International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

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

S. Mohan[1], Dr. P. Vimala[2]
[1]Research Scholar, Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, Annamalai University, Annamalai Nagar, Chidambaram, Tamil Nadu, 608 002, India
Email: mohann85@yahoo.co.in
[2]Asst. Professor, Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, Annamalai University, Annamalai Nagar, Chidambaram, Tamil Nadu, 608 002, India
Email: vimalakathirau@gmail.com

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 for-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 (CH) selection, it efficiently selects the CH and improves the network efficiency. The Ridge Regression Classification algorithm is presented in this work to sense the malicious nodes in the network and the data is transmitted using trusted Mobile nodes for the QoS enactment metric improvement. A trust-based routing protocol (TBRP) is introduced utilizing the Atom Emperor Penguin Optimization (AEPO) algorithm, it identifies the best-forwarded path to moderate the routing overhead problem in MANET. The planned method is implemented using Matlab software and the presentation metrics are packet delivers ratio, packet loss ratio (PLR), routing overhead, throughput, end-to-end delay (E2ED), transmission delay, energy consumption and network lifetime. The suggested AEPO algorithm is compared with the prevailing 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 PLR, packet delivers ratio, throughput, and E2ED and network lifetime. The sender nodes can increase their information transmission rates and reduce delays in appreciation of this evaluation. Additionally, the suggested technique has a perfect benefit in terms of demonstrating the genuine contribution of distinct nodes to trust evaluation (TE).

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

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are self-contained systems fabricated 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, movement, and external noise working 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 custom of MANETs. 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, private sectors, and commercial. 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 flexibility are insufficient to ensure efficient transmission [5]. To ensure efficient transmission and avoid malicious attacks, a TBRP is used.

MANET Security

In MANETs, security often entails protecting and maintaining data integrity and confidentiality, in addition to each network node supplying 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 members of the network is essential to the MANET's feasibility. To deal with data forging and hacking attacks, a range of security measures have been developed, such as message encryption algorithms,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

secure authentication, and message integrity verification [7]. Moreover, in many other attacks like denial of service, node capture attacks, etc., these solutions are ineffective. The resistance efficiency is lower nonetheless by node captured causes the internal attacks and external attacks are effectively fought by the outdated safety mechanisms [8]. Data are essential to 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 gathering attitude based on TE was implemented in [9] for the identification of the malicious node. The planned 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 to this system, allowing nodes to indicate more experienced next-hop forwarders. 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 these nodes, the trustworthiness of a node, flexibility 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 selected CH will be the most efficient for almost all node characteristics are taken into account when calculating weights. [15]. accordingly, by maintaining both trust and energy efficiency, a TBRP is developed is the most difficult task in developing a TE for MANET [16]. The residual portion of the work is organized as follows, the study's literature survey is shown in part 2, while the problem statement and research rationale are exposed in section 3. The suggested research approach is demonstrated in section 4, the experiments and results are explained in section 5, and the study conclusion is revealed in section 6.

II. LITERATURE SURVEY

The study of secure MANET communication utilising various algorithms forms the basis of the literature survey. The survey portrays the routing methods for secure transmission and in this research, an AEPO algorithm is proposed for finding the best forwarding path, respectively. 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 dispersed weighted cluster-based protocol (CBPMD), TWCBRP shows improved presentation in footings of control overhead, packet delivery ratio (PDR), delay, and throughput when tested with Network Simulator (NS).

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.

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. TBSMR, a trust-based multipath routing protocol, was suggested by Sirajuddin et al. [20] to improve the overall performance of the MANET. Hassan Jari*et al* [21] examine the effects of a black dump attack on MANET routing systems. The aim of trust management (TM) is to retain 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. C. Gopala Krishnan *et al* [22] concentrated on detecting unstable CH and removing and replacing them with nodes that employ the self-configurable clustering method. To train the trust prediction model, JasleenKaur*et al* [23] suggested using the Adaptive neuro-fuzzy inference system (ANFIS) TM. The hyper-parameters of the ANFIS model are then tuned using a non-dominated sorting genetic algorithm-III (NSGA-III). In MANET, J. Anitha Josephine *et al* [24] proposed Tanimoto Support Vector Regression Based Corrective Linear Program Boost Classification (TSVR-CLPBC) as an ensemble

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

approach. 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 nevertheless also the presence of IoT devices and their trustworthiness. Trust and trust computations were discussed by Rakesh Kumar *et al* [26]. To limit the effects of attacks, a trust-based fuzzy bat (TBF) optimization model is suggested and implemented in this paper.

III. RESEARCH PROBLEM DEFINITION AND MOTIVATION

MANET is a hotspot for study for 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. Since mobile nodes enter and exit the network at unpredictable intervals, MANET does not have a fixed topology. Sensor nodes, in reality, have limited resources and other unique characteristics, making WSN TM more important and difficult.

Among the main research problems in networks is to implement effective routing with improved QoS. Scaling down ad-hoc networks and improving effective routing are two issues that are thought to be primarily solved by the clustering of nodes. From this, a recent algorithm is proposed for efficient routing and CH selection, and network lifetime improvement, respectively.

IV. 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 the unreliability of MANET wireless infrastructures, nodes are susceptible to several different security attacks, which disrupt the network structure. The architecture of the anticipated work is portrayed in figure 1.

Figure 1: Flow Diagram of the Proposed Work

In this MANET, the basis node is transferred to the destination node, initially, a Hybrid FCRO algorithm is proposed in this work for CH selection. Subsequently, a Ridge Regression Classification algorithm is presented to discover the malicious node in this network.

A. 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. A single machine is a node that is in control of data processing and archiving. A Hybrid Firefly Cyclic Rider Optimisation (FCRO) method for the best CH selection (CHS) is then suggested in this study to increase the MANET network's energy efficiency and lifespan.

Cluster Formation: According to the multi-hop communication technique, 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.

1. CH Selection

The best CH for data transmission necessity, therefore, be selected when clusters are established. Consequently, this research aims to select the greatest CH while taking into account key fitness criteria such as energy, distance, and latency, which have been noted as problems when choosing the CH.

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

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

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

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

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 D_y the distance of normal data and the count of nodes.

In (2), $f_{(a)}^{dis}$ the value needs to add a distance to it hence that the packets connected with it can be transferred quickly from the common node to the CH and the destination. The exact value obtained should be small and fall between [0, 1].

Energy: Equation (5) illustrates the fitness function for energy.

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

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.

Delay: The fitness function of the delay is directly proportional to the member count within the cluster. The fitness function for the delay is represented by equation (6).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

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

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.

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. Using the following objective function, the firefly's brightness is determined.

The variance in light intensity $I(r)$ is controlled by the inverse square law.

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

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

$$\beta = \beta_0 e^{-\gamma r^2} \quad (8)$$

Where the light absorption coefficient is denoted as γ and β_0 is the fluctuation of attractiveness $r = 0$. The distance between both fireflies at the location x_i x_j is calculated using the Euclidean distance. Consequently, it can be characterized as follows:

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

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

Utilizing a Gaussian delivery at the time t, the third term $\in_i^t$ denotes the production of random vectors.

3. Hybrid Firefly Cyclic Rider Optimization (FCRO) Approach

Every iteration of the firefly algorithm results in the brighter firefly attracting the less bright one. Consequently, in the position's random movement, this algorithm is effective at finding the correct response, however, it ignores firefly's best position for CH selection, and for finding the best solution, it influences the global exploration behaviour. The g_{best} p_{best} values derived by ROA are utilized by each firefly.

Optimal Selection of Cluster Count and CH: The two main optimisation problems that this research seeks to resolve are optimal cluster numbers and the selection of optimal CH. The best cluster counts k objective function OB_1 can be established in (11).

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

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

$$OB_2 = \min\left(F_3\right) \quad (12)$$

Where, $F_3 = \alpha * (F_2) + (1-\alpha) * f_i^{del}$,

$F_2 = \gamma * (F_1) + (1-\gamma) * \frac{1}{QoS}$, and $F_1 = \beta * \left(f_i^{dis}\right) + (1-\beta) * \frac{1}{f_i^{ene}}$.

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. Cyclic ROA Approach

ROA is a fictitious algorithm of computing constructed on the inspiration of a group of riders that strive to reach a specific destination to win the race. Follower, Bypass rider, overtake, and attacker are the four groups. The following methods are used by each group to reach the target:

- The path of leading is avoided to get to the destination is the main objective of bypass rider.
- To reach the destination, point as quickly as possible, the attackers capture the rider's path.

The winner is then announced with the leading driver. The Cyclic ROA model process is presented in table 1.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

TABLE I: 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 Brake 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
Select 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

Update Procedure for Bypass Rider: The bypass rider's position update is offered on a random basis for they bypass the normal path without following the leading riders. Consequently, this is depicted in (13).

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

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 the 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 $A_{x,c}^t$.

Update Procedure for Overtaker: The overtaker's position update equation is represented in equation (15). The direction indicator for the x th rider is given $M_t(x)$ at the time t.

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

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)

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

Even if the ROA is relatively rapid in identifying the best solutions, it makes sense if the algorithm is improved for a better problem-solving scenario. Consequently, this work aims to offer a new enhanced idea in ROA called FCRO, which is based on the firefly method.

B. Malicious Node Detection

Identifying malicious, selfish, and compromised nodes that have been authenticated requires TM. Accordingly, it has been widely explored in a variety of network contexts, including grid and pervasive computing, peer-to-peer networks, etc.

1. Ridge Regression Algorithm

In a MANET, each normal node has a classifier that can detect malicious 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:

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

The difficulty of optimization is therefore the following formulation:

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

The ridge regression optimization challenge 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 α, commonly known as the regularization constant, to solve this problem with optimization. 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 α 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.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

C. Trust-Based Routing Protocol

The routing of trustworthy nodes is permitted, nonetheless, malicious/selfish nodes are promptly eliminated. To reduce routing overhead in MANET. Consequently, by reducing network traffic, it can be achieved. Subsequently, to identify the best-forwarded path in MANET to reduce routing overhead, the AEPO method is used to introduce a trust-based secure routing protocol

1. Atom Emperor Penguin Optimization (AEPO) Algorithm

Atom search optimization (ASO) is a recently proposed optimization process based on molecular dynamics. 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:

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

$$v_i(t+1)=rand\times v_i(t)+a_i(t) \quad (22)$$

Where rand is an arbitrary number between [0, 1] and $a_i(t)$ the hastening of the i th atom in the t th iteration is determined as follows:

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

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

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

$$h_{ij}(t)=\begin{cases}h_{\min} & \frac{r_{ij}(t)}{\sigma(t)}<h_{\min}\\ \frac{r_{ij}(t)}{\sigma(t)} & h_{\min}\le\frac{r_{ij}(t)}{\sigma(t)}\le h_{\max}\\ h_{\max} & \frac{r_{ij}(t)}{\sigma(t)}>h_{\max}\end{cases}, \text{ and } m_i(t)=\frac{M_i(t)}{\sum_{j=1}^{N}M_j(t)}.$$

The α depth weight $r_{ij}(t)$ is hence the separation between the i th and j th atoms at the t th iteration $h_{\min}$, $h_{\max}$, $\sigma(t)$, and $M_i(t)$ is computed as follows:

$$h_{\min}=g_0+g(t),\quad h_{\max}=u,\quad \sigma(t)=x_{ij}(t),\quad \frac{\sum_{j\varepsilon Kbest}x_{ij}(t)}{K(t)},$$

and $M_i(t)=e^{-\frac{Fit_i(t)-Fit_{best}(t)}{Fit_{worsrt}(t)-Fit_{best}(t)}}$.

Where g_0 is predicted to be 1.1, is u anticipated to be 1.24, and $K(t)$ are estimated as:

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

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

The location N of the atoms' number. The position and expense of each penguin are then determined. Price comparisons between penguins are made. The EPC algorithm is explained using pseudo-code in algorithm 1. For this algorithm, the enumerated guidelines apply:

- All of the original population's penguins emit heat, and they are all attracted to those who have the same thermal absorptivity.
- The body surface area of all penguins is believed to be the same.
- When the penguin absorbs all of the thermal radiation, the effect of the earth's surface and atmosphere is not taken into account.
- The heat radiation from penguins is linear.

$$Q_{penquin}=A\varepsilon\sigma T_s^4 \quad (26)$$

The total surface area $0.56\,m^2$ is denoted as A, where heat transfer $Q_{penquin}$ is defined as that which will be calculated for unit time (W), is the absolute temperature in Kelvin (K), and 35 degrees Celsius $(^\circ C)$ is equivalent to 308.15 K, and ε is the emissivity of bird plumage. There are $\sigma(5.6703\times 108 W/m^2 k^4)$ other names for the Stefan-Boltzmann constant.

Attractiveness: The final definition of attractiveness Q is,

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

Spiral Movement: In this scenario, the system's structure features have uncertain borders and a spiral pattern around the centre.

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

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

When the signals have been rebuilt and all parameters and variables have been acquired after a predetermined number of repetitions, the data window is advanced in one step, and the recovery method is then redone. Consequently, this AEPO algorithm finds the best forwarding paths to route the nodes in the MANET.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

V. EXPERIMENTATION AND RESULT DISCUSSION

The suggested method's performance is assessed using Matlab software running on Windows 10 Home and the R2021a version. The simulation settings are listed, including the number of nodes used in this work (100), the beginning energy of each node (0.5 J), and the amount of energy needed for the transmitter and receiver to operate a circuit $50*10^{-9}$J As a result, there are 200 decision variables, 0 dead nodes at the beginning, 128 bytes in the message, and 100 iterations, correspondingly.

TABLE II: SIMULATION PARAMETERS

Parameters	Values
Node of Numbers	100
Each Node Initial Energy	0.5 (Joule)
Energy Needed for the Circuity of the Transmitter	$50*10^{-9}$(Joules /bit)
Receiver Energy Obligatory 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 anticipated technique's performance is evaluated based on various parameters including PDR, PLR, E2ED, throughput, normalized energy analysis, and normalized routing overhead. The suggested AEPO algorithm is therefore contrasted with the current 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- 30].

Packet Delivery Ratio: PDR is calculated as the proportion of data packets returned to all data packets transmitted through trusted nodes. As shown here, PDR is formalized.

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

The preceding equation (30) R_x symbolises the reception and T_x transmission of n_{Dp_i} numerous data packets. The PDR is expressed as a percentage (%).

Figure 2: Performance Graph for Packet Delivery Ratio

Figure 2 represents the PDR graph and the values of the anticipated AEPO algorithm compared with the existing PSO-GA, TID-CMGR, and MFFA methods. The PDR shows many of the packets that were intended to be delivered were actually sent and effectively accepted at the destination end. The PDR of the recommended AEPO algorithm is around 2% higher than the other prevailing approaches.

Packet Loss Rate: When calculating PLR, the amount of data packets lost is compared to the entirety of data packets sent. The formalized PLR is as follows:

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

From (31), n_{Dp_i} indicates several packets of data, 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 efficiency of the proposed AEPO algorithm outperforms the current PSO-GA algorithm by 5%, the TID-CMGR technique by 3%, and the MFFA algorithm by 1.5%.

End-to-End Delay: The interval of time between the data packet transmitted from the cause node and the data packet that arrived at the destination is used to determine E2E latency. The formalized E2E latency is as follows:

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

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 E2ED graph is portrayed in figure 4. The E2ED for the offered AEPO algorithm is compared with the existing PSO-GA, TID-CMGR, and MFFA. 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.

$$Throughput=\frac{Packets\,\mathrm{Re}ceived\times Packet\,Size}{t} \qquad (33)$$

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.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

Routing Overhead (RO): The quantity of commands (hello packets) and packet routing essential for network communication as a whole is known as network overhead.

$$Overhead(in\ ratio)=\frac{Total\ Contol\ and\ Routing\ Packet}{Number\ of\ Data\ Packets\ Received} \quad (34)$$

Figure 6: Graph for Routing Overhead

Figure 6 elucidates the performance and the comparison graph for routing overhead. The trial outcomes demonstrated that the suggested algorithm works have 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 shows the suggested AEPO model and the standard models compared in terms of the analysis of living nodes. The existing methods like PSO-GA, and TID-CMGR. For the AEPO algorithm, the number of live nodes ought to be at its highest. The amount of live nodes is at its peak right at the beginning, and as the rounds progress, it starts to decline. A maximum of 500 live nodes are present at the beginning. After then, the number progressively drops until it settles between 150 and 200.

Figure 8: Normalized Network Energy Analysis

Figure 8 describes the examination of the normalized energy of the suggested approach over the traditional models. The existing methods like PSO-GA, and TID-CMGR. The initial range for the fixed normalized network energy is 0.05 to 0.06. Consequently, during the 2000th round, the energy would steadily decline to the bottom, until the energy normalized of the offered 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

Figure 9 shows the examination of the cost functions of the suggested and traditional models. The performance of the AEPO algorithm consistently reaches the lowest cost function at the eighth iteration, which is 3%, 3.5%, and 3.1% better than PSO-GA, TID-CMGR, and MFFA, respectively. The investigation has demonstrated that the elected model outperforms other relevant conventional models in terms of cost function.

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 value of the AEPO algorithm is greater than that of the competing techniques. The existing methods like PSO-GA, TID-CMGR, and MFFA. The CH has a maximum lifetime than the other techniques already in custom 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

Figure 12 depicts much energy the AEPO algorithm uses; it demonstrates that the AEPO algorithm has less energy consumption than the other existing methods. 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 generation graph for the AEPO algorithm is portrayed in figure 13. The length of the network 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 III: 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	**Node Density**	**100**	1.08	0.77	0.7	0.62

(mJ)		**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, E2ED, throughput, average transmission delay, network lifetime, energy consumption, 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

Figure 14 shows the AEPO algorithm's transmission success rate graph. The graph demonstrates that the proposed method has a higher transmission success rate than the other methods currently in service. 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 planned technique is associated with the existing PSO-GA, TID-CMGR, and MFFA methods. In contrast to these current methods, the suggested method generates a few nodes that are incorrectly classified.

VI. CONCLUSION

The distinctive characteristic of MANETs that makes them noticeable is the absence of any needed infrastructure-related organizations or units. The network is laid out in a variety of hop topologies. Extreme mobile nodes then form and a network that is ad hoc is powered with the aid of an extensive supply known as energy. In this research, a FCRO algorithm is presented to select the CH. Accordingly, it improves the MANET network efficiency. Accordingly, FCRO algorithm is presented to route the nodes to the destination node.

- ❖ Subsequently, the suggested method is applied using MATLAB software.
- ❖ Packet deliver ratio, packet loss rate, routing overhead, throughput, E2ED, transmission latency, network longevity, and energy usage are the concert metrics.
- ❖ The AEPO algorithm is compared with the existing PSO-GA, TID-CMGR, and MFFA.
- ❖ The presentation of the planned AEPO algorithm is roughly 3.2%, 1.5%,3% , 2%, and 4% higher than the existing methods for PDR, PLR, E2ED, throughput, and network lifetime. Table 4 shows the abbreviations used in the article.

TABLE IV: 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] J. Xu et al., "An algorithm for determining data forwarding strategy based on recommended trust value in MANET," *Int. J. Embed. Syst*., vol. 12, no. 4, p. 544, 2020.

[2] A. O. Alkhamisi, S. M. Buhari, G. Tsaramirsis, and M. Basheri, "An integrated incentive and trust-based optimal path identification in ad hoc on-demand multipath distance vector routing for MANET," *Int. J. Grid Util. Comput*., vol. 11, no. 2, p. 169, 2020.

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

[4] S. Nandgave-Usturge, "Water spider monkey optimization algorithm for trust-based MANET secure routing in IoT," *Int J Scientific Res Eng Trends*, vol. 6, no. 2, pp. 980–984, 2020.

[5] K. J. Abhilash and K. S. Shivaprakasha, "Secure routing protocol for MANET: A survey," *in Lecture Notes in Electrical Engineering, Singapore: Springer Singapore*, 2020, pp. 263–277.

[6] N. A. Malik and M. Rai, "Enhanced secure and efficient key management algorithm and fuzzy with trust management for MANETs," *SSRN Electron. J.*, 2020.

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

[8] S. Thapar and S. K. Sharma, "Direct trust-based detection algorithm for preventing jellyfish attack in MANET," *in*

2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2020.

[9] V. Gomathy, N. Padhy, D. Samanta, M. Sivaram, V. Jain, and I. S. Amiri, "Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks," *J. Ambient Intell. Humaniz. Comput*., vol. 11, no. 11, pp. 4995–5001, 2020.

[10] M. Gupta, P. Garg, S. Gupta, and R. Joon, "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*, vol. 13, no. 4, pp. 99–111, 2020.

[11] K. L. Hassan, J. K. Mandal, and S. Mondal, "A dynamic threshold-based trust-oriented intrusion detection system in MANET," *in Advances in Intelligent Systems and Computing, Singapore: Springer Singapore*, 2020, pp. 699–711.

[12] H. Fatemidokht and M. Kuchaki Rafsanjani, "QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks," *J. Syst. Softw*., vol. 165, no. 110561, p. 110561, 2020.

[13] K. Gu, X. Dong, and W. Jia, "Malicious node detection scheme based on correlation of data and network topology in fog computing-based VANETs," *IEEE Trans. Cloud Comput*., vol. 10, no. 2, pp. 1215–1232, 2022.

[14] S. A. M. Ghaleb and V. Vasanthi, "Energy Efficient Multipath Routing Using Multi-Objective Grey Wolf Optimizer based Dynamic Source Routing Algorithm for MANET," *International Journal of Advanced Science and Technology*, vol. 29, no. 3, pp. 6096–6117, 2020.

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

[16] S. V. Balshetwar and R. M. Tugnayat, "Techniques for Analyzing Framed Data," *Global Journal of Engineering Science and Researches*, vol. 2, no. 8, pp. 80–83, 2015.

[17] R. Aruna, R. Subramanian, P. Sengottuvelan, and J. Shanthini, "Optimized energy efficient route assigning method using related node discovery algorithm in MANET," *Cluster Comput*., vol. 22, no. S1, pp. 469–479, 2019.

[18] Anugraha and D. Krishnaveni, "SRTE: Security resource allocation for trust model in evaluate the strong node," *Webology*, vol. 19, no. 1, pp. 1387–1397, 2022.

[19] M. V. Das, P. Premchand, and L. R. Raju, "Security Enhancing based on Node Authentication and Trusted Routing in Mobile Ad Hoc Network (MANET)," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 14, pp. 5199–5211, 2021.

[20] M. Sirajuddin, C. Rupa, C. Iwendi, and C. Biamba, "TBSMR: A trust-based secure multipath routing protocol for enhancing the QoS of the mobile ad hoc network," *Secur. Commun. Netw*., vol. 2021, pp. 1–9, 2021.

[21] H. Jari, A. Alzahrani, and N. Thomas, "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*, 2021.

[22] C. Gopala Krishnan, A. H. Nishan, S. Gomathi, and G. Aravind Swaminathan, "Energy and trust management framework for MANET using clustering algorithm," *Wirel. Pers. Commun*., vol. 122, no. 2, pp. 1267–1281, 2022.

[23] J. Kaur and S. Kaur, "Novel trust evaluation using NSGA-III based adaptive neuro-fuzzy inference system," *Cluster Comput*., vol. 24, no. 3, pp. 1781–1792, 2021.

[24] J. Anitha Josephine and S. Senthilkumar, "Tanimoto support vector regressive linear program boost based node trust evaluation for secure communication in MANET," *Wirel. Pers. Commun*., vol. 117, no. 4, pp. 2973–2993, 2021.

[25] P. Sathyaraj and D. Rukmani Devi, "RETRACTED ARTICLE: Designing the routing protocol with secured IoT devices and QoS over Manet using trust-based performance evaluation method," *J. Ambient Intell. Humaniz. Comput*., vol. 12, no. 7, pp. 6987–6995, 2021.

[26] R. Kumar and S. Shekhar, "Trust-based fuzzy bat optimization algorithm for attack detection in Manet," *in Smart Innovations in Communication and Computational Sciences, Singapore: Springer Singapore*, 2021, pp. 3–12.

[27] F. Hamza and S. M. C. Vigila, "Cluster Head Selection Algorithm for MANETs Using Hybrid Particle Swarm Optimization-Genetic Algorithm," *Int. J. Comput. Netw. Appl*, vol. 8, no. 2, pp. 119–129, 2021.

[28] S. Venkatasubramanian, A. Suhasini, and C. Vennila, "An Energy Efficient Clustering Algorithm in Mobile Adhoc Network Using Ticket Id Based Clustering Manager," *International Journal of Computer Science & Network Security*, vol. 21, no. 7, pp. 341–349, 2021.

[29] M. Kumar, "An Optimized Utilization of Battery Backup in MANET Using Modified Firefly Algorithm," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 2, pp. 2086–2094, 2021.

[30] S. V. Balshetwar and R. M. Tugnayat, Cumulative Effect. *International Conference on Energy, Communication, Data Analytics and Soft Computing*.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

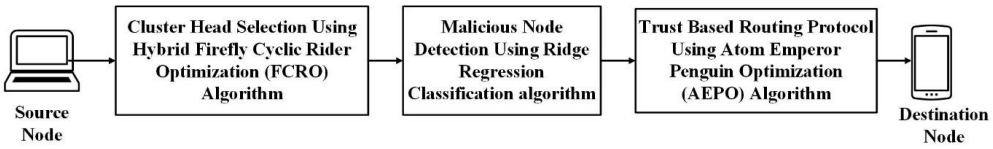

Figure 1: Flow Diagram of the Proposed Work

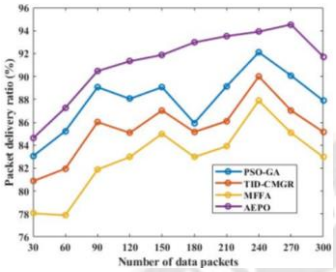

Figure 2: Performance Graph for Packet Delivery Ratio

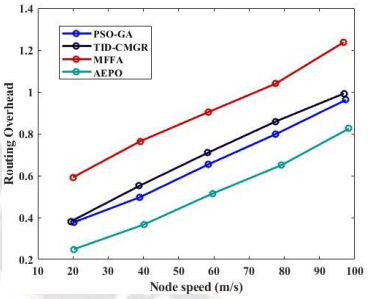

Figure 6: Graph for Routing Overhead

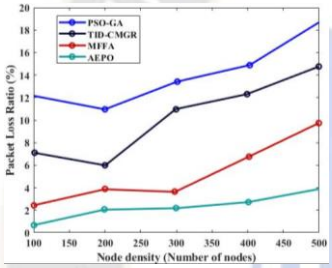

Figure 3: Performance Graph for Packet Loss Ratio

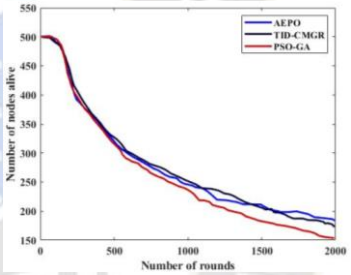

Figure 7: Graph for Number of Alive Nodes

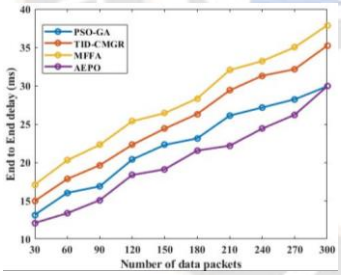

Figure 4: Result for End-to-End Delay

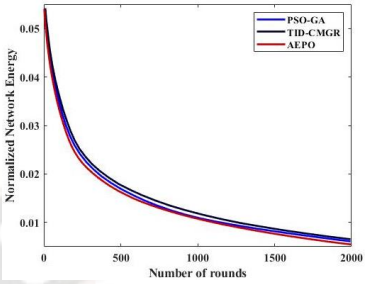

Figure 8: Normalized Network Energy Analysis

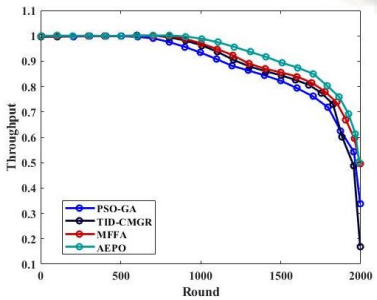

Figure 5: Performance Graph for Throughput

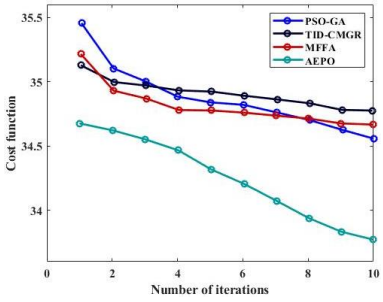

Figure 9: Cost Function of the AEPO Algorithm

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

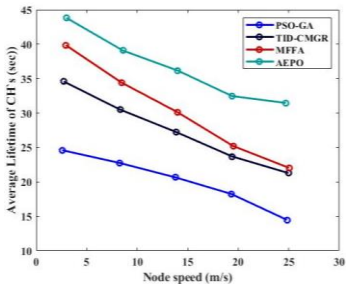

Figure 10: Performance Graph for Average Life Time of CH

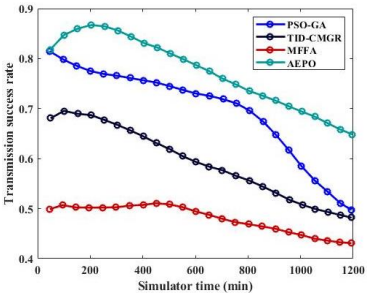

Figure 14: Graph for Transmission Success Rate

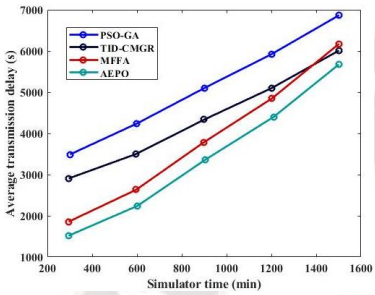

Figure 11: Performance Graph for Average Transmission Delay

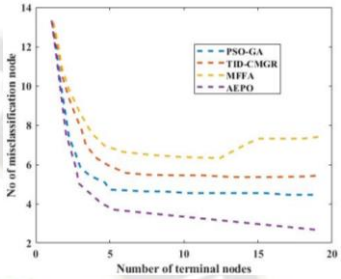

Figure 15: Misclassification Node vs Terminal Node

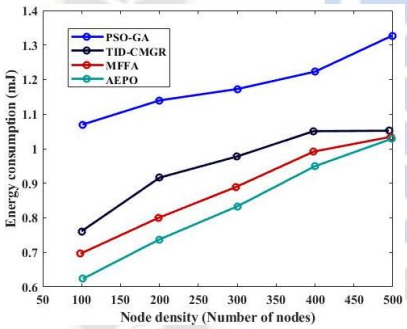

Figure 12: Performance Graph for Energy Consumption

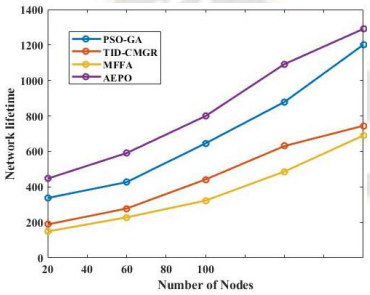

Figure 13: Performance Graph for the Network Lifetime