Received: September 27, 2024. Revised: November 4, 2024.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Multi-objective-Trust Aware Improved Pelican Optimization Approach for Secure and Energy Efficient Clustering and Routing in Wireless Sensor Network

Sreelakshmi Tadigotla[1]* **Jayanthi K. Murthy[1]**

[1]*Department of Electronics & Communication Engineering, B.M.S. College of Engineering, Bengaluru, India*
* Corresponding author's Email: sreeluperuru@gmail.com

Abstract: Wireless Sensor Networks (WSNs) have multitudinous Sensor Nodes (SN) with low-power, low-cost, and miniature characteristics. These nodes are data-centric and responsible for gathering appropriate data in the target area and they transmit to the control centre or Base Station (BS) in a single-hop or multi-hop manner. However, WSN faces certain difficulties like security enhancement and energy optimization due to their limited resources, working environments, and communication characteristics to provide network security. This research proposes a Multi-objective-Trust Aware Improved Pelican Optimization Approach (M-TAIPOA) to achieve a secure and energy-efficient clustering and routing process. POA is enhanced using sine chaos mapping, the fusion of Sine Cosine Optimization (CSO) and levy flight strategy for enhancing search diversity, convergence accuracy, and to jump out of local optima. M-TAIPOA selects Secure Cluster Head (SCH) based on node degree, distance among the neighbour nodes, location factor, distance between BS and CH, and trust. Then, distance and energy are used for the secure routing process. M-TAIPOA achieves a lower energy consumption of 4.5J for 10 rounds for scenario 3 when compared to the existing technique, Energy Optimization Routing by utilizing an improved Artificial Bee Colony (EOR-iABC).

Keywords: Multi-objective-trust aware improved pelican optimization approach, Secure cluster head, Secure routing, Sine cosine optimization, Wireless sensor networks.

1. Introduction

A Wireless Sensor Network (WSN) is a heterogeneous computing application with small networks, advanced sensor hubs, low power, and one or more Base Stations (BS) [1, 2]. Physical elements are determined by these nodes while they interrelate with their surroundings [3]. Energy consumption is one of the primary problems because the batteries utilized in sensors are unable to be rechargeable and replaceable [4, 5]. Every cluster has a coordinator node known as the Cluster Head (CH), while the remaining nodes are named as cluster members [6]. Therefore, every sensor transmits obtained data to the associating CH, and CH sends a gathered data to BS neither by single hop nor multi-hop communication [7]. Clustering is a Nondeterministic Polynomial (NP) time-hard issue that is addressed by utilizing the optimization approach to increase the network efficiency [8, 9].

Cluster-based routing protocol addresses certain significant challenges because of its scalability, energy efficiency, and reliability of data delivery [10] [11, 12]. Additionally, security is a significant research area for enabling reliable data communication between the nodes in an environment [13]. The SN deployment for a particular task application is completely based on the ability to forward data, energy capacity, and ability to transfer the aggregated data to the sink node [14, 15]. Furthermore, the SN's residual energy indicates the key indicator via WSN's lifetime which is determined accurately to predict its longevity [16] [17]. However, WSN faces challenges of security and energy consumption because of the limited resources, working environments, and communication characteristics to generate a fortified network. In this research, M-TAIPOA is proposed to transmit data securely using clustering and routing procedures which reduce the consumption of energy and assure security.

The primary contribution is described below in detail:

- In POA, CSO is utilized to maximize the convergence accuracy and search diversity, while the levy flight is employed to avoid the local optima. This leads to a more reliable and effective CH selection and routing which optimizes the energy consumption, ensuring robust trust management in the network.
- To choose SCH from a normal sensor, the distance among the neighbor nodes, node degree, distance between BS and CH, location factor, and trust threshold are utilized for handling an effective and reliable SN process.
- Distance and energy are used for the routing process which leads to minimized consumption of energy and increased security data transmission.

This research paper is further organized as follows: Section 2 describes a literature survey of the existing approach, Section 3 represents a clear description of the proposed methodology, while Section 4 determines results for the existing approach and proposed approach, and lastly, the conclusion of this research is given in Section 5.

2. Literature survey

The literature survey about secure trust and energy efficient clustering and routing protocol using WSN are discussed in this section along with their benefits and limitations.

Prakash [18] implemented a Fractional Artificial Lion (FAL) to choose the best paths during routing phase effectively. The CH selection and routing algorithm was attained successfully by incorporating Artificial Bee Colony (ABC), Lion Optimization Approach (LOA), and fractional calculus. However, the FAL struggled to choose optimal paths because of its limited ability for dynamic security threats as it majorly focuses on path effectiveness rather than integrating robust security measures.

Santhosh and Prasad [19] suggested an Energy Optimization Routing by utilizing improved ABC (EOR-iABC) for cluster-based WSN. An energy-efficient fitness node determined an optimal path from CH to BS, enhancing the network data collection efficiency. However, EOR-iABC suffered from premature convergence due to the algorithm settling on the suboptimal solution before exploring the search space which led to suboptimal energy distribution.

Paruvathavardhini and Sargunam [20] presented an Energy-Efficient Cluster-based Routing Algorithm for Improved Firefly algorithm and Ant Colony Optimization (EECRAIFA) in WSN. The communication between CH and BS was single-hop or multi-hop which balanced the network's energy consumption and reduced energy utilization of network. However, EECRAIFA suffered from increased energy consumption because of its reliance on frequent communication among clusters which drained the resource of battery more rapidly.

Osamy [21] introduced a Neuro-Fuzzy clustering with Sparrow Search Optimization (NF-SSOA) to generate an energy-efficient trust-aware approach in WSN. The NF-SSOA increased the reliability and energy efficiency by applying the NF approach. Nonetheless, the introduced approach faced scalability challenges with large-scale networks as it was based on NF parameters that limited its effectiveness by increasing the network size.

Han [22] developed an energy-aware and Trust-based routing protocol utilizing an Adaptive Genetic Algorithm (TAGA) for WSN. TAGA enhanced security by constructing an adaptive approach to determine a comprehensive trust value of every node in resisting common attacks. However, TAGA exhibit less security due to developed approach based on fuzzy logic which results in ambiguous decision-making in the presence of adversarial inputs.

From the overall analysis, it is seen that the existing methods have limitations like to choose optimal paths, increased energy consumption, and less security. To overcome these problems, the M-TAIPOA is proposed to transmit the data securely by utilizing various fitness functions. By efficiently balancing the trade-off among secure data transfer and energy consumption, the M-TAIPOA makes the reliable communication. Hence, this approach significantly minimizes the overall energy consumption while managing robust security which enhance the network effectiveness.

3. Proposed methodology

This section discusses information about WSN and the energy model to evaluate energy usage in the network. The M-TAIPOA is employed for energy-efficient trust-aware clustering and routing processes in WSN which are briefly explained in the following sub-sections.

3.1 Network model

WSN has one sink node indicated as R_m with SN n and wireless link denotes a direct message between SN at a particular radio range. Here, every SN is equally allocated at Q_k and P_k sizes with maximum communication radio range. The Q_k and P_k indicates parameters specific to k^{th} sensor node. The position of SN is calculated with their P_k and Q_k coordinate values. The term B_m refers to individual SN which is stimulated and $CH(R_r)$ refers to CH characterized by its operational range R_r, r indicates channel, and R represents maximum effective communication distance associated with channel. B_m^z indicates a collection of SN in group B_m, m defines SN within the overall network and z indicates particular characteristics associated with node's collection. The distance among normal node q^{th} to y^{th} CH is represented as $s_{q,y}$ after SN is in a predetermined place, where the distance between y^{th} CH to BS.

3.2 Energy model

The initial energy of each sensor node H_0 does not need to be re-energized because each packet transmits energy from q^{th} normal node to y^{th} CH based on a multipath fading approach among the transmitter and receiver to avoid malicious nodes. D_c determines electronic energy for spreading, digital coding, modulation, amplifier, and filtering using Eq (1).

$$D_c = D_s + D_c \tag{1}$$

Where D_s indicates the transmitted energy, D_c denotes data aggregation, s indicates source node, c determines cluster nodes, and $||J^a - R_r^a||$ determines the distance among normal and CH node, J^a illustrates attribute associated with normal node, R_r^a defines attribute associated with CH, r represents index, and a indicates attributes. If CH node attains A_p data bytes, the dissipation of energy by the receiver is formulated in Eq. (2).

$$D_b = (R_r^a) = D_c * A_p \tag{2}$$

Where D_b indicates energy dissipation associated with receiver at CH and b refers to category of dissipation. A node with energy values is updated through sending and receiving A_p data bytes which is expressed in Eqs. (3) and (4).

$$D_{g+1}(J^a) = D_s(J^a) - D_b(J^a) \tag{3}$$

$$D_{g+1}(R_r^a) = D_s(R_r^a) - D_b(R_r^a) \tag{4}$$

Where p determines packet number, D_{g+1} refers energy dissipation for the next node $g+1$. The nodes with zero energy are represented as dead nodes. The above process is repetitive till each node are transmitted as a dead node.

3.3 Secure CH discovery using M-TAGOA

An efficient SCH and routing process is established to achieve reliable and secure data transmission in M-TAIPOA to avoid malicious nodes. Fig. 1 indicates a block diagram for the M-TAIPOA technique.

3.3.1. Sensor initialization

The sensors are deployed randomly within a WSN area. In a prior section, a network and energy models are determined. The following subsection presents a secure and routing discovery using the M-TAIPOA.

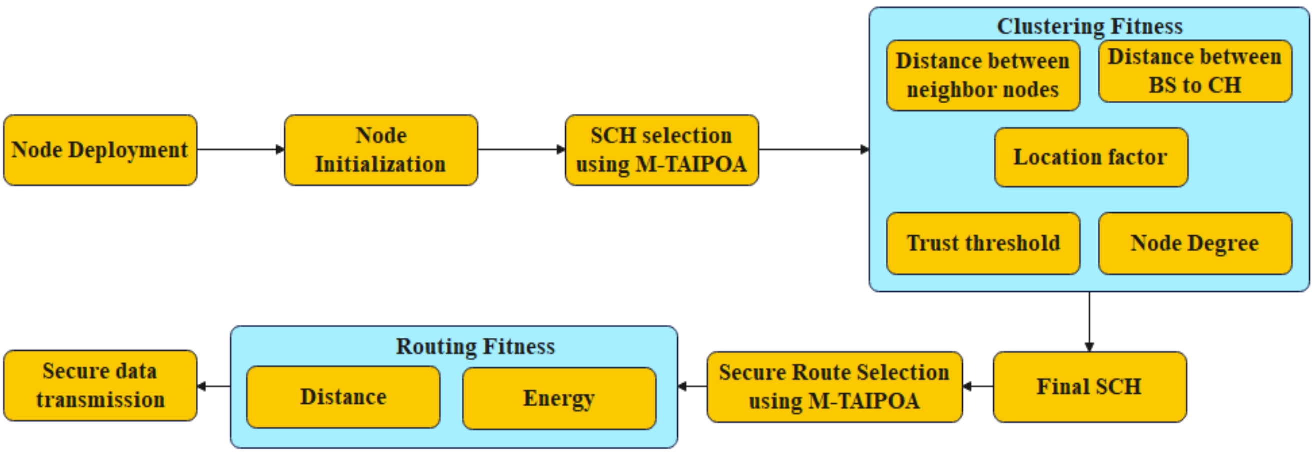


Figure. 1 Block diagram for M-TAIPOA

3.3.2. SCH using M-TAIPOA

In this phase, best SCH from normal sensors is established by employing M-TAIPOA approach. During hunting, POA [23] simulates pelican's natural behaviour that is split into 2 primary stages: approaching prey stage and surface flight stage. During the exploration stage, the mathematical formula for pelican behaviour is expressed in Eqs. (5) to (7).

$$P_i = X_k, i = 1,2,\dots,N, k = 1,2,\dots,N \tag{5}$$

$$x_{ij}^{P1} = \begin{cases} x_{i,j} + rand.\left(p_j - I.x_{i,j}\right), & F_p < F_i \\ x_{i,j} + rand.\left(x_{ij} - P_j\right), & else \end{cases} \tag{6}$$

$$X_i = \begin{cases} X_i^{P_1}, & F_i^{P_1} < F_i \\ X_i, & else \end{cases} \tag{7}$$

Where, P_i represents the prey location chosen by i^{th} pelican, F_i indicates objective function value, k denotes a random natural number, and $X_i^{P_1}$ refers to i^{th} pelican's new state in j^{th} dimension. $F_i^{P_1}$ determines adaptation value, $rand$ and I express the random numbers utilized to provide a random POA behaviour in the update and search processes. The mathematical formula for the second phase is expressed in Eqs. (8) and (9).

$$x_{ij}^{P2} = x_{ij} + R.\left(1 - \frac{\tau}{T}\right).(2rand - 1).x_{ij} \tag{8}$$

$$X_i = \begin{cases} X_i^{P_2}, & F_i^{P_2} < F_i \\ X_i, & else \end{cases} \tag{9}$$

Where, t represents a present number of iterations, T denotes the maximum number of iterations, R determines a constant, $x_{i,j}^{P_2}$ denotes i^{th} the pelican's new state in j^{th} dimension, and $F_i^{P_2}$ refers to the respective fitness value in a new state. However, POA converges slowly and easily into local optima. The sine chaos mapping, fusion of CSO, and levy flight strategy are employed to overcome this issue which enhance the search diversity, convergence accuracy, and jump out of local optima which are briefly explained below.

3.3.1.1 Sine chaos initialization

The chaotic mapping is utilized to enhance quality and initial population's uniform distribution. Instead of random initialization, it enables a more uniform population using Eq. (10).

$$x_{k+1} = \frac{a}{4}\sin(\pi x_k), a \in (0,4] \tag{10}$$

Where a represents scaling factor.

3.3.1.2 Fusion of sine cosine optimization method

A spiral search method incorporates sine cosine optimization to maximize the algorithm's search diversity, convergence accuracy, and local pioneering ability. The iterative equations are categorized into two kinds which are, sine or cosine iterative equations, as expressed in Eq. (11).

$$X_i^j(t+1) = \begin{cases} X_i^j(t) + r_1.\sin(r_2).\left|r_3 P_{best}(t) - X_i^j(t)\right|, & if\ r_4 > 0.5 \\ X_i^j(t) + r_1.\cos(r_2).\left|r_3 P_{best}(t) - X_i^j(t)\right|, & if\ r_4 < 0.5 \end{cases} \tag{11}$$

Here, t indicates the number of present iterations, $X_i^j(t)$ represents a component of individual position i in j^{th} dimension at iteration t, r_1, r_4 denotes a random number between [0,1], and r_2, r_3 determines a random number between $[0,2\pi]$. POA is applied inspired by spiral predation approach of Whale Optimization Approach (WOA). Integrating this approach with SCO, initial phase mathematical formula of POA after fusing these two strategies is expressed in Eq. (12).

$$x_{ij}^{P1} = \begin{cases} e^{z.l}.\cos(2\pi l).x_{i,j} + r_1.\sin(r_2).\left|r_3.x_{i,j} - p_j\right|, & F_p < F_i \\ e^{z.l}.\cos(2\pi l).x_{i,j} + r_1.\cos\ (r_2).\left|r_3.x_{i,j} - p_j\right|, & else \end{cases} \tag{12}$$

3.3.1.3 Levy flight approach

It is used to increase the POA's capability to avoid local optima which are expressed in Eqs. (13) to (15).

$$\sigma = \left[\frac{\Gamma(1+\beta)\sin\left(\frac{\pi\beta}{2}\right)}{\Gamma\left(\frac{1+\beta}{2}\right)\beta.2^{\frac{\beta-1}{2}}}\right]1/\beta \tag{13}$$

$$u \sim N(0,\sigma^2), v \sim N(0,1) \tag{14}$$

$$levy(x) = 0.01 \times \frac{u.rand}{|v|^{1/\beta}} \tag{15}$$

Where σ indicates step size, Γ denotes gamma function, β represents control the shape, $\sin\left(\frac{\pi\beta}{2}\right)$ refers trigonometric function, $N(0,\sigma^2)$ determines normal distribution with mean and variance, u and v defines random variables. After incorporating levy flights, the formula of the second phase of POA is expressed in Eq. (16).

$$x_{i,j}^{p_2} = levy.x_{i,j} + R.\left(1 - \frac{t}{T}\right).(2rand - 1).x_{i,j} \quad (16)$$

This leads to more reliable and effective clustering and routing which optimizes the energy consumption with robust trust management in a network.

3.3.3. Fitness for SCH and Secure Routing Process

- **Distance between neighbour nodes**

Once the node is chosen, each CH identifies a neighbor CH and transfers an acknowledge message to the node degree and distance BS which is represented in Eq. (17).

$$f1 = \sum_{i=1}^{n} f(XCH_i) \qquad \forall i \in N \quad (17)$$

Where XCH_i represents i^{th} CH across the network X.

- **Distance between BS and CH**

It calculates the distance between BS and CH and analyzes the node's energy consumption in Eq. (18).

$$f2 = \sum_{i=1}^{m} d(CH_{j,}BS) \quad (18)$$

Where, $d(CH_{j,}BS)$ indicates the distance between CH and BS

- **Location factor**

According to the distance between CH nodes and sink nodes, the inter-cluster location factor is employed as a fitness function which is shown in Eq. (19).

$$f_3 = \underset{i=1,2,\dots,M}{Max} d_{p_i,}Sink/d_{c_k},Sink \quad (19)$$

Where, $d_{p_i,}Sink$ represents the distance among every node and sink node, $d_{c_k},Sink$ indicates the distance among chosen CH and sink node, p_i defines individual node in i^{th} index, c_k represents specific CH node.

- **Node degree**

It is dependent on a load of neighbour nodes that is formulated in Eq. (20).

$$f4 = ND_{min} = \sum_{i=1}^{h^T} CM_i \quad (20)$$

Where, ND_{min} represents the minimum node degree, h^T indicates the number of CH, and CM_i determines the overall selected CH neighbours.

- **Trust**

The main fitness utilized in M-TAIPOA is the trust threshold with Direct Trust (DT), Indirect Trust (IDT), and Recent Trust (RT) using in Eq (21) to (23). The $RT_i^d(\tau)$ represents Recent Trust at distance d in i^{th} node and τ defines relational force. The trust threshold fitness function is expressed in Eq. (24).

$$DT_i^d(\tau) = \frac{1}{3}\left[DT_i^d(\tau - 1) - \left(\frac{\tau_{appx} - \tau_{est}}{\tau_{appr}}\right) + \omega\right] \quad (21)$$

$$IDT_i^d(\tau) = \frac{1}{r} DT_i^d(d) \quad (22)$$

$$RT_i^d(\tau) = \alpha * DT_i^d(\tau) + (1 - \alpha) * IDT_i^d(\tau) \quad (23)$$

$$f5 = DT + IDT + RT_i^d(\tau) \quad (24)$$

- **Distance and Energy:**

It evaluates the distance between CH to BS and next-hop node using Eq (25). The SN's residual energy is calculated by considering depleted energy in Eq. (26).

$$f6 = D''_{xdis} = \frac{1}{T_{tch} * N_{nch}} \sum_{n=1}^{T_{tch}} \sum_{o=1}^{N_{nch}} \left[1 - \frac{(D''_{xdis})_{no}}{N_{nch}}\right] \quad (25)$$

$$f7 = E''_{xenr} = \frac{1}{T_{tch}} \sum_{n=1}^{T_{tch}} (E''_{xenr})_n \quad (26)$$

Where N_{nch} represents overall neighboring nodes, D''_{xdis} indicates distance metrics for CH-BS, E''_{xenr} determines residual energy after considering energy usage over time, and $(E''_{xenr})_n$ denotes Residual energy for a time interval n. Every function $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, and\ \alpha_7$ are generated according to min-max normalization. The fitness function is represented in Eq. (27).

$$fitness\ function = \alpha_1 f1 + \alpha_2 f2 + \alpha_3 f3 + \alpha_4 f4 + \alpha_5 f5 + \alpha_6 f6 + \alpha_7 f7 \quad (27)$$

Where $\sum_{i=1}^{7} \alpha_i = 1$; and $\alpha_i \epsilon (0,1)$, τ_{appx} represents the approximate period, τ_{est} defines the estimated period, ω determines node's opinion parameter, r indicates overall node neighbor i, and

Received: September 27, 2024. Revised: November 4, 2024.

$\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, and\ \alpha_7$ denotes weighting factor.

3.4 Clustering stage

Selecting the CH first before establishing the cluster makes effective resource management and network organization. To determine the clusters, the distance and measures are used depending on potential function (S_i) that are expressed in Eq. (28).

$$Potential\ function\ (S_i) = \frac{E_{SCH}}{dis(S_i, SCH)} \tag{28}$$

After the clustering phase, the route phase discovery is determined by utilizing M-TAIPOA to find the SCH's transmission of data to BS.

3.5 Secure routing discovery using M-TAGOA

Initialization and routing selection are the two stages contained in the routing process. Initialization phase ensures that all nodes are organized to be involved in the routing operations. M-TAIPOA evaluates the transmission of data paths between CH and BS. To adjust route discovery process, a route request data transmission is transferred from the source to neighbor node. At that point, the next node with a higher fitness rating sends data back to CH through a reverse path. Then, the source CH obtains data from the neighbor nodes after the routing path are determined. Once the routing path is created, data transmission is initiated via a network.

3.6 CH maintenance

Preserving the cluster stage is one of the essential phases in stabilizing the cluster's load. Efficient CH maintenance ensures optimal aggregation of data and minimizes redundant transmissions which conserve energy. Additionally, it enhances robustness by adapting to node failure and maintaining a reliable communication pathway which is significant in sustaining network performance and efficiency.

4. Results

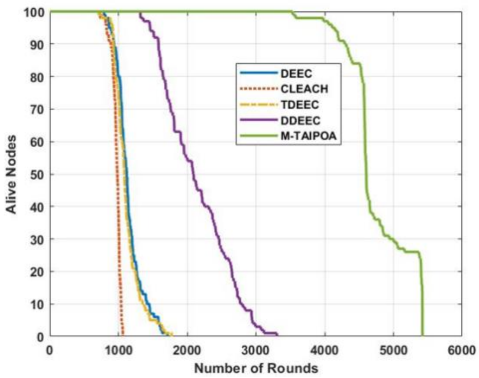
The M-TAIPOA is simulated using MATLAB2018a with a 64-bit Operating System, 6GB RAM, and Intel (R) Core (TM) i5-3570 CPU @ 3.40GHz 3.80 GHz. The E_{elec} represents energy consumption required by electronics of SN per bit of data and ε_{mp} indicates energy for multipath fading. Table 1 determines the simulation parameter of M-TAIPOA approach for scenario 1.

4.1 Performance analysis

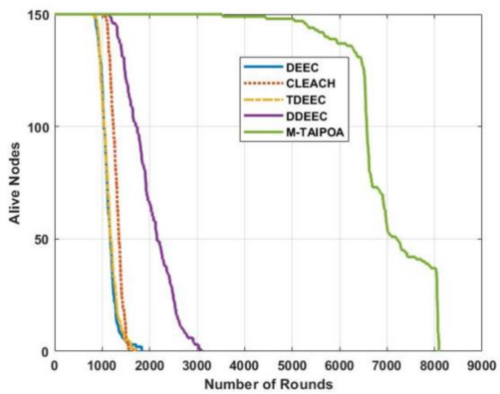
The M-TAIPOA is analyzed with different performance metrics of dead nodes, alive nodes, energy consumption, First Node Dead (FND), Half Node Dead (HND), Last Node Dead (LND), throughput, and Packet Loss Ratio (PLR). The proposed M-TAIPOA is compared with the existing techniques of Centralized LEACH (CLEACH), Threshold DEEC (TDEEC), Distributed Energy-Efficient Clustering (DEEC), and Developed DEEC (DDEEC).

Table 1. Simulation parameters for scenario 1

Parameter	Values
Network size	$200m \times 200m$
Number of nodes	100, 150
Initial energy	0.55 J
E_{elec}	$50nJ/bit/m^2$
Packet size	4000 bits
ε_{fs}	$10pJ/bit/m^2$
ε_{mp}	$0.0013pJ/bit/m^2$



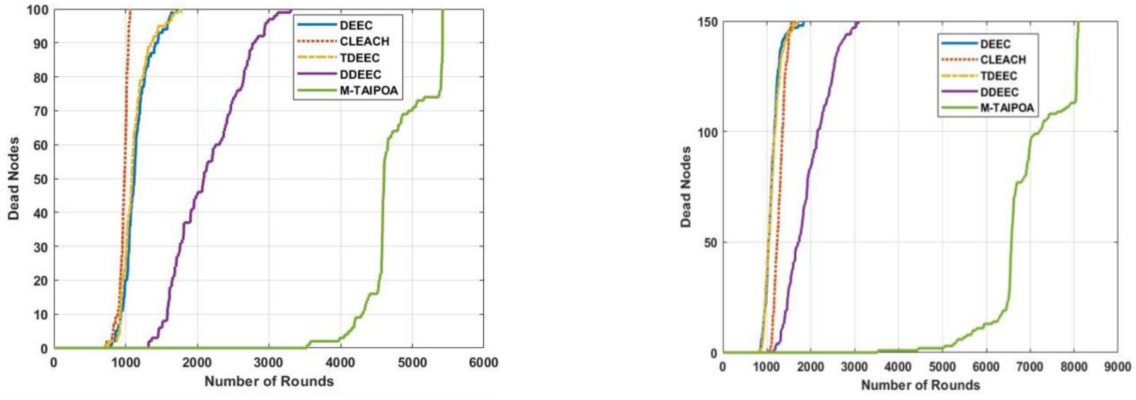
(a)



(b)

Figure. 2 Performance analysis of alive nodes: (a) 100 nodes and (b) 150 nodes

Received: September 27, 2024. Revised: November 4, 2024.



(a) (b)

Figure. 3 Performance analysis of dead nodes: (a) 100 nodes and (b) 150 nodes

4.1.1. Alive nodes

Fig. 2 represents a performance analysis of alive nodes for 100 and 150 nodes. Alive nodes are active network nodes that are presently operational and capable of communicating with other nodes. The analysis represents that M-TAIPOA maintains a higher number of alive nodes because it conserves the energy by preventing malicious nodes in SCH and route discovery processes.

4.1.2. Dead nodes

Fig. 3 indicates the performance evaluation of dead nodes. M-TAIPOA achieves a less dead nodes because of effectively balancing energy consumption and trust management, optimizing node deployment, and increasing network lifetime.

4.1.3. Energy consumption

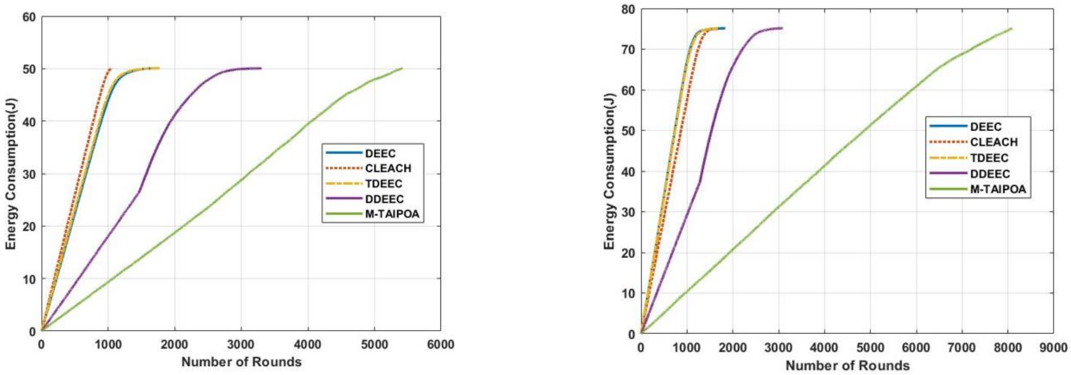
Fig. 4 determines an evaluation of energy consumption for 100 and 150 nodes. The obtained results show that M-TAIPOA achieves lesser energy consumption because of optimizing the routing path and energy usage by a multi-objective method which leads to a more balanced and effective energy distribution between the nodes.

4.1.4. FND, HND, and LND

Fig. 5 indicates the analysis of FND, HND, and LND for 100 and 150 nodes. Several rounds are established with 100 and 150 nodes ranging from 0 to 5000 and 0 to 7000 nodes. Due to M-TAIPOA's available node energy, it attains a high FND, HND, and LND, increased by balancing the energy through routing and CH process without the interference of malicious node.

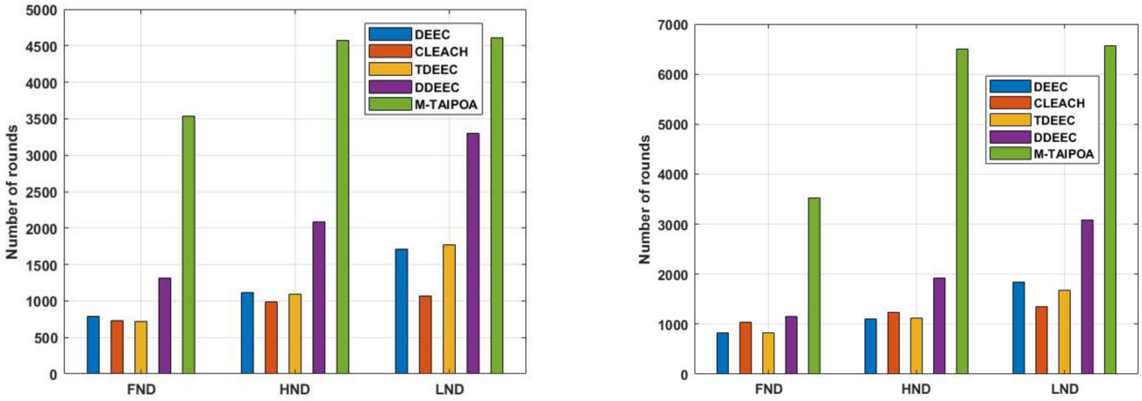
4.1.5. Throughput

Fig. 6 represents the performance analysis of throughput for 100 nodes. M-TAIPOA attains a high throughput when compared to DEEC, CLEACH, TDEEC, and DDEEC for optimizing routing paths and minimizing energy consumption which leads to effective data transmission. It makes sure that the data is transferred reliably while the throughput performance is improved.



(a) (b)

Figure. 4 Performance analysis of energy consumption: (a) 100 nodes and (b) 150 nodes



(a) (b)

Figure. 5 Performance analysis of FND, HND, and LND: (a) 100 nodes and (b) 150 nodes

4.1.6. PLR

Fig. 7 illustrates a performance analysis of PDR for 100 and 150 nodes. The outcomes show that M-TAIPOA achieves high data delivery when compared to the existing methods, DEEC, CLEACH, TDEEC, and DDEEC. Due to its prevention of malicious and failure nodes, the packet loss in the routing process is minimized.

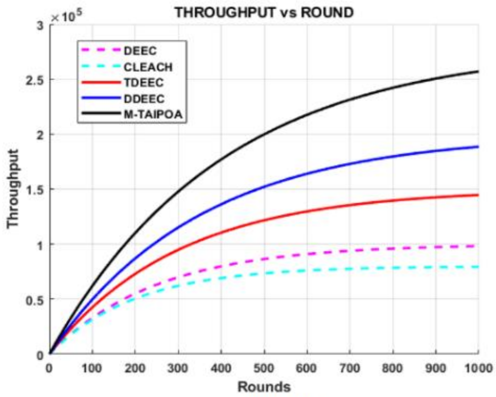


Figure. 6 Performance analysis of throughput

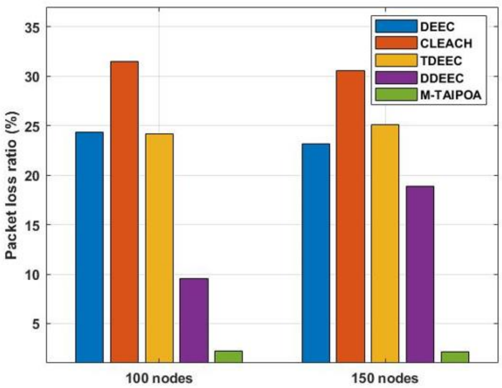


Figure. 7 Performance analysis of PLR

4.1.7. Delay

Fig. 8 determines a performance analysis of delay for 100 nodes. The proposed M-TAIPOA achieves a less delay compared to existing methods like DEEC, LEACH, TDEEC, and DDEEC. Due to proposed M-TAIPOA selects a best route path which minimize delay and increase network efficiency.

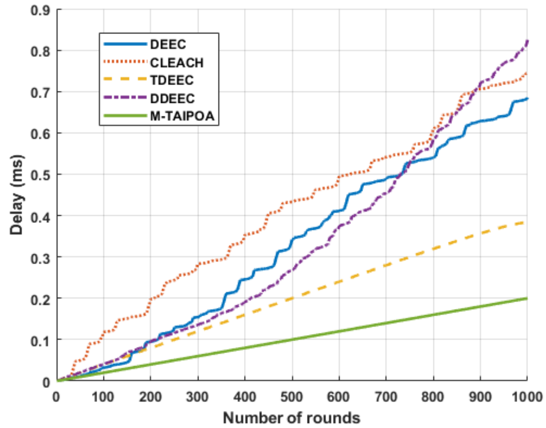


Figure. 8 Performance analysis of delay

Table 2. Specification of different scenarios

Parameters	Scenarios		
	2	3	4
Area	$xm \times ym$ (100 m × 100)	N/A	100 m × 100 m, 1000m × 1000m
No. of. nodes	100	100	100,1000
Initial energy E_0/ Energy assign	0.5	50 J	1J

4.2 Comparative analysis

Table 2 evaluates a specification of different scenarios based on performance measures. The FAL [18] is taken for scenario 2, while EOR-iABC [19] and TAGA [22] are taken for scenarios 3 and scenario 4. The M-TAIPOA is configured to measure the specification performance mentioned in Table 2. The scenarios 2, 3, and 4 contains parameters like area, No. of. nodes, and Initial energy E_0/ Energy assign in Table 2. Tables 3, 4, and 5 exhibit the comparative analysis of M-TAIPOA with FAL [18], EOR-iABC [19], and TAGA [22]. The $xm \times ym$ indicates a field dimension- x maximum (xm) and field dimension-y maximum (ym). The remaining parameter values for scenario 2, 3, and 4 are similar to the Table 1. For example, energy consumption in M-TAIPOA for 10 rounds is 4.5J while EOR-iABC has 9.2J in 100 nodes due to the balanced energy usage and trust management in SCH, alongside the routing process which results in more effective resource allocation and minimized energy wastage across the WSN.

4.3 Discussion

The advantages of M-TAIPOA and the limitations of the existing methods are briefly discussed in this section. The existing methods' limitations like FAL [18] struggled to choose optimal paths, EOR-iABC [19] suffered from premature convergence, and TAGA [22] exhibit less security. The proposed M-TAIPOA overcomes these existing method limitations. The M-TAIPOA process secures data transmission in WSN by balancing its various fitness functions that optimize the routing path and node selection. This comprehensive approach makes optimal cluster formation and reliable routing paths which increases data transmission reliability and network lifetime. Also, trust-aware processes assist in reducing security threats and maintaining robust communication links.

5. Conclusion

In this research, M-TAIPOA is proposed to secure data transmission using the clustering and routing process in WSN. The distance among the neighbor nodes, node degree, the distance among BS and CH, location factor, trust threshold, distance, and energy are used to select SCH and routing from a normal sensor which makes an effective and reliable SN process. POA is enhanced using sine chaos mapping to augment the quality and uniform distribution of the initial population. CSO is employed to increase convergence accuracy and search diversity, while levy flight is deployed to avoid the local optima. This leads to a more reliable and effective clustering and routing which optimizes the energy consumption and makes robust trust management in a network.

Table 3. Comparative analysis of M-TAIPOA with FAL

Method	Performance measures	No. of. nodes	No. of. rounds				
			200	400	600	800	1000
FAL [18]	Residual Energy (J)	100	0.39	0.27	0.2	0.17	0.13
	No. of. alive node		97	81	64	42	33
	Throughput (%)		96	95.5	95.2	93.8	91
Proposed M-TAIPOA	Residual Energy (J)		0.49	0.46	0.44	0.43	0.42
	No. of. alive node		100	100	100	100	100
	Throughput (%)		99	98.8	98.2	97.7	97.5

Table 4. Comparative analysis of M-TAIPOA with EOR-iABC

Method	Performance measures	No. of. nodes	No. of. rounds				
			10	20	30	40	50
EOR-iABC [19]	No. of. Alive nodes	100	100	85	68	52	30
	Energy consumption (J)		9.2	12.7	14.3	15.4	17.3
	Delay m/s		0.189	0.165	0.142	0.127	0.103
Proposed M-TAIPOA	No. of. Alive nodes		100	100	100	100	100
	Energy consumption (J)		4.5	7.2	8.7	9.8	11.4
	Delay m/s		0.062	0.071	0.078	0.081	0.084

Table 5. Comparative analysis of M-TAIPOA with TAGA

Method	Performance measures	No. of. nodes	No. of. rounds				
			200	400	600	800	1000
TAGA [22]	Energy consumption (J)	100	17.3	38.8	64.2	82.3	97.9
Proposed M-TAIPOA		100	2.57	4.82	6.98	9.83	12.47

Received: September 27, 2024. Revised: November 4, 2024.

When compared to EOR-iABC, the M-TAIPOA achieves less energy consumption of 4.5J for 10 rounds in scenario 3. In the future, advanced optimization techniques will be used for clustering and routing processes in WSN.

Notation list

Symbols	Description
R_m	sink node
n and wireless link	direct message between SN at a particular radio rang
P_k and Q_k	Parameters specific to k^{th} sensor node
B_m	Individual SN
B_m^z	a collection of SN in group B_m
m	SN within the overall network
z	Particular characteristics associated with node's collection
$CH(R_r)$	CH characterized by its operational range R_r
r	channel
R	Maximum effective communication distance associated with channel
$s_{q,y}$	Distance between normal CH q and CH y
R_m	Distance between CH and BS at index m
H_0	Initial energy of each sensor nodes
D_b	Energy dissipation associated with receiver at CH
b	Category of dissipation
D_{g+1}	Energy dissipation for the next node
$g+1$	Next node
σ	step size,
Γ	gamma function
β	control the shape
$\sin\left(\frac{\pi\beta}{2}\right)$	trigonometric function
$N(0,\sigma^2)$	normal distribution with mean and variance
u and v	random variables
D_s	Transmitted energy
s	Source node
D_c	Data aggregation
c	Central node
$\lvert\lvert J^a - R_r^a \rvert\rvert$	Distance among normal and CH node
J^a	Attribute associated with normal node
R_r^a	Attribute associated with CH
r	Index
a	Attribute
A_p	Data bytes
p	Packet number
P_i	Prey location chosen by i^{th} pelican
F_i	Objective function value in i^{th} index
k	Random natural number
$X_i^{P_1}$	i^{th} pelican's new state in j^{th} dimension
$F_i^{P_1}$	Adaptation value
$rand$ and I	Random numbers
t	Present number of iterations
T	Maximum number of iterations
R	Constant
$x_{i,j}^{P_2}$	i^{th} pelican's new state in j^{th} dimension
$F_i^{P_2}$	Respective fitness value in a new state
$X_i^j(t)$	Component of individual position with i^{th} index in j^{th} dimension at iteration t
r_1, r_4	Random numbers between [0,1]
r_2, r_3	Random numbers between $[0,2\pi]$
$d(CH_j, BS)$	Distance between CH and BS
$d_{p_i}, Sink$	Distance among every node and sink node
p_i	Individual node in i^{th} index
$d_{c_k}, Sink$	Distance among chosen CH and sink node
c_k	Specific CH node
ND_{min}	Minimum node degree
h^T	Number of CH at maximum number of iterations T
CM_i	Overall selected CH neighbours
N_{nch}	Overall neighboring nodes
nch	each neighbor channels
τ_{appx}	Approximate period
τ_{est}	Estimated period
ω	Node's opinion parameter
r	Overall node neighbor i
S_i	Potential function at i^{th} index
DT	Direct Trust
IDT	Indirect Trust
$RT_i^d(\tau)$	Recent Trust at distance d in i^{th} node
τ	Relational force
XCH_i	i^{th} CH across the network X
D''_{xdis}	Distance metrics for CH-BS
E''_{xenr}	Residual energy after considering energy usage over time
$(E''_{xenr})_n$	Residual energy for a time interval n
$\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5,$	weighting factor
E_{elec}	Energy consumption required by electronics of SN per bit of data
ε_{mp}	Energy for multipath fading
$xm \times ym$	field dimension- x maximum (xm) and field dimension- y maximum (ym)
E_0	Initial energy

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 1st author. The supervision and project administration, have been done by 2nd author.

References

[1] K. Veerabadrappa, and S. C. Lingareddy, "Trust and Energy Based Multi-Objective Hybrid Optimization Algorithm for Wireless Sensor Network", *International Journal of Intelligent Engineering & Systems*, Vol. 15, No. 5, pp. 71-80, 2022, doi: 10.22266/ijies2022.1031.07.

[2] S. Kumar, and R. Agrawal, "A hybrid C-GSA optimization routing algorithm for energy-efficient wireless sensor network", *Wireless Networks*, Vol. 29, No. 5, pp. 2279-2292, 2023.

[3] Z. Yang, L. Li, F. Gu, X. Ling, and M. Hajiee, "TADR-EAODV: A trust-aware dynamic routing algorithm based on extended AODV protocol for secure communications in wireless sensor networks", *Internet of Things*, Vol. 20, p.100627, 2022.

[4] M.R. Reddy, R.M.L. Chandra, P. Venkatramana, and R. Dilli, "Energy-Efficient Cluster Head Selection in Wireless Sensor Networks Using an Improved Grey Wolf Optimization Algorithm", *Computers*, Vol. 12, p. 35, 2023.

[5] K. Veerabadrappa, and S.C. Lingareddy, "Secure Routing using Multi-Objective Trust Aware Hybrid Optimization for Wireless Sensor Networks", *International Journal of Intelligent Engineering & Systems*, Vol. 15, No. 1, pp. 540-548, 2022, doi: 10.22266/ijies2022.0228.49.

[6] B. Kranthikumar, and L.R. Velusamy, "Trust aware secured energy efficient fuzzy clustering-based protocol in wireless sensor networks", *Soft Computing*, 2023.

[7] 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.

[8] N. Subramani, S.K. Perumal, J.S. Kallimani, S. Ulaganathan, S. Bhargava, and S. Meckanizi, "Controlling energy aware clustering and multihop routing protocol for IoT assisted wireless sensor networks", *Concurrency and Computation: Practice and Experience*, Vol. 34, No. 21, p. e7106, 2022.

[9] S.S. Kalburgi, and M. Manimozhi, "Taylor-spotted hyena optimization algorithm for reliable and energy-efficient cluster head selection based secure data routing and failure tolerance in WSN", *Multimedia Tools and Applications*, Vol. 81, No. 11, pp. 15815-15839, 2022.

[10] S.K. Barnwal, A. Prakash, and D.K. Yadav, "Improved African buffalo optimization-based energy efficient clustering wireless sensor networks using metaheuristic routing technique", *Wireless Personal Communications*, Vol. 130, No. 3, pp. 1575-1596, 2023.

[11] A. Vinitha, M.S.S. Rukmini, and Dhirajsunehra, "Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm", *Journal of King Saud University-Computer and Information Sciences*, Vol. 34, No. 5, pp. 1857-1868, 2022.

[12] D. Mehta, and S. Saxena, "Hierarchical WSN protocol with fuzzy multi-criteria clustering and bio-inspired energy-efficient routing (FMCB-ER)", *Multimedia Tools and Applications*, Vol. 81, No. 24, pp. 35083-35116, 2022.

[13] R.I. Sajan, V.B. Christopher, M.J. Kavitha, and T.S. Akhila, "An energy aware secure three-level weighted trust evaluation and grey wolf optimization based routing in wireless ad hoc sensor network", *Wireless Networks*, Vol. 28, No. 4, pp. 1439-1455, 2022.

[14] M.K. Roberts, and P. Ramasamy, "Optimized hybrid routing protocol for energy-aware cluster head selection in wireless sensor networks", *Digital Signal Processing*, Vol. 130, p. 103737, 2022.

[15] A. Ali, A. Ali, F. Masud, M.K. Bashir, A.H. Zahid, G. Mustafa, and Z. Ali, "Enhanced Fuzzy Logic Zone Stable Election Protocol for Cluster Head Election (E-FLZSEPFCH) and Multipath Routing in wireless sensor networks", *Ain Shams Engineering Journal*, Vol. 15, No. 2, p. 102356, 2024.

[16] M. Al-Sadoon, and A. Jedidi, "A secure trust-based protocol for hierarchical routing in wireless sensor network", *International*

Journal of Electrical & Computer Engineering, Vol. 12, No. 4, pp. 3838-3849, 2022.

[17] R. Nagaraju, C. Venkatesan, J. Kalaivani, G. Manju, S.B. Goyal, C. Verma, C.O. Safirescu, and T.C. Mihaltan, "Secure Routing-Based Energy Optimization for IoT Application with Heterogeneous Wireless Sensor Networks", *Energies*, Vol. 15, p. 4777, 2022.

[18] S.P. Prakash, D. Kavitha, and P.C. Reddy, "Safe and secured routing using multi-objective fractional artificial lion algorithm in WSN", *Concurrency and Computation: Practice and Experience*, Vol. 34, No. 21, p. e7098, 2022.

[19] G. Santhosh, and K.V. Prasad, "Energy optimization routing for hierarchical cluster based WSN using artificial bee colony", *Measurement: Sensors*, Vol. 29, p. 100848, 2023.

[20] J. Paruvathavardhini, and B. Sargunam, "Stochastic Bat Optimization Model for Secured WSN with Energy-Aware Quantized Indexive Clustering", *Journal of Sensors*, Vol. 2023, No. 1, p. 4237198, 2023.

[21] W. Osamy, A.M. Khedr, D. Vijayan, and A. Salim, "TACTIRSO: Trust aware clustering technique based on improved rat swarm optimizer for WSN-enabled intelligent transportation system", *The Journal of Supercomputing*, Vol. 79, No. 6, pp. 5962-6016, 2023.

[22] Y. Han, H. Hu, and Y. Guo, "Energy-aware and trust-based secure routing protocol for wireless sensor networks using adaptive genetic algorithm", *IEEE Access*, Vol. 10, pp. 11538-11550, 2022.

[23] P. Trojovský, and M. Dehghani, "Pelican Optimization Algorithm: A Novel Nature-Inspired Algorithm for Engineering Applications", *Sensors*, Vol. 22, p. 855, 2022.