Enhancing Congestion Control and QoS Scheduling Using Novel Rate Aware-Neuro-Fuzzy Algorithm in MANET

S. MOHAN[1*], P. VIMALA[2]
[1*]Department of Electronics and Communication Engineering, FEAT, Annamalai University, Annamalai Nagar, Chidambaram, Tamil Nadu, INDIA.
[2]Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, Annamalai University, Annamalainagar-608 002, INDIA.

Abstract: Mobile Ad Hoc Networks (MANET) provides a vibrant atmosphere wherein data may be substituted deprived of the necessity of human authority or a centralized server, as long as nodes work together for routing. As long as security throughout the multipath routing protocol and data transfer over many routes in a MANET is a difficult problem, this work offers a message security technique. This study presents the congestion control and QoS scheduling mechanism. The goal of this study is to examine standardized MAC protocols on MANET, to measure performance under various node densities and MAC protocols. Initially, this work presents the Centralized Congestion Detection method to detect congestion with baseline parameters. Accordingly, the congestion is avoided using Novel Rate Aware-Neuro-Fuzzy based Congestion Controlling strategy. This method effectively controls the congestion in the Network. This mechanism has been proposed which defines three levels of congestion based on which the data rate, throughput, overhead and delay. However, after controlling the congestion, the optimal routes are given to the packets by proposing an Ambient Intelligence-based Ant colony optimization quality-aware energy routing protocol (AIACOAR). This method finds the most efficient route to a destination and decreases the time and energy required. Accordingly, for securing the network against malicious attacks, an Elliptic Curve Cryptography (ECC) encryption mechanism is presented. Consequently, the multihop scheduler performs QoS-based scheduling in MANET. Schedulers in MANET take into account various QoS parameters such as end-to-end packet delay, packet delivery ratio, flow priority, etc. The proposed method is implemented using Matlab software, and the evaluation metrics are PDR, jitter, congestion detection time, delay, route selection time, and throughput. The performance of the proposed method is compared to the existing AIFSORP and LF-SSO techniques. While compared to these methods, the proposed method's performance is improved in terms of PDR, delay, throughput, etc. The PDR value of the proposed method reaches approximately 99%, and it produces a very low delay. This produces reliable route discovery, optimized congestion control, and better QoS scheduling, therefore, these improve the system performance. In future, a recent bio-inspired technique is presented to even more minimize energy consumption and further improve the system's performance.

Keywords: MANET, MAC Protocols, Congestion Control, Routing, QoS Scheduling, Elliptic Curve Cryptography, Ambient Intelligence, and Ant Colony Optimization.

Received: May 25, 2022. Revised: May 11, 2023. Accepted: June 20, 2023. Published: July 20, 2023.

1. Introduction

Mobile Ad-hoc Networks (MANET) are very enticing for cutting-edge applications. The creation of a MANET network is fraught with several issues and difficulties. End-systems will acquire information about each used path, including its capabilities, delay, and congestion condition, at the transport layer. The traffic will then be diverted away from engorged techniques as a result of this information responding to network congestion occurrences. MANET are infuriatingly stunning components for modern apps. Because of the active topological structure and node modification on location every second in MANET, congestion is one of the ongoing difficulties. In MANET,

a sender node must broadcast an initial broadcast routing packet over the network and locate the destination through the shortest or minimal intermediary hop if it has to relay information to the specified receiver [1] [2]. The dynamic implementation of efficient collision avoidance and resolution techniques is necessary for the creation of efficient contention-based Medium Access Control (MAC) protocols for mobile wireless ad hoc networks [3].

To maximize channel use and maintain the quality of service (QoS) for every node, a multi-hop scheduler plans transmissions [4]. Due to the numerous characteristics of MANET that result in distinctive queuing dynamics, QoS-based scheduling in these networks must be achieved under time-critical circumstances. In MANET, schedulers take into account a variety of QoS factors, including flow priority, end-to-end packet delay, and packet delivery ratio. Additionally, scheduling in MANET can be fair, opportunistic, distributed priority, etc. [5]. Due to real-time content delivery in online games and video conferences, multimedia traffic has sharply increased during the past ten years. In some situations, MANET is essential to everything being hyperconnected in multimedia services. A new scheduling method based on the connectivity of context-aware mobile nodes is used in [6].

The most significant and difficult concepts in ad-hoc networks currently are routing, reliability improvement, load balancing, and congestion control. Every node will perform routing to send both its messages and those of the other nodes. All nodes function as routers. It has long been recognized for these reasons that mobile nodes use more energy than wired nodes [7]. Due to the various utility of routing in the MANET, there are some limitations on bandwidth and communication range. These limitations are making routing and data transfer more difficult, in addition to the dynamic network structure. Due to these issues, traditional approaches are ineffective, particularly when it comes to traffic regulation and congestion [8]. Therefore, it is necessary to suggest fresh ideas for these kinds of networks. To reduce congestion and balance the beneficial loads on the routes, multipath routing based on the original protocol Ad-Hoc On-Demand Multipath Distance Vector (AOMDV) is introduced [9]. Nodes constantly alter the network by using their mobility characteristic to construct new paths between themselves. A fuzzy Logic System is utilized in intermediate and destination nodes as a dynamic tool to control the congestion problem in MANET in a cross-layer strategy that spans the transport, network, and MAC layers. The DSR routing algorithm is utilized at the network layer, and messages sent back and forth between nodes are contained in ACK packets. [10]

Due to its effectiveness in overcoming the specific drawbacks of single-route routing, multipath routing technology is widely used in MANET. However, achieving energy-effective secure MR is a huge issue in MANET due to the lack of trusted centralized authority and also insufficient resources. The secret key-centred hybrid honey encryption technique is used to protect the DPs from data transfer (DT) assaults to overcome these difficulties. To find the best way out of the multipath chosen, the levy flight-centred shuffled shepherd optimization algorithm is then used [11]. LEACH protocol, in which the CHs and CMs are fixed for data transport in the network, is recommended for node clustering. To prevent battery depletion and network failure, the energy is distributed through the LEACH. Also, the DoS Pliancy Algorithm is used for acknowledgement-based flooding assaults [12]. Congestion State prediction algorithm (CSPA) based on cross-layered routing architecture is introduced in [13]. CSPA aids in differentiating between packet loss brought on by link failure and random packet loss. Since the packet outlet directive operates sequentially at the node, current group, and all preceding group levels.

By performing the default network nodes in Network Simulator NS2.35 with the AODV and DSR routing techniques, congestion control AODV was used to control congestion. As a result, the performances are better in terms of packet delivery ratio and throughput [14]. Equipping each device to keep the data necessary for appropriate traffic routing is the

main problem facing the MANET. MANET can be studied in a variety of methods, for as by using simulation tools like OpNet, NetSim, or NS2 [15]. "A Novel Method for Avoiding Congestion in a Mobile Ad Hoc Network for Maintaining Service Quality in a Network" In this title, under the mobile ad-hoc network system, the main reason for causing congestion is the limited availability of resources. The rest of the work is organized as follows, section 2 portrays the literature survey of the work, section 3 illustrates the problem definition and motivation, and section 4 demonstrates the proposed research methodology. Section 5 reveals the experimentation and result discussion, and the conclusion of the research is presented in section 6.

2. Literature Survey

The MANET network is an autonomous, self-organizing system that doesn't rely on any pre-existing infrastructure. It is a wireless network with interconnected devices. Congestion is the network's main issue because it is wireless. The network's high volume of traffic (packets) is the cause of this congestion. A routing technique called Congestion Control AODV is introduced in addition to Sumathi, *et al* [16] proposed congestion control by simulating default network nodes using Network Simulator NS2.35 with the Routing Technique of AODV and DSR. As a result, the final result shows the viability and improved performance in packet delivery ratio and throughput from this proposed work. To determine the least congested way, the cross-layer protocol and evolutionary game theory technique were developed by Thanappan, *et al* [17]. To prevent congestion, cross-layering in MANET uses the transport layer and MAC layer. One evolutionary game theory method used to identify the Least Congested Node is Linear Rank Selection. According to simulations, the proposed protocol performs better than the GPSR protocol.

Researchers have focused on coming up with superior methods for operating the likelihood of MANET. It is now possible to use machine learning techniques to prepare artificial intelligence to increase the most effective strategies for this function. It is suggested in [18] to use Machine Learning-based Efficient Clustering and Improve QoC in MANET. In this study, the clustering method enhances the QoS considerations for selecting Cluster Heads. Even if the streaming protocols were correctly created, media transfer or streaming would be nearly impossible if QoS criteria were not applied. Classes for QoS Scheduling aid in managing packet priorities and streamlining network traffic. The analysis of QoS scheduling classes using video traffic in a MANET is presented in [19]. It is advised to utilize the ertPS scheduling class in MANET where QoS consideration is of the utmost importance, notably in multimedia streaming applications. The DE route method is designed for secure communication in the Internet of Things architectures with mobile, ad-hoc Internet of Things nodes. The Diffie-Hellman key exchange technique generates secret keys that are used to encrypt the node's addresses to prevent the route list from being modified [20]. To identify secure nodes, the fuzzy system with trust parameters, such as historical, indirect, and direct trust factors, is taken into consideration.

The test score examines both trusted and untrusted nodes from the source initially to find the best route for packet transmission in MANET. An adaptive trust-based secure and optimal route selection utilizing a hybrid fuzzy optimization model was presented by Ravi *et al* [21] based on the trusted nodes. An Advanced Encryption Standard based on an Adaptive Chaotic Grey Wolf Optimization algorithm delivers secure communication after the Fuzzy Butterfly Optimization Algorithm is used to find the best routes. In MANET and cloud systems, security is crucial for preventing damaging assaults. Therefore, a MANET using cloud-based 5G communications needs a trusted environment. To defend the network from attackers, Alghamdi [22] provided a brand-new framework in this study termed the trust-aware intrusion detection and prevention system (TA-IDPS). A MANET, a cloudlet, and a cloud service layer make up TA-IDPS. Utilizing well-known measures, the

effectiveness of the proposed TA-IDPS and earlier techniques is examined.

Satyanarayana, *et al* [23] used a key-based safety feature identification mechanism in conjunction with trust ratings. To improve communication security, this study also identifies three categories of trust ratings, including direct, indirect, and overall trust scores. A cluster-based secured routing system chooses the head of a cluster from among the nodes based on QoS metrics and trust ratings. The final path that must be chosen to carry out the safe routing operation as effectively as feasible depends on path trust, energy consumption, and hop number. Vinayakan, *et al* [24] proposes a message security technique that combines multipath Ad hoc on Demand Multipath Distance Vector (AOMDV) routing established on trust with soft encryption in MANET, resulting in the Trust based Ad hoc on Demand Multipath Distance Vector (T-AOMDV) protocol. Security throughout the multipath routing protocol and data transfer over many routes in a MANET remain challenging problems. Simulation results utilizing ns2 show that the system is much more secure than conventional multipath routing algorithms. In [25], the Hybrid Genetic Fuzzy Neural Network (HGFNN) technology was developed to create an energy-efficient routing protocol and cross-layer congestion detection system. This protocol detects the type of event occurring when a networking event occurs to handle it appropriately. Throughput is intended to be increased by reducing energy consumption, transmission latency, and packet delivery ratio. The effectiveness of the suggested solution is determined by evaluating its performance in a network simulator in terms of energy consumption, transmission delay, and packet delivery ratio.

3. Research Problem Definition and Motivation

Packet drop occurs due to congestion-related issues like limited bandwidth, link failure and interference also misbehaving node drops the packet to harm the network. Differentiating packet loss due to congestion or malicious node is a tedious job. Securing mobile nodes from attackers has become one of the crucial aspects of providing QoS since nodes are weak to different kinds of attacks and threats that impact network connectivity and functionality. Congestion occurs in MANET which has a limited number of resources. Interference and fading are experienced during packet transmission in these networks because of the shared wireless channel and dynamic topology. Congestion results in packet victims and bandwidth degradation; as a result, time and energy are wasted while recovering from it. When using a congestion-aware protocol, it is possible to avoid congested areas by bypassing the affected links. Congestion-related problems such as severe throughput degradation and massive fairness issues have been identified, among other things. These issues arise at the MAC, protocol routing, and transport layers, among other levels of the protocol stack.

Congestion Control (CC), as the core networking task to efficiently utilize network capacity, received great attention and is widely used in various Internet communication applications such as 5G, Internet-of-Things, UAN, and more. A range of measures has been suggested to alleviate congestion in MANET. MANET efficiency must be improved to ensure data transmission to the respective destination, especially safety messages. Managing data in MANET has many problems and difficulties wherein congestion control has evolved as a prominent field of study. The benefits of using data congestion management for MANET include reduced end-to-end delay, enhanced reliability, and packet delivery ratio. To reduce energy consumption and end-to-end delay while simultaneously improving packet delivery ratio and throughput, the suggested architecture makes use of the cross-layer idea. Security and QoS targets may not necessarily be similar but this framework seeks to bridge the gap for the provision of an optimal functioning MANET. The framework is evaluated for throughput, jitter, and delay against a sinkhole and malicious attack presented in the network.

4. Proposed Research Methodology

Congestion in the network is not only the cause of unnecessary data but there may be other factors such as contention, link failure, and interference. Congestion in the network increases the packet loss ratio, delays, and degrades the overall network performance. One of its greatest challenges is ensuring Quality of Service (QoS) owing to channel sharing, high traffic and topology changes in MANET. Congestion control should be properly considered to improve the network performance and transmission of messages over MANET. However, there seem significant limitations to most of the other current congestion control mechanisms. There are many problems and challenges in coming up with a MANET network. Congestion is one of the live challenges in MANET because of the active topology structure and node amendment each second on its position.

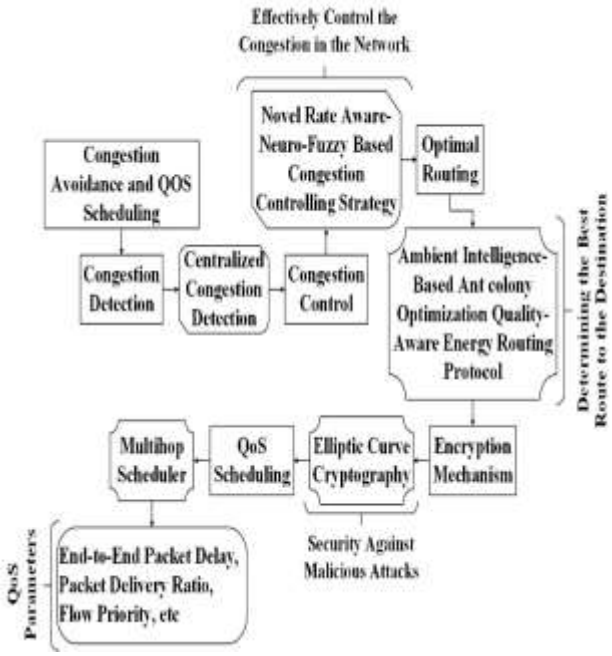

Figure 1: Flow Diagram of the Proposed Work

Figure 1 depicts the workflow diagram of the research work. The goal of this study is to examine standardized MAC protocols on MANET, to measure performance under various node densities and MAC protocols. Because of the ubiquitous deployment of MAC protocols for MANET, it is vital to evaluate them from the perspective of the transport layer, which benefits from the advantage of decisive data transmission over the Internet. The nodes have limited bandwidth and processing capability. The routing protocols cannot handle the congestion due to the heavy load in mobile ad hoc networks. Several routes are established in the network, and some intermediate nodes are common. The routing protocol establishes the connection between the sender and the receiver. The efficient routing approach uses the concept of load balancing to reduce packet loss in a network. In this paper, an enhanced congestion control model and QoS scheduling scheme is proposed. QoS scheduling makes decisions about the assignment of resources and services to the nodes at a current time.

MAC Layer: Medium Access Control (MAC) Algorithms are used to let several users share a single communication channel at the same time to maximize channel utilization while minimizing conflict and collisions. MAC is comparable to highway traffic restrictions. For example, on a highway, numerous vehicles may cross the same road at the same time, but there are laws in place to prevent collisions, such as following traffic lights and constructing flyovers. Layer 1 of the OSI reference model is the Data Link Control layer, and layer 2 is the MAC. The Media Access Control layer and the Logical Link Control (LLC) layer make up Layer 2. The DLC's job is to create a secure point-to-point or point-to-multipoint connection between two or more devices over wired or wireless media.

4.1 Congestion Control

Cross-layer involves the transport layer and MAC layer of MANET to avoid congestion. In this research, Centralized Congestion Detection and a Novel Rate Aware-Neuro-Fuzzy based Congestion Controlling strategy in MANET is utilized. In this work, a rate-aware and centralized Congestion Detection is employed to detect congestion with baseline parameters like queue size, channel occupancy against the capacity, and utilization rate. Besides the congestion detection, the Novel Rate Aware-

Neuro-Fuzzy based Congestion Controlling strategy is employed to avoid negative impacts to the maximum extent. The Rate Aware defines three levels of congestion based on which the data rate, throughput, overhead and delay, which effectively control the congestion in the Network. The MAC layer is responsible for accessing the communication channel. At MAC, a control channel is used in the selection of collision-free paths for data transfer.

4.1.1 Centralized Congestion Control

Centralized Congestion Control approaches assume a central controller such as RSU to control the signal parameters and path information to guide the vehicles. The RSUs and OBUs direct all DSRC-connected vehicles to provide on-demand information about the ongoing network traffic such as speed, position, acceleration, braking status, etc. of the neighbouring vehicles. Centralized approaches are easier to implement because they incur less overhead in routing connectivity.

In this paper, a distributed congestion avoidance scheme is selected, rather than employing centralized servers and/or road-side infrastructure. Also, consider a reactive mechanism (i.e., request/reply) rather than a system that relies on all-out periodic broadcasts.

There are several advantages of centralized congestion avoidance algorithms. First, a centralized server can have more complete knowledge of its realm, assuming it can receive and hold information originating from anywhere on the map. This may help deduce more accurate navigation decisions, especially over longer distances. Second, centralized methods do not require vehicles to have computation power and full knowledge of the map. They can share very little information with a vehicle (e.g., an optimal route to the intended destination), as opposed to continuous reports of congestion levels.

4.1.2 Novel Rate Aware-Neuro-Fuzzy based Congestion Controlling Strategy

In this section, the Rate aware congestion control mechanism (RACC) mechanism has been proposed in the phases namely the detection/management phase. The details of this phase are explained below:

Detection and Management Phase

In this phase, the buffer management strategy is incorporated to reduce traffic congestion. Generally, the mobile nodes communicate with their upstream and downstream nodes. The role of mobile nodes is to get the traffic from the upstream and forward the same to the downstream node. To prevent the nodes from congestion, the issue of congestion can be easily eliminated. Congestion is predicted in time 'C_t' (when several mobile connections are 10) for buffer management strategy.

Even SN computes the number of packets received from its upstream and the number of packets forwarded to its downstream SNs. The threshold value of buffer size (BS_i) for any i^{th} node is half of its original size. Original buffer size (BS_o). In the detection phase, if the value of the congestion index (CI_i) at i^{th} node is greater than BS_i but less than BS_o, then it is considered that the congestion is at the intermediate level and therefore, the value of CI is lowered by reducing the date rate (DR) of traffic by 2%. This state of congestion is called an intermediate load state. On the other hand, if the value of traffic is equal to BS_i, then means that there is very less congestion. In this case, the value of CI is lowered by reducing the DR by only 1%. This state is known as a low-congestion state. Alternatively, if the value of CI is greater than BSo, then it is considered to be an alarming state also known as buffer overflow. Therefore, the DR is reduced to 3% of its current data rate. Thus, in this way congestion amid nodes can be considerably reduced or managed.

C_{t+1} is the time of prediction of congestion when the number of mobile connections is 15, and C_{t+2} is when the number of connections is 20 and C_{t+3} is when the number of mobile connections is 25. CI is an index value that is computed based on the number of packets a buffer can hold. The value of CI is less than BS_i (number of mobile connections less than 10), it means that there is no congestion and the traffic flow is normal. Therefore, based on observations, the RACC mechanism is

triggered to mitigate the congestion phenomenon.

Neuro-Fuzzy Based Congestion Control Mechanism

A fuzzy system is made of a fuzzifier, a defuzzifier, an inference engine, and a rule base as shown in figure 2. The role of the fuzzifier is to map the crisp input data values to fuzzy sets defined by their membership functions depending on the degree of "possibility" of the input data. The goal of the defuzzifier is to map the output fuzzy sets to a crisp output value. It combines the different fuzzy sets with different degrees of possibility to produce a single numerical value. The fuzzy inference engine defines how the system should infer through the rules in the rule base to determine the output fuzzy sets.

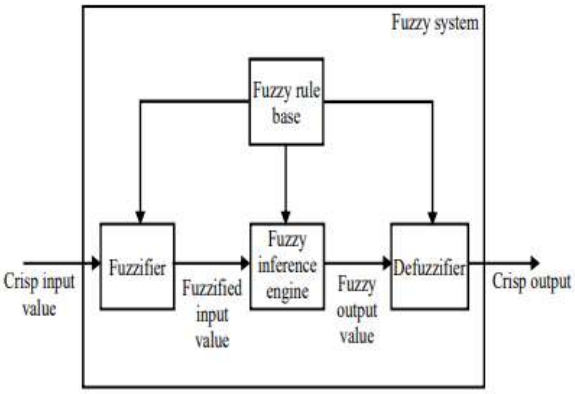

Figure 2: Flow Diagram for Fuzzy System

A binary threshold divides the buffer space into two parts. Below or equal to the threshold level, every arriving cell is given entry to the network and above the threshold, every cell is rejected. The change from entry in the network to rejection is abrupt. A gradual change is more intuitive here. This can be done with a fuzzy threshold. A typical example is given in the following section.

Neuro-Fuzzy Membership Functions

This technique enables the network for finding the shortest path of the nodes to the cluster heads and then to the sink node by applying neuro-fuzzy rules. For this purpose, the NFIS uses the triangular and trapezoidal membership functions along with a convolutional neural network to form decision rules. Moreover, the neuro-fuzzy rule system uses the fuzzy membership functions which are given in equations (1) and (2).

$$\mu_{A1}(z) = \begin{cases} 0 & z \le a1 \\ \frac{z-p1}{q1-p1} & p1 \le z \le q1 \\ \frac{r1-z}{r1-q1} & q1 \le z \le r1 \\ 0 & r1 \le z \end{cases} \quad (1)$$

$$\mu_{A1}(z) = \begin{cases} 0 & z \le a1 \\ \frac{d2-x}{d2-r2}, & r2 \le z \le d2 \\ 1, & q2 \le z \le r2 \\ \frac{d2-x}{d2-r2} & r2 \le z \le d2 \\ 0, & d2 \le z \end{cases} \quad (2)$$

Here, the variables z and x represent the fuzzy and actual distances in which the fuzzy distance value is measured using the membership functions.

The last step in the fuzzy rule-based inference process is the de-fuzzification step. To obtain the crisp output value corresponding to the fuzzy values, the de-fuzzification step has been applied in this work. Among the de-fuzzification methods which are available in the literature, the Center of Area method is the most widely used method and hence this work adopted the COA method shown in (3).

$$COA = \frac{\int \mu_A(z).z\, dz}{\int \mu_A(z)\, dz} \quad (3)$$

However, utilizing this centralized congestion detection, and rate-aware neuro-fuzzy technique detects the congestion in the network and it avoids or controls the congestion in the network layer. Accordingly, after the congestion control, a secure routing process is required which is described in the following subsection.

4.2 Routing Protocol

This paper proposes the Ambient Intelligence-based Ant colony optimization quality-aware energy routing protocol (AIACOAR) to find the most efficient route to a destination and decrease the time and energy required. This quality-aware energy routing is developed

based on a cross-layer. The multipath routes are to be discovered primarily using the parameters such as delay, channel occupation, link quality and residual energy. In AIACOAR, nodes quickly notify their neighbours when they discover a possible route to their target. Only when the route meets the threshold criterion is it picked for data transmission and shared with neighbouring nodes. This method identifies the finest path among the selected relay nodes in the direction of the destination. Optimization plays a significant part in AIACOAR towards determining the best route to the destination. Subsequently, the cross-layer interaction parameter-based link residual lifetime calculation is used to assess the link's stability.

4.2.1 Ambient Intelligence Function

The ambient intelligence feature is included in AIACOAR to enhance the ant's different movement patterns (AIF). AIACOAR will employ the AIF with all ants' behaviour to avoid making abrupt turns instead of smooth turns. It is the primary goal of the AIACOAR to determine the quality of the food (i.e., route) in the immediate area and then work to raise the overall consistency of the cluster.

To account for abrupt changes in ant movement, AIACOAR uses its function (the Ambient Intelligence Function (AIF)). The AIF is utilized to map extensive routing information into a region between zero and one. The curve is created using this function, and it will be in the shape of S. As an alternative, the AIF may be used when a mathematical model can't be found. Equation (4) represents the mathematical representation of AIF.

$$AIF(i) = \frac{D}{1+h^{-i,+i}} \tag{4}$$

In equation (4), the natural logarithm is denoted as h, the maximum value of a curve is indicated as D, and i is indicated to represent an integer that falls between $-\infty$ and $+\infty$.

4.2.2 Ant Colony Optimization

In MANET, ensuring the throughput rates is important to meet the client demands with an effective QoS. Due to different plan hardships and imperative satisfaction, conventional conventions fail to address user challenges. Hence, upgrading throughput turns into a basic issue to fulfil client needs and application support. Therefore, throughput is the significant factor for rendering the required QoS for any kind of MANET application and in this research, MACO streamlining technique considers throughput as one of the factors in selecting the optimal routing path for MANET communication.

Solution Representation

In an optimization algorithm, the solution representation signifies the solution declared by the algorithm. In this research, the solution is the routing path with the source node as the initiating node or the data sender S and destination node D as the terminating node or the receiver, with the intermediating nodes $(I_1, I_2, \ldots, I_n)$ such that $(n < m)$ are the communicating nodes between the source and destination nodes.

Where, m is the total nodes in the MANET with n being the intermediate nodes in the communicating nodes.

Fitness Measure

The optimal solution, which is the optimal routing path, is decided by MACO using the fitness measures, such as throughput, PDR, routing overhead, and delay. The solution is selected as optimal when the throughput and PDR are high with minimal overhead and transmission delay.

The ACO builds the connection's packet transmission rate, bringing about a reasonable course choice arrangement. Forward "ant" is begun by the source hub at arbitrary to visit the entirety of the open hubs in the course. During their crossing, the ants leave a little amount of pheromone on the visited joins. At the point when the ants show up at their objective, the ants update the pheromone of all hubs visited all through the crossing. A hub's throughput is treated as a pheromone for this situation. The throughput work is utilized to refresh a hub's pheromone.

Equation (5) is used to calculate $f(t)$.

$$f(t) = max \sum_{i=1}^{k} \frac{p(i)}{t(i)} \tag{5}$$

Where, k denotes the packet transmission limit, $p(i)$ is the number of packets successfully transferred, and $t(i)$ denotes the packet transmission time.

An ant (A) is a collection of routes that link all nodes. MACO's fitness function shown in equation 6, also known as the objective function, is shown as follows:

$$Fitness\ of\ ant = \sum_{i=1}^{n-1} d(i,j) \qquad \forall j = n \wedge j = i + 1 \tag{6}$$

The pheromone is updated cyclically during each traversal of a link l. Equation 7 is used to calculate the likelihood of an ant 'm' visiting node 'j' from node i.

$$\rho_{ij}^{d}(t) = \frac{[\tau_{ij}(t)]^{\alpha}.[\mu_{ij}(t)]^{\beta}.[e_j(t)]^{\gamma}}{\sum_{j\in N}[\tau_{ij}(t)]^{\alpha}.[\mu_{ij}(t)]^{\beta}.[e_j(t)]^{\gamma}} \tag{7}$$

The pheromone concentration in link ij is τ_{ij}, e_j is the energy of the node, control parameters are α, β, and γ, and the throughput heuristic value μ_{ij} is $f(t)$. Equation 8 is used to calculate the pheromone concentration as it decreases over time.

$$\tau_{ij} = (1-\rho) * \tau_{ij} + \sum_{n=1}^{m} \Delta_{ij}^{n} \tag{8}$$

Where, Δ_{ij}^{n} is the change in pheromone amount in the link ij, updated by the mth ant, and $(1-\rho)$ is a decreasing pheromone constant. The following generation of ants migrates to their goal via increasing pheromone concentration nodes.

This cycle has proceeded until the state of stagnation is satisfied. The street that arises after a time of balance is viewed as the best way for correspondence. This methodology is done for every information transmission. This progression flags the beginning of the organization's transmission interaction.

Alternate Path Building by ACO

If the network concentration is scarce all the above schemes are avoided to save unwanted energy consumption. The simple ACO is considered and the shortest path is formed by the high concentration pheromone value of ANTS.

4.2.3 Quality Aware Energy Routing Protocol

A good link quality metric should (i) accurately represent the quality of the physical channel; (ii) be sensitive to gradual changes in the link quality (such as mobility); (iii) not be sensitive to the temporary changes in the link quality (such as fading); and (iv) not be sensitive to the link load. Denoting the SNR value of the n^{th} a packet sent by node A by $S_{n,A}$, the Smoothed SNR (SSNR) value to node A can be formulated as

$$SSNR_{n,A} = \sum_{i=0}^{n} \alpha(1-\alpha)^{n-i} S_{i,A} \tag{9}$$

Where, α is a parameter between 0 and 1. The larger the α value, the more sensitive the SSNR is to the current SNR. By using this exponential averaging, each SNR sample gradually loses its influence on the current SSNR value as newer packets from the same source arrive.

Route Selection Mechanism

During the route discovery process, the source node broadcasts the Route Request packet (RREQ) which also includes an additional 32-bit Route Quality (RTQ) field in the packet header. Upon receiving the RREQ, a node updates the RTQ in the packet header with its current SSNR if it is the first node receiving the RREQ or if the RTQ in the packet header is larger than its current SSNR. Note that the RTQ in the packet header represents the signal quality of the weakest link in the route. Each routing table entry also contains a 32-bit RTQ field, which will also be updated if either of the following conditions is satisfied:

i. The sequence number is higher than the sequence number stored in the routing table.
ii. The sequence numbers are equal, but the hop count in the RREQ + 1 is smaller than the hop count stored in the routing table.
iii. The sequence numbers are equal, the RTQ in the routing table is smaller than the pre-defined RTQ_THRESHOLD, which is used to distinguish between good and bad routes, and the RTQ in the packet header is larger than RTQ_THRESHOLD.
iv. The routing table contains no entry with the destination sequence specified in the packet header in routing table.

By doing this, the proposed protocol can maintain the connectivity of the network and keep the overhead low.

4.3 Data Encryption and QoS Scheduling

The final phase is securing the network against malicious attacks. This is achieved by designing a secure cryptography-based mechanism for MANET that employs an Elliptic Curve Cryptography (ECC) encryption mechanism that provides security against malicious attacks and gives high throughput. Throughput in MANET is increased considerably if protected against malicious attacks. A multi-hop scheduler schedules transmissions so that the channel utilization is maximized while guaranteeing the quality of service (QoS) for all nodes. QoS-based scheduling in MANET must be obtained under time-critical conditions as these networks have several features that produce unique queuing dynamics. Schedulers in MANET take into account various QoS parameters such as end-to-end packet delay, packet delivery ratio, flow priority, etc. Also, scheduling in MANET takes many forms such as distributed priority, fair, opportunistic, etc.

4.3.1 Elliptic Curve Cryptography (ECC)

The ECC technique is implemented after establishing the secured path between the source and destination to encrypt the original data into an unknown format. It is one of the widely used cryptographic techniques in network security, which offers fast computation and reduced resource consumption. Also, this technique establishes equivalent security with minimized cost. The strength of this algorithm is, it fully depends on the key and alphabetical table. Also, it provides a better solution for the data by enabling the secure transmission of keys between the communicating entities. Furthermore, different characteristics are symbolized in this technique as the coordinates of the curves. The group of the structure of ECC is formed by the curve that has a finite number of integer points with determinate points. In this work, the main reason for using ECC encryption is, it creates complexity in the encrypted data, so the unauthenticated user cannot easily access the data.

Key Mechanism: The private key of the node is only known to the sender (signer) and used to create the signatures. Whereas, the public key is distributed to all the partners in the communication and can be verified by anyone of the trusted party.

Key Generation: In ECC, the sender selects the private key randomly and computes its public key using a mathematical equation 10.

$$B = d.A \tag{10}$$

Where, d is the private key of the sender and A is the coordinates of the elliptic curve.

Key Sharing Mechanism: The private key is only known to the sender and the public key is provided to the receiver via a secure channel like Dife–Hellman key exchange or any other key exchange mechanism.

Signing Mechanism: The first step of this mechanism is the pre-computation of the hash or the digest of the message to be signed using the secure hash algorithm. The second step is to compute the random number with the help of a random number generator, this random number provides the value for the elliptic curve computations. After this, the message is signed and the sender sends a random number along with a signed message to the receiver.

Verifying Mechanism: The third mechanism is known as verifying mechanism, the signed message when received at the receiver end and can be verified the authenticity of the message using the public key of the authenticator i.e. sender in this case. With the help of the same hash algorithm which is used for signing the message, again the hash is computed on the receiver end along with the public key and the parameters of digital signatures. These hashes are then compared and verified the signatures if match otherwise the verification can be failed.

Communication Mechanism: There are two types of nodes which are being categorized for the implementation of AWSC. The first step is where the nodes need to authenticate themselves using their already stored information.

Signature Generation: After encrypting the data, Schnorr's signature generation algorithm is utilized to generate the signature for the encrypted data. It is a kind of key generation mechanism that integrates both digital signature schemes and public-key encryption schemes. It analyses the discrete logarithmic problem for generating the digital signature, which increases the security of the network. This signature generation has the following steps:

- Setup
- Key generation at the sender side
- Key generation at the receiver side
- Signcryption
- Unsigncryption

In this technique, the source verifies the public key of the packet by using the certificate. Then, the integer is randomly selected, and based on this the keys that are used for generating the ciphertext are computed. Also, the one-way keyed hash function is utilized to generate the encrypted text, and it is forwarded to the destination with the generated signature. The working procedure of ECC-based encryption and signature generation algorithms is illustrated in table 1.

Table 1: Encryption and Signature Generation Algorithm

Algorithm 1: Encryption and Signature Generation
Source verifies the public key of Py by using its certificate;
Randomly select an integer v, where $v \geq P_O$
Compute $k_1 = hash(vE_{bp})$
Compute $(k_2, k_3) = hash(vPy)$
The symmetric encryption algorithm is used to generate cipher text$ct = E_{k_2}(msg)$
Use the one-way keyed hash function to generate, $\gamma = KH_{k_3}[ct \| k_1 \| ID_X \| ID_Y)$
Computes $s = \frac{v}{\gamma + v_x} mod\ p$
Compute $T = \gamma E_{bp}$
Sends the signature added ciphertext (cr, T, s) to the receiver;

4.3.2 Quality of Service (QoS) Scheduling

It is a guarantee by the network to provide certain performance for flow in terms of quantities such as jitter, bandwidth, and packet loss probability. The heterogeneity of applications on the Internet has challenged the network which can provide best-effort service voice, live video and file transfer are some examples. Thus, the delivery of the best quality to the users gives rise to QoS.

Multi-Hop Scheduler

A scheduler (figure 3) includes the following components: (1) an error-free service model that describes how the algorithm provides service to flows with error-free channels; (2) a lead/lag counter for each flow that indicates whether the flow is leading, in synch with, or lagging its error-free service model and by how much; (3) a compensation model used to improve fairness among flows. A lagging flow is compensated at the expense of leading flows when its link becomes error-free again; (4) separate slot and packet queues for each flow can be used to support delay-sensitive and error-sensitive flows. When a packet arrives, it is time-stamped and placed in the packet queue; (5) a means for monitoring and predicting the channel state for every backlogged flow.

A wireless scheduler should possess the following properties:

Efficient Link Utilization: The scheduler should not assign a transmission slot to a flow with a currently bad link;

Delay Bound: The algorithm should provide delay bound guarantees for individual flows;

Fairness: The algorithm should distribute available resources fairly across flows;

Throughput: The scheduler should provide guaranteed short-term throughput for error-free flows and guaranteed long-term throughput for all flows;

Low Complexity: A low-complexity algorithm is preferred as scheduling decisions in MANET have to be made very rapidly;

Graceful Service Degradation: A flow that has received excess service should experience a smooth service degradation when relinquishing the excess service to lagging flows whose links are now good;

Isolation: The algorithm should isolate a flow from the ill effects of misbehaving flows;

Energy Consumption: The algorithm should take into account the need to prolong the battery life of the mobile device. To conserve energy, a node must transmit/receive in contiguous time slots and then go into a sleep (very low energy consumption) mode for an extended period rather than rapidly switch between transmit, receive, and sleep modes. This preference has to be balanced against the need to maintain QoS levels. For example, the Sleep and awake scheduler enables the channel during the data transmission only;

Delay/Bandwidth Decoupling: For multimedia applications, the delay must be tightly coupled with the reserved rate;

Scalability: As the number of flows increases, the algorithm should operate efficiently;

Topology-Transparency: A topology-independent scheduler is preferred as it works efficiently regardless of how frequently and unpredictably the MANET topology changes;

Low Connectivity Information Requirement: A scheduler should keep the communication of network connectivity information to a minimum, as this communication consumes bandwidth.

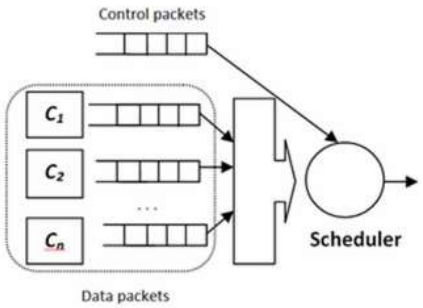

Figure 3: Priority Scheduler for Data Packets

Figure 3 shows a scheduler that serves data packets in a weighted round-robin fashion. Each $C_i(i = 1, \dots, n)$ represents a data flow that can be identified by a source and destination pair. Round-robin scheduling maintains per-flow queues, while each flow queue is allowed to send one packet at a time. Different weights (priorities) can be assigned to data flows. A weighted round-robin scheduler can be used as a priority scheduler that guarantees that all flows (service classes) are served according to their priorities. Data packets in the queues are transmitted based on priority levels. Priority can be defined by using QoS parameters such as bounded end-to-end packet delay, remaining hops to traverse, remaining distance, etc.

5. Experimentation and Result Discussion

The proposed method will be discussed in this part utilizing Matlab software. Analysis of different MANET routing protocols may be done with this tool. In this section, the performance of existing and proposed security mechanisms is evaluated by using various performance measures that include congestion detection time, Packet Delivery Ratio (PDR), delay, route selection time, and throughput. A comparison of the proposed routing protocol to current routing protocols was carried out using the Matlab software. It's no secret that MANET's protocol simulation and implementation characteristics have long baffled researchers, especially regarding the network's overall performance. The simulation configuration table for the proposed method is presented in the following table 2.

Table 2: Simulation System Configuration

Simulation System Configuration	
MATLAB	Version R2021a
Operation System	Windows 10 Home
Memory Capacity	6GB DDR3
Processor	Intel Core i5 @ 3.5GHz
Simulation Time	10.190 seconds

The simulation system configuration of the proposed work is portrayed in table 2. Subsequently, the proposed technique is evaluated and tested under the Matlab R2021a software. The proposed work operates under windows 10 home and its memory capacity is 6GB DDR3. Additionally, it utilizes an Intel Core i5 @ 3.5GHz processor and the simulation time of the work is 10.190 seconds.

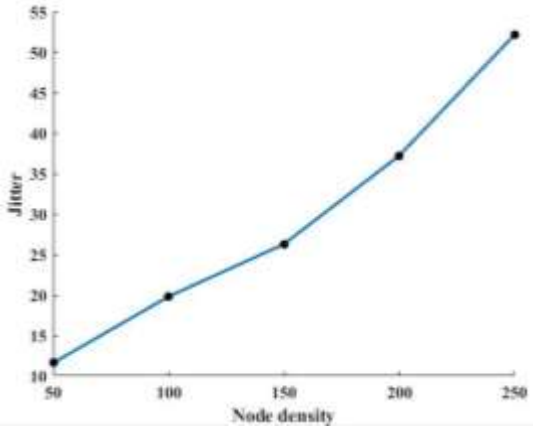

Figure 4: Jitter for Node Density

Figure 4 depicts the performance graph for jitter for different node densities. This figure 4 demonstrated that the node density is taken from 50 to 250, when the node density is 50, the jitter value reaches 12, and when the node density is 250, the jitter value reaches 52 If Jitter is considered as a performance metric for testing different modulation schemes, it experiences least time delay in sending the data packets over a network consisting of a varying number of mobile connections.

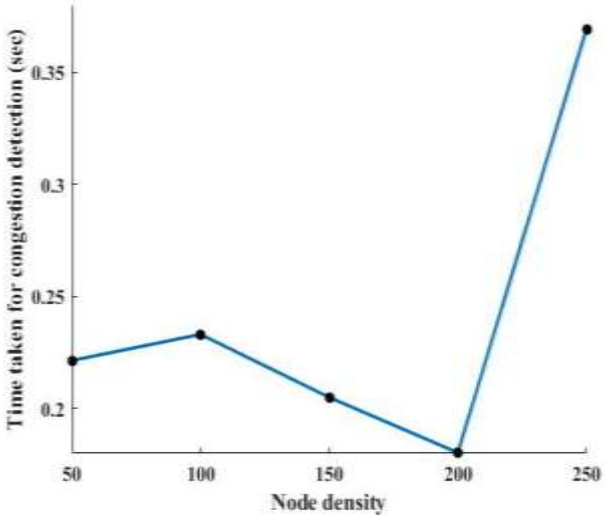

Figure 5: Congestion Detection Time

Figure 5 demonstrates the congestion detection time of the proposed method. The time taken for congestion detection is evaluated based on the node densities. However, the node density is taken from 50 to 250. When the node density is 50, the congestion detection time is 0.24, and when the node density is 250, the congestion detection time is 0.375, respectively.

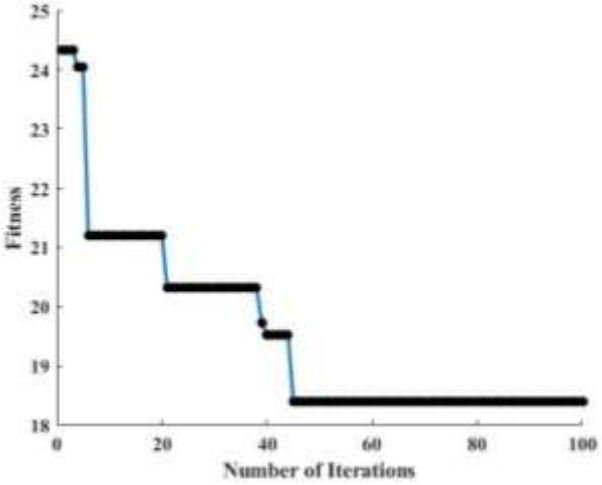

Figure 6: Fitness Graph for the Proposed Methodology

The fitness graph for the proposed work is presented in figure 6. The number of iterations is taken from 0 to 100. For the evolutionary strategies, the fitness at each generation (epoch with an increase in fitness) and the resulting finesses for each test are plotted in figure 6. In this figure, the fitness values reach approximately 18.5%.

Delay: Delay is the time taken for a packet to go from sender to receiver.

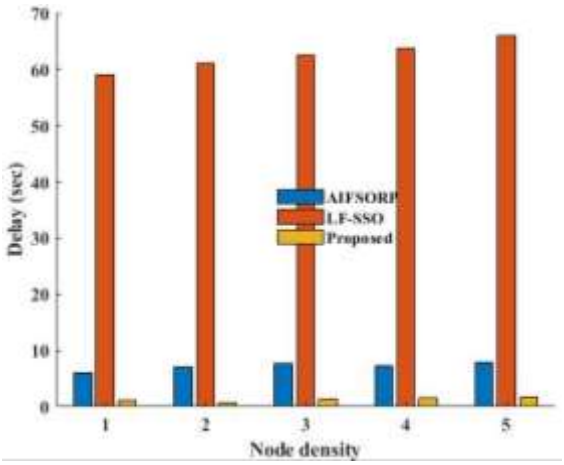

Figure 7: Comparison Graph for Delay with Node Density

Figure 7 portrays the comparison graph for the delay, it is compared with existing Ambient Intelligence-based Fish Swarm Optimization Routing Protocol (AIFSORP) [16] and Levy Flight centred Shuffled Shepherd Optimization (LF-SSO) Algorithms [11]. The above figure represented the delay faced by the packet in every protocol with different node densities. In this figure 7, the X-axis represents the node density, whereas the Y-axis represents the delay, measured in milliseconds. Figure 7 shows that the proposed routing protocol has a minor delay from other present routing protocols, which is easy to comprehend. It employs a sharing strategy to take advantage of the most efficient path. The uses of the current position of nodes to find a better route rather than utilizing the old position of nodes. The considered current routing protocols use the previous position of nodes rather than the updated position of nodes, which ends them facing more delay.

Packet Delivery Ratio

The PDR is estimated based on the fraction of the number of packets that are transmitted by a traffic source and the number of packets received by a traffic sink. Also, it is used to evaluate the efficiency and correctness of the routing protocols by estimating the loss rate. The PDR is calculated as follows,

$$PDR = \frac{Received\ Packets}{Transmitted\ Packets} \times 100 \quad (11)$$

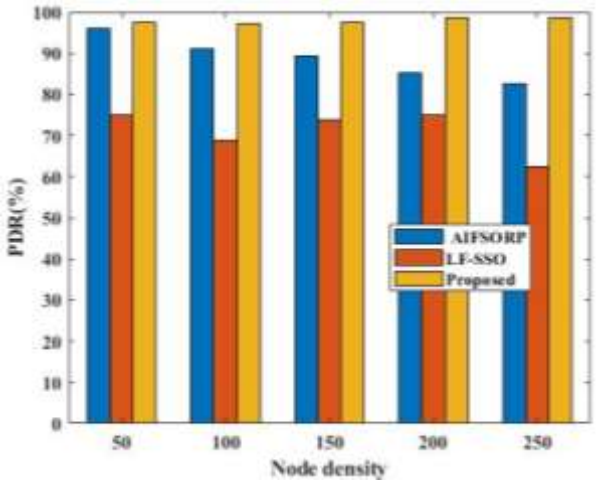

Figure 8: PDR vs Node Density

Figure 8 shows the comparison graph for the PDR of the proposed protocol with the existing protocols for node density. The proposed method is compared with the existing AIFSORP and LF-SSO techniques. From the evaluation, it is observed that if the node density is the PDR of the proposed model can be increased, but the other existing method can be decreased. When compared to the other techniques, the proposed method provides a better PDR by increasing the node density. Also, it uses multiple paths for forwarding the packets, if there is any failure in the current, it uses an alternate path for further communication, which increased the PDR. However, the PDR of the proposed method reaches approximately 99% when the node density is 250.

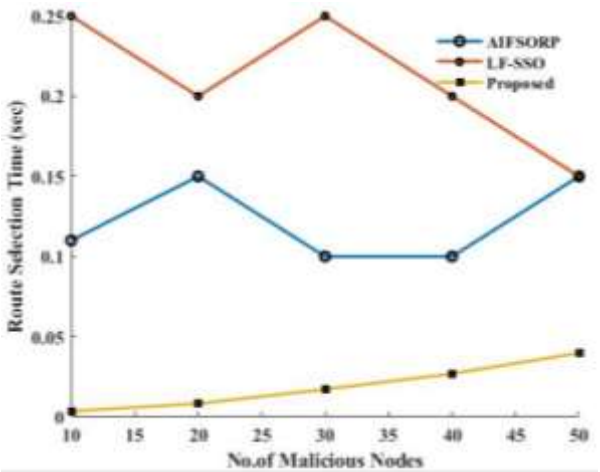

Figure 9: Route Selection Time

Figure 9 demonstrates the comparison graph for the route selection time with the existing methods. The comparison techniques are AIFSORP and LF-SSO methods. Figure 9 demonstrates that the proposed scheme produces the quickest route selection time. The proposed systems require reliable routes in message routing as there have been several instances when the proposed scheme is unable to rapidly find disjoint paths for routing, owing to the presence of critical nodes in identified chosen paths. While utilizing the existing scheme, this is not essential for routing as the latter can discover trustworthy node-disjoint routes that cope through critical nodes'

presence. When compared to these approaches, the route selection process of the proposed technique is much quicker.

Throughput

The throughput is defined as the average rate of successful data delivery over the communication channel. The throughput of the network is calculated as follows:

$$Throughput = \frac{Number\ of\ Data\ Packets\ Received\ (bits)}{Simulation\ Time\ Period\ (secs)} \quad (12)$$

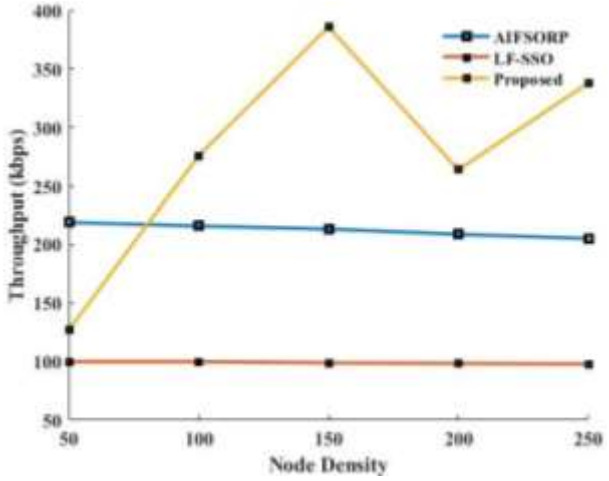

Figure 10: Comparison Graph for Throughput

Figure 10 shows the analysis of throughput for both existing and proposed methods for the number of attackers. During this calculation, the time window is estimated for measuring the throughput based on the successfully delivered packets per unit of time. In this evaluation, it is proved that the proposed SSVC technique has increased throughput when compared to the other techniques.

6. Research Conclusion

Mobile Ad-hoc networks (MANET) are made up of several mobile wireless nodes that may move around and join or depart at any moment. Most networks strive to provide good security and an acceptable level of performance. Quality of service (QoS) plays an important role in the performance of a network. Mobile ad hoc networks (MANET) are a decentralized and self-configuring type of wireless network. MANET is generally challenging and the provision of security and QoS, and congestion problems become a huge challenge. In this research, a Centralized Congestion Detection and Novel Rate Aware-Neuro-Fuzzy based Congestion Controlling strategy is presented to detect and avoid congestion in the network. Accordingly, an Ambient Intelligence-based Ant colony optimization quality-aware energy routing protocol is presented for routing the data packet. This method identified the most efficient route to a destination and decreases the time and energy required. The elliptic Curve Cryptography (ECC) encryption method is presented to secure the network against malicious attacks. However, QoS-based scheduling in MANET is performed by using the multi-hop scheduler. The proposed method is implemented using Matlab software. The proposed congestion is based on which the PDR, throughput, and delay. The performance of the proposed method is compared with the existing AIFSORP and LF-SSO methods. While compared to these existing methods, the proposed technique reduces transmission delay, and route selection time, and enhances the packet delivery ratio, hence increasing throughput. Consequently, the presented Routing Protocol discovers the most efficient route and reduces delay faced and energy spent. Subsequently, QoS Scheduling classes help in network traffic optimization and the priority management of packets. However, to minimize energy consumption and further improve the system performance, a recent bio-inspired technique is presented in future studies.

References

[1] Kankane, S., Jhapate, A. and Shrivastava, R., 2022. Light Load Path Selection Techniques for Control Congestion in MANET (ENBA). International Journal of Advanced Computer Technology, 11(4), pp.1-7.

[2] Esiefarienrhe, B.M., Phakathi, T. and Lugayizi, F., 2022, June. Node-Based QoS-Aware Security Framework for Sinkhole Attacks in Mobile Ad-Hoc Networks. In Telecom (Vol. 3, No. 3, pp. 407-432). MDPI.

[3] Kant Vishwakarma, E.R., Sahu, M. and Sharma, D., Performance Evaluation of MAC Protocol in Mobile Ad-Hoc Wireless Network. Journal homepage: www.ijrpr.com ISSN, 2582, p.7421.

[4] HAMAMREH, R.A., 2019. SDCM: Secure Dynamic End-To-End Congestion Avoidance Protocol for MANET. Journal of Theoretical and Applied Information Technology, 97(21).

[5] Kanellopoulos, D.N., 2019. Recent progress on QoS scheduling for mobile ad hoc networks. Journal of Organizational and End User Computing (JOEUC), 31(3), pp.37-66.

[6] Nasralla, M.M., García-Magariño, I. and Lloret, J., 2021. MASEMUL: A simulation tool for movement-aware MANET scheduling strategies for multimedia communications. Wireless Communications and Mobile Computing, 2021.

[7] Nithyapriya, J., Jothi, R.A. and Palanisamy, V., 2019, May. Protecting Messages Using Selective Encryption Based ESI Scheme for MANET. In 2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW) (pp. 50-54). IEEE.

[8] Singha, S., 2021. Design of an effective Congestion Control Routing Protocol for Mobile-Ad-Hoc Network (Doctoral dissertation, Vidyasagar University, Midnapore, West Bengal, India,).

[9] Yazdinejad, A., Kavei, S. and Razaghi Karizno, S., 2019. Increasing the performance of reactive routing protocol using the load balancing and congestion control mechanism in MANET. Computer and Knowledge Engineering, 2(1), pp.33-42.

[10] Suraki, M.Y., Haghighat, A.T. and Gholipour, M., 2018. FCLCC: fuzzy cross-layer congestion control in mobile ad hoc networks. IJCSNS, 18(1), p.155.

[11] Alappatt, V. and PM, J.P., 2021. Trust-based energy efficient secure multipath routing in MANET using LF-SSO and SH2E. Int. J. Comput. Netw. Appl., 8(4), p.400.

[12] Anbarasan, M., Prakash, S., Antonidoss, A. and Anand, M., 2020. Improved encryption protocol for secure communication in trusted MANET against denial of service attacks. Multimedia Tools and Applications, 79(13), pp.8929-8949.

[13] Appaji, V.V. and Srinivas, J.V.S., Cross Layer Congestion Control Mechanism for MANET using CSPA algorithm.

[14] Kashid, M.T.S.V., Patidar, M. and Sharma, H.M.K., 2021. Multipath Congestion Control and Predication and Detection of Attacks in MANET.

[15] Miriyala, S. and Sairam, M.S., 2020. Improving privacy in SDN-based MANET using hybrid encryption and decryption algorithm. Microprocessors and Microsystems, p.103501.

[16] Sumathi, K. and Kumar, D.V., Ambient Intelligence-Based Fish Swarm Optimization Routing Protocol for Congestion Avoidance in Mobile Ad-Hoc Network. Networks, 6, p.15.

[17] Thanappan, R. and Perumal, T., 2022. Congestion Aware MANET Routing Using Evolutionary Game Theory and Cross-Layer Design. ECS Transactions, 107(1), p.1699.

[18] Reddy, V.S.N. and Mungara, J., 2021. Machine Learning-Based Efficient Clustering and Improve Quality of Service in Manet. Indian Journal of Computer Science and Engineering, 12(5), pp.1392-1399.

[19] Phakathi, T., Esiefarienrhe, B.M. and Lugayizi, F., 2021. Comparative analysis of quality of service scheduling classes in mobile ad-hoc networks. ArXiv preprint arXiv:2106.07051.

[20] Usturge, S. and Pavan Kumar, T., 2022. DEroute: trust-aware data routing protocol based on encryption and fuzzy concept for MANET secure communication in IoT. Information Security Journal: A Global Perspective, pp.1-16.

[21] Ravi, S., Matheswaran, S., Perumal, U., Sivakumar, S. and Palvadi, S.K., 2022. Adaptive trust-based secure and optimal route selection algorithm for MANET using

hybrid fuzzy optimization. Peer-to-Peer Networking and Applications, pp.1-13.

[22]Alghamdi, S.A., 2022. Novel trust-aware intrusion detection and prevention system for 5G MANET–Cloud. International Journal of Information Security, 21(3), pp.469-488.

[23]Satyanarayana, P., Nihani, V.G.V., GA, J.D., DVA, K.R. and CH, S.A., 2022, March. Design and Implementation of Trust Based Routing Algorithm to Enhance QoS for MANET. In 2022 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET) (pp. 64-68). IEEE.

[24]Vinayakan, K., Srinath, M.V. and Adhiselvam, A., 2022. Security for Multipath Routing Protocol using Trust based AOMDV in MANET. Specialusis Ugdymas, 2(43), pp.1640-1654.

[25]Saraswathi, R., Srinivasan, J. and Aruna, S., 2022. An Energy Efficient Routing Protocol and Cross Layer Based Congestion Detection Using Hybrid Genetic Fuzzy Neural Network (HGFNN) Model for MANET. Journal of Algebraic Statistics, 13(2), pp.1007-1019.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.