Received: July 11, 2023. Revised: September 15, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Trust Based Multi Objective-Pelican Optimization Algorithm for Mobile Ad Hoc Networks

Lavanya Nagichetty Lakshminarayana[1]* **Shashi Rekha Gangadharaiah[1]** **Madhushree[1]**

[1]*Department of Computer Science and Engineering, Sapthagiri College of Engineering, Bengaluru, India*
* Corresponding author's Email: lavanyaanand96@gmail.com

Abstract: The approach to ensuring secure transmission in a mobile Ad hoc network (MANET) involves safeguarding the information exchanged between devices. It involves using encryption and authentication techniques to make sure that only authorized devices can access the data and that the data remains unchanged and trustworthy. However, implementing secure broadcasting can be challenging due to factors like limited resources, the dynamic nature of networks, and trust management. To overcome those issues, the trust-based multi-objective-pelican optimization algorithm (TMO-POA) method is used in this paper to offer great security for the data packets and stop malevolent attacks. The energy efficacy of the node and trust values are evaluated. The superior cluster head is selected for that TMO-POA appraisal of the cost function. Let's detect the malevolent node in the network, decrease the packet loss, and evaluate the trust value of the node in its neighbourhood. Upgrading the routing detail is made easier by the trust value and maximizes the network throughput. The outcomes attained from the simulation show that the suggested TMO-POA succeeded in excellent execution according to various parameters metrics. From the results, the proposed TMO-POA, succeeded in achieving maximum throughput (550.01 Kbps), Average energy consumption (0.90J), routing overhead (0.0550), PDR (0.999) and delay (11.23ms), which is much better than the existing bacteria foraging optimization algorithm (BFOA), cat slapped solo algorithm (C-SSA), and trust-based efficiency routing (TER) algorithms.

Keywords: Clustering, Malevolent attacks, Mobile Ad hoc network, Multi-objective pelican optimization algorithm, Routing, Secure transmission.

1. Introduction

A mobile Ad hoc network (MANET) is a self-contained wireless network that enables the seamless integration of mobile devices like laptops, personal digital assistants and cell phones into the system [1]. So that the quality of MANET makes the method constantly vulnerable to malevolent attacks [2]. Likewise, malevolent attacks in the MANET are the worst due to the worst physical security efforts [3]. The primary objective of a MANET routing protocol is to establish an accurate and efficient route between multiple nodes, enabling messages to be transmitted optimally [4]. Data privacy is commonly achieved by utilizing cryptography and its safety processes based, nevertheless, on a trustworthy and secure key organization system [5]. Since 128-bit encryption is considered to be logically toughened, integrating advanced encryption method (AES) with other routing protocols may offer an efficient routing protocol [6]. Mostly bio-inspired algorithm (BIA) was suggested as a routing protocol for MANET that was implemented as a hybrid with acknowledged multipath routing rules such as Ad Hoc on-demand multipath distance vector (AOMDV) and multi-path dynamic source routing (MP-DSR) [7].

The limitations of easy bi-decomposition methods can be minimized by utilizing the augmented lagrangian (AL) frame [8]. Presenting a novel approach related to clustering and infinite belief networks to enhance the attack detection rate included in intrusion detection systems (IDSs) in a MANET [9]. The recent trust-based approach in the MANET concentrates only on detailed routing without taking safety into account [10]. The emergence of the Internet of Things increased the number of devices linked to wireless networks in a desperate manner [11]. An intercommunication of software defined network (SDN) and software defined ratio (SDR) would expand the accessibility of SDN down to medium access control (MAC) layers [12]. However, this argument may highlight the poorest performance in networks, as the path with the fewest number of hops include unused steps that can significantly reduce the overall throughput [13]. The suggested approach selects the optimal multipath based on factors such as energy, throughput, connectivity, and delay [14, 15]. To overcome these issues, this paper improves a secure, trust-based method to develop the efficacy of the MANET.

The major contributions of the article are offered as follows:

- A secure cluster head selection is succeeded by utilizing TMO-POA, at which point it is enhanced by utilizing trust value, residual energy, intra-cluster distance, distance from the Cluster Head (CH) to the Base Station (BS) and node degree.
- Furthermore, a secure routing path is improved by utilizing the TMO-POA related to trust, residual energy, distance, and node degree.
- A secure and energy-efficient cluster-related routing system is built for obtaining dependable communication.

The rest of the paper is detailed as follows: section 2 represents the related works, and the method explanation is detailed in section 3. The outcomes and analysis are offered in section 4. Finally, section 5 concludes this article.

2. Literature survey

This portion illustrates the related work of secure transmission in MANET as follows.

Srilakshmi [16] implemented a secure optimization routing algorithm for MANET. In this research, the focus was on identifying the optimal number of hops in developing the routing, aimed to establish a secure and efficient route direction approach with trust-related considerations. The bacteria foraging optimization algorithm (BFOA) was utilized as a means to achieve this objective. At the beginning phase, the fuzzy clustering method was utilized to evaluate the CHs. Then the cluster heads with the highest trust values for the direct, indirect, and current trust was calculated. The implemented method has a quicker convergence rate and enhanced storage, throughput, and route connection margin. However, while using this approach, there was an increase in computational complexity and bandwidth utilization during the routing process.

Veeraiah [17] implemented trust aware secure energy efficacy hybrid protocol for MANET. To demonstrate the proposed approach, this research implemented a hybrid method called the cat slapped solo algorithm (C-SSA). Initially, fuzzy clustering was employed to determine cluster heads. The CHs were also engaged compared to the multiple jumps routing, and the variety for the most path depends on the predicted hybrid rules. The implemented approach comprised a great max confluence speed and even a hybrid vehicle concentrated on warehouse, and throughput. However, the implemented approach required an analysis for the execution of the suggested method by employing an additional quantity of security attacks.

Srilakshmi [18] implemented an improved hybrid secure multipath routing protocol for MANET. The routing protocol genetic algorithm hill climbing (GHAC) depicted in this research displayed a hybrid GA-Hill climbing approach. Initially, a fuzzy C-means approach based on density peaks was developed. In this approach, CH were selected using a projected method. The implemented method yielded excellent results and outperformed the previous approach even in the presence of attacks. Still, it faces the issues are limited scalability and increased computation.

Suganthi [19] suggested the trust-based efficiency routing (TER) protocol for MANET. The source nodes select a single community as their next hop node using the efficient parameter (EP) technique. The residual energy, the velocity of that node, distance, and engaged queue space were estimated by EP. This method introduces a data forfeiture option and incorporates trust. These rules enhance the decision-making process and contribute to overall trust-based node selection. However, the major challenges occur in Potential trust manipulation, increased overhead in communication/computation, scalability limitations, and complexity.

Rajeswari [20] implemented an adaptive neuro fuzzy inference system energy-efficient secure clustering model (ANFIS-EESC) for MANET security. The main goal of this model was to create energy-efficient and stable trust-based clusters within the network. The weight-based trust estimation (WBTE) algorithm focused on measuring the solidity of nodes and mitigating the presence of malevolent nodes. This method enhances the overall efficiency

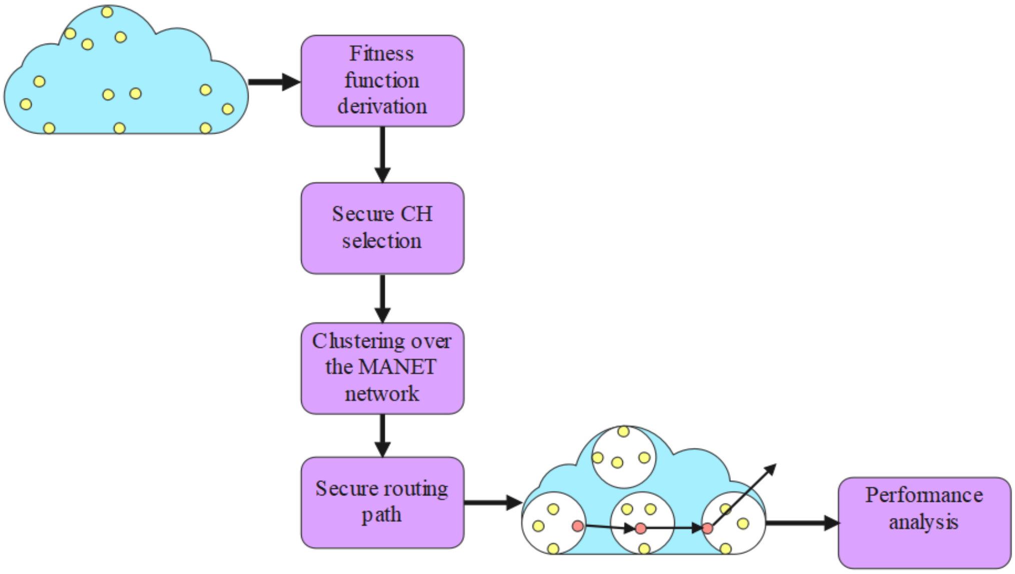
Fitness function derivation
Secure CH selection
Clustering over the MANET network
Secure routing path
Performance analysis

Figure. 1 Block diagram of the TMO-POA method

and reliability of the clustering process within the MANET. However, security-based routing was deliberated as a major issue which needs to be discussed in detail.

3. TMO-POA method

In this section, the influence and mathematical model of the trust related multi-objective Pelican Optimization Algorithm (TMO-POA) are explained. The block diagram of the TMO-POA method is shown in Fig. 1.

This method is trust-based and aims to enhance energy efficiency routing through clustering, to maximize the network's lifespan and improve the packet delivery ratio. The placing of sensors, choosing of secure cluster head (SCH), and producing the paths for clustering and routing are each significant processes in the attainment of TMO-POA. During the process of selecting SCH and establishing routes, nodes that are deemed malicious are disregarded. Instead, the trustworthiness of nodes is evaluated to determine their suitability for participating in the SCH selection and routing process.

3.1 Initialization of sensors

Initially, the sensor nodes are randomly deployed within the large-scale network area. In this scenario, two sinks are considered to create a multi-sink configuration for the large-scale network environment. The process of SCH selection and route establishment using TMO-POA will be elaborated in the subsequent section.

3.1.1. SCH selection utilizing TMO-POA

In this section, protected cluster heads are chosen to develop the security and energy utilization of the network. The SCH selection is utilized to neglect the threat nodes. The selection process of secure cluster heads is executed to create elevation in the security method of the system of the network. The selection stage of SCH is primly used in the process of neglecting the malevolent nodes. The TMO-POA approach calculates the fitness function of each to classify the pelican. The exploration within the neighborhood of the water's surface is elaborated in the following sections.

3.2 Representation and Initialization

The potential resolution is illustrated by each pelican, then the candidate solution is named as pelicans which illustrates the group of CHs that is acquired to be chosen as CH from the standard sensors. In Eq. (1), each pelican location is initialized with the ID of the irregular node between 1 and N the sum of sensors in the network is N. ith candidate solution of the TMO-POA.

$$x_i = (x_{i,1}, x_{i,2}, .., x_{i,NCH}) \quad (1)$$

The location of the pelican is $x_{i,d}$, $1 \leq d \leq NCH$ mentions candidate sensors between the sums of sensors.

3.3 Influence and behavior of pelicans while hunting

The pelican is large and has a wide peak with a big bag in its pharynx. It mainly consumes the prey as fish and spares hardly of toads. Usually, pelicans hunt their prey together. Indeed, certain species descend to lower altitudes to forage for food. The important influence in the model of the suggested TMO-POA is hosted compared to the designing of the observed plan.

3.4 Mathematical Model of the Suggested TMO-POA

The suggested TMO-POA is an inheritance-related approach where pelicans are candidates of this inheritance. In the inheritance-related approach, the individual population candidates a contender resolution. In the beginning, inheritance candidates are erratically installed respectively to the bottom bound and top bound of the issue utilizing Eq. (2).

$$x_{i,j} = l_j + \text{rand}.\left(u_j - l_j\right), \mathrm{I} = 1,2,\ldots\ldots, \mathrm{N}, \mathrm{j} = 1,2,\ldots\ldots, \mathrm{m}, \quad (2)$$

The symbol $x_{i,j}$ represents the value of the jth variable specified by the i th candidate solution. N denotes the number of populations, and m represents the number of problem parameters. $rand$ is an independent number within the interval [0, 1]. The variables l_j and u_j represent the lower and upper bounds, respectively, of the jth problem parameter.

The population of pelicans in the suggested TMO-POA are identified using a candidate solution, where the columns of the matrix represent the proposed values for the problem parameters.

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix} = \begin{bmatrix} x_{1,1} & \cdots & x_{1,j} & \cdots & x_{1,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{i,1} & \cdots & x_{i,j} & \cdots & x_{i,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{N,1} & \cdots & x_{N,j} & \cdots & x_{N,m} \end{bmatrix} \quad (3)$$

The inhabitance matrix of pelicans is X and X_i is the ith pelican which is represented in Eq. (3).

From the suggested TMO-POA, the individual inhabitance associate is a pelican that the given issue for the candidate resolution. Thus, the fitness function of the inclined issue can be estimated related to each individual of the contender resolution. The points obtained for the objective operation are determined by utilizing a vector referred to as the fitness function vector in Eq. (4).

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix} = \begin{bmatrix} F(X_1) \\ \vdots \\ F(X_i) \\ \vdots \\ F(X_N) \end{bmatrix} \quad (4)$$

The symbol F is the fitness operation vector and F_i is the fitness operation value of the ith contender resolution.

The suggested TMO-POA represents the attitude and plan of the pelican meanwhile assaulting and trapping prey to upgrade contender resolutions. Those trapping plans are represented the two phases. They are,

- Shifting through to prey (exploration stage).
- Flying on the water's outer surface (exploitation stage)

Stage 1: Shifting through to prey (exploration stage)

In the initial stage, the pelicans locate the region of the prey and then proceed to move toward this identified region. The design of this pelican's plan focuses on directing its exploration of the search space, utilizing the exploration capability of the suggested TMO-POA to detect diverse regions within the exploration space. The above ideas and the pelican plan in shifting through to the region of food are statistically modulated in Eq. (5).

$$x_{i,j}^{P_i} = \begin{cases} x_{i,j} + rand\,.\left(p_j - I.x_{i,j}\right), & \mathrm{Fp} < F_i; \\ x_{i,j} + rand.\left(x_{i,j} - p_j\right), & else, \end{cases} \quad (5)$$

The symbol $x_{i,j}^{P_i}$ is the trend strategy of the ith pelican in the jth variable related to stage 1, I is an unrelated number that is equivalent to one or two, p_j is the region of prey in the jth variable, and the fitness function value of that is Fp. The argument I is a number where it can be erratically equal to 1 or 2. This argument is erratically chosen for individual repetition and for individual candidates.

The trend position for a pelican is acknowledged in the suggested TMO-POA. This type of enhancement prevents the approach from deviating toward non-optimal regions. This procedure is designed utilizing Eq. (6).

$$x_i = \begin{cases} x_i^{P_1}, & F_i^{P_1} < F_i; \\ x_i, & else, \end{cases} \quad (6)$$

The symbol $x_i^{P_i}$ is the trend strategy of the ith pelican and $F_i^{P_1}$ is its fitness operation worth related to the stage.

Stage 2: Flying on the water's outer surface (Exploitation stage)

From the subsequent stage, pelicans make an outer surface of the water and fetch the fish in their pharynx bag. TMO-POA evaluates the values in the community of the Pelican region to gather for a good resolution. This attitude of pelicans while trapping is statistically simulated in Eq. (7)

$$x_{i,j}^{P_2} = x_{i,j} + \mathrm{R}.(1 - \frac{t}{T}).(2.\mathrm{rand} - 1).\ x_{i,j} \quad (7)$$

The symbol $x_{i,j}^{P_2}$ represents the trend strategy of the ith pelican in the jth dimension for stage 2. In this context, the constant R is equivalent to 0.2 and, $R\,.\left(1 - \frac{t}{T}\right)$ denotes the community radius of $x_{i,j}$ at a given time, where t represents the iteration counter and T represents the maximum number of iterations. In the initial iteration, the value of this factor is large, leading to a broader region where each individual is considered. In this stage, efficacy upgrading has also been utilized to confirm or ignore the trend pelican location that is designed in Eq. (8).

$$x_i = \begin{cases} x_i^{P_2}, & F_i^{P_2} < F_i; \\ x_i, & else, \end{cases} \quad (8)$$

The symbol $x_i^{P_2}$ is the trend status of the ith pelican as well as $F_i^{P_2}$ is its fitness function value related to stage 2.

3.5 Multi objective cost function for CH selection

The cost functions measured in the TMO-POA for selecting optimal CHs are trust, residual energy, intra-cluster distance, separation from the CH to BS, and node degree. Those cost functions are transformed into a single fitness as displayed in the Eq. (9).

$$Cost = \gamma_1 \times f_1 + \gamma_2 \times f_2 + \gamma_3 \times f_3 + \gamma_4 \times f_4 + \gamma_5 \times f_5 \quad (9)$$

The symbols $\gamma_1,\ \gamma_3, \gamma_3, \gamma_4$ and γ_5 represented as the weighted arguments placed on each fitness argument; the trust value of the node is denoted as f_1; residual energy is represented as f_2; intra-cluster distance is illustrated as f_3; distance from the CH to BS is f_4 and node degree is f_5.

- The main cost value measured in this TMO-POA is the trust value of each node which measures two distinct trust values direct and indirect trust values. Direct trust (DT) value is the ratio between the received packets and transmitted packets from the source node which is revealed in Eq. (10). Contrastingly, indirect trust (IDT) is evaluated respectively to the direct trust considered from the destination node that is revealed in Eq. (11). Therefore, the evaluation of the final trust value is displayed in Eq. (12).

$$DT = \frac{R_{a,b}(t)}{S_{a,b}(t)} \quad (10)$$

$$IDT = \frac{1}{NN} \sum_{u=1}^{U} DT_{u,s} \quad (11)$$

$$f_1 = \sum_{i=1}^{P} (DT + IDT)/P \quad (12)$$

The symbol $R_{a,b}(t)$ and $S_{a,b}(t)$ are illustrated that the received and sent packets among the node a and b at time t and NN represents the quantity of adjacent nodes to the node s and P specifies total quantity of engaged nodes.

- During the interaction, the energy appliance of the CH becomes high due to that it performs different works like packet receiving, aggregation, and transmitting through the network. Therefore, the sensor with maximum residual energy is preferred as CH and the residual energy is revealed in Eq. (13).

$$f_2 = \sum_{i=1}^{NCH} \frac{1}{E_{CH_i}} \quad (13)$$

The symbol E_{CH_i} the residual energy of the ith CH.

- There are two variant distances intra cluster distance and separation from the CH to BS are measured in the fitness, due to the energy consumption of the node being primly based on the broadcasting distance through the network. Eq. (14) and (15) reveals the intra-cluster distance and separation from the CH to BS.

$$f_3 = \sum_{j=1}^{M} \left(\sum_{i=1}^{I_j} dis(N_i, CH_j)/I_j \right) \quad (14)$$

$$f_4 = \sum_{i=1}^{M} dis(CH_i, BS) \quad (15)$$

Received: July 11, 2023. Revised: September 15, 2023.

Where distance from ith node to jth CH and distance from the ith CH to BS are represented as $dis(N_i, CH_j)$ and $dis(CH_i, BS)$ accordingly; the amount of standard sensors in the cluster j is mentioned as I_j.

- The amount of standard nodes correlates to the next hop node in node degree that is revealed in Eq. (16).

$$f_5 = \sum_{i=1}^{M} I_j \tag{16}$$

3.6 Cluster formation

The standard sensors are established for the chosen CHs in the cluster creation stage. In this section, the cluster is made respectively to the residual energy and distance while the potential function utilized to configure the cluster is revealed in the Eq. (17).

$$Potential\ of\ sensor\ (N_i) = \frac{E_{CH}}{dis(N_i, CH)} \tag{17}$$

The acquired potential function is utilized to establish the standard sensor node to the CH with least transmission distance and maximum residual energy.

3.7 Routing path generation using TMO-POA

The production of routing paths was accomplished by implementing the TMO-POA method. There are four optimal fitness functions trust, residual energy, distance, and node degree for enhancing the production of the transmission path. The procedures for the routing phase are discussed as follows:

- In the beginning, the pelicans are initialized with possible ways from the source CH to the BS. Each dimension is equivalent to the number of intermediate nodes that exist in the path.
- Subsequently, the position and pheromone upgrade are finished respectively to the fitness of each path. The detail about position and pheromone upgrade are detailed previously in the former portions.
- The fitness measured at the same time producing the transmission path are residual energy, the distance between CH and BS, and node degree. The fitness utilized in the TMO-POA-related route production is displayed in Eq. (18).

$$Cost = \varphi_1 \times \sum_{i=1}^{P} \frac{(DT+IDT)}{P} + \varphi_2 \times \sum_{i=1}^{NCH} \frac{1}{E_{CH_i}} + \varphi_3 \times \sum_{i=1}^{M} dis(CH_i, BS) + \varphi_4 \times \sum_{i=1}^{M} I_j \tag{18}$$

The symbols $\varphi_1, \varphi_2, \varphi_3$ and φ_4 are weighted arguments established for each fitness of route production. This aids to find the path with maximum residual energy, least transmission distance and least node degree.

4. Result and analysis

This study, employed MATLAB R2018a to evaluate the execution of the TMO-POA. The feature of the system comprises an i7 processor with 8GB RAM.

The output of the simulation is a trace file, which contains valuable data for estimating various performance metrics and analyzing this trace file and utilizing the AWK programming language. By utilizing NS2 and the AWK programming language, we successfully simulated the network, collected essential data, and conducted a comprehensive analysis to assess the efficiency of the overhead algorithms.

4.1 Throughput

Throughput is detailed that the volume of data that could be broadcasted through to network in a specific period and measured in bit per second (bps). Here, Fig. 2 depicts the throughput differentiation for the TER, C-SSA, BFOA, and TMO-POA. Table 1 provides throughput values of TMO-POA are higher than the other approaches TER, C-SSA, and BFOA. The outcomes show that the data transmission of TMO-POA is developed by neglecting the threatened node at the same time transmitting the data packets. Eq. (19) and Eq. (20) denote the quantity of packets delivered by the destination within a given time interval and are calculated as the impact of a routing protocol. The suggested approach of TMO-POA succeeded with better accuracy in fifth node of 550.01 higher than the former approaches of 540.09, 532.24, and 520.12 respectively.

$$Throughput = \frac{File\ size}{Transmission\ time\ (bps)} \tag{19}$$

$$Transmission\ time\ (bps) = \frac{File\ size}{Bandwidth\ (\mathrm{sec})} \tag{20}$$

Received: July 11, 2023. Revised: September 15, 2023.

Table. 1 Throughput differentiation of proposed TMO-POA and the former system

S.NO	Number of nodes	Throughput (Kbps)			
		BFOA [16]	C-SSA [17]	TER [19]	TMO-POA
1	5	540.09	532.24	520.12	550.01
2	10	515.98	500.36	481.23	530.24
3	15	375.01	350.98	349.79	384.12
4	20	300.10	289.58	278.24	318.33

Table. 2 Packet Delivery ratio differentiation of TMO-POA and an existing system

S.NO	Number of nodes		Packet Delivery Ratio			
		BFOA [16]	C-SSA [17]	GHAC [18]	TER [19]	TMO-POA
1	5	1	1	0.994	1	1
2	10	1	1	0.991	1	1
3	15	1	1	0.998	0.999	1
4	20	0.991	0.995	0.893	0.989	0.999

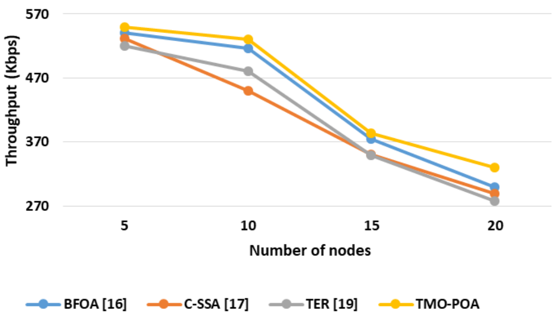

Figure. 2 Throughput comparison among proposed and existing approaches

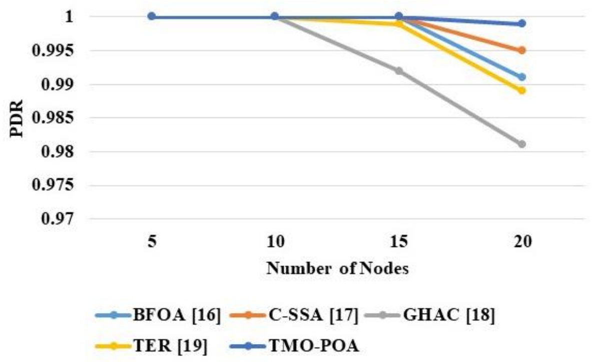

Figure. 3 Performance analysis of packet delivery ratio

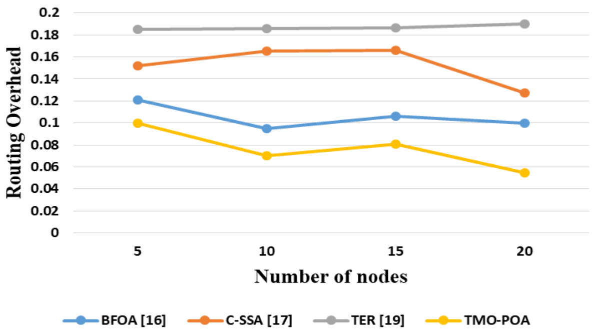

Figure. 4 Routing overhead comparison among proposed and existing approaches

4.2 Packet delivery ratio

Packet delivery ratio (PDR) is termed as the ratio between the number of packets made from sources and the number of packets obtained by the recipient. Table 2 provides the performance analysis of packet delivery ratio. In that Table 2, the proposed TMO-POA compared with the other existing approaches such as BFOA [16], C-SSA [17], GHAC [18] and TER [19]. The graphical presentation of PDR is shown in Fig. 3. Then the outcome of TMO-POA attains to neglect the malicious node while the data is broadcasting. The ratio of the data delivered to the destination of the data sent out by the source is demonstrated in Eq. (21).

$$PDR = \left(\frac{Received\ packets}{Sent\ packets}\right) * 100 \qquad (21)$$

For analysis purpose, the existing GHAC [18] has implemented for different number of nodes (0 to 20) in terms of PDR. From the Table 2, it clearly shows that the proposed TMO-POA attained a better result of PDR in 20th node of 0.999 which is superior than the existing approaches of 0.991, 0.995, 0.893 and 0.999 for BFOA [16], C-SSA [17], GHAC [18] and TER [19] respectively.

4.3 Routing overhead

The sum of the quantity of routing packets is standardized by the sum of quantity of obtained packets. This suggested approach has decreased the routing approach. Then, Table 3 represents the values of the routing node along with the proposed and existing methods. Fig. 4 illustrates the superior accuracy of the execution of the proposed TMO-POA which is maximum execution than the former approaches.

Table. 3 Routing overhead differentiation of TMO-POA and existing approach

S.NO	Number of nodes	Routing Overhead			
		BFOA [16]	C-SSA [17]	TER [19]	TMO-POA
1	5	0.1208	0.1523	0.1854	0.0999
2	10	0.0949	0.1655	0.186	0.0705
3	15	0.1059	0.1660	0.1863	0.0810
4	20	0.0999	0.1271	0.1902	0.0550

Table. 4 Average energy consumption comparison of TMO-POA and existing approach

S.NO	Number of nodes		Average energy consumption (J)			
		BFOA [16]	C-SSA [17]	TER [19]	ANFIS-EESC [20]	TMO-POA
1	5	0.98	1	1.07	6.21	0.90
2	10	2	2.05	2.08	5.37	1.02
3	15	3.34	4.02	4.83	4.02	2.99
4	20	3.91	5.57	6.97	3.56	2.85

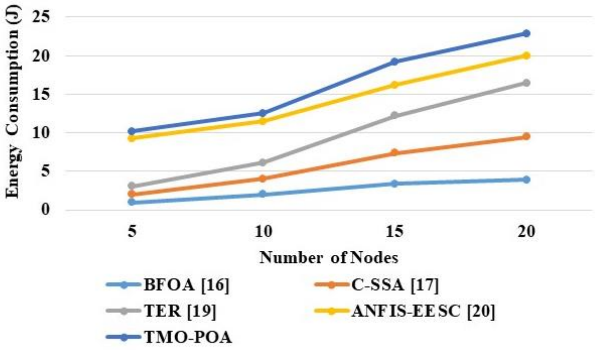

Figure. 5 Performance analysis of average energy consumption

It is utilized to research the effect of maximum mobility, dynamic topologies, and routing because of the additional dynamic modification in the network which is used to optimize the MANET. Eq. (22) denotes the sum of the quantity of control or routing (RTR) packets produced by the routing protocol while the modulation. Each packet dispatched or move through to the network layer is assumed routing overhead. The suggested approach of TMO-POA succeeded with better accuracy in 10th node of 0.0705 more than the former approaches of 0.0949, 0.1655, and 0.186 respectively.

$$Routing\ overhead = Number\ of\ RTR\ packets \quad (22)$$

4.4 Average energy consumption

The energy consumption of the network is detailed as the number of depleted energy while the time of obtaining and transmitting packets which consist of data. Table 4 gives the energy consumption analysis of proposed TMO-POA with existing BFOA [16], C-SSA [17], TER [19], ANFIS-EESC [20]. Then it succeeds in the maximum energy consumption due to its failure to mitigate the threat nodes and also it executes individual jump transmission. Furthermore, TMO-POA succeeds in maximum energy efficacy due to the mitigation of threat nodes utilizing trust and production of shortest route. The graphical depiction of average energy consumption is depicted in Fig. 5. Eq. (23) represents the total energy utilized by each node (TE) to the number of nodes (N).

$$AEC = \frac{TE}{N} \quad (23)$$

From the Table 4, the proposed TMO-POA succeeded with a better result in 20th node of 2.85J which is lower than the existing approaches which achieved 3.91J, 5.57J, 6.97J and 3.56J for BFOA [16], C-SSA [17], TER [19], ANFIS-EESC [20] respectively.

4.5 End to end delay

End-to-end delay has amounted to a maximum of each enduring data packet to the destination from the source. The differentiation of end to end delay was represented in Fig. 6 and Table 5 offers end to end delay values that maximize the execution of the proposed approach TMO-POA for preventing the malicious node and generation of the shortest route. Eq. (24) illustrates that the NP is the sum of the number of packets delivered, denoted as Rti, divided by the time it took for packet i to be delivered, represented by $St(i)$. The suggested approach of TMO-POA succeeded with a better accuracy in 5th node of 11.23ms greater than the existing approaches of 9.03, 5.54, and 3.77 respectively.

$$Average\ E2ED = \frac{1}{NP}\sum_{i=0}^{NP}((Rt(i) - St(i)) \quad (24)$$

Table. 5 End-to-end delay differentiation of suggested TMO-POA and former system

S.NO	Number of nodes	End to End Delay (ms)			
		BFOA [16]	**C-SSA [17]**	**TER [19]**	**TMO-POA**
1	5	9.03	5.54	3.77	11.23
2	10	9.54	5.4523	5.57512	13.02
3	15	11.34	9.025	8.462	18.99
4	20	13.914	10.572	9.902	19.850

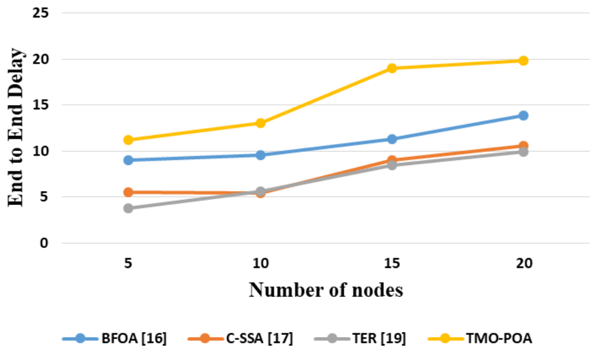

Figure. 6 End to end delay differentiation of suggested TMO-POA and former system

5. Conclusion

Secure transmission in mobile Ad-hoc networks ensures the confidentiality, integrity, and authenticity of the information transmitted between devices. Here, an efficient routing approach is applied utilizing the trust based multi objective-pelican optimization algorithm (TMO-POA) estimation. The selection of CH and production of routing path utilizing TMO-POA increasingly includes the usage of parameters based on trust, residual energy, intra-cluster distance, distance from the CH to BS and node degree. Due to those fitness functions, the proposed TMO-POA achieves better performances in all the nodes. From the result analysis, it clearly shows that proposed TMO-POA obtained better results in terms of Throughput (550.01 Kbps), PDR (0.999), routing overhead (0.0550), average energy consumption (0.90J) and delay (11.23 ms). The above results states that proposed TMO-POA is superior over existing methods. In future work, a novel optimization algorithm will be implemented to improve the secure transmissions in MANET.

Notation list

Notation	Description
$x_{i,d}$	Location of the pelican
N	Number of populations
m	Number of problem parameters
$rand$	Random number between [0, 1]
l_j and u_j	Lower and Upper bounds
X	Inhabitance matrix of pelicans
F	Fitness operation vector
F_i	Fitness operation value of the ith contender resolution
$x_{i,j}^{P_i}$	Trend strategy of the ith pelican in the jth variable
I	Unrelated number
p_j	Region of prey in the jth variable,
Fp	Fitness function value
$R.\left(1-\frac{t}{T}\right)$	Community radius of $x_{i,j}$
R	Radius
t	Iteration counter
T	Maximum number of iterations
f_1	Trust value of the node
f_2	Residual energy
f_3	Intra-cluster distance
f_4	Distance from the CH to BS
f_5	Node degree
$Cost$	Cost functions
γ_1, γ_3, γ_3, γ_4 and γ_5	Weighted arguments
$R_{a,b}(t)$ and $S_{a,b}(t)$	Received and Sent packets

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

For this research work all authors' have equally contributed in Conceptualization, methodology, validation, resources, writing—original draft preparation, writing—review and editing.

References

[1] K. Rajkumar and M. K. Jeyakumar, “Energy efficient clustering for certificate revocation scheme in a mobile ad-hoc network”, *Wireless Personal Communications*, Vol. 118, No. 1, pp. 647-662, 2021.

[2] M. Bounouni, L. B. Medjkoune, A. Beraza, and A. Daoud, “Eliminating selective dropping

attack in mobile ad hoc network", *Wireless Personal Communications*, Vol. 123, pp. 3291-3308, 2022.

[3] E. Devi, S. Ahila, Radhika, and A. Chandrasekar, "An energy-efficient MANET relay node selection and routing using a fuzzy-based analytic hierarchy process", *Telecommunication Systems*, Vol. 83, pp. 209-226, 2023.

[4] G. M. Borkar, and A. R. Mahajan, "Security aware dual authentication-based routing scheme using fuzzy logic with secure data dissemination for mobile Ad-hoc networks", *Journal of Applied Security Research*, Vol. 13, No. 2, pp. 223-249, 2018.

[5] S. Venkatasubramanian, A. Suhasini, and C. Vennila, "Cluster Head Selection and Optimal Multipath detection using Coral Reef Optimization in MANET Environment", *International Journal of Computer Network & Information Security*, Vol. 14, No. 3, pp. 88-99, 2022.

[6] M. M. Mukhedkar and U. Kolekar, "E-TDGO: An encrypted trust-based dolphin glowworm optimization for secure routing in mobile ad hoc network", *International Journal of Communication Systems*, Vol. 33, No. 7, p. e4252, 2020.

[7] S. Sarhan and S. Sarhan, "Elephant herding optimization Ad Hoc on-demand multipath distance vector routing protocol for MANET", *IEEE Access*, Vol. 9, pp. 39489-39499, 2021.

[8] S. Hashempour, A. A. Suratgar, and A. Afshar, "Distributed nonconvex optimization for energy efficiency in mobile ad hoc networks", *IEEE Systems Journal*, Vol. 15, No. 4, pp. 5683-5693, 2021.

[9] S. Dilipkumar and M. Durairaj, "Epilson Swarm Optimized Cluster Gradient and deep belief classifier for multi-attack intrusion detection in MANET", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 14, No. 3, pp. 1445-1460, 2023.

[10] T. K. Saini and S. C. Sharma, "Flexible multipoint relay selection for suitable route in mobile ad hoc networks", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, pp. 8173-8186, 2021.

[11] N. Shah, H. E. Ocla, and P. Shah, "Adaptive Routing Protocol in Mobile Ad-Hoc Networks Using Genetic Algorithm", *IEEE Access*, Vol. 10, pp. 132949-132964, 2022.

[12] D. Kafetzis, S. Vassilaras, G. Vardoulias, and I. Koutsopoulos, "Software-defined networking meets software-defined radio in mobile ad hoc networks: State of the art and future directions", *IEEE Access*, Vol. 10, pp. 9989-10014, 2022.

[13] S. Tabatabaei, "A new routing protocol for energy optimization in Mobile ad hoc networks using the cuckoo optimization and the TOPSIS multi-criteria algorithm", *Cybernetics and Systems*, Vol. 52, No. 6, pp. 477-497, 2021.

[14] N. Veeraiah and B. T. Krishna, "An approach for optimal-secure multi-path routing and intrusion detection in MANET", *Evolutionary Intelligence*, Vol. 15, No. 2, pp. 1313-1327, 2022.

[15] M. N. Ahmed, A. H. Abdullah, H. Chizari, and O. Kaiwartya, "F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs", *Journal of King Saud University-Computer and Information Sciences*, Vol. 29, No. 3, pp. 269-280, 2017.

[16] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah, and Y. Alotaibi, "A secure optimization routing algorithm for mobile ad hoc networks", *IEEE Access*, Vol. 10, pp. 14260-14269, 2022.

[17] N. Veeraiah, O. I. Khalaf, C. V. P. R. Prasad, Y. Alotaibi, A. Alsufyani, S. A. Alghamdi, and N. Alsufyani, "Trust aware secure energy efficient hybrid protocol for manet", *IEEE Access*, Vol. 9, pp. 120996-121005, 2021.

[18] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf, and B. V. Subbayamma, "An improved hybrid secure multipath routing protocol for MANET", *IEEE Access*, Vol. 9, pp. 163043-163053, 2021.

[19] R. Suganthi, I. Poonguzhali, J. Navarajan, R. Krishnaveni, and N. N. Saranya, "Trust based efficient routing (TER) protocol for MANETS", *Materials Today: Proceedings*, Vol. 80, No. 3, pp. 2014-2021, 2023.

[20] A. R. Rajeswari, W. C. Lai, C. Kavitha, P. K. Balasubramanian, and S. R. Srividhya, "A Trust-Based Secure Neuro Fuzzy Clustering Technique for Mobile Ad Hoc Networks", *Electronics*, Vol. 12, No. 2, p. 274, 2023.