# Performance Analysis of Routing Protocol Using Trust-Based Hybrid FCRO-AEPO Optimization Techniques

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 (MANETs) offer numerous benefits and have been used in different applications. MANETs are dynamic peer-to-peer networks that use multi-hop data transfer without the need forpre-existing infrastructure. Due to their nature, for secure communication of mobile nodes, they need unique security requirements in MANET. In this work, a Hybrid Firefly Cyclic Rider Optimization (FCRO) algorithm is proposed for Cluster Head selection, it efficiently selects the cluster head and improves the network efficiency. The Ridge Regression Classification algorithm is presented in this work to detect the malicious nodes in the network and the data is transmitted using trusted Mobile nodes for the QoS performance metric improvement. A trust-based routing protocol is introduced using the Atom Emperor Penguin Optimization (AEPO) algorithm, it identifies the best-forwarded path to moderate the routing overhead problem in MANET. The proposed method is implemented using Matlab software and the performance metrics are packet delivers ratio, packet loss ratio, routing overhead, throughput, end-to-end delay, transmission delay, network lifetime, and energy consumption. The proposed AEPO algorithm is compared with the existing PSO-GA, TID-CMGR, and MFFA. The AEPO algorithm's performance is approximately 1.5%, 3.2%, 2%, 3%, and 4% higher than the existing methods for packet delivers ratio, packet loss ratio, end-to-end delay, and throughput and network lifetime. This evaluation enables the sender nodes to improve their data transmission rates and minimizes the delay. Additionally, the suggested technique has a clear benefit in terms of demonstrating the genuine contribution of distinct nodes to trust evaluation.

Keywords: Mobile Ad Hoc Networks, Cluster Head Selection, Hybrid Firefly Cyclic Rider Optimization, Malicious Node Detection, Ridge Regression Classification Algorithm, Atom Emperor Penguin Optimization.

Received: May 29, 2022. Revised: May 13, 2023. Accepted: June 22, 2023. Published: July 20, 2023.

## 1. Introduction

Mobile Ad Hoc Networks (MANETs) are self-contained networks made up of wireless mobile nodes that operate independently of any infrastructure [1]. Over radio frequencies, Nodes in a MANET can dynamically and freely interact with another node. In the absence of fixed infrastructure, MANETs enable mobile users to interact with one another [2]. Due to the transmission interference, mobility, and external noise to work correctly, the routes in the MANETS are frequently unable. In a diversity of vital applications, the advancement of the internet in recent years has greatly increased the use of MANETs. In order to construct Internet of Things (IoT)-based smart networks, MANETs have recently been used [3]. Consequently, for these networks, the consistency and safety standards should be thoroughly re-evaluated. MANET is widely used in the military, commercial, and private sectors. MANETs are subject to the variability of security threats, including rushing attacks, black holes, and wormholes [4]. In MANET, secure communication is achieved by using several traditional approaches. Nevertheless, in terms of network security, QoS, wireless time-varying networks and frequent node mobility are insufficient to ensure efficient transmission [5]. For instance, the presence and

collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations. In order to ensure efficient transmission and to avoid the malicious attack, a trust-based routing protocol is used.

**MANET Security**

In MANETs, security often entails protecting and maintaining data integrity and confidentiality, as well as each network node supplied the availability of network services and legitimate usage [6]. In the route discovery processes, the ability of nodes to actively participate and to honestly forward data packets to other nodes in the network is essential to the MANET's feasibility. In order to deal with data forging and hacking attacks, a range of security measures have been developed, such as message encryption algorithms, secure authentication, message integrity verification, and so on [7]. Moreover, in many other attacks like denial of service, node capture attacks, etc., these solutions are ineffective. The resistance efficiency is lower but by node captured causes the internal attacks and external attacks are effectively resisted by the traditional security mechanisms [8]. Data must be transmitted through a node inside the communication scope of forwarding nodes to ensure communication security. Consequently, the data transmission will be more secure. Accordingly, for effective transmission, a clustering approach based on trust evaluation was implemented in [9] for the identification of the malicious node. The proposed technique does not take into account QoS measurements. Subsequently, by detecting malicious nodes, the secure network communications performance is improved by suggesting a new trust formation technique [10]. Accordingly, based on trust level, link quality, and geographical position, three different measures for next-hop selection are added in this system, allowing nodes to choose more experienced next-hop forwarders. In order to find the trusted nodes, the developed approach ignores node characteristics.

**Trusted Node Communication Security**

The most difficult issue in MANET is providing efficient and secure communication [11]. Nodes in a geological site developed clusters to provide good communication. MANET can be managed more efficiently by dividing the entire network into clusters. Clustering is the process of forming clusters. In the network, the communication among the constrained nodes provides better with the help of clustering. Gateway nodes, Cluster Heads (CH), and cluster members made each cluster [12]. Numerous sorts of research are being conducted in this area and many clustering strategies have been developed; nevertheless, the MANET sustainable clustering methodology has yet to be established. Many properties of nodes can be clustered, including the weight of the nodes, the trustworthiness of the nodes, mobility of the node, Node ID, spatial and temporal locations, and so on [13]. According to the numerous properties of the node considered at once, clustering based on weight will be the most efficient of all the strategies. The node's weight is made up of its velocity, transmission ranges, residual energy, degree, and other factors [14]. Among all nodes in the cluster, the chosen CH will be the most efficient because almost all node characteristics are taken into account when calculating weights. In the future of ubiquitous devices, MANET routing protocols are a critical component. Increased bandwidth utilization, better throughput, longer network life, and lower end-to-end delay are the number of benefits of the multipath approach. Consequently, route failures are protected and network congestion is reduced [15]. There are routing protocols utilized for better energy efficiency and delay management in Mobile Adhoc Networks. Classification of these protocols can be done based on their method of routing from source to destination. Depending on the congestion of traffic, node density and mobility rate such routing protocols are categorized. Accordingly, by maintaining both trust and energy efficiency, a trust-based routing protocol is developed is the most difficult task in developing a trust evaluation method for

MANET [16]. The remaining part of the work is organized as follows, section 2 portrays the literature survey of the study, and section 3 exhibits the problem definition and motivation of the research. Section 4 illustrates the proposed research methodology, section 5 elucidated the experimentation and result in a discussion, and section 6 exposes the research conclusion.

## 2. Literature Survey

The literature survey is based on the study of secure communication of MANET using different algorithms. The survey portrays the routing methods for secure transmission and in this research, an Atom Emperor Penguin Optimization (AEPO) algorithm is proposed for finding the best forwarding path, respectively.

In order to safeguard transmitted packets from malicious nodes, a dual cluster head-based trust aware mechanism is proposed by Aruna Subramanian *et al* [17] as an alternative to cryptographic techniques. TWCBRP is a proposed protocol that splits the network into one-hop overlapping clusters with primary and secondary CH in charge of all routine activities. Replacing primary CH with secondary CHs, also guarantees the CH's trustworthiness, once the former turns malicious. Cluster members ensure a secure channel by routing packets exclusively through gateway nodes and trustworthy CH. When compared to a distributed weighted cluster-based protocol (CBPMD), TWCBRP shows improved performance in terms of control overhead, packet delivery ratio (PDR), throughput, and delay when tested with Network Simulator.

The Hybrid Ant Colony Optimization with DSR protocol (H-ACO-DSR) method is presented by M. Anugraha*et al* [18] for better resource allocation in the MANET context to increase safe data transfer. In the MANET system, Hybrid Trust Cluster-based Multiple Routing (H-TCMR) produces trustworthiness and efficient clusters. Accordingly, to determine trusted nodes and the malicious node in the system utilizing the Adaptive Booting Technique (ABT). The data transmission, as well as the MANET's trusted nodes, are carried out with the trustworthy MN to enhance the QoS metric's efficiency. Finally, modelling results produce Routing overhead, Throughput, Average Delay, enhanced PDR, and low-cost Energy when compared to different techniques.

M. Venkat Das *et al* [19] advocated using the "Node Authentication and Trusted Routing method (NATR)" to improve security. Through output data delivery and better security, NATR strives to eliminate aberrant node interference in MANET. Additionally, by examining the three most typical actions taken by a node throughout the connection process, the predictability of a node is determined. When it comes to custom network security, node licencing is crucial. Monitor the data success rate node trust, RREQ, and RREP's success rates using this method. The loss or drop of packets and the successful delivery of packets are used to assess data delivery dependability. Routing overhead decreased by 40% and package delivery increased by 25% as depicted based on the experimental results. In order to evaluate Adhoc network efficiency, NATR is compared to AODV and SAR TMS.

Sirajuddin*et al* [20] proposed a trust-based multipath routing protocol called TBSMR to enhance the MANET's overall performance. The main strength of the proposed protocol is that it considers multiple factors like congestion control, packet loss reduction, malicious node detection, and secure data transmission to intensify the MANET's QoS. The performance of the proposed protocol is analyzed through the simulation in NS2. Our simulation results justify that the proposed routing protocol exhibits superior performance to the existing approaches.

Hassan Jari*et al* [21] examine the effects of a black hole attack on MANET routing systems. The goal of trust management is to keep a network safe from hostile activity. Accordingly, a new trust-based MANET routing protocol called ITAODV is presented in this study, which is developed from the normal AODV protocol. Accordingly, for packet forwarding, the proposed protocol

employs an indirect trust mechanism that considers the reliability of each node. The network simulator NS-3 was utilized for the ITAODV and AODV performance evaluation. The ITAODV protocol's effectiveness against the Blackhole attack is demonstrated by the experimental results.

C. Gopala Krishnan *et al* [22] concentrated on detecting unstable CH and replacing them with nodes that use the self-configurable cluster technique. To successfully designate CH, a self-configurable cluster method is presented with the k-means protocol technique. Periodic irregular CH rotations or changing the number of clusters are used in the suggested k-means approach. Additionally, to avoid and detect MANET vulnerabilities, this research, offers a trust management technique. Accordingly, the trust management method should only employ local data because of the limited resources (computing, power, and bandwidth) and the constantly changing topology. Consequently, the suggested approach with the k-means procedure and its experimental findings use less power than previous protocols and provide an optimal system for trust management.

In order to train the trust prediction model, JasleenKaur*et al* [23] suggested using the Adaptive neuro-fuzzy inference system (ANFIS) trust management. The hyper-parameters of the ANFIS model are then tuned using a non-dominated sorting genetic algorithm-III (NSGA-III). A fitness function with many objectives is designed using root means squared error, precision, and recall measurements. Subsequently, for comparative analysis, the optimized link state routing (OLSR) protocol is used. In order to collect the dataset, three separate attacks are used on the designed network: jellyfish, link spoofing, and grey hole attacks. According to a comparison of performance measures, the suggested trust assessment model beats competitive trust evaluation models in terms of routing overheads, throughput, average end-to-end latency, and PDR. Consequently, the suggested protocol is more resistant to different security risks.

In MANET, J. Anitha Josephine *et al* [24] proposed Tanimoto Support Vector Regression Based Corrective Linear Program Boost Classification (TSVR-CLPBC) as an ensemble approach. In order to improve secure communication with a higher PDR and minimal end-to-end delay is the major goal of the suggested method. In order to investigate node characteristics such as node history, cooperative communication, and residual energy, Tanimotokernelized SVR is first used as a weak learner. Based on the analysis, the nodes are classed as malicious or trusted. Consequently, for secure data transfer, the trusted MN is identified by the Linear Program Boost ensemble classifier using 'n' number of weak learners (i.e., base classifier).

Accordingly, for secure routing in MANET, P. Sathyaraj*et al* [25] suggested a real-time secure route analysis (RSRA) technique. The technique takes into account not only the strategy of intermediary nodes along the detected route but also the presence of IoT devices and their trustworthiness. Subsequently, by generating a list of possible paths between any two points, the method starts. Subsequent, the trustworthiness of each mobile node is confirmed by taking into account its energy, the number of transmissions involved, mobility speed, its neighbour list, location, etc. Based on their previous contributions to the network, the IoT devices' trustworthiness is determined. Due to the mobile nodes, the approach measures mobile node secure route support (MSRS), whereas, for IoT devices, it measures device support (DS). Accordingly, by taking into account the number of IoT devices in the route, the approach calculates the data forwarding support (DFS) value. A single route has been chosen based on the DFS measure, which enhances MANET QoS.

Trust and trust computations were discussed by Rakesh Kumar *et al* [26]. In order to limit the effects of attacks, a trust-based fuzzy bat (TBF) optimization model is suggested and implemented in this paper. Subsequently, carried out the sensitivity analysis in different network scenarios. The evaluation is based on performance indicators

such as PDR and normalized routing overhead. The distrust threshold, trust update interval, and trust component weight are all changed. In an untrusted Manet's environment, a security solution is guaranteed by employing a fuzzy bat with a trust evaluation model. The TFB algorithm outperforms existing approaches in terms of network lifetime and throughput, as well as end-to-end delay and energy consumption as revealed in the results.

## 3. Research Problem Definition and Motivation

MANET is a hotspot for study because of its numerous drawbacks and benefits. Providing secure communication between mobile nodes, dealing with misbehaviour and location updates, lowering overhead, and recognizing node positions are all difficult problems in ad-hoc networks, subsequently, in this network trust methods are essential. Over self-organized networks, MANET supports several basic operations such as packet forwarding, routing, communication, and network administration. Since mobile nodes enter and exit the network at unpredictable intervals, MANET does not have a fixed topology. Consequently, it affects the network's memory computations, energy, and bandwidth. Identifying compromised, malevolent, and selfish nodes that have been authorized requires trust management. Sensor nodes, in reality, have limited resources and other unique characteristics, making WSN trust management more important and difficult. Until now, to improve robustness and security, research on WSN trust management systems has mostly concentrated on node trust evaluation. Subsequently, MANET lacks a centralized infrastructure, and establishing trust is a critical task. The multi-hop module and one-hop module are defined by the distributed and adaptive trust metrics for MANET. Recommendation and direct trust are calculated in the one-hop module, whereas indirect trust is calculated in the multi-hop module. Energy trust and communication trust are examples of direct trust. When assessing communication trust, not only look at the present value; predict it based on the network's status. The presence of misbehaving nodes in the network's numerous problems. Owing to the waste of important resources can cause the network to go down. Accordingly, this encourages the search for a secure communication environment.

Effective routing with enhanced QoS become one of the major research challenges in networks. The process of clustering nodes is considered one of the major solutions for scaling down ad-hoc networks and enhancing effective routing. Hence, finding a suitable procedure of cluster formation for efficient routing in the network topology acts as a primary concern for researchers. Thus, QoS-aware security-based clustering in such network act as a challenging and popular area of research. MANETs suffer from security issues due to the open and dynamic nature of the network environment. In other words, MANET is vulnerable to attacks caused by malicious nodes but the dynamic nature of the ad-hoc network plays a vital role in developing secure and stable routing in MANET. In addition, clustering can improve routing performance and enhance secure route connectivity between nodes. Consequently, the lifetime of wireless nodes is considered very important in MANETs, so optimization of energy utilization plays a vital role in MANETs. Transmission power, reception power, and energy consumption by devices are significant energy utilization constraints in a MANET. This scheme is introduced to increase the network lifetime, PDR and its forwarding rates in the network to establish a connection between two hops in a multi-hop approach. When the communication nodes' distance increases in Mobile Ad Hoc Network, energy or power utilization also increases and decreases the wireless node's whole lifetime. When the packets are forwarded to the neighbour node in Mobile Ad Hoc Network, the power utilization increases, and the node consumes more power while it transmits or receives the information. The power management technique may be accustomed to optimize the power within the Mobile Ad Hoc Network. From this, a recent algorithm is

proposed for efficient routing and cluster head selection, and network lifetime improvement, respectively.

## 4. Proposed Research Methodology

MANET is a wireless network made up of several mobile nodes that self-heal and self-configure without the need for a fixed infrastructure. Due to their self-configuring nature, MANETs may be easily accepted in different situations, including battlefield communications, rescue, and emergency operations. Due to the unreliability of MANET wireless communications, nodes are susceptible to a variety of security attacks, which disrupt the network structure. Due to the malicious node, a Mobile Node (MN) may provide erroneous routing information to subsequent nodes, and it drops the DP instead of forwarding it. So, these challenges are overcome and the network security is improved by deploying trust-based node evaluation techniques. The architecture of the proposed work is portrayed in figure 1.

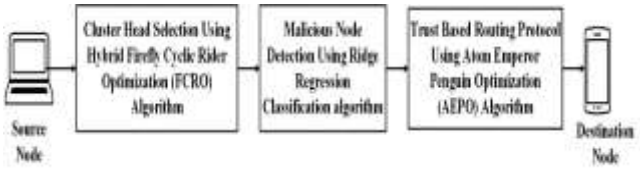


**Figure 1:** Flow Diagram of the Proposed Work

In this MANET, the source node is transferred to the destination node, initially, a Hybrid Firefly Cyclic Rider Optimization algorithm is proposed in this work for CH selection. Subsequently, a Ridge Regression Classification algorithm is presented to detect the malicious node in this network. Accordingly, Atom Emperor Penguin Optimization (AEPO) algorithm is presented to route the network and find the best forwarding path, respectively.

### 4.1 Cluster Head Selection Using FCRO Algorithm

Clustering is an important concept in MANET where several nodes join to form a group based on common features. The node is a single system which is responsible to store and process data. Whereas Cluster is formed based on the collection of multiple nodes which communicates with each other to perform a set of operation. Furthermore, selecting an efficient CH node is a difficult task due to the limited battery power supply in MANET. In terms of the power allocation of nodes to clusters, cluster formation is a valuable operation. Every cluster has one or more CH, which are connected to build networks and disseminate data. The CH node is a trusted node that scans a node's performance and other security-related tasks are performed. Malicious nodes can quickly drain energy and degrade the overall longevity of networks; hence a CH should be able to function in low-energy and resource-constrained contexts. Subsequently, this research proposes a Hybrid Firefly Cyclic Rider Optimization (FCRO) algorithm for optimal CH selection (CHS) to improve the MANET network's energy efficiency and lifetime. Additionally, the network's dead nodes, overall throughput, residual energy of nodes, convergence rate, alive nodes, and network survivability index are all improved.

**Cluster Formation:** Due to the energy efficiency reflection, the logical identification accounts for the cluster are almost often. The use of a sensible cluster count can improve network connection efficiency while also balancing node energy loss and extending network lifespan. Subsequently, in inter-cluster communication, this framework uses the multi-hop routing mechanism. The distance between the BS and the extreme CH is expressed as $Di$, which is classified as many hops. $Di = k.le$, here the equidistance length is $le$ and the number of clusters is $k$. Under the multi-hop communication method, the energy consumption is given as (1).

$$E_{mh} = E_{Rx} + E_{DA} + E_{Tx} \tag{1}$$

Where, $E_{mh}$ is represented as energy consumption in multi-hop communication, $E_{Rx}$, and $E_{Tx}$ are denoted as energy

consumption in receiver and transmitter data, respectively.

### 4.1.1 CH Selection

Accordingly, in the establishment of clusters, the best CH for data transmission must be chosen. Consequently, this research aims to choose the best CH while taking into account key fitness criteria such as energy, distance, and latency, which have already been identified as issues when selecting the CH. Additionally, the distance should be minimised by using the shortest path selection, and the presentation of data transfer is improved. Another highly serious issue is the energy usage of each node. Accordingly, the information distribution is the largest problem with the shortest length and the least amount of energy. Furthermore, practically all optimisation algorithms hold a high level of responsibility for distance and energy expenditure while choosing on CH selection. Subsequently, to improve the node's life expectancy, multiple objectives are required. Finally, the primary criteria to consider while selecting the CH from a group of sensor nodes are latency, energy, and distance.

**Distance:** Equation (2) depicts the distance fitness function.

$$f_i^{dis} = \frac{f_{(a)}^{dis}}{f_{(b)}^{dis}} \tag{2}$$

$$f_{(a)}^{dis} = \sum_{x=1}^{N_x} \left\lfloor \left\| F_x - B_s \right\| + \sum_{y=1}^{N_y} \left\| F_X - D_X \right\| \right\rfloor \tag{3}$$

$$f_{(b)}^{dis} = \sum_{x=1}^{N_x} \sum_{y=1}^{N_y} \left\| D_x - D_y \right\| \tag{4}$$

Where $f_i^{dis}$ illustrates the fitness function for the distance, $f_{(a)}^{dis}$ and $f_{(b)}^{dis}$ are the distance of two nodes. Subsequently, $F_x$ is the distance of CH, $B_s$ the distance of BS, $D_x$ and $D_y$ the distance of normal data and the count of nodes.

In (2), $f_{(a)}^{dis}$ the value must add a distance to it so that the packets connected with it can be transferred quickly from the common node to the CH and the destination. The obtained specific value must be low and lies between [0, 1]. The value $f_i^{dis}$ grows in proportion to the distance between the common node and CH. In (3), $F_x - B_s$ which illustrates the distance between the CH and BS, $F_x - D_x$ defines the distance between the CH and normal node, and $D_x - D_y$ refers to the distance between the two normal nodes, and the count of nodes not provided in $x$ th and $y$ th CH is referred to as $N_x$ and $N_y$ the node that is available within the CH is referred to as $R_x$ for the $x$ th CH.

**Energy:** The fitness function for energy is shown in equation (5).

$$f_i^{ene} = \frac{f_{(a)}^{ene}}{f_{(b)}^{ene}} \tag{5}$$

Where $f_i^{ene}$ represented as the fitness function for the energy, $f_{(a)}^{ene}$ and $f_{(b)}^{ene}$ are portrayed as the fitness function for the cumulative clusters. Where the cumulative CH $f_{(a)}^{ene}$ and $f_{(b)}^{ene}$ is taken into account as a rise in energy value, the $f_i^{ene}$ value is presumed to be greater than one and increases the number of CHs.

**Delay:** The fitness function of the delay is directly proportional to the member count within the cluster. Accordingly, the CH owns a certain number of members for delay reduction. The fitness function for the delay is represented by equation (6).

$$f_i^{del} = \frac{\max\left(\left\| F_x - D_x \right\|\right)_{x=1}^{N_c}}{N_c} \tag{6}$$

Where $f_i^{del}$ portrays the fitness function of delay, the maximum amount of CH is contained in the numerator and the denominator $N_c$ contains every node in the network. $f_i^{del}$ value is relay within the interval [0, 1] and it has to be lower for the filter CH selection.

### 4.1.2 Firefly Algorithm (FA)

The firefly algorithm is a biologically inspired algorithm that inspires the firefly's flashing behaviour. Subsequently, this algorithm employs the following three rules.

1. The fireflies are attracted to the opposite mate.
2. The firefly's attraction is calculated using the brightness value. The attraction of the firefly reduces as the distance between the two fireflies grows. The brighter firefly attracts the less-brighter firefly, while the less-brighter firefly attracts the brighter firefly.
3. The firefly's brightness is calculated using the objective function below.

The inverse square law governs the variation in light intensity $I(r)$.

$$I(r)=\frac{I_s}{r^2} \tag{7}$$

Where $I_s$ is the source's intensity and $r$ is the distance to the source. Lumens are the metric for light intensity. The firefly's attractiveness is depicted as

$$\beta=\beta_0 e^{-\gamma r^2} \tag{8}$$

Where the light absorption coefficient is denoted as $\gamma$ and $\beta_0$ is the fluctuation of attractiveness at $r=0$. Euclidean distance is used to compute the distance between any two fireflies at the coordinates $x_i$ and $x_j$. Consequently, it can be characterized as follows:

$$r_{ij}=\left\|x_i-x_j\right\|=\sqrt{\sum_{k=1}^{d}\left(x_{i,k}-x_{j,k}\right)^2} \tag{9}$$

Where $x_{i,k}$ is the $k$ th component of the $i$ th firefly's spatial coordinate $x_i$. The brighter firefly $j$ attracts the less bright firefly $i$. The firefly's movement is illustrated by

$$x_i^{t+1}=x_i^t+\beta_0 e^{-\gamma r_{ij}^2}\left(x_j^t-x_i^t\right)+\alpha_t \in_i^t \tag{10}$$

The current position is $x_i^t$. The second word refers to the firefly's mutual attraction. Utilizing a Gaussian distribution at the time $t$, the third term $\in_i^t$ denotes the production of random vectors. When $\beta_0=0$; the second term in equation 10 is omitted, the firefly takes a random walk.

### 4.1.3 Hybrid Firefly Cyclic Rider Optimization (FCRO) Approach

The brighter firefly attracts the less bright one in every iteration of the firefly algorithm. Consequently, in the position's random movement, this algorithm works well for identifying the solution, but it ignores firefly's best position for CH selection, for finding the best solution, it has an impact on the global search behaviour. The ROA algorithm paired with the firefly algorithm overcomes the above-mentioned restrictions. Subsequently, by finding better solutions in CH selection, the ROA algorithm improves network performance. The $p_{best}$ and $g_{best}$ values derived by ROA are used by each firefly. Furthermore, to attain greater results during the riding process, this strategy strikes a balance between exploitation and exploration. The convergence speed is increased and the precision of the solution is determined by the movement of each firefly.

**Optimal Selection of Cluster Count and CH:** This research aims to solve two major optimization challenges optimal cluster counts and Optimal CH selection. The best cluster counts $k$ objective function $OB_1$ can be established in (11).

$$OB_1=\min\left(Eg_{tot}\right) \tag{11}$$

The optimal CH selection's objective function $OB_2$ is defined in (12)

$$OB_2=\min\left(F_3\right) \tag{12}$$

Where, $F_3=\alpha*(F_2)+(1-\alpha)*f_i^{del}$, $F_2=\gamma*(F_1)+(1-\gamma)*\frac{1}{QoS}$, and $F_1=\beta*\left(f_i^{dis}\right)+(1-\beta)*\frac{1}{f_i^{ene}}$. Subsequently, $\alpha$, $\beta$, and $\gamma$ are the constant values that are fixed at 0.3, 0.3, and 0.9, respectively. Where $CH_z$; $z=1,2,\ldots,N_{CH}$ is the number of CHs

and $k_i$; $i=1,\ldots,N_k$ is the number of clusters that are optimally selected.

### 4.1.4 Cyclic ROA Approach

ROA is a fictitious computing algorithm based on the inspiration of a group of riders that strive to reach a specific destination to win the race. Accordingly, they are divided into four groups, with the number of riders split evenly among the four groups. Bypass rider, follower, overtaker, and attacker are the four groups. The following methods are used by each group to reach the target:

- The leading path is avoided to get to the destination is the main goal of bypass rider.
- In the majority axis, the follower tends to follow the leading rider.
- According to the leading rider's location to achieve the target, the overtaker is the one that follows their path.
- To reach the destination, point as quickly as possible, the attackers capture the rider's path.

The riders follow a pre-planned strategy, with the appropriate use of the accelerator, gear, steering, and brake being the most important aspects to consider when achieving the goal. Riders alter their position for each instant of time while approaching the goal by regulating these factors, and based on the current success rate, it continues with the pre-planned strategy, to the distance between the rider's destination and the current location, which is inversely related. The leading rider is mentioned based on the current success rate. Consequently, this process will continue until the riders have been given the maximum amount of time. The winner is then announced with the leading driver. The Cyclic ROA model algorithm is presented in table 1.

**Table 1:** Algorithm for Cyclic ROA Model

| |
|---|
| Input: Rider's random positions, $R^t$ |
| Output: Leading rider, $R^I$ |
| Allot the population |
| Allot the rider components: Steering angle $A$, Gear $G$, |
| Accelerator $a$ and Break $Br$ |
| Determine the success rate |
| While $T<T_{off}$ |
| for $x=1$ to $R$ |
| Update bypass position rider as per equation (13) |
| Update follower position rider as per equation (14) |
| Update overtaker position rider as per equation (15) |
| Update attacker position rider as per equation (16) |
| Grade riders based on the success rate |
| Choose a rider with a higher success rate as the leading one. |
| Update the rider constraints |
| Return $Z^L$ |
| $t=t+1$ |
| end for |
| end while |
| End |

**Rider's Position Update:** By updating the rider's position in each set, the leading rider is identified.

**Update Procedure for Bypass Rider:** The bypass rider's position update is offered on a random basis because they bypass the normal path without following the leading riders. Consequently, this is depicted in (13). Where $\eta$ and $\xi$ are values assigned with a random integer with ranges between 1, and RN $\delta$ and $\beta$ are random values between 0 and 1.

$$R_{t+1}^{B}(x,y)=\delta\left[R_t(\eta,y)+\beta(y)+R_t(\xi,y)*[1-\beta(y)]\right] \quad (13)$$

**Update Procedure for Follower:** Due to the follower location being updated by tracking the main rider's position, these riders achieve the destination successfully and quickly. Based on the coordinate selector, the location update of the follower is also computed for the specified values $P$ and is reported in (14)

$$R_{t+1}^{F}(x,c)=R^I(I,c)+\left[\cos\left(A_{x,c}^{t}\right)*R^I(I,c)*dis_x^t\right] \quad (14)$$

The distance that has to be travelled by $x$th rider is shown $dis_x^t$ and the leading rider's

position is presented as $R^I$ $x$ th rider's steering angle at $c$ the coordinate is shown as $A^t_{x,c}$.

**Update Procedure for Overtaker:** The coordinate selector, relative success rate, and direction indicator are all important variables in the overtaker update process. The overtaker's position update equation is represented in equation (15). The direction indicator for the $x$ th rider's is given $M_t(x)$ at the time $t$.

$$R^O_{t+1}(x,c)=R_t(x,c)+\left[M_t(x)*R^I(I,c)\right] \quad (15)$$

**Update Procedure for the Attacker:** As it seeks to steal the leading rider position, the attacker uses the same method as a follower to update its position. The attacker's position is updated in the following manner (16)

$$R^A_{t+1}(x,y)=R^I(I,c)+\left[\cos\left(A^t_{x,y}\right)*R^I(I,c)\right]+dis^t_x \quad (16)$$

Even if the ROA is relatively quick in identifying the best solutions, it makes sense if the algorithm is improved for a better problem-solving scenario. Consequently, the goal of this work is to offer a new enhanced idea in ROA called FCRO, which is based on the firefly method. The following is the proposed algorithm: Each iteration $t$ is evaluated to see if the current $t$ one achieves the optimal answer compared to the prior one $t-1$. The procedure is carried out as usual, if the evaluation is correct (finding the best option over the prior $t-1$). The parameter trail is set to 0 and the iterations continue if it is not improved. Consequently, the Hybrid - FCRO algorithm chooses the best CH and improves the network efficiency.

### 4.2 Malicious Node Detection

Identifying malicious, selfish, and compromised nodes that have been authenticated requires trust management. Accordingly, it has been widely explored in a variety of network contexts, including grid and pervasive computing, peer-to-peer networks, etc. Alternatively, for assessing a node's trust, trust management systems are tools as well as detecting unexpected node behaviour (either faulty or malicious) and hence selecting a node for routing. To increase the QoS metric performance, the research suggested a Ridge Regression Classification technique that finds the MANET's trustworthy nodes and transmission of data is carried on with the trusted MN. While allowing trustworthy nodes to route, effectively removing malicious and selfish nodes, the suggested technique effectively detects harmful and selfish nodes.

Clustering algorithms are employed in various detection tactics to detect malicious nodes, and they cluster the nodes into two groups, such as malicious and benign groups. Furthermore, the behaviour of other nodes along a node's linked multi-hop pathways might affect its trust value, lowering the performance of detection algorithms. Cluster the nodes into three groups: low trust value group (LTG), medium trust value group (MTG), and high trust value group (HTG) to improve detection accuracy. In order to capture additional information about them, inject the packets back into the network and improve the routing of broadcast packets to evaluate whether MTG nodes are benign or malicious, which can help the regression learn better. Subsequently, classify the nodes into malicious or benign using a clustering method based on the received trust levels.

#### 4.2.1 Ridge Regression Algorithm

In a MANET, each normal node has a classifier that can detect malicious nodes. Additionally, this strategy, which employs the observed behaviour of the nearby nodes by the normal node and the classifiers, is used by each normal node to regulate whether or not the neighbouring nodes are malicious. To make an accurate detection, there is adequate information about the observed behaviour and the detection operation can be carried out at any moment. When there is insufficient data, the Machine learning algorithms fail, therefore frequent execution of malicious node detection is unlikely. In these experiments, normal nodes determine whether or not their surrounding nodes are malicious after observing their behaviour for a length of time (e.g., 50 seconds or more). Consequently, the technique for detecting malicious nodes does

not suffer the significant computation costs of the normal nodes.

The ridge regression approach is used to detect the malicious node in this study. When the data is supplied as $(x_i, y_i)$ where $x_i = (x_{i1}, x_{i2}, \cdots, x_{ip})^T$ is the input and $y_i$ the output in the ridge regression process, a linear regression model can be stated as:

$$y_i = \beta_1 x_{i1} + \beta_2 x_{i2} + \cdots + \beta_p x_{ip} \quad (17)$$

Where the regression coefficients for various $x_i$ are represented as $\beta_1, \beta_2, \cdots, \beta_p$. The goal of linear regression is to select those $\beta_i$ with the smallest residual sum of squares. The optimization problem is therefore formulated as follows:

$$\min_{\beta} \left[ \sum_{i=1}^{N} \left( y_i - \sum_j \beta_j x_{ij} \right)^2 \right] \quad (18)$$

However, this model does not generalize well to new data (i.e., data with a lot of variation), resulting in overfitting. Ridge regression is utilised to solve this problem since it progressively narrows the regression coefficients, resulting in a stable model. Subsequently, by adding a constraint to the optimization problem of (18), ridge regression solves this problem. Consequently, the ridge regression optimization problem can be phrased as follows:

$$\min_{\beta} \left[ \sum_{i=1}^{N} \left( y_i - \sum_j \beta_j x_{ij} \right)^2 \right], s.t. \sum_j |\beta_j|^2 \le 1 \quad (19)$$

Introduce the Lagrange multiplier $\alpha$, commonly known as the regularization constant, to solve this optimization problem. The Ridge estimate $\hat{\beta} = (\hat{\beta}_1, \hat{\beta}_2, \cdots, \hat{\beta}_p)^T$ is then supplied as follows:

$$\hat{\beta} = \arg\min_{\beta} \left[ \sum_{i=1}^{N} \left( y_i - \sum_j \beta_j x_{ij} \right)^2 \right] + \alpha \sum_j |\beta_j|^2 \quad (20)$$

Subjected to the condition that for each $x_{ij}$, $\sum_i {x_{ij}}^2 / N = 1$. Where $\alpha$ the constant that determines the amount of regularization is applied and $\sum_j |\beta_j|^2$ is the regularization term. Set $\alpha = 1$ the maximum iterations to 10 in this experiment.

### 4.3 Trust-Based Routing Protocol

The routing of trustworthy nodes is permitted, but malicious/selfish nodes are promptly eliminated. To reduce routing overhead in MANET, the multipath routing technique is implemented. Consequently, by reducing network traffic, it can be achieved. Accordingly, the broadcasting message's effectiveness is improved is the goal of this study and it is also used to reduce the routing overhead. Routing is the method of transferring data from one location to another. In order to reach their destination, it also allows messages to travel from one driving node to another. Subsequently, to identify the best-forwarded path in MANET to reduce routing overhead, the Atom Emperor Penguin Optimization (AEPO) method is used to introduce a trust-based secure routing protocol. In order to choose the best path for trust evaluation criteria such as average encounter rate (AER), forwarding rate, Successful Cooperation Frequency (SCF), and integrity factor, the developed algorithm is used. Consequently, the sender nodes can reduce delay and enhance their data transmission rates as enabled by this evaluation.

#### 4.3.1 Atom Emperor Penguin Optimization (AEPO) Algorithm

Atom search optimization (ASO) is a recently proposed optimization algorithm based on molecular dynamics. In order to discover the optimal forwarding path, the ASO is paired with the emperor penguin colony optimization method. The location of atoms in ASO is updated by:

$$x_i(t+1) = x_i(t) + v_i(t+1) \quad (21)$$

Where $x_i(t+1)$ is the $i$th atom's position in the $(t+1)$th iteration, $x_i(t)$ is the $i$th atom's location in the $t$th iteration, and $v_i(t+1)$ is the $i$th atom's velocity in the $(t+1)$th iteration, and is computed as follows:

$$v_i(t+1)=rand\times v_i(t)+a_i(t) \tag{22}$$

Where $a_i(t)$ the acceleration of the $i$th atom in the $t$th iteration and the rand is a random number in [0, 1] is determined as follows:

$$a_i(t)=-\eta(t)\sum_{j\in K\,best}\frac{rand\left[2\times\left(h_{ij}(t)\right)^{13}-\left(h_{ij}\right)^{7}\right]}{m_i(t)}\times\frac{x_i(t)-x_j(t)}{x_i(t),x_j(t)_2}+\beta e^{-\frac{20t}{T}}\times\frac{x_{best}(t)-x_i(t)}{m_i(t)} \tag{23}$$

Where $\beta$ is the multiplier weight, $T$ is the maximum number of iterations, $x_{best}$ is the best atom in the current iteration, and $Kbest$ is a subset of the best atoms, $\eta(t)$, $h_{ij}(t)$, and $m_i(t)$ are determined using equations 4, 5, and 6.

Where, $\eta(t)=\alpha\times\left(1-\frac{t-1}{T}\right)^3\times e^{-\frac{20t}{T}}$,

$$h_{ij}(t)=\begin{cases}h_{\min} & \frac{r_{ij}(t)}{\sigma(t)}<h_{\min}\\ \frac{r_{ij}(t)}{\sigma(t)} & h_{\min}\le\frac{r_{ij}(t)}{\sigma(t)}\le h_{\max}\\ h_{\max} & \frac{r_{ij}(t)}{\sigma(t)}>h_{\max}\end{cases},$$ and

$m_i(t)=\frac{M_i(t)}{\sum_{j=1}^{N}M_j(t)}$. Accordingly, $\alpha$ the depth weight $r_{ij}(t)$ is the distance between $i$th and $j$th atoms at the $t$th iteration, $h_{\min}$, $h_{\max}$, $\sigma(t)$, and $M_i(t)$ are calculated as: $h_{\min}=g_0+g(t)$, $h_{\max}=u$, $\sigma(t)=x_{ij}(t)$, $\frac{\sum_{j\,\varepsilon\,Kbest}x_{ij}(t)}{K(t)}$, and $M_i(t)=e^{-\frac{Fit_i(t)-Fit_{best}(t)}{Fit_{worsrt}(t)-Fit_{best}(t)}}$.

Where $g_0$ is equal to 1.1, $u$ is equal to 1.24, $g(t)$ and $K(t)$ are estimated as:

$$g(t)=0.1\times\sin\left(\frac{\pi}{2}\times\frac{t}{T}\right) \tag{24}$$

$$K(t)=N-(N-2)\times\sqrt{\frac{t}{T}} \tag{25}$$

Where $N$ is the number of atoms. Subsequently, each penguin's cost and location are calculated. Penguins are priced against one another. Penguins will always choose a penguin with a low absorption cost (high heat intensity). The cost is influenced by the temperature and the length of the journey involved. During the attraction process, the heat strength will be adjusted as necessary. The best answer is chosen after all others have been sorted. Heat radiation, association, and heat absorption are all subjected to a damping ratio. In algorithm 1, pseudo-code for the EPC algorithm is described. The following are the rules that apply to this algorithm:

- Every penguin in the original population radiates heat and is drawn to others with a similar thermal absorptivity.
- All penguins are thought to have the same body surface area.
- The influence of the earth's surface and atmosphere are not taken into account when the penguin absorbs all of the thermal radiation.
- Penguin heat radiation is a straight line.
- The attraction between two penguins is determined by the quantity of heat that separates them. Longer distances receive less heat, while shorter distances receive more heat.
- Accordingly, there is a variation with a consistent distribution in the spiral movement of the penguins during the absorption process.

**Heat Radiation:** The heat radiation transfer must be computed to determine the intensity and attractiveness of the heat. Each penguin's body surface area must be calculated to determine how much heat it radiates.

$$Q_{penquin}=A\varepsilon\sigma T_s^4 \tag{26}$$

Where heat transfer is defined as $Q_{penquin}$ that will be calculated for unit time $(W)$, the total surface area $0.56 m^2$ is denoted as $A$. $T_s^4$ is the absolute temperature in Kelvin (K) and 35 degrees Celsius $(^\circ C)$ is equal to 308.15 K, the emissivity of bird plumage is $\varepsilon$. The Stefan–Boltzmann constant is also known as $\sigma(5.6703\times 108 W/m^2 k^4)$.

**Attractiveness:** Finally, the attractiveness Q is defined as,

$$Q = A\varepsilon\sigma T_s^4 e^{-\mu s} \tag{27}$$

**Spiral Movement:** In this scenario, the system's structure features have uncertain borders and a spiral pattern around the centre. The centre of the huddle is the warmest temperature, whereas the outside is significantly colder. Penguins do not compete for personal advantage. Consequently, the entire huddle moves in a leisurely spiral motion, with each penguin taking turns at all spots in the formation.

$$x_k = ae^{b\frac{1}{b}\ln\left\{(1-Q)e^{b\tan -i\frac{yj}{xi}}\right\}}\cos\left\{\frac{1}{b}\ln\left\{(1-Q)e^{b\tan -i\frac{yj}{xi}}+Qe^{b\tan -i\frac{yj}{xi}}\right\}\right\} \tag{28}$$

$$y_k = ae^{b\frac{1}{b}\ln\left\{(1-Q)e^{b\tan -i\frac{yJ}{xi}}\right\}}\sin\left\{\frac{1}{b}\ln\left\{(1-Q)e^{b\tan -i\frac{yj}{xi}}+Qe^{b\tan -i\frac{yj}{xi}}\right\}\right\} \tag{29}$$

**New Position:** Equation (15) is used to calculate the new position, and it is multiplied by the mutation factor and by a random vector, respectively, to arrive at the new position. The random vector's coefficient is tacked on in this fashion.

The data window is moved one step forward when the signals are reconstructed and all parameters with variables are obtained after a certain number of iterations, then the recovery algorithm is reworked again. Subsequently, for each initialization, global convergence can be provided by EPC and solves the problem of convex optimization. Consequently, this Atom Emperor Penguin Optimization (AEPO) algorithm finds the best forwarding paths to route the nodes in the MANET.

## 5. Experimentation and Result Discussion

The proposed method's performance is evaluated using the Matlab software with the version R2021a, their operating system is Windows 10 Home. The memory capacity of the proposed method is 6 GB DDR3, with the processor of Intel Core i5 @ 3.5 GHz. MATLAB simulation software is utilized for verifying the validity of the proposed AEPO algorithm. Subsequently, the detailed settings of simulation parameters are listed in Table 2. The simulation parameters are described, that the number of nodes utilized in this work is 100, the initial energy of each node is 0.5 J, transmitter and receiver required to run circuity is $50*10^{-9}$J/bit. Accordingly, the number of decision variables is 200, the number of initial dead nodes is 0, the size of the message is 128 bytes, and the number of iterations is 100, respectively.

**Table 2:** Simulation Parameters

| Parameters | Values |
|---|---|
| Number of Nodes | 100 |
| Initial Energy of Each Node | 0.5 (Joule) |
| Transmitter Energy Required to Run Circuity | $50*10^{-9}$(Joules /bit) |
| Receiver Energy Required to Run Circuity | $50*10^{-9}$J/bit |
| Number of Decision Variables | 200 |
| Data Aggregation Energy | $50*10^{-9}$(Joules /bit) |
| Number of Initial Operating Nodes | 100 |
| Number of Initial Dead nodes | 0 |
| Packet Size | 128 bytes |
| Number of Iterations | 100 |

Subsequently, the proposed technique's performance is evaluated based on various

parameters including PDR, packet loss ratio (PLR), end-to-end delay, throughput, normalized energy analysis, and normalized routing overhead. Accordingly, the proposed AEPO algorithm is compared with the existing Hybrid Particle Swarm Optimization-Genetic Algorithm (PSO-GA)Hamza, F, *et al* (2021)[27], Ticket ID Cluster Manager (TID-CMGR) Venkatasubramanian, *et al* (2021)[28], and Modified Firefly Algorithm (MFFA)Kumar, (2021)[29].

**Packet Delivery Ratio:** PDR is calculated as the ratio of the number of data packets received to the total number of data packets sent via trusted nodes. PDR is formalized as below,

$$PDR = \left( \frac{n_{Dp_i} R_x}{n_{Dp_i} T_x} \right) * 100 \tag{30}$$

The above equation (30), $n_{Dp_i}$ indicates several data packets, $R_x$ symbolizes received $T_x$ and is then transmitted. PDR is calculated in percentage (%).

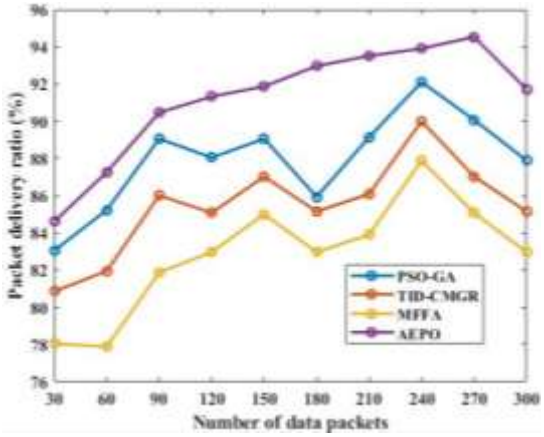


**Figure 2:** Performance Graph for Packet Delivery Ratio

Figure 2 represents the PDR graph and the values of the proposed AEPO algorithm compared with the existing PSO-GA, TID-CMGR, and MFFA methods. The PDR represents the number of packets successfully received at the destination end from the packets to be sent. The PDR of the proposed AEPO algorithm is approximately 2% higher than the other existing methods.

**Packet Loss Rate:** The ratio of the number of data packets lost to the total number of data packets send is used to calculate PLR. The formalized PLR is as follows:

$$PLR = \left( \frac{n_{Dp_i} lost}{n_{Dp_i} T_x} \right) * 100 \tag{31}$$

From (31), $n_{Dp_i}$ indicates several data packets, $T_x$ are then transmitted. PLR is calculated in percentage (%).

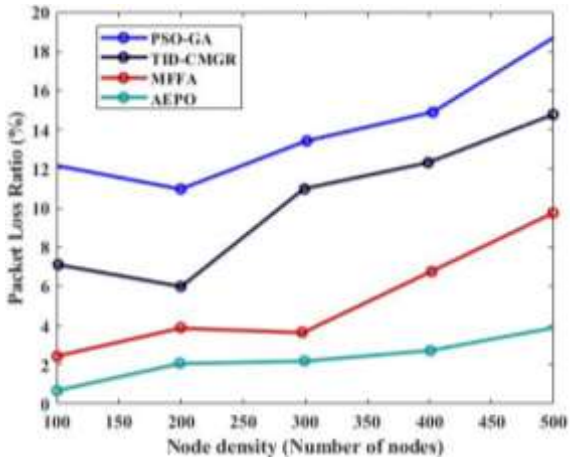


**Figure 3:** Performance Graph for Packet Loss Ratio

Figure 3 illustrates the graph of PLR compared with different existing methods like PSO-GA, TID-CMGR, and MFFA methods. The PLR is measured based on the node density subsequently, the performance of the proposed AEPO algorithm is 5% higher than the existing PSO-GA, 3% higher than the TID-CMGR, and 1.5% higher than the MFFA methods.

**End to End Delay:** E2E delay is calculated as the time difference between the data packet arriving at the destination and the data packet sent from the source node. E2E delay is formalized as below,

$$E2E\ delay = \left( T_{al} - T_{sd} \right) \tag{32}$$

From (32), the data packet arrival time is indicated as $T_{al}$, and the data packet sending

time is indicated as $T_{sd}$. In milliseconds (ms), the $E2E\,delay$ is determined.

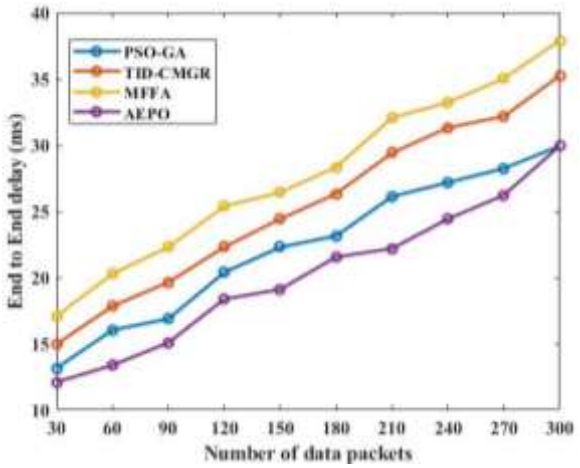


**Figure 4:** Result for End-to-End Delay

The end-to-end delay graph is portrayed in figure 4. The end-to-end delay for the proposed AEPO algorithm is compared with the existing PSO-GA, TID-CMGR, and MFFA. Subsequently, it depicted that the AEPO algorithm performs the best performance than the other existing methods. Accordingly, it portrays that the AEPO method is approximately 2% higher than the other existing methods, respectively.

**Throughput:** The throughput measure defines the total packets sent by the transmitter node to the total packets received at the receiver end.

$$Throughput = \frac{Packets\ \mathrm{Re}ceived \times Packet\ Size}{t} \tag{33}$$

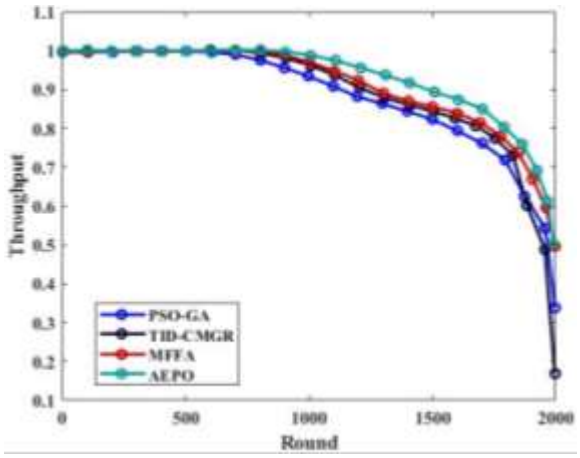


**Figure 5:** Performance Graph for Throughput

Figure 5 depicts the throughput of the proposed AEPO algorithm. Consequently, the suggested method is compared to the existing PSO-GA, TID-CMGR, and MFFA. The throughput is evaluated based on the rounds from 0 to 2000, and the initial throughput value is 1. When the round is 1000 to 1500, the throughput is gradually decreased to 0.8 and when it reaches 1500 to 2000, the throughput is suddenly reduced to 0.17. Consequently, the AEPO algorithm performs better than the other methods, and it is roughly 3% higher than the existing methods.

**Routing Overhead (RO):** Network overhead is the number of control (hello packets) and routing packets required for overall network communication.

$$Overhead\,(in\ ratio) = \frac{Total\ Contol\ and\ Routing\ Packet}{Number\ of\ Data\ Packets\ \mathrm{Re}ceived} \tag{34}$$

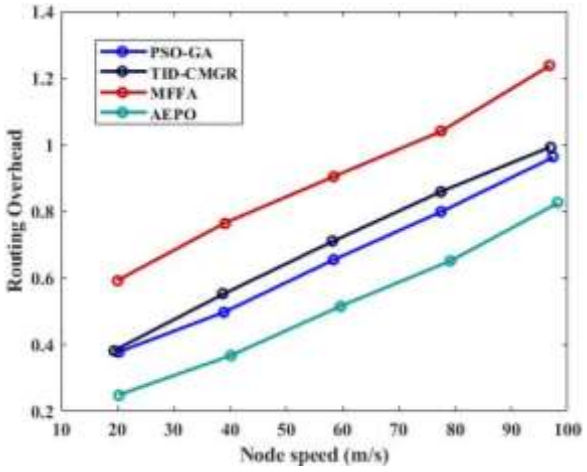


**Figure 6:** Graph for Routing Overhead

Figure 6 elucidates the performance and the comparison graph for routing overhead. The AEPO algorithm is compared with the various algorithm including PSO-GA, TID-CMGR, and MFFA. The experimental results proved that the proposed algorithm has taken very less RO when compared with other existing algorithms. Subsequently, their performance of the AEPO algorithm is approximately 4% higher, respectively.

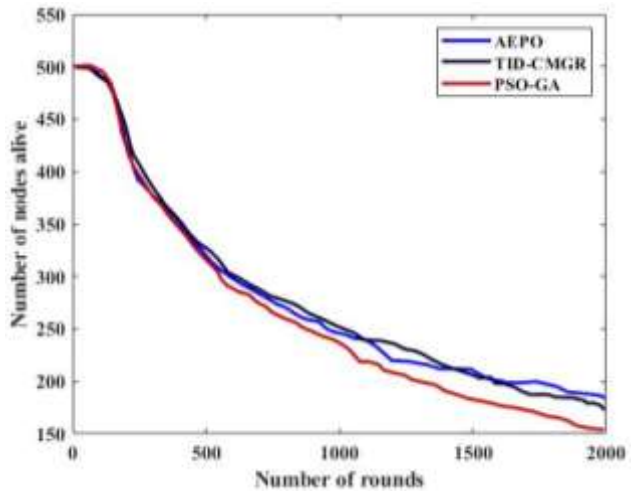


**Figure 7:** Graph for Number of Alive Nodes

Figure 7 delineates the analysis of alive nodes of the proposed AEPO model and the conventional models. The existing methods like PSO-GA, and TID-CMGR. The alive nodes have to be at maximum for the AEPO algorithm. From the starting itself, the alive nodes are at maximum and in the subsequent rounds, it gets decreases as the rounds increase. The alive nodes are initially at maximum with a count of 500. Subsequently, it gradually decreases and reaches the count within the range of 150–200.

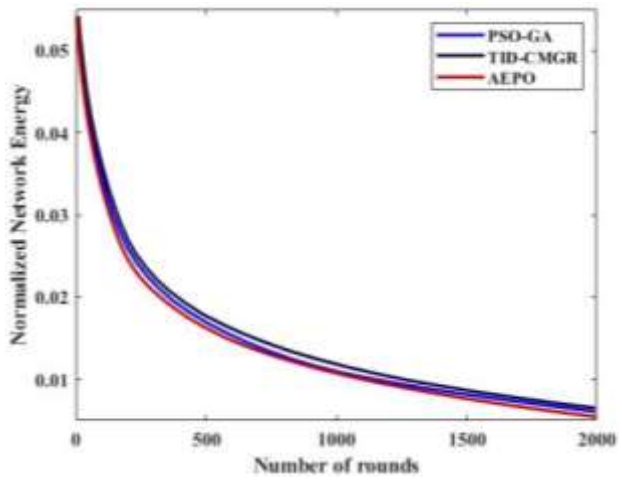


**Figure 8:** Normalized Network Energy Analysis

The analysis of the normalized energy of the proposed over the conventional models is described in figure 8. The existing methods like PSO-GA, and TID-CMGR.Initially, the normalized network energy is fixed within the interval of 0.05 to 0.06. Consequently, during the 2000th round, the energy would steadily decline to the bottom, until the normalized energy of the proposed AEPO algorithm reaches a value in the range of 0 to 0.01 and is maximal when compared to other traditional models.

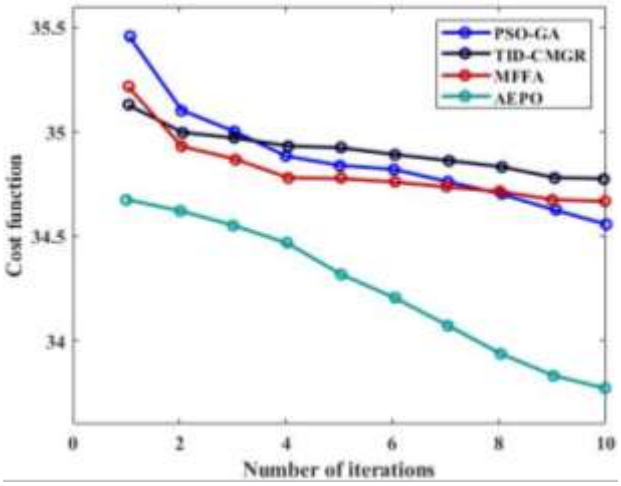


**Figure 9:** Cost Function of the AEPO Algorithm

The analysis of the cost function of the proposed and classical models is depicted in figure 9. The graph explains the AEPO algorithm with a lower cost function than any of the other models. Continuously, at the eighth iteration, the performance of the AEPO algorithm achieves the lowest cost function which is 3%, 3.5%, and 3.1% better than PSO-GA, TID-CMGR, and MFFA, respectively. The analysis has made clear that the adopted model achieves a lower cost function than the other related conventional models.

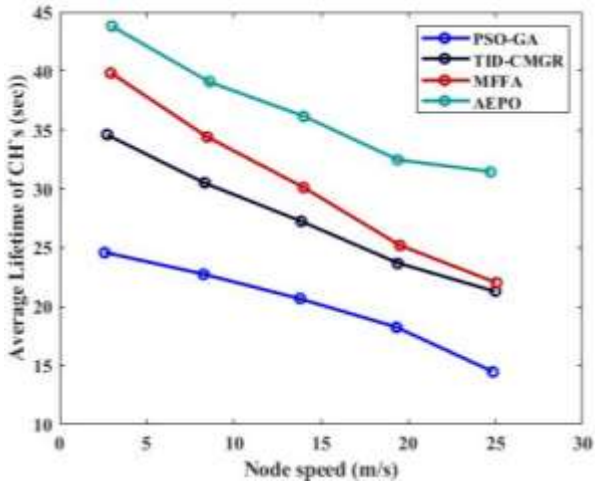


**Figure 10:** Performance Graph for Average Life Time of CH

The average lifetime of CH is portrayed in figure 10; it compares the AEPO method with the existing methods. The AEPO algorithm has a higher value than the other existing methods. The existing methods like PSO-GA, TID-CMGR, and MFFA. The CH has a maximum lifetime than the other existing methods and the AEPO algorithm is approximately 5.1%, 4.2%, and 3.5% higher than the existing methods.

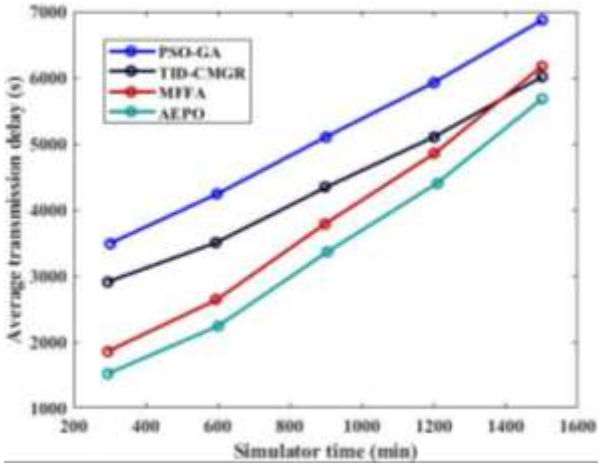


**Figure 11:** Performance Graph for Average Transmission Delay

The average transmission delay graph is demonstrated in above figure 11. The transmission delay for the AEPO algorithm is less than the other, subsequently, the AEPO algorithm is higher than the existing PSO-GA, TID-CMGR, and MFFA. The average transmission delay is measured with the simulation time as 200 minutes to 1600 min, respectively.

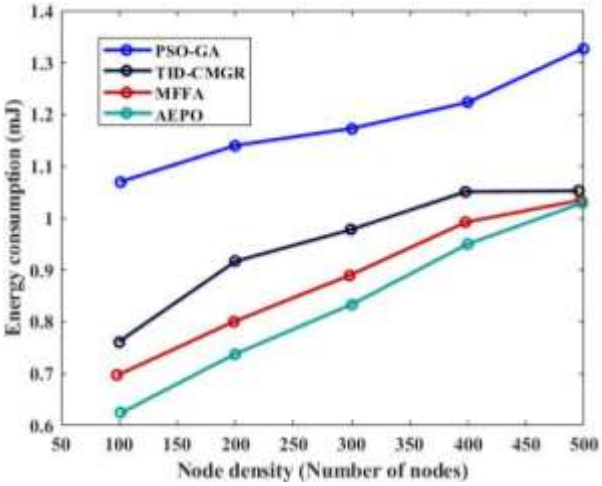


**Figure 12:** Performance Graph for Energy Consumption

The energy consumption of the AEPO algorithm is illustrated in figure 12; it demonstrates that the AEPO algorithm has less energy consumption than the other existing methods. The energy consumption is evaluated based on the node density, in this work, the node density is taken between 50 to 500. Subsequently, the AEPO algorithm is approximately 4.8%, 2.3%, and 0.8% higher than the PSO-GA, TID-CMGR, and MFFA.

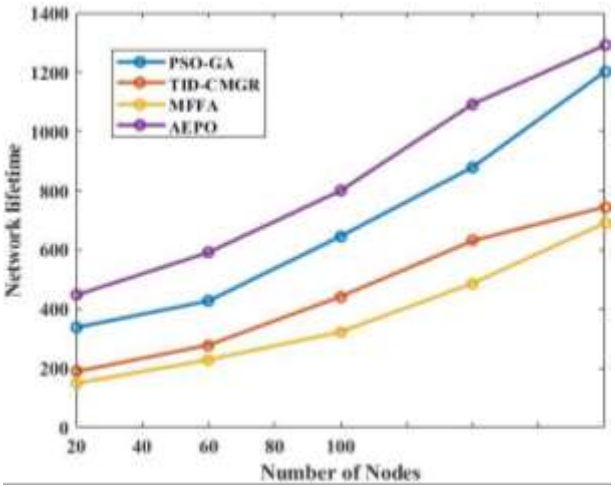


**Figure 13:** Performance Graph for the Network Lifetime

The network lifetime graph for the AEPO algorithm is portrayed in figure 13. Additionally, it depicted that the network lifetime of the AEPO algorithm produces higher values than the other methods. The network lifetime is evaluated for the number of nodes from 20 to 100. The AEPO algorithm is 2%, 3.5%, and 4% higher than the existing PSO-GA, TID-CMGR, and MFFA.

**Table 3:** Comparison Table of the Research Work

| | | | **PSO-GA** Hamza *et al.,* 2021 | **TID-CMGR** Venkatasubramanian *et al.,* 2021 | **MFFA** Kumar *et al.,* 2021 | **AEPO Proposed** |
|---|---|---|---|---|---|---|
| **PDR (%)** | **No.of Packets** | **30** | 83.1 | 80.8 | 78 | 84.8 |
| | | **300** | 88 | 85.3 | 83 | 91.1 |
| **PLR (%)** | **No.of Nodes** | **100** | 12 | 7.3 | 2.2 | 0.53 |
| | | **500** | 18.8 | 14.5 | 10 | 3.94 |
| **End to End Delay (ms)** | **No.of Packets** | **30** | 13.5 | 15 | 17.5 | 12 |
| | | **300** | 30 | 35 | 35 | 30 |
| **Throughput** | **Round** | **500** | 1 | 1 | 1 | 1 |
| | | **2000** | 0.34 | 0.17 | 0.497 | 0.5 |
| **Average Transmission Delay (s)** | **Simulator Time (min)** | **300** | 3500 | 2990 | 1900 | 1500 |
| | | **1500** | 6980 | 6000 | 6150 | 5800 |
| **Energy Consumption (mJ)** | **Node Density** | **100** | 1.08 | 0.77 | 0.7 | 0.62 |
| | | **500** | 1.33 | 1.05 | 1.03 | 1.02 |
| **Network Lifetime** | **No.of Nodes** | **20** | 340 | 200 | 180 | 430 |
| | | **180** | 1200 | 750 | 690 | 1310 |
| **Normalized Network Energy** | **No.of Rounds** | **500** | 0.017 | 0.018 | - | 0.0165 |
| | | **2000** | 0.002 | 0.004 | - | 0.001 |
| **Transmission Success Rate** | **Simulator Time (min)** | **200** | 0.78 | 0.69 | 0.502 | 0.87 |
| | | **1200** | 0.5 | 0.49 | 0.54 | 0.65 |

Table 3 reveals the comparison table of the work, it portrays the performance values for PDR, PLR, end-to-end delay, throughput, average transmission delay, energy consumption, network lifetime, normalized network energy, and transmission success rate. The table portrays both the existing and proposed methods, the existing methods like PSO-GAHamza, F, *et al* (2021), TID-CMGR Venkatasubramanian, *et al* (2021), and MFFAKumar, (2021).

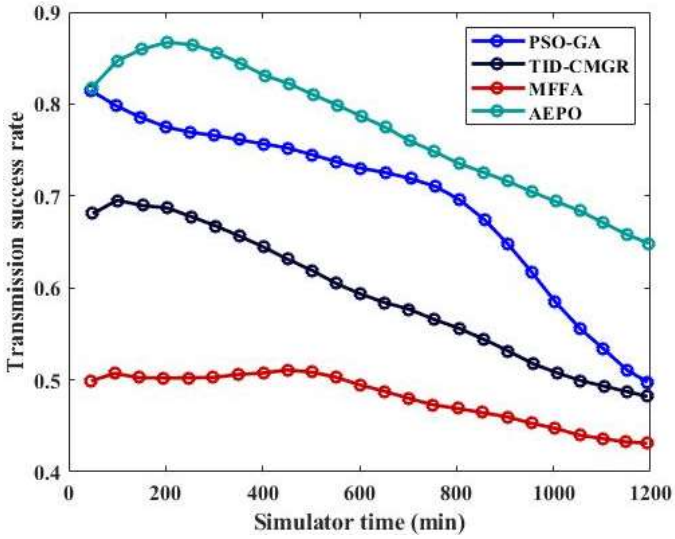


**Figure 14:** Graph for Transmission Success Rate

The transmission success rate graph of the AEPO algorithm is portrayed in figure 14. The figure demonstrates that the transmission success rate of the proposed method is higher than the other existing methods. The transmission success rate of the AEPO algorithm ranges from 0.8 to 0.65 for the simulation time of 0 to 1200 min. The AEPO algorithm is approximately 4%, 4.1%, and 5.4% higher than PSO-GA, TID-CMGR, and MFFA, respectively.

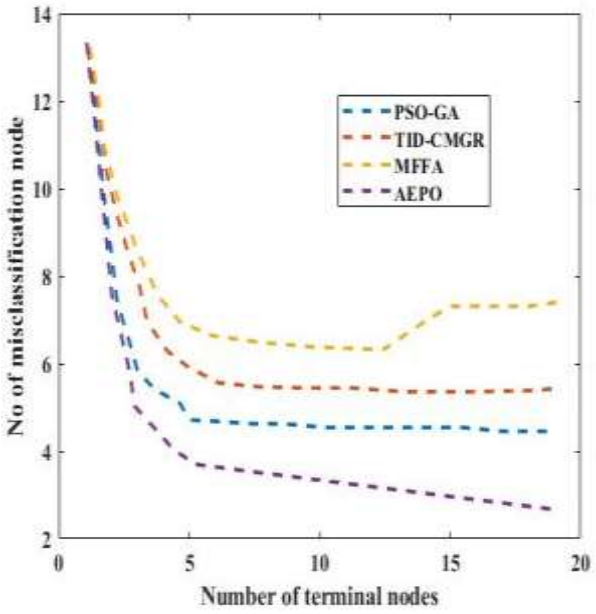


**Figure 15:** Misclassification Node vs Terminal Node

Figure 15 portrays the graph for the number of misclassification nodes vs the number of terminal nodes. The proposed method is compared with the existing PSO-GA, TID-CMGR, and MFFA methods. While compare to these existing methods, the proposed method produces low misclassification nodes.

## 6. Conclusion

MANETs are noticeable by an individual feature which contains the nonappearance of any essential organization else any necessitate for infrastructure unit. Many hop topologies are outlined in the network. Subsequently, with the help of a comprehensive source known as energy, extreme mobile nodes form and an ad hoc network is powered. Accordingly, there has been no major improvement in the domain of energy characteristics to reduce energy usage, the lifespan of a network is heavily reliant on the technology incorporated within the rules' sequence. In this research, a Hybrid Firefly Cyclic Rider Optimization (FCRO) algorithm is presented to select the CH. Accordingly, it improves the MANET network efficiency. Subsequently, malicious node detection is an important process, in this malicious node is detected using the Ridge Regression

Classification algorithm, which classifies malicious nodes and trusted nodes. Accordingly, Hybrid Firefly Cyclic Rider Optimization (FCRO) algorithm is presented to route the nodes to the destination node.

- ❖ Subsequently, the proposed method is implemented using MATLAB software.
- ❖ The performance metrics are packet deliver ratio, packet loss ratio, Routing overhead, throughput, end-to-end delay, transmission delay, network lifetime, and energy consumption.
- ❖ The AEPO algorithm is compared with the existing PSO-GA, TID-CMGR, and MFFA.
- ❖ The performance of the proposed AEPO algorithm is approximately 1.5%, 3.2%, 2%, 3%, and 4% higher than the existing methods for PDR, PLR, end-to-end delay, throughput, and network lifetime.

Accordingly, this analysis allows sender nodes to reduce the delay and improve their data transmission speeds. In terms of demonstrating the true contribution of different nodes to trust evaluation, the proposed method has an obvious advantage. Consequently, the routing technique will be used in future investigations to achieve a secure and effective transmission. Future work should focus on improving data transmission security by utilising authentication approaches to manage the increased demand and higher security. Table 4 shows the abbreviations used in the article.

**Table 4:** Abbreviations

| | |
|---|---|
| PSO-GA | Hybrid Particle Swarm Optimization-Genetic Algorithm |
| TID-CMGR | Ticket ID Cluster Manager |
| MFFA | Modified Firefly Algorithm |
| FCRO | Hybrid Firefly Cyclic Rider Optimization |
| AEPO | Atom Emperor Penguin Optimization |
| PDR | Packet Delivery Ratio |
| PLR | Packet Loss Rate |
| CH | Cluster Heads |
| QoS | Quality of Service |
| MN | Mobile Node |
| RO | Routing Overhead |

*References*

[1] Xu, J., Feng, S., Liang, W., Ke, J., Meng, X., Zhang, R. and Shou, D., 2020. An algorithm for determining data forwarding strategy based on recommended trust value in MANET. International Journal of Embedded Systems, 12(4), pp.544-553.

[2] Alkhamisi, A.O., Buhari, S.M., Tsaramirsis, G. and Basheri, M., 2020. An integrated incentive and trust-based optimal path identification in ad hoc on-demand multipath distance vector routing for MANET. International Journal of Grid and Utility Computing, 11(2), pp.169-184.

[3] Yang, H., 2020. A study on improving secure routing performance using trust model in MANET. Mobile Information Systems, 2020.

[4] Nandgave-Usturge, S., 2020. Water spider monkey optimization algorithm for trust-based MANET secure routing in IoT. Int J Scientific Res Eng Trends, 6(2), pp.980-984.

[5] Abhilash, K.J. and Shivaprakasha, K.S., 2020. Secure routing protocol for MANET: A survey. In Advances in communication, signal processing, VLSI, and embedded systems (pp. 263-277). Springer, Singapore.

[6] Malik, N.A. and Rai, M., 2020, April. Enhanced secure and efficient key management algorithm and fuzzy with trust management for MANETs. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC).

[7] Panwar, A., Panwar, B., Rao, D.S. and Sriram, G., 2020. A trust based approach for avoidance of wormhole attack in Manet. International Journal of Computer Science and Mobile Computing, 9, pp.47-57.

[8] Thapar, S. and Sharma, S.K., 2020, November. Direct Trust-based Detection Algorithm for Preventing Jellyfish Attack in MANET. In 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 749-753). IEEE.

[9] Gomathy, V., Padhy, N., Samanta, D., Sivaram, M., Jain, V. and Amiri, I.S., 2020. Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks. Journal of Ambient Intelligence and Humanized Computing, 11(11), pp.4995-5001.

[10] Gupta, M., Garg, P., Gupta, S. and Joon, R., 2020. A Novel Approach for Malicious Node Detection in Cluster-Head Gateway Switching Routing in Mobile Ad Hoc Networks. International Journal of Future Generation Communication and Networking, 13(4), pp.99-111.

[11] Hassan, K.L., Mandal, J.K. and Mondal, S., 2020. A Dynamic Threshold-Based Trust-Oriented Intrusion Detection System in MANET. In Proceedings of the Global AI Congress 2019 (pp. 699-711). Springer, Singapore.

[12] Fatemidokht, H. and Rafsanjani, M.K., 2020. QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks. Journal of Systems and Software, 165, p.110561.

[13]Gu, K., Dong, X. and Jia, W., 2020. Malicious node detection scheme based on correlation of data and network topology in fog computing-based VANETs. IEEE Transactions on Cloud Computing.

[14] Ghaleb, S.A.M. and Vasanthi, V., 2020. Energy Efficient Multipath Routing Using Multi-Objective Grey Wolf Optimizer based Dynamic Source Routing Algorithm for MANET. International Journal of Advanced Science and Technology, 29(3), pp.6096-6117.

[15] Chen, Z., Zhou, W., Wu, S. and Cheng, L., 2020. An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET. IEEE Access, 8, pp.44760-44773.

[16] Balshetwar, S.V., Tugnayat, R.M. 2015. Techniques for Analyzing Framed Data, Global Journal of Engineering Science and Researches, 2(8), 80-83.

[17] Aruna, R., Subramanian, R., Sengottuvelan, P. and Shanthini, J., 2019. Optimized energy efficient route assigning method using related node discovery algorithm in MANET. Cluster Computing, 22(1), pp.469-479.

[18] Anugraha, M. and Krishnaveni, S.H., 2022. SRTE: Security Resource Allocation for Trust Model in Evaluate the Strong Node. Webology, 19(1).

[19] Das, M.V., Premchand, P. and Raju, L.R., 2021. Security Enhancing based on Node Authentication and Trusted Routing in Mobile Ad Hoc Network (MANET). Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(14), pp.5199-5211.

[20] Sirajuddin, M., Rupa, C., Iwendi, C. and Biamba, C., 2021. TBSMR: a trust-based secure multipath routing protocol for enhancing the QoS of the mobile ad hoc network. Security and Communication Networks, 2021..

[21] Jari, H., Alzahrani, A. and Thomas, N., 2021, November. A Novel Indirect Trust Mechanism for Addressing Black hole Attacks in MANET. In Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (pp. 27-34).

[22] Gopala Krishnan, C., Nishan, A.H., Gomathi, S. and AravindSwaminathan, G., 2022. Energy and Trust Management Framework for MANET using Clustering Algorithm. Wireless Personal Communications, 122(2), pp.1267-1281.

[23] Kaur, J. and Kaur, S., 2021. Novel trust evaluation using NSGA-III based adaptive neuro-fuzzy inference system. Cluster Computing, 24(3), pp.1781-1792.

[24] Anitha Josephine, J. and Senthilkumar, S., 2021. Tanimoto support vector regressive linear program boost based node trust evaluation for secure communication in MANET. Wireless Personal Communications, 117(4), pp.2973-2993.

[25] Sathyaraj, P. and Rukmani Devi, D., 2021. Designing the routing protocol with secured IoT devices and QoS over Manet using trust-based performance evaluation method. Journal of Ambient Intelligence and Humanized Computing, 12(7), pp.6987-6995.

[26] Kumar, R. and Shekhar, S., 2021. Trust-Based Fuzzy Bat Optimization Algorithm for Attack Detection in Manet. In Smart Innovations in Communication and Computational Sciences (pp. 3-12). Springer, Singapore.

[27]Hamza, F. and Vigila, S.M.C., 2021. Cluster Head Selection Algorithm for MANETs Using Hybrid Particle Swarm Optimization-Genetic Algorithm. Int. J. Comput. Netw. Appl, 8(2), pp.119-129.

[28]Venkatasubramanian, S., Suhasini, A. and Vennila, C., 2021. An Energy Efficient Clustering Algorithm in Mobile Adhoc Network Using Ticket Id Based Clustering Manager. International Journal of Computer Science & Network Security, 21(7), pp.341-349.

[29]Kumar, M., 2021. An Optimized Utilization of Battery Backup in MANET Using Modified Firefly Algorithm. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(2), pp.2086-2094.

**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.