Semiconductor Optoelectronics
ISSN: 1001-5868

DESIGN AND PERFORMANCE ASSESSMENT OF A NOVEL FRAMEWORK FOR DETECTION AND RECUPERATION AGAINST BLACKHOLE ASSAULT IN WIRELESS NETWORKS: MANET

Manmohan Sharma
Department of Computer Science and Engineering, RIMT University
Mandi Gobindgarh, India

Mohanjeet Singh
Department of Computer Science, Patel Memorial National College
Rajpura, India

Abstract— Nodes that can both transmit and receive messages are necessary for communication. Intermediary nodes may be used by nodes that are communicating with each other. Because of the continuous expansion of the communication sector, the number of communicating nodes will inevitably rise in the next years. Requirements were also taken into consideration when designing multiple types of networks, such as MANET. Increasing the scale of the network will lead to new obstacles and problems, as well as all the benefits of the network, making communication easier and more likely to take place. However, there are a slew of factors to take into account while putting together a network, including the number of nodes, type of nodes, message types supported by nodes and networks, message and packet sizes, and the presence of intermediate nodes. Any of the parameters on this list that are compromised will result in a failure, be it at the node level or at the network level. To accept a node without actually knowing its intents might lead to severe issues, such as numerous attacks on the network, such as denial-of-service attacks, Black Hole attack. Once initiated, these assaults might affect a node or the entire network, disrupting communication. A neural network is considered as adaptable to input that is changing. Neural Network is having group of algorithms that will use information for processing, implementation to get improved results. Such system is assumed as having existence of Neurons. The idea of neural networks, which has its origins in artificial intelligence, is fast gaining prominence in the development of other Application fields as well. These roots can be traced back to the early days of computer programming.

Keywords— MANET, Black Hole Attack, Neural Network, Packet Delivery Ratio

Introduction

In everyday life, there is a greater variety of options for storing portable electronic gadgets. Users are less interested in making commitments in stationary devices and more interested in using gadgets that have mobility as a feature. Because of the curiosity shown by customers, businesses are increasingly producing products that are able to quickly relocate themselves in response. The majority of recently built electronic products now come equipped with this

functionality. Because of this function, the gadget can now function without human intervention. However, the criteria for communication remains the same as before, which is that the devices need to be able to interact with one another. Communication between a series of diverse nodes is what makes up a network. These nodes might be located at a certain distance apart from one another. The following step is for these nodes to attempt to build a network in which the establishment of communication should always be feasible. It is impossible to even conceive of the possibility of data transfer between mobile nodes unless these devices make use of protocols helping in communication and algorithms those are specifically used in routing for data transfer. Without these, the connection between these devices would not be successful. The term "Mobile Adhoc Network" refers to a specific category of network in which mobile nodes actively participate and maintain communication with one another (MANET). It should come as no surprise that the modern world has a great variety of formats for data and information. This data may be presented as a picture, a textual explanation, an audio recording, or a video. There is a possibility that this is also offered in combination. This information might either be sensitive or non-sensitive, depending on the context. As a result, it is imperative that adequate protections against data breaches be put into place. However, this protection might be breached at any point when we are thinking about or concentrating on any one of the parameters [10].

Since every node in a MANET is autonomous and able to independently configure itself, this type of network is referred to as a self-configurable network [2]. A network like this does not require any kind of pre-existing infrastructure in its different forms. As a result, MANET also possesses the characteristic of not requiring infrastructure. The devices that are part of this network already have adequate amounts of the resources or components they need. Devices are able to be treated as independent nodes with the assistance of these resources as component of device, and devices are able to configure themselves in accordance with the requirements at any given moment. With such nodes, a network may be quickly and simply constructed using this method. Every single one of these nodes is intended to deliver the finest features and performance possible; but, there is always going to be a gap in either the device capabilities, the network environment circumstances, or the user requirements. This always leaves room for development [16][17][18]. As a result of all of these different factors, nodes and the network as a whole can be put at risk, and the node that ends up in charge of the network might not have good intents toward the network.

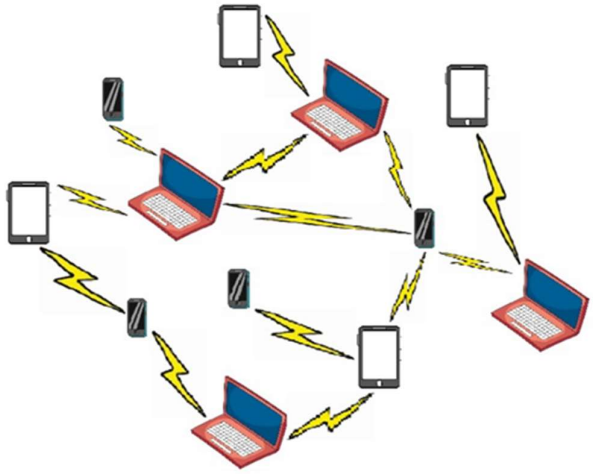

Figure1: Mobile AdHoc Network (MANET)

Since it is essential, once the network has been successfully implemented, the nodes should immediately begin communicating with one another. As a result, nodes and networks need to employ any routing protocol that enables them to interact exclusively in accordance with the guidelines established by the routing protocol, depending on the type or requirements of the nodes and networks involved. From among these three distinct sorts of routing protocols, any one might be chosen to implement. Hybrid, Reactive, and Proactive Strategies The dynamic and infrastructure-less nature of MANET and its nodes is justified by the fact that every one of the nodes that participate in MANET are welcome to walk anywhere and at any time [1].

Because the very dynamic and often unknown circumstances of its environment that are characteristic of wireless networks, the design of contemporary wireless networks, which requires decision making and the optimization of parameters, may be rather difficult. In today's contemporary networks, there is a prevalent tendency toward the incorporation of artificial intelligence (AI) approaches as a means of coping with the design complexity. The well-established artificial intelligence framework of neural networks (NNs), which are well-known for their impressive generality and versatility, has indeed been utilized in a diverse range of settings in wireless networks. While a majority of AI techniques have been used in the wireless networks community with positive results, the application of these techniques has been profitable. Specifically, NNs are becoming more popular for applications that require categorization, learning, or optimization. Therefore, it is essential to have knowledge of the various NN models as well as the applications of NNs in wireless network systems. In addition to this, it is necessary to identify the potential hazards and difficulties associated with the implementation of NNs, in particular when contemplating alternate AI models and approaches [19]. So, one need to remain active about all the latest trends to know about Computer systems, nodes, their behavior and working culture to properly understand the difference between genuine node and unauthenticated [64] or malicious node. This could further help the users and administrators to arrange them in clusters. Clusters can be formed based upon defined parameters like remaining power of node, malicious nodes and so many other parameters can also be defined [70].

Literature Review

Chavda et al. [45] proposed an approach that is characterized by the comparison procedure being executed. As per this paper, it is mentioned that abnormal difference in Sequence numbers of nodes should not be allowed and with help of such steps, high performance can be achieved. when compared to the traditional AODV protocol. This was proved by the fact that the method had a higher PDR value.

Mistry et al. [46] provides a method, in which they modified the working of the source node by introducing some new function into it. This new function included a timer, database, and Mali node id for the purpose of keeping record of everything bad. Mistry and his colleagues came up with this novel approach. When this technology is utilized, there is a subsequent rise in the amount of memory and time overhead. The operation of the source node was modified by Mistry et al. [46] that introduced a new function, which further keep record of Malicious Node ID. This is helping to detect black hole node. Such record of all malicious nodes present in network can also be maintained. These enhancements were implemented so that the source node may have a greater ability to monitor all of the malicious nodes. By using this strategy, the RREP message that is entered into the database and has the highest value of the destination sequence number is the one that is thrown away. In addition, the node that was responsible for sending the RREP will be judged to be malicious, and the identification of that node will be stored as the malicious id for the network. The improved packet delivery ratio helps to compensate for the increased strain of utilizing this technique, despite the fact that it results in a bigger memory and time cost.

After making adjustments to the conventional AODV protocol, Kaur et al. [47] proposed a modified technique as a means of detecting and guarding against black hole assaults. Due to a number of flaws in the AODV routing protocol, MANETs are susceptible to a broad variety of assaults, which may be initiated by a large number of nodes located both within and outside the network. These attacks can be launched from anywhere in the world. Through the employment of this technology, the performance of the network is improved.

Patel and Dadhaniya [48] introduced a host-based intrusion detection technique that consisted of three steps. According to their method, each node functioned as its own IDS. In this, Sequence Number of Source node and replying node both are checked to identify malicious node. The findings of the simulations that were carried out in order to compile this article revealed that there was an increase not just in the PDR but also in the average throughput.

Deng et al. [49] presented an approach as a possible solution to the problem posed by the Black Hole Attack. When utilizing this approach, in addition to the RREP message, information on the neighbor of the node that is answering is also asked. After receiving RREP, Source is not believing RREP message but is sending another message to confirm the Path now. In case, node found not reliable then it is considered as malicious, so ignored to get selected for message sharing. In addition to this, it presupposed that nodes associated with black holes could not communicate with one another.

In their research work titled [50] Raj and Swadas presented a method for locating black hole nodes known as DPRAODV. This technique makes use of the RREP sequence number in conjunction with a threshold value. This RREP sequence number is compared and if found larger than the threshold value, then this node could be considered as malicious, And ALARM will be generated for every other node.

Neha et al. [51] provided a comparison analysis of the work that has been done in Mobile Adhoc Network and the work that is still necessary to be done. After doing research on a variety of approaches, a table-based summary of the findings was made available.

Neha et al. [52] introduced a Step Verification Algorithm that may be used in MANET and focused to find and isolate Black Hole attacks. At multiple steps the verification was performed in an attempt to reach to malicious node, and also maintained record of it accordingly.

Farahani G. [53] discussed about Black Hole Attack Detection in Mobile Ad Hoc Networks Using the K-Nearest Neighbor Algorithm and Reputation Calculation. Here, A black hole attack may be recognized by the anomaly-based intrusion detection system (IDS) because to its use of KNN clustering and fuzzy inference to choose cluster heads. Additionally, certain techniques like beta distribution and Josang mental logic would be utilized in order to compute the trust level of each individual node. Communications using unicast, multicast, and broadcast protocols are all supported by AODV. In the event that the path link is severed, this protocol is able to restore the route on the local level. The AODV protocol is able to accommodate a large number of nodes those are available in the defined network. This protocol could help in departing or joining of nodes in the network in any arbitrary fashion. When a viable path to the destination cannot be found between the source node and the destination, the protocol's path discovery procedure is activated. The following four messages are sent with one another throughout the routing process:

(i) RREQ (ii) RREP (iii) Route error (RERR) (iv) Route reply acknowledgment (RREP-ACK)

The RREQ message will be generated in order to build a route from the source to the destination, and the route will be found in the network using the flood approach. Following the completion of the phase involving the submission of the routing request packet, the RREP is then transmitted from the destination node in the forward direction to the source node. Proposed methodology here in this paper is using KNN for Node clustering. Fuzzy system is used for rules definition, calculating trust of nodes, etc. Scope is still there to find out other types of attacks, improving the performance parameters results.

Dhaliwal B.K. et.al [54] in the work has presented a routing protocol that in itself is considered as having features like Security and energy efficiency. Name of model is considered as: SEETA-IoT [55].

A neighbourhood-based technique was suggested by B. Sun et al. in 2003 [57] as a way to determine whether or not a blackhole attack is present, and a route recovery protocol was provided as a way to establish a valid path to the actual destination. When compared to other approaches that solely rely on cryptography-based authentication, this method has the amazing benefit that the number of encryption and decryption operations for authentication is drastically reduced. As a result, a significant amount of system resources may be saved.

S. Ramaswamy et al. published a proposal for an algorithm in 2003[58] that aimed to combat co-operative black hole assaults in ad hoc networks. This technique is unable to defend against grey hole attacks since it is predicated on a trust connection between the nodes in the network. Even when there is no threat to the network, the algorithm takes longer to finish since it involves extensive cross-checking.

G. Wahane et al. 2014 [59] made a suggestion for modifying the Ad Hoc on Demand Distance Vector Routing Protocol. According to this, a proper record of routing information alongwith Node cross verification must be performed. This can be accomplished by using the protocol to

identify multiple blackhole nodes within the MANET.

An Artificial Neural Network (ANN)-based automated Black Hole node identification strategy was proposed by A. Mitra et al. in 2013[60]. The nature of the proposed ANN-based system is one that is dynamic. Because it functions on both the CRC side and the TTR side, the implemented intercommunication mechanism for detecting the presence of a Black Hole node helps to update the routing table in a more dynamic manner. This is because it is implemented at both ends.

M. Shurman et al. 2004[61] published their findings and presented two distinct solutions to the black hole attack. The first approach is for the sender node to make use of the redundancy that the network provides in order to validate the identity of the node that is responsible for initiating the RREP packet. The goal of this proposed approach is to identify many paths leading to the intended destination. The second possible approach is to record in the database both the most recent sequence number of a packet that was sent and the most recent sequence number of a packet that was received. Every time a new packet is received or sent, an update is made to here. When one node receives a reply from another node, the first thing it does is verify the most recent sequence number that was transmitted and received. If there is even the slightest inconsistency, an ALARM will sound, which will signal the presence of a black hole node. This solution is not only quicker and more reliable, but it also does not require any overhead.

Gerhards et al. In their study published in 2007[62] developed a centralized method that makes use of topological graphs to locate nodes that are attempting to produce a black hole. For the purpose of performing plausibility checks on the routing information that is propagated by the nodes in a network, well-established methods are utilized to gather knowledge about the network topology. This knowledge is then used in conjunction with the acquired knowledge to execute the checks. Malicious behavior on the part of a node is indicated when it produces false routing information. As a result, an alert will be triggered in the event that the plausibility check is unsuccessful. Using this method, it is feasible to already identify the effort to generate a black hole before the actual impact happens. This is a significant advantage over other methods.

A technique based on fuzzy logic was presented by Poonam Yadav et al. in 2012[63] in order to determine whether or not a node has been affected by a black hole assault. The presented research offers a solution to the problem of packet loss in the event that a blackhole attack is launched against the network.

In the first step, a fuzzy rule is applied in order to locate the blackhole node. On the basis of the response time of the node's communication, the fuzzy rule is implemented. The data that would normally be sent on this node will instead be passed on to it from the nodes that are surrounding it. This node will only handle the transmissions that are specifically directed to it.

The clustering technique was presented by A. Afsharfarnia and A. Karimi [67] as a method for reducing the amount of energy that is used in MANET. In this study, the weight of each node was determined by calculating a number of different parameters, such as the degree of sharing in the neighborhood, the speed of a particular link, and its energy.

The clustering-based approach for enhancing the lifespan of the network was reported by R. Kumar et al. [68]. The dynamic creation of clustering has been done by after checking the battery power, mobility, and from the serve time in order to extend the lifespan of MANET. This was done for the purpose of prolonging the lifetime of MANET.

The authors M. Singhet al. [69] presented the research of several cluster head algorithms for

MANET, the purpose of which was to lower the amount of energy that was consumed, boost the network's level of security, and lengthen the network's lifetime. The selection of the cluster head may be done using one of two approaches: the first is called distance constrained selection, and the second is called size constrained selection. The greatest energy level is the criterion that nodes use to choose the cluster head.

related work

Communication could be Wired [23] or Wireless like WSNs, MANET, CRNs [24]. Many researchers had already started applying their knowledge to work in area of Adhoc Networks, Artificial Intelligence, Machine Learning, Attacks and still regularly research is being updated. Each individual piece of study offered their own thoughts and approaches in relation to these Adhoc networks. Every piece of research must have specific criteria in order to present its own particular set of qualities. For the purpose of this review, having a substantial understanding of metrics is essential. Because Adhoc networks have self-configuring feature, so nodes are itself responsible for configuring the network, to maintain the network and its node those are part of it, proper communication, and ensuring the proper delivery of packets to their respective end nodes. When absolutely necessary, ad hoc networks will also sometimes accept assistance from an intermediary node. This is often done when the sender node and the destination node are not in immediate range of each other. At that time, the Sender node looks for engagement from the Destination node in order to ensure that the packet is delivered to its desired location without any more work being required. When this occurs, the sender does not need to contact any intermediary nodes in order for the packet to be delivered to its destination since the destination is already within its range. Sender has a more in-depth familiarity with the destination node and practically all of the necessary background information on the destination node at this time. Therefore, communication might be formed in a more straightforward manner by significantly involving fewer intermediary nodes. In terms of both its formation and its communication, the complexity of the network is increased by all of these processes and involvements. Each piece of study is conducted with the intention of resolving issues like these and developing a process that is sound from every conceivable angle. The level of problems can also be reduced through the development of a new methodology at each and every opportunity. Every approach has a number of benefits as well as some drawbacks. When the technique is examined based on specified performance criteria, only then will these benefits and drawbacks become apparent. A literature review was carried out on a few research articles that gave their approach in an ad hoc network, and an evaluation of the given methodology was carried out on performance metrics such as end-to-end delay, throughput, packet delivery ratio, jitter, energy consumption, and so on. There were a few factors that seemed to be almost identical to one another in nature, such as the Packet Delivery Ratio and the Packet Delivery Rate. Although these factors might potentially provide a variety of outcome values, they are all connected in some way to the process of delivering packets to their intended locations. In a manner similar to this, a few additional parameters might also be included, each of which could be connected to the others in the process of generating result values.

The potential of computers to solve problems has generally been limited to the circumstances in which the answer can be explicitly coded, despite the fact that computers are frequently used in some capacity that involves problem solving. When it comes to wireless networks, there are a lot of issues for which standard programming approaches do not give solutions that are either

optimum or generalizable. For instance, it is very challenging to build algorithms that might enable cognitive radios for learning and adaption, or that could forecast user movement in order to maximise the resources of a wireless network.

Wireless networks come with their own special set of difficulties and security requirements. These problems are the result of the features of wireless networks [51]:

Wireless networks, on the other hand, is not having any common defence lines to safeguard its users in the same way that wired networks do. In order for an attacker to target any node from any direction, it is not required for the attacker to have direct physical access to the link.

- Because mobile nodes in a wireless network tend to move about quite a bit, especially in larger networks, it can be difficult to maintain track of all of the nodes in the network.
- In wireless networks, one can never promise centralised and integrated structure, like router. As a consequence of this, their methods to network security are frequently decentralised, distributed, and dependent on the joint efforts of all network nodes.
- Nodes itself have to play the role of routers to transfer packets, so packet might need to travel through multiple hops. Because of this, it is hard to place one hundred percent of one's reliance in any given node to carry out a duty such as routing.

The lack of a predetermined topology and the limited access that wireless networks have to resources like as energy, processors, and memory are two additional fundamental factors that contribute to the development of security problems in the system.

In recent years, this form of network, known as ad hoc networks, has gained a lot of relevance in particular application areas, such as civilian and military activities, among other things. Because of the nature of some aspects of ad hoc networks, an adversary has a number of opportunities to create disturbances inside these networks. All of these characteristics come together to form the characteristics of a decentralised network. The MANET has a number of features, all of which are listed below, each of which contributes to the complexity of its operation [53][56]:

Because of the large distance that separates them, it is difficult for two nodes to have direct contact with one another. As a consequence of this, the nodes are considered that are employed to transfer the packets from their point of origin to the location that will serve as their ultimate destination. Such nodes in this network are considered as intermediate nodes.

When employing nodes, it is not required to have a central administrator since the nodes may arrange the operations of the internal network on their own.

Nodes have In the same way that there is a limited amount of energy level and there is also a limited number of resources, all of which are shared with other types of electronic equipment.

- MANET allows contribution from a broad diversity of wireless devices, which may join the network and start sharing data as soon as they do so. The term "heterogeneity" is used to describe this characteristic.
- There are no limitations placed on the ability of a node to enter or leave the network. As a direct consequence of this, there is no predetermined benchmark for the quantity of nodes that ought to be existing in a MANET.
- Mobile nodes have a shorter lifespan for their batteries than fixed nodes because they are wireless devices.

- Individual nodes in a network with a dynamic topology are given the freedom to join or leave the network at will. The upkeep of the network is difficult as a direct result of this, and route discovery must also be carried out several times, which means repeatedly.

The development of artificial intelligence (AI) and machine learning (ML) is helping the society and continuously making it more possible for computers to circumvent this limiting limitation by opening the door to inference and the making of complicated decisions. This overview study concentrate on Artificial Neural Networks (ANNs), also known as Neural Networks (NNs) [40][3], which are one of the most often used machine learning models in the existing body of academic research. ANNs are made up of artificial 'neurons' that are linked to one another in a structure that attempts to emulate the neural processing (organisation and learning) of biological neurons and the behaviour of real neurons.

NNs are designed to function in a manner that is analogous to that of the human brain's learning system, which is composed of a vast number of organic neurons coupled in networks that are responsible for regulating all aspects of human behaviour. ANNs are complex systems that are formed by a network of nodes that are referred to as artificial neurons. This network is patterned after the human brain. Different sorts of NN models may be created depending on how these nodes are arranged and how they are linked to one another. In a general sense, machine learning systems may be broken down into three distinct types of learning systems, which are as follows: Supervised learning; Unsupervised learning; and Reinforcement learning. Using these learning algorithms, NNs are able to make predictions about outputs based on a set of inputs that are provided [19][65].

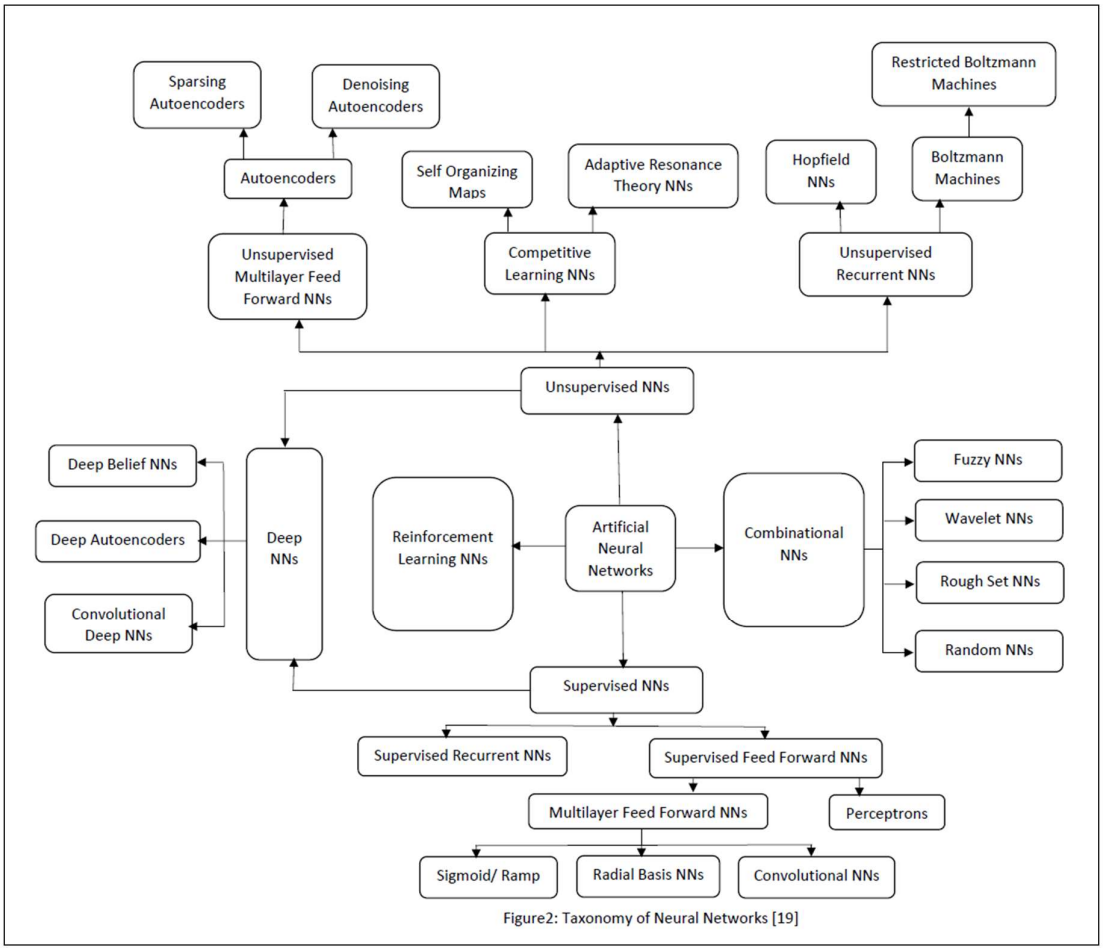

Figure2: Taxonomy of Neural Networks [19]

TAXONOMY OF NEURAL NETWORKS

Different machine learning methods alongwith NN models exist that utilizes the learning methodologies which are important for them. These NNs and its relationships can be checked in Figure 2 [19].

Supervised Neural Networks

The majority of the time, supervised learning-based neural network models are used for classification issues. Feed- Forward Neural Networks (FFNNs) and Recurrent Neural Networks (RNNs) are the two primary NN models (RNNs).

Tsagakaris et al. [26], who have employed unsupervised SOM NNs for bit rate prediction, have shown that supervised neural networks have limits when it comes to learning inside CRs.

Feed-Forward NNs:

Among all varieties of NNs, feed-forward neural networks (FFNNs) are by far the most common. They are made up of neurons that are stacked in layers over their whole. Through the use of weighted connections, every neuron in one layer is linked to each and every neuron in the layer behind it. Because every neuron in the network, from the input layer all the way up to the output layer, conforms to this pattern, the final network is one in which "neurons feed their values in the forward direction."

Perceptrons:

FFNNs were first shown as Singlelayer perceptrons [41] when they were originally introduced.

In the 1960s, the first artificial neural networks (ANNs) were developed. The input nodes of the perceptron network are different characteristics or aspects of the data that are being read in. Take, for instance, the scenario in which we want to model and forecast the productivity of an AND gate. In this scenario, the values that are supplied into the AND gate serve as the features that are utilized as inputs by the perceptron network. After calculating an overall value and comparing it to a threshold, which is determined by comparing the overall value to the weighted sum of all of these feature nodes, If the value that was computed is higher than the threshold, then the output of the perceptron for the information that was provided is considered to be positive. A negative reading is assigned to the input if it is determined that the value is lower than the threshold.

Multi-Layer Feed-Forward NNs:

On either hand, multi-layer feedforward NNs, also known as ML-FFNN, are much more expressive and have the ability to represent non-linear functions while increasing generalisation. In contrast to perceptrons, ML-FFNNs are made up of many layers. Between the input and output layers, these networks include extra neural layers for processing information [19]. The ability of these NNs to tackle complicated issues is down to these hidden layers. On the other hand, it might be challenging to understand the functioning and purpose of these hidden levels. Multi-Layer Feed-Forward NNs is also used in various methodologies to improve the systems like Mobile Robot Obstacle Avoidance system [42].

Recurrent NNs:

Modeling and forecasting sequential data calls for a methodology that is distinct from the conventional regression or classification techniques. Fortunately, there is a distinct category of Neural Networks known as Recurrent Neural Networks (RNNs) that are particularly intended for the task at hand. [30][19]

Unsupervised Neural Networks

The term "unsupervised learning" refers to the process by which a network may learn to represent certain input designs in a manner that reproduces the numerical arrangement of the whole collection of input designs or patterns. Unsupervised learning techniques, such as clustering, are often used in this process, which divides the photographs into two distinct groups or sets according to certain intrinsic characteristics of the pictures, such as colour, size, etc [43].

When it comes to the task of initialising SOMs, one might employ methods. However, the performance of random initialised weights is superior than that of Principal Component Analysis [27].

Competitive Learning:

An approach to unsupervised learning in which the output nodes of the network compete with one another to provide the highest possible value for a given function. The neuron that was determined to have the highest value for such a function was selected as the winner, and its weights were modified in such a way that they "moved closer to the input pattern." The weights assigned to the remaining neurons have not been altered in any way.

Unsupervised ML-FFNNs (Autoencoders):

Autoencoders are a kind of ML-FFNN that differ in that, inside the output layer, the neural networks attempt to recreate the input data. These autoencoders seek, inside the hidden layers of these ML-FFNNs, to discover representations of the inputs that they were given. A high

number of neurons are used in the hidden layer by the Sparse Autoencoder and the Denoising Autoencoder, both of which are variations of the autoencoder [5].

Unsupervised Recurrent NNs:

In contrast to RNNs, Unsupervised RNNs (URNNs) represent systems as 'energy functions' by using methodologies that do not need human supervision. Hopfield Networks and Boltzmann Machines are the two most common types of unsupervised recurrent neural networks (URNNs).

Reinforcement Learning and NNs

The field of Reinforcement Learning (RL) focuses on controlling the behaviour of agents operating within an environment. Each transition in the environment leads to a reward, the nature of which is determined by a numeral of factors including the previous state, the action chosen, and the next state transitioned to. Agents in the environment make decisions that move them from one state to another in accordance with the rules of the environment.

The primary objective is to make decisions that will, in the long term, provide the greatest possible profits. RL has access to a wide variety of tools, one of which is neural networks (NNs), which may be utilised to enhance the performance of the latter. RL encompasses a very large area.

Combinational NN Models

In most cases, these models improve upon existing systems by combining NNs with several additional mathematical models. Examples of such NNs are 1. Fuzzy NNs, 2. Rough Set NNs, 3. Wavelet NNs, and 4. Random NNs.

Deep NNs

For the purpose of tackling classification tasks like numeric digit recognition, ML-FFNNs with just a few hidden layers (between one and three hidden neural layers) are optimal. These shallow neural networks are not strong enough for more intricate classification issues since they struggle to discover characteristics that might give variances within input. This makes it difficult for them to classify data. Deep neural networks, also known as DNNs, are more successful than traditional NNs when applied to issues of such complicated categorization. DNNs have the potential to have superior feature representation in a distributed way when they have numerous hidden neural layers. This indicates that every buried neural layer offers a distinct representation of the features being considered.

The majority of applications for deep neural networks, also known as DNNs, are in the image processing [28] and voice recognition [29] fields. Learning representations of data is the key to the success of the machine learning (ML) approach known as deep learning, which is used by DNNs [34][35].

An intelligent network framework known as Cognition Based Networks (COBNET) has already been proposed. The goal of this framework is to construct network-wide, cross-layer internal representations of various network parameters by leveraging breakthroughs in DNNs [39].

The pretraining phase is approached in a variety of ways depending on the specific DNN. DNNs may take many forms, but some examples include autoencoders, deep belief networks, and convolutional neural networks. DNNs are less prone to the issue of overfitting than other types of neural networks because unsupervised learning makes it possible for them to construct generalised feature representations of their hidden layers in a compact form.

During the course of the last decade and few years, several strategies have been developed as a means of addressing the difficulties brought forth by backpropagation on deeper networks [37]. The advancement of computer technology has made it possible to train DNNs more effectively. When combined with the recent increases in the performance of graphics processing units (GPUs), deep neural networks (DNNs) have been delivering performance levels that have never been seen before in a wide variety of contexts.

NEURAL NETWORKS IN WIRELESS NETWORKS

Neural Networks can be deployment in Wireless Networks [7] and this deployment within Wireless Networks of different types [8][20] is helping in multiple applications [33] to get benefitted in Localization [30][31], QoS Routing, Load Balancing [6], Improved Security [25], Quality of Experience [32][38]. For this, as the multiple NN models are available so those different type of NN can help in this depending upon the requirement.

Because the nodes that are involved are mobile, the routing protocols really have to speed up the methods that they use in order to maintain the network in a resilient condition. The artificial neural network, in combination with fuzzy logic and genetic algorithms [66], is what the study employs to solve this challenge [21]. By turning this data to fuzzy logic, we are able to account for the natural imprecision that exists in distance and position for mobile nodes, as well as traffic density.

Despite the fact that NNs are able to represent complicated non-linear situations, they are not without their share of flaws. The fact that neural networks are a "black box" method that does not provide any domain-specific insights into the model [22] or network that has been constructed is one of the most common and significant objections levelled against them. In practical applications, one would likely want modelling approaches that will offer insight into how the characteristics are associated with the goal function.

There is also the possibility that NN will result in an overfit to the data. This has been referred to be one of the most common criticisms levelled against NNs [44]. Having said that, it is essential to highlight the fact that every single statistical modelling technique has this issue. Providing more training data and ensuring that it is an accurate representation of the test set is a basic approach that can be taken to mitigate the effects of overfitting. On the other hand, such a luxury does not always exist in actual reality. In these kinds of situations, complex networks have the potential to overfit the data by exaggerating the modelling of noise as correlations in the data, which, in the long run, limits the accuracy of generalization. There are many different ways to avoid overfitting, some of which include restricting the training as soon as the validation error continues to worsen on the test set or utilizing regularization techniques that penalize the model when it emphasizes noise as correlations while it is being trained [36]. Both of these methods are examples of overfitting prevention strategies. In artificial neural networks (ANNs), empirical risk minimization is used, whereas support vector machines (SVMs) utilize structural risk minimization; as a result, SVMs are less likely to overfit the data. Because of these factors, SVMs are also quite significant, and for certain wireless applications, they could even be more suitable than NNs.

PROPOSED METHODOLOGY

In this Section, detailed discussion is included regarding proposed methodology which will help to have idea about the process.

For making this methodology, there were a number of points that was required to kept in mind,

because it is not only about transfer of information. There are so many other things also required that also expects good result alongwith successful data transfer. While designing this methodology, it was expected that data transfer should occur between Source Node and Destination Node successfully, but this all should happened without the effect of malicious i.e. unauthorized node. So, it became very important to recognize and identify the malicious nodes. Malicious nodes are entering into the network with wrong intentions i.e. to disturb the working environment of network. These malicious nodes might not directly present that they are going to initiate any attack and may start the communication with Source node like a normal node does. Therefore, while designing this methodology it was focused that Black Hole attack affect must be minimized and successful data transfer results should be there with some improvements in comparison to scenarios under attack. This methodology is having the capability to learn and train the dataset from its own experience to take better decisions.

Step1: Start with RREQ Message
Step2: Note down the Current_Time (CT) of RREQ when it is sent. [Keep record of all such entries, when RREQ is sent in a table having name i.e. RREQ_CT]
Step3: Wait for RREP to come and Get the waiting time in which RREP are coming.
Step4: Maintain Tables that should store the values of Running_Time (RT) and Waiting_Time (WT). [This may further help administrator/operator to do analysis about correctness of logic/ condition/ formula defined in Step5.]
Step5: While (Running_Time <= Waiting_Time)
Allow RREP to come and start accepting it.
[This proposed methodology is capable to perform verification of received RREP messages by multi-step verification.]
5.1: Start checking RREP in Mal_Table with Node_ID.
If Node_ID is available/found in Mal_Table
Then Reject RREP
Else
Move ahead from Step 5.2.
5.2: Source will ask and collect a confirmation from the trustful node about the node who has replied for RREQ to confirm a valid and trustful path through RREP node.
For this, the below procedure will be followed:
(i): Source will ask about the data regarding Node_ID about neighbour node of the RREP node alongwith reply of RREQ messages.
(ii): Check for the existence of neighbour node in Neighbour_Table.
(iii): If Node_ID exists in Neighbour_Table
Then move ahead with Step (iv)
Else
Reject RREP [As node was claiming to have Neighbour rights]
(iv): Check for the existence and details of Neighbour node in Trust_Table.
(v): If RREP Neighbours Node_ID found in Trust_Table
Then move ahead with Step (vi)
Else
Go to Step (vii.c)
(vi): Check Trust_Value from Trust_Table of RREP Neighbour Node_ID.
(vii): If (Trust_Value == 0) or (Trust_Value == 1)
Then GoTo Step (vii.b)
Elseif (Trust_Value == 2)
Then GoTo Neighbour_Table to check Neighbour Node_ID of this Neighbour Node.
[This includes another level of confirmation about Node_ID.]

(vii.a): If Neighbour Node_ID exists in Neighbour_Table
Then GoTo Trust_Table in Step (vii.a.i)
Else
Reject the information that claims of having neighbour connect.
(vii.a.i): If (Trust_Value == 0) or (Trust_Value == 1)
Then GoTo Step (vii.b)
Else
GoTo Neighbour_Table again to check Neighbour Node_ID of this Neighbour Node and Perform Steps (vii), (vii.a), (vii.a.i) as and when required.

(vii.b): Select the originator Neighbour node from the Trust_Table that is holding minimum Drop Value.

(vii.c): Move for identification of Trustful node.

(i): Generate a fake Destination message and allow Source to send this message to all the neighbour nodes of RREP. This is done to check whether the node is malicious or not.

(ii): Ask Source node to send a fake Destination Message.

(iii): Check Flag_Value in DR_Table.

If Flag_Value == 0; even after transmission of fake destination message

Then node drops this fake destination message which means that it is a malicious node; not a trustful node.

So, Store Node_ID and Seq_No in Mal_Table and also Discard RREP.

Else

Node Flag_Value will update and Flag_Value == 1

This means that node is not a malicious node; but a Trustful_Node. Therefore, Store it in Trust_Table.

(viii): Upon after selection of trustful node, there will be need to confirm and check whether RREP node has path to destination or not.

If Trustful Node confirms the path through RREP

Then Move ahead to check Drop_Ratio of RREP via Trust_Table.

If RREP Drop_Ratio > Threshold Value

Then Store Node_ID and Seq_No in Mal_Table with Doubt Flag as ACTIVE and Update Counter value for RREP Mal_Table of this node.

While Counter < Max_Number of Attempts

Do Select RREP

Else Select RREP.

Else Discard RREP after storing Node_ID and Seq_No in Mal_Table.

Step6: For Running_Time > Waiting_Time;
Stop accepting RREP for RREQ message to store in RREP_Table.

Step7: Start reading RREP_Table and Select a Seq_No from this table.
While
RREP_Table is not reached to its end
Do
Perform Multi-Step verification
(7.1): Select one Seq_No and start comparing with other Seq_No in RREP_Table
If the Seq_No is too HIGH
Then it is expected that Node_ID and Seq_No is Doubtful,
But visit Step (7.2) before discarding this entry from Table.
(7.2): Check Packet Loss Ratio of this node.
If Node_PLR > Expected_PLR
Then Store Node_ID in Mal_Table.

Else

Keep the Node_ID in RREP_Table only

Step8: Once all Seq_No are traced and verified in RREP_Table, Select the highest Seq_No from RREP_Table.

Step9: Check Battery Power of this selected node.

If Current_Battery_Power (C_B_P) >= Expected_Battery_Power (E_B_P)

Then Select the node

And GoTo Step10

Else

Follow the above mentioned steps to find suitable Node with required Battery Power

Step10: Start sending and transmitting the packets through selected node and path.

Step11: Delete the entries from RREP_Table and keep it updated accordingly.

.

RESULTS

This section includes the results found by using this proposed methodology. As it can be seen that multi step verification has been used here in this methodology, so it was expected that result will definitely improve and help the network to move toward improvement. A high success ratio will be there to find malicious nodes those were affecting the network performance. Below given are the results for parameters.

In all these instances, it was tried to find that maximum number of packets should reach to Destination node that Source node intends to transfer. As it is a Mobile Adhoc Network so nodes count can increase or decrease and accordingly network size will update and updates in other factors can also be seen. While finding the result, this network is observed with different multiple scenarios like on the basis of Number of nodes. All these mentioned parameters are checked even when the number of nodes are also changing like finding Throughput for number of nodes: 20, 40, 60, 80, so on and etc.

Throughput: It can be seen as the total number of received packets in a particular time. In this case, this time could be considered as Simulation Time.

$$Throughput = \frac{Total\ Number\ of\ Received\ Packets}{Time}$$

As in the network, User i.e. Destination node is always concerned about the total count of packets those are received. While performing every research, major focus is to increase this count so that Performance of Network can be increased. Figure3 shows the results of throughput. In this figure, it can be seen that Throughput is calculated for different set of nodes, and accordingly variation in Throughput can also be seen.

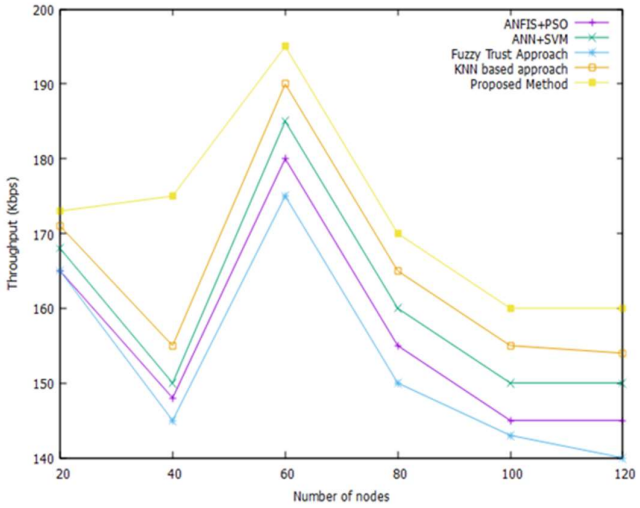

Figure 3: Throughput

Packet Delivery Ratio: In this case, there will be need to consider the total number of received packets and the total number of transmitted packets, as well.

$$PDR\ (\%) = \frac{Total\ count\ of\ Received\ Packets}{Total\ count\ of\ Transmitted\ Packets}\ X\ 100$$

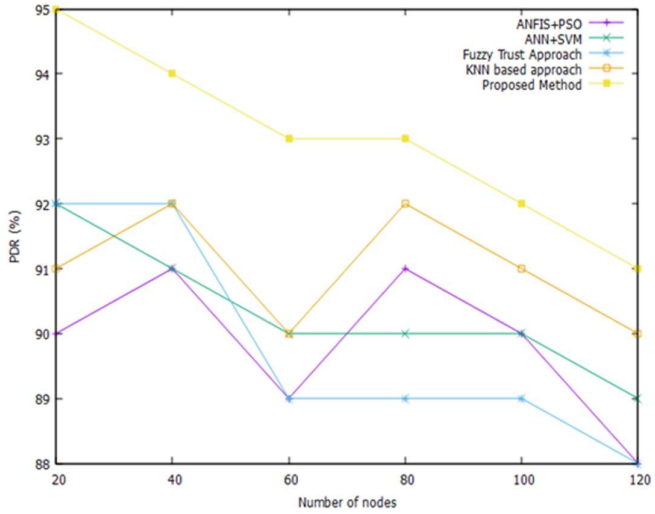

Figure 4: Packet Delivery Ratio (PDR)

Figure4 shows the result of Packet Delivery Ratio. It can be checked from the figure that, with proposed methodology, the greater number of packets can be delivered to Destination. In case there will be improvement in number of packets those reach the Destination node then this will also improve performance overall.

Packet Loss ratio (PLR): For this parameter, it is always expected that the minimum number of packets should be lost. Whatever is the methodology / way / route is being used for transmission of packets, but always maximum number of packets must be successfully transmitted between Source node and Destination node. In case, the packets will be lost again and again then sometimes there might be the possibility of retransfer that information but this cannot be expected everytime and in all the situations. Therefore, there should be a proper

solution that should help the nodes to transfer the packets without any major loss of packets. As it is clear that practically it is impossible to have a 100% efficient network, but atleast it should be tried to minimize this Packet Loss Ratio.

$$PLR\ (\%) = \frac{TNTP - TNRP}{TNTP}\ X\ 100$$

Whereas $TNTP$: $Total\ Number\ of\ Transmitted\ Packets$
TNRP: $Total\ Number\ of\ Received\ Packets$

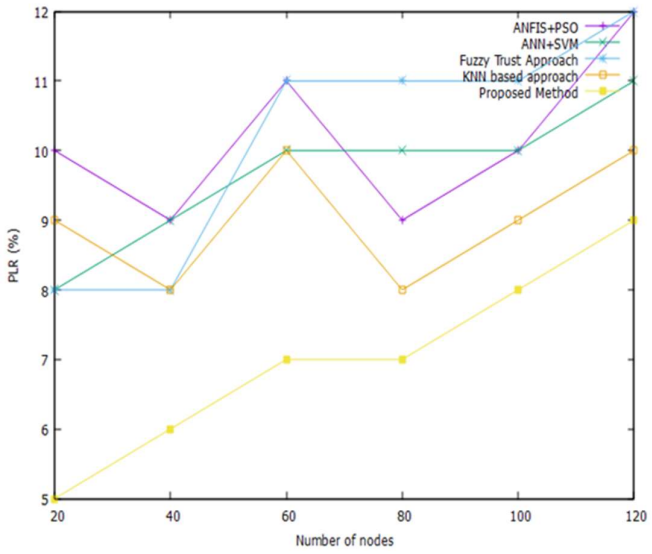

Figure 5: Packet Loss Ratio (PLR)

As the number of nodes are increasing in the network, then it is obvious that these nodes will start participating in communication either directly or indirectly, which means to say that Source is having direct connection with Destination node or Source node is having indirect connection with Destination node. In this later case, Source node will confirm about intermediate node(s) and may take help of these intermediate node(s).

Normalized Routing Load (NRL): This can be calculated based upon the details about the total number of routing packets transmitted per the number of data packets delivered at destination. The equation of calculating NRL can be seen below:

$$NRL\ = \frac{Number\ of\ Transmitted\ Routing\ Packets}{Number\ of\ Delivered\ Data\ Packets}$$

Figure 6 is showing the result of Normalized Routing Load. While doing research, this should also be kept in mind carefully that Load of packets, routes, nodes, etc. should not affect the performance. Methodology must be well organized so that setting up routes should not become a major trouble. There is no doubt that finding appropriate route is also a challenging task, but it must also be a focused area while performing any research, because this will also directly impact the network performance.

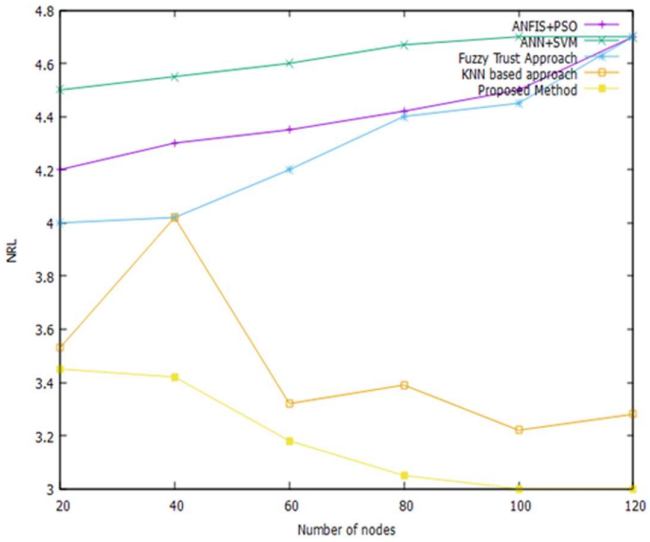

Figure 6: Normalized Routing Load (NRL)

In this figure, Normalized Routing Load is also calculated for proposed methodology and previous methodologies as well to check the difference clearly.

As per proposed methodology, it can be checked that data is also being collected and maintained. Thenafter this collected data is helping the proposed methodology to work properly and efficiently. This process of collecting data, building Dataset, training the data and then finally using that data for future purposes like taking decisions that support performance improvements, etc. are almost similar to Neural Network characteristics.

Conclusion and Future Work

There may be some categories of Wireless networks but it is important to check the actual requirement and working of the network and its nodes. While looking or developing the techniques it should be focused that metrics representing performance of nodes and network, etc. for the transmission of packets must be as per requirement and properly set. The ability to monitor and evaluate an ad hoc network will be much improved as a result of this. Analysis, in the sense of making comparisons between different networks and the protocols that are utilized in a network, may be done in a manner that is both simple and effective. When carrying out any kind of study, it is necessary to carry out a literature review, and at that time, the most difficult task is comparing the approaches that are discussed in the various articles. Although each approach that has been created is excellent in its own right, a comparison may still be lacking depending on the needs of the researcher. Therefore, the purpose of this study is to give a concept about a some set of parameters and Neural Networks that may assist researchers in determining a solution for the effective transmission of packets from the source to the destination. And evaluate several approaches based on the particular metrics they use, then choose one that is appropriate for their task. As the size of the literature survey grows, the likelihood of the presence of more performance measures and other data transmission methods also rises. This is because of the exponential growth of the literature survey. In next time to come, work can be expanded to cover more number of parameters and to identify the presence of any other kind of attack.

References

Navinderdeep Kaur, "Analysis of MAODV MANET Routing Protocol on Different Mobility Models", IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT), May19-20, 2017, India.

Nitin Rathod, Nilima Dongre, "MANET Routing Protocol Performance for Video Streaming", IEEE International Conference on Nascent Technologies in the Engineering Field (ICNTE-2017), January27-28,2017, India.

R. V. Kulkarni, A. Forster, and G. K. Venayagamoorthy, "Computational intelligence in wireless sensor networks: A survey," Communications Surveys & Tutorials, IEEE, vol. 13, no. 1, pp. 68–96, 2011.

Kashif Naseer Qureshi, Abdul Hanan Abdullah, Anwar Mirza, Raja Waseem Anwar, "Geographical Forwarding Methods in Vehicular Ad hoc Networks", International Journal of Electrical and Computer Engineering (IJECE), Vol. 5, No. 6, pp. 1407-1416, December 2015.

A. Ng, "Sparse autoencoder," CS294A Lecture notes, vol. 72, 2011.

M. Barabas, G. Boanea, and V. Dobrota, "Multipath routing management using neural networks-based traffic prediction," in EMERGING 2011, The Third International Conference on Emerging Network Intelligence, pp. 118–124, 2011.

A. Omri, R. Hamila, M. O. Hasna, R. Bouallegue, and H. Chamkhia, "Estimation of highly selective channels for downlink lte mimo-ofdm system by a robust neural network.," JUSPN, vol. 2, no. 1, pp. 31–38, 2011.

B. Ustundag and O. Orcay, "A pattern construction scheme for neural network-based cognitive communication," Entropy, vol. 13, no. 1, pp. 64–81, 2011.

Adwan Yasin, Mahmoud Abu Zant, "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique", Wireless Communications and Mobile Computing, Wiley, Hindawi, Volume 2018, Article ID 9812135, pages 1-10.

Arathy K S, Sminesh C N, "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET" Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST), Science Direct, Procedia Technology 25, 2016, 264-271.

Vinay Rishiwal, Sandeep Kumar Agarwal, Mano Yadav, "Performance of AODV Protocol for H-MANETs", International Conference on Advances in Computing, Communication, & Automation (ICACCA), April8-9, 2016, India.

Aswathy P Sreevatsan, Diya Thomas, "An Optimal Weighted Cluster Based Routing Protocol for MANET", International Conference on Data Mining and Advanced Computing (SAPIENCE), March16-18, 2016, India.

Amit Barve, Ashwin Kini, Onkar Ekbote, Jibi Abraham, "Optimization of DSR Routing Protocol in MANET using Passive Clustering", International Conference on Communication Control and Intelligent Systems (CCIS), November18-20, India.

Mohanjeet Singh, Kanwalpreet Kaur, "Physical Distance based Peer Organization in P2P network", IEEE IEMCON 2017, 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference, University of British Columbia, Vancouver, BC, Canada, 3-5 October 2017.

Mohanjeet Singh, Anuj Kumar Gupta, "Structured P2P Overlay Networks for Multimedia Traffic", IEEE International Conference on Innovation and Challenges in Cyber Security

[ICICCS 2016], Amity University, Greater Noida, 3-5 February 2016.
Hemant Rai, "A Comparison of Performance Metrics for Various Routing Protocols in MANET", International Journal of Computer Science and Mobile Computing, Vol. 3, Issue 6, June 2014, pp 239-246.
Swati Bhasin, Ankur Gupta, Puneet Mehta, "Comparison of AODV, OLSR and ZRP Protocols in Mobile Ad-hoc Network on the basis of Jitter" International Journal of Applied Engineering Research, Vol.7 No.11, 2012.
Zishan Haider Y. Noorani, "Performance Analysis of DSDV, AODV and ZRP Routing Protocol of MANET and Enhancement in ZRP to Improve its Throughput", International Journal of Scientific and Research Publications, Volume 3, Issue 6, June 2013, pp. 1-6.
Nauman Ahad, Junaid Qadir, Nasir Ahsan, "Neural networks in wireless networks: Techniques, applications and guidelines", (https://www.sciencedirect.com/science/article/pii/S1084804516300492), Journal of Network and Computer Applications, Volume 68, 2016, Pages 1-27, ISSN 1084-8045.
S. Bahanfar, H. Kousha, and L. Darougaran, "Neural networks for error detection and data aggregation in wireless sensor network," International Journal of Computer Science Issues (IJCSI), vol. 8, no. 5, 2011.
K. Muralidhara and M. N. Harihar, "Routing in ad hoc wireless networks using soft computing techniques and performance evaluation using hypernet simulator," International Journal of Soft Computing and Engineering, vol. 1, 2011.
M. Karlaftis and E. Vlahogianni, "Statistical methods versus neural networks in transportation research: Differences, similarities and some insights," Transportation Research Part C: Emerging Technologies, vol. 19, no. 3, pp. 387–399, 2011.
B. Yuhas and N. Ansari, Neural networks in telecommunications. Springer Publishing Company, Incorporated, 2012.
S. Pattanayak, P. Venkateswaran, and R. Nandi, "Artificial neural networks for cognitive radio: A preliminary survey," in Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on, pp. 1–4, IEEE, 2012.
R. Gargi, Y. Chaba, and R. Patel, "Improving the performance of dynamic source routing protocol by optimization of neural networks," IJCSI International Journal of Computer Science Issues, vol. 9, no. 3, 2012.
K. Tsagkaris, A. Bantouna, and P. Demestichas, "Self-organizing maps for advanced learning in cognitive radio systems," Computers & Electrical Engineering, vol. 38, no. 4, pp. 862–881, 2012.
A. A. Akinduko and E. M. Mirkes, "Initialization of self-organizing maps: Principal components versus random initialization. a case study,"arXiv preprint arXiv:1210.5873, 2012.
D. Ciresan, U. Meier, and J. Schmidhuber, "Multi-column deep neural networks for image classification," in Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on, pp. 3642–3649, IEEE, 2012.
G. Hinton, L. Deng, D. Yu, G. E. Dahl, A.-r. Mohamed, N. Jaitly, A. Senior, V. Vanhoucke, P. Nguyen, T. N. Sainath, et al., "Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups," Signal Processing Magazine, IEEE, vol. 29, no. 6, pp. 82–97, 2012.
S. Li, B. Liu, B. Chen, and Y. Lou, "Neural network based mobile phone localization using

bluetooth connectivity," Neural Computing and Applications, vol. 23, no. 3-4, pp. 667–675, 2013.
R. Khan, S. U. Khan, S. Khan, and M. U. A. Khan, "Localization performance evaluation of extended Kalman filter in wireless sensors network," Procedia Computer Science, vol. 32, pp. 117–124, 2014.
T. Ghalut and H. Larijani, "Non-intrusive method for video quality prediction over lte using random neural networks (rnn)," in Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2014 9th International Symposium on, pp. 519–524, IEEE, 2014.
A. Testolin, M. Zanforlin, M. De Filippo De Grazia, D. Munaretto, A. Zanella, and M. Zorzi, "A machine learning approach to qoe-based video admission control and resource allocation in wireless systems,"in Ad Hoc Networking Workshop (MED-HOC-NET), 2014 13th Annual Mediterranean, pp. 31–38, IEEE, 2014.
C. Li, X. Xie, Y. Huang, H. Wang, and C. Niu, "Distributed data mining based on deep neural network for wireless sensor network,"International Journal of Distributed Sensor Networks, 2014.
M. Abu Alsheikh, P. K. Poh, S. Lin, H.-P. Tan, and D. Niyato, "Efficient data compression with error bound guarantee in wireless sensor networks", in Proceedings of the 17th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems, pp. 307–311, ACM, 2014.
N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov,"Dropout: A simple way to prevent neural networks from overfitting," The Journal of Machine Learning Research, vol. 15, no. 1, pp. 1929–1958, 2014.
Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.
P. A. Kumar and S. Chandramathi, "Intelligent video qoe prediction model for errorprone networks," Indian Journal of Science and Technology, vol. 8, no. 16, 2015.
M. Zorzi, A. Zanella, A. Testolin, M. De Filippo De Grazia, and M. Zorzi, "Cognition-based networks: A new perspective on network optimization using learning and distributed intelligence," Access, IEEE, vol. 3, pp. 1512–1530, 2015.
S. Haykin and N. Network, "A comprehensive foundation," Neural Networks, vol. 2, no. 2004, 2004.
M. L. Minsky and S. Papert, Perceptrons. MIT, 1969.
Zheng, W., Wang, HB., Zhang, ZM. et al. Multi-layer Feed-forward Neural Network Deep Learning Control with Hybrid Position and Virtual-force Algorithm for Mobile Robot Obstacle Avoidance. Int. J. Control Autom. Syst. 17, 1007–1018 (2019).
Dike, H. U., Zhou, Y., Deveerasetty, K. K., & Wu, Q. (2018, October). Unsupervised learning based on artificial neural network: A review. In 2018 IEEE International Conference on Cyborg and Bionic Systems (CBS) (pp. 322-327). IEEE.
G. P. Zhang, "Avoiding pitfalls in neural network research," Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, vol. 37, no. 1, pp. 3–16, 2007.
K. S. Chavda and A. V. Nimavat, Removal of black hole attack in AODV routing protocol of MANET, 4th ICCCNT - 2013, July 4 -6, 2013, Tiruchengode, India, IEEE-31661.
N. Mistry, D.C. Jinwala, M. Zaveri, "Improving AODV Protocol against Black hole Attacks", in Proc. of the International Multi Conference of Engineer and Computer Science, Vol. 2, 2010.

Jaspinder Kaur and Birinder Singh, “Detect and isolate black hole attack in MANET using AODV Protocol”, Inter. J. Adv. Res. Comp. Eng. & Tech. 3(2) (2014), 334-338.

N. Patel, A. Dadhaniya, "Detection of Black Hole Attack in MANET using Intrusion Detection System", International Journal of Advance Engineering and Research Development (IJAERD, Vol 1, Issue 5 May 2014.

H. Deng, W. Li, and D.P. Agrawal, “Routing Security in Wireless Ad Hoc Network”, IEEE Communications Magazines, vol. 40, no. 10, October 2002.

P.N. Raj, P.B. Swadas, “DPRAODV: A Dyanamic Learning System against Black Hole Attack in AODV Based MANET”, IJCSI International Journal of Computer Science Issues, Vol. 2, pp 54-59 2009.

Neha, M. Sharma, “A Survey on Black Hole Attack Detection and Prevention Techniques”, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol.3, Issue IV, April 2015.

Sharma Manmohan, Neha, “Step verification for detection of black hole attack in MANET”, Inter. Conf. Adv. in Appl. Engineer. & Tech., 10(2) (2015).

Farahani, G. (2021). Black hole attack detection using K-nearest neighbor algorithm and reputation calculation in mobile ad hoc networks. Security and Communication Networks, 2021.

Dhaliwal, B. K., & Datta, R. K. (2019). Secure and energy efficient trust aware routing protocol in IoT using the optimized artificial neural network: SEETA-IoT. International Journal of Engineering and Advanced Technology, 8(6), 4341-4353.

Qiu, Tie, et al. "ERGID: An efficient routing protocol for emergency response Internet of Things." Journal of Network and Computer Applications 72 (2016): 104-112.

A. Vij and V. Sharma, “Security issues in mobile adhoc network: a survey paper,” in Proceedings of the International Conference on Computing, Communication and Automation, Greater Noida, India, April 2016.

B. Sun, Y. Guan, J.Chan,U.W. Pooch, “Detecting Black-hole Attack In Mobile adhoc Networks” in EPMCC, 2003.

S. Ramaswamy, Huirong Fu, M. Sreekantaradhya, John Dixon, and Kendall Nygard, ”Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks” in Proceedings of 2003 International Conference on Wireless Networks (ICWN’03), Las Vegas, Nevada, USA, pp. 570-575.

G. Wahane, A. Kanthe, s”Techniques for detection of cooperative Black hole Attack in MANET” in IOSRJCE, 2014.

A. Mitra, R. Ghosh, A. Chakraborty, D. Srivastva, “An Alternative Approach to Detect Presence of Black HoleNodes in Mobile Ad-Hoc Network Using Artificial Neural Network” in IJARCSSE, 2013.

Mohammad AL-Shurman,Seon-Moo Yoo and Seungiin Park,” Black Hole Attack in Mobile Ad Hoc Networks” in ACMSE’04, April 2-3,2004, Huntsville, AL,USA.

Gerhardss-Padilla,E., Aschenbruck N. ,Martini, P. , Jahnke, M. , Tolle, J., “Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs” in IEEE, 2007, pp.1043-1052.

Yadav P., Kumar N., Gill R.K., “A Fuzzy Based Approach to Detect Black Hole Attack” in International Journal of Soft Computing And Engineering (IJSCE), ISSN: 2231-2306, Volume-2, Issue-3, July 2012.

N. Komninos, D. Vergados, C. Douligeris,"Detecting unauthorised and compromised nodes in mobile adhoc networks" in Adhoc Networks 5, 2007, pp. 289-298.

Moradi Zahra, Teshnehlab M., Rahmani A. M., "Implementation of Neural Networks for Intrusion Detection in MANET", (IEEE), 2011.

Sujatha K.S. , Dharmar V. , Bhuvaneswaran R.S., "Design of genetic algorithm based IDS for MANET", IEEE (2012), pp.28-33.

Abbas Afsharfarnia, Abbas Karimi, "A New Clustering Algorithm Using Links' Weight to Decrease Consumed Energy in MANETs", TELKOMNIKA, Vol.12, No.2, June 2014, pp. 411~418.

Ritul Kumar and Ruchika Monga, "Cluster Based Energy Efficient Protocol To Increase Network Lifetime In MANETS", Special Issue, Vol. 1, No. 2, July 2015 National Conference on "Emerging Trends in Electronics & Communication" (ETEC-2015) © 2015 IJEETC.

M. Singh, G. Singh, "Secure and Efficient Cluster Head Selection Algorithm for MANET", Journal of Network Communications and Emerging Technologies (JNCET), Vol. 2, Issue 2, June (2015).

Nath Ira, Rituparna Chaki, BHAPSC: A new black hole attack prevention system in clustered MANET, Inter. J. Adv. Research in Comp. Sci. and Soft. Eng., 2(8) (2012), 113-121.

H.S. Bedi, K.K. Sharma, and R. Gupta, "A Review Paper on Performance Analysis of IEEE 802.11 e", 1st International Conference on Computing, Communications, and Cyber-Security (IC4S 2019), 2020, pp. 47-56.

Z.G. Khaki, and H.S. Bedi, "Transient correction using EDFA: in-line optical fibre with feedback", International Conference on Computing Sciences, 2012, pp. 233-238.

Bedi, Harpreet, Kamal Kumar, and Gupta Raghav. "A review paper on improving the network efficiency of IEEE 802.11 e networks." Intelligent Circuits and Systems (2021): 206-211.

Harpreet Bedi, Kamal Kumar Sharma; Analyses of CSMA/CA Protocol Without Using Virtual Channel Sensing in DCF Mode, Global Emerging Innovation Summit (GEIS-2021) (2021) 1: 484.

Harpreet Singh Bedi, Kamal Kumar Sharma, Shakti Raj Chopra and Balraj Singh Analysis of QoS parameters using different back off window algorithm in the IEEE 802.11e networks, Advances and Applications in Mathematical Sciences Volume 21, Issue 10, August 2022, Pages 6147-6157 © 2022 Mili Publications, India

Performance comparison of companding techniques and new d-cast method for reduction of PAPR in OFDM Bedi, H., Puri, I., Sharma, R.K., Verma, S. International Journal of Control Theory and Applications, 2016, 9(24), pp. 217–222.

Soft computing based robust and dynamic road traffic control system-a initiative to development of intelligent transportation system (ITS) Mittal, P., Bedi, H.S., Arora, K.Journal of Engineering and Applied Sciences, 2016, 11(2), pp. 210–215.

Singh, Harpreet, Shekhar Verma, and Gaganpreet Kaur Marwah. "The new approach for medical enhancement in texture classification and feature extraction of lung MRI images by using gabor filter with wavelet transform." Indian Journal of Science and Technology 8.35 (2015): 1-7.

Fingerprint Image Identification System: An Asset for Security of Bank Lockers Apoorva, M., Pavan, S., Bedi, H.Digital Forensics and Internet of Things: Impact and Challenges, 2021, pp. 227–235.

Analysis of a adaptive Backoff algorithm to improve the utilization of the network Bedi, H.S.2022 1st International Conference on Sustainable Technology for Power and Energy Systems, STPES 2022, 2022

Utilization of a Wireless Network Performing CSMA/CA with Random Backoff Algorithm Bedi, H.S.,2022, 2327(1), 012060.

A survey on enhancing quality of service in wireless sensor networks Bedi, H.S., Verma, S., Singh, B. International Journal of Control Theory and Applications, 2016, 9(41), pp. 37–42

Performance comparison of companding techniques and new d-cast method for reduction of PAPR in OFDM Bedi, H., Puri, I., Sharma, R.K., Verma, S. International Journal of Control Theory and Applications, 2016, 9(24), pp. 217–222