IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 6, December 2026, pp. 5312~5328
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i6.pp5312-5328

Trust-aware multi-objective control parameter-based bobcat optimization algorithm for wireless sensor networks routing

Sowmyashree Malligehalli Shivakumaraswamy[1], Saritha Ibakkanavar Guddappa[1], Seema Swamy Gowda[2]
[1]Department of Electronics and Communication Engineering, B. M. S. Institute of Technology and Management, Bengaluru, India
[2]Department of Electronics and Communication Engineering, Sir M. Visvesvaraya Institute of Technology, Bengaluru, India

Article Info

Article history:

Received Oct 8, 2025
Revised Aug 5, 2026
Accepted Aug 31, 2026

Keywords:

Base station
Cluster head
Clustering and routing
Control parameter-based bobcat optimization algorithm
Load balancing factor
Mean node energy

ABSTRACT

Wireless sensor networks (WSN) have been developed as an essential technology for applications such as healthcare, military surveillance, environmental monitoring, and disaster management. However, traditional clustering and routing methods face challenges, including ineffective cluster head (CH) selection, uneven energy consumption (EC), premature node failures, and vulnerability to malicious attacks that reduce the network lifetime and data reliability. To address these issues, this research proposes a trust-aware multi-objective control parameter-based bobcat optimization algorithm (TMO-CPBOA) for secure clustering and routing of WSN. A proposed TMO-CPBOA integrates adaptive control parameter (CP) with the bobcat optimization algorithm (BOA) to achieve a balanced trade-off among exploration and exploitation, thereby enhancing CH selection and routing efficiency. The fitness function includes distance among sensor nodes (SNs), distance among CH and base station (BS), load balancing factor (LBF), mean node energy (MNE), and trust to find secure and optimal CH and routing paths. The efficiency of the proposed TMO-CPBOA is estimated through metrics, such as alive and dead nodes, EC, packet delivery ratio (PDR), delay, and network lifetime. The network lifetime of TMO-CPBOA is 4,100 rounds over 500 nodes, which outperforms the trust-aware neuro-fuzzy-based sparrow search optimization algorithm (NF-SSOA) for the similar number of nodes.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Sowmyashree Malligehalli Shivakumaraswamy
Department of Electronics and Communication Engineering
B. M. S. Institute of Technology and Management
Bengaluru, Karnataka, India
Email: sowmyashree.m.s@bmsit.in

1. INTRODUCTION

Clustering-based wireless sensor network (WSN) is a new and effective mechanism for arranging massive sensor networks [1]. These sensors are affordable, versatile and are by design resource-constrained. They are capable of gathering, processing, and sharing data between them, and are regularly used in places that humans have no access to sense and monitor the environment [2], [3]. WSNs are essential in computer networking, especially in data collection and search space [4]. They find applications in different fields, including monitoring, data storage, health care, military surveillance, and other industries [5]. A typical WSN is constituted by a base station (BS) and a large number of sensor nodes (SNs) in a given geographical location [6]. When these sensors are used to collect data, they measure temperature, humidity, pressure, vibration, and sound [7]–[9]. The sensed data is relayed to the BS by each node to be aggregated [10]. The

most critical issue with WSN is to maximize network lifetime because primary nodes are usually constrained in sending data to sink nodes [11]. In applications of data collection, each node has sensing and transmitting data packets to the sink node [12]. Clustering is used to overcome this problem by breaking the network into smaller sub-networks, otherwise known as clusters [13]. Every cluster designates a cluster head (CH) through a selection process [14]. The CH plays a central role in the network because it also performs other functions such as data collection, aggregation, transmission, and cluster management [15]. In contrast, cluster members (CM) send data to the CH during certain time slots to conserve energy [16]. Traditional protocols, such as low-energy adaptive clustering hierarchy protocol (LEACH) and its derivatives have proven effective, but still face the issue of CH selection, which remains a critical factor in the performance of cluster-based networks [17], [18]. Furthermore, the information transferred between nodes is very sensitive and vulnerable to numerous attackers [19].

However, security has not been given much consideration in hierarchical cluster networks [20]. Data security at several levels is vital for protecting against attackers. Trust-based security models overcome this by examining and forecasting host behavior based on prior performance [21]. Nodes that behave similarly and predictably receive higher values of trust, thus becoming more secure [22], [23]. However, conventional trust-based models are limited by the fact that they are slow to identify malicious nodes, are inappropriate in protecting against a variety of attacks, and consume too much energy [24]. Most of the existing clustering and routing approaches in WSN optimize energy efficiency (EE) and security against independently, thereby resulting in limited network reliability. The use of randomly tuned control parameters (CPs) in metaheuristic algorithms leads to premature convergence, ineffective CH selection and suboptimal routing paths. The existing trust-based models suffer from higher overhead and delays in identifying malicious nodes thereby leading uneven energy depletion and reduced network lifetime. To overcome these gaps, trust-aware multi-objective control parameter-based bobcat optimization algorithm (TMO-CPBOA) introduces adaptive CPs, multi-objective and trust-aware optimization that improves EE, security and routing in WSN. The major contribution of this research is pointed.

i) The TMO-CPBOA for CH selection is developed using fitness operations such as distance among SNs, distance among CH and BS, load balancing factor (LBF), mean node energy (MNE), and trust. This ensures balanced EC while maintaining secure and reliable clustering in the WSN.
ii) The adaptive CP in the TMO-CPBOA improves a balance among exploration and exploitation, thereby improving network lifetime. By dynamically adjusting the coefficients based on fitness values, the TMO-CPBOA mitigates premature convergence and local optima, thereby achieving an optimal CH and efficient route path selection.
iii) The trust-aware mechanism of TMO-CPBOA estimates node reliability using direct, indirect, and recent trust values, which enhances threat adaptation, isolates malicious nodes, reduces packet loss and enhances overall data integrity in WSN.
iv) The TMO-CPBOA based route selection provides secure multi-hop routing where the residual energy of CH and distance to a BS are considered as a fitness function during path selection. This enhances the EE of a network's lifespan and ensures reliable data transmission under dynamic network conditions.

The rest of the paper is organized as follows. Section 2 analyzes the literature review. The proposed methodology is elaborated in section 3. The results and discussion are presented in section 4. Lastly, conclusion of this research is given in section 5.

2. LITERATURE REVIEW

This section examines existing research on clustering and routing in WSN to achieve secure and reliable data transmission, with its limitations. Dinesh and Kumar [25] developed a trust-aware neuro-fuzzy-based sparrow search optimization algorithm (NF-SSOA) to have secure and efficient clustering and routing of data transmission in WSN. Neuro-fuzzy clustering was used to choose optimal CH, while the sparrow search optimization algorithm (SSOA) was applied to define optimum route path. NF-SSOA used pseudo-random individuality generation as a method of authentication to provide security during transmission. Gowda *et al.* [26] suggested a random differential leader pool strategy with electric eel foraging optimization (RDLPS-EEFO) for CH and routing to enhance EE and network analysis. A fitness for CH selection was energy, distance among CH and BS, distance of neighbor nodes, and node centrality correspondingly. Furthermore, electric eel foraging optimization (EEFO) was utilized for effective data transformation, thereby improving the network lifetime. Wang *et al.* [27] introduced an intelligent clustering and routing protocol for WSN named as intelligent clustering and routing protocol based on quantum-inspired Harris hawk optimizer and deep reinforcement learning (ICR-HHODRL), that integrated quantum-inspired Harris hawk optimizer (QHHO) for clustering and deep reinforcement learning (DRL) to enhance EE and network lifetime. Moreover, ICR-HHODRL utilized dueling double deep Q-network

(D3QN) with priority experience replay (PER) for adaptive learning of routing policies, thereby providing dynamic network situations and improving load balancing.

Jayachandran and Devi [28] designed hybrid EE routing with cluster-based genetic Harris hawk optimization algorithm (EER-CGHHOA) used to select a pathway. EER-CGHHOA was a combination of the genetic algorithm and the Harris hawk optimizer (HHO) that identified EE routes, which minimized the total energy usage and improved network lifetime. The fitness was evaluated and used to select routes, mutation and crossover operations created new routes, preferring to use those with higher residual energy and lower intermediates, and rejecting fewer fit routes. Alshammri [29] presented an improved squirrel search algorithm (I-SSA), which chooses optimal CH selection in WSN. It integrated series enhancement to accelerate convergence and provide solution quality. An enhancement refines ability to provide search space efficiently, thereby leading to effective convergence to optimal solutions. Shivakumaraswamy *et al.* [30] suggested trust-based modified moth flame optimization (T-MMFO) for secure cluster-based routing in WSN. The T-MMFO was applied to choose a secure cluster head (SCH) and route to attain communication, thereby enhancing EE. The secure route path was selected by T-MMFO that minimized packet loss and irrelevant energy consumption (EC), which leads to malicious attacks. The cluster density and traffic rate were applied to improve EE when enhancing network security against malicious attacks.

From the overall analysis, the clustering and routing algorithms in the WSN have the following significant limitations: premature convergence caused by the lack of strong balancing between exploration and exploitation, the inefficient use of energy as it consequently leads to shorter network lifetime, the lack of integrated trust-oriented routing mechanisms to curb malicious behavior, and high overhead in communications that leads to loss and delay in packets. Further, most of the current optimization models are either energy efficient or security conscious, thus undermining the overall network reliability. The TMO-CPBOA is proposed to address these issues as a multi-objective optimization framework that manages exploration and exploitation by tuning the parameters of adaptive control to select optimal CHs and routing paths. Moreover, its trust function increases the strength towards malicious nodes, reduces delay, increases the reliability of packet delivery, and increases the overall network lifetime. Energy-efficient clustering and routing in WSN is challenged in terms of uneven EC through inefficient clustering, high-EC as a result of inter-cluster communication over long distances, and non-optimal routing paths that limit the lifetime of the network.

Additionally, the sensitive information shared between nodes is very susceptible to malicious attacks, and the traditional trust-based models are slow to identify threats, waste a lot of energy and disintegrate in case of multiple attacks. Therefore, a solution combating both EE and trust-based security in clustering and routing is required. The objective of this research is to enhance network lifetime and secure communication in WSN through designing a trust-conscious energy-efficient clustering and routing scheme. The research provides balanced EC by optimal selection of CH, saves on transmission cost by efficient inter-cluster routing and also incorporates trust verification to promptly identify and remove bad nodes. With the ability to be energy-conscious and security-conscious, the strategy enhances the reliability of packet delivery, minimizes the delay of communication, and ensures resilient network operation.

3. PROPOSED METHODOLOGY

This research proposes the TMO-CPBOA as a means for EE and secure clustering and routing at data transmission to BS. The proposed model is divided into different stages: node deployment, CH selection, route selection and cluster formation. To enhance resilience against malicious nodes, both SCH selection and route path determination are performed at the same time as data packet broadcasting. The goal of the TMO-CPBOA is the minimization of EC and transmission delay under secure communication. Figure 1 shows the workflow of TMO-CPBOA for SCH and route selection in WSN.

3.1. System model

In this section, a convention made for a WSN and an EC utilized for this work are defined. First, the CH are chosen and clusters are designed across a network. Information obtained by an individual SN is fused at a corresponding CH and communicated to BS over a multi-hop routing mechanism in the network. Furthermore, an efficient communication is utilized to reduce redundant data transmission and enhance overall network lifetime through balancing EC among SNs and CHs.

3.2. Network model

Subsequent assumptions are taken for WSN:

- Sensors are randomly distributed in a fixed network and are self-contained and have no human intervention and each node has a separate identifier.

- All SNs are isomorphic, which means they have the same communication range, initial energy and computation power. Each sensor has a non-replaceable battery power supply with a limited amount of power.
- All sensors are able to compute their own position and the Euclidean distance [27] metric is utilized to compute inter-node distances. Power is independently optimized for the distance of communication.
- Sensors can be placed anywhere to sense and collect data. If the total energy of a node is consumed, sensor is regarded as dead in the simulation procedure.

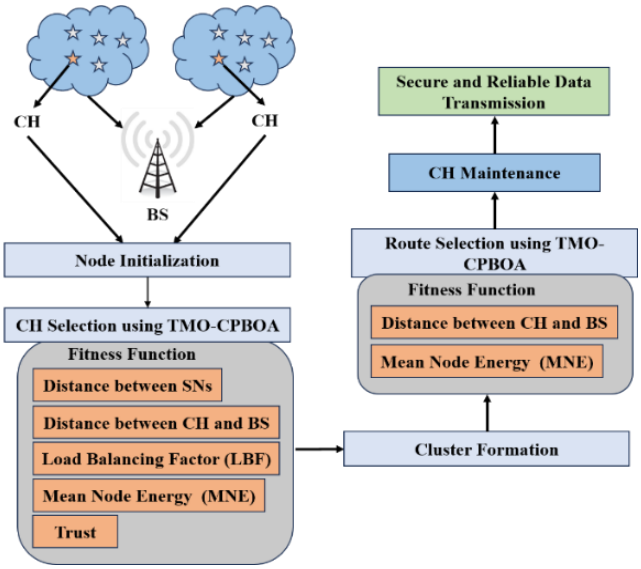


Figure 1. Workflow of the proposed TMO-CPBOA for SCH and route path selection in WSN

3.3. Energy consumption

The EC of the sensors was estimated using a first-order radio model [27]. Based on the distance among sender and receiver, free-space propagation of energy proportional to d^2 and multi-path fading of energy proportional to d^4 are considered. The total energy to transmit a packet of m bits over a distance d is expressed mathematically by (1). Where E_{elec}—energy for transferring per bit, $d_0 = \sqrt{\varepsilon_{fs}/\varepsilon_{mp}}$ denotes a distance threshold, and ε_{fs} and ε_{mp} denote the multipath fading and free-space models, respectively. The energy essential for collecting a bit note m at a distance d is given by (2), and concatenating m is given in (3).

$$E_{TX}(m,d) = \begin{cases} m \times E_{elec} + m \times \varepsilon_{fs} \times d^2, d \leq d_0 \\ m \times E_{elec} + m \times \varepsilon_{mp} \times d^4, d > d_0 \end{cases} \quad (1)$$

$$E_{RX}(m,d) = m \times E_{elec} \quad (2)$$

$$E_{FX}(m,d) = m \times E_{DA} \quad (3)$$

3.4. Secure cluster head selection and routing using TMO-CPBOA

Based on the proposed TMO-CPBOA, the network is divided into several clusters and energy-aware CH selection and routing are provided to reduce EC, delay, and security risks. It maximizes cluster formation and routing while minimizing energy usage, thereby ensuring communication security. As compared with traditional optimization, BOA [31] is strong in dealing with nonlinear and dynamic optimization problems due to its exploration (prey searching) and exploitation (prey chasing) phases. However, BOA suffers from premature convergence and local optima trap, resulting in suboptimal CH and route selection.

To overcome this drawback, TMO-CPBOA is proposed, which uses a CP update strategy in which the random coefficients of the conventional BOA are substituted with adaptive fitness-aware coefficients. This adaptive tuning makes a better trade-off among exploration and exploitation in early iterations, explores the search space in order to prevent premature convergence and reinforces exploitation in later iterations to fine-tune solution. By incorporating trust and multiple performance goals into the fitness function,

TMO-CPBOA improves solution quality, achieves optimal CH selection, balances energy cost among nodes and improves routing reliability. As a result, the method enhances the network lifetime, provides secure data transmission and resilient operation of the WSN.

3.4.1. Node deployment and initialization

First, the SNs are randomly distributed over the network based on network and energy models described in aforementioned section. To ensure reliable communication, every node is initialized with unique identification, residual energy that helps in effective clustering and routing. The best CHs and routing are then found by TMO-CPBOA as explained in the following.

3.4.2. Secure cluster head selection

In this section, a TMO-CPBOA is used to select the best CH from CM and route paths. The algorithm simulates the heuristic optimization characteristics of the bobcat in prey searching and hunting. It is based on three phases: i) initialization, ii) exploration, and iii) exploitation. TMO-CPBOA combines the adaptive CPs and multi-objective fitness evaluation to find the optimal CH and route paths from the CM.

i) Initialization

The BOA is a population-based optimization and acquires optimal solutions for optimization issues through performing an iteration-based search procedure through searching capability of its members in search space. Consequently, in BOA, every bobcat, as a member of population, represents a position in problem-solving space that corresponds to values of decision variables. Thus, location of every bobcat is treated as a candidate solution, that is mathematically represented as a vector, with every vector element representing a decision variable. The initial location of bobcats in problem-solving space is initialized randomly in (4).

$$x_{i,d} = LB_d + r \cdot (UB_d - LB_d) \tag{4}$$

Where, $x_{i,d}$ is candidate solution in search space in dimension d, the r is a random number in interval of $[0, 1]$, LB_d and UB_d are lower and upper bounds of dimension d correspondingly. Computed values of objective function of problem are used as performance indicators to determine the value of every BOA member in producing feasible solutions.

Accordingly, the member whose objective function value is optimal is recognized as the best-performing bobcat and the member whose objective value is the worst-performing bobcat is recognized as the weakest-performing bobcat. Within the BOA framework, the positions of bobcats in problem-solving space are updated at every iteration, which also updates candidate solutions and their objective function values. Hence, in every iteration, it relies on relative evaluation of the objective function values, optimal member from a BOA that is redefined and updated.

ii) Exploration phase

In initial phase of BOA, locations of population members in problem-solving space are changed by simulating the exploration behavior of bobcats while they seek prey. The modelling of bobcats' motion toward prey leads to substantial variations in population members' locations in problem-solving space, thereby increasing exploration capability of BOA to efficiently address global search process. Within BOA framework, for every bobcat position of other members of population with an optimal objective function value is defined as position of prey. Accordingly, candidate prey set of every bobcat is defined by (5).

$$CP_i = \{X_k : F_k < F_i \; and \; k \neq i\}, where \; i = 1,2, \dots, N \; and \; k \in \{1,2, \dots, N\} \tag{5}$$

Where, CP_i is a set of candidate prey location for bobcat i, X_k is a population member with an objective function than bobcat i, F_k is an objective function value. In BOA, every bobcat is expected to randomly pick one prey from the pool of prey and try catching it. In this stage, the CB member moves toward its prey and the position change of a bobcat is modelled using (6) to calculate a new location for every BOA member. If a new position gives a better objective function value according to (7), it replaces the member's previous position.

$$x_{i,j}^{P1} = x_{i,j} + \left(1 - 2r_{i,j}\right) \cdot \left(SP_{i,j} - I_{i,j} x_{i,j}\right) \tag{6}$$

$$X_i = \begin{cases} X_i^{P1}, & F_i^{P1} \leq F_i, \\ X_i, & else \end{cases} \tag{7}$$

Where, $SP_{i,j}$ is a selected prey by bobcat i and dimension j, the $X_{i,j}^{P1}$ is a new position estimated for the bobcat i and dimension j based on exploration phase of BOA, F_i^{P1} is its objective function value, $r_{i,j}$ is a random number from interval of $[0,1]$, the $I_{i,j}$ is a number which is randomly designated as 1 or 2. In traditional BOA, the exploration step is scaled by a random coefficient $r_{i,j}$. Although randomness supports diversity, it lacks adaptivity to the problem landscape. As a result, if the step size is large, it leads to unstable exploration; if it is small, it leads to premature convergence. To address this, this research replaces the $r_{i,j}$ with adaptive step-size parameter $\alpha_{i,j}^t$ as defined by (8).

$$\alpha_{i,j}^t = \begin{cases} 0.001\frac{t}{T}(UB - LB), & k = 1 \\ 0.001\frac{t}{T}\left\| X_s + \frac{a_1}{a_1+a_2}\left[X_b^t(i,j) - X_i^k\right] - X^t(i,j)\right\| + rand, & k \neq 1 \end{cases} \quad (8)$$

Where, $\alpha_{i,j}^t$ is a step size for bobcat i in dimension j at iteration t, the t and T are present and maximum iteration numbers, UB and LB are upper and lower bound of search space, X_s is a location of selected solution, $X_b^t(i,j)$ is an optimal bobcat location in dimension j at iteration t. The X_i^k is a location of bobcat i in the competing population member indexed by k, the $X^t(i,j)$ is the present position of bobcat i in dimension j at iteration t. An a_1 and a_2 are adaptive coefficients controlling the influence of best and competing members, $rand$ is a random value in $[0,1]$ and k is a condition switch deciding which update rule applies.

Through this adaptive modification, weak-performing solutions are encouraged to sample more widely, and stronger solutions focus their search with smaller adjustments. The main advantage of this mechanism is to preserve population diversity to prevent premature convergence and to allow the algorithm to explore a higher search space. In the case of WSN applications, this translates to more reliable CH selection, since multiple candidate nodes are considered before convergence, thus providing balanced energy utilization and protection to malicious attacks.

iii) Exploitation phase

In this phase, the location of population members in a problem-solving space was restructured by simulating the exploitation behavior of a bobcat and its prey at hunting procedure. This pursuit occurs close to the prey's habitat, which eventually allows the bobcat to catch prey. Although this chase-catch phase is brief, simulation of bobcat's movement causes a slight displacement of the population members' position, which enhances the exploitation ability of BOA for improving local search efficiency. Based on modelled bobcat positional changes during this process, a new location is generated for every BOA member closer to the hunting area through (9). If this updated position offers a better objective function value, previous location of respective member is updated by (10).

$$x_{i,j}^{P2} = x_{i,j} + \frac{(1-2r_{i,j})}{1+t} \cdot x_{i,j} \quad (9)$$

$$X_i = \begin{cases} X_i^{P2}, & F_i^{P2} \leq F_i, \\ X_i, & else \end{cases} \quad (10)$$

Where, $X_{i,j}^{P2}$ is a new position estimated for bobcat i and dimension j based on the exploitation phase of BOA, F_i^{P2} is its objective function value, $r_{i,j}$ are random numbers from interval of $[0,1]$ and t is an iteration count. In the traditional BOA, the exploitation phase depends on a random coefficient $r_{i,j}$. As this coefficient is not adaptive, the convergence behavior either aggressive, thereby leading the population to cluster prematurely around a local optimum, if it is weak, it leads to delayed convergence. To overcome this, the $r_{i,j}$ is replaced with an adaptive interaction parameter $\beta_{i,j}^t$ as defined in (11).

$$\beta_{i,j}^t = X_s + \frac{a_3}{a_3+a_2}\left[X_t^1(i,j) - X_i^k\right] - \frac{a_2}{a_3+a_2}\left[X^t(i,j) - X_i^k\right] \quad (11)$$

Where, $\beta_{i,j}^t$is an alternative update value for bobcat i in dimension j at iteration t, the $X_t^1(i,j)$ is a location of first candidate solution in dimension j at iteration t, X_i^k is a competing solution position for bobcat i, the $X^t(i,j)$ is a present position of bobcat i, the a_2 and a_3 are adaptive coefficients balancing exploration and exploitation. In this paper, a fitness-aware interaction factor is defined to adaptively control the attraction toward the global best solution in (11). If the leader's fitness outperforms the current bobcat's fitness by a large amount, the attraction will be correspondingly larger, which will lead to convergence in less time. Conversely, the smaller the fitness gap, the weaker the attraction, which can avoid over-exploitation and

ensure algorithmic stability, thereby producing a smoother and accurate convergence process. In WSN, the above behavior improves route path optimization as the algorithm converges to routing paths that minimize EC, provide trust and increase packet delivery reliability.

3.5. Fitness function

SCH and routing fitness are important to reduce EC and prolong the network lifetime. The fitness function integrates multiple parameters such as residual energy, intra-cluster distance, and distance to the BS to ensure optimal CH selection and effective data transmission. Moreover, security metrics such as trust value and communication reliability are integrated to secure data integrity and prevent malicious node participation during routing. Multi-objective fitness operations applied for SCH and routing are described in detail as follows.

3.5.1. Distance between sensor nodes, distance from cluster head to base station

The distance between SNs and CH (D_{S-CH}) and distance from CH to BS (D_{CH-BS}) are presented in (12) and (13) respectively. The higher the transmission distance of a CH to the BS, the higher the energy needed for the data transmission. Therefore, CHs with shorter transmission distances are significant in WSN. Where, CM_j is a CM of cluster j, the $dis(S_i, CH_j)$ is a distance between ith sensor and jth CH, $dis(CH_i, BS)$ us a distance between ith CH and the destination BS.

$$D_{S-CH} = \sum_{j=1}^{n} \left(\sum_{i=1}^{CM_j} \frac{dis(S_i, CH_j)}{CM_j} \right) \tag{12}$$

$$D_{CH-BS} = \sum_{i=1}^{n} dis(CH_i, BS) \tag{13}$$

3.5.2. Load balancing factor

Because SNs were deployed randomly, there is an increased chance of forming clusters of uneven size—some large, some small. To solve this, an EC balance parameter is introduced as given in (14). An LBF measures the number of local degree differences between clusters [29]. A smaller LBF indicates a more even distribution of SNs between CHs, which results in less communication load on individual CHs. This trade-off ensures that some CHs are not depleted early and energy is distributed evenly across the WSN.

$$LBF = \sum_{j=1}^{m} \frac{n}{m} - l_j \tag{14}$$

3.5.3. Mean node energy

The MNE of SNs is necessary to prevent recurrent selection of the same SNs as CHs. Each SN's energy is sustained or used according to its network role. SNs are considered advanced, super, or normal nodes depending on MNE. Super nodes have the highest energy and are long-term sustainable. Advanced nodes are mid-level among super nodes and normal nodes and have moderate energy, which is crucial to keep the network running. In simulation, based on simulation, two nodes are classified as high-performance (0.6–0.8), superior (0.8–1), and normal (0.5–0.6) using energy normalization to the range [0, 1] based on (15). MNE provides nodes with high energy are designated as CH to improve reliability and network lifetime. The normalization over energy holes classifies the sensors into normal, advanced, and super nodes, which helps to prevent the overloading of weaker nodes to enable suitable CH rotation and to prevent node failure. Where, E_i is the energy utilized by ith sensor and the entire sensor in the cluster is CM.

$$MNE = \frac{1}{CM} \sum_{i=1}^{CM} E_i \tag{15}$$

3.5.4. Trust

Trust evaluation is built in to support security and coordination among nodes, so that misbehaving nodes are quickly identified. In this work, trust is calculated with direct trust (DT), indirect trust (IDT) and recent trust (RT). DT is a ratio of number of packets received to number of packets sent from a source node based on (16). IDT is calculated from DT values by target node as in (17). Thus, RT is calculated through adding DT and IDT, and considering their validity and meaning based on source or destination node, prescribed in (18) and (19).

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

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

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

$$f6 = W_1\, DT_i^d(\tau) + W_2\, IDT_i^d(\tau) + W_3 RT_i^d(\tau) \quad (19)$$

Where, W_1, W_2, and W_3 denote a weight factor of DT, IDT, and RT like that $W_1 + W_2 + W_3 = 1$. The τ_{appx} establishes an approximate time, τ_{est} defines the estimated time to authenticate a public key, r is a total neighbor node, ω is a node's opinion parameters, DT_i^d, RT_i^d, and IDT_i^d evaluate DT, RT, and IDT respectively, at a distance d for node i. Because every fitness function various unit and range, especially distance and location-based fitness metrics, they are normalized through min-max normalization to normalize values between [0, 1], as illustrated in (20).

$$F(x) = \frac{f_i - f_{min}}{f_{max} - f_{min}} \quad (20)$$

Here, f_i is a fitness value, f_{min} and f_{max} are the minimum and maximum fitness value, $F(x)$ is normalized value among $[0, 1]$. After normalization, a final objective value is obtained by a weighted sum calculation that enables every metric to be adjusted according to its significance to a performance of an entire network. The weighted factors of CH selection are denoted as $\gamma_1, \gamma_2, \gamma_3, \gamma_4$, and γ_5 are applied to convert the multiple fitness metrics into one objective function. These weights are given values of 0.25, 0.25, 0.15, 0.15 and 0.2 correspondingly. Therefore, this single function is adopted to choose an optimal CH from CM, which is called CH fitness, estimated by (21). Where, $\sum_{i=1}^{5} \gamma_i = 1,\ \gamma_i \in (0, 1)$ and the $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ and γ_5 are a weight allocated to every fitness function.

$$Fitness = \gamma_1 \times D_{S-CH} + \gamma_2 \times D_{CH-BS} + \gamma_3 \times LBF + \gamma_4 \times MNE + \gamma_5 \times Trust \quad (21)$$

3.6. Cluster formation

After the CH selection with TMO-CPBOA, normal nodes are allocated to their appropriate CH. During this stage, every node estimates the residual energy of nearby CHs before joining the suitable one thereby ensuring balanced cluster sizes and reduced inter-cluster communication cost. Furthermore, dynamic re-clustering is performed to adapt energy depletion and topology variations thereby maintaining stability and prolonged network lifetime. Clusters are created by a potential function in terms of energy and distance constraints as defined in (22).

$$Potential\ Function\ (S) = \frac{E_{CH}}{dis(S,CH)} \quad (22)$$

Data transmission is realized using single-hop transmission for source nodes to a BS, and multi-hop routing is adopted for more remote nodes for balanced utilization of SNs' energy. TMO-CPBOA computes multi-hop routes through its energy and distance-based multi-hop routing mechanism between CHs and the BS. The route discovery in TMO-CPBOA consists of the following steps.

i) A route discovery phase, which is performed by building possible paths relayed from CH to BS, with relay nodes that position is proportional to the number of relays.
ii) The route discovery process consists of an iterative path selection mechanism, which updates the positions of each node along the path according to the route fitness function F defined as (23), which is eventually used to choose the optimal route.

$$F = \delta_1 \times \sum_{i=1}^{n} E_{CH_i} + \delta_2 \times \sum_{i=1}^{n} dis(CH_j, BS) \quad (23)$$

Where, F is a fitness function of route discovery. An early portion of F it is influenced by the CH energy to ensure that the CH is better enough and the latter part takes the CH-BS. Weighted factors such as δ_1 and δ_2 (each with a value of 0.5) are used to even out these two constituents. This means that nodes that don't have enough energy are not used during routing, eliminating packet loss in the network. A main objective of route optimization is to decrease overall EC at data transmission between CH and BS. TMO-CPBOA consider two major factors for consideration, remaining energy of CH and distance of transmission. By preferring routes with CHs with greater residual energy and with shorter transmission distances, TMO-CPBOA avoids premature exhaustion of nodes, thereby obtaining load balancing, which is of major importance in energy-constrained networks.

3.7. Cluster maintenance

Data reliability, effective EC, and network lifetime are important parameters of a WSN. The CH is easily drained of its energy, which can result in failures in the network that is not maintained. The cluster

reformation helps distribute the EC between nodes, and there is no premature connection disconnection. In addition, effective maintenance helps reduce the effect of malicious nodes by reassigning tasks in the case of node failure or node movement, thereby improving the overall network performance. The pseudocode of the proposed TMO-CPBOA for CH selection and secure routing is formally outlined in Algorithm 1.

Algorithm 1. TMO-CPBOA for CH selection and routing
1: Input: Number of populations N, Maximum iterations T, SN positions and energy, fitness functions
2: Output: Optimal CH and secure routing paths.
3: Initialize population of bobcats with random positions using (4).
4: Evaluate fitness of each bobcat using multi-objective fitness function using (21).
5: Identify the best bobcat (global best) and worst bobcat.
6: For $t = 1 \rightarrow Tt = 1$ do
7: For each bobcat $i = 1 \rightarrow N$:
8: Exploration phase:
9: Generate candidate prey set using (5)
10: Update position of bobcat iii using adaptive step size using (6) to (8).
11: If new position improves fitness, update position.
12: Exploitation phase:
13: Update position near prey using adaptive interaction parameter using (9) to (11).
14: If new position improves fitness, update position.
15: Fitness evaluation:
16: Recompute fitness of updated bobcat using normalized multi-objective function using (21).
17: Update global best if current fitness is superior.
18: End For
19: Save current best solution (CH set and routing path).
20: End For
21: Return best CHs and routing path (optimal solution).

4. RESULTS AND DISCUSSION

The simulation results of TMO-CPBOA are presented in this section, where the simulation is performed using MATLAB R2023a with 16 GB RAM, Windows 10 operating system and an Intel i7 processor. MATLAB provides a quick prototype and seamless integration with real-time data, thus being extremely suited to testing optimization-based WSN algorithms, including TMO-CPBOA. The TMO-CPBOA provides the WSN with reliable and trust-conscious data communication. Table 1 provides simulation parameters to evaluate TMO-CPBOA. Among them, node counts are one of the most important parameters that affect network lifetime, alternative node setups are considered to analyze the results.

Table 1. Simulation parameters used for evaluating the proposed TMO-CPBOA in WSN

Parameters	Values
Number of nodes	100
Area	1,500 m × 1,500 m
BS location	130 × 130
Initial energy	0.5 J
SN speed	0.5
Mobility	Random waypoint
Packet size	4,000 bits
E_{elec}	50 nJ/bit/m2
ε_{mp}	0.0013pJ/bit/m2
ε_{fs}	10pJ/bit/m2
Transfer flow	5
Malicious node	5, 10, 15, 20, and 25
Attack	Blackhole attack
Number of iterations	100
Number of populations	30

4.1. Performance analysis

The EC in Figure 2 indicates that the TMO-CPBOA achieves lower EC in comparison to LEACH, distributed energy-efficient clustering (DEEC), threshold distributed energy-efficient clustering (TDEEC), golden jackal optimization (GJO), chicken swarm optimization (CSO), and BOA. The multi-objective nature

of the offered method merges distance metrics, leftover energy metrics and trust metrics to guarantee low and even communication expenses. Conversely, the baseline algorithms demand a higher amount of energy because they cannot select paths efficiently, nor do they perform adaptive balancing. This low consumption with TMO-CPBOA is the direct cause of the prolonged life of the network.

As Figure 3 indicates, the alive nodes of 100 nodes over 1,000 rounds illustrate that the proposed TMO-CPBOA maintains more active nodes throughout the rounds than the baseline models of LEACH, DEEC, TDEEC, GJO, CSO, and BOA. The TMO-CPBOA is trust-conscious and multi-objective, which makes CH selection based on residual energy of the system and the reliability of the nodes, preventing the rapid wear-out of certain nodes. In contrast, the baseline models show a faster decay in alive nodes because of the unequal distribution of energy and the lack of trust analysis. This shows that the TMO-CPBOA balances the workload more efficiently, resulting in longer network operability.

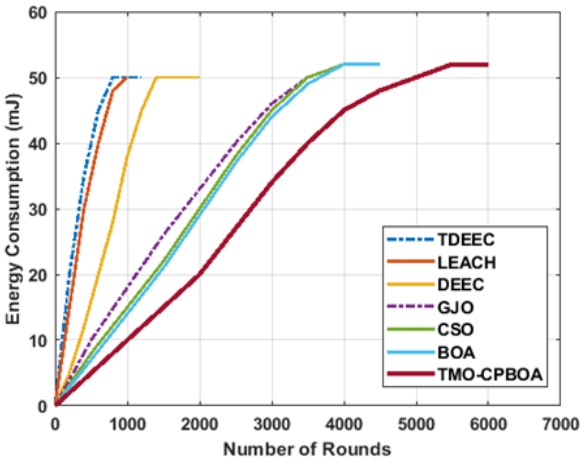


Figure 2. EC analysis of TMO-CPBOA compared with baseline models, showing efficiency in minimizing energy

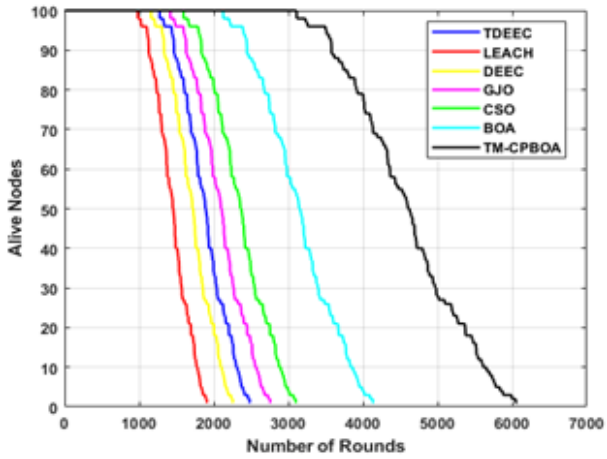


Figure 3. Alive nodes analysis of TMO-CPBOA compared with baseline models, showing prolonged network activity

Figure 4 demonstrates the dead node curve of 100 nodes over 1,000 rounds and it ensures that the TMO-CPBOA is slower than LEACH, DEEC, TDEEC, GJO, CSO, and BOA in terms of delaying the death of a node. The TMO-CPBOA delays the early death of nodes by preventing the aggregation of untrustworthy nodes and distributing communication loads equally, whereas the baseline techniques are characterized by the quick death of nodes because they are unable to prevent overloading some of them. This gradually growing number of dead nodes with TMO-CPBOA justifies its capability of prolonging the life of the entire network. As shown in Figure 5, the delay reveals that the TMO-CPBOA has lower end-to-end latency with

100 nodes simulated in 1,000 rounds than LEACH, DEEC, TDEEC, GJO, CSO, and BOA. The proposed algorithm does not use unreliable paths, as the malicious nodes are filtered off, avoiding retransmission and minimizing queuing delays. Baseline methods are not trust-conscious and lead to choosing unstable paths, thereby increasing delays. The TMO-CPBOA dynamics further ensure that the packets pass through shorter and more consistent paths.

As indicated in the packet delivery ratio (PDR) of Figure 6, it ensures that TMO-CPBOA attains better PDR during 1,000 rounds than the baseline methods with 100 nodes. LEACH, DEEC, and the like are faced with the problem of packet loss due to congestion and malicious behavior, whereas the trust-aware feature of TMO-CPBOA eliminates the problem of packet loss through non-reliable nodes. This is ensured by the mechanism of higher delivery success, and the multi-objective optimization makes the route more stable, which leads to higher communicational reliability. Figure 7 shows that throughput results for 100 nodes over 1,000 rounds indicate that TMO-CPBOA has higher data delivery rates than LEACH, DEEC, TDEEC, GJO, CSO, and BOA. The efficient routing and CH of TMO-CPBOA avoid bottlenecks and realize balanced transmission. The baseline approaches exhibit a decline in performance because of poor EC and retransmission of packets. The adaptive chaotic exploration of TMO-CPBOA ensures that stability is maintained at different loads, which translates into constant and increased throughput.

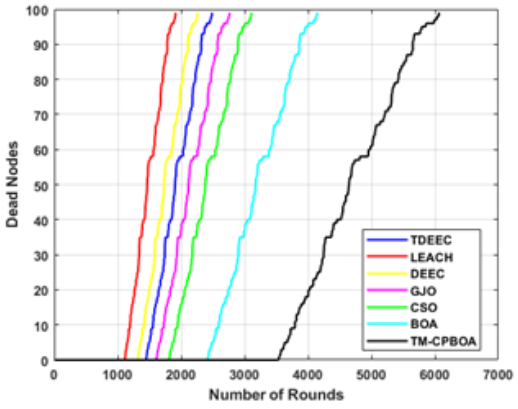


Figure 4. Dead nodes analysis of TMO-CPBOA compared with baseline models, demonstrating delayed node failures

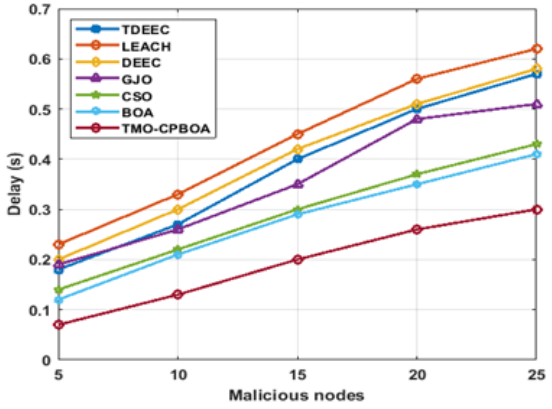


Figure 5. Delay analysis of TMO-CPBOA compared with baseline models, achieving lower latency

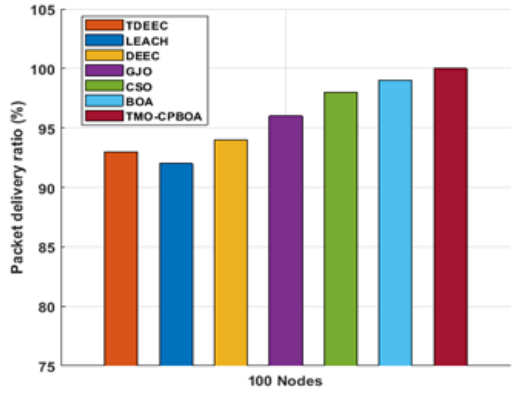


Figure 6. PDR analysis of TMO-CPBOA compared with baseline models, ensuring higher data reliability

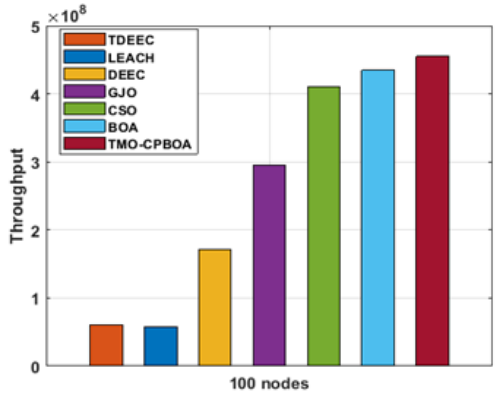


Figure 7. Throughput analysis of TMO-CPBOA compared with baseline models, demonstrating improved data transmission

Figure 8 shows the network lifetime performance of 100 nodes over 1,000 rounds using the TMO-CPBOA, wherein the network life was maintained considerably longer than LEACH, DEEC, TDEEC, GJO, CSO, and BOA. Although the baseline models have the disadvantage of uneven depletion of energy in specific nodes, the TMO-CPBOA ensures fairness in resource utilization because energy, trust, and location

are all considered. This balanced solution enables the network to achieve more rounds of functionality, demonstrating the better performance of the TMO-CPBOA in lifetime extension.

Figure 9 indicates that of the 100 nodes, over 100 iterations of TMO-CPBOA converge to optimal fitness values more quickly and efficiently than the baseline algorithms. LEACH, DEEC, TDEEC, GJO, CSO, and BOA lead to premature convergence or slower stabilization, thereby giving suboptimal solutions. The TMO-CPBOA, introducing chaotic dynamics, has the benefit of searching the search space extensively during the initial iterations and focusing on exploitation. This balanced strategy ensures rapid convergence on high-quality solutions and supports the optimization ability of TMO-CPBOA.

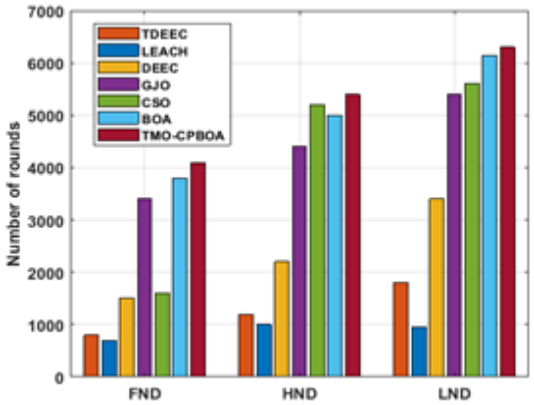


Figure 8. Network lifetime analysis of TMO-CPBOA compared with baseline models, extending operational duration

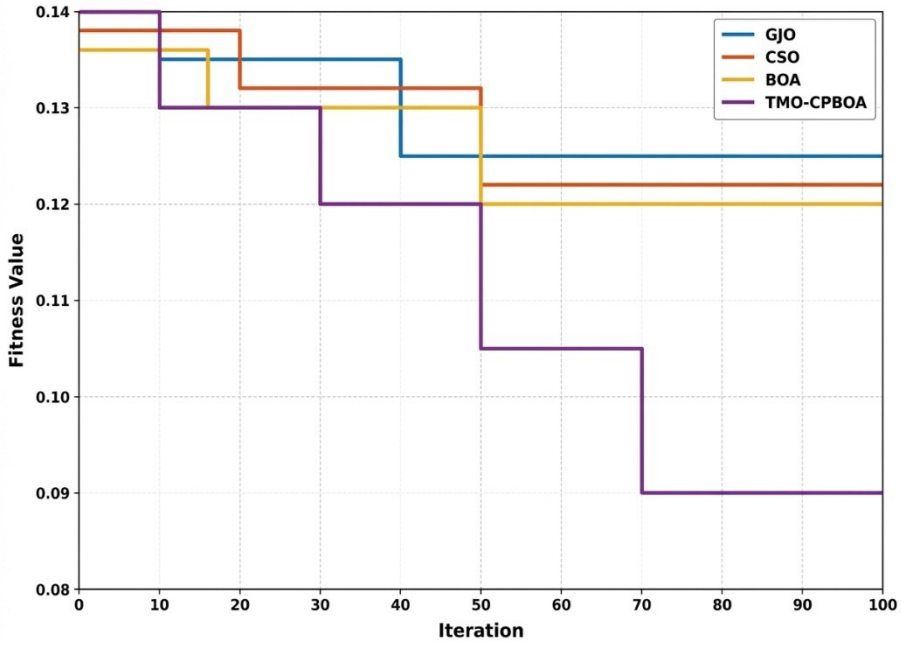


Figure 9. Convergence graph of TMO-CPBOA and baseline models, achieving faster, and stable optimization

4.2. Statistical analysis

A comparative analysis of various optimization algorithms is performed by statistical analysis in terms of non-parametric tests such as Friedman aligned rank and Friedman test. Table 2, the p-value represents probability that the differences in rankings are by chance only and the statistical value is used to quantify the level of difference in performance rankings across algorithms. The statistical value and the p-value were found as 65.3000 and 0.0067 respectively, which is lower than the significance level of 0.05. It

means that TMO-CPBOA performance is statistically significant and cannot have been received by chance. The average rank also ensures that TMO-CPBOA attains better ranking in all simulation metrics, which justifies its superiority over the baseline approaches.

Table 2. Statistical analysis of optimization algorithms using the Friedman test, showing TMO-CPBOA achieves best ranking

Models	Friedman	
	Mean rank	Rank
LEACH	7.25	7
DEEC	6.50	6
TDEEC	5.70	5
GJO	4.80	4
CSO	3.90	3
BOA	2.85	2
TMO-CPBOA	1.20	1
P-value	0.0067	
Statistical value	65.3000	

4.3. Different network size and mobility analysis

The size of the network has a direct effect on the efficiency of communication and EC. The flexibility of the algorithm to the size of the network is discussed by testing the proposed TMO-CPBOA performance at the various deployment areas such as 100 × 100 m^2, 1,000 × 1,000 m^2, and 1,500 × 1,500 m^2. EC, delay, and PDR improve as the deployment area increases, thereby resulting in longer communication distances. The results in Table 3 ensure that TMO-CPBOA has better throughput, and less energy use, and a higher PDR than the baseline techniques, even when deployed on a large scale.

Mobility is a substantial factor that determines the strength of the proposed algorithm. TMO-CPBOA performance is examined at various speeds of mobility, such as 0 m/s, 5 m/s, and 10 m/s with the help of the random waypoint model. With growing mobility, link stability decreases as topology changes frequently, resulting in diminished throughput and PDR and excessively increased delay and EC. Table 4 demonstrates that even under high mobility, TMO-CPBOA is successful in maintaining more alive nodes and providing better reliability when compared to baseline models, thereby indicating its robustness in dynamic environments.

Table 3. Performance evaluation of TMO-CPBOA across different network sizes in terms of efficiency and reliability

Network size (m^2)	EC (mJ)	Alive nodes	Delay (s)	PDR (%)	Throughput
100 × 100	75	95	0.110	97	185
1,000 × 1,000	125	82	0.140	94	165
1,500 × 1,500	190	75	0.165	90	152

Table 4. Performance of varying mobility speeds on TMO-CPBOA performance metrics compared with baseline approaches

Mobility (m/s)	EC (mJ)	Alive nodes	Delay (s)	PDR (%)	Throughput
0 (static)	180	75	0.165	90	152
5	200	70	0.190	88	147
10	230	64	0.220	85	140

4.4. Comparative analysis

The comparative analysis of TMO-CPBOA with existing optimization-based clustering and routing under various simulation conditions is presented in Table 5. The existing methods such as NF-SSOA [25], RDLPS-EEFO [26], and EER-CGHHOA [28] are utilized for a comparison to estimate the efficiency of TMO-CPBOA. To estimate the effectiveness, three scenarios are considered in this research. Among the various scenarios, scenario 1 presents NF-SSOA [25] (Table 6), scenario 2 presents RDLPS-EEFO [26] (Table 7) and scenario 3 presents EER-CGHHOA [28] (Table 8). The comparative results illustrate the superiority of TMO-CPBOA in achieving balanced energy utilization, reduced delay, and enhanced network lifetime.

Table 5. Comparative parameter setup of NF-SSOA, RDLPS-EEFO, and EER-CGHHOA optimization techniques

Parameter	Scenario 1	Scenario 2	Scenario 4
Area	1,000 × 1,000 m^2	100 × 100 m^2	100 × 100 m^2
Initial energy	1 J	0.3 J	0.5 J
Packet size	4096 bits	4000 bits	4000 bits
Number of nodes	500	20	100

Table 6. Scenario 1 comparison of NF-SSOA [25] and proposed TMO-CPBOA across different number of nodes and metrics

Methods	Metrics	Number of nodes				
		100	200	300	400	500
NF-SSOA [25]	EC (mJ)	0.10	0.21	0.27	0.31	0.35
	End-to-end delay (ms)	12	13	13	15	18
	PDR (%)	90	91	91	92	93
	Throughput (Mbps)	95	95	94	94	93
	Network lifetime	1,520	2,000	2,500	3,100	3,900
Proposed TMO-CPBOA	EC (mJ)	0.08	0.18	0.23	0.28	0.32
	End-to-end delay (ms)	10	11	12	13	15
	PDR (%)	93	94	95	96	97
	Throughput (Mbps)	98	98	97	97	96
	Network lifetime	1,700	2,200	2,700	3,300	4,100

Table 7. Scenario 2 comparison of RDLPS-EEFO [26] and proposed TMO-CPBOA across different numbers of rounds and metrics

Methods	Metrics	Number of rounds				
		100	200	300	400	500
RDLPS-EEFO [26]	EC (J)	0.31	0.40	0.32	0.32	0.35
	RE (J)	0.92	0.86	0.79	0.74	0.61
	Throughput (Kbits/sec)	178	165	154	140	120
	PDR (%)	97	98	99	90	94
	Alive nodes	89	84	78	68	61
	End-to-end delay (ms)	120	145	165	97	91
Proposed TMO-CPBOA	EC (J)	0.25	0.34	0.28	0.27	0.30
	RE (J)	0.95	0.90	0.84	0.80	0.68
	Throughput (Kbits/sec)	185	172	160	150	132
	PDR (%)	98	99	99	94	96
	Alive nodes	92	88	83	73	65
	End-to-end delay (ms)	110	130	150	90	85

Table 8. Scenario 3 comparison of EER-CGHHOA [28] and proposed TMO-CPBOA across different numbers of nodes and metrics

Methods	Metrics	Number of nodes				
		200	400	600	800	1,000
EER-CGHHOA [28]	EC (mJ)	143.52	166.09	204	281.04	311.06
	End-to-end delay (s)	0.021	0.029	0.034	0.039	0.045
	PDR (%)	91.28	92.93	94.28	95.72	98.02
Proposed TMO-CPBOA	EC (mJ)	130.20	152.10	190.00	260.00	290.50
	End-to-end delay (s)	0.018	0.026	0.031	0.036	0.041
	PDR (%)	93.50	95.10	96.20	97.00	98.50

4.5. Research implications

The proposed TMO-CPBOA for clustering and routing in WSN has some significant implications, which are discussed.

i) Addressing the dual issue of energy saving and security in WSN: combining trust-awareness and adaptive multi-objective optimization, this approach tackles issues such as uneven EC, premature node failures, and vulnerability to malicious attacks. The use of trust values in the CH selection and routing algorithm is resilient to both blackhole and other malicious node behaviors, whilst at the same time balancing EC. This two-way solution enhances the integrity of data, as well as network lifetime, which are essential in the practical application of WSN.

ii) Increasing the ability to generalize within dynamic settings: TMO-CPBOA has an adaptive CP that strikes the balance between exploration and exploitation. This not only avoids early convergence of optimization, but it also enhances the stability of routing in the face of large-scale networks and dynamic

node mobility. This flexibility illustrates the wider applicability of the method to heterogeneous and dynamic WSN conditions, not just to the simulation-based situation that is not dynamic.

iii) Better WSN operations scalability and strength: statistical and comparative analysis ensures that TMO-CPBOA is effective than the existing methods like LEACH, DEEC, TDEEC, BOA and NF-SSOA regarding their EC, PDR, throughput, delay, and network lifetime. These enhancements indicate that the algorithm can be applied to large scale WSN deployed in sensitive applications, such as healthcare monitoring, disaster management, and military surveillance, where the life cycle and safe data transfer are crucial.

iv) Increased applicability to the future WSN: the research shows the possibility of applying multi-objective trust-aware optimization to other networked systems than the traditional WSN, such as IoT-enabled sensor networks and cyber-physical systems. The proven ability to withstand malicious attacks and securely integrate with mobility suggests that the algorithm can be extended to smart city monitoring, industrial IoT, and intelligent transport systems. Overall, this research contributes to the development of clustering and routing algorithms in WSN, considering energy saving, trust-based security and adaptive optimisation. It is part of the long-term objective of creating sustainable, secure and intelligent sensor networks that can sustain robust operation in highly dynamic and resource-constrained environments.

5. CONCLUSION

In WSN, ensuring both EE and security is challenging because of uneven EC and the presence of malicious nodes. To address these issues, trust-aware and energy-efficient clustering and routing methods provide a better solution. In this work, TMO-CPBOA is proposed for EE clustering WSN. A TMO-CPBOA combines adaptive CP adjustment with multi-objective fitness operations, like distance between SN, distance among CH and BS, LBF, MNE, and trust evaluation to attain optimal CH selection and reliable route selection. Through this process, optimal power usage, safety in clustering, and efficient routing are guaranteed, hence optimal data transfer and network resilience are achieved. The performance of the TMO-CPBOA is supported by simulations, which show that the proposed approach significantly enhances the overall metrics in comparison with the existing methods. Compared to NF-SSOA, the proposed TMO-CPBOA achieves EC of 0.08 mJ, 0.18 mJ, 0.23 mJ, 0.28 mJ and 0.32 mJ for 100, 200, 300, 400, and 500 nodes, respectively. The TMO-CPBOA achieves enhanced EE and security however, the present evaluation is limited to simulation-based experiments. The integration of trust and multi-objective optimization enhances computational overhead that affects scalability in large networks. Additionally, the model assumes homogeneous SNs and considered only limited attack scenarios. In the future, data aggregation techniques can be used to reduce redundant transmissions and enhance communication efficiency among nodes in a WSN network.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Sowmyashree Malligehalli Shivakumaraswamy	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓
Saritha Ibakkanavar Guddappa		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	
Seema SwamyGowda	✓		✓	✓	✓		✓	✓	✓	✓	✓		✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] M. K. Roberts, P. Ramasamy, and F. Dahan, "An innovative approach for cluster head selection and energy optimization in wireless sensor networks using zebra fish and sea horse optimization techniques," *Journal of Industrial Information Integration*, vol. 41, 2024, doi: 10.1016/j.jii.2024.100642.

[2] G. Mahalakshmi, S. Ramalingam, A. Manikandan, and S. Murugesan, "An energy efficient clustering and routing protocol with data fault prediction using hybrid EAAM with BiLSTM-GRU-IDS in wireless sensor networks," *Ain Shams Engineering Journal*, vol. 16, no. 11, 2025, doi: 10.1016/j.asej.2025.103655.

[3] C. Lei, "An energy-aware cluster-based routing in the internet of things using particle swarm optimization algorithm and fuzzy clustering," *Journal of Engineering and Applied Science*, vol. 71, no. 1, 2024, doi: 10.1186/s44147-024-00464-0.

[4] S. S. Babu and N. Geethanjali, "Lifetime improvement of wireless sensor networks by employing trust index optimized cluster head routing (TIOCHR)," *Measurement: Sensors*, vol. 32, 2024, doi: 10.1016/j.measen.2024.101068.

[5] R. M. Bhavadharini, S. Sellamuthu, G. Sudhakaran, and A. A. Elngar, "Fuzzy based energy efficient rider remora routing protocol for secured communication in WSN network," *Sustainable Computing: Informatics and Systems*, vol. 44, 2024, doi: 10.1016/j.suscom.2024.101043.

[6] A. R. Mahadeva, R. H. Ranganathasharma, and Y. A. Chandrashekaraiah, "Secure routing using hybrid sine cosine reptile search and remora optimization algorithm for WSN," *International Journal of Intelligent Engineering and Systems*, vol. 17, no. 5, pp. 76–87, 2024, doi: 10.22266/ijies2024.1031.08.

[7] J. Amutha, S. Sharma, and S. K. Sharma, "An energy efficient cluster based hybrid optimization algorithm with static sink and mobile sink node for wireless sensor networks," *Expert Systems with Applications*, vol. 203, 2022, doi: 10.1016/j.eswa.2022.117334.

[8] M. Manoharan, B. Subramani, and P. Ramu, "An optimal energy efficient routing in WSN using adaptive entropy bald eagle search optimization and density based adaptive soft clustering," *Sustainable Computing: Informatics and Systems*, vol. 43, 2024, doi: 10.1016/j.suscom.2024.101003.

[9] S. Karim, K. N. Qureshi, A. O. Ibrahim, A. W. Abulfaraj, and K. Z. Ghafoor, "Enhanced centroid-based energy-efficient clustering routing protocol for serverless based wireless sensor networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 5, 2024, doi: 10.1016/j.jksuci.2024.102067.

[10] N. D. Tan and V. H. Nguyen, "EE-TLT: energy-efficient routing protocol using two-level tree-based clustering in wireless sensor network," *Journal of Communications and Networks*, vol. 25, no. 6, pp. 734–749, 2023, doi: 10.23919/JCN.2023.000038.

[11] J. K. Jain and D. Chauhan, "Optimized secure and energy-efficient approach for IoT-enabled wireless sensor networks," *Pervasive and Mobile Computing*, vol. 110, 2025, doi: 10.1016/j.pmcj.2025.102049.

[12] S. Kaviarasan and R. Srinivasan, "Developing a novel energy efficient routing protocol in WSN using adaptive remora optimization algorithm," *Expert Systems with Applications*, vol. 244, 2024, doi: 10.1016/j.eswa.2023.122873.

[13] M. Akram *et al.*, "EEMLCR: Energy-efficient machine learning-based clustering and routing for wireless sensor networks," *IEEE Access*, vol. 13, pp. 70849–70871, 2025, doi: 10.1109/ACCESS.2025.3562368.

[14] I. Surenther, K. P. Sridhar, and M. K. Roberts, "Enhancing data transmission efficiency in wireless sensor networks through machine learning-enabled energy optimization: a grouping model approach," *Ain Shams Engineering Journal*, vol. 15, no. 4, 2024, doi: 10.1016/j.asej.2024.102644.

[15] M. K. Roberts, J. Thangavel, and H. Aldawsari, "An improved dual-phased meta-heuristic optimization-based framework for energy efficient cluster-based routing in wireless sensor networks," *Alexandria Engineering Journal*, vol. 101, pp. 306–317, 2024, doi: 10.1016/j.aej.2024.05.078.

[16] L. Yuebo, Y. Haitao, L. Hongyan, and L. Qingxue, "Fuzzy clustering and routing protocol with rules tuned by improved particle swarm optimization for wireless sensor networks," *IEEE Access*, vol. 11, pp. 128784–128800, 2023, doi: 10.1109/ACCESS.2023.3332914.

[17] P. Phalaagae, A. M. Zungeru, B. Sigweni, S. Rajalakshmi, H. Batte, and O. S. Eyobu, "An energy efficient authentication scheme for cluster-based wireless IoT sensor networks," *Scientific African*, vol. 25, 2024, doi: 10.1016/j.sciaf.2024.e02287.

[18] L. K. Ketshabetswe, A. M. Zungeru, C. K. Lebekwe, and B. Mtengi, "A compression-based routing strategy for energy saving in wireless sensor networks," *Results in Engineering*, vol. 23, 2024, doi: 10.1016/j.rineng.2024.102616.

[19] K. Anusha *et al.*, "HOEEACR: hybrid optimized energy-efficient adaptive clustered routing for WSN," *IETE Journal of Research*, vol. 70, no. 7, pp. 6027–6039, 2024, doi: 10.1080/03772063.2023.2298510.

[20] P. Vijayaragavan *et al.*, "FOAEAUC-SARP: a novel energy-efficient protocol integrating unequal clustering and intelligent routing for sustainable wireless sensor networks," *Results in Engineering*, vol. 25, 2025, doi: 10.1016/j.rineng.2024.103806.

[21] B. Suresh and G. S. C. Prasad, "An energy efficient secure routing scheme using LEACH protocol in WSN for IoT networks," *Measurement: Sensors*, vol. 30, 2023, doi: 10.1016/j.measen.2023.100883.

[22] M. F. Tewelgne, S. A. Demilew, and D. W. Girmaw, "Energy efficient inter-cluster multi-hop communication routing protocol for wireless sensor network based on centralized energy efficient clustering routing protocol," *Discover Applied Sciences*, vol. 7, no. 7, 2025, doi: 10.1007/s42452-025-07348-9.

[23] V. B. S. Prasad and H. R. Roopashree, "Energy aware and secure routing for hierarchical cluster through trust evaluation," *Measurement: Sensors*, vol. 33, 2024, doi: 10.1016/j.measen.2024.101132.

[24] X. Chai, Y. Wu, and L. Feng, "Energy-efficient scalable routing algorithm based on hierarchical agglomerative clustering for wireless sensor networks," *Alexandria Engineering Journal*, vol. 120, pp. 95–105, 2025, doi: 10.1016/j.aej.2025.02.018.
[25] K. Dinesh and S. V. N. S. Kumar, "Energy-efficient trust-aware secured neuro-fuzzy clustering with sparrow search optimization in wireless sensor network," *International Journal of Information Security*, vol. 23, no. 1, pp. 199–223, 2024, doi: 10.1007/s10207-023-00737-4.
[26] K. P. Gowda, S. G. Devarajulu, S. Sadashiviah, and B. S. Rajan, "Energy-efficient clustering and routing in wireless sensor network using random differential leader pool strategy with electric eel foraging optimization algorithm," *International Journal of Intelligent Engineering and Systems*, vol. 18, no. 6, pp. 247–263, 2025, doi: 10.22266/ijies2025.0731.16.
[27] C. Wang, H. Hu, and X. Fan, "Intelligent clustering and routing protocol for wireless sensor networks using quantum inspired Harris Hawk optimizer and deep reinforcement learning," *Ad Hoc Networks*, vol. 178, 2025, doi: 10.1016/j.adhoc.2025.103914.
[28] J. Jayachandran and K. V. Devi, "EER-CGHHOA: a hybrid genetic algorithm driven dynamic clustering for energy efficient routing in border surveillance WSNs," *IEEE Access*, vol. 12, pp. 108185–108200, 2024, doi: 10.1109/ACCESS.2024.3438191.
[29] G. H. Alshammri, "Enhancing wireless sensor network lifespan and efficiency through improved cluster head selection using improved squirrel search algorithm," *Artificial Intelligence Review*, vol. 58, no. 3, 2025, doi: 10.1007/s10462-024-11088-4.
[30] S. M. Shivakumaraswamy, S. I. Guddappa, and N. I. Guddappa, "Secure cluster based routing using trust-based modified moth flame optimization algorithm for WSN," *International Journal of Intelligent Engineering and Systems*, vol. 17, no. 4, pp. 16–25, 2024, doi: 10.22266/IJIES2024.0831.02.
[31] Z. Benmamoun, K. Khlie, G. Bektemyssova, M. Dehghani, M. and Y. Gherabi, "Bobcat optimization algorithm: an effective bio-inspired metaheuristic algorithm for solving supply chain optimization problems," *Scientific Reports*, vol. 14, no. 1, 2024, doi: 10.1038/s41598-024-70497-1.

BIOGRAPHIES OF AUTHORS



Sowmyashree Malligehalli Shivakumaraswamy completed B.E. (Electronics and Communication Engineering), from Oxford College of Engineering, Bangalore, and M.Tech. (Electronics and Communication) from SMVIT Bengaluru, and completed Ph.D. (WSN) from Visvesvaraya University, Belagavi. She has 18 years of teaching and 8 years of research experience. At present, working as an associate professor in the Department of Electronics and Communication Engineering, BMS Institute of Technology and Management, Bengaluru. Member for professional bodies, ISTE and IETE. Organized and attended many workshops, Faculty Development Programs (FDPs), and Short-Term Training Programs (STTPs). Guided undergraduate (UG) projects. Published many technical papers in national/international journals/conference. She can be contacted at email: sowmyashree.m.s@bmsit.in.



Saritha Ibakkanavar Guddappa completed B.E (TCE), from MVIT, Bangalore, and M.Tech. (Digital Electronics and Communication) from MSRIT Bengaluru, and completed Ph.D. (Cyber Security) from Visvesvaraya University, Belagavi. She has 19 years of teaching and 9 years of research experience. Currently serving as an associate professor in the Department of Electronics and Communication Engineering at BMS Institute of Technology and Management, Bengaluru. A member of the professional bodies ISTE and IAPURAI, with experience in organizing and attending various workshops, FDPs and STTPs. Has guided UG projects and published numerous technical papers in national and international journals and conference proceedings. She can be contacted at email: pmelin@tectijuana.mx.



Seema Swamy Gowda is currently serving as an associate professor in the Department of Electronics and Communication Engineering at Sir. M. Visvesvaraya Institute of Technology, Yelahanka, Bengaluru, with over 18 years of experience in teaching and research. She holds a B.E. in Electronics and Communication Engineering, an M.Tech. in Digital Electronics, and a Ph.D. in Underwater Wireless Sensor Networks from Visvesvaraya Technological University, Belagavi, Karnataka, India. She has authored and presented over 10 research papers in Scopus-indexed journals and IEEE Xplore. She has been invited as a resource person for numerous workshops and has also served as a reviewer for IEEE conferences. She can be contacted at email: seema_ec@sirmvit.edu.