2	It required to receive the true shortest path and detect malicious node whose create wormhole tunnel.	2012
4.D.S Kushwaha et. al.	Improved Trustful Routing Protocol	NS2	Threshold is main part of this Technique. It is calculated by checking average number of hops between nodes in network.	2013
5.Muhammad Imran et. al	Detection Feature for wormhole Attack in MANET	NS2	Intrusion Detection System(IDS) and RREQ to detect wormhole attack .	2015
6.Vikas Raina et. al	Genetic Algorithm and AODV Protocol	MATLAB	Increase Throughput and PDR, decrease Delay	2017

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 3, ISSN No. 2455-2143, Pages 582-588
Published Online July 2020 in IJEAST (http://www.ijeast.com)

In this paper various methodologies are introduced for the detection and prevent of wormhole attack in MANET and alongside that another technique is proposed which is utilized for discovery of the attack. Consequently, a providing a superior way to deal with battle against this kind of attacks in which ill-conceived clients utilize weakness present in the system

IV. PROPOSED METHODOLOGY

This proposed methodology to divided into 3 parts:

- Route discovery process
- Route optimization process
- Wormhole attack detection process

4.1 Route Discovery Process

In this process firstly the nodes environment is created with various nodes. Source node want to establish the connection for transmitting the data to the destination node. Source node sends the data packets to the destination using some middle nodes. These middle nodes are called the Routers. If the source find the Route from source to destination node then it sends the data packets otherwise it sends the RREQ (Route Request) to the destination node for finding the data path. If route is Discovered then the destination node sends the RREP (Route Reply) message to the source node which contains the node ID, Sequence number and other details. If these details are matched with the source node details then connection is established otherwise connection is lost.

In Figure 3, various routes are available from source to destination and we have to choose best route for the data transfer.

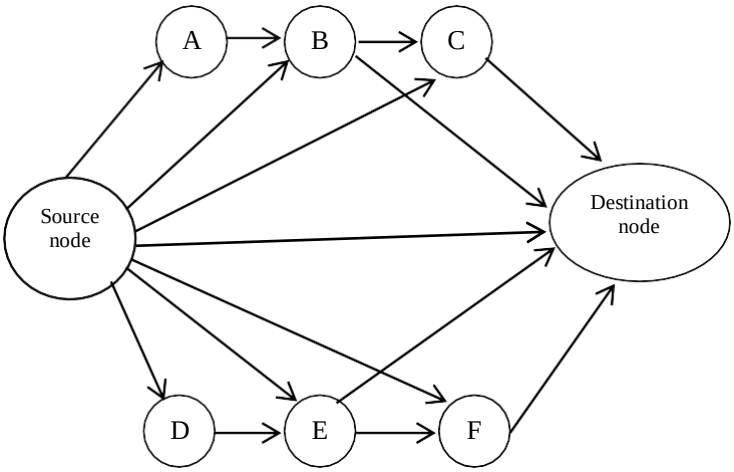


Fig 3: Route Discovery

4.2 Route Optimization Process

In this section , the GA (Genetic Algorithm) is used for the route optimization. Genetic algorithm are used in artificial intelligence like other search algorithm are used in artificial intelligence- to search a space of potential solution to find one which solves the problem. We are using **Genetic algorithm** for feature selection and **SVM** for classification. The nodes locates the optimal solution by moving through nodes environment space for representing all possible outcomes.

4.2.1 Advantage of Genetic Algorithm

- GA support multi-objective optimization.
- GA is give positive feedback.
- GA use objective function information, not derivatives.

4.3 Wormhole Attack Detection Process

In this proposed work, two optimization algorithm GA (Genetic Algorithm) and SVM (Support Vector Machine) are used. Our proposed method provides an efficient detection method that detects malicious information; a wormhole attack deployed in an ad hoc network with normal and malicious nodes that trace output file.

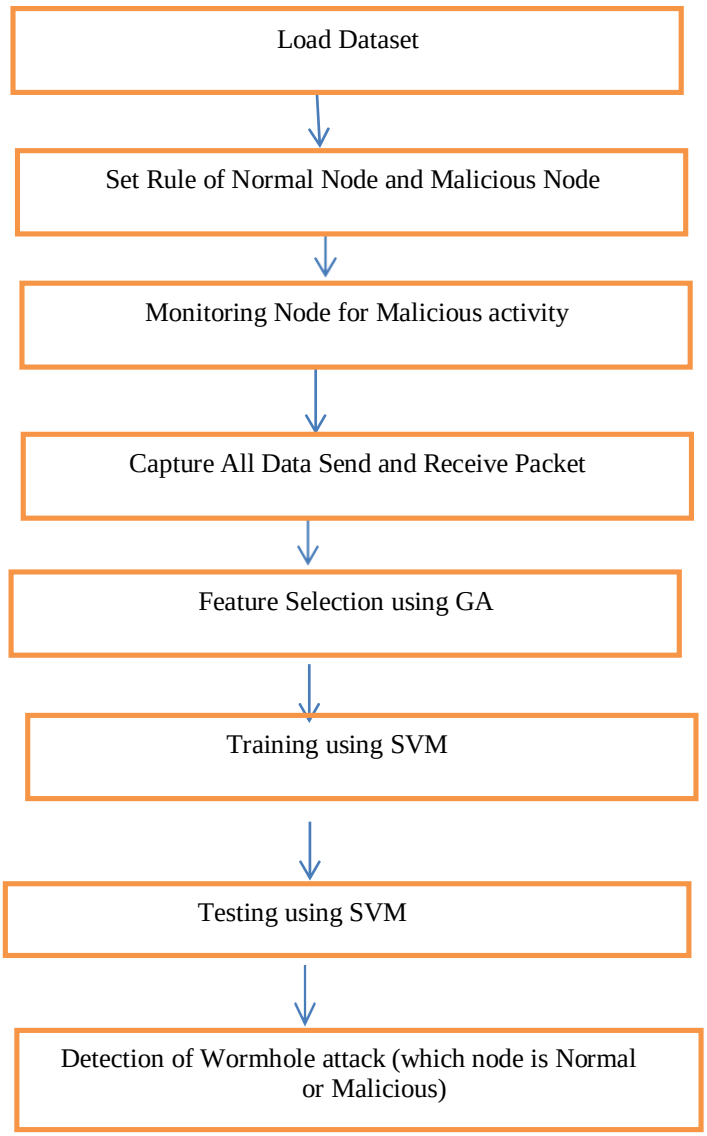


Fig 4: Proposed Methodology

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 3, ISSN No. 2455-2143, Pages 582-588
Published Online July 2020 in IJEAST (http://www.ijeast.com)

We apply machine learning algorithm for feature selection and information collection. At first, we characterize the quantity of typical nodes and malignant nodes with their practices.
In this arrangement between the malicious nodes make a tunnel and just transfer the message or packets over the tunnel. At the point when the malicious node is neighbor of the main typical node, at that point move message without including data of itself. At that point, follow data of every node of moving and accepting a message that helps in data collection where the determination of significant feature can expand the framework execution. We have chosen 20 significant feature at that point make a dataset that marked with the assistance of an exceptional hub address. Hence, apply two famous machine learning classifiers that order into two classifications specifically ordinary and malicious information of test samples. We are using **Genetic algorithm** for feature selection and **SVM** for classification. The performance of the system evaluated on different statistical parameters and compared with the recent methods.

Security of MANET is fundamental to prevent the harm that could be caused by various sorts of attacks. The worm-hole attack is viewed as one of the well known attacks that harm the system and intend to prevent any connection in the system. AODV routing protocol attempts to locate the shortest path between two node that need to convey in the system when the path is required.

Dataset Feature Attribute

S. No	Feature name	Type
1	Duration	continuous
2	Protocol	discrete
3	Packet size	continuous
4	Flag	discrete
5	header length	continuous
6	hop count	continuous
7	life time	continuous
8	message type	discrete
9	destination sequence number	continuous
10	message sequence number	continuous
11	stream index	continuous
12	Land	Discrete
13	Message transfer Mode	Discrete
14	number of neighbors	Continuous
15	highest flow	Continuous
16	average flow	Continuous
17	lowest flow	Continuous
18	average hop count	Continuous
19	number of failed connection	Continuous
20	failed connection rate	Continuous

V. MATERIALS AND METHODS

This research has developed a novel algorithm for the detection of wormhole attack using **Genetic algorithm** for feature selection and **SVM** for classification. The performance of the system evaluated on different statistical parameters and compared with the recent methods.

5.1 Genetic Algorithm (GA)

Genetic algorithm are used in artificial intelligence like other search algorithm are used in artificial intelligence- to search a space of potential solution to find one which solves the problem. They are commonly used to generate high quality solutions for optimization problems and search problems by relying on biologically inspired operators such as mutation, crossover, chromosome and selection.

5.2 Support Vector Machine (SVM)

In machine learning, Support-vector machines are regulated learning models with related learning calculation that examine information utilized for characterization and regression analysis. In any case, essentially they are utilized for classification problems. SVM have their one of a kind method of execution when contrasted with other AI calculations.

The target of SVM calculation is to discover a hyperplane in a N-dimensional space that distinctively order the information point. The hyperplane will be create in an iterative way by SVM with the goal that the error can be limited. The objective of SVM is to isolate the datasets into classes to locate a maximum marginal hyper plane.

VI. SIMULATED RESULTS

In proposed work simulation version of MATLAB 2018a form is utilized. It is most generally utilized device for MANET. Here the simulation area is 1000 × 1000 meter. There are 20 nodes conveyed in random position. All the node are SVM-GA

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 3, ISSN No. 2455-2143, Pages 582-588
Published Online July 2020 in IJEAST (http://www.ijeast.com)

empowered sending the route request for goal node In this situation node D is utilized source of the worm hole and node U is utilized as worm hole sink to apply tunnel between them. The coverage area of nodes are arranged 100m. Each packet begins from source to goal with a randomly chosen speed. A delay time of 200 seconds was chosen. From this simulated environment the 21 system layer highlights are gathered. What's more, these system layer features are utilized in the framework to recognize the attacks. Simulation has been done in MATLAB R2018A environment and the performance has been examined with and without optimization and classification. Performance of Existing and Proposed protocols in MANET can be realized by quantitative study of values of different metrics used to measure performance of routing protocols which are as follows:

Simulation Profile

The simulation profile is listed in table below:

PARAMETER	VALUE
Number of nodes	20
Coverage Area	1000m * 1000m
Channel Type	Wireless Channel

Table 2: Simulation Profile

6.1 Packet Delivery Ratio

The greater value of packet conveyance ration implies better execution of the convention. It is proportion of number of packets effectively conveyed to the goal to the total packet created by sources. The Packet conveyance proportion of system, when the quantity of nodes are 20 is given in arrange.

6.2 Network Throughput

In total simulation time, the ratio of amount of data transferred from one end towards another end is known as throughput. Throughput is the quantity of information parcels conveyed from source to goal per unit of time. Throughput is determined as gotten throughput in bit every second at the goal.

Analysis:
It is the proportion of number of parcels dropped by nodes because of different reasons. The lower estimation of the packet lost methods the better execution of the protocol.

Packet lost = No of packet send - No of packet received.

Evaluated the performance of GA and SVM algorithm with wormhole and without wormhole attack by observing change occurred in the value of various performance metrics such as Packet delivery ratio, end-to-end delay, throughput, packet loss , as well obtained simulation results by varying number of nodes in the network from 10 to 50 .

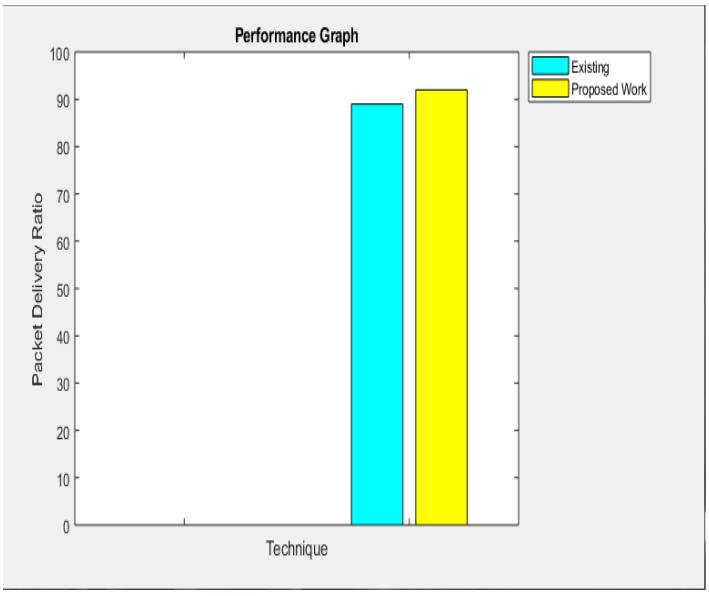
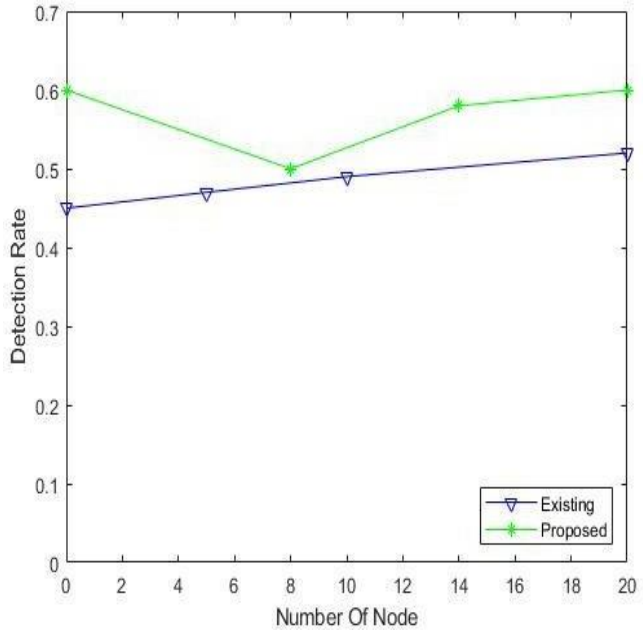


Fig: Performance Graph



VII. CONCLUSION

In this paper, a technique for learning a machine dependent on the SVM-GA classifier is proposed to recognize the prediction of malicious nodes and attack to MANET and consider node attributes in the system. By identifying healthy and destructive nodes, it is conceivable to predict the attacks on the path. Subsequently, with the expectation of attack on the route, there could be a protected route and a sheltered route. The simulation results show that the proposed technique has high accuracy in ordering and predicting harmful nodes in the system. The accuracy of the proposed strategy is about 85%, which is similar with past methods in predicting malicious nodes and system invasion.

Later on, in the field of recognizing and anticipating attacks in the mobile case systems, one can combine class divisions to build the precision of order and forecast of bad nodes and, at

last, attacks on the system. Also, by mix of probabilistic capacities with class divisions can be another enhancement for this article, which permits you to examine and predict new and unknwon kinds of attacks.

VIII. REFERENCES

[1] Muhammad Imran, Farukh Aslam Khan,Tauseef Jamal,Muhammad Durad, et. al. Analysis of Detection Feature for Wormhole Attack in MANETs ,in: Procedia Computer Science 56(2015)384-390.

[2] Ashka Shastri, Jignesh Joshi, et. al. A Wormhole Attack in Mobile Ad-hoc Network: Detection and Prevention , in:ICTCS'16,March 04-05,2016.

[3] Richa Mudgal, Rohit Gupta, et. al. An Efficient Approach for Wormhole detection in MANET,in:ICTCS'16,March 04- 05,2016.

[4] Aakanksha Kadam, Nirav kumar Patel,Vaishali Gaikwad, et. al. Detection and Prevention of Wormhole attack in MANET, in: IRJET, Volume 03 Issue:0|Mar-2016.

[5] Gauri Mathur,Raj Karan Singh,M.Vijaya Raju, et. al. Implementation and Comparison of a New Wormhole Detection Technique with Existing Techniques,in:IOSR- JCE,e-ISSN:2278- 0661,p-ISSN:2278-8727Volume 16(May- Jun,2014),PP 84-91.

[6] Marcus Okunlola Johnson,Arish Siddiqui,Amin Karami, et. al. A Wormhole Attack Detection and Prevention Technique in Wireless Sensor Networks, in: International Journal of Computer Applications(0975-8887)Volume 174-No-4,September 2017.

[7] Dr. V. Khanna, Dr. C. Nalini ,et. al. A Supervised Learning Approach Using Support Vector Machine for Intrusion Detection System in MANET, in: International Journal of Pure and Applied Mathematics Volume 117 No.21 2017.

[8] Suresh,KC& Prakash, et.al.'MAC and Routing Layer Supports for QoS in MANET: A Survey', International Journal of Computer Applications, Vol.60, No.8, December 2012, pp.41- 46.

[9] V. Karthik Raju &K. Vinay Kumar, et. al. 'A Simple and Efficient Mechanism to Detect and Avoid Wormhole Attacks In Mobile Ad Hoc Networks', International Conference on Computing Sciences, 978-0-7695-4817-3/12 2012 IEEE.

[10] Aatmprakash Dwivedi &Abhishek Pandey, et. al. 'An Approach to Provide Security Against Wormhole Attack in MANET',International Journal of Modern Engineering & Management Research, Volume 5 Issue 4| December 2017.

[11] Chaki, Rituparna; Chaki, Nabendu; et. al. "IDSX: A Cluster Based Collaborative Intrusion Detection Algorithm for Mobile Ad-Hoc Network"; Proc. of the 6th Int'l Conf. on Computer Information Systems and Industrial Management Applications (CISIM '07); pp. 179 - 184, June 2007; ISBN: 0-7695-2894-5

[12] Wenwu He and Yang Liu; et. al." To regularize or not: Revisiting sgd with simple algorithms and experimental studies."; Expert Systems with Applications, 112:1– 14, 2018.

[13] Korkmaz T.; et. al."Verifying Physical Presence of Neighbours against Replay based Attacks in Wireless Ad Hoc Networks"; Proc. International Conference on Information Technology: Coding and Computing 2005, ITCC 2005, pp. 704-709, 2005

[14] C. Chigan, R. Bandaru; et. al. "Secure Node Misbehaviors in Mobile Ad Hoc Networks"; Proc. of IEEE Conf. on Vehicular Technology Conference, VTC 2004, Vol. 7, pp. 4730-4734, 2004

[15] T. J. Nagalakshmi, P. C. Kishore Raja, S. Pravin Kumar, V. Veeramanikandan, et. al."Intrusion Detection System using One Class SVM with and without Feature Selection in Wormhole Attack Detection", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-2S4, December 2019.