Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

# Security Analysis Of Malicious Attacks In MANET Through Machine Learning Algorithm

**[1] Surabhi Srivastava , [2] Chandra Shekhar Yadav , [3] Pradeep Kumar**

[1]M. Tech. (CSE) , [2](Head of Department) , [3](Professor)

**[1,2,3]** Department of computer science and engineering Noida institute of engineering and technology.

---

**Abstract:** There are more nodes in this network that are vulnerable to denial-of-service (DoS) attacks because to the network's more complicated and frantic routing method, making the topology of MANET more volatile than other networks. For example, AODV is more popular than table-driven routing, which relies on flooding to discover the best route. Attackers have taken use of this idea to launch denial-of-service attacks (DoS) similar to floods; the black hole and grey hole attacks are the MANET-branded ones. Network form flexibility and movable node mobility are fundamental aspects of MANETs, which are distinct from other types of networks. Network speed, latency and packet transfer rate are the topic of this essay. A neural network known as a jump field is used to transmit packets. Both end-to-end delays and packet transfer rates and throughput improve. Additionally, there is a section on how to recover from wireless mobile node network congestion. Machine learning applications may prevent packet loss in the future by iterating on the iteration that began. Embedded network applications are discussed in general terms after a look at the research outcomes. There was a lot of emphasis on the in-network processing approaches that were selected and compared to the Hopfield neural network and the back propagation network based on their physical appearance. The number of mobile nodes in a network may be increased. In the next neural network, a new context is introduced. Our test implementation has produced encouraging results so far and we need to describe how neural networks might be employed in a mobile node network.

**Keyword:** MANET, Denial-of-Service Attack, AODV, Neural Networks, Gray hole Attack

## I. INTRODUCTION

Ad-hoc networks are considered to be decentralised networks. This kind of network is known as an ad hoc network because it does not rely on a central infrastructure such as routers (in wired networks) or access points (in wireless networks with controlled architecture) to function. There are no wired restrictions on hosts in wireless networks. Network topology may be dynamic and

faulty because of this. As an alternative to established network infrastructure, MANET uses multiple-hop peer-to-peer routing. When the nodes are not within radio range of each other, we use multi-hop routing. Each infected host serves as a gateway. Nodes are able to move and join freely, resulting in a constantly shifting network structure. No permanent routers exist; instead, each node functions as a router and forwards traffic from other nodes to itself. With its dynamic nature, this network's routing process is more complicated and nervous, which makes it more subject to assault from malicious nodes or intruders, making it more prone to denial-of-service attacks (DoS). Communication security is a major worry in today's world. There are numerous layers of defences in place to protect a network from a malicious node in modern security practises. A very vulnerable network like MANET needs secure communication. " MANET is a dynamic network made up of mobile nodes linked by a wireless medium [2]. Military, rescue, and health care are just a few of the domains where MANETs may be used since they don't need the development of a network infrastructure. Furthermore, in important situations like combat communication, the security of this network is a must. The network's security flaws make it an enticing target for attackers who want to infiltrate it. In order to prevent any harmful behaviour on the network, it's essential to implement a security system that's both efficient and versatile. The topology of a MANET is constantly changing due to the dynamic nature of mobile nodes, making it very difficult to deploy any security measure. The network is self-configured and self-deployed, and there is no central authority for communication [3]. The network is more vulnerable to mistakes and security risks due to the fact that the communication between the nodes takes place through a wireless channel. There is also multi-hop communication, in which data packets are sent by several nodes along the way. Each node is also linked to other nearby nodes. As a result, the dynamic nature of MANET infrastructure creates new research opportunities in the domain of MANET security [4]. In an ad hoc context, machine learning techniques may be used to construct a prediction model for identifying unknown security vulnerabilities. As a result, the next parts of this article detail precisely how ML-based algorithms contribute to MANET security.

### 1.1 Security Approaches in MANETs

Decentralization, self-management, and other aspects of MANETs draw a variety of assaults. A wide range of security techniques have been presented in the previous decade to identify and mitigate threats. Here is a breakdown of the many approaches: The original MANET security protocols depended on the use of cryptography to protect the network. Threshold cryptography was used in 1999 to develop a key management method for securing ad hoc networks. Some nodes in the proposed system were designated as servers, while others were designated as administrators. A more secure variant of AODV, code-named SAODV, has also been suggested [5]. For cryptographic security in ad hoc networks, the suggested solution used digital signatures and hash chains. Countless cryptographic schemes relied on a centralised certificate issuing authority to provide certificates for authentication [6]. Other approaches, like the PGP web of trust model, have tweaked the central supervision notion [7]. Thus, the authentication procedure comprises a certificate chain that is saved at each node's end in these approaches. Cryptographic processes have

been shown in literature to cause considerable delays in communication and need a pre-existing link between nodes, which is not practicable in ad hoc networks, as has been seen. It was for this reason that the researchers put together a vast variety of hybrid techniques for MANET security enhancements.

MANET nodes are vulnerable to a wide range of assaults, both active and passive. Denial of service attacks, man in the middle attacks and floods are only few examples of popular assaults. Black hole and grey hole attacks are also prevalent. A variety of intrusion detection systems have been developed in literature to detect a variety of threats. Security in MANETs has traditionally relied on a variety of cryptographic procedures, but in the recent decade, academics have turned to new technologies like machine learning and deep learning, AI, and genetic algorithms in their hunt for the most effective and efficient ways to secure MANETs. Due to the need for security solutions, this paper provides cutting-edge technologies that have already proven themselves. A variety of secure routing protocols and machine learning-based detection, prevention, prediction, and mitigation techniques were used.

## II. MANET SECURITY AND ATTACKS

The relevance of MANET security is discussed by Baadache et al. According to the authors [8,] MANET security involves ensuring mutual confirmation of participants' nodes, confidentiality and integrity of transmitted data, availability of network resources, access control to the communication channel, and anonymity. Attacks on MANETs often involve trying to discard or edit packets, as well as obtaining justification or authorisation by introducing fraudulent packets into a data stream. There are many different sorts of assaults, some of which are mentioned here. [18]

**A. Service of Denial Attack (DoS**): DoS attack [11] conducted by the intruder injecting packets onto networks to eat network resources. If, for example, a suspicious node floods the MANET with route request packets, the malicious node may easily take the bandwidth.

**B. Flooding Attack:** It is a denial-of-service attack in which a malicious node transmits a large number of useless packets in an attempt to consume network resources. In most on demand routing protocols, flooding assail is possible.

**C. Routing Table Runoff:** Route request packets sent by misbehaving nodes might attack the routing database of other nodes by looking for non-existent nodes. Routing tables may be updated by non-existent networks after receiving route request packets from rogue networks. As a result of the memory limitations, the routing tables of the targeted nodes will eventually be cleared.

**D. Impersonation:** To convey falsified routing information, a node may pose as another node to fool the recipient. Malicious nodes may also get unlawful access to resources and perceptive information, and even give false instructions or status information to other nodes.

**E. Power Consumption:** The power consumption of mobile nodes is critical in ad hoc mobile networks. It is possible for a node that is misbehaving but has enough of power to transmit large numbers of packets to attack other nodes. Once these packets have been received, these mobile nodes may be required to relay them or record route information. These packets, as a consequence, consume power from mobile hosts.

### 2.1 Security Solutions Based on Machine Learning

Packets and routing protocols need to be secure in order to function properly on a network. The network's important security aspects must be taken into account while creating sensitive applications. Predictive models may be built using machine learning approaches that use training data for certain attack patterns, and then testing data for the remaining data. The learning model's accuracy is measured by its ability to recognise new assault patterns. There are a wide variety of assaults that may target MANET nodes, including flooding, denial-of-service (DoS) attacks and other forms that take advantage of the network's openness. Multi-hop communication implies that a packet is sent from one node to another before it reaches its final destination in a MANET. Communication is dependent on the cooperation of all the nodes in a particular network Since a result, determining the trustworthiness of nodes is critical for network security, as packets should not be routed to any node that is either untrustworthy or hostile. If you want to increase network security, there are a variety of trust assessment techniques available. MANET security measures may therefore be classified as illustrated in Figure 1 into the following subcategories. The security of mobile ad-hoc networks is further enhanced by the use of machine learning. A variety of machine learning methods may be used to detect intrusions and particular attack patterns in MANETs. Nevertheless, a number of reputable techniques have been put up in the literature as a means of enhancing network security. Three particular security concerns in MANETs are addressed using ML-based approaches:

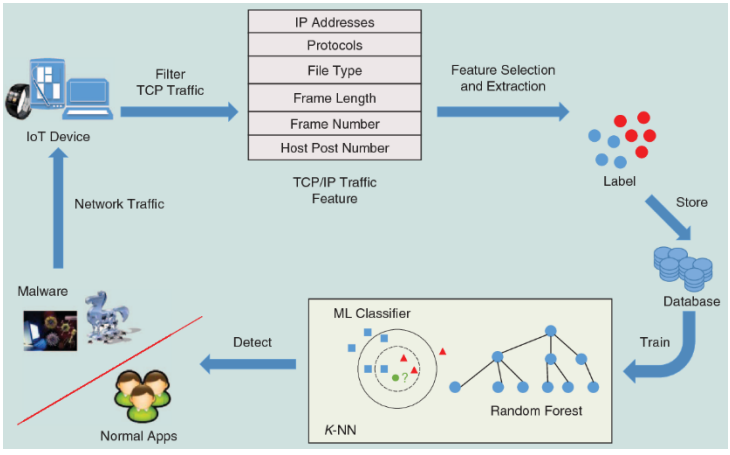


**Fig. 1:** Classification of Security Approaches in MANETs [23]

## III. MACHINE LEARNING BASED INTRUSION DETECTION SYSTEM

MANETs are equipped with an intrusion detection system (IDS) that monitors and investigates suspicious occurrences. Network problems may be detected via a variety of ways. Nodes may join and depart MANETs at any moment, making the network more exposed to a variety of threats. The primary goal of an IDS is to prevent the network from being harmed by any malicious activity. Every MANET node has an IDS as a security measure to keep out intruders. Real-world IDS implementation is complicated by the limited resources available to nodes in MANETs. There are many new dangers and vulnerabilities that may be discovered using machine learning approaches. Machine learning approaches like as fuzzy logic, genetic algorithms, Bayesian theory, and neural networks may be used to customise IDS.

Anomaly detection systems, abuse detection systems, and signature-based detection systems are all examples of IDS. It is possible to identify illegal or outlier nodes via the use of anomaly detection systems that compare the activities of nodes to the regular, usual patterns. An intrusion occurs when a node is identified to be acting abnormally. It is not possible to utilise a signature-based or abuse detection system to identify new assaults since they depend on the recorded signature or behaviour patterns. Because an intruder never follows a predetermined attack strategy, anomaly detection systems excel in terms of finding unexpected vulnerabilities, but the tradeoff is that they generate more false alarms. For researchers, ML-based IDSs have become an intriguing option for deploying various strategies that aid in minimising true negatives and false negatives in the systems and increasing security in MANETs. ML classification methods may be used to distinguish between regular and invader nodes. New IDSs based on hierarchical and distributed architectures were presented in 2003.

### 3.1 Detection of Compromised or Outlier Nodes in MANETs using Machine Learning

The difficulty of identifying and mitigating different types of assaults is a major problem inherent in the operation of MANETs. Due to the open wireless nature of the network, nodes in MANETs are very vulnerable. A number of researchers have been motivated to use cutting-edge technology to maintain their personal safety as a result of this. SVM classification method was developed as a model for flooding attack detection. Flooding attacks were used to train the SVM, and the model was evaluated in the simulated environment. However, the findings demonstrate that the model is able to correctly detect flooding attacks, but it is incapable of providing adequate results for multi-attack models. Classifying wireless network nodes by their behaviour patterns, such as message forwarding rate, fluctuating number of destinations while sending messages, etc., was emphasised in an enhanced attack classification model using KNN (K Nearest Neighbors). In spite of the implementation's accuracy, there's no way to generate data sets from it. In addition, a new model for classifying MANET nodes based on their behaviour was devised]. Nodes' packet dropping behaviour is used to classify SVM models using Ad-hoc on-demand routing protocols, according to this study. The approach's performance was assessed by determining the percentage of packets delivered, the percentage of packets modified, and the percentage of packets misrouted.

Self-organized feature maps and genetic algorithms combined into one detection method. Neutrosophic conditional variables in MANETs were defined using the SOFM's unsupervised learning capabilities. These variables and training data are used by the GA to examine the most effective rules for detecting unique attack patterns, which are then sent back into the GA. When it came to identifying assaults, the authors claimed 99.3 percent accuracy. Detection of Denial-of-Service Attacks using a unique SVM-based technique was also shown. The model's accuracy and computing time were examined by the researchers. Researchers have recently used a similar strategy that focuses on computing time in order to detect rogue nodes. Nodes were classified into normal and banned by using an ANN classification model. Despite the authors' efforts, they were only able to achieve an accuracy of 88.23% in their prediction model for detecting numerous assaults in MANETs.

## IV. BACKGROUND

Prasad and others (2022), Detection methods for harmful and non-malicious information have been suggested in this study. For the suggested intrusion detection approach to work, a dataset of mobile node activity must first be gathered. A series of steps are followed, including simulations of mobile networks with malicious nodes, feature selection, and packet-capture data collecting. For this project, intensive NS-3 simulations are conducted. Experiments reveal that the suggested strategy outperforms current systems when it comes to information categorization. Singh and Mondal (2022), In order to safeguard IoT networks, this article suggests a machine learning network-based IDS. In the proposed method, network packets are classified as either legitimate or malicious using classification algorithms. An ESP8266 wi-fi module and a Node MCU were used to train the model on a dataset of network logs from a network transferring data to a server. Arduino and Node MCU were used to monitor a network and collect data from an ultrasonic sensor. There were eight classification-based detection models examined in order to choose the best one. When compared to other classification methods, the decision tree and random forest are the most accurate models. The results section discusses and analyses the comparison of various models. Popli and colleagues (2021), In order for a computer system to be able to learn and adapt to its surroundings, machine learning (ML) methods are used. The primary objective of ML is to detect and act on complicated patterns. Mobile ad hoc networks are secured using a variety of ML methods. It is difficult to establish security mechanisms in MANETs because of the lack of an infrastructure. For MANET security, this article gives a complete and methodical investigation into numerous recent techniques. Pachhala and others (2021), Machine learning approaches for malware detection, with a focus on deep learning techniques, will be reviewed in this paper in order to help in the identification of malware. Classical machine learning workflows for malware detection and classification are described in this study, as well as the constraints and limits of traditional machine learning. The research also covers current developments and advances in the area, with a focus on deep learning techniques. Aside from these points, (iv) it focuses on issues related to current approaches and (v) analyses what the future holds for research in this area. To benefit researchers in their work, the survey findings give fresh information on malware detection and the new

advancements and directions in research being investigated by the scientific community. Zardari and his associates, for example (2021), As each node generates the main and secondary trust values to identify an attacking node by the suggestion of nearby nodes and trust metrics, this method integrates nodes' authentications and trustworthiness with the k-NN algorithm for the detection of jellyfish assaults. It is based on their behaviour that k-NN isolates the jellyfish from other genuine nodes. The hierarchical trust assessment attribute of nodes would subsequently be used to choose dependable nodes for routing packets. Network delays and throughput may be improved by avoiding jellyfish nodes, according to an experiment.

In the work of Laqtib and colleagues (2020), Inception-CNN, BLSTM, and DBN were all compared in this paper, and the goal was to provide basic guidance on the selection of deep learning models in MANET. Muratchaev and others (2020), Using clustering techniques to overcome difficulties in MANET routing networks is the focus of this essay. MANET network difficulties were examined in depth, with the prospect of fixing them using neural network clustering. A multi-criteria selection of network characteristics is used to construct specific cluster algorithm implementations for use in routing. Classical routing protocols like AODV and OLSR may make use of these methods. Mathematical models of the method and the results of implementation in current routing protocols are provided.

Using machine learning techniques, Ravi & Ramachandran (2020) suggested a resilient IDS (MLT). The power of ensembles is critical to making effective use of MLT. In this study, classifier ensembles such as Random Forest (RF), KNN, and Nave Bayes (NB) are all employed to classify data. The suggested IDS is tested and verified in a secure test environment before being implemented. The results of the experiments also show that the suggested IDS is strong enough to resist and identify any intrusions, and it is also highlighted that the proposed IDS surpasses the state-of-the-art IDS with over 95% accuracy. Eid al-Fitr and Hikal (2020), Stable and powerful classifiers may be built utilising the suggested strategy, which uses AdaBoost-SVM on a clustering technique based on the AOMDV-LEACH clustering method to balance chosen nodes' attributes. The detection accuracy and routing overhead of the suggested method are evaluated and tested. For diverse mobility situations, results demonstrate up to 97% detection accuracy in improved execution time. As wireless communication technology continues to evolve, ad-hoc networking has made tremendous strides in the last several years. Because they are a subtype of the ad hoc network, the mobile ad hoc networks face many of the same difficulties in determining a path for data transfer from one point to another. Because of this, a path that is both short and stable is proposed in the study, which is based on reinforcement learning. Throughput may be increased by reducing power consumption and transmission latency, as well as increasing the delivery ratio of packets. Validating the method's performance in the network simulator-II in terms of energy consumption, transmission latency, and packet delivery ratio reveals whether or not it is efficient.

## V. METHODS AND MATERIALS

### A. Wormhole Attack

Wormholes provide a severe security risk to MANETs. MANET routing protocols (DSR) such as AODV, OLSR, and DSR are vulnerable. Wormhole attacks are identified utilising private channels known as tunnels by at least two hostile nodes. It is at this point that the wormhole tunnel will begin to gather and transmit the data packets. A control packet is received by a malicious node on the other side of the tunnel. There is an intriguing node on the opposite end of the private channel where the packet is retransmitted locally. The private channel is the preferred method of communication between a source and a destination because it offers better metrics, such as fewer hops and a shorter transit time, than alternative routes. In most cases, the attack is carried out in two stages. In the initial stage, the wormhole nodes are interested in many routes. This is when the malicious nodes start to show up in the packets. There are several ways in which these nodes might impair the network's performance. A wormhole node may intentionally drop, change, or transfer data to an outsider for nefarious intentions. This allows for a variety of attacks, including denial-of-service attacks, eavesdropping, and development. MANET is a network. Figure 2 shows how MANET operates during a wormhole assault.

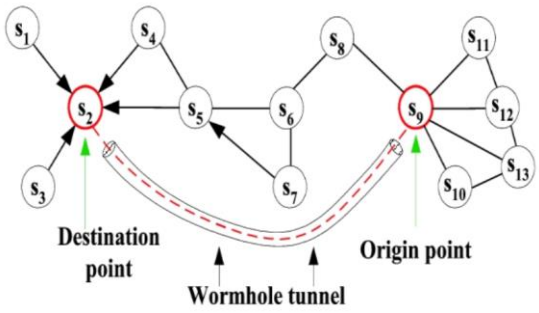


**Fig. 2:** The diagram of the wormhole attack [24]

### A. Support Vector Machine (SVM)

SVM is a kind of supervised machine learning that uses a hyperplane to classify each observation from a given dataset. SVM is better suited to big datasets since it can handle both linear and nonlinear problems. SVM is introduced to WSNs to handle a variety of difficulties, including routing, localisation, fault detection, congestion management, and communication.

### B. Nearest Neighbor (KNN)

The -nearest neighbour method is the most often used example-based strategy to solving regression and classification issues (KNN). KNN is primarily responsible for determining the distance between a given sample and the model being measured. The Hamming distance, the Euclidean distance, the Manhattan distance, and the Chebyshev distance function are all well-known distances in KNN. These metrics are lowered by detecting missing samples from the highlighted room. Data aggregation and anomaly detection are how KNN was first used in WSN applications.

### D. Deep Learning

It is a sort of machine learning with a multi-layer understanding that is part of the ANN family [69]. Detection and segmentation may be used in various research, such as transportation and routing networks, as well as health care. It also mimics the brain's communication and information processing machinery and processes data for object identification, language translation and voice recognition and decision making. For example, anomaly and fault detection, energy harvesting, data efficiency computation and routing are all handled by DL in WSNs. Detection systems, virus scanners, and spam filters have all benefited from the use of deep learning models in their development of data safety, categorization, and prediction operations. Intelligence is used in a variety of ways to provide a framework for identifying "normal" and "malicious" samples, such as assaults and regular packets. Attack planning tools are becoming more sophisticated as deep learning models expand at an exponential pace.

### E. Naïve Bayesian Learning

The mathematical method known as Bayesian learning aims to discover patterns in data by identifying conditional dependencies across a variety of statistical techniques. Bayesian learning uses prior probability curves and fresh information to estimate posterior likelihoods.

It's more likely that p() will be greater if Y1,Y2,Y3,...Yn represents a succession of inputs and returns a mark than if it doesn't. In wireless sensor networks (WSNs), Bayesian learning algorithms have addressed several issues, including routing, data localization, aggregation, and defect prediction.

### F. Decision Trees (DT)

There are several algorithms that utilise it in combination with other criteria in order to increase the readability of their output. In DT, there are two main types of trees to choose from. One is the leaf node, while the other is the decision node. DT produces a training model based on training data and predicts a class or objective based on the judgement criteria. Transparency, simplicity, and thoroughness are just a few of the benefits that decision trees provide. It's common for decision trees to be utilised in WSNs to tackle various connection and data aggregation issues, as well as mobile device management issues.

### G. Convolutional Neural Network

Most often used for deep learning and neural networks with huge datasets such as photographs and videos are the CNN (Convolutional Neural Network). Using cortical neurobiology, we've been able to create a multi-level neural network. A convolution and a fully connected layer are both included in this structure. Between these two levels, there may be subsampling layers. With the complexity of DNNs in well-scaled and multidimensionally localised input data, they obtain the best of DNNs. As a result, CNN is immediately implemented in datasets with a reasonably large number of nodes and components that need to be trained.

## VI. PROCEDURE

**Create a network of 20 nodes that are organized in a circular pattern.**
From the list of nodes, choose the source and destination nodes as well as the mobile node.
It is still necessary to use pattern recognition neural networks to reroute data from the node where packet loss has been detected so that it is received by a different node in the network.
Then, from the source node, re-start the broadcast.
Else
Use a network protocol to send data between nodes.
Determining E2E delays, PDRs & TCP/IP
When you're satisfied, repeat the test
Create an Excel Chart for the Test Results
Compile data to create an end-of-trend line.

### 6.1 Execution Process

The goal of the current investigation is to identify the PDR, E2Edelay, and throughput of packet drops in MANETs. For this experiment, we use neural networks (machine learning) to improve the probability of a packet being dropped during transmission. Because it records each communication using a memory frame, it is more accurate in detecting malicious MANET activity. The flow diagram depicting the planned work's overall execution is shown below.

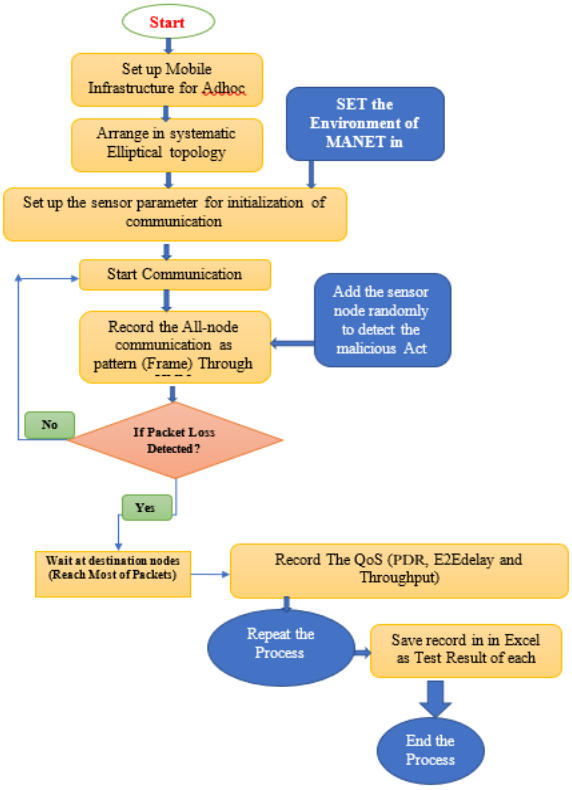


**Fig. 3:** Execution Process (Created by Researcher)

The network's common and abusive nodes need mathematical modelling. The stroke process nodes are sampled and analysed using Markov. This section examines how black hole neighbours isolate nods. Black hole nodes are possible because the hoc network is able to discover their presence.

## VII. SIMULATION & RESULT

To make better use of network resources and extend the life of your network, these practical solutions may use machine learning. As a summary, this study gives a complete literature review of machine learning algorithms from 2002 to 2018 that are used to address prevalent difficulties in Mobile Adhoc Networks (MANETs). It is determined which algorithm is most suited for the job at hand by looking at its strengths and weaknesses. Designers of MANETs might use this as a guide in creating a customised machine learning solution for their specific needs. There were comparisons made between each classifier's performance in terms of packet delivery, latency, and throughput. To make comparisons easier, we've included these criteria.

**a) Packet delivery ratio**- Each subscriber node gathers the total number of published messages from all publisher nodes for subscriber node events, and this ratio is expressed as a percentage.

The following formula may be used to figure it out:

**PDR**= ((total packets-loss)/total packets)

**b) End 2 End Delay**- The time it takes a packet to travel from its point of origin to its point of destination in a network is referred to as the packet delay.

**c) Throughput** –Packet throughput is defined as the number of packets that move across a channel in a given length of time. When there are more and more nodes in the network, this metric shows how many packets have been successfully sent from the source node to the destination node.
A network's response to an arbitrary query is equal to the number of mobile nodes (k) that are present and active at the moment the query is received, according to the formula outlined above.

The following formula may be used to figure it out:
**Throughput**=total packets/End2EndDelay

### 7.1 Proposed Methodology

The MANET must be monitored by a machine learning system, such as a Neural network. The suggested neural network might be used to keep track of unexpected shifts in the network's activity pattern. This study's primary conclusions are the latency and loss of communication packets in the proposed network. Modified neural networks that can do 3500 round computations have been incorporated into this thesis, which previously only had the capacity to perform 1000 round computations. Before, the parameter had been modified to an elliptical shaper, which had previously been circular.
The following table lists the starting values for each of the parameters.

- Assigning a frame to monitor memory allocation, nr fr=12.
- Initialize the value of packets to a range between 100 and 200.
- The number of packets transferred is set to 18 by setting Packet Trans=1.
- Inienr = 10 * 10; Set the initial energy delivered to each node to a value of 10.
- Energy is counted for each time communication is used.
- Chance of a node dropping to a dead node: 0.10%.
- At the start of the game, set the loss to zero.
- To begin, set the delay to zero.
- code for neural network: train Param.epochs = 3500. With a new value of 1,000,000, the suggested scenario may now be thoroughly tested.

It has been used in MATLAB code to perform simulations and produce estimates of PDF, E2E latency, and throughput on the command prompt. MATLAB Code might potentially be used to solve this problem. It will take a long time to calculate and self-insert the test condition, though. A different outcome may be expected from a given situation but its fundamental nature will stay the same. It's as follows, thanks to the GUI we built.

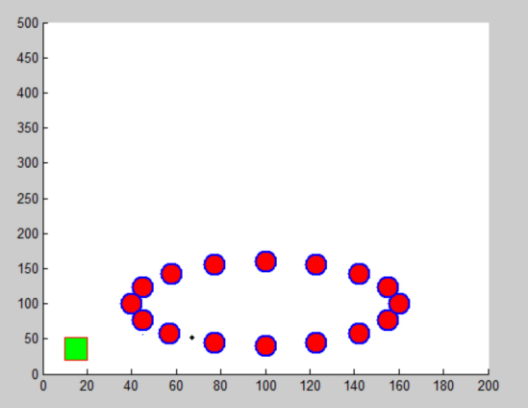


**Fig. 4:** Layout for MANET – Hopfield (MATLAB Outcome)

This is the MTALAB-2013 GUI that was built. Nodes are organised in an elliptical architecture, with two sink nodes serving as the base station nodes.

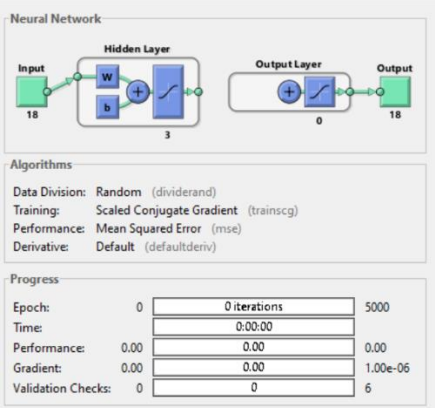


**Fig. 5:** Status of neural network (Hopfield Neural Network) **(**MATLAB Outcome)

MANET nodes and network parameters are used to build the neural network seen above. In order to determine the current state of a packet.

**Table 1: Output Parameter**

| Bn Test condition | Packet transmitted | Packet drop | PDR | E2E Delay | Through put |
|---|---|---|---|---|---|
| Test 1 | 170 | 8 | 95.5 | 0.1262 | 1346.9 |
| Test 2 | 170 | 12.6000 | 92.5882 | 0.1219 | 1394.1 |
| Test 3 | 150 | 0 | 100 | 0.0444 | 3380.2 |
| Test 4 | 190 | 21.0000 | 88.9474 | 0.1239 | 1533.5 |
| Test 5 | 200 | 10.5000 | 94.7500 | 0.0805 | 2483.7 |
| Test 6 | 150 | 0 | 100 | 0.0418 | 3587.8 |
| Test 7 | 210 | 12.6000 | 94 | 0.0885 | 2373.7 |
| Test 8 | 190 | 16.8000 | 91.1579 | 0.1193 | 1592.3 |
| Test 9 | 200 | 10.5000 | 94.7500 | 0.0793 | 2521.3 |
| Test 10 | 150 | 0 | 100 | 0.0771 | 1945.1 |
| Test 11 | 180 | 6.3000 | 96.5000 | 0.0820 | 2195.6 |
| Test 12 | 190 | 12.6000 | 93.3684 | 0.1174 | 1617.7 |
| Test 13 | 180 | 6.3000 | 6.5000 | 0.0851 | 2115.1 |
| Test 14 | 170 | 4.2000 | 97.5294 | 0.1147 | 1482.3 |
| Test 15 | 210 | 23.1000 | 89.0000 | 0.1136 | 1848.6 |

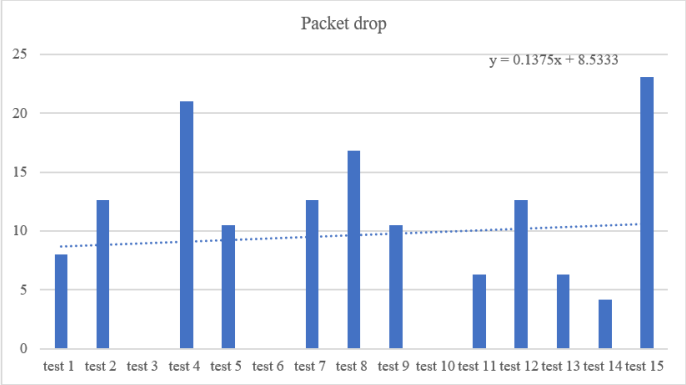


**Fig. 6:** Packet Drop (MATLAB Outcome)

To analyse packet status, we use a neural network to apply to the MANET nodes and network parameters. This results in packet drop. What are the following test cases: 8-PD, 12-6000-PD, 0-

PD, 21.0000-PD, 10-5000-PD, 6-PD, 12-6000-PD, 6.3000-PD, 12-6000-PD, 6.3000-PD, Test 14 (4.2000-PD), Test 15 (23.1000-PD).

*PD-Packet Drop

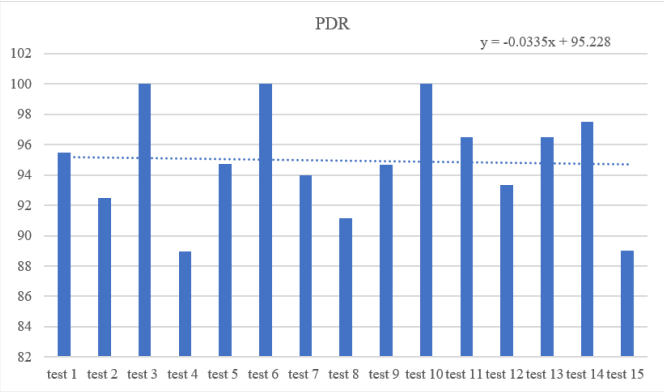


**Fig. 7**: PDR (MATLAB Outcome)

With the help of a neural network built on top of MANET nodes and network characteristics like Packet Drop Ratio (PDR), we can assess the health of individual packets in a large network. The following tests are listed: Test 1 (95.5-PDR), Test 2 (92.5882-PDR), Test 3 (100-PDR), Test 4 (88.9474-PDR), Test 5 (94.7500-PDR), Test 6 (100-PDR), Test 7 (94-PDR), Test 8 (91.1579-PDR), Test 9 (94.7500-PDR), Test 10 (100-PDR), Test 11 (96.5000-PDR), Test 12 (93.3684 (89.0000-PDR).

*PDR-Packet Drop Ratio

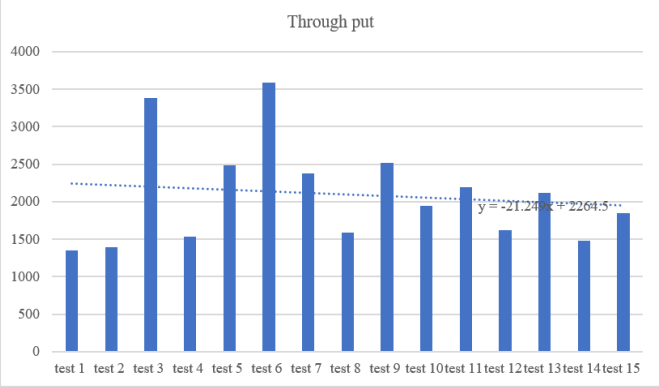


**Fig. 8:** Throughput (MATLAB Outcome)

Applying neural networks to MANET nodes and network characteristics allows us to analyse the packet status by running 15 test cases via each network node. Test 1 (1346.9-TP), Test 2 (1394.1-TP), Test 3 (3380.2-TP), Test 4 (1533.5-TP), Test 5 (2483.7-TP), Test 6 (3587.8-TP), Test 7 (2373.7-TP), Test 8 (1592.3-TP), Test 9 (2521.3-TP), Test 10 (1945.1-TP), Test 11 (1945.1-TP), Test 12 (1617.7-TP), Test 13 (2115.1-TP), Test 14 (1482.3-TP), Test 15 (3587.8-TP) (1848.6-TP).

*TP-Through Put

## VIII. CONCLUSION AND FUTURE SCOPE

MANETs are unique in that they can take any network configuration and can have any number of mobile nodes. In this post, we'll talk about a network's throughput, latency, and packet transfer rate. In order to send packets throughout the transmission process, a neural network is employed. Packet transmission speeds and throughput increase, while latency decreases. A section on resolving wireless mobile node network congestion is also included in the guide. By iterating on the iterating process, machine learning applications will be able to help reduce packet loss in the future. In this article, embedded network applications are explained in broad terms, and then the study's findings are analysed. As well as comparing and contrasting the Hopfield and back propagation neural networks in terms of their physical appearance, we reviewed the techniques used for in-network processing. The mobile node network may be expanded. A fresh context is added in the following neural network. There are two critical aspects to this discussion: how neural networks function in a mobile node network environment, and how our test implementation performed. Mobile node nodes may be used to simulate and experiment with a wider range of network topologies. The VANET scenario, which is being purposely strengthened by the usage of 5G technology, will also profit in the future from this experiment. The 5G communication platform provides a framework for the MANET mobile node and its highly dependent use in various data collection systems.

## References

1. Basagni, S., Conti, M., Giordano, S., & Stojmenovic, I. (Eds.). (2004). Mobile ad hoc networking. John Wiley & Sons.
2. Goyal, N., & Gaba, A. (2013). A new approach of location aided routing protocol using minimum bandwidth in mobile ad-hoc network. International Journal of Computer Technology and Applications, 4(4), 653.
3. Popli, R., Garg, K., & Batra, S. (2016, March). SECHAM: Secure and efficient cluster head selection algorithm for MANET. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIA Com) (pp. 1776-1779). IEEE.
4. Kamboj, P., & Goyal, N. (2015). Survey of various keys management techniques in MANET. International Journal of Emerging Research in Management & Technology, 4(6).
5. Zapata, M. G., & Asokan, N. (2002, September). Securing ad hoc routing protocols. In Proceedings of the 1st ACM workshop on Wireless security (pp. 1-10).
6. Zhou, L., & Haas, Z. J. (1999). Securing ad hoc networks. IEEE network, 13(6), 24-30.
7. Hubaux, J. P., Buttyán, L., & Capkun, S. (2001, October). The quest for security in mobile ad hoc networks. In Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing (pp. 146-155).

8. Baadache, A., & Belmehdi, A. (2012). Fighting against packet dropping mis behavior in multi-hop wireless ad hoc networks. Journal of Network and Computer Applications, 35(3), 1130-1139.
9. Karpijoki, V. (2000). Security in ad hoc networks. In Proceedings of the Helsinki University of Technology, Seminars on Network Security, Helsinki, Finland.
10. Lundberg, J. (2000). Routing security in ad hoc networks. Helsinki University of Technology, http://citeseer. nj. nec. com/400961. html.
11. Papadimitratos, P., & Haas, Z. (2002). Secure routing for mobile ad hoc networks. In Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002) (No. CONF). SCS.
12. Bandyopadhyay, A., Vuppala, S., & Choudhury, P. (2011, February). A simulation analysis of flooding attack in MANET using NS-3. In 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE) (pp. 1-5). IEEE.
13. Prasad, M., Tripathi, S., & Dahal, K. (2022). An enhanced detection system against routing attacks in mobile ad-hoc network. Wireless Networks, 1-18.
14. Mondal, B., & Singh, S. K. (2022). A Comparative Analysis of Network Intrusion Detection System for IoT Using Machine Learning. In Internet of Things and Its Applications (pp. 211-221). Springer, Singapore.
15. Popli, R., Sethi, M., Kansal, I., Garg, A., & Goyal, N. (2021, August). Machine Learning Based Security Solutions in MANETs: State of the art approaches. In Journal of Physics: Conference Series (Vol. 1950, No. 1, p. 012070). IOP Publishing.
16. Pachhala, N., Jothilakshmi, S., & Battula, B. P. (2021, October). A Comprehensive Survey on Identification of Malware Types and Malware Classification Using Machine Learning Techniques. In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 1207-1214). IEEE.
17. Zardari, Z. A., He, J., Pathan, M. S., Qureshi, S., Hussain, M. I., Razaque, F., ... & Zhu, N. (2021). Detection and prevention of Jellyfish attacks using kNN algorithm and trusted routing scheme in MANET. International Journal of Network Security, 23(1), 77-87.
18. Laqtib, S., El Yassini, K., & Hasnaoui, M. L. (2020). A technical review and comparative analysis of machine learning techniques for intrusion detection systems in MANET. International Journal of Electrical and Computer Engineering, 10(3), 2701.
19. Muratchaev, S. S., Volkov, A. S., Martynov, V. S., & Zhuravlev, I. A. (2020, January). Application of clustering methods in MANET. In 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EI Con Rus) (pp. 1711-1714). IEEE.
20. Ravi, N., & Ramachandran, G. (2020). A robust intrusion detection system using machine learning techniques for MANET. International Journal of Knowledge-based and Intelligent Engineering Systems, 24(3), 253-260.

21. Eid, M. M., & Hikal, N. A. (2020, October). Enhanced Technique for Detecting Active and Passive Black-Hole Attacks in MANET. In International Conference on Advanced Intelligent Systems and Informatics (pp. 247-260). Springer, Cham.
22. Duraipandian, M. (2019). Performance evaluation of routing algorithm for Manet based on the machine learning techniques. Journal of trends in Computer Science and Smart technology (TCSST), 1(01), 25-38.
23. Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? IEEE Signal Processing Magazine, 35, 41-49.
24. Sharma, Samiksha & Shekhawat, Hema & Pokharana, Anchal. (2018). Analysis & study of Routing protocols for Authentication of MANETs. 7.