International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/19 Volume 12, Issue 2, March – April (2025)

RESEARCH ARTICLE

Secretary Bird Optimization with Differential Evolution (SBODE) and Trust Energy Aware Clustering Routing (TREACR) Protocol for Wireless Sensor Network (WSN)

Amsaveni Manigandan
Department of Computer Science, P. K. R Arts College for Women, Gobichettipalayam, Tamil Nadu, India.
✉ amsaveni.confident@gmail.com

M. Saranya
Department of Computer Science, P.K.R. Arts College for Women, Gobichettipalayam, Tamil Nadu, India.
drmsaranyamcapersonal@gmail.com

Received: 16 February 2025 / Revised: 19 April 2025 / Accepted: 26 April 2025 / Published: 30 April 2025

Abstract – In Wireless Sensor Networks (WSNs), nodes with limited battery power transmit data to a Base Station (BS). Ensuring security and Energy Efficiency (EE) is crucial, but traditional protocols lack a balanced approach. This study introduces the Trust Energy Aware Clustering Routing (TREACR) protocol to enhance energy efficiency and secure Data Transmission (DT). TREACR selects Cluster Heads (CHs) using Secretary Bird Optimisation with Differential Evolution (SBODE), extending Network Lifetime (NL) through efficient energy distribution. The SBODE algorithm and fitness measure effectively detect attacks, optimizing CH Election (CHE) based on mobility, latency, energy, trust, and CH distance. The TREACR protocol employs a Dynamic Trust (DT) model to assess node behavior using Wormhole (WH), flooding, Black Hole (BH), Sink Hole (SH), and Grey Hole (GH) probabilities. Evaluation results demonstrate TREACR's effectiveness in improving Packet Delivery Ratio, Packet Loss Rate, NL, Residual Energy (RE), and End-to-End Delay (E2ED).

Index Terms – Wireless Sensor Network, Secretary Bird Optimization, Trust Energy Aware Clustering, Routing, Trust Model, Security, Optimization, Energy Efficiency.

1. INTRODUCTION

Many small, lightweight wireless SNs are placed throughout widely distributed networks known as WSNs to control the environment. Numerous Real-Time (RT) applications can benefit from the well-established study area of WSN [1], [2]. The BS or sink node receives the information collected by the SN after they have detected the environment [3]. The Destination Node (DN) is another name for the sink node. In addition to being a sink node or DN, the SN can also be a source, intermediate, or cluster node [3–4]. Applying EE in various applications is necessary to maintain the network functioning regularly [5]. Thus, the energy constraint in nodes becomes the main obstacle. Therefore, several Cluster-Based (CB) protocols with different features were developed in recent works [6] to address this issue and enhance the network's Quality of Service (QoS).

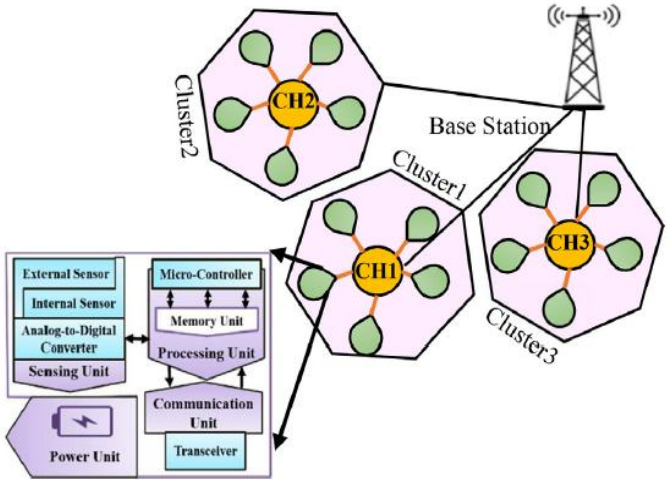

Figure 1 Cluster Formation Architecture

Cluster Members (CM) are the members of a cluster formed by clustering node, as shown in Figure 1. The CH selected by each cluster gathers data and transmits it to the BS. To balance the Energy Consumption (EC) of CH, the CH Selection (CHS) procedure requires proper addressing. If not, the overburden of the Data Collection (DC) and DT procedure could cause them to pass away very soon. In many other methods, CHs are selected initially randomly, but in a small

RESEARCH ARTICLE

area network, they are chosen depending on distance and RE [7].

The data is transmitted to the designated destination after every node has an exclusive address (ID). While dynamic clustering creates a cluster reactively close to the event sensing nodes, static clustering proactively divides the network into clusters. Extensive clustering techniques have been implemented to optimize the CHS and validate the network's dependability for DT. Any meta-heuristic (MH) method not confined to local optima incorporates the solution spaces (SS) with a globally optimal solutions.

The greatest results require a balance between exploration and exploitation [8]. Choose a well-known MH algorithm for the CHS process because the search for the optimal solution has been accomplished. Therefore, intelligent clustering algorithms can lower EC by selecting the best nodes to become CHs or lowering the average distance between the CMs and their respective CHs. MH algorithms and optimization techniques are presented to enhance network performance and create efficient routing decisions [9-10]. Security procedures should be secure against the network's vulnerability to attacks (VoA) due to certain security considerations.

The primary purpose of current methods is to infer network intrusions [11-12]. But, a difficult problem in current research is identifying legitimate and safe SN. Furthermore, attackers frequently relocate to carry out malicious activities throughout the network [13-14]. An essential element of cybersecurity is trust. This component determines the security level of SN during their interactions with one another. In addition to preventing security threats brought on by invasions of privacy, data alteration or deletion, and other cyberattacks, it actively finds trusted nodes. This demonstrates the significance of reliable routing protocols and their necessity.

EC management is crucial for building a Trust Mechanism (TM) because of the unique features of SN, such as their tiny size, restricted memory capacity, constrained energy source, and low computational capability. In WSN, security and EE are two crucial ideas. Therefore, the current Routing Protocols (RP) in WSNs must have robust security features to safeguard the DT process. The TREACR protocol is presented in this study to accomplish EE and security-aware DT. The CH of the TREACR protocol is chosen by SBODE, which extends the NL by conserving the RE through an energy distribution mechanism. Three trust criteria, the WH probability, the flooding probability, and the BH, SH, and GH probabilities, are used in the TREACR protocol's DT model to examine SN behavior.

1.1. Problem Statement

Environmental monitoring, military surveillance, and smart city applications are some of the most important uses of WSNs. Problems with energy consumption, scalability, and security make them underperforming, especially in contexts with limited resources and high levels of change. Due to insufficient energy efficiency and lack of secure data transfer, traditional routing and clustering protocols often cause nodes to fail before their time and shorten the lifespan of networks. A further concern is the increased likelihood of data loss and malicious interference caused by unstable communication channels due to the lack of a reliable way to assess node trustworthiness. It is critical to have a clustering and routing mechanism that is smart, trust-aware, and efficient with energy so that networks can run well and reliably. To overcome these obstacles, this study proposed a hybrid metaheuristic-based routing architecture incorporating energy awareness and trust assessment into data forwarding and cluster creation.

The main contributions of the paper are:

- Introduces a novel combination of Secretary Bird Optimization (SBO) with Differential Evolution (DE) termed SBODE to optimally select energy-efficient and trustworthy cluster heads, balancing exploration and exploitation in dynamic WSN environments.
- The TREACR protocol integrates node trustworthiness and residual energy into routing decisions, ensuring secure and energy-conscious data transmission while mitigating malicious or unreliable nodes.
- Results show significant improvements in network lifetime, packet delivery ratio, and resilience against trust-based attacks compared to conventional protocols through simulation and performance analysis under varying network conditions.

The remaining arrangements are presented in the following order: Section 2 presents a detailed literature review of existing clustering, routing, and trust-aware models for wireless sensor networks. Section 3 presents the proposed Trust Energy Aware Clustering Routing (TREACR) protocol integrated with Secretary Bird Optimization and Differential Evolution (SBODE) for secure and energy-efficient routing. Section 4 presents the simulation results and performance discussion of the proposed method compared to existing models. The conclusion and future work directions are presented in section 5.

2. LITERATURE REVIEW

For the Low Energy Adaptive Clustering Hierarchical-Centralized (LEACH-C) technique and to find the optimal CHS, Pitchaimanickam, and Murugaboopathi [15] developed a hybrid method called Firefly Algorithm (FA) with Particle Swarm Optimisation (HFAPSO). The hybrid method ensures optimal CH location and enhances Firefly's Global Search (GS) behavior through PSO. The number of

RESEARCH ARTICLE

live nodes, RE, and Throughput (T) were utilized to assess the HFAPSO's performance. The outcomes demonstrate how the NL has improved, resulting in more alive nodes and lower EC. It was found that the recommended procedure overtakes the FA by T and RE. However, it ignores energy balance and Trust-Based Routing (TBR).

A novel model for determining the CH and the most effective path in a WSN for Internet of Things (IoT) applications was put forth by Joshi and Raghuvanshi [16]. A Multi-Objective (MO) Rider Optimisation Algorithms (ROA) that considers three objectives, distance, energy, and delay, is used to select the CH, a clustering component. The MO sailfish optimization algorithm (SFO) is utilized to choose effective and ideal route for routing. From the outcomes, the recommended model executes superior in contrast to other similar recent research by execution time, energy depletion, network delay, T, PDR, alive nodes in networks, and the increase in dead nodes. Experiments on a dense sensor network show that, compared to similar MO routing and clustering strategies, the suggested work can reduce EC by 30–40% and delay by 40–60%. It lacks Attack Detection (AD) support and has the highest time complexity.

Kathiroli and Selvadurai [17] suggested an EE CHS by Enhanced Sparrow Search Algorithm with Differential Evolutions (EECHS-ISSADE) to solve the EE problem by CHS in WSN. The suggested approach uses the vivid potential of DE, which extends the lifetime of nodes, and the High-Level (HL) search effectiveness of SSA. This hybrid model's performance uses T, RE, and the number of alive and dead nodes. Compared to previous algorithms, the ISSADE model suggested for selecting the optimal CH exhibits improvements in RE and T. The RP without considering AD into account.

To minimize the rate of EC and increase the NL in a WSN, Ramalingam et al. [18] presented the EECHS-Artificial Rabbits Optimisation (EECHS-ARO) technique. While choosing the best CHs, the EECHS-ARO approach strikes an equilibrium between enriched exploration and exploitation during the search process. A Matrix Laboratory 2021 (MATLAB 2021a) platform with different SN was used for the experiment.

A new cluster RP for WSN was presented by Yang et al. [19]. To prolong the method's lifespan and save network energy, the system uses the Minimum Spanning Trees (MST) algorithm for inter-cluster routing and the multi-policy fusion snake optimizers (MSSO) to choose CHs and relay nodes. This article presents strategies that use adaptive alpha mutations, bi-directional search optimization, and dynamic parameter updates in MSSO to find the best clustering scheme. These methods broaden the accessible search space and dramatically speed up algorithm convergence. Additionally, a brand-new, effective clustering routing model for WSN is introduced. Considering variables like location, energy, BS distance, inter-cluster separation, intra-cluster compactness, and other pertinent criteria, the model produces various Objective Functions (OF) for choosing CHs and relay nodes. The Fuzzy C-Means (FCM) method is incorporated into MSSO to enhance the algorithm's optimization performance when choosing CHs. Based on distance, RE, and direction, the relay node chooses the next hop node when inter-cluster routing is planned.

A new trust-based safe and EE RP (TBSEER) for WSN was suggested by Hu et al. [20]. With adaptive direct (TV) trust value, indirect TV, and energy TV, TBSEER determines the complete TV. Hello flood, SH, BH, and selective forwarding attacks do not affect TBSEER. The volatilization factor and adaptive penalty mechanism are used to detect malicious nodes (MN) quickly. To minimize the EC brought on by repetitive computations, the nodes are only necessary to compute the direct TV; the Sink determines the indirect TV. Lastly, the CHs actively prevent WH attacks by determining the benign Multi-Hop Route (MHR) depending on the complete TV. The suggested TBSEER resists all typical attacks, lowers network EC, and expedites the detection of MN. It was demonstrated in the simulation outcomes. Based on the TV of CH in WSN, CH has been selected.

Kavitha and Ananthakumaran [21] suggested the effective Enhanced Fuzzy C means and Adaptive time division multiple access Scheduling (ECATS) technique to improve network communication. For the Mobile Sink (MS) to receive Data Packets (DP) on time. CH selection is based on energy used to control the data aggregation (DA) among several WSN nodes. A hybridization of Time Division Multiple Access based ALO scheduling is presented to select the best CH and improve EE. PDR, T, minimum EC, communication overhead, and E2ED are the WSN performance characteristics optimized by the ECATS technique. Neither defining a routing strategy between CHs nor assessing this method's resilience to different types of attacks.

Rathee et al. [22] suggested the ACO-based QoS aware energy balancing secure routing (QEBSR) method for WSN. The trust factors of the nodes on the routing paths and the end-to-end (E2E) transmission delay are computed using improved heuristics. Two current algorithms contrast the suggested method: distributed energy-balanced routing and EE routing with node-compromised resistances. Regarding performance, the QEBSR algorithm executes superiorly to the other two methods. Certain situations make determining weight vectors impossible or extremely challenging, making it impossible to assess how resistant this scheme is to different attacks and requiring much time.

A trust-aware optimized compressed sensing-based DA and routing algorithms for clustered WSNs was suggested by Gilbert et al. [23]. DA from SN with lower overhead is

RESEARCH ARTICLE

accomplished by compressed sensing. Utilizing the Artificial Bee Colony (ABC) algorithm, ACO, DE, FA, and Particle Swarm Optimisation (PSO), Nature-Inspired Optimization (NIO) has been used to achieve a trade-off between transmission distance, hop counts (HC), number of transmitted messages, and most trusted paths.

To gather data from faultless nodes, Saleh et al. [24] presented the Trust-Aware Routing Mechanism (TARM), which makes use of an edge node (EN) with mobility features. The EN uses a trust evaluation mechanism to separate anomalous and faulty nodes from normal ones. TARM forms the clusters from the deployed SN using a modified version of Grey Wolf Optimisation (GWO). Following the clusters' formation, each cluster's TV is determined, and the EN begins gathering data solely from trusted nodes over the analogous CH. The ABC algorithm carries out the most optimal routing path between the reliable and mobile edge nodes. It is time-consuming and does not assess how resistant this method is to various attacks.

A clustering approach with a trust model that uses energy and data trust to identify untrusted nodes has been suggested by Hriez et al. [25]. Additionally, the suggested clustering methodology extends the NL by utilizing the positive aspects of stochastic fractal search optimization. A new Fitness Function (FF) is finally offered to select the CH from the trusted nodes. The subsequent four variables form the basis of the function: 1) the nodes' RE; 2) their density; 3) the separation among each nodes and the BS; and 4) the energy the network dissipates. It ignores QoS limitations and falls into the local minimum.

In WSN, a cluster-tree-based trusted routing technique named CTTRG, which uses the grasshopper optimization algorithm (GOA), has been suggested by Hosseinzadeh et al. [26]. Three trust criteria, the WH probability, the flooding probability, and the BH, SH, and GH probabilities, are used to analyze the behavior of SN using the distributed time-variant trust (TVT) model.

Additionally, to create robust and secure communication channels among SN and BS, GOA-based trustworthy routing trees (GTRT) are introduced. Three parameters, the energy of CHs, the trust level, and the distance amongst CH and their parent nodes are used to create an MO FF to assess each GTRT. The evaluation findings regarding MN detection speed, PLR, and E2ED demonstrate that CTTRG performs appropriately and effectively.

Venkatesan Cherappa et al. [27] suggested the Adaptive Sailfish Optimization (ASFO) and a Cross-Layer-Based Expedient Routing Protocols for WSN. Through energy stabilization, distance reduction, and latency minimization between nodes, the major goal of the research is to improve the selection of cluster heads. Due to these limitations, the optimal usage of energy resources is a critical issue in WSNs. The quickest path is determined using energy-efficient cross-layer-based expedient routing protocols (E-CERP), which dynamically minimizes network overheads. Compared to previous methodologies, the suggested approach outperformed them while testing packet delivery ratios (PDRs), packet delays, throughputs, power consumption, network lifetimes, packet loss rates, and error estimations.

Roberts and Ramasamy [28] proposed enhanced high-performance clustering-based routing protocols for WSNs in IoT. This study proposes an upgraded, dependable, cluster-based, energy-efficient, high-performance, secure routing architecture. This protocol's standout feature is its attention to energy efficiency, congestion control, encrypted data transport, and attacker node monitoring, all of which contribute to better data management. When wireless sensor nodes have network isolation and segmentation issues, they may become inoperable and unable to communicate with the base station.

S. Ramalingam et al. [29] recommended the improved elephant herd optimization algorithm for Performance improvement of effective clustering and routing protocols for WSN. After applying the proposed hybrid method in MATLAB, the outcomes were compared to those of four popular approaches: IABC-C, GA, PSO, and the HCCHE method for hierarchical clustering-based hillside optimization.

Performance parameters, including energy utilization, end-to-end latency, packet delivery ratio, network lifespan, and buffer occupancy, are enhanced by the Fuzzy with ASFO approach, which increases the Quality of Service (QoS). In comparison to the current techniques (PSO, GA, IABC-C, and HCCHE algorithms), the proposed Fuzzy with SFO has superior packet delivery ratio (99.8%), packet delay (1.12 s), throughput (98 bps), energy use (10.90 mJ), network lifespan (5400 cycles), and packet loss ratio (0.6%).

Huangshui Hu et al. [30] discussed the quantum particle swarm optimization (PSO) and fuzzy logic (QPSOFL) for WSN for energy-efficient clustering and routing protocols. During initialization, QPSOFL utilizes Sobol sequences for population diversification and an improved quantum PSO method to choose the best cluster heads. It also uses location updates based on Gaussian perturbations and Lévy fights to avoid local optima trapping. The effectiveness of QPSOFL has been confirmed by benchmark studies comparing it to other popular methods in the optimization space, emphasizing accuracy, search capacity, and convergence time. These methods include Grey Wolf Optimization (GWO), Quantum PSO (QPSO), and PSO. A fuzzy logic system in QPSOFL uses characteristics like energy deviation, relay distance, and residual energy to find the optimal next-hop cluster head. Table 1 shows the summary of the existing models.

RESEARCH ARTICLE

Table 1 Summary of Existing Models

Ref. No.	Author(s)	Methodology	Results	Limitations
[15]	Pitchaimanickam & Murugaboopathi	Hybrid FA with PSO (HFAPSO) for LEACH-C	Improved number of live nodes, residual energy (RE), and throughput (T); outperformed standalone FA in T and RE.	Does not address energy balance and lacks Trust-Based Routing (TBR).
[16]	Joshi & Raghuvanshi	Multi-Objective Rider Optimization Algorithm (ROA) for CH selection; Sailfish Optimization (SFO) for routing	Reduced energy consumption by 30–40% and delay by 40–60%; enhanced performance in execution period, energy depletion, packet delivery ratio (PDR), network delay, throughput, and alive nodes.	High time complexity; lacks Attack Detection (AD) support.
[17]	Kathiroli & Selvadurai	Energy-Efficient CH Selection using Enhanced Sparrow Search Algorithm with Differential Evolution (EECHS-ISSADE)	Enhanced residual energy and throughput; extended node lifetime.	Does not consider Attack Detection (AD).
[18]	Ramalingam et al.	Energy-Efficient CH Selection using Artificial Rabbits Optimization (EECHS-ARO)	Balanced exploration and exploitation; improved performance over TLBO, ALO, and QOBOA in energy consumption and network lifetime.	Less size dataset
[19]	Yang et al.	Multi-Strategy Fusion Snake Optimizer (MSSO) with Minimum Spanning Tree (MST) and Fuzzy C-Means (FCM) for clustering	Accelerated convergence; improved CH selection and routing; enhanced energy efficiency and network lifespan.	Low Energy Efficiency
[20]	Hu et al.	Trust-Based Secure and Energy-Efficient Routing (TBSEER) with adaptive trust evaluation and penalty mechanisms	Resisted common attacks; reduced energy consumption; expedited malicious node detection.	Fewer Data size for attack prediction
[21]	Kavitha & Ananthakumaran	Improved Fuzzy C-Means and Adaptive TDMA Scheduling (ECATS) with Neural Elliptic Galois (NEG) cryptography	Improved packet delivery rate, throughput, reduced energy consumption, communication overhead, and delay.	Does not define routing strategy between CHs; lacks assessment against various attack types.
[22]	Rathee et al.	ACO-based QoS-aware Energy Balancing Secure Routing (QEBSR)	Superior performance in energy balancing and secure routing compared to existing methods.	Difficulty in determining weight vectors; lacks comprehensive attack resistance assessment.
[23]	Gilbert et al.	Trust-aware optimized compressed sensing-based data aggregation and routing using various Nature-Inspired Optimization.	Achieved trade-off between hop count, transmission distance, number of messages, and trust; effective compressed data reconstruction at the base station.	Does not consider energy parameters in routing decisions.

RESEARCH ARTICLE

[24]	Saleh et al.	Trust-aware routing Mechanism (TARM) using mobile edge nodes and modified Grey Wolf Optimization (GWO)	Efficient data collection from trusted nodes; optimal routing paths established.	Time-consuming; lacks assessment against various attack types.
[25]	Hriez et al.	Clustering with trust model using energy and data trust; stochastic fractal search optimization for CH selection	Extended network lifetime; effective CH selection based on trust and energy parameters.	Ignores Quality of Service (QoS) limitations; susceptible to local minima.
[26]	Hosseinzadeh et al.	Cluster-tree-based trusted routing utilizing Grasshopper Optimization Algorithm (GOA) and time-variant trust model	Robust and secure communication; effective in detecting malicious nodes; improved packet loss rate and end-to-end delay.	Does not consider energy parameters in routing decisions.
[27]	Venkatesan Cherappa et al.	ASFO with Cross-Layer-Based Expedient Routing Protocol (E-CERP)	Achieved 100% packet delivery ratio, 0.05s latency, 0.99 Mbps throughput, 1.97 mJ power consumption, 5908 rounds network lifetime, and 0.5% packet loss rate.	Time-consuming; lacks assessment against various attack types.
[28]	Roberts & Ramasamy	Enhanced high-performance clustering-based routing protocol for WSNs in IoT	Enhanced energy efficiency, congestion control, encrypted data transport, and attacker node monitoring; improved data management.	Less number of network nodes.
[29]	S. Ramalingam et al.	Enhanced Elephant Herd Optimization algorithm for effective clustering and routing	Superior packet delivery ratio, packet delay, throughput, energy use, network lifespan, and packet loss ratio	Not consider energy parameters.
[30]	Huangshui Hu et al.	Quantum PSO and Fuzzy Logic (QPSOFL) for energy-effective clustering and routing	Outperformed other protocols in network lifespan, throughput, energy consumption, and scalability; effective in avoiding local optima.	The number of sensor nodes is the minimum

3. PROPOSED METHODOLOGY

This paper introduces the Trust Energy Aware Clustering Routing (TREACR) protocol to attain EE and security-aware DT. SBODE elects TREACR protocol, CH, and extends NL by conserving the RE using an energy distribution method. The best way to identify attacks is to use the SBODE algorithm and fitness measure. Maximum fitness is regarded as the optimal option for the CH election. It is computed based on the distance between every CH and its parent and mobility, delay, energy, and trust. Three trust criteria, the WH likelihood, the flooding probability, and the BH, SH, and GH probabilities, are used in the TREACR protocol's DT model to examine SN behavior. The PDR, PLR, NL, RE, and E2ED evaluation findings demonstrate that the TREACR protocol does well. Figure 2 shows the suggested system's overall workflow.

The system model comprises the threat model, EC mechanism, and network parameters.

3.1. Network Settings

In the network environment, SN ($SN_1, SN_2, \ldots, SN_i, \ldots, SN_N$ Here, the node count can be denoted as N) and has been positioned randomly in TREACR. The network model is shown in Figure 1. Furthermore, CHs are rotatedly chosen from SN, and the LEACH procedure is employed to divide the nodes into several clusters. For the network model utilized in TREACR, the following presumptions are summed up:

- The BS and network nodes are static.
- BS uses a limitless supply of energy.

RESEARCH ARTICLE

- Because they share a common energy source, network nodes are homogeneous.
- Positioning devices and radio communication modules are among the equipment mounted on SN.
- Every SN_i has a unique identifier.

Many uniform nodes with comparable processing and communication capabilities are randomly placed in WSN data structures for a 2D sensing area. After placing, the nodes become stationary and don't require monitoring. No position discovery mechanism is involved because the nodes do not know the location. Stable, wireless, and symmetric communication links exist between the nodes in the transmission range. One of the hierarchical RP methods that offers a scalable network with low EC is cluster formation. The transmission distance and RE are used to elect the CH for each cluster. CM can only be assigned to any CH inside the transmission radius.

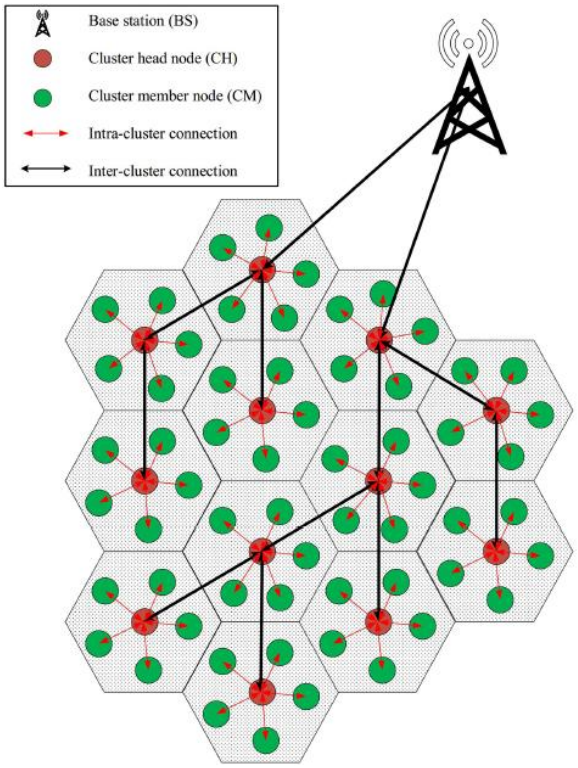

Figure 2 Network Model in TREACR

Similarly, throughout the iteration, CH and BS remain unaltered. A single iteration is defined as the time it takes for a CHE to complete before the CHS of the next CH. Every cycle of an iteration consists of three stages: setup, intra-cluster (IC), and inter-cluster communication. Depending on whether a new CH has to be picked, nodes during a distinct setup phase may send messages for network setup and maintenance. One or more CHs may be executed. During the IC communication, CH consolidates the messages it gets from CM into a single cluster message. During the inter-cluster communication, the radio is kept on by just CH so that the compressed data may be sent to the BS.

For every CH to stay awake and connect to the radio, they employ carrier-sense multiple access with collision avoidances (CSMA/CA). The CM might take a nap during communications between clusters to save power. CSMA/CA facilitates communication inside and across clusters. Within the sensing zone, the BS may move to collect useful network data. Every node broadcasts its unique identification (Node ID) and is ranked using a ranking mechanism. They all employ the CSMA MAC protocol. Selecting the next CH is aided by this rank's positive integer value. It also provides the BS with the RE to determine whether the BS has attained the energy threshold required to be elected as CH.

3.2. Energy Model

Based on energy depletion straight relative to the distance "d" between the transmitter and the receiver, the suggested model considers the radio wave propagation models. The total energy cost utilises $En_S(n,d)$ & $En_R(n)$ as in Equation (1), if "d" is less than the threshold values, then the free space (fs) technique with EC $En_{fs} * d^2$; otherwise, the MP method with EC $En_{mp} * d^4$. Energy expended on current ($En_{current}$) and in an idle state (En_{idle}).

$$En_{NetTotal} = En_S(n,d) + En_R(n) + En_{idle} + En_{current} \quad (1)$$

Additionally, according to Equation (2), the energy needed to convey an n-bit message across $'d'$ with a crossover distance of $d_0 = \sqrt{\frac{En_{fs}}{En_{mp}}}$

$$En_s(n,d) = \begin{cases} n * En_{elec} + n * En_{fs} * d^2, if\ d < d_0 \\ n * En_{elec} + n * En_{mp} * d^4, if\ d \geq d_0 \end{cases} \quad (2)$$

The energy required by electronic circuits is denoted by En_{elec}. The energy needed by an amplifier in fs is denoted as En_{fs}. The energy that MP requires is denoted as En_{mp}. Digital coding, modulation, filtering, and signal dispersion are some factors that make up En_{elec}. Equation (3) provides the energy needed if the sender transmits an n-bit message.

$$En_{STotal}(n,d) = En_{Selec}(n) + En_{Samp}(n,d) \quad (3)$$

Here, the energy the sender requires to transmit a "n" bit message is denoted by $En_{Selec}(n)$. It seems that the length of the message plays a more significant role in determining the sender's EC than the distance involved. $En_{Samp}(n,d)$, considering both the communication distance and the message length, which is the energy needed to intensify the signals to range receiver circuits. When the receiver requires more energy to effectively receive $n-bit$ messages, according to Equation (4).

RESEARCH ARTICLE

$$En_{Relec}(n) = n * En_{elec} \quad (4)$$

Here, the energy needed to receive $n - bits$ at the receiver is denoted $En_{Relec}(n)$. Equation (5) represents the RE.

$$En_{RE} = En_{Current} - En_S(n,d) + En_R(n) \quad (5)$$

Only DT among CM and CH uses energy. Equation (6) states that the rate of RE to the Euclidean Distance (ED) between CH and BS is the LT of CH.

$$LT(node, CH) = \frac{En_{RE}}{En_{Net_{Total}}} \quad (6)$$

The overall EC determines NL. If $En_{RE} \leq 0$ the node energy drops below the threshold values, it is considered dead.

3.3. ATTACK MODEL

The security risks associated with dynamic topology, deployment in hazardous areas, the absence of a central controller, and wireless connectivity must be avoided or minimized in WSNs. An essential element of cybersecurity is trust. Communicating with other SNs assesses each node's degree of trust [31]. Since security risks can compromise privacy, alter or remove data, and serve as a foundation for additional cybersecurity attacks, lowering security risks and actively identifying trusted nodes are actual objectives of a security system. This demonstrates how crucial a Trusted RP (TRP) is [31]. BH, SH, WH, GH, and flooding attacks (FA) are among the routing attacks that TREACR handles.

- To communicate with other nodes, the BH node constructs fake network paths. The purpose of this communication is to erase all DP and stop them from reaching their destination. The BH node waits for route request (RREQ) from other network nodes to construct a fake route. The BH nodes promptly replies to the demanding node after receiving the request. Remember that there is no path to the required node; therefore, these routes are fake [32].
- The BH node enhances the appeal of these fake routes by optimizing the parameters linked to them, including delay and hops, under ideal conditions. To attract more network traffic, the BH nodes fine-tune the characteristics of these simulated paths, focusing on factors like delay and the number of hops. In ideal circumstances, the BH node successfully raises the appealing nature of these fake routes by altering the related metrics, such as delay and hops.
- Except for identifying the location of sink nodes and attempting to direct all traffic toward them, the SH node is comparable to BH nodes. After that, it stops the packets from going to the sink. BH is less risky than the attack.
- DP are not entirely removed by GH. However, GH eliminates all packets sent to a given node or focusses on a specific type. It exhibits typical behaviour in other situations [33].
- Two attacker nodes will execute the WH attack. Between these two nodes, a tunnel is formed, and additional nodes are requested to pass their DP through this tunnel. They make this tunnel extremely appealing by routing parameters to draw in network traffic. DP can be copied, altered, or removed, and the attack offers a perfect platform for tracking transmitter node communications.
- The FA node targets a particular node, which attacks it with fake route requests. The target node's energy level is significantly lowered and its memory overflows due to processing these requests and storing some data. This makes it impossible for the DN to respond to real requests from reliable nodes. This attack seriously damages the network due to the limited energy of SN.

3.4. Trust Energy Aware Clustering Routing (TREACR) Protocol

This section will introduce the TREACR for WSN using the SBODE. The DT model and SBODE-based trusted routing are the two primary processes in this approach.

3.4.1. Dynamic Trust (DT)

The TV remains constant throughout each period, even though the nodes' trust is periodically updated in a traditional trust model. However, this is untrue, as trust is a variable that changes over time and has no fixed value. Consequently, a more accurate estimate of the TV may be obtained if a dynamic (WC) Weight Coefficient is measured for the trust variables. A decentralized DT model is suggested in TREACR to determine the TV of nodes. Direct trust (DIT), REcommended trust (RET), and Dynamic Final Trust (DFT) are the three parts of DT.

Direct trust (DIT) component: The DIT component of TREACR consists of a dynamic coefficient and an initial value. The SH, BH, and GH likelihood (pr_{SBG}),), the WH likelihood (pr_{WH}), and the FA likelihood (pr_{FA}) are the 3 trust criteria that determine the initial value. These three criteria were established based on an investigation of how SNs behave when interacting with one another. Let's assume that SN_i makes an effort to determine the TV that corresponds accurately. The three criteria pr_{SBG}^j, pr_{WH}^j, and pr_{FA}^j are acquired by direct interaction between SN_i and SN_j to accomplish this purpose.

pr_{SBG}^j: The probability that SN_j is a SH, BH, or GH node is investigated using this criterion. There are not many differences between these three attacks; they are all fairly comparable. Most significantly, the SH, BH, and GH nodes destroy all or most of the DP and have extremely poor packet

RESEARCH ARTICLE

transmission rate (PTR) and Packet reception rates (PRR). Thus, using Equation (7), pr_{SBG}^{j} is attained.

$$pr_{SBG}^{j} = \lambda\left(1 - \frac{Pa_j^{received}}{Pa_j^{total-receiving}}\right) + (1-\lambda)\left(1 - \frac{Pa_j^{sent}}{Pa_j^{total-sending}}\right) \quad (7)$$

$Pa_j^{received}$ indicates how many packets SN_j has received. $Pa_j^{total-receiving}$ is a representation of the total amount of packets that SN_jshould receive. Additionally, the number of packets transmitted by SN_j is represented by Pa_j^{sent}.

The $Pa_j^{total-sending}$ specifies the overall number of packets that SN_j will transmit.

Another fixed number modified in [0, 1] is λ. To assess the comparative significance of the PTR and the PRR, the weight linked to the reception ratio is expressed using λ. Depending on the needs of the application, this weight might be changed.

pr_{WH}^{j}: The probability that SN_j is a WH node is investigated by this criterion. The tendency of WH nodes to create several pathways and absorb traffic from neighbouring nodes is their most important feature. The WH nodes become congested due to this capacity to handle network traffic.

A very long queuing delay will be an outcome. Due to the elimination of several received packets, these nodes' second feature is their poor package reception rate. The ability of WH nodes to duplicate DP and forward them around the network is another feature. As a result, their redundancy rate is significant. At last, Equation (8) defines pr_{WH}^{j}.

$$pr_{WH}^{j} = \Psi_1\left(\frac{T_j^Q}{\max\limits_{SN_k \in N_i}\{T_k^Q\}}\right) + \Psi_2\left(1 - \frac{Pa_j^{received}}{Pa_j^{total}}\right) + \Psi_3\left(\frac{DPa_j}{NPa_j + DPa_j}\right) \quad (8)$$

Here, SN_j queuing delay is indicated by T_j^Q. Hello packets contain this parameter. The collection of neighbours of SN_i is expressed by N_i. Lastly, the number of duplicate and new packets received SN_j are described by DPa_j and NPa_j, respectively. Furthermore, so that Ψ_1, Ψ_2, and Ψ_3 are fixed numbers in [0, 1] and $\sum_{i=1}^{3}\Psi_i = 1$, Ψ_1 is the WC associated with the delay parameter, Ψ_2 is the WC related to PRR, and Ψ_3 is the WC associated with the redundancy rate. These weights can be adjusted to meet the application's needs and demonstrate these factors' significance.

pr_{FA}^{j}: The probability that SN_j is an FA node is investigated by this criterion. FA nodes' high EC and high route request sending rate are their two most crucial features. A significant quantity of duplicate packets is an additional feature of these nodes. In Equation (9) pr_{FA}^{j} is computed.

$$pr_{FA}^{j} = \ell_1\frac{\left(\frac{En_j^{res,t-1} - En_j^{res,t}}{\max\limits_{SN_k \in N_i}\{T_k^Q\}}\right)}{\Delta t} + \ell_2\frac{\left(\frac{Pa_j^{sent}}{\max\limits_{k \in N_j \& SN_j}\{Pa_k^{sent}\}}\right)}{\Delta t} + \ell_2\left(\frac{DPa_j}{NPa_j + DPa_j}\right) \quad (9)$$

Here, the WC associated with the energy factor is denoted by ℓ_1. With ℓ_1, ℓ_2, and ℓ_3 being fixed values in [0, 1] and $\sum_{i=1}^{3}\ell_i = 1$, ℓ_2 is the WC related to the PTR, and ℓ_3 is the WC associated with the redundancy rate. These weights can be adjusted to meet the application's needs and demonstrate these factors' significance. The RE of SN_j in 2 times, t and t − 1, is represented by $\llbracket En_j^{res,t}$and $En_j^{res,t-1}$ correspondingly. SN initial energy is denoted by En_{ini}. Equation (10), which defines $En_j^{res,t}$,

$$En_j^{res,t} = En_{ini} - EC_j^t \quad (10)$$

Here, EC of the SN_j at time t is expressed by EC_j^t. Based on the energy model, Equation (11),

$$EC_j = \sum_{x=1}^{n_{EC}}\left(En_{tx}^{j} + En_{rx}^{j}\right) \quad (11)$$

Here the energy needed for packet transmission, packet reception, and the amount of DT processes carried out SN_j are expressed by En_{tx}^{j}, En_{rx}^{j}, and n_{EC}, correspondingly. At last, Equation (12) defines the initial value of the DIT component in [t − 1, t] ($i.e.\,\mathrm{DIT}_{ij}(t-1)$).

$$DIT_{ij}(t-1) = 1 - \max\{pr_{SBG}^{j}, pr_{WH}^{j}, pr_{FA}^{j}\} \quad (12)$$

Equation (13) will now be used to calculate $DIT_{ij}(t)$,

$$DIT_{ij}(t) = DIT_{ij}(t-1)e^{-\rho t}, [t-1, t] \quad (13)$$

Accordingly, the time-variant dynamic coefficient is $e^{-\rho t}$. Equation (14) yields the conventional value of $DIT_{ij}(t-1)$ this coefficient, which is equal to ρ.

$$\rho = \frac{DIT_{ij}(t-1) - \mu_{DIT}}{\sigma_{DIT}} \quad (14)$$

μ_{DIT} and σ_{DIT},stand for the mean and standard deviation of $DIT_{ij}(t)$.

Equations (15-16) shows it,

$$\mu_{DIT} = \int_{t=0}^{t-1} tDIT_{ij}(t)dt \quad (15)$$

$$\sigma_{DIT} = \left[\sqrt{E\left(DIT_{ij}^2\right) - \left(E\left(DIT_{ij}\right)\right)^2}\right] \quad (16)$$

REcommended trust (RET) component:

DT model's RET component. RET SN_i considers the TV

RESEARCH ARTICLE

suggested by the recommended nodes (RN_k) in addition to its interactions to determine the trust of SN_j . $R = \{RN_1, RN_2, \ldots, RN_k, \ldots, RN_{|R|}\}$ is a set that contains all RN_knodes, and RN_k is a common node between $SN_i$and SN_j in DT. When accepting the trust that each RN_k recommends in DT, SN_i consider a weight coefficient $CT_{ik}(t-1)$. This coefficient expresses the significance of the advice given by. It is derived using Equation (17) and has two criteria.

Initial trust of SN_i relative to RN_k $(DIT_{ik}(t-1))$. SN_i disregards the recommendation made by an untrusted RN_k based on this criterion.

The discrepancy between SN_i computed trust and RN_k recommended trust. As per this criterion, SN_i favours RN_k nodes whose DT value is nearer to DT value of SN_i.

$$CT_{ik}(t-1) = DIT_{ik}(t-1)\left(1 - \frac{|DIT_{ij}(t-1) - DIT_{kj}(t-1)|}{\max\limits_{RN_k \in R}\{DIT_{kj}(t-1)\}}\right) \quad (17)$$

Equation (18) is used to calculate RET_{ij} based on the aforementioned conditions.

$$RET_{ij} = \frac{1}{|R|}\sum_{k\in R}^{|R|}\left(CT_{ik}(t-1).DIT_{kj}(t-1)\right) \quad (18)$$

In this case, |R| is the number of members of $R = \{RN_1, RN_2, \ldots, RN_k, \ldots, RN_{|R|}\}$. $DIT_{kj}(t-1)$ is the initial TV of RN_k concerning SN_j.

Dynamic Final Trust (DFT) component:

Since DT is a time-variant function. Consequently, a TVT function is another definition of DFT. Equation (19) is expressed as,

$$\mathrm{DFT}_{ij}^{t} = \alpha DT_{ij}(t) + (1-\alpha)RET_{ij} \quad (19)$$

In this case, the regulatory coefficient is $\alpha \in [0, 1]$.

3.4.2. SBODE

The optimal security against attacks and QoS metrics are calculated using the SBODE method and fitness measure. The maximum fitness is regarded as the optimal option for CHE. It is computed using the following factors: mobility, delay, energy and trust, and the distance among every CH and its parent.

A MO FF is considered when evaluating the best CH and route in the SBODE creation method. Each iteration will then update the bird positions according to this FF. Relocating CH in the routing is the objective of this update procedure.

Using a MO approach, the SBODE algorithm chooses the CH based on four criteria: the CH's trust level, mobility, delay, and distance from its parent node. It also considers the RE of the CH. Equation (20) measures fitness in the CHS search space with established bird positions.

$$F_{fitness} = \frac{1}{4}(\mathrm{f_1} + \mathrm{f_2} + \mathrm{f_3} + \mathrm{f_4}) \quad (20)$$

The emphasis on each CH distance from its parent is shown by $\mathrm{f_1}$. Based on their trust and energy, $\mathrm{f_2}$ shows the CHs on way. The fitness of mobility is denoted by $\mathrm{f_3}$. The routing system uses $\mathrm{f_4}$ to represent the delay in data transfer. For AD, the fitness measure calculates the best solution.

The BS searches the routing tree for a tree where each CH has a minimal distance to its parent. This element was chosen because it determines whether the distance among every CH and its parent node is the shortest during the DT process among a CH node and the BS. This CH will send DP faster (less delay) to its parent node in the route. It will use less energy during the DT process as a result. Therefore, $\mathrm{f_1}$, which is determined using Equation (21),

$$f_1 = \frac{1}{\sum_{i=1}^{Q} \mathrm{d(CH_i, Parent_i)}} \quad (21)$$

Here, $\mathrm{d(CH_i, Parent_i)} = \sqrt{(\mathrm{x_i} - \mathrm{x_p})^2 + (\mathrm{y_i} - \mathrm{y_p})^2}$.

Additionally, $\mathrm{CH_i}$ coordinates are expressed by $(\mathrm{x_i}, \mathrm{y_i})$, $(\mathrm{x_p}, \mathrm{y_p})$ and its parent $(\mathrm{Parent_i})$ by $(\mathrm{x_p}, \mathrm{y_p})$. Therefore, using Equation (22), the selection of CH in route based on their energy and trust is the focus of f_2.

$$f_2 = \sum_{D=1}^{[\log Q]}\frac{1}{D}\sum_{x=1}^{2^D}\left(\partial\left(\frac{\mathrm{En_{res,t}^x} - \mathrm{En_{min}}}{\mathrm{En_{ini}} - \mathrm{En_{min}}}\right)\right) + (1-\partial)\left(\frac{\mathrm{DFT_x(t)} - \min\limits_{\mathrm{CH_k}\in \mathrm{TR}}\{\mathrm{DFT_k(t)}\}}{\max\limits_{\mathrm{CH_k}\in \mathrm{TR}}\{\mathrm{DFT_k(t)}\} - \min\limits_{\mathrm{CH_k}\in \mathrm{TR}}\{\mathrm{DFT_k(t)}\}}\right) \quad (22)$$

Here, the RE of CH_x is described by $\mathrm{En_{res,t}^x}$. The primary energy of the network nodes is indicated by $\mathrm{En_{ini}}$, The minimum energy threshold is denoted as $\mathrm{En_{min}}$= 15%$\mathrm{En_{ini}}$. Additionally, D is the tree depth, in [0, 1], @ is a fixed value, and $\mathrm{DFT_x(t)}$ is the trust of CH_x.

Mobility Model: Node movements are specified and the routing mechanism for DT in WSN is evaluated in the mobility model. In real-time applications, the mobility model simulates the nodes' movements.

An optimal analysis approach is a random mobility scheme due to its accessibility and ease of application. Two SN, denoted by the terms a and b, having initial positions of (r_1, s_1) and (r_2, s_2). As the x-axis velocity changes, these nodes move with angles θ_1 and θ_2. Nodes a and b move with distances d_1 and d_2 at time interval t. At the tth time, following the mobility process, they relocate. The following describes the distance $(\mathrm{dis_{a,b}})$ among the nodes $a(r_1, s_1)$ and $b(r_2, s_2)$ in Equation (23).

RESEARCH ARTICLE

$$f_3 = dis_{a,b} = \sqrt{|r_1 - r_2|^2 + |s_1 - s_2|^2} \quad (23)$$

Delay: The average time needed to transmit a packet from the source node to the BS is the delay.

The SBOA method is classified as a population-based MH approach. It considers each Secretary Bird (SB) member of the algorithm's population [34].

Equation (20) establishes the FF values based on each SB's location inside the search space. Thus, the SB positions provide potential solutions to the CHS problem using the SBOA technique. The placements of the SB in the CH search space are randomly initialized in the first implementation of the SBOADE using Equation (24).

$$X_{i,j} = lb_j + r \times (ub_j - lb_j), i = 1, \ldots., N, j = 1,2, \ldots Dim \quad (24)$$

The position of the ith SB of the jth CH position is indicated by X_i. CH's lower bound (lb) and upper bound (UB) are denoted by lb_j and ub_j, correspondingly. A random numbers between 0 and 1 is indicated by r. According to Equation (25), the SBOA uses a population-based technique in which optimization starts with populations of potential CH solutions. These candidate CH solutions X are generated randomly in the (ub) and (lb) parameters limits for the CHS problem in WSN. The optimal CH solution identified thus far is roughly considered the ideal solution in every iteration.

$$X = \begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,j} & \cdots & x_{1,Dim} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,j} & \cdots & x_{2,Dim} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{i,1} & x_{i,2} & \cdots & x_{i,j} & \cdots & x_{i,Dim} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{N,1} & x_{N,2} & \cdots & x_{N,j} & \cdots & x_{N,Dim} \end{bmatrix}_{N \times Dim} \quad (25)$$

The CHS was done using the SB group, which was indicated by X. The ith SB was mentioned by X_i. The ith SB jth CHS of a variable was stated by $X_{i,j}$. The number of group members (the secretary) is N. The issue with CHS is Dim. Every SB is a candidate CH routing solution. Equation (26) is then utilized to compile the resulting Objective Functions (OF) values into a vector.

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N \times 1} = \begin{bmatrix} F(X_1) \\ \vdots \\ F(X_i) \\ \vdots \\ F(X_N) \end{bmatrix}_{N \times 1} \quad (26)$$

Here, F specifies the vector of OF values. For jth CHs, F_i is the OF value that the ith SB obtained. The SBOADE members have been updated utilizing two dissimilar SB natural behaviors. These 2 categories of actions include

(a) The hunting policy of the SB:

(b) The SB's escape policy.

3.4.2.1. Hunting Strategy of SB (Exploration Phase)

Searching for, overriding, and attacking prey are the three main phases of SB hunting behavior when feeding on snakes.

Stage 1 (Searching for Preys): The first stage in SB hunting is searching for potential prey, especially snake. Differential Evolution (DE) increases model diversity and Global Search (GS) abilities by leveraging individual variances to produce new solutions. Diversity can prevent local optima from becoming imprisoned by introducing differential Mutation Operations (MO). Examining multiple area of the solution space increases the probability of identifying the global optimum. Consequently, equations (27–28) can be used to simulate updating the SB location throughout this phase quantitatively.

$$\text{While } t < \frac{1}{3}T, x_{i,j}^{new,P1} = x_{i,j} + (x_{random1} - x_{random2}) \times R_1 \quad (27)$$

$$X_i = \begin{cases} X_i^{new,P1}, \text{if } F_i^{new,P1} < F_i \\ X_i, \text{else} \end{cases} \quad (28)$$

In this case, t stands for the current iteration number. T stands for the maximum numbers of iteration.

In the first stage, the fresh state of the ith SB is signified by $X_{i,j}^{newP1}$i. In the initial stage iteration, the random candidate solutions are represented as $x_{random1}$ and $x_{random2}$. The randomly produced array of dimensions 1 × Dim from the interval [0, 1] is represented by the symbol $R_1$1. Here, Dim is the CH solution space's dimensionality. The value of the jth CH is represented by $x_{i,j}^{new,P1}$, while the OF is represented by $F_i^{new,P1}$.

Stage 2 (Consuming Preys): An SB utilizes a unique hunting method after finding a snake. At this point, the SB may stop often to use its keen vision to pinpoints the snake's position. Brownian motion and $xbest$ (individual historical best CH position) are used here. Therefore, equations (29–31) can be used to mathematically simulate updating the SB location in the Consuming Prey phase.

$$RB = randn(1, Dim) \quad (29)$$

$$\text{While } \frac{1}{3}T < t < \frac{2}{3}T, x_{i,j}^{new,P1} = x_{best} + \exp\left(\left(\frac{t}{T}\right)^4\right) \times (RB - 0.5) \times (x_{best} - x_{i,j}) \quad (30)$$

$$X_i = \begin{cases} X_i^{new,P1}, \text{if } F_i^{new,P1} < F_i \\ X_i, \text{else} \end{cases} \quad (31)$$

Here, x_{best} is the current best value.

A randomly generated 1 × Dim array with standard normal

RESEARCH ARTICLE

distributions (mean 0 and standard deviations 1) is termed randn (1, Dim).

Stage 3 (Attacking Preys): The SB recognizes the opportunity when the snake is exhausted and quickly moves to strike with its strong leg muscles. To strengthen the optimizer's GS abilities, lower the possibility of SBOA becoming trapped in local solutions, and increase the algorithm's convergence accuracy, the Levy flight (LF) strategy is added to the random search process. Therefore, equations (32–33) can be used to quantitatively simulate updating the SB position in the Attacking Prey stage.

$$\text{Whilet} > \frac{2}{3}\text{T}, \text{x}_{\text{i,j}}^{\text{new,P1}} = \text{x}_{\text{best}} + \exp\left(\left(1 - \frac{\text{t}}{\text{T}}\right)^{\left(2\times\frac{\text{t}}{\text{T}}\right)}\right) \times \text{x}_{\text{i,j}} \times \text{RL} \quad (32)$$

$$\text{X}_\text{i} = \begin{cases} \text{X}_\text{i}^{\text{new,P1}}, \text{if } \text{F}_\text{i}^{\text{new,P1}} < \text{F}_\text{i} \\ \text{X}_\text{i}, \text{else} \end{cases} \quad (33)$$

Optimising the algorithm's accuracy by using the weighted LF or RL.

$$\text{RL} = 0.5 \times \text{Levy(Dim)} \quad (34)$$

In this case, Levy(Dim) signifies the LF distribution functions in Equation (34).

It is computed in this way represented Equation (35),

$$\text{Levy(D)} = \text{s} \times \frac{\mu\times\sigma}{|\nu|^{1/\eta}} \quad (35)$$

Here, η and s are fixed constants of 1.5 and 0.01, respectively. Random numbers in the range [0, 1] are u and v in Equation (36). The following is the formula for σ:

$$\sigma = \left(\frac{\Gamma(1+\eta)\times\sin\left(\frac{\pi\eta}{2}\right)}{\Gamma\left(\frac{1+\eta}{2}\right)\times\eta\times2\left(\frac{\eta-1}{2}\right)}\right)^{\frac{1}{\eta}} \quad (36)$$

The gamma function has values of 1.5, denoted by Γ.

3.4.2.2. Escape Strategy of SB (Exploitation Phase)

Due of their ability to attack or steal their food, large predators like hawks, eagles, foxes, and jackals are SB's natural enemies.

It can be divided into two primary categories. In the first method, SB first looks for suitable camouflage environment when they sense the occurrence of predators. Here, $\left(1 - \frac{t}{T}\right)$ is used to represent a dynamic perturbation factor. The algorithm balances exploration and exploitation with the support of this $\left(1 - \frac{t}{T}\right)$.

In conclusion, Equation (37), which may be used to characterize both of the evasion tactics used by SB quantitatively, can express this updated condition.

$$\text{x}_{\text{i,j}}^{\text{new,P2}} = \begin{cases} \text{C}_1\text{: x}_{\text{best}} + (2 \times \text{RB} - 1) \times \left(1 - \frac{\text{t}}{\text{T}}\right)^2 \times \text{x}_{\text{i,j}}, & \text{if rand} < \text{r}_\text{i} \\ \text{C}_2\text{: x}_{\text{i,j}} + \text{R}_2\left(\text{x}_{\text{random}} - \text{K} \times \text{x}_{\text{i,j}}\right), & \text{else} \end{cases} \quad (37)$$

$$\text{X}_\text{i} = \begin{cases} \text{X}_\text{i}^{\text{new,P2}}, \text{if } \text{F}_\text{i}^{\text{new,P2}} < \text{F}_\text{i} \\ \text{X}_\text{i}, \text{else} \end{cases} \quad (38)$$

If r = 0.5, R_2 is the random production of an array of dimensions (1 × Dim) from the standard distribution in Equation (38).

The current iteration's random candidates CH solution is represented by the x_{random}. Equation (39) can be used to identify K, the random selection of integers 1 or 2.

$$\text{K} = \text{round}\left(1 + \text{rand}(1,1)\right) \quad (39)$$

The random generation of an integer between 0 and 1 is denoted as $\text{rand}(1,1)$. SBOADE pseudocode appears in Algorithm 1.

1. Set Problem Settings (Dim, ub, lb Pop_size (N)), Max_Iter(T), Curr_Iter(t))
2. Set the population randomly
3. For t 1: T
4. Update SB X_{best}
5. For i = 1: N
6. Exploration:
7. if $t < \frac{1}{3}T$
8. Compute novel status of the i[th] SB by Equation (27)
9. Update the i[th] SB by Equation (28)
10. else if $\frac{1}{3}T < t < \frac{2}{3}T$
11. Compute novel status of the i[th] SB by Equation (30)
12. Update the i[th] SB by Equation (31)
13. else
14. Compute novel status of the i[th] SB by Equation (32)
15. Update the i[th] SB by Equation (33)
16. end if
17. Exploitation:
18. if r < 0.5
19. Compute novel status of the i[th] SB by C_1 in Equation (37)
20. else

RESEARCH ARTICLE

21. Compute the novel status of the i[th] SB by C_2in Equation (37)
22. end if
23. Update the i[th] SB by Equation (38)
24. end for i = 1: N
25. keep the best candidate solution so far.
26. end for t = 1: T
27. The optimal solution is attained via SBOADE for a given optimization problem.
28. Return the best solution.

Algorithm 1 Pseudocode of SBOADE

The unique hybrid optimization approach known as Secretary Bird Optimization with Differential Evolution (SBODE) combines the Trust Energy Aware Clustering Routing (TREACR) protocol to produce the suggested model. By including node trustworthiness and residual energy in the cluster head assortment and routing procedure, this integration aims to improve WSNs. In contrast to more conventional models like LEACH, TEEN, or SEP, which ignore node behavior in favor of random or energy-based criteria for cluster head selection, the suggested model uses a trust evaluation mechanism to identify and remove untrustworthy nodes from data transmission. Combining Secretary Bird Optimization's exploration strength with Differential Evolution's exploitation capabilities, the SBODE algorithm further refines the selection process, resulting in a balanced and optimum decision-making process. For the model to function, it first computes trust for each node using its energy level and past behavior. Then, it uses SBODE to choose the best cluster heads. The TREACR protocol improves network lifespan, reduces packet loss, and enhances overall dependability by managing routing by favoring secure and energy-efficient pathways after clusters are created.

4. RESULTS ANALYSIS AND DISCUSSION

MATLAB R2018a has been used to simulate the TREACR algorithm's performance on an Intel(R) Core (TM) i5 processor running Windows 10 with a CPU speed of 2.80 GHz and 16 GB of RAM. The experiments assume a WSN configuration with nodes and BS located in a 200*200 m2 region. Table 2 provides the parameters for the model that is being presented. The hierarchical clustering protocol model is used in the suggested model. The suggested model considered the homogeneous network. Every node has the same amount of memory, processing speed, and capacity for both transmission and reception. In this work, "n" bits of data are sent using the fs network model at a distance of "d" between transmitters in transmitting circuits and receivers in receiving circuits. Initialisation, population, crossover likelihood rate $(CPR) \in [0.5,1]$, variation factor $(F) \in [0,2]$, and maximum iteration $(I_{max})$are all components of DE. The degree of disturbance in the mutation process is determined by the scaling factor (SF). The high value of the CPR performs better if the limit is co-related. The performance of the proposed TREACR is analyzed based on metrics like packet delivery ratio, packet loss ratio, network lifetime, end-to-end delay, and residual energy than other existing models ECATS-ALO, EECHS-ISSADE, EECHS-ARO, and EECHS-HMAOA-DE.

Table 2 Simulation Setup

Parameters	Value
Area	200× 200 m^2
Total node (n)	500
% of CH	5-10%
Radio Propagation models	fs
BS's Min and max positions	[0,500]
Initial node energy(En_0)	Standard nodes = 0.5 J; progressive nodes = 2 J
Energy$_{elec}$	70 nJ/bit
En_{fs}	10 pJ/bit/m^2
En_{mp}	0.00013 pJ/bit/m^4
d_0	87 m
Communication radius	40 m
Energy DA	5 nJ/bit/signal
Packet size	4096 bits
% of CHs (p)	0.1
Range of TV	[0, 1]
Trust Threshold	0.35
MAC	802.11
Number of rounds (I_{max})	2000
SF	1

4.1. Packet Delivery Ratio (PDR)

The PDR is the total $data\_received$ divided by the total of the DT. Equation (40) describes it.

$$PDR = 100 - \frac{data\_received}{data\_transmitted} \times 100 \qquad (40)$$

PDR results comparison of various methods like QEBSR, TARM, TBSEER, CTTRG, and TREACR are illustrated in Figure 3. The outcomes are measured by different node counts as 100, 200, 300, 400, and 500. From the results, it indicates that the suggested technique has the maximum PDR outcomes of 92.59%; other approaches, such as QEBSR, TARM, TBSEER, and CTTRG, have PDR of 86.78%, 87.91%, 89.21%, and 90.64% for 100 nodes. The suggested

RESEARCH ARTICLE

method has 6.2%, 4.91%, 2.83%, and 2.13% highest values compared to QEBSR, TARM, TBSEER, and CTTRG methods.

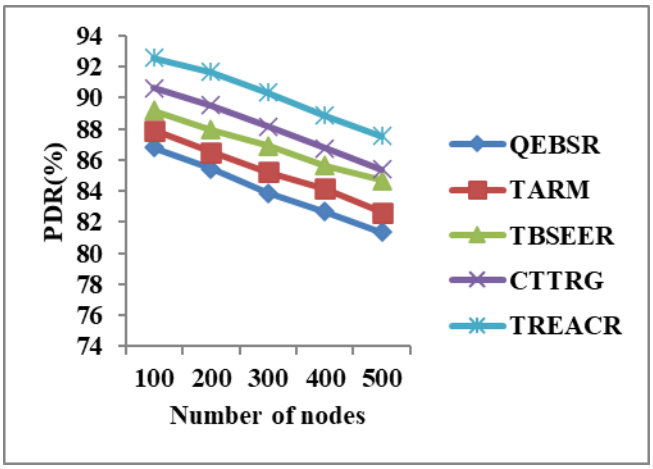

Figure 3 PDR Comparison of Trust-Based Routing Methods

4.2. Packet Loss Ratio (PLR)

Data losses that occur both during transmission from the source node to the DN and during reception at the DN are packet losses. 500 nodes are defined as the ratio of DT to data received. The PLR in WSN is calculated using Equation (41).

$$PLR = 100 - \frac{data\_transmitted}{data\_received} \times 100 \quad (41)$$

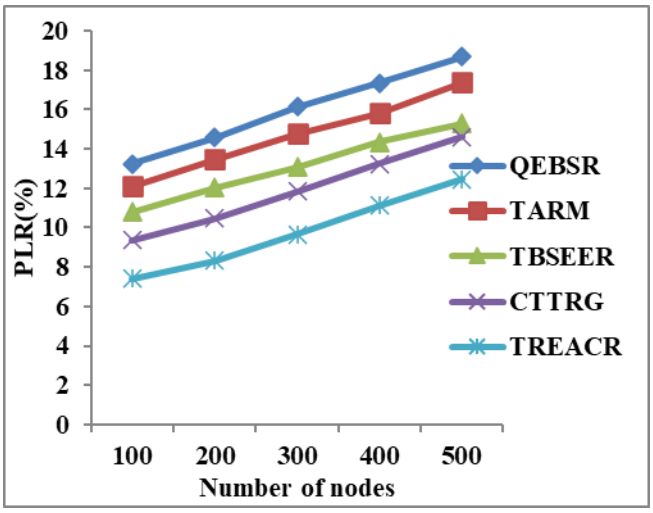

Figure 4 PLR Comparison of Trust-Based RP

PLR results comparison of various methods like QEBSR, TARM, TBSEER, CTTRG, and TREACR are illustrated in Figure 4. The outcomes are measured by different numbers of nodes, such as 100, 200, 300, 400, and 500. From the results, it shows that the suggested method has the minimum PLR results of 7.41%; other approaches such as QEBSR, TARM, TBSEER, and CTTRG have PLR of 13.22%, 12.09%, 10.79%, and 9.36% for 100 nodes. According to outcomes, TREACR has the minimum PLR and decreases it by 6.2%, 4.91%, 2.83%, and 2.13% in comparison with QEBSR, TARM, TBSEER, and CTTRG for 500 nodes, respectively.

4.3. Network Lifetime (NL)

An important determining metric in WSN is NL, which is calculated as the period of time until the initial sensor energy runs out. In a traditional WSN, every SN is set up to send data collected to the sink via the use of multi-hop communication.

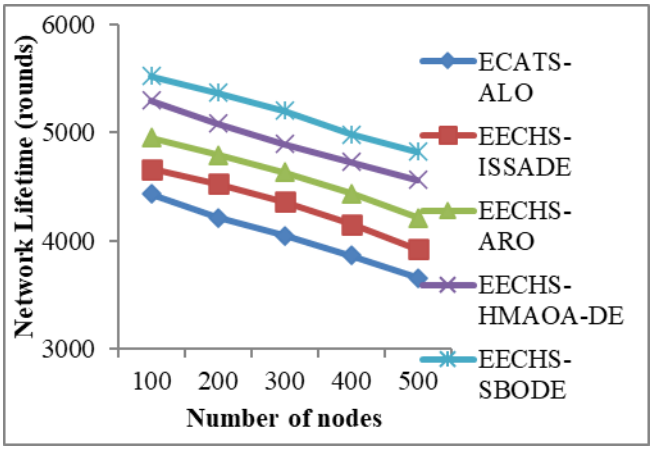

Figure 5 Network Lifetime Vs. Clustering Methods

NL comparison of clustering methods like ECATS-ALO, EECHS-ISSADE, EECHS-ARO, EECHS-Hybrid Mutation Albatross Optimization Algorithm with Differential Evaluation (HMAOA-DE) and proposed EECHS-SBODE has been illustrated in figure 5. The outcomes show that the suggested method has the highest NL of 4825 rounds, while other methods such as ECATS-ALO, EECHS-ISSADE, EECHS-ARO, and EECHS-HMAOA-DE give the lowest lifetime of 3657 rounds, 3925 rounds, 4211 rounds, and 4563 rounds for 500 nodes. It has 24.20%, 18.65%, 12.72%, and 5.43% improved network lifetime when compared to the ECATS-ALO, EECHS-ISSADE, EECHS-ARO, and EECHS-HMAOA-DE methods, respectively.

4.4. End 2 End Delay (E2ED)

The transmission and reception of data within the same network to reach the DN is referred to as the E2ED. The route E2ED is determined using Equation (42).

$$End\ to\ End\ Delay = time_{taken_{data_{receiving}}} + time\_taken_{data\_transmitting} \quad (42)$$

The RE comparison of several clustering methods, including ECATS-ALO, EECHS-ISSADE, EECHS-ARO, EECHS-HMAOA-DE, and the suggested EECHS-SBODE, is shown in Figure 6.

RESEARCH ARTICLE

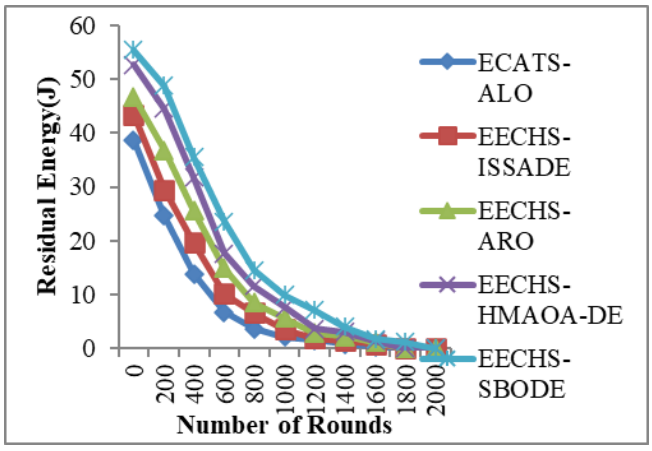

Figure 6 Residual Energy Comparison Vs. Clustering Approaches

From the outcomes, it shows that the suggested method has the highest RE of 5.78 J; other methods such as ECATS-ALO, EECHS-ISSADE, EECHS-ARO, and EECHS-HMAOA-DE have the lowest residual energy of 0.42 J, 0.83 J, 2.32 J, and 3.11J for 1400 rounds. It has 77.87%, 49.73%, 32.43%, and 22.16% increased residual energy remains when compared to the ECATS-ALO, EECHS-ISSADE, EECHS-ARO, and EECHS-HMAOA-DE methods.

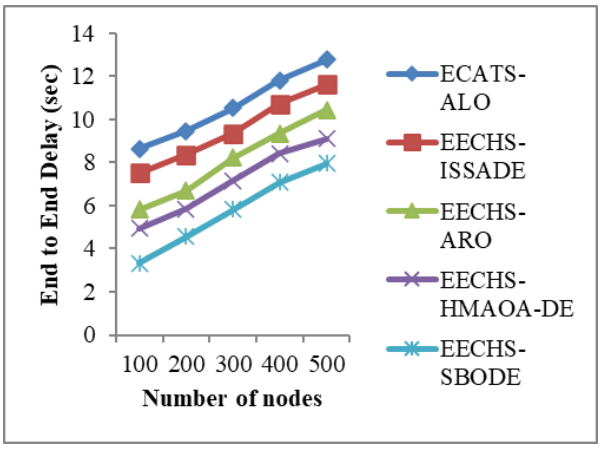

Figure 7 E2ED Comparison Vs. Clustering Methods

ECATS-ALO, EECHS-ISSADE, EECHS-ARO, EECHS-HMAOA-DE, and suggested EECHS-SBODE with respect to E2ED have been illustrated in Figure 7. According to the simulation, it shows that the suggested system has the lowest delay of 7.95 seconds; other methods such as ECATS-ALO, EECHS-ISSADE, EECHS-ARO, and EECHS-HMAOA-DE have the highest delay of12.78 seconds, 11.62 seconds, 10.45 seconds, and 9.12 seconds for 500nodes. It has 37.79%, 31.58%, 23.92%, and 12.83% has reduced delay when compared to the ECATS-ALO, EECHS-ISSADE, EECHS-ARO, and EECHS- HMAOA-DE methods.

5. CONCLUSION AND FUTURE WORK

This study introduces the TREACR protocol to achieve EE and security-aware DT. TREACR contains two mechanisms: The Dynamic Trust (DT) and the Secretary Bird Optimization with Differential Evolution (SBODE)-based CHE model. To evaluate SN's behavior and assess their level of trust, the BH, GH, and SH probabilities, the WH likelihood, and the FA likelihood are the three criteria that the DT mechanism employs. DIT, RET, and DFT are the three parts of DT. TREACR was implemented to provide CHs and BS with secure and reliable communication channels. Maximal fitness is regarded as the optimal solution for CHE in the SBODE-based CHE model. It determines the distance between every CH and its parent, mobility, delay, energy, and trust. SBODE, two distinct natural behaviors, the hunting strategy and the escape strategy of the SB, have been applied to choose the best CH in the clustering. Consequently, the DT process will use less energy, extending the NL. QEBSR, TARM, TBSEER, CTTRG, and TREACR methods have been evaluated by PDR and PLR. Network lifetime, residual energy, and E2ED have been experimented with using ECATS-ALO, EECHS-ISSADE, EECHS-ARO, EECHS-HMAOA-DE, and EECHS-SBODE methods. The suggested model's potential can be used to improve coverage and connectivity problems in the future. By combining all significant characteristics of CHS with any MH technique to create innovative hybrid approaches, the network performance may be further enhanced.

REFERENCES

[1] W. Elsayed, M. Elhoseny, S. Sabbeh, & A. Riad, "Self-maintenance model for wireless sensor networks," Computers & Electrical Engineering, vol. 70, pp. 799-812, 2018.

[2] J. S. Pan, Trong-The Nguyen, T. K. Dao, T. S. Pan, & S.C. Chu, "Clustering Formation in Wireless Sensor Networks: A Survey," J. Netw. Intell., vol. 2, no. 4, pp. 287-309, 2017.

[3] E. R. Montiel, M. E. Rivero-Angeles, G. Rubino, H. Molina-Lozano, R. Menchaca-Mendez, & R. Menchaca-Mendez, "Performance analysis of cluster formation in wireless sensor networks," Sensors, vol. 17, no. 12, pp. 2902, 2017.

[4] H. R. Farahzadi, M. Langarizadeh, M. Mirhosseini, & S. A. Fatemi Aghda, "An improved cluster formation process in wireless sensor network to decrease energy consumption," Wireless Networks, vol. 27, pp. 1077-1087, 2021.

[5] Y. Li, & Y. Tian, "A lightweight and secure three-factor authentication protocol with adaptive privacy-preserving property for wireless sensor networks," IEEE Systems Journal, vol. 16, no. 4, pp. 6197-6208, 2022.

[6] M. Elshrkawey, S. M. Elsherif, & M. E Wahed, "An enhancement approach for reducing the energy consumption in wireless sensor networks," Journal of King Saud University-Computer and Information Sciences, vol. 30, no. 2, pp. 259-267, 2018.

[7] T. Ahmad, M. Haque, & A. M. Khan, "An energy-efficient cluster head selection using artificial bee's colony optimization for wireless sensor networks," Advances in nature-inspired computing and applications, pp. 189-203, 2019.

[8] P. Subramanian, J. M. Sahayaraj, S. Senthilkumar, & D. S. Alex, "A hybrid grey wolf and crow search optimization algorithm-based optimal cluster head selection scheme for wireless sensor networks," Wireless Personal Communications, vol. 113, no. 2, pp. 905-925, 2020.

RESEARCH ARTICLE

[9] D. Chandirasekaran, & T. Jayabarathi, "Cat swarm algorithm in wireless sensor networks for optimized cluster head selection: a real time approach," Cluster Computing, vol. 22, pp. 11351-11361, 2019.
[10] T. A. Alghamdi, "Energy efficient protocol in wireless sensor network: optimized cluster head selection model," Telecommunication Systems, vol. 74, no. 3, pp. 331-345, 2020.
[11] W. Osamy, A. M. Khedr, A. Salim, A. I. Al Ali, & A. A. El-Sawy, "Coverage, deployment and localization challenges in wireless sensor networks based on artificial intelligence techniques: a review," IEEE Access, vol. 10, pp. 30232-30257, 2022.
[12] M. Faris, M. N. Mahmud, M. F. M. Salleh, & A. Alnoor, "Wireless sensor network security: A recent review based on state-of-the-art works," International Journal of Engineering Business Management, vol. 15, pp. 18479790231157220, 2023.
[13] C. Dai, & Z. Xu, "A secure three-factor authentication scheme for multi-gateway wireless sensor networks based on elliptic curve cryptography," Ad Hoc Networks, vol. 127, pp. 102768, 2022.
[14] Y. Han, H. Hu, & 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.
[15] B. Pitchaimanickam, & G. Murugaboopathi, "A hybrid firefly algorithm with particle swarm optimization for energy efficient optimal cluster head selection in wireless sensor networks," Neural Computing and Applications, vol. 32, pp. 7709-7723, 2020.
[16] P. Joshi, & A. S. Raghuvanshi, "A multi-objective metaheuristic approach based adaptive clustering and path selection in iot enabled wireless sensor networks," International Journal of Computer Networks and Applications, vol. 8, no. 5, pp. 566-584, 2021.
[17] P. Kathiroli, & K. Selvadurai, "Energy efficient cluster head selection using improved Sparrow Search Algorithm in Wireless Sensor Networks," Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 10, pp. 8564-8575, 2022.
[18] R. Ramalingam, S. Basheer, P. Balasubramanian, M. Rashid, & G. Jayaraman, "EECHS-ARO: Energy-efficient cluster head selection mechanism for livestock industry using artificial rabbits' optimization and wireless sensor networks," Electronic Research Archive, vol. 31, no. 6, 2023.
[19] L. Yang, D. Zhang, L. Li, & Q. He, "Energy efficient cluster-based routing protocol for WSN using multi-strategy fusion snake optimizer and minimum spanning tree," Scientific Reports, vol. 14, no. 1, pp. 16786, 2024.
[20] H. Hu, Y. Han, M. Yao, & X. Song, "Trust based secure and energy efficient routing protocol for wireless sensor networks," IEEE access, vol. 10, pp. 10585-10596, 2021.
[21] V. Kavidha, & S. Ananthakumaran, "Novel energy-efficient secure routing protocol for wireless sensor networks with Mobile sink," Peer-to-Peer Networking and Applications, vol. 12, pp. 881-892, 2019.
[22] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy, & R. Patan, "Ant colony optimization-based quality of service aware energy balancing secure routing algorithm for wireless sensor networks. IEEE Transactions on Engineering Management, vol. 68, no. 1, pp. 170-182, 2019.
[23] E. P. K. Gilbert, K. Baskaran, E. B. Rajsingh, M. Lydia, & A. I. Selvakumar, "Trust aware nature inspired optimised routing in clustered wireless sensor networks," International Journal of Bio-Inspired Computation, vol. 14, no. 2, pp. 103-113, 2019.
[24] A. Saleh, P. Joshi, R. S. Rathore, & S. S. Sengar, "Trust-aware routing mechanism through an edge node for IoT-enabled sensor networks," Sensors, vol. 22, no. 20, pp. 7820, 2022.
[25] S. Hriez, S. Almajali, H. Elgala, M. Ayyash, & H. B. Salameh, "A novel trust-aware and energy-aware clustering method that uses stochastic fractal search in IoT-enabled wireless sensor networks," IEEE Systems Journal, vol. 16, no. 2, pp. 2693-2704, 2021.
[26] M. Hosseinzadeh, O. H. Ahmed, J. Lansky, S. Mildeova, M. S. Yousefpoor, E. Yousefpoor, & A. M. Rahmani, "A cluster-tree-based trusted routing algorithm using Grasshopper Optimization Algorithm (GOA) in Wireless Sensor Networks (WSNs)," Plos one, vol. 18, no. 9, pp. e0289173, 2023.
[27] Cherappa, V., Thangarajan, T., Meenakshi Sundaram, S. S., Hajjej, F., Munusamy, A. K., & Shanmugam, R. (2023). Energy-efficient clustering and routing using ASFO and a cross-layer-based expedient routing protocol for wireless sensor networks. Sensors, 23(5), 2788.
[28] Roberts, M. K., & Ramasamy, P. (2023). An improved high performance clustering based routing protocol for wireless sensor networks in IoT. Telecommunication Systems, 82(1), 45-59.
[29] Ramalingam, S., Dhanasekaran, S., Sinnasamy, S. S., Salau, A. O., & Alagarsamy, M. (2024). Performance enhancement of efficient clustering and routing protocol for wireless sensor networks using improved elephant herd optimization algorithm. Wireless Networks, 30(3), 1773-1789.
[30] Hu, H., Fan, X., & Wang, C. (2024). Energy efficient clustering and routing protocol based on quantum particle swarm optimization and fuzzy logic for wireless sensor networks. Scientific reports, 14(1), 18595.
[31] M. Ezhilarasi, L. Gnanaprasanambikai, A. Kousalya, & M. Shanmugapriya, "A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks," Soft Computing, vol. 27, no. 7, pp. 4157-4168, 2023.
[32] A. Pathak, I. Al-Anbagi, & H. J. Hamilton, "An adaptive QoS and trust-based lightweight secure routing algorithm for WSNs," IEEE Internet of Things Journal, vol. 9, no. 23, pp. 23826-23840, 2022.
[33] I. Ashraf, Y. Park, S. Hur, S. W. Kim, R. Alroobaea, Y. B. Zikria, & S. Nosheen, "A survey on cyber security threats in IoT-enabled maritime industry," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 2, pp. 2677-2690, 2022.
[34] Y. Fu, D. Liu, J. Chen, & L. He, "Secretary bird optimization algorithm: a new metaheuristic for solving global optimization problems," Artificial Intelligence Review, vol. 57, no. 5, pp. 1-102, 2024.

Authors

Mrs. Amsaveni Manigandan is a Research Scholar in the Department of Computer Science at P. K. R. Arts College for Women, Gobichettipalayam, Tamil Nadu, India.

Dr. M. Saranya is an Associate Professor in the Department of Computer Science at P. K. R. Arts College for Women, Gobichettipalayam, Tamil Nadu, India.

How to cite this article:

Amsaveni Manigandan, M. Saranya, "Secretary Bird Optimization with Differential Evolution (SBODE) and Trust Energy Aware Clustering Routing (TREACR) Protocol for Wireless Sensor Network (WSN)", International Journal of Computer Networks and Applications (IJCNA), 12(2), PP: 291-306, 2025, DOI: 10.22247/ijcna/2025/19.