International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A QoS Perception Routing Protocol for MANETs Based on Machine Learning

Dr. N. Sivapriya[1], **Dr. R. Mohandas**[2], **Karthik Kumar Vaigandla**[3]

Submitted: 27/08/2023 **Revised**: 22/10/2023 **Accepted**: 02/11/2023

Abstract: Machine learning (ML) approaches facilitate the acquisition of knowledge by a system and promote its capacity to adapt to the environment, relying on a multitude of logical and statistical processes. The primary objective of ML is to identify intricate patterns and derive decisions from the obtained outcomes. A range of ML methods have been used for the purpose of enhancing the security of mobile ad-hoc networks (MANETs). The recent progress in wireless communication has prompted researchers to focus their efforts on the development of MANETs. These networks include nodes communicating with one other in order to provide real-time entertainment services as required. Nevertheless, the establishment of safe routing in MANETs remains a formidable challenge, mostly attributed to the wireless connection and decentralized design of these networks. The Ad-hoc On-demand Distance Vector (AODV) routing protocol is extensively used in MANETs due to its broad range of applications, commendable performance, and scalability. However, the AODV routing protocol is considered to be a non-optimal solution since it offers simply an alternative route rather than an optimized one. This research presents a suggested ML based AODV Routing Protocol (ML-AODV) for the purpose of mitigating flooding and blackhole attacks in MANETs. The assessment of the suggested methodology is conducted using the NS-2 simulator and compared to established routing frameworks. This work aims to conduct a comparative analysis and investigation of the AODV, DSDV, and ML-AODV protocols. The analysis will primarily focus on evaluating the performance of these protocols using different metrics, including throughput (TP), packet delivery ratio (PDR), average end-to-end latency (E2EL), packet loss rate (PLR), and energy consumption (EC). The results indicate that the performance of ML-AODV outperforms that of DSDV and AODV. The ML-AODV algorithm demonstrates enhanced performance and reliability compared to previous techniques, while significantly reducing latency, routing overhead (RO), and PLR.

Keywords: *AODV, Attack, Machine learning (ML), ML-AODV, MANETs, mobile node, SVM, Routing protocol, DSDV.*

1. Introduction

A MANET is comprised of mobile nodes that are interconnected by a wireless medium inside a dynamic network without a fixed infrastructure [1]. The distinctive characteristics of MANETs contribute to their expanded use in contexts where the establishment of traditional infrastructure is impractical, as seen in domains such as military operations, rescue missions, healthcare services, and virtual conferences. Moreover, in essential contexts such as combat communication, ensuring security inside this network is an unavoidable concern. The presence of vulnerabilities inside the network makes it an appealing option for the implementation of attacks aimed at compromising its security. Therefore, it is crucial to choose a security system that is both efficient and adaptable, capable of effectively identifying and mitigating any harmful activity inside the network [2]. The exponential growth of mobile communication in recent years, particularly in the domains of mobile systems, WLAN, and ubiquitous computing, has been widely recognized [3-4]. A spontaneous ad hoc network (ANET) is formed by a collection of mobile terminals that are in close proximity to one other and engage in communication, sharing of services, resources, or computing time within a defined time frame and restricted physical area. The transparency of network management to the user is crucial. These networks are characterized by autonomous centralized management, allowing users to join and exit the networks with ease. One of the crucial study domains in MANETs pertains to the establishment and sustenance of ANETs by means of routing protocols [5-6]. Routing is a fundamental process in networking wherein a traffic route is determined for the purpose of transmitting and receiving data, either inside a single network or across numerous interconnected networks. The process involves the routing of logically addressed packets from their origin to their final destination by means of intermediate nodes. A routing protocol refers to the process of directing packets according to certain rules and regulations. Each routing protocol uses a distinct mechanism to locate and sustain routes. Every routing protocol is equipped with a data structure that is responsible for storing route information and making necessary modifications to the routing table in

[1] *Assistant Professor, Department of Computer Application, Cauvery College for Women, Trichy, TamilNadu, India*

[2] *Associate Professor, Department of ECE, Balaji Institute of Technology & Science, Warangal, Telangana, India*

[3] *Assistant Professor, Department of ECE, Balaji Institute of Technology & Science, Warangal, Telangana, India*

** Corresponding Author Email: nmsivapriya@gmail.com*

order to maintain the routes. A routing metric refers to a numerical number used by a routing algorithm to assess the relative performance of several routes. Metrics include a range of factors including bandwidth, latency, hop count, route cost, load, dependability, and communication cost. The routing table only retains the most optimal routes, but link-state or topological databases have the capacity to hold additional information beyond this. MANETs represent a significant advancement within the realm of telecommunications [7].

A MANET is a kind of wireless network that consists of mobile nodes and lacks a centralized administration for packet routing [8-9]. The mobile nodes exhibit variations in their velocities, communication coverage, and periods of inactivity. Therefore, the fundamental objective is to provide secure packet routing mechanisms that can effectively mitigate the intrinsic behaviour of the network. In this regard, there are conventional MANET routing techniques known as topology-based and location-based protocols. Moreover, these routing strategies may be classified into three distinct forms, namely reactive/on-demand, proactive, and hybrid routing protocols. In pursuit of this objective, the conventional AODV routing system has emerged as the predominant reactive protocol for facilitating packet delivery [10]. The AODV protocol, because to its incorporation of both route identification and repair methods, is often used for the efficient distribution of emergency and multimedia data inside MANETs. Nevertheless, the aspect of security remains a vital consideration in light of the prevalence of wireless communication and the constraints imposed by limited energy resources. Hence, MANETs are susceptible to a range of assaults, such as blackhole, wormhole, and grey hole, which have a detrimental impact on the network's overall performance [11-12]. MANETs have a notable susceptibility to blackhole attacks, leading to substantial degradation in packet transmission. This is mostly due to the routing algorithms used, which often rely on blind confidence in neighbouring nodes for packet forwarding. Furthermore, the detection of blackhole attacks is a challenge since it is difficult to discern if packet drops are a result of such attacks or simply a consequence of the network's natural behaviour. The invaders first entice the adjacent nodes within the network and thereafter broadcast the presence of a novel route to the intended destination. Subsequently, nodes with malicious intent proceed to discard all packets without any further transmission. In order to achieve this objective, there are various studies available that focus on detecting blackhole attacks in MANETs via the modification of the classic AODV protocol [13-15].

2. Related Works

Numerous research projects have been undertaken in recent years to assess the efficacy of different routing protocols in MANETs. Various routing protocols use different strategies or metrics to find the optimal route between a source node and a destination node. Some of these protocols utilize the available bandwidth, while others rely on hop count measurements between network nodes. Each of these protocols have advantages and disadvantages [16]. In their research, conducted a comparative analysis to assess the efficiency of the AODV and DSDV routing protocols in terms of node speed. The evaluation was carried out using the NS2 simulator. According to the findings of the simulation, it was observed that AODV exhibits superior performance compared to DSDV in terms of metrics such as TP, latency, and PDR [17]. According to [18], DSDV has superior performance in terms of energy usage compared to AODV. A comparable research is given by the authors in [19]. The authors assert that AODV exhibits superiority over AOMDV, DSR, and DSDV with respect to CBR connection. DSR demonstrates superior performance compared to AODV, AMDV, and DSDV with regard to TCP connections.

In the context of MANET, the dynamic nature of node positions, characterized by frequent changes resulting from their inherent motions in various directions and speeds, introduces significant complexity to the management of network traffic. The efficacy of static algorithms in accommodating changing circumstances has been shown to be inadequate. The routing technique proposed by the authors in reference [20] use the Reinforcement Learning (RL) algorithm to get an optimal solution rather than just selecting the shortest route. The findings suggest that RL-based solutions exhibit superior performance compared to the shortest route strategy as the packet load increases. In their study, the authors of reference [21] sought to tackle the issue of energy depletion in WSNs with the aim of prolonging the network's lifespan. This challenge arises from the impracticality of routing the sensor nodes' battery power, given their placement in hazardous locations. The authors use the Support Vector Machine (SVM) technique in order to provide a unique Hierarchical Routing system. The proposed routing approach aims to assign sensor nodes to the nearest cluster while also ensuring a balanced distribution of energy dissipation across cluster heads. The authors in reference [22] address the topic of network reconfiguration, a practice used by network operators to facilitate effective troubleshooting and network optimization. Software-Defined Networking (SDN) facilitates the centralized and programmable control of the whole network, as opposed to the conventional approach of relying on scattered control planes across various network devices. The Q-learning approach was presented by the authors in [23] as a means to address the challenges of developing an adaptive and energy-efficient routing protocol for Underwater delay tolerant networking (DTN). The authors elucidate the need of including energy economy into the protocol design as a means to address the challenges posed by adverse circumstances in underwater sensor networks, which render the replacement of sensor batteries both expensive and difficult [24-26].

The authors in [27] have provided a detailed explanation of a secure AODV routing method that utilizes sequence numbers for the purpose of detecting attackers inside the network. Routing protocols use a predetermined threshold to discern the sequence number of Route Reply (RREP) at regular intervals. In a study conducted by Su et al. [28], a solution using suspicion values was provided to identify blackhole attacks in MANETs . In this study, a novel parameter called "suspicion value" is introduced into the routing tables of nodes that participate in data transmission. In a previous study [29], a skilled trust-based intrusion detection technique was introduced, which utilizes local information for data transfer in a highly dynamic MANET. The issue of blackhole and grey-hole attacks was mitigated by the implementation of a strategy that included the selection of trustworthy nodes in order to enhance security measures. The authors in [30] have introduced an upgraded AODV routing strategy with the objective of enhancing security in MANETs. Researchers in the referenced study conducted an analysis on the black-hole attack in MANETs specifically focusing on its impact on the route building process using the AODV routing protocol. In their study, Kumar et al. [31] have investigated the issue of packet loss in wireless networks and proposed a congestion management method based on neural networks. The objective of their research is to ensure steady data transmission in MANETs. In the study conducted by the authors [32], a cross-layer intrusion detection technique was introduced. This approach facilitated the interchange of routing information across various levels of two nodes and their neighbouring nodes.

3. Machine Learning (ML)

ML is a specialized domain within the subject of Artificial Intelligence (AI), which is dedicated to the investigation and advancement of algorithms and methodologies that empower computers and other computational devices to acquire knowledge and skills via self-learning processes, without the need for explicit programming. Machines has the ability to acquire knowledge and extract specific information with the purpose of uncovering hidden patterns within a given set of samples. These latent patterns are used to predict and deduce appropriate behaviour in a novel situation or instance. Hence, the use of ML methodologies enhances the efficacy of system operations as time progresses. ML-empowered gadgets exhibit enhanced intelligence and contextual awareness as a result of extensive experiences and training.

3.1. Supervised learning (SL)

Supervised learning refers to the iterative process of acquiring knowledge on the relationship between a given set of input factors and an output variable. This acquired knowledge is then used to make predictions about the outcomes of unfamiliar data. In the context of SL, it is necessary to have labelled training data prior to generating a classification model. This model may then be used to assign labels to new testing data. The aim of the ML task is to create a model of high quality. As seen in Figure 1, the development of a ML model requires the execution of many steps.

Data collection - The first stage in determining the objectives of an ML model is to establish the problem statement. Subsequently, it becomes necessary to gather suitable input data to be used by the machine. The significance of this stage in the ML model development process lies in the fact that the efficacy of the model is contingent upon the quantity and quality of the data used. Data may be acquired from pre-existing databases or generated from scratch.

Data preprocessing - The dataset that has been gathered often exhibits several defects, including incomplete/missing/noisy data that includes mistakes or outliers, and inconsistent data that contains disparities in codes [33]. The effectiveness of decision outcomes is contingent upon the quality of the data that is provided. Therefore, this phase primarily focuses on the cleansing and preparation of the data in a format that is suitable and applicable for the knowledge extraction process. Hence, the process of data preprocessing plays a crucial role in establishing the basis for accurate data analyses and is often required to guarantee the dependability of data analysis using diverse methodologies.

Model training - After the data has undergone the process of cleaning and preparation, it is then partitioned into the training set and the testing set. The process of model training involves providing a ML algorithm with training data in order to facilitate the identification and acquisition of optimal values for all relevant variables. The phrase "ML model" refers to the model decision function that is generated via the process of training. In the context of supervised learning, the objective of model training is to provide a precise mathematical depiction of the association between qualities of data and a designated target label. A variety of supervised learning algorithms are employed in the process of training a model.

Model validation - The primary objective of model validation is to assess the precision and reliability of the trained model. One effective method for assessing the effectiveness of a ML model involves evaluating the model's performance by subjecting it to a test dataset. Once the test result has been deemed acceptable, the model is deemed suitable for deployment. Alternatively, a tuning procedure is conducted to readjust the training parameters in order to enhance the accuracy of the model.

Model deployment - During this stage, the model that has been developed is used to make predictions on the labels of forthcoming samples. The built model is used to classify fresh samples and assign them to the proper class.

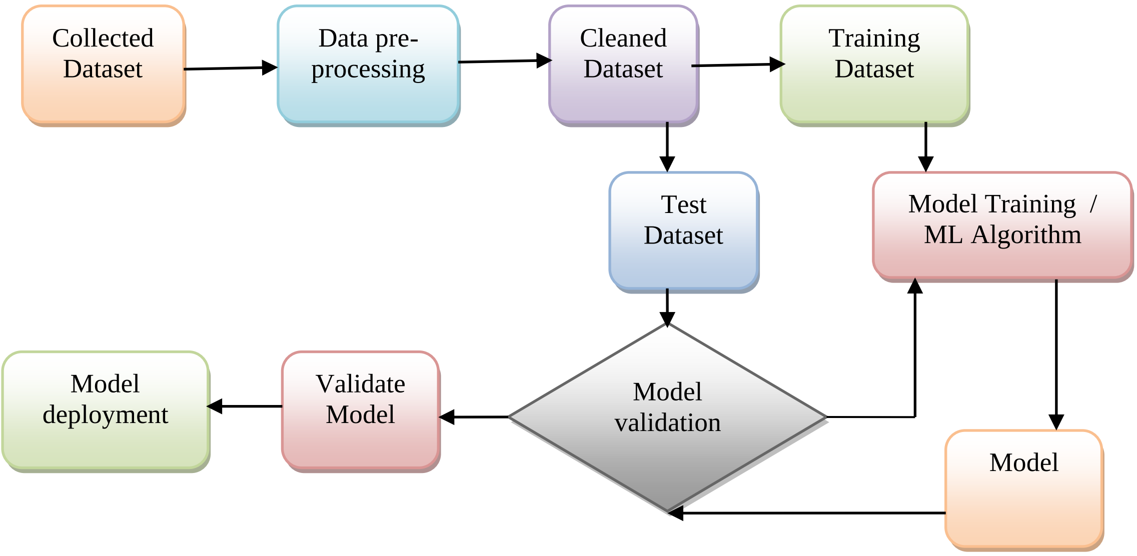

Fig 1. Flow of supervised learning

3.2. Unsupervised learning (USL)

When the dataset provided lacks labels and the expected outcomes are unknown, this approach proves to be beneficial. Within this particular learning paradigm, the computer endeavours to discern commonalities across many samples, analyze the gathered data, and construct its own models.

3.3. Reinforcement learning (RL)

The discipline of RL is concerned with the challenge of how an independent agent may effectively make choices within a given environment. The objective is to choose the most advantageous action that maximizes the overall reward, while simultaneously adapting its state transitions.

4. Approaches and solutions for Protecting Data in MANETs

The distinctive characteristics of MANETs, such as decentralization and self-management, make them susceptible to a variety of network assaults. Over the course of the last decade, a multitude of security measures have been presented with the aim of detecting assaults and minimizing their impact. The first security protocols used in MANETs were predicated on the utilization of cryptographic methods. The implementation of a key management system using threshold cryptography to facilitate authentication in ad-hoc networks occurred in 1999. Within the proposed system, some nodes are designated to fulfill the function of servers, while a limited number of nodes assume the role of administrators. Additionally, a secure variant of the AODV routing protocol was developed and referred to as Secure AODV (SAODV). The solution that was presented included the use of digital signatures and hash chains as means of ensuring cryptographic security inside ad hoc networks. Numerous cryptographic procedures have been developed that rely on a central authority for the issuance of authentication certificates [34]. However, several other approaches have adapted the notion of central oversight, similar to the PGP web of trust architecture [35]. These approaches include nodes that are capable of storing their own certificates. As a result, the authentication process consists of a series of certificates that are stored at the respective ends of the nodes. In the realm of literature, scholars have noted that the use of cryptographic algorithms in communication systems has resulted in a notable time delay. Additionally, it has been recognized that establishing a pre-existing link between nodes is impractical inside ad-hoc networks. The researchers assembled an extensive assortment of hybrid techniques aimed at enhancing security in MANETs [38-41].

The establishment of robust security measures is a fundamental need for the effective functioning of network operations, including aspects such as packet transmission and routing protocols. When developing sensitive apps, it is essential to take into account the essential security characteristics of the network. ML methods are used to develop a predictive model, which is trained using a designated set of training data that contains specified attack patterns. The model is then evaluated using the remaining test data. The evaluation of the learning model's accuracy is determined by its ability to accurately detect and classify novel assault patterns. The open nature of the network in MANETs renders the nodes more susceptible to many forms of assaults, including but not limited to black hole, worm hole, grey hole, flooding, and DoS attacks. In addition, it is worth noting that the nodes inside MANETs engage in multi-hop communication, whereby the source node transmits packets to many intermediary nodes prior to reaching the destination node. Effective communication is contingent upon the collaborative efforts of the many nodes involved. In order to ensure network security, it is essential to ascertain the trustworthiness of nodes, hence preventing the forwarding of packets to any untrustworthy or hostile nodes inside the network. In order to achieve this objective, many trust assessment approaches have been developed in the existing body of literature with the aim of bolstering network security. Therefore, the security techniques used in MANETs may be classified into several groups, as seen in Figure 2.

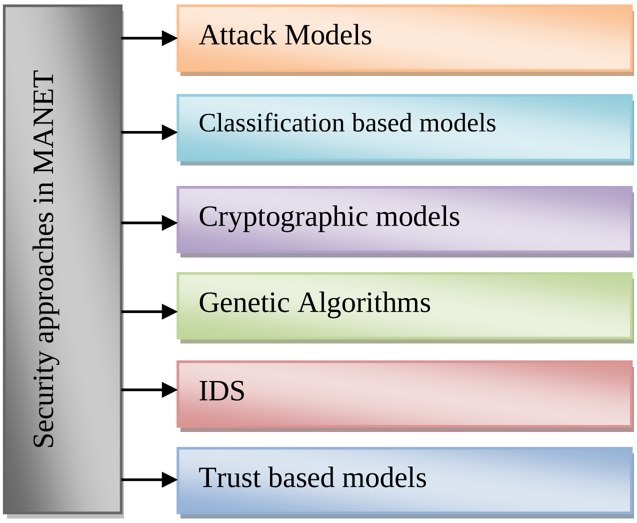

Fig 2. Categorization of security methodologies in MANETs

5. Routing Protocols

Routing protocol study for MANETs has gained significant attention since it is a widely used wireless network. Several routing protocols, including OLSR, DSDV, AODV, DSR, and ZRP, have been recognized by the industry.

5.1. Ad Hoc On-demand Distance Vector Routing (AODV)

The AODV routing protocol is a kind of on-demand routing protocol that incorporates elements from both the DSDV and DSR protocols. It utilizes the routing discovery and maintenance mechanisms of DSR, while also including the hop and routing features of DSDV. The protocol exhibits favorable characteristics as an on-demand routing protocol when it is integrated with the benefits of both. This protocol has the capability to be used in a mobile node inside a particular network, enabling it to determine a path to the intended destination within a constantly evolving point-to-point network. The features included in this context are rapid access speed, little processing, less memory footprint, and less network burden. The use of the destination sequence number field inside the routing table ensures that the route does not create a loop, regardless of any unexpected behavior shown by the routing control unit. This mechanism effectively prevents the occurrence of network loops and the associated issue of endless counting in conventional networks. The AODV routing protocol has three communication mechanisms, including the route request (RREQ), RREP, and routing error (RERR) methods.

RREQ – When a node wishes to deliver a packet but lacks knowledge of the route to the destination, it initiates the route discovery process by sending a multicast RREQ message. Adjacent nodes maintain a record of the message's origin and facilitate its transmission to their adjacent nodes until it reaches the intended destination node.

RREP – The destination node provides a response in the form of a RREP, which follows the same route as the RREQ back to the starting node. As the RREP packet travels back to the originating node, intermediate nodes establish forward routes. In the event that an intermediate node has knowledge of the path leading to the destination, it has the capability to transmit a RREP as a response to a received RREQ. This facilitates the ability of nodes to access and use an established route. The initiation of communication between the source and the destination occurs with the arrival of the RREP at the source node, therefore establishing a viable route.

REER – The AODV protocol is often associated with lower overhead compared to proactive protocols due to its reactive nature, resulting in fewer route maintenance messages. When a connection interruption occurs and the route becomes non-functional, meaning that messages cannot be transferred, an RERR message is sent by a node that detects the disruption in the link. The communication is redistributed via other network nodes. The RERR notification indicates the presence of an unreachable destination. The deactivation of the route occurs when the message receiving nodes become inactive.

5.2. Destination Sequenced Distance Vector (DSDV)

The DSDV protocol is a routing mechanism designed for MANETs. It operates using a table-driven approach and is built upon the Bellman-Ford algorithm. In this network architecture, every node functions as a router, responsible for maintaining a routing table and transmitting periodic routing changes, regardless of the need of these routes. Each route or path to the destination is assigned a sequence number in order to minimize the occurrence of routing loops. Routing updates are exchanged continuously, even during periods of network inactivity, resulting in the use of battery power and network bandwidth resources. Therefore, extremely dynamic networks are not preferred. The DSDV routing protocol addresses two critical issues in network routing: the prevention of routing loops and the mitigation of the counting-to-infinity problem. The distribution of an update, meanwhile, has a somewhat sluggish pace. The primary cause of substantial losses in mobility may be attributed to the use of antiquated table entries [36-37].

5.3. ML based AODV (ML-AODV)

This paper demonstrates the use of ML techniques, namely artificial neural network (ANN) and SVM, for the purpose of mitigating various attacks in MANETs. The primary function of the ANN is to discern the most effective and ideal path. Subsequently, the SVM classifier is employed to detect the presence of an intruder inside the designated path.

In the context of MANETs, the majority of routing systems have shown a preference for using shortest route algorithms to facilitate packet transmission. However, it is important to note that this strategy may not always be the most optimal choice for efficient packet transmission. This is mostly due to the inherent variations in node speeds, energy consumption levels, and congestion levels within the network. Hence, in the ML-AODV architecture under consideration, each mobile node initially maintains a list of immediate or 1-hop neighbours by periodically exchanging HELLO packets. Subsequently, the source or originator node verifies the presence of a viable route to the destination by consulting its routing database. In the event that the route is accessible, the source initiates the transmission of data packets. However, if the route is not available, the source proceeds to broadcast a new RREQ packet to its immediate 1-hop neighbours in order to establish a new route. Upon receipt, the node verifies the destination. If the node is not the destination, the trust value is computed and compared to the threshold value. If the trust value exceeds the predetermined threshold, the trust value is thereafter saved inside the ML-AODV RREQ packet. The structure of the RREQ field includes supplementary fields in addition to those included in the conventional AODV protocol.

In a MANET, the absence of centralized management results in mobile nodes functioning as routers, facilitating the exchange of data by relying on mutual confidence among all nodes in the network. However, regardless of one's awareness of the energy levels and expiry time of links, placing faith in all relay nodes might result in the flooding of control packets or the needless utilization of resources via rerouting. Upon receiving the RREQ packet, intermediate nodes generally do two tasks. First, they verify whether the packet's destination matches their own node's address. whether there is a match, further processing is not required. Second, if the destination does not match, the intermediate nodes calculate the link expiry time and the residual energy. These calculations are necessary for determining the viability of forwarding the packet to the next node in the network. The routing database at each node maintains records of both the Link Expiration Time (LET) and Route Expiration (RE) values that exceed a specified threshold. Furthermore, the same procedure is subsequently repeated. Nodes with trust values beyond the threshold are classified as dynamic relay forwarders, while those with trust values below the threshold are recognized as invaders responsible for flooding and blackhole attacks. The trust value is contained in both the RREQ message of the ML-AODV protocol and the routing database of the source node. Moreover, the trust value of each node is documented based on the most recent data exchange with its neighbouring nodes, therefore maintaining a record of its reliability. The aforementioned procedure is consistently repeated at regular intervals upon reaching the destination, resulting in the accumulation of several RREQ messages.

$$LET = \frac{\sum_{k=0}^{N} PRT_k - PDT_k}{N}$$

$$RE = \sum_{k=0}^{N} EBS_k - EAS_k$$

Threshold values are

$$T_{LET} = \frac{RTR}{2}$$

$$T_{RE} = \frac{Initial\ Energy}{2}$$

where PRT and PDT denote the timings at which packets are received and delivered, EBS is the initial energy before simulation and ESA is the energy after simulation at a certain node k, respectively.

Artificial Neural Networks (ANN):

The structural and functional characteristics of the human brain serve as a source of inspiration for the development of artificial neural networks. The ANN consists of several linked neurons or nodes, organized into three primary layers as seen in figure 3: the input layer, hidden layers, and output layer. It is essential to note that the nodes inside each layer do not possess any interconnections. Every node inside the system is a computing unit that is linked. The primary purpose of the role is to compute the sum of the incoming values (X_i) multiplied by their corresponding weights (W_i). Additionally, it incorporates a bias term (B_k) that regulates the input to the activation function, which is subsequently added to the summation of the multiplied values. Subsequently, the output Y_k of the neuron is sent via an activation function f, which facilitates the delimitation process, as seen in Figure 4.

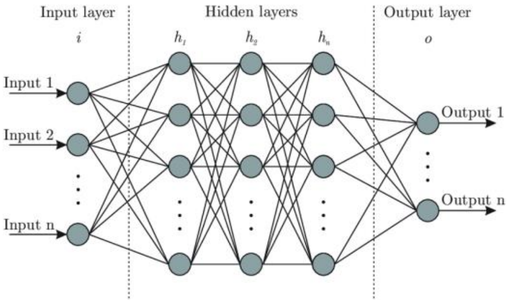

Fig 3. ANN structure

The neuron output Y_k is represented by the following function,

$$Y_k = f\left(W_1X_1 + W_2X_2 + ... + W_nX_n + B_k\right)$$

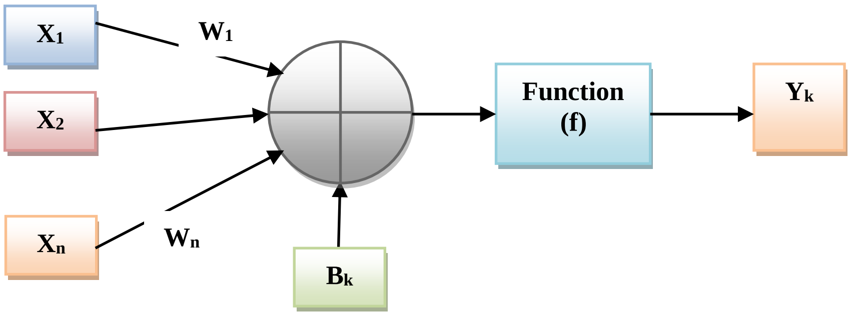

Fig 4. AN model

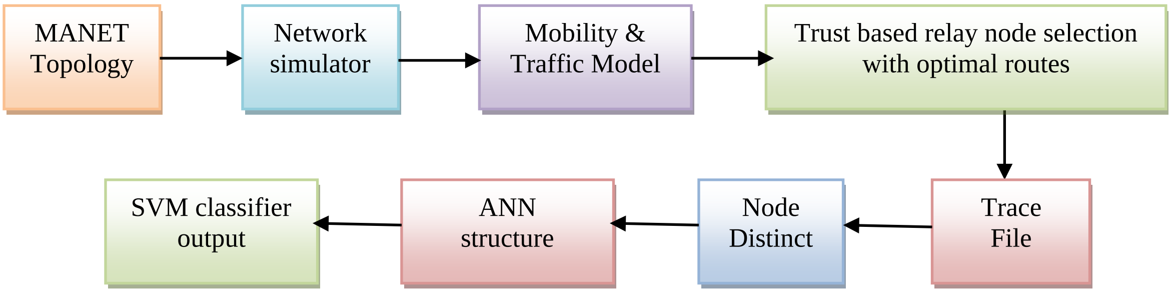

Fig 5. ML-AODV framework

Support Vector Machine (SVM) classifier :

The SVM is considered to be the optimal choice for doing intrusion detection in high-accuracy network environments. Hence, the use of an integrated ANN and SVM is deemed appropriate for the identification and classification of malevolent nodes. The model shown in Figure 5 illustrates the suggested approach for detecting both flooding and blackhole attacks utilizing the AODV protocol, ANNs, and SVMs. The figure illustrates that the distinctive characteristics of a node along a certain path are used as inputs for the SVM model inside the ANN process. The SVM algorithm uses the Gaussian Kernel to extract the characteristics of nodes as input, facilitating the transformation of the data into a suitable format for processing from the source to the destination. The MANET model is provided as input to the ANN and then processed by further layers. The network testing and training process has been conducted using the NS-2 acquired trace file. This trace file provides a representation of the network's continuous traffic and aids in the identification and distinction of normal and suspicious behaviours inside the network. Furthermore, the trace file contains data pertaining to both arriving and exiting packets inside the network. SVMs are used for the purpose of identifying intruders along a certain route. Subsequently, ANNs are utilized to confirm the identified node and its associated formulas.

6. Simulation Results

In recent days, the use of simulation has become vital in the examination of complex networks, enabling the assessment of their performance and behaviour prior to implementation. There are other network simulators, such as OMNET, NS2, and OPNET, that aim to accurately represent real-time implementation in their output. In this, the NS-2.34 was used to conduct a comparative analysis and performance evaluation of the AODV, ML-AODV and DSDV in a MANET. The simulation used several node configurations to thoroughly evaluate the efficiency of these protocols with respect to performance metrics.

Table 1. Simulation Parameters

Parameter	Value
Area	1200 m × 1200 m
Control channel packet size	128 Bytes
Channel type	Wireless channel
MAC Type	Mac /802.11
Simulator	NS-2
Max Speed	0 - 30 m/s
Mobility model	Random way point model
Nodes	50
Packet Size	1024 bytes
Routing Protocols	DSDV, AODV, ML-AODV
Source Type / Traffic Source	CBR
Simulation Time	500s
Transfer model	WaveLan model
Transmission Range	250 m
Wireless channel bandwidth	12 Mbps

Packet Delivery Ratio (PDR) : The metric under consideration is the ratio between the number of data packets successfully delivered to the destination node and the number of data packets created by the Constant Bit Rate (CBR) source node. Alternatively, it may be interpreted as the throughput received by the destination node. It is the ratio between the total number of data bits received and the total number of data bits transmitted from the source to the destination.

According to the Figure 6, ML-AODV has demonstrated superior performance compared to both DSDV and AODV as the number of nodes increases. The PDR of ML-AODV ranges from 720 to 1680. The PDR of the DSDV routing protocol is between the range of 255 to 910.

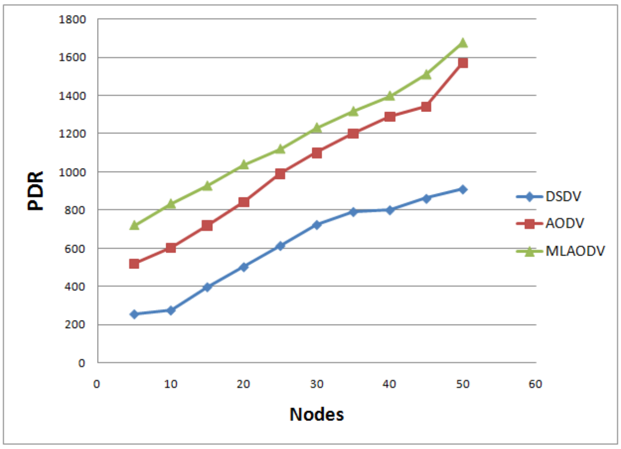

Fig 6. Nodes vs PDR

The relationship between node movement speed and PDR is inversely proportional, as an increase in node movement speed leads to a drop in PDR. The data shown in Figure 7 indicates that the performance advantage of ML-AODV is not notably significant when the speed of node movement rises. However, it can be seen that ML-AODV exhibits superior performance compared to DSDV.

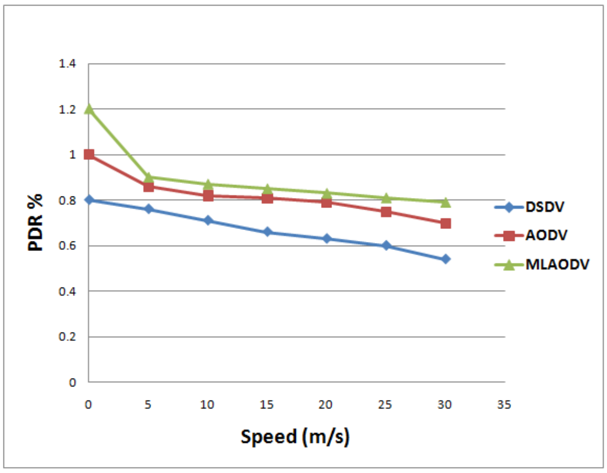

Fig 7. Speed vs PDR

End-to-End average Delay (E2ED): The time delay refers to the duration it takes for a data packet to be sent from the source node to the destination node. The calculation of the average time difference between the sending and receiving of individual packets involves dividing the overall time difference by the total number of packets received. It refers to the duration required for a data packet to reach its intended destination inside a network. The factors included in this set of considerations consist of the latency associated with buffering, the delay caused by interface queuing, the delay resulting from MAC layer retransmissions, the delay caused by airborne propagation, and the time used for route lookup transitions.

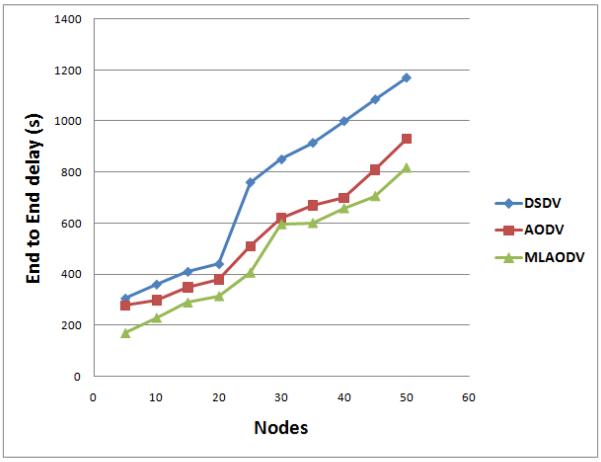

Fig 8. Nodes vs E2E delay

The figure 8 illustrates the variability in average E2ED in packet routing between various nodes, comparing the proposed ML-AODV with the current AODV protocols. The performance of ML-AODV exhibits little latency as compared to AODV, even in scenarios where the number of nodes is increased. The findings indicate that ML-AODV outperforms DSDV. The E2ED of the DSDV routing protocol has a higher magnitude compared to the ML-AODV routing protocol. The DSDV protocol maintains routing tables in order to facilitate packet delivery. Consequently, it establishes new routes whenever there is a modification in the network topology. On the other hand, the ML-AODV protocol operates as an on-demand routing protocol. It initiates the routing discovery process whenever there is a need to construct a new route. The ML-AODV protocol facilitates the transmission of necessary packets in response to communication requests between nodes.

As seen in Figure 9 , the ML-AODV protocol demonstrates a notable reduction in the average latency experienced in end-to-end communication. This improvement may be attributed to the ML-AODV's capacity to consider the diverse circumstances existing between nodes, resulting in a much lower risk of routing failures compared to the DSDV protocol. The average latency of both DSDV and ML-AODV protocols exhibits an upward trend as the speed of node movement rises.

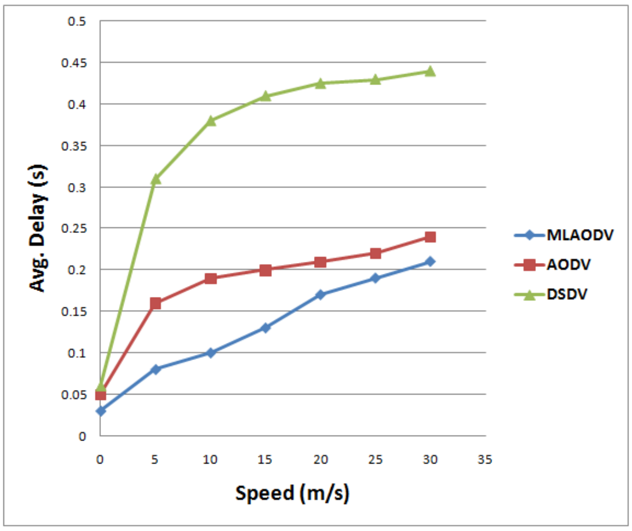

Fig 9. Speed vs delay

Routing Recovery Frequency (RRF) and **Normalized Routing Load (NRL)**: RRF represents the frequency at which route lookup procedures are launched. NRL refers to the aggregate count of routing packets sent in order to facilitate the successful delivery of individual data packets. A packet's transition across the network is represented by one hop.

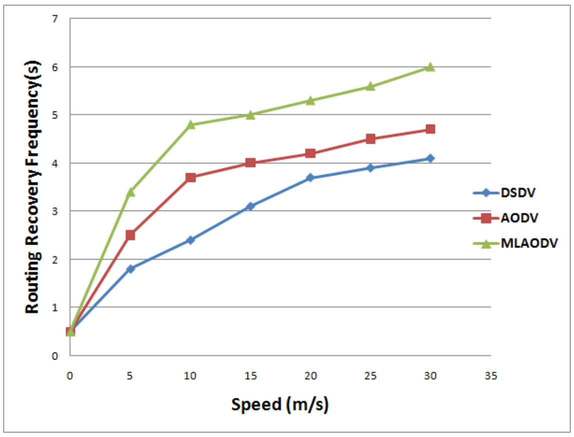

Fig 10. Speed vs RRF

Figures 10 and 11 provide a comparative analysis of RRF and NRL. The simulation findings indicate that there is a closeness to the average latency. The simulation findings provide further confirmation that the AODV protocol is specifically intended to promptly adapt to changes in network topology. This protocol exhibits a high degree of flexibility in terms of routing and managing mobile nodes. However, it does not priorities the stability of the route. When the node undergoes rapid movement, the topology experiences swift changes, leading to frequent initiation of the Route Discovery by AODV. Consequently, this imposes a heavier load on the network.

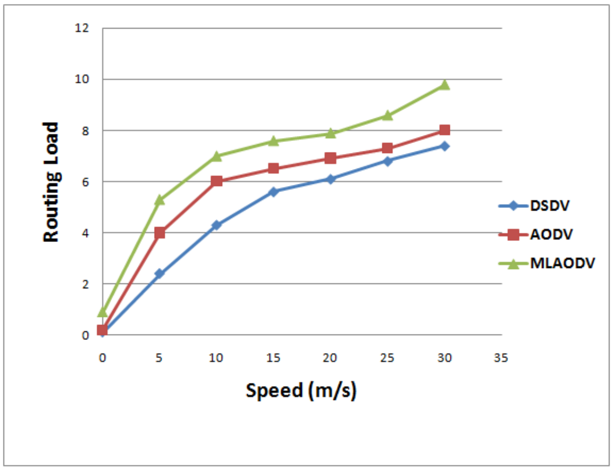

Fig 11. Speed vs NRL

Routing overhead (RO): It is the ratio of the number of control/routing packets to the total number of packets. The figure 12 illustrates the change in RO across various nodes, with the ML-AODV exhibiting lower overhead compared to the AODV and DSDV schemes. There is a noticeable increase in the use of control packets while transitioning from 5 to 50 nodes in all three scenarios. Moreover, ML-AODV demonstrates reduced RO compared to AODV techniques, particularly in scenarios with increased node density. The reason for this phenomenon may be attributed to the use of trust estimate for the selection of relay nodes, as well as the incorporation of the AAN model inside the ML-AODV framework.

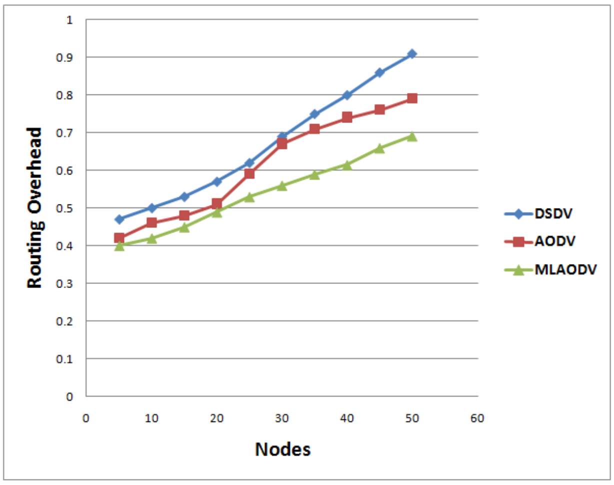

Fig 12. Nodes vs Routing overhead

Packet Lost Rate(PLR) : It refers to the sum of all packets that were lost while running the simulation. PLR are ones that were transmitted from the source but were never received by the destination. It is determined by subtracting the total number of packets transmitted from the total number of packets lost during the routing process.

The figure 13 illustrates the fluctuation in packet loss over various node densities in both the ML-AODV protocol, which is being proposed, and the current AODV and DSDV protocols. There is a perception that there is an increase in packet loss when there is a change in node density in ML-AODV and other current techniques. In contrast, ML-AODV demonstrates a reduction of 12% in packet loss compared to current systems while operating in environments with increased node density.

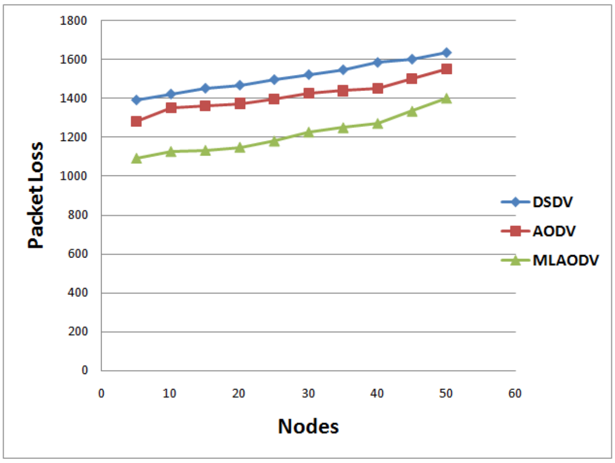

Fig 13. Nodes vs packet loss

Throughput (TP) : It is defined as the rate at which a certain amount of data may be sent across a given communication channel and arrive at its intended destination. The rate of successful receptions is calculated for a certain simulation period. Higher throughput values indicate a safer and more efficient network.

The figure 14 shown depicts the comparative performance of ML-AODV, DSDV, and AODV in relation to throughput, specifically in response to variations in node density. Moreover, ML-AODV demonstrates a greater TP compared to already used techniques. The reason for this may be attributed to the use of trust-based selection of relay nodes and the incorporation of the AAN model into the current AODV protocol.

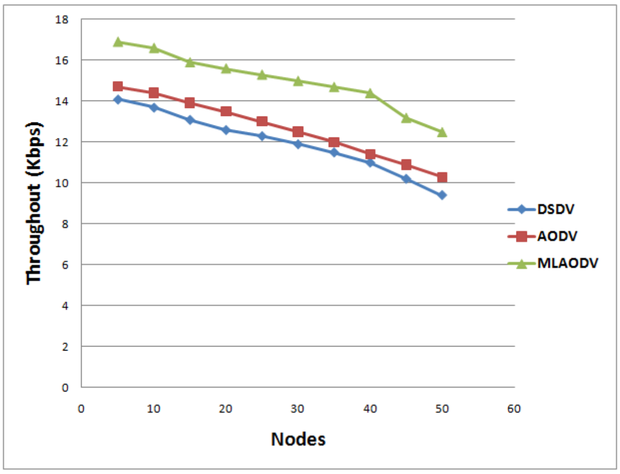

Fig 14. Nodes vs TP

Reliability: The rate at which data packets are received after being sent is the reliability.

The data shown in the figure 15 indicates that the success rate of receiving data packets relative to the number of packets delivered is greater when using ML-AODV compared to AODV, across various node densities. Moreover, it is apparent that ML-AODV exhibits a greater level of dependability compared to the already used methods. This result is due to the introduction of a unique relay selection method and ANN model for packet routing in the context of ML-AODV.

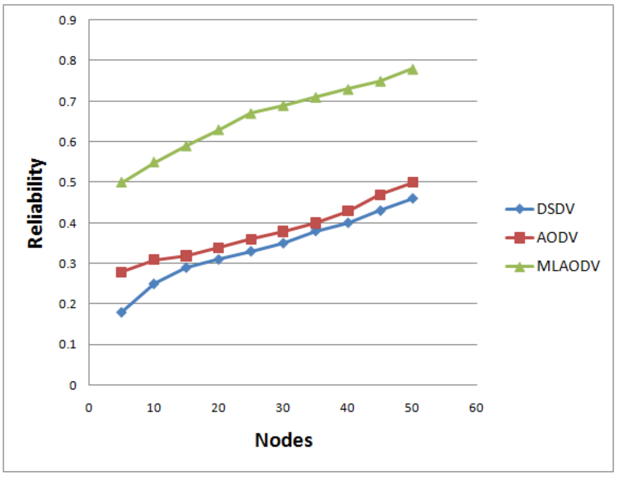

Fig 15. Nodes vs Reliability

Energy Consumption (EC) : The mean amount of power used by mobile nodes for routing and data transmission.

In figure 16, it can be seen that ML-AODV exhibited a higher energy consumption for medium estimate MANETs, which subsequently decreased for bigger MANETs. Conversely, DSDV demonstrated a comparatively lower EC for small, medium, and larger MANETs.

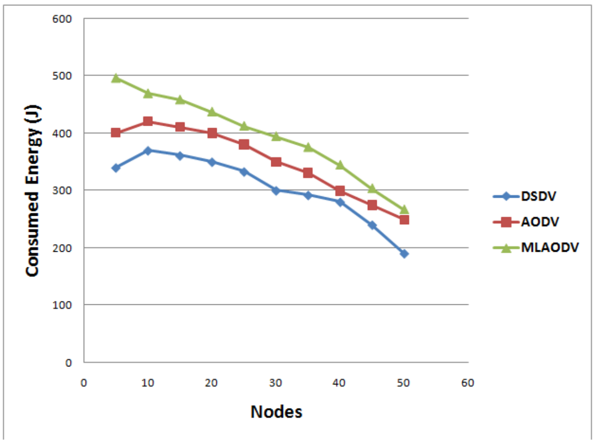

Fig 16. Nodes vs Energy

7. Conclusion

The introduction of security measures in MANETs is a significant problem due to the dynamic nature of their architecture. In order to mitigate security risks, many security methodologies have been suggested in scholarly literature. Machine learning approaches have gained popularity among researchers due to their potential in identifying previously overlooked or unknown hazards. This study provides a complete categorization of security measures in MANETs that are based on ML algorithms. Enhancing the performance of routing protocols and improving the overall performance of MANETs has emerged as a significant area of research and discussion. This is particularly relevant considering the prominent role of routing protocols in MANETs. The establishment of routing in the context of AODV is facilitated by the use of a mechanism known as ML. This study presents a novel approach, namely the ML-AODV scheme, which utilizes machine learning techniques to enhance the security of the AODV routing protocol in MANETs. The evaluation of the ML-AODV protocol has been conducted in comparison to the AODV and DSDV protocols, considering various node densities and speeds. The ML-AODV algorithm is evaluated using a network consisting of 50 nodes, each with a maximum speed of 30m/s. The simulation the results indicate that ML-AODV is better than both AODV and DSDV.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Goyal N and 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 pp 653.

[2] Sivapriya, N. ., Mohandas, R. ., Kumar, P. K. ., & Vaigandla, K. K. . (2023). Dissection of Mobility Model Routing Protocols in MANET on QoS Criterion. International Journal on Recent and Innovation Trends in Computing and Communication, 11(8), 357–365. https://doi.org/10.17762/ijritcc.v11i8.8030

[3] K. K. Vaigandla, "Communication Technologies and Challenges on 6G Networks for the Internet: Internet of Things (IoT) Based Analysis," *2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)*, 2022, pp. 27-31, doi: 10.1109/ICIPTM54933.2022.9753990.

[4] Karthik Kumar Vaigandla, J.Benita, "PRNGN - PAPR Reduction using Noise Validation and Genetic System on 5G Wireless Network," *International Journal of Engineering Trends and Technology*, vol. 70, no. 8, pp. 224-232, 2022. https://doi.org/10.14445/22315381/IJETT-V70I8P223

A. Arya and J. Singh, “Comparative Study of AODV , DSDV and DSR Routing Protocols in Wireless

Sensor Network Using NS-2 Simulator," vol. 5, no. 4, pp. 5053–5056, 2014.

[5] M. Manjunath and D. H. Manjaiah, "Performance Comparative of AODV, AOMDV and DSDV Routing Protocols in MANET Using NS2 Alamsyah1,2," *Int. J. Commun. Netw. Syst.*, vol. 004, no. 001, pp. 18–22, 2018, doi: 10.20894/ijcnes.103.004.001.005.

[6] M. G. K. Alabdullah, B. M. Atiyah, K. S. Khalaf, and S. H. Yadgar, "Analysis and simulation of three MANET routing protocols: A research on AODV, DSR & DSDV characteristics and their performance evaluation," *Period. Eng. Nat. Sci.*, vol. 7, no. 3, pp. 1228–1238, 2019, doi: 10.21533/pen.v7i3.717.

[7] Salam, T. and Hossen, M., 2020. Performance analysis on homogeneous LEACH and EAMMH protocols in wireless sensor network. Wireless Personal Communications, 113(1), pp.189-222. https://link.springer.com/article/10.1007/s11277-020-07185-6

[8] Hossen, M., 2019. DTN routing protocols on two distinct geographical regions in an opportunistic network: an analysis. Wireless Personal Communications, 108(2), pp.839-851. https://link.springer.com/article/10.1007/s11277-019-06431-w.

[9] AL-Dhief, F.T., Sabri, N., Salim, M.S., Fouad, S. and Aljunid, S.A., 2018. MANET routing protocols evaluation: AODV, DSR and DSDV perspective. In MATEC web of conferences (Vol. 150, p. 06024). EDP Sciences.

[10] Singh, R.K. and Nand, P., 2016, April. Literature review of routing attacks in MANET. In 2016 International Conference on Computing, Communication and Automation (ICCCA) (pp. 525-530). IEEE.

[11] Singh, U., Samvatsar, M., Sharma, A. and Jain, A.K., 2016, March. Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol. In 2016 Symposium on Colossal Data Analysis and Networking (CDAN) (pp. 1-6). IEEE.

[12] Kamel, M.B.M., Alameri, I. and Onaizah, A.N., 2017, March. STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET. In 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (pp. 1278-1282). IEEE.

[13] Deshmukh, S.R., Chatur, P.N. and Bhople, N.B., 2016, May. AODV-based secure routing against blackhole attack in MANET. In 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 1960-1964). IEEE.

[14] Talukdar, M.I., Hassan, R., Hossen, M.S., Ahmad, K., Qamar, F. and Ahmed, A.S., 2021. Performance improvements of AODV by black hole attack detection using IDS and digital signature. Wireless Communications and Mobile Computing, 2021. https://www.hindawi.com/journals/wcmc/2021/6693316/

[15] T. H. Sureshbhai, M. Mahajan, and M. K. Rai, "An investigational analysis of DSDV, AODV and DSR routing protocols in mobile Ad Hoc networks," *Proc. - 2nd Int. Conf. Intell. Circuits Syst. ICICS 2018*, pp. 286–289, 2018, doi: 10.1109/ICICS.2018.00064.

A. Hariharan, A. Gupta and T. Pal, "CAMLPAD: Cybersecurity Autonomous Machine Learning Platform for Anomaly Detection," *Proc. Future of Information and Communication Conference (FICC), San Francisco, CA, USA*, pp. 705-720, 2020.

[16] S. El Khediri, N. Nasri, A. Benfradj, A. Kachouri, and A. Wei, "Routing protocols in MANET: Performance comparison of AODV, DSR and DSDV protocols using NS2," *2014 Int. Symp. Networks, Comput. Commun. ISNCC 2014*, 2014, doi: 10.1109/SNCC.2014.6866519.

[17] B. Paul, K. A. Bhuiyan, K. Fatema, and P. P. Das, "Analysis of AOMDV, AODV, DSR, and DSDV routing protocols for wireless sensor network," *Proc. - 2014 6th Int. Conf. Comput. Intell. Commun. Networks, CICN 2014*, pp. 364–369, 2014, doi: 10.1109/CICN.2014.88.

[18] Routray, S.K., Sharmila, K.: Routing in dynamically changing node location scenarios: A reinforcement learning approach. In: 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), pp. 458–462. IEEE, (2017). https://doi.org/10.1109/AEEICB.2017.7972354

[19] Khan, F., Memon, S., Jokhio, S.H.: Support vector machine based energy aware routing in wireless sensor networks. In: 2016 2nd International Conference on Robotics and Artificial Intelligence (ICRAI), pp. 1–4. https://doi.org/10.1109/ICRAI.2016.7791218

[20] Troia, S., Rodriguez, A., Mart´ın, I., Hern´andez, J.A., De Dios, O.G., Alvizu, R., Musumeci, F., Maier, G.: Machine-learning-assisted routing in sdn-based optical networks. In: 2018 European Conference on Optical Communication (ECOC), pp. 1–3. https://doi.org/10.1109/ECOC.2018.8535437

[21] Hu, T., Fei, Y.: An adaptive and energy-efficient routing protocol based on machine learning for

underwater delay tolerant networks. In: 2010 IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, pp. 381–384. https://doi.org/10.1109/MASCOTS.2010.45

[22] Vaigandla, Karthik Kumar and Benita, J. ‘Selective Mapping Scheme Based on Modified Forest Optimization Algorithm for PAPR Reduction in FBMC System’. Journal of Intelligent & Fuzzy Systems, vol. 45, no. 4, pp. 5367-5381, October 2023, DOI: 10.3233/JIFS-222090.

[23] Vaigandla, K. K. ., & Benita, J. (2023). A Novel PAPR Reduction in Filter Bank Multi-Carrier (FBMC) with Offset Quadrature Amplitude Modulation (OQAM) Based VLC Systems. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(5), 288–299. https://doi.org/10.17762/ijritcc.v11i5.6616

[24] Karthik Kumar Vaigandla and J.Benita (2022), Novel Algorithm for Nonlinear Distortion Reduction Based on Clipping and Compressive Sensing in OFDM/OQAM System. IJEER 10(3), 620-626. https://doi.org/10.37391/IJEER.100334.

[25] Shrestha, S., Baidya, R., Giri, B. and Thapa, A., 2020, March. Securing blackhole attacks in MANETs using modified sequence number in AODV routing protocol. In 2020 8th International Electrical Engineering Congress (iEECON) (pp. 1-4). IEEE.

[26] Su, M.Y., 2011. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Computer Communications, 34(1), pp.107-117.

[27] Sargunavathi, S. and Martin Leo Manickam, J., 2019. Enhanced trust based encroachment discovery system for Mobile Ad-hoc networks. Cluster Computing, 22(2), pp.4837-4847.

[28] Li, J.S. and Lee, C.T., 2006. Improve routing trust with promiscuous listening routing security algorithm in mobile ad hoc networks. Computer communications, 29(8), pp.1121-1132.

[29] Kumar, P., Tripathi, S. and Pal, P., 2018, March. Neural network based reliable transport layer protocol for MANET. In 2018 4th International Conference on Recent Advances in Information Technology (RAIT) (pp. 1-6). IEEE.

[30] Arthur, M.P., 2018, September. An SVM-based multiclass IDS for multicast routing attacks in mobile ad hoc networks. In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 363-368). IEEE.

[31] Garc´ıa, S., Ram´ırez-Gallego, S., Luengo, J., Ben´ıtez, J.M., Herrera, F.: Big data preprocessing: methods and prospects. Big Data Analytics 1(1), 1–22 (2016). https://doi.org/10.1186/s41044-016-0014-0

[32] Buiati F, Puttini R, de Sousa R, Abbas C J B, Villalba L J G 2004 Authentication and Auto configuration for MANET Nodes 2004 Embedded and Ubiquitous Computing EUC 2004 Lecture Notes in Computer Science 3207 Springer.

[33] Capkun S, Buttya L and Hubaux J P 2003 Self-Organized Public-Key Management for Mobile Ad Hoc Networks IEEE Transactions on Mobile Computing 2.

[34] N. F. Rozy, R. Ramadhiansya, P. A. Sunarya, and U. Rahardja, “Performance Comparison Routing Protocol AODV, DSDV, and AOMDV with Video Streaming in Manet,” *2019 7th Int. Conf. Cyber IT Serv. Manag. CITSM 2019*, 2019, doi: 10.1109/CITSM47753.2019.8965386.

[35] M. Y. and E. A., “Comparative Analysis of Routing Protocols AODV DSDV and DSR in MANET,” *Ijarcce*, vol. 5, no. 12, pp. 470–475, 2016, doi: 10.17148/ijarcce.2016.512107.

[36] N.Sivapriya et al. (2019). A framework for Fuzzy-based Fault Tolerant Routing mechanism with Capacity Delay Tradeoff in MANET. *International Journal of Advanced Science and Technology*, *28*(17), 420 - 429. http://sersc.org/journals/index.php/IJAST/article/view/2281

[37] N.Sivapriya, and T.N.Ravi “Efficient Fuzzy based Multi-constraint Multicast Routing with Multi-criteria Enhanced Optimal Capacity–Delay Tradeoff”, International Journal of Scientific & Technology Research, vol.8, issue no. 8, pp. 1468-1473, ISSN 2277-8616, August 2019.

[38] Dr.R.Mohandas, Dr.N.Sivapriya, “TSP implementation for MANET using NS2”, NeuroQuantology, Volume 20, Issue 10, Page 847-854, ISSN 1303-5150, August 2022.

[39] Mohandas, R., Krishnamoorthi, K. & Sudha, V. Energy Sensitive Cluster Level Security Selection Scheme for MANET. Wireless Pers Commun 105, 973–991 (2019). https://doi.org/10.1007/s11277-019-06131-5