Received: October 17, 2024. Revised: November 13, 2024.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Secure and Energy Efficient Clustering and Routing Using Multi-Objective Trust Aware Cosine Tasmanian Devil Optimization Algorithm in WSN

M. DharmaTeja[1]* R. Srinivasan[1]

[1]*Department of Computer Science & Engineering, School of Computing,*
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India
* Corresponding author's Email: dharmatejamd@gmail.com

Abstract: Wireless Sensor Networks (WSNs) are a distributed group of Sensor Nodes (SN) that are dispersed geographically in the organized environment to monitor and collect data on environmental conditions. In the network, each node has a limited wireless transmission range hence it is significant for nodes to transfer data through intermediatory nodes to reach the destination, which is a Base Station (BS). However, energy consumption with secure communication is a primary challenge due to resource-constraint nature of device and its communication is unfriendly and open environment. This research proposes Multi-objective Trust-Aware Cosine Tasmanian Devil Optimization Algorithm (M-TACTDOA) to select the Secure Cluster Head (SCH) and routing path in WSN. The TDOA is improved by using Cosine Perturbation Differential Evolution mechanism (CPDE) which addresses local optima issue and rapid convergence speed. By applying fitness function, the M-TACTDOA determine and avoid malicious nodes which provides secure and reliable data transmission. The proposed M-TACTDOA achieves a less energy consumption of 0.08 J compared to existing techniques like Energy Optimization Routing by employing improved Artificial Bee Colony (EOR-iABC).

Keywords: Base station, Cosine perturbation differential volution, Multi-objective trust-aware cosine Tasmanian devil optimization Algorithm, Secure cluster head, Wireless sensor networks.

1. Introduction

A Wireless Sensor Network (WSN) has a huge number of spatially distributed microelectronic devices. A Sensor Node (SN) generates a global view of an observed area with local detection via each sensor [1]. These nodes manage components of their environments and communicate with their peers or transmit directly to a Base Station (BS). The nodes reliably consume more energy during the communication process [2]. In WSN, SN clustering is energy efficient and contains better topology management. Clustering minimizes the delay in transferring data from SN to BS. The routing protocols are established which have better stability, prolonged network lifetime, and throughput [3]. The Cluster Head (CH) is one SN while the remaining SN are called Cluster Members (CM) [4]. In WSN, inter-cluster and intra-cluster communication are the two ways for clusters to communicate with each other. Every cluster contains its own CH interface among its CM and BS [5]. SN has inadequate storage capacity and computing power and it is driven by a battery with constraint energy [6]. It is challenging to replace the battery in time to supplement energy once the energy is exhausted [7]. Hence, while constructing a WSN routing protocol, increasing energy consumption and extending network lifetime are the significant aims to be considered in the presence of malicious nodes [8, 9].

Security is another significant concern in WSN and meanwhile, SNs are deployed randomly in an open and hostile environment for various environments [10, 11]. The nodes are vulnerable to different kinds of security attacks due to their self-configuring nature which affects the routing [12]. The attacks produced by malicious nodes interrupt the data routing, permanently, or temporarily stop the

communication exchange, and divert the network functioning [13]. Trust-based security provides an effective relationship and increases security between the nodes [14]. In trust-based approaches, future actions are forecasted depending on the behavior of prior nodes and enable an efficient decision in malicious nodes [15]. If a node is identified, it becomes isolated and neighboring nodes are notified to join it for aggregation, data delivery, or any other processing functions [16, 17]. Also, the trust-based neighbor selection is efficient in validating the neighbor nodes and increases the reliability and privacy of data transmission [18]. However, energy consumption with secure communication remains a main challenge because of resource-constraint nature of device and its communication is unfriendly and open environment. To solve this issue, the M-TACTDOA is proposed for SCH and routing path selection in WSN by considering different multi-objective function which increase security and minimize energy consumption.

The main contribution of this research is as follows:

- By optimizing the selection of SCH and route path, data efficiency is enhanced in M-TACTDOA which minimizes redundant transmission of data and ensures energy-efficient communication between trusted nodes.
- Distance among neighbor node, location factor, distance among CH and BS, node degree, and trust metrics are performed in SCH selection as multi-objective function which provides the reliability and effectiveness.
- Energy, node degree, and distance are used as multi-objective function for secure routing path which maximize network lifetime and reduces delay in IoT.

This research paper is organised as follows: Section 2 details the literature survey and Section 3 explains the proposed methodology. Section 4 provides the simulation results, and the conclusion of this research paper is given in Section 5.

2. Literature survey

The related work about energy efficient clustering and routing in WSN were discussed along with their advantages and disadvantages

Han [19] developed an energy-aware Trust-based routing by utilizing an Adaptive Genetic Approach (TAGA) for WSN. The threshold function was used to choose the optimal CH by considering the dynamic node change based on residual energy and comprehensive trust values. Then, the GA with adaptive crossover and mutation probability was employed which provides the best secure routing for CH. TAGA increased security by constructing an adaptive trust approach to determine each node's comprehensive trust value for resisting primary and special attacks. However, TAGA suffer from high energy consumption because of frequent genetic process which drain limited battery resources rapidly in SN.

Mansour [20] implemented an Energy-Aware Fault Tolerant Clustering with Routing for Improved Survivability (EAFTC-RIS) for enhanced survivability in WSN. EAFTC-RIS chooses the optimal routes and CH to destination in ideal manner with a fault tolerance approach. EAFTC-RIS employs the Moth Flame Optimization (MFO)-based clustering to select the CH and cluster structure. Additionally, the fault tolerance approach was considered to increase network survivability. Nevertheless, EAFTC-RIS struggled with high latency during the transmission of data because of additional overhead from clustering and routing protocols which prioritize fault tolerance and energy conservation.

Reddy and Murthy [21] introduced a Multi-objective Trust Centric Reptile Search Algorithm (M-TCRSA) to generate a secure cluster-based routing in WSN. M-TCRSA was utilized to ensure the Secure CH and route discovery to attain reliable communication among the WSN. The developed approach provides enhanced security against malicious attacks when increasing energy efficiency. M-TCRSA reduces the packet loss and undesirable consumption of energy produced by malicious attacks. However, the M-TCRSA suffers from high consumption of energy due to complex process involved in trust evaluation and CH formation.

Vinitha [22] presented a Taylor-based Cat Salp Swarm Approach (Taylor C-SSA) for secure and energy-aware multi-hop routing in WSN. At first, the energy-efficient CH was chosen by utilizing Low Energy Adaptive Clustering Hierarchy (LEACH) to communicate the data effectively. Then, the SN transmitted the data among CH to BS via the selected optimal hop. The best hop selection was performed by utilizing a presented Taylor C-SSA. However, Taylor C-SSA struggled with reduced throughput because of potential congestion in heavily traffic nodes that results in enhanced packed loss and delays.

Santhosh and Prasad [23] suggested an Energy Optimization Routing by employing an improved Artificial Bee Colony (EOR-iABC) for SCH and route path selection in WSN. The suggested approach adapts a distinctive search mechanism by utilizing

iABC to select the energy-efficient CH via mutation and crossover process. A best path CH to BS was determined by energy-efficient fitness node which enhances network efficiency. Nevertheless, EOR-iABC had minimum convergence because of suboptimal solutions prior discovering the search space that resulted in suboptimal energy distribution.

In the overall evaluation, the existing techniques had limitations such as high energy consumption, less throughput, high delay, and slow convergence. To overcome this issue, the M-TACTDOA is proposed for SCH and routh path selection in WSN. By focusing on both energy efficiency and secure communication, it minimizes energy consumption and delays during the transmission of data. Moreover, the M-TACTDOA increase throughput by choosing the optimal routes for data packets which results in rapid convergence and improved network performance in WSN.

3. Proposed methodology

In this research, reliable and secure communication is ensured by utilizing M-TACTDOA. It contains four stages: sensor deployment, SCH discovery, route discovery, and cluster formation. The SCH and secure route path are established to avoid malicious attacks when broadcasting the data packets. Hence, the consumption of energy and unwanted packet drop is decreased by applying M-TACTDOA. Fig. 1 represents the network structure of WSN.

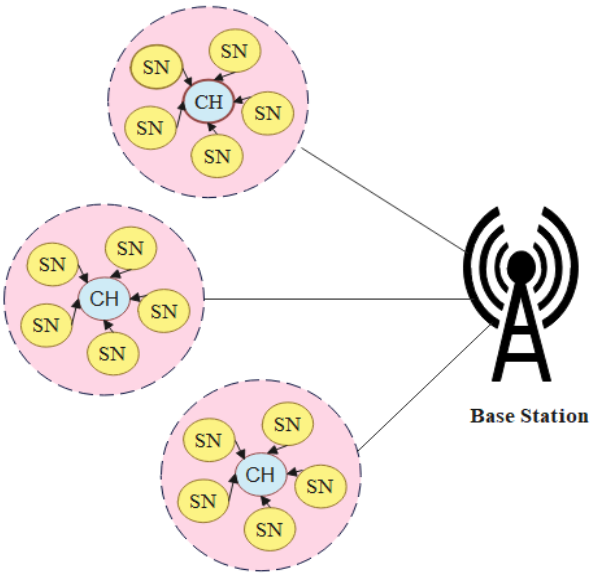


Figure. 1 Network model for WSN

3.1 System model

This section makes certain assumptions regarding WSN and enlarges the energy consumption model. A node does not yield global data and each SN obtains local data and transmits it to the corresponding CH during every round. To obtain data, gateway aggregates to eliminate redundant and irrelevant data and transmits aggregated data to BS with other CH as subsequent relay nodes. Each node turns off its radios among two neighboring rounds to save energy.

3.2 Network model

It makes a subsequent assumption regarding network model which is explained below

- Area observed by WSN is a flat regular graph in that SN is distributed randomly. The position of each node is fixed and no more human intervention after network is positioned. Also, all node involves a globally unique network identifier.
- Each SN is isomorphic, i.e. each nodes contain an identical initial energy, computing power, and communication ability. The SNs are driven by limited energy batteries that do not replenish.
- The node distinguishes its position to compute the distance to the transmitter based on established signal strength. According to communication distance, the power of wireless transmission is self-regulated and their power is chosen independently.
- Then, the BS is placed inside or outside the observed area and its computing power and energy are unlimited.

3.3 Energy consumption

Depending on distance among a transmitting and receiving ends, both free space and multipath (mp) fading channel is employed. If a distance is smaller than threshold value d_0, free space f_s deployed then a multipath model is applied. Consider $E_{elec}, \varepsilon_{fs}$, and ε_{mp} indicates the energy consumed by electronic circuits during transmission, energy expenditure per unit distance, and energy associated with multipath fading channel propagation. Then, the energy required by radio to transmit l-bit binary message and distance d is formulated in Eq. (1).

$$E_T(l,d) = \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2 & for\ d < d_0 \\ lE_{elec} + l\varepsilon_{mp}d^4 & for\ d \geq d_0 \end{cases} \quad (1)$$

Energy required by radio for receiving an l-bit message $E_R(l)$ is expressed in Eq. (2).

$$E_R(l) = lE_{elec} \quad (2)$$

However, the amplifier energy $\varepsilon_{fs}d^2/\varepsilon_{mp}d^4$ is dependent on distance among transmitting and receiving nodes and the appropriate Bit Error Rate (BER). Typically, the radio wave propagation is an variable approach that complicates the progress.

3.4 SCH Selection using M-TACTDOA

In M-TACTDOA, a significant SCH and secure route path is accomplished to secure and reliable transmission of data. M-TACTDOA is selected for SCH and routing in WSN because of its ability to simultaneously optimize multiple objectives like energy efficiency and security. Also, it balances the exploration and exploitation which increases robustness and security. While Particle Swarm Optimization (PSO) suffers from premature convergence, Rain Optimization Algorithm (ROA) and Dung Beetle Optimization (DBO) are less effective in managing dynamic and complex environments. However, the TDOA has a more adaptive and effective mechanism to determine optimal solutions in WSN due to the unique approach to problem-solving which enhances overall security and network performance. Initially, SCH is determined from the normal sensors by applying distance among neighbor nodes, node degree, distance among CH and destination, location factor, and trust. Then, the M-TACTDOA is employed to determine the secure path from SCH to Mobile Sink (MS) by employing energy, node degree, and distance. Fig. 2 depicts the block diagram of the M-TACTDOA approach.

3.4.1. Node deployment

Initially, the nodes are positioned randomly in WSN followed by a secure path and optimal SCH is established by utilizing M-TACTDOA which assists in obtaining a secure reliable data transmission in the network. This process increases the security and reliability of data transmission over the network by ensuring that the chosen communication path and node deployment are optimized for secure and effective data exchange.

3.4.2. Node initialization

It provides optimal handling and balancing multi-objectives by pretending the foraging behavior of the Tasmanian devil. It extends the SN lifespan and network performance in dynamic WSNs. Consider, the Tasmanian devil i involves $X_i = (X_{i,1}, X_{i,2}, \ldots, X_{i,n})$ where n determines that M-TACTDOA's dimension is equivalent to number of CH, X_i determines candidate solution of i^{th} individual in the population, $X_{i,1}, X_{i,2}, \ldots, X_{i,m}$ represents 1^{st}, 2^{nd} up to m^{th} component of candidate solution of X_i for the Tasmanian devil algorithm. Once the initialization of node is performed, the SCH is established by utilizing M-TACTDOA.

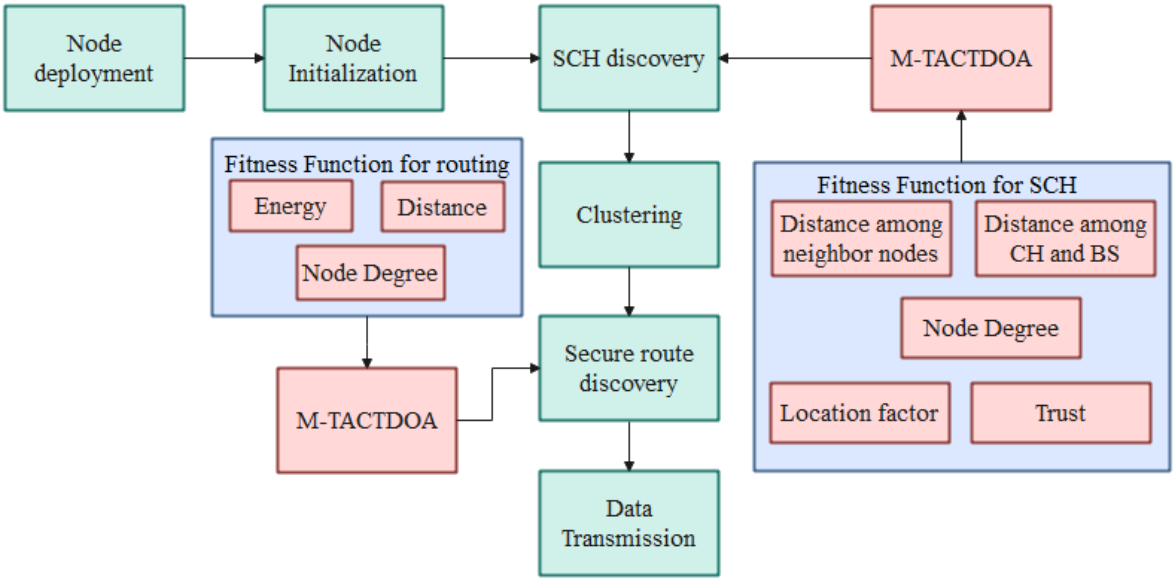


Figure. 2 Block diagram for the M-TACTDOA approach

3.4.3. SCH process

The optimal SCHs from the normal nodes are recognized by applying M-TACTDOA with different fitness metrics. TDOA is a population-based stochastic approach using Tasmanian devils according to the search agents based on the exploration and exploitation process which are described in detail below:

3.4.2.1. Initialization

The initial population of agents is generated randomly depending on the constraints of the issue. The TDOA's population member acts as searchers in solution space which provides candidate values for issue variables depending on their search space positions. The collection of TDOA members is modeled by utilizing a matrix which is expressed in Eq. (3).

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_2 \\ \vdots \\ X_3 \end{bmatrix}_{N\times m} = \begin{bmatrix} x_{1,1} & \cdots & x_{1,j} & \cdots & x_{1,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{i,1} & \cdots & x_{1,j} & \cdots & x_{i,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{N,1} & \cdots & x_{N,j} & \cdots & x_{N,m} \end{bmatrix}_{N\times m} \quad (3)$$

Where X indicates Tasmanian devil population, X_i represents i^{th} candidate solution X, $x_{i,j}$ denotes candidate value of i^{th} solution in j^{th} variable, N determines Tasmanian devil search, and m illustrates number of variables. The objective function is computed by evaluating each candidate solution using a variable defined in the objective function as formulated in Eq. (4).

$$F(X) = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} F\ (X_1) \\ \vdots \\ F\ (X_i) \\ \vdots \\ F\ (X_N) \end{bmatrix}_{N\times 1} \quad (4)$$

Where F represents objective function vector value, F_i denotes obtained value of objective function via i^{th} candidate solution. The candidate solution results in optimal objective function value which is regarded as population's optimal member and it is updated depending on newly acquired values at every iteration.

3.4.2.2. Exploration stage

Tasmanian devil prefers feeding on carrion found within their territory rather than actively hunting for prey. In the TDOA, the other population member position in search space is considered as the carrion position. Eq. (5) represents the random selection where i^{th} Tasmanian devil selects the k^{th} population as carrion. Hence, k is a chosen randomly among 1 when i is chosen oppositely which is formulated in Eq. (5).

$$C_i = X_k, i = 1,2,\ldots,M, k \in \{1,2,\ldots,M | k \neq i\} \quad (5)$$

Where C_i represents selected carrion by i^{th} Tasmanian devil, X_k indicates variable X associated with population k. Based on chosen carrion, the Tasmanian devil's new location is expressed in Eqs. (6) and (7).

$$x_{i,j}^{new,S1} = \begin{cases} x_{ij} + r.\left(c_{ij} - I.x_{ij}\right), & Fc_i < F_i \\ x_{ij} + r.\left(x_{ij} - c_{ij}\right) & otherwise \end{cases} \quad (6)$$

$$X_i = \begin{cases} x_{i,j}^{new,S1}, & Fc_i < F_i \\ X_i & otherwise \end{cases} \quad (7)$$

Where $x_{i,j}^{new,S1}$ represents new location of i^{th} Tasmanian devil in exploration stage, $F_i^{new,S1}$ indicates an objective function value, Fc_i determines objective function for selected carrion, r illustrates random numbers in [0, 1] range, and I defines a random integer number.

3.4.2.3. Exploitation stage

During the attack process, the Tasmanian devil is split into two phases. In the initial phase, it chooses prey by scanning the information and initiates attacks. Then, after obtaining near to the prey, it intercepts and chases the prey and starts feeding [24]. However, TDOA has limitations like local optima issues and slow convergence in later iterations. To address this issue, the Cosine Perturbation Differential Evolution mechanism (CPDE) is developed during the exploitation phase. The cosine perturbation factor employs the cosine function by balancing the exploitation and exploration which prevents the approach from escaping into local optima issues and increases global search performance. The randomness of this factor manages population diversity and increases convergence speed as well as robustness which enables it appropriate for different issues and search stages. It integrates the cosine perturbation factor and differential evolution

mechanism while the attack condition and goal selection are met. The updated position of enhanced Tasmanian Devil is expressed in Eq. (8).

$$x_{i,j}^{new,S1} = x_{ij} + r_{cf} \times (x_{rdm1} - x_{rdm2}) \quad (8)$$

Where x_{rdm1} and x_{rdm2} represents two distinct randomly chosen individuals in present iteration, r_{cf} indicates randomly produced numbers following cosine-style variation which is formulated in Eq. (9).

$$r_{cf} = (\cos(2 \times rand) + 1) \times rand \quad (9)$$

To sum up, the distribution of motion strategy for exploitation and exploration phase for the 1st phase is represented using Eqs. (10) and (11).

$$x_{i,j}^{new,S1} = \begin{cases} x_{top\_T\_devil} + RL_{Slf_{ad}} \times \left(x_{top_{T_{devil}}} - I \times x_{ij}\right), \\ Fc_i < F_i \\ x_{i,j} + R_{Brownian} \times \left(c_{ij} - I \times x_{ij}\right), \\ otherwise \end{cases} \quad (10)$$

$$x_{i,j}^{new,S2} = \begin{cases} x_{i,j} + r \times \left(p_{ij} - c \times x_{ij}\right), & if\ Fp_i < F_i \\ x_{i,j} + r_{cf} \times (x_{rdm1} - x_{rdm2}), & otherwise \end{cases} \quad (11)$$

Where $x_{i,j}^{new,S1}$ indicates a new updated value at (i,j) position in exploitation stage, $x_{top\_T\_devil}$ represents reference or target value, $RL_{Slf_{ad}}$ determines random learning factor or self-adaptive factor, c illustrates constant. Differential evolution mechanisms which rely on differential processes, provide global search abilities for addressing non-linear and non-smooth issues. The cosine perturbation factor generates better robustness and additional flexible parameter adjustments. This integration obtains a balance between local optimization and global search, which enhances adaptability and model performance.

3.5 Fitness function

The SCH and secure route path fitness help to increase lifetime of network and minimize energy consumption for evaluating different performance metrics which are explained below,

Distance between neighbor nodes: Each CH determines a neighbor CH and transfers the message to node degree and CH after the node is selected which is formulated in Eq. (12).

$$f1 = \sum_{i=1}^{n} f(XCH_i) \quad \forall i \in B \quad (12)$$

Where X represents certain point of data or vector, XCH_i illustrates a feature associated with i^{th} neighboring node, $f(XCH_i)$ denotes function applied to XCH_i, B indicates set of all neighboring nodes, and n denotes total number of nodes.

Distance between BS and CH: The node calculates the distance between BS and CH and analyzes the node's energy consumption based on the transmission path using Eq. (13).

$$f2 = \sum_{i=1}^{p} d(CH_{j,}BS) \quad (13)$$

Where $d(CH_{j,}BS)$ determines a distance between BS and CH and p illustrates the total number of CH

Node Degree: It is some non-CH membership associated with its corresponding mobile node which is used for both SCH and secure route path. If the mobile node has fewer members, then it sustains for a long duration as described in Eq. (14).

$$f3 = ND_{min} = \sum_{i=1}^{h^T} CM_i \quad (14)$$

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

Location Factor: Based on the distance among the sink node and CH node, the location factor is applied using Eq. (15).

$$f4 = \underset{i\,=\,1,2,\ldots,M}{Max} d_{pi,Sink}/d_{ck,Sink} \quad (15)$$

Where $d_{pi,Sink}$ refers to distance among each node pi and sink node as well as $d_{ck,Sink}$ indicates the distance among chosen CH ck and sink node.

Trust: It is observed as a primary parameter in CH selection to enhance security. The mutual trust made in certain period is employed to accomplish the transmission. Direct Trust (DT) is calculated on approximate communication period between i^{th} node and d^{th} destination using Eq. (16). Moreover, the node without a witness parameter is authenticate through Indirect Trust (DT) is represented in Eq. (17). Recent Trust (RT) is evaluated by DT and IDT with vital validity and declared the sink or destination using Eq. (18). Comprehensive trust integrates DT and IDT to determine if the node is trusted or not which generates trustworthy nodes and high security using Eq. (19). The overall fitness function of trust is represented using Eq. (20).

$$DT_i^d(\tau) = \frac{1}{3}[DT_i^d(\tau-1) - \left(\frac{\tau_{appx}-\tau_{est}}{\tau_{appx}}\right) + \omega] \quad (16)$$

$$IDT_i^d(\tau) = \frac{1}{r}\sum_{i=1}^{r} DT_i^d(d) \quad (17)$$

$$RT_i^d(\tau) = \propto^* DT_i^d(\tau) + (1-\propto)^* IDT_i^d(\tau) \quad (18)$$

$$CT_{(i,j)}^n = \begin{cases} (1-\beta) * DT_{(i,j)}^n + \beta * IDT_{(i,j)}^n & if\, n_j \neq m \\ (1-\beta) * IDT_{(i,j)}^n + \beta * DT_{(i,j)}^n & else\ n_j = m \end{cases} \quad (19)$$

$$f5 = DT_i^d(\tau) + IDT_i^d(\tau) + RT_i^d(\tau) + CT_{(i,j)}^n \quad (20)$$

Where τ_{appx} represents approximate period, τ_{est} indicates estimated period for authenticating public keys, ω defines node's opinion parameter, r determined overall node neighbor, DT_i^d illustrates Direct Trust at distance d in i^{th} node, IDT_i^d represents Indirect Trust at distance d in i^{th} node, $RT_i^d(\tau)$ defines Recent Trust at distance d in i^{th} node, and $CT_{(i,j)}^n$ represent Comprehensive Trust in entity ij at n^{th} iteration

Distance: It is a Euclidean distance among the node to next-hop and the energy consumption is evaluated by the transmission distance. If it is less, then it consumes a less amount of energy using Eq. (21).

$$f6 = D''_{xdis} = \frac{1}{T_{tch}*N_{nch}}\sum_{n=1}^{T_{tch}}\sum_{o=1}^{N_{nch}}[1 - \frac{(D''_{xdis})_{no}}{N_{nch}}] \quad (21)$$

Where N_{nch} represents an overall neighboring node, D''_{xdis} denotes distance for CH to BS, and no determines two ranges.

Energy: The SN's energy is computed by combining energy depletion through every node state using Eq. (22).

$$f7 = E''_{xenr} = \frac{1}{T_{tch}}\sum_{n=1}^{T_{tch}}(E''_{xenr})_n \quad (22)$$

Where T_{tch} indicates total number of CH, E''_{xenr} indicates residual energy after determining usage of energy at time, $(E''_{xenr})_n$ represents residual energy for a time internal n. The distance between neighbor node $f1$, distance between BS and CH $f2$, node degree $f3$, location factor $f4$, trust $f5$, distance $f6$, and energy $f7$ are applied for SCH and secure routing path by M-TACTDOA that are transformed as 1 objective function F using Eq. (23).

$$F = \rho_1 \times f1 + \rho_2 \times f2 + \rho_3 \times f3 + \rho_4 \times f4 + \rho_5 \times f5 + \rho_5 \times f6 + \rho_7 \times f7 \quad (23)$$

Where $\rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6, \rho_7$ represents weighting factor.

3.6 CH formation

SCH formation is significant to maintain the reliability and integrity of a network. It contains a choosing a SCHs depending on criteria like trustworthiness, node energy, and proximity to others to ensure effective communication and minimize the risk of attacks. Initially, selecting a SCH is essential because it helps to effectively handle the communication in clusters which increases the resource utilization and transmission of data among nodes. The normal sensors are assigned to the SCH in the process of cluster generation. The energy and distance are measured as a potential function which is represented in Eq. (24).

$$Potential\ function\ (N_i) = \frac{E_{SCH}}{dis(N_i,SCH)} \quad (24)$$

Where N_i represents potential function, and E_{SCH} indicates energy level of SCH. Then, the determination of routing path is updated using M-TACTDOA to identify CH data transmission to BS.

3.7 Route Path using M-TACTDOA

The M-TACTDOA is applied to determine the route path discovery. The following steps managed in the route path discovery are detailed below:

- The probable paths from the source SCH to BS are evaluated as the initial solutions to discover the route path. Each solution dimension is equivalent to the amount of transmit SCH exist in the route.
- Also, the fitness metrics is calculated by utilizing energy and distance are determined using Eq. (21) and (22) which is applied to update the solution location. The route path discovery's location update is established depending on iterative process of M-TACTDOA.

Therefore, the best secure route is chosen to enhance the security of WSN while improving the data delivery.

3.8 Cluster maintenance

Updating the cluster structure is essential for ensuring network efficiency and stability. This involves like reselecting nodes or electing new CH depending on network dynamics and energy levels. It helps the network to make better use of resource which extends node lifetimes, and manages reliable communication. Efficient cluster maintenance assists in preventing network failures and minimizes the impact of node failure and energy depletion. It acquires a reliable transmission of data by establishing this progress effectively.

4. Simulation results

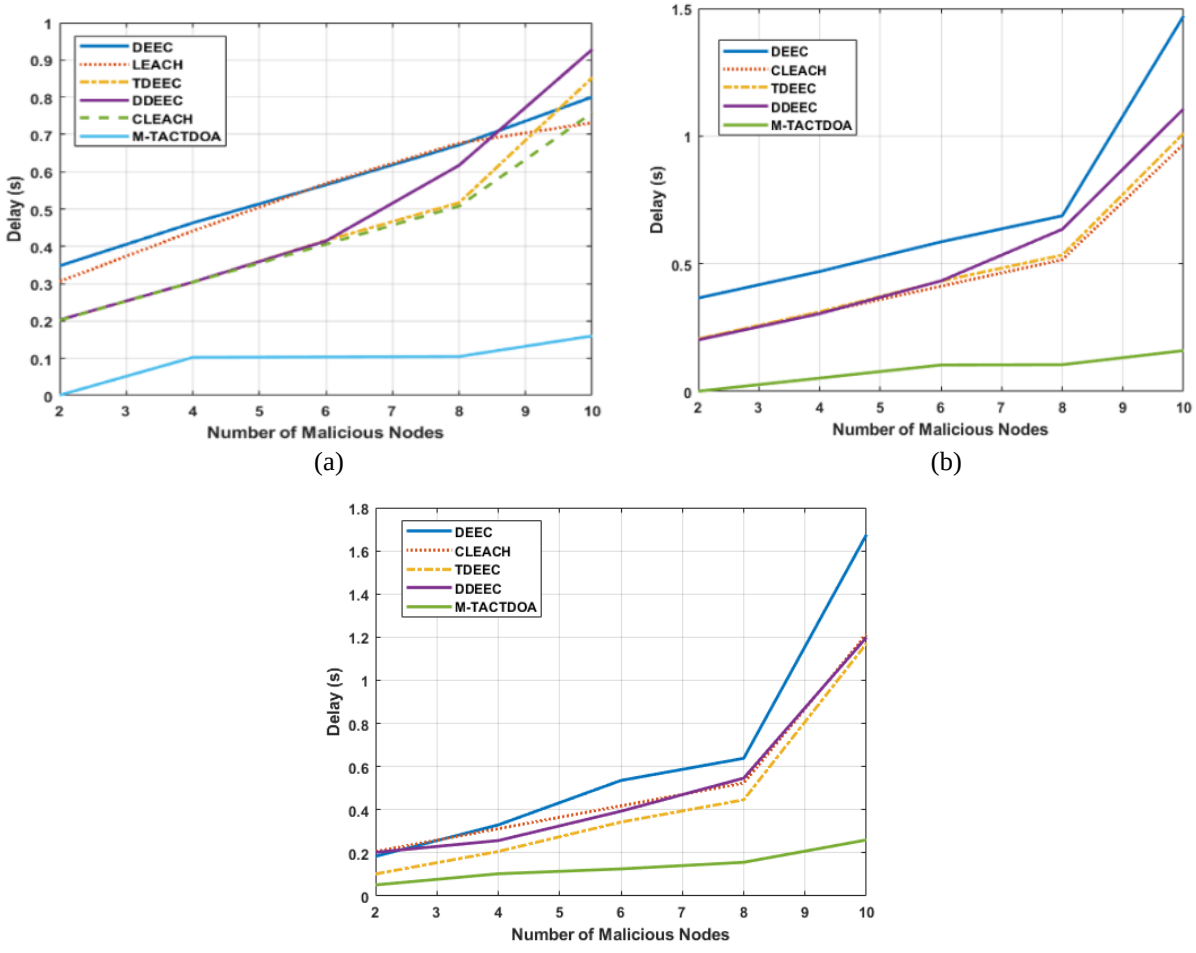
This section provided the performance analysis of proposed M-TACTDOA by using MATLAB R2018a to determine the SCH and routing in WSN. The system is functioned with 6GB RAM, Windows 10 operating system, and an i7 Intel processor. The SCH and route path discovery are performed by utilizing M-TACTDOA to attain the secure communication. Table 1 provides the simulation parameters of M-TACTDOA technique.

4.1 Performance Analysis

Fig. 3 shows a performance analysis of delay (s). The proposed M-TACTDOA is compared with existing methods like Developed DEEC (DDEEC), LEACH, Energy-Efficient Clustering (DEEC), Centralized LEACH (CLEACH), and Threshold DEEC (TDEEC). Delay refers to amount of time it takes for data packets to travel from a source to destination (BS). It has processing, propagation, transmission, and queuing delays. When compared to these techniques, the proposed M-TACTDOA obtains a lesser delay because M-TACTDOA selects the optimal route path that decreases the distance and maximizes the network efficiency.

Table 1. Simulation parameter of M-TACTDOA

Parameters	Values
Simulation time	100 ms
Number of nodes	50, 100, 150
Network size	$200m \times 200m$
Packet size	6000 bits
Initial energy	0.55 J



(a) (b)

(c)

Figure. 3 Performance analysis of delay: (a) 50 nodes, (b) 100 nodes, and (c) 150 nodes

Fig. 4 determines the performance analysis of alive nodes. Alive nodes define that SNs are still executes their function like communication and processing. Managing a high number of alive nodes is significant to extend the network lifespan and ensuring reliable data transmission. When compared to existing techniques, the proposed M-TACTDOA obtains a high time period due to it choosing the most relevant node for SCH and transmission of data that preserves less energy and increases network lifetime.

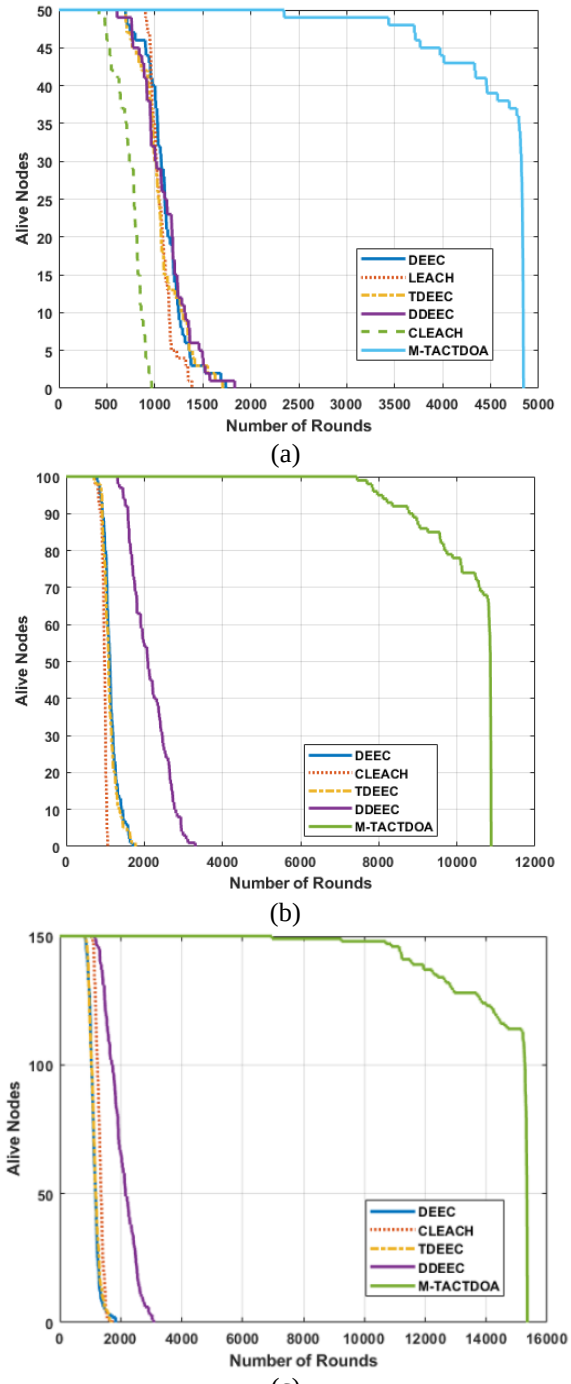


Figure. 4 Performance evaluation of alive nodes: (a) 50 nodes, (b) 100 nodes, and (c) 150 nodes

Fig. 5 indicates a performance evaluation of dead nodes. Dead nodes refer to SNs which have depleted their energy resources and no longer contribute to network activities. The presence of dead nodes disturbs network connectivity, minimizes coverage, and decreases overall network performance. The proposed M-TACTDOA reduces the dead node occurrence by optimizing SCH selection process and transmission of data nodes compared to existing methods.

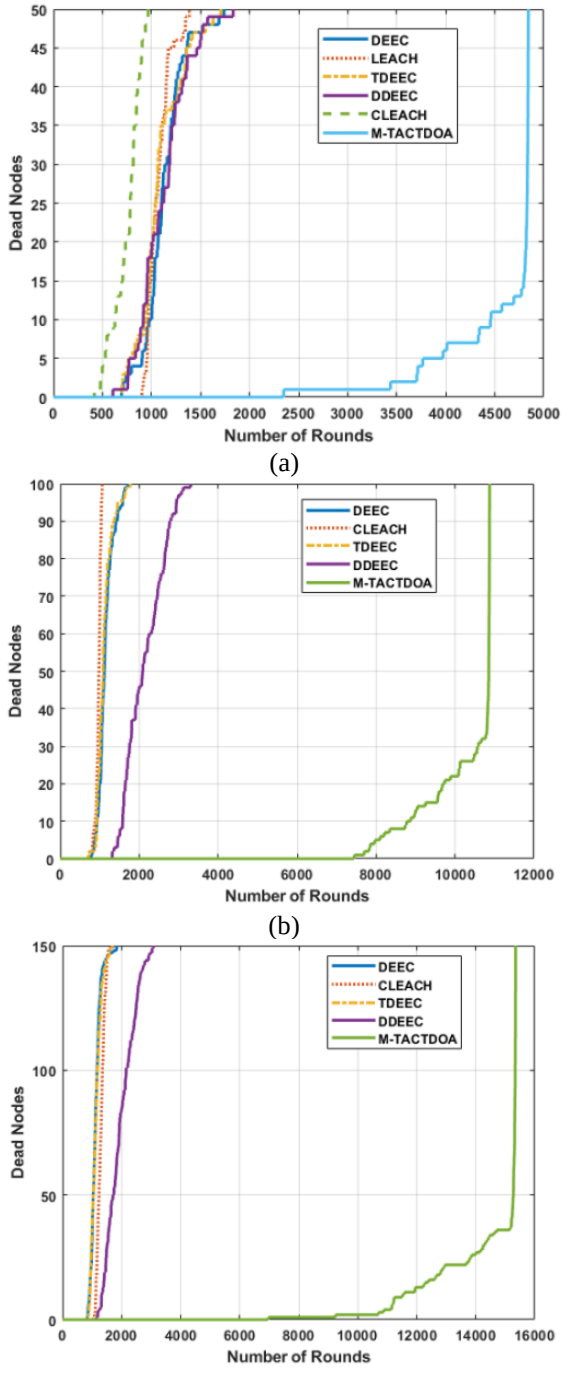
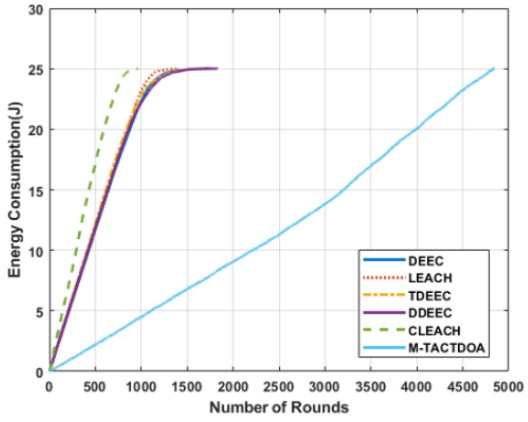
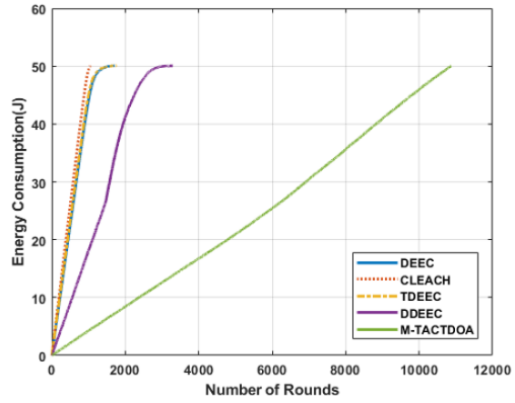


Figure. 5 Performance evaluation of dead nodes: (a) 50 nodes, (b) 100 nodes, and (c) 150 nodes

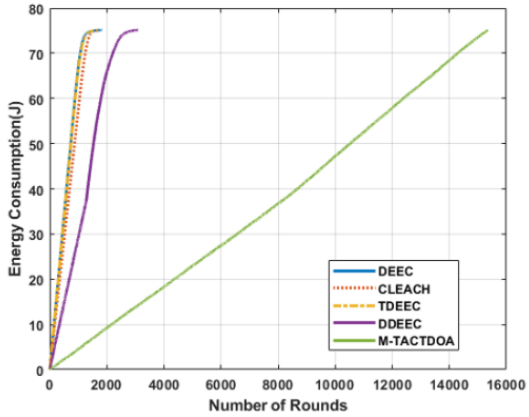
Fig. 6 depicts a performance analysis of energy consumption. Energy consumption is a significant factor because SNs typically have limited battery life. Optimizing energy consumption is crucial to extend the network lifespan and ensure a sustainable process. Compared to LEACH, CLEACH, DEEC, DDEEC, and TDEEC, the proposed M-TACTDOA obtains less energy consumption due to selecting SCH and routing paths by analyzing paths and nodes depending on energy efficiency.



(a)

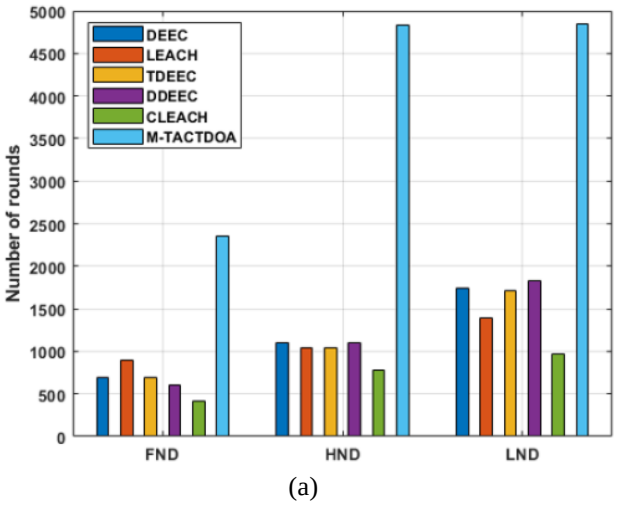


(b)

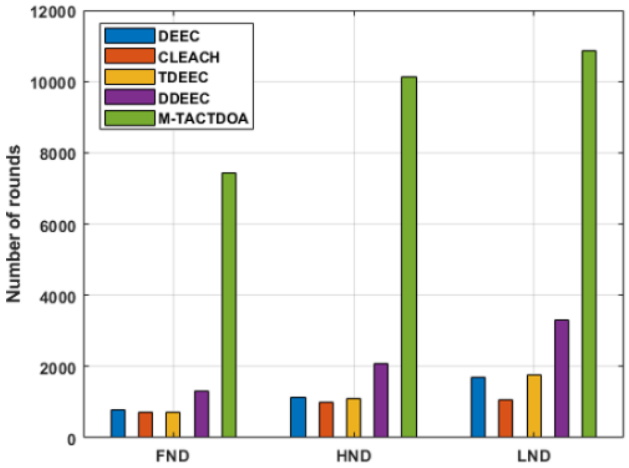


(c)

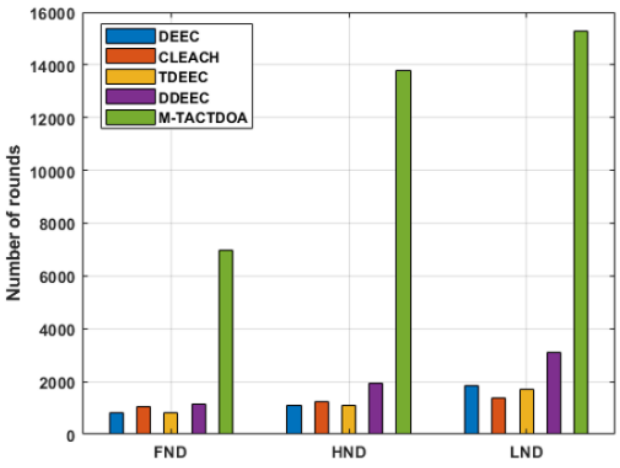
Figure. 6 Performance analysis of energy consumption: (a) 50 nodes, (b) 100 nodes, and (c) 150 nodes



(a)



(b)



(c)

Figure. 7 Performance analysis of FND, HND, and LND: (a) 50 nodes, (b) 100 nodes, and (c) 150 nodes

Fig. 7 represents the performance evaluation of First Node Dead (FND), Last Node Dead (LND), and Half Node Dead (HND). FND refers to time while the

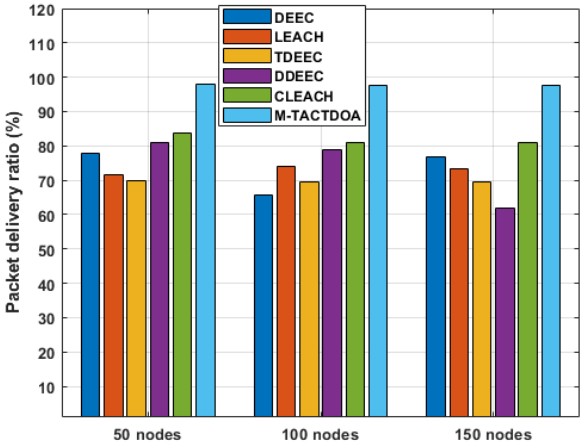


Figure. 8 Performance analysis of PDR

initial SN runs out of energy, LND defines that when the last node depletes its energy leads to complete network failure. HND represents when half of the network nodes are dead which results in network robustness and lifetime. The proposed M-TACTDOA obtains a better performance due to its increased ability to balance the consumption of energy between nodes and SCH selection which leads to enhanced network lifetime and stability.

Fig. 8 determines the Packet Delivery Ratio (PDR). PDR refers to the ratio of successfully received packets of data to the overall sent packets from a source to a destination. When compared to existing methods, the M-TACTDOA attains a high PDR for 50 nodes because most of the transferred data packets reach their destination effectively which results in a strong and stable network signal.

Fig. 9 illustrates a performance evaluation of the Packet Loss Ratio (PLR). PLR measures the percentage of data packets that are dropped or lost during transmission. The proposed M-TACTDOA obtains a lower PLR because of reliable hardware and optimized transmission strategies which contribute to fewer packet drops compared to existing methods.

Fig. 10 depicts a performance analysis of throughput. It refers to the rate at which successfully delivered data packets are transmitted across the network. The proposed M-TACTDOA obtains a high performance because of extending the network time resulting in better transmission of data compared to CLEACH, TDEEC, LEACH, DEEC, and DDEEC.

4.2 Comparative Analysis

Table 2 indicates a different scenario performance. The TAGA [19] is for scenario 1, Taylor C-SSA [22] is for scenario 2, and EOR-iABC [23] is for scenario 3. Tables 3, 4, and 5 represent a comparative analysis of M-TACTDOA with TAGA [19], Taylor C-SSA [22], and EOR-iABC [23]. The results demonstrate that M-TACTDOA obtains a better performance compared to existing methods. For instance, the proposed M-TACTDOA achieves a lower energy consumption of 0.08 J compared to [23] because of balancing energy efficiency and security effectively through multi-objective functions, SCH, and routing path.

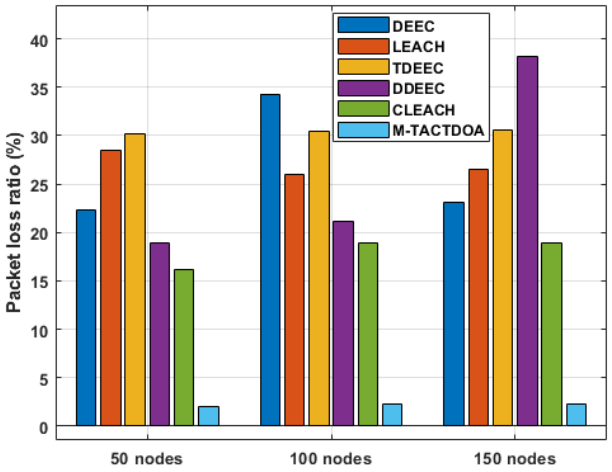


Figure. 9 Performance evaluation of PLR

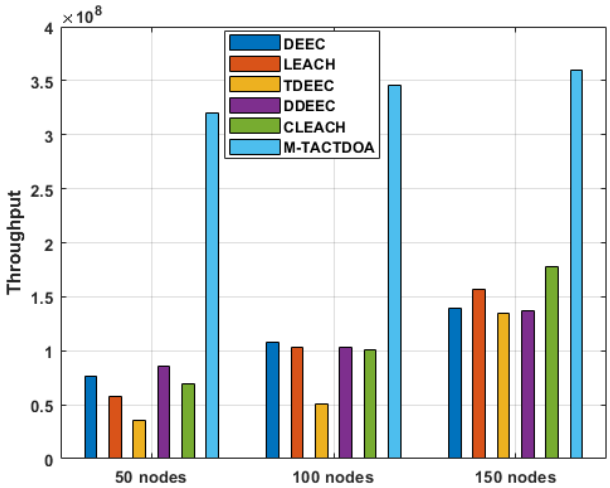


Figure. 10 Performance analysis of throughput

Table 2. Different scenario performance

Parameters	Scenarios		
	1	2	3
Number of nodes	100	50, 100	100
Area / Network size	$100m \times 100m$	$100 \times 100m$	$1200 \times 1200mts$
Energy	1J	0.5 J	50 J

Table 3. Comparative analysis of M-TACTDOA with TAGA

Method	Performance measures	No. of. nodes	No. of. rounds				
			200	400	600	800	1000
TAGA [19]	Energy consumption (J)	100	18.2	38.5	64.2	75.6	95.8
Proposed M-TACTDOA			2.20	4.45	6.37	8.90	11.15

Table 4. Comparative analysis of M-TACTDOA with Taylor C-SSA

Method	Performance measures	Number of nodes	Number of rounds
			2000
Taylor C-SSA [22]	No. of. Alive nodes	50	25
		100	42
	Energy consumption (J)	50	0.188
		100	0.129
	Delay m/s	50	0.291
		100	0.465
	Throughput rate	50	0.1
		100	0.1
Proposed M-TACTDOA	No. of. Alive nodes	50	36
		100	97
	Energy consumption (J)	50	0.15
		100	0.10
	Delay m/s	50	0.205
		100	0.4011
	Throughput rate	50	1.45
		100	1.48

Table 5. Comparative analysis of M-TACTDOA with EOR-iABC

Method	Performance measures	No. of. nodes	No. of. rounds				
			10	20	30	40	50
EOR-iABC [23]	No. of. Alive nodes	100	100	85	68	52	30
	Delay m/s		0.189	0.165	0.142	0.127	0.103
	Energy consumption (J)		9.2	12.7	14.3	15.4	17.3
Proposed M-TACTDOA	No. of. Alive nodes		100	100	100	100	100
	Delay m/s		0.002	0.004	0.006	0.008	0.010
	Energy consumption (J)		0.08	0.180	0.288	0.390	0.513

4.3 Discussion

The advantages of proposed M-TACTDOA and disadvantages of existing techniques are discussed. The disadvantage of existing techniques like TAGA [19] had difficulties in adapt to dynamic network conditions due to adaptation and re-evaluations that results in inefficiency and instability performance. Taylor C-SSA [22] struggled with adapting to dynamic network topologies in WSN which comprises the security by exposing vulnerabilities during routing updates. EOR-iABC [23] had minimum convergence because of suboptimal solution prior discovering the search space that resulted in suboptimal energy distribution. The proposed M-TACTDOA overcomes this existing method limitation. The M-TACTDOA effectively balances multiple objectives like decreasing energy consumption and managing high trustworthiness in communication. The M-TACTDOA's cosine-based searching abilities increase exploitation and exploration which results in better solution accuracy and convergence rates. By integrating trust awareness, M-TACTDOA ensures secure communication by choosing reliable SN which enhances overall network performance and flexibility against malicious attacks.

5. Conclusion

In this research, the M-TACTDOA is proposed for energy efficient SCH and secure route path selection in WSN. In TDOA algorithm, the CPDE mechanism is incorporated which solves the local optima issue and enhances convergence speed in the later iterations. In SCH, the distance between neighbor nodes, the distance between BS and CH, the location factor, node degree, and trust metrics are used to determine the fitness function. This

comprehensive algorithm ensures optimal cluster formation to enhance security. Energy, node degree, and distance are used in secure routing path selection which balances the network durability with reliable transmission of data which leads to effective, secure, and robust performance. By processing this function, the M-TACTDOA achieves a less energy consumption of 0.08 J compared to existing methods like EOR-iABC. In the future, an advanced optimization algorithm will be considered to enhance the model performance.

Notation Description

Symbols	Description
mp	Multipath fading channel
d_0	Distance is smaller than threshold value
f_s	Free space
E_{elec}	Energy consumed by electronic circuits during transmission
ε_{fs}	Energy expenditure per unit distance
ε_{mp}	Energy associated with multipath fading channel propagation
l	Energy required by radio to transmit l-bit binary message
d	Distance
$E_R(l)$	Energy required by radio for receiving an l-bit message
$\varepsilon_{fs}d^2/\varepsilon_{mp}d^4$	Distance between transmitting and receiving nodes and the appropriate Bit Error Rate (BER|)
n	M-TACTDOA's dimension is equivalent to number of CH
X_i	Solution vector of i^{th} individual in the population
$X_{i,1}, X_{i,2}, \ldots, X_{i,n}$	1^{st}, 2^{nd} up to n^{th} component of solution vector of X_i for the Tasmanian devil algorithm
$x_{i,j}$	Candidate value of i^{th} solution in j^{th} variable
N	Tasmanian devil search
m	Number of variables
F	Objective function vector value
F_i	Obtained value of objective function via i^{th} candidate solution
k	Population as carrion
C_i	Selected carrion by i^{th} Tasmanian devil
X_k	Variable X associated with population k
$x_{i,j}^{new,S1}$	New location of i^{th} Tasmanian devil in exploration stage
$F_i^{new,S1}$	Objective function value
Fc_i	Objective function for selected carrion
r	Random numbers in [0, 1] range
I	Random integer number
x_{rdm1} and x_{rdm2}	Two distinct randomly chosen individuals in present iteration
r_{cf}	Randomly produced numbers following cosine-style variation
$x_{i,j}^{new,S1}$	New updated value at (i,j) position in exploitation stage
$x_{top\_T\_devil}$	Reference or target value
$RL_{Slf_{ad}}$	Random learning factor or self-adaptive facto
c	Constant
X	Certain point of data or vector
XCH_i	Feature associated with i^{th} neighboring node
$f(XCH_i)$	Function applied to XCH_i
n	Total number of nodes
B	Set of all neighboring nodes
$d(CH_j, BS)$	Distance between BS and CH
p	Total number of CH
h^T	CH number
ND_{min}	Minimum node degree
CM_i	Overall neighbour of selected CH at node i
$d_{pi,Sink}$	Distance among each node pi and sink node
$d_{ck,Sink}$	Distance among chosen CH ck and sink node
τ_{appx}	Approximate period
τ_{est}	Estimated period for authenticating public keys
ω	Node's opinion parameter
r	Overall node neighbor
DT_i^d	Direct Trust at distance d in i^{th} node
IDT_i^d	Indirect Trust at distance d in i^{th} node
$RT_i^d(\tau)$	Recent Trust at distance d in i^{th} node
$CT_{(i,j)}^n$	Comprehensive Trust in entity ij at n^{th} iteration
N_{nch}	Overall neighboring node
D''_{xdis}	Distance for CH to BS
no	Two ranges
T_{tch}	Total number of CH
E''_{xenr}	Residual energy after determining usage of energy at time

$(E''_{xenr})_n$	Residual energy for a time internal n
$f1$	Distance between neighbor node
$f2$	Distance between BS and CH
$f3$	Node degree
$f4$	Location factor
$f5$	Trust
$f6$	Distance
$f7$	Energy
F	Objective function
$\rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6, \rho_7$	Weighting factor
N_i	Potential function
E_{SCH}	Energy level of SCH

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, methodology, software, formal analysis, resources, data curation, and writing original draft preparation, writing-review, editing, corresponding author: Dharmateja M, and Supervision: Srinivasan R.

References

[1] S. Nasirian, P. Pierleoni, A. Belli, M. Mercuri, and L. Palma, "Pizzza: A Joint Sector Shape and Minimum Spanning Tree-Based Clustering Scheme for Energy Efficient Routing in Wireless Sensor Networks", *IEEE Access*, Vol. 11, pp. 68200-68215, 2023.

[2] M. Wu, Z. Li, J. Chen, Q. Min, and T. Lu, "A dual cluster-head energy-efficient routing algorithm based on canopy optimization and K-means for WSN", *Sensors*, Vol. 22, No. 24, p. 9731, 2022.

[3] G.S. Prashanth, and P. Manjunatha, "Cluster based energy efficient routing protocol for heterogeneous wireless sensor networks", *Concurrency and Computation: Practice and Experience*, Vol. 35, No. 21, p. e7693, 2023.

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

[5] M.U. Farooq, X. Wang, A. Hawbani, A. Khan, A. Ahmed, S. Alsamhi, and B. Qureshi, "POWER: Probabilistic weight-based energy-efficient cluster routing for large-scale wireless sensor networks", *The Journal of Supercomputing*, Vol. 78, pp. 12765-12791, 2022.

[6] Z. Wang, H. Ding, B. Li, L. Bao, Z. Yang, and Q. Liu, "Energy efficient cluster based routing protocol for WSN using firefly algorithm and ant colony optimization", *Wireless Personal Communications*, Vol. 125, No. 3, pp. 2167-2200, 2022.

[7] S. Vijayalakshmi, G. Kavithaa, and N.V. Kousik, "Improving Data Communication of Wireless Sensor Network Using Energy Efficient Adaptive Cluster-Head Selection Algorithm for Secure Routing", *Wireless Personal Communications*, Vol. 128, No. 1, pp. 25-42, 2023.

[8] D. Bhanu, and R. Santhosh, "Fuzzy enhanced location aware secure multicast routing protocol for balancing energy and security in wireless sensor network", *Wireless Networks*, 2023.

[9] M. Selvakumar, and B. Sudhakar, "Energy efficient clustering with secure routing protocol using hybrid evolutionary algorithms for mobile adhoc networks", *Wireless Personal Communications*, Vol. 127, No. 3, pp. 1879-1897, 2022.

[10] K. Biswas, V. Muthukkumarasamy, M.J.M. Chowdhury, X.W. Wu, and K. Singh, "A multipath routing protocol for secure energy efficient communication in Wireless Sensor Networks", *Computer Networks*, Vol. 232, p. 109842, 2023.

[11] M. Selvi, G. Kalaiarasi, S.C. Mana, R. Yogitha, and R. Padmavathy, "Energy and Security Aware Hybrid Optimal Cluster-based Routing in Wireless Sensor Network", *Wireless Personal Communications*, Vol. 137, No. 3, pp. 1395-1422, 2024.

[12] 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.

[13] V. Narayan, A.K. Daniel, and P. Chaturvedi, "E-FEERP: Enhanced fuzzy based energy efficient routing protocol for wireless sensor network", *Wireless Personal Communications*, Vol. 131, No. 1, pp. 371-398, 2023.

[14] N. Kumar, P. Rani, V. Kumar, S.V. Athawale, and D. Koundal, "THWSN: Enhanced energy-efficient clustering approach for three-tier heterogeneous wireless sensor networks", *IEEE Sensors Journal*, Vol. 22, No. 20, pp. 20053-20062, 2022.

[15] G. Thahniyath, and M. Jayaprasad, "Secure and load balanced routing model for wireless sensor

networks", *Journal of King Saud University-Computer and Information Sciences*, Vol. 34, No. 7, pp. 4209-4218, 2022.

[16] I. Adumbabu, and K. Selvakumar, "Energy efficient routing and dynamic cluster head selection using enhanced optimization algorithms for wireless sensor networks", *Energies*, Vol. 15, No. 21, p. 8016, 2022.

[17] S. Hao, Y. Hong, and Y. He, "An energy-efficient routing algorithm based on greedy strategy for energy harvesting wireless sensor networks", *Sensors*, Vol. 22, No. 4, p. 1645, 2022.

[18] M. Bilal, E.U. Munir, and F.K. Alarfaj, "Hybrid clustering and routing algorithm with threshold-based data collection for heterogeneous wireless sensor networks", *Sensors*, Vol. 22, No. 15, p. 5471, 2022.

[19] 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.

[20] R.F. Mansour, S.A. Alsuhibany, S. Abdel-Khalek, R. Alharbi, T. Vaiyapuri, A.J. Obaid, and D. Gupta, "Energy aware fault tolerant clustering with routing protocol for improved survivability in wireless sensor networks", *Computer Networks*, Vol. 212, p. 109049, 2022.

[21] S.V.K. Reddy, and J.K. Murthy, "Secure Cluster based Routing Using Multiobjective Trust Centric Reptile Search Algorithm for WSN", *International Journal of Intelligent Engineering & Systems*, Vol. 16, No. 2, pp. 526-535, 2023, doi: 10.22266/ijies2023.0430.43.

[22] 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.

[23] 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.

[24] M. Dehghani, Š. Hubálovský, and P. Trojovský, "Tasmanian devil optimization: a new bio-inspired optimization algorithm for solving optimization algorithm", *IEEE Access*, Vol. 10, pp. 19599-19620, 2022.