SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I1P121

Volume 12 Issue 1, 211-221, January 2025

Original Article

Secure Clustering and Routing Based Multi Objective Walrus Optimization Algorithm for Wireless Sensor Networks

M. Venkata Krishna Rao[1], C. Atheeq[2]

[1,2]Department of Computer Science & Engineering, GITAM University, Telangana, India.

[1]Corresponding Author : venkat9965@gmail.com

Received: 16 November 2024 Revised: 18 December 2024 Accepted: 18 January 2025 Published: 25 January 2025

Abstract - *Wireless Sensor Networks (WSNs) contain many small automatic devices distributed by the area of interest where the wireless links transmit the gathered data. However, the WSN nodes are vulnerable to various security threats due to the nodes being positioned in open environments. This research proposes the Secured-Multi Objective Walrus Optimization Algorithm (S-MOWaOA) for secure clustering and routing in WSN. The secure Cluster Heads (CHs) are selected by using S-MOWaOA with less energy consumption, avoiding malicious nodes during the selection of CHs. Then, the clusters are generated using the potential function, while the routing is performed by S-MOWaOA. The optimum routes are chosen through S-MOWaOA with a shorter distance and enhanced network lifetime. The S-MOWaOA is determined with different key metrics namely, alive nodes, energy consumption, delay, throughput, Packet Delivery Ratio (PDR), and Packet Loss Ratio (PLR). The S-MOWaOA consumes a lesser energy of 3J for 1000 rounds, 6J for 2000 rounds, 8J for 3000 rounds, 12J for 4000 rounds, and 16J for 5000 rounds, proving to be more effective when compared to Tuna Swarm optimization and Fuzzy Control theory (TSFC).*

Keywords - *Multi objective, Routing, Secure cluster heads, Walrus optimization algorithm, Wireless Sensor Networks.*

1. Introduction

Wireless Sensor Networks (WSNs) are developed as simple monitoring systems that comprise numerous distributed sensor nodes for military applications and are focused on information gathering and transmission [1-3]. The recently developed applications in wireless communication, such as WSNs, have significant attention across different sectors, including healthcare, the Internet of Things (IoT), and so on [4, 5]. Primarily, sensors deployed in different applications are battery-powered with a limited lifespan [6]. Hence, there is a growing need for an appropriate method that enables effective data transmission while minimizing energy consumption [7]. The reliable method for attaining a good trade-off between computation overhead and energy utilization through organizing sensor nodes into groups is called clusters [8]. These clusters are accomplished through their respective members, called Cluster Heads (CHs), responsible for effective data transmission. Therefore, clustering is an essential process to ensure network scalability and network availability [9]. To achieve the clustering objectives, it is crucial to determine a much more reliable and effective route for data transmission [10]. In recent times, routing has been a generally adopted mechanism utilized for determining a much more effective route for reliable communication of data sources while employing respective Base Stations (BS) with less delay and energy consumption [11-14]. Based on recent research, it is seen that an effective utilization of the routing algorithm is established for enhancing the sensor node's lifespan with lesser energy consumption [15]. Hence, to prevent early energy exhaustion and manage the network's performance under dynamic conditions, effective clustering and routing mechanisms become significant solutions for WSN sustainability [16, 17]. There has been substantial growth in optimization algorithms as a solution for managing the effectiveness of WSNs by routing and energy management [18]. However, with the dynamic network, the traditional optimization algorithms have established their effectiveness in addressing the issue of multi-objectives related to energy constraints and real-time deployment [19, 20]. The significant contributions of the research are given as follows.The primary objective of this research is to develop the S-MOWaOA algorithm, which enhances energy efficiency and network security in WSNs by addressing the limitations of traditional clustering and routing methods through secure CH selection and optimal route discovery.

- The S-MOWaOA is proposed for selecting secure CHs from the clusters with various fitness functions. Choosing the secure CHs avoids malicious nodes during the selection process and reduces energy consumption.

- The S-MOWaOA-based optimal routing discovery is performed to select optimal routes for reliable data transfer and enhance the network's lifetime.

This study introduces the novel S-MOWaOA approach, which integrates secure CH selection and optimal routing discovery, addressing energy efficiency and network security more effectively than existing methods.This research paper is arranged as follows: Section 2 analyzes the recent year's research as the literature review. Section 3 provides the details of the proposed methodology, while Section 4 gives the results, discussion, and comparative analysis of the proposed methodology. The conclusion of this research is given in Section 5.

The introduction section has been revised to explicitly highlight the research gap by emphasizing the limitations of traditional optimization algorithms in addressing multi-objective issues like energy constraints and real-time deployment in dynamic WSN environments. Additionally, the problem is clearly introduced by focusing on the need for secure and energy-efficient clustering and routing mechanisms to enhance network sustainability.

2. Literature Review

In this section, the recent research in secure clustering and routing in WSN is discussed, along with its advantages and drawbacks.

Yao et al. [21] suggested the Tuna Swarm optimization and Fuzzy Control theory (TSFC) method for balancing the network energy and enhancing energy efficiency. The TSO was used for optimizing network clustering by considering the mean and standard deviation of distances, to enhance the compactness of the cluster architecture. Next, in the Cluster Head (CH) selection phase, the fuzzy controller to choose CHs was developed depending on the fuzzy control theory. The suggested method minimized and balanced the energy consumption by optimizing the selection of CH. However, the suggested algorithm had lesser PDR, which led to a loss of data packets in transmission due to high network density.

Roberts et al. [22] presented the integration of two meta-heuristic algorithms, Sail Fish Optimization (SFO) and Spotted Hyena Optimization (SHO), for clustering and routing in WSN. The exploration of the SFO algorithm was used for an effective clustering and optimum selection of CH. Then, the exploitation capability of the SHO algorithm was utilized to optimize the effective routing paths. The presented method significantly enhanced the network lifetime and PDR. The presented method did not consider the integrity factor, which led to security threats and increased network congestion.

Jing [23] introduced the Harris Harks Optimization Clustering with Fuzzy Routing (HHOCFR) to improve the network lifetime. The HHO algorithms were used to select the effective CHs and generate the optimum clusters through the novel encoding mechanism. Then, the Fuzzy Logic System (FLS) considered the residual energy, alongside the energy consumption of clusters, to overcome the hot spot issue. The introduced method maintained the clusters that minimized the network energy consumption. The introduced algorithm faced high packet loss that increased the network delay due to the retransmission of packets.

Han et al. [24] employed the energy and trust-based routing protocol utilizing an Adaptive Genetic Algorithm named TAGA. The TAGA developed the trust values of nodes depending on the values of direct trust and those of indirect trust with a filtering mechanism. The threshold function was utilized for choosing the optimum CHs that considered the node's dynamic changes, trust values and residual energy. At last, GA was employed for identifying an optimum, secure routing for CHs. The employed method failed to consider the node degree fitness function, which resulted in a short network lifetime because of the high energy consumption.

Dinesh and Kumar [25] deployed Honey Badger Optimization (HBO) to choose the CHs that optimized the network energy consumption. The Remora Optimization (RO) algorithm was assigned to finding the optimum path during network routing. Additionally, the protocol employed the Identify-based Digital Signature with Conditional Privacy Preservation Algorithm (IDS-CPPA) for formulating an effective authentication between nodes in the network. The method exhibited lesser performance in identifying the shortest path due to its high energy consumption.

The proposed SPAR-SSO [26] protocol integrates security-aware routing with power-efficient mechanisms using Salp Swarm Optimization (SSO) to optimize network performance, enhance Packet Delivery Ratio (PDR), and reduce end-to-end delays in WSNs. However, while SPAR-SSO effectively minimizes energy consumption, it does not address network scalability challenges or dynamic node mobility, which could impact performance in larger, highly dynamic networks.

Neuro-fuzzy-based clustering with Sparrow Search Optimization Algorithm (NF-SSOA) [7] enhances WSN performance by enabling energy-efficient, trust-aware clustering and secure routing. Utilizing ECC-based digital signatures and anonymous authentication improves energy consumption, throughput, and PDR. However, challenges like increased computational complexity and scalability issues remain, highlighting the need for further optimization in dynamic networks.

The analysis of recent research shows that the existing algorithms have less PDR, do not consider the distance among the nodes and node degree, and struggle with high packet loss and energy consumption. This proposed S-MOWaOA-based dynamic network considers the fitness functions of distance among nodes, distance between BS and CH, node degree, trust value and integrity factor. Considering these fitness functions, the S-MOWaOA effectively minimizes energy consumption and selects the optimal secure CHs.

3. Proposed Methodology

This research proposes the Secured-Multi Objective Walrus Optimization Algorithm (S-MOWaOA) for secure clustering and routing in WSN. The secure CHs are chosen using S-MOWaOA with different fitness functions like distance among nodes, distance between BS and CH, node degree, trust value and integrity factor. Then, the clusters are formed, and optimal paths are selected by S-MOWaOA with energy and distance fitness functions. The process of S-MOWaOA-based clustering and routing is depicted in Figure 1.

The secure Cluster Heads (CHs) in the S-MOWaOA algorithm are selected using a combination of fitness functions, including node-to-node distance, distance to the base station, node degree, trust value, and integrity factor. These metrics collectively ensure optimal CH selection by evaluating energy efficiency, connectivity, and security, enhancing overall network performance.

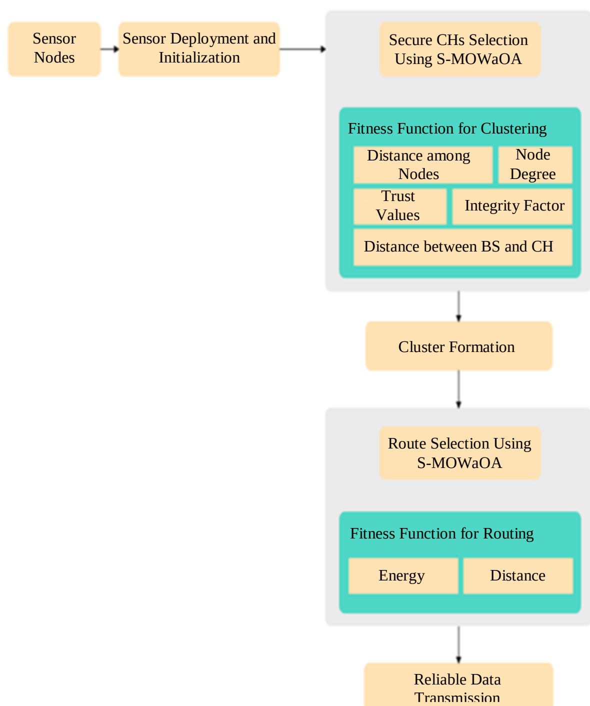

Fig. 1 Process of S-MOWaOA-based clustering and routing

3.1. Sensor Deployment

In dynamic networks, the sensor nodes are initially randomly positioned in the network. Then, the secure optimal CHs and routes are chosen through S-MOWaOA to facilitate secure, reliable data transmission in the network. This method dynamically chooses the optimal CHs and routes, which ensures efficient communication by changing the network conditions. This dynamic strategy helps for robust and reliable data transmission in the network.

3.2. Secure CHs Selection Using S-MOWaOA

The S-MOWaOA selects the secure best CHs from clusters to attain a secured data transmission in the network. The S-MOWaOA avoids malicious nodes during the selection of CHs. The S-MOWaOA selects the CHs from the network by utilizing five fitness functions: distance between neighbor nodes, the distance between BS and CH, node degree, integrity factor and trust values. The process of selecting secure CHs is explained in the sections below.

3.2.1. Representation

In the process of secure CHs selection, the population dimension is the same as the number of CHs in WSN. It is considered that $x_i = x_i^1, x_i^2, \dots, x_i^n$ is the ith population,, where each position $x_i^d = (a_i^a, a_i^d)$ represents the nodes and is mapped to their 2D dimension in the network.

3.2.2. Exploration Phase (Feeding Strategy)

Walruses contain varied diets and feed on sixty species of marine organisms like soft corals, tunicates, sea cucumbers, shrimp, tube worms and different mollusks. Walruses initially desire benthic bivalve mollusks, specifically clams. They forage through grazing on the sea floor using their sensitive vibrissae and energetic flipper movements to seek out and detach their food. During the search process, the strongest walrus with the highest tusks guide various walruses in a set for identifying the food. Hence, a good candidate solution with the best value for fitness function is considered the strongest walrus in the set. The behaviour of search in walruses causes various scanning spaces of search space that enhance the exploration capability of WaOA in global search. The updation process of the position of walruses is modelled depending on the feeding mechanism with the guidance of many essential group members. The new position of the walrus is initially produced by using Equation (1). Then, this position is replaced by the past position when the value of the fitness function is enhanced, as given in Equation (2),

$$x_{i,j}^{P_1} = x_{i,j} + rand_{i,j} \cdot (SW_j - I_{i,j} \cdot x_{i,j}) \tag{1}$$

$$X_i = \begin{cases} X_i^{P_1}, F_i^{P_1} < F_i \\ X_i, \ else, \end{cases} \tag{2}$$

In the above Equations (1) and (2), the $X_i^{P_1}$ represents the newly generated location for ith walrus depending on the first stage, $x_{i,j}^{P_1}$ represents the jth dimension, $F_i^{P_1}$ represents the value of fitness function, the $rand_{i,j}$ denotes the random number between the range [0,1], SW_j signifies the strongest walrus with a good value of fitness function and the $I_{i,j}$ denotes the integers chosen randomly as 1 or 2.

3.2.3. Migration

The natural behaviour of the walruses is its migration for outcrops because of air warming in late summer. The migration process in WaOA is assigned to guide the walruses through the search space, which also aids in finding an appropriate field in the search space. This model assumes that every walrus migrates to other walrus locations in the search space. The mathematical expressions for the behavior mechanism are given in Equations (3) and (4). The new location is initially generated using Equation (3), and then by Equation (4), the new location enhances the fitness function value that replaces the past position of the walrus.

$$x_{i,j}^{P_2} = \begin{cases} x_{i,j} + rand_{i,j} \cdot (x_{k,j} - I_{i,j} \cdot x_{i,j}), & F_k < F_i \\ x_{i,j} + rand_{i,j} \cdot (x_{i,j} - x_{k,j}), & else, \end{cases} \quad (3)$$

$$X_i = \begin{cases} X_i^{P_2}, & F_i^{P_2} < F_i \\ X_i, & else \end{cases} \quad (4)$$

In the above Equations (3) and (4), $X_i^{P_2}$ represents the newly generated location for ith walrus depended on the second stage, $x_{i,j}^{P_2}$ represents the jth dimension, $F_i^{P_2}$ signifies their value of fitness function, the $x_{k,j}$ signifies their jth dimension, and the F_k is the value of the fitness function.

3.2.4. Exploitation Phase (Escaping and Fighting against the Predators)

The walruses are always exposed to attacks by polar bears and killer whales. The escaping strategy and fighting the predators cause changes in the location of walruses in the locality in which they are positioned. By this, the natural behavior of walruses enhances the exploration ability of WaOA in local search in the issue-solving space around the candidate solutions.

To simulate this phenomenon in WaOA, the neighborhood is employed around every walrus, which initially generates a new location in the neighborhood by utilizing Equations (5) and (6). Next, the fitness function value is enhanced, while the new location replaces the past location as a numerically formulated Equation (7).

$$x_{i,j}^{P_3} = x_{i,j} + \left(lb_{local,j}^t + \left(ub_{local,j}^t - rand \cdot lb_{local,j}^t\right)\right) \quad (5)$$

$$Local\ bounds: \begin{cases} lb_{local,j}^t = \frac{lb_j}{t} \\ ub_{local,j}^t = \frac{ub_j}{t} \end{cases} \quad (6)$$

$$X_i = \begin{cases} X_i^{P_3}, F_i^{P_3} < F_i \\ X_i, & else \end{cases} \quad (7)$$

In the above Equations (6) and (7), $X_i^{P_3}$ denote the newly generated location for ith the walrus depending on the third stage, $x_{i,j}^{P_3}$ denote the jth dimension, $F_i^{P_3}$ represent the fitness function value, t signify the iteration, $lb_{local,j}^t$ and $ub_{local,j}^t$ signify the local lower and local upper bound of jth the variable, lb_j and the ub_j are the lower and upper bounds of jth the variable for simulating local search in the neighborhood of the candidate solutions.

3.2.5. Fitness Function for CHs Selection

The fitness functions for choosing the CHs are the distance between the neighbor nodes (CH_{F1}), the distance between BS and CH (CH_{F2}), the node degree (CH_{F3}), trust values (CH_{F4}) and the integrity factor CH_{F5}. The mathematical formulation of the fitness function (CH_{FF}) is given in Equation (8).

$$CH_{FF} = \gamma_{F1} \times CH_{F1} + \gamma_{F2} \times CH_{F2} + \gamma_{F3} \times CH_{F3} + \gamma_{F4} \times CH_{F4} + \gamma_{F5} \times CH_{F5} \quad (8)$$

In Equation (8) γ_n represents the weight values of respective fitness functions. The value γ_{F1} is 0.35, the value of γ_{F2} is 0.24, the value of γ_{F3} is 0.12, the value of γ_{F4} is 0.11, and the value of γ_{F5} is 0.18. The weight values of fitness functions fall in a different range, acquired by normalizing the weight values of fitness functions, further normalizing to a certain uniform range. In this research, the min-max normalization technique is used to normalize the weight values of fitness functions. A detailed explanation of fitness functions is given below.

3.2.6. Distance between Neighbor Nodes

The distance between neighbor nodes defines the range between normal nodes and their respective CHs. The energy dissolution for the node is majorly based on the distance of the transmission route. If the selected node is closer to the BS and has a shorter transmission distance, the energy consumption is lesser. This is considered the first fitness function for CH selection, and its mathematical formulation is given in Equation (9).

$$CH_{F1} = \sum_{j=1}^{m} \sum_{i=1}^{I_j} D(S_i, CH_j/I_j) \quad (9)$$

The above Equation (9) $D(S_i, CH_j/I_j)$ represents the distance between sensor nodes, S_i denotes the sensor, CH_j represents the distance of CH, and I_j denotes the quantity of sensor belonging to CH.

3.2.7. Distance between BS and CH

The node's energy consumption is analyzed depending on the distance through the transmission route. When the BS is located away from the CHs, data transmission requires high energy. As an outcome, the sudden drop in CHs is because of the increased energy usage. The node nearer to the BS is chosen as the throughput data transfer. This is considered the second fitness function for the CH's selection, and its mathematical formulation is given in Equation (10).

$$CH_{F2} = \sum_{i=1}^{m} D\left(CH_j, BS\right) \quad (10)$$

The above Equation (10) the $D\left(CH_j, BS\right)$ represents the distance between the CH_j and BS.

3.2.8. Node Degree

The node degree defines how many sensor nodes every CH contains. The CHs with many cluster members lose their energy for a shorter time, so the CHs with few sensors are selected. The node degree is the third fitness function, and its mathematical formulation is given in Equation (11).

$$CH_{F3} = \sum_{i=1}^{m} I_i \quad (11)$$

The above Equation (11) I_i represents the number of CH_i sensor nodes.

3.3. Security Aspects for WSN

3.3.1. Trust Value

The trust value is utilized for evaluating the node trust. In this research, three kinds of trust, namely, direct $T_{i,j}^{direct}$, indirect $T_{i,j}^{indirect}$ and recent $T_{i,j}^{recent}$ trust, are utilized. Initially, when transmission is initialized in nodes, trust is set to a maximum. This is considered the fourth fitness for CH selection, and its mathematical formulation is given in Equation (12).

$$CH_{F4} = T_{i,j}^{direct} + T_{i,j}^{indirect} + T_{i,j}^{recent} \quad (12)$$

Direct Trust

It is based on the deviation in the actual and estimated time, and this execution is dependent on the witness factor, which contributes more to the improvement of node trust. The mathematical formulation for the direct trust is given in Equation (13).

$$T_{i,j}^{direct}(t) = \frac{1}{3}\left[T_{i,j}^{direct}(t-1) - \left[\frac{T^{key} - E^{key}}{T^{key}}\right] + \omega\right] \quad (13)$$

The above Equation (13) T^{key} represents the relevant time needed for sending the key, E^{key} denotes an expected time to receive the key, and ω represents the witness factor for jth dimensions.

Indirect Trust

It defines the worthiness of trust for nodes, and mathematical formulation for measuring the indirect trust of nodes is given in Equation (14).

$$T_{i,j}^{indirect}(t) = \frac{1}{N}\sum_{i=1}^{N} T_{i,x}^{indirect}(x) \quad (14)$$

The above Equation (14) N denotes the total number of neighbor nodes in the ith node.

Recent Trust

It is executed as node regression of indirect and direct trust of nodes in the network. The mathematical formulation for recent trust is given in Equation (15).

$$T_{i,j}^{recent}(t) = \alpha \times T_{i,j}^{direct}(t) + (1-\alpha) \times T_{i,j}^{indirect}(t) \quad (15)$$

In the above Equation (15), $\alpha = 0.3$.

3.3.2. Integrity Factor

When the data packet is transferred to the neighbor node, the source node monitors whether the data packet is delayed. It also verifies whether the data packet is transferred within a particular time and ensures the integrity and accuracy of data. This is considered the fifth fitness function, and its mathematical formulation is given in Equation (16).

$$CH_{F5} = \frac{U^z(k,k+1)}{E^z(k,k+1)} \quad (16)$$

In the above Equation (16) $U^z(k, k+1)$ represents the amount of fully forwarded packets and $E^z(k, k+1)$ signifies the number of packets forwarded.

3.4. Cluster Formation

The selected optimal secure CHs by S-MOWaOA are given to the sensor nodes. In the previous research, the selected CH are not appropriate in terms of energy, connectivity, and so on. Because the clusters are already formed, the options for CH are limited to the members of every cluster. If the chosen CH is inappropriate, it leads to high communication overhead and minimized network effectiveness.

In this research, by choosing the appropriate CH at first, the network ensures that the CH handles the additional load. This process reduces the communication overhead and enhances the overall performance and lifetime of the network. The sensor nodes with less transmission distance and high residual energy are employed for the CHs. The mathematical formulation for cluster formation using potential function is given in Equation (17).

$$Potential\ Function = \frac{z \times E\left(CH_j\right)}{D\left(s_i, CH_j\right)} \quad (17)$$

In the above Equation (17) z represents the proportionality constant, $D\left(s_i, CH_j\right)$ signifies the distance between the sensor and cluster head, and $E\left(CH_j\right)$ represents the residual energy of CH. The distance between two CHs and sensor nodes is equal, and the sensor is merged to CHs with high energy.

3.5. Routing Using S-MOWaOA

The optimal routes for data transmission are chosen by S-MOWaOA. The S-MOWaOA effectively perform both clustering and routing and improves the performance of the network. The S-MOWaOA guarantees optimum CH selection and balances the cluster formation by minimizing energy consumption and maximising the network lifetime. Then, it optimizes the routes to minimize the communication overhead and adapts to the dynamic network conditions.

3.5.1. Representation

In the process of routing, the dimension of every population is dependent on the number of nodes if it is considered $x_i = x_i^1, x_i^2, \dots, x_i^n$ the ith population, where every population dimension $x_i^1 = (0,1)$ is randomly initialized. The main aim is to choose the neighbor's optimum path from every node to the BS.

The fitness functions used for routing are distance and energy. The optimized node is chosen from routing to generate the paths from nodes to BS. After generating the path from source to destination, the source node transfers data to the destination. The mathematical formulation for the fitness function of routing is given in Equation (18).

$$RF = \delta_1 \times \sum_{i=1}^{m} D(CH_j, BS) + \delta_2 \times \sum_{i=1}^{m} \frac{1}{CH_j} \tag{18}$$

In the above Equation (18), δ_1 and δ_2 represents the weight values of distance and energy fitness function. The value of δ_1 is 0.5 and the value of δ_2 is 0.5. The S-MOWaOA is deployed to elevate network security by securing nodes at every communication level. Further, routing is performed to attain reliable data transmission. Hence, the S-MOWaOA attains high PDR and less energy consumption.

3.6. CH Maintenance

The CHs handle more communication and data broadcasting than the regular nodes, which degrade their energy quickly. Regular CH maintenance ensures that the CHs are replaced before their energy is exhausted, which prevents the partitioning of the network and maximizes the network lifetime. In S-MOWaOA, after the first round, the maintenance mechanism monitors the running of every cluster.

Once the CH residual energy is lesser than the average energy of every node in the cluster, the node with a higher ratio of residual energy to the distance to the centroid is rotated as the cluster CH. The message is then transmitted to the neighbor CHs, and each neighbor CH determines whether an update is required for its corresponding relays. If no update is needed, the CH continues its role as a CH and completes the data transmission process.

4. Experimental Results

This section describes the results, discussion and comparative analysis of the proposed S-MOWaOA, simulated using MATLAB 2018a with a system configuration of i5 processor, 8GB RAM and Windows 10 OS. The Distributed Energy-Efficient Clustering (DEEC), Low-Energy Adaptive Clustering Hierarchy (LEACH), Threshold DEEC (TDEEC), Developed DEEC (DDEEC) and Centralized LEACH (CLEACH) are considered for the analysis.

The key metrics used for evaluating the S-MOWaOA are alive nodes, energy consumption, delay, Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR) and throughput. The simulation parameters used for evaluation are described in Table 1.

The experimental setup involves simulating the S-MOWaOA in MATLAB R2022a. The network area is set to 100 × 100 m² with 100 nodes deployed randomly. Parameters such as the initial energy of nodes (2J), transmission range, and BS location are predefined. The simulation considers energy consumption, Packet Delivery Ratio (PDR), and network lifetime performance metrics.

Assumptions include uniform energy distribution and static BS. Limitations include idealized conditions, excluding external interference, and potential scalability issues for larger networks.

Table 1. Simulation parameters of S-MOWaOA

Parameters	Values
Simulation Area	200 x 200
Number of Nodes	50, 100, 150
Initial Energy	0.5 J
Mobility	Random Mobility Point
Number of Packets	4000

4.1. Alive Node Analysis

The number of alive nodes is an essential metric utilized to represent the durability of network nodes and process effectiveness. This reflects the ability of the network to perform its processes over time before the energy of nodes in cluster depletion. The performance evaluation of alive nodes and their comparison is described in terms of the number of rounds for 50 and 100 nodes and is given in Figures 2 and 3.

Figures 2 and 3 show that the S-MOWaOA maintains a high number of alive nodes by varying number of nodes when compared with DEEC, LEACH, TDEEC, DDEEC and CLEACH. This represents that the S-MOWaOA helps maintain the node energy, which extends the network lifetime.

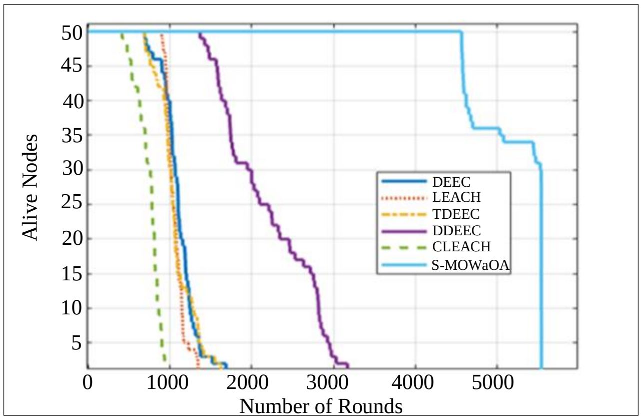

Fig. 2 Alive nodes for 50 nodes

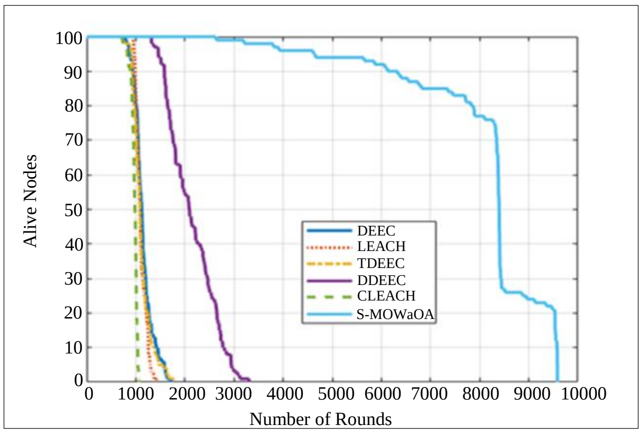

Fig. 3 Alive nodes for 100 nodes

4.2. Energy Consumption Analysis

Energy consumption has a high influence on the lifetime of the network. The performance evaluation of energy consumption and their comparison is described in terms of the number of rounds for 50 and 100 nodes, as illustrated in Figures 4 and 5. Figures 4 and 5 show that the S-MOWaOA consumes lesser energy by varying nodes when compared with DEEC, LEACH, TDEEC, DDEEC and CLEACH. The residual energy in S-MOWaOA remains at a high level, that the S-MOWaOA efficiently minimizes the network energy consumption and extends the network's lifetime.

4.3. Delay Analysis

Delay is the essential metric utilized to analyze the duration of time taken by data packets to complete transmission from the source node to the destination. The performance evaluation of delay and their comparison is described in terms of the number of rounds for 50 and 100 nodes and is given in Figures 6 and 7. Figures 6 and 7 show that the S-MOWaOA consumed less time duration by varying nodes when compared with DEEC, LEACH, TDEEC, DDEEC and CLEACH. This minimization in delay represents that the S-MOWaOA effectively manages data communication and network congestion compared to existing algorithms.

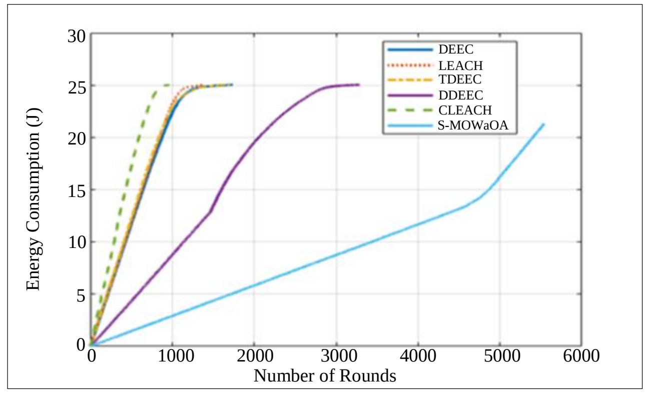

Fig. 4 Energy consumption for 50 nodes

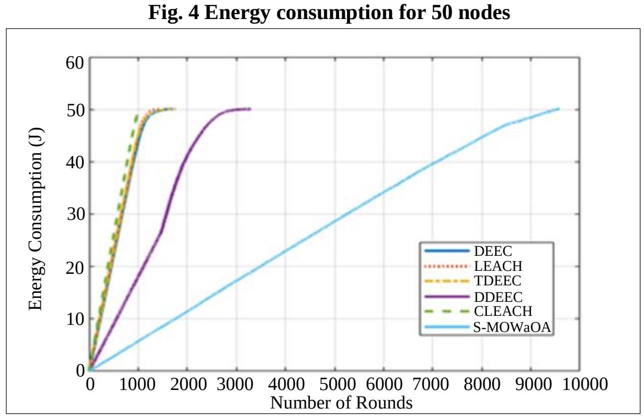

Fig. 5 Energy consumption for 100 nodes

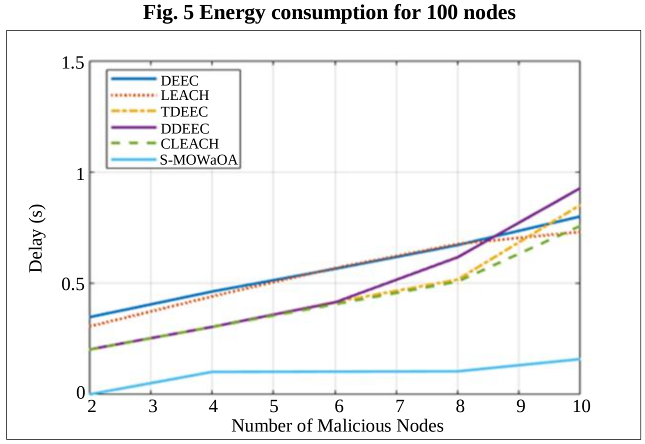

Fig. 6 Delay for 50 nodes

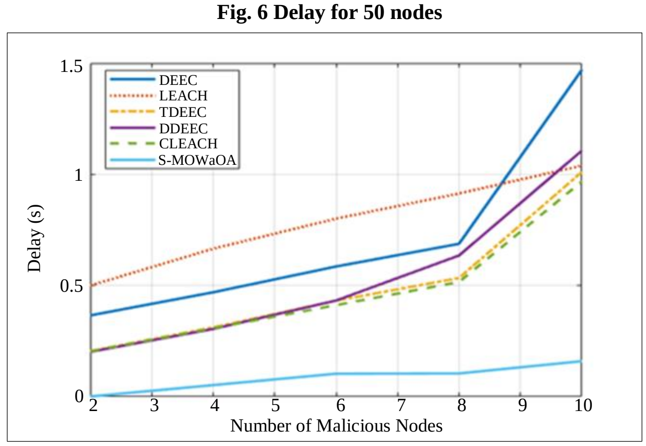

Fig. 7 Delay for 100 nodes

4.4. PDR and PLR Analysis

The PDR is an essential metric that plays a significant role in determining the overall effectiveness and reliability of data transmission. The high PDR helps calculate the reliability and performance of the network through error-free transmission of data packets to the destination. The performance evaluation of PDR and PLR and their comparison are described in terms of 50 and 100 nodes, as illustrated in Figures 8 and 9. From Figures 8 and 9, the S-MOWaOA is seen to obtain both high PDR and less PLR with varying numbers of nodes when compared with DEEC, LEACH, TDEEC, DDEEC and CLEACH. These consistent increments in S-MOWaOA for different nodes effectively facilitate reliable data transmission.

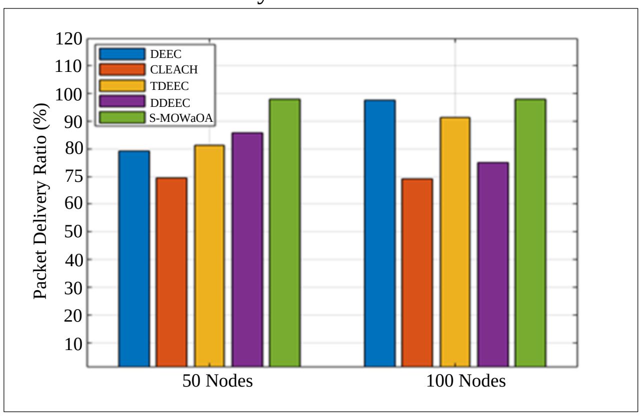

Fig. 8 PDR vs Number of nodes

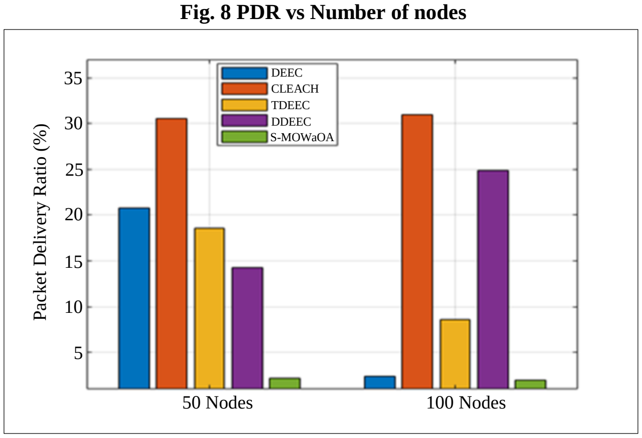

Fig. 9 PLR vs Number of nodes

4.5. Throughput Analysis

Throughput is an essential metric used to measure the rate at which the network completes data packet transmission to the destination without any redundancy. The S-MOWaOA obtains a high throughput that enhances their coverage and feasibility in handling high loads of data. The performance evaluation of throughput and their comparison is described in terms of 50 and 100 nodes, as depicted in Figure 10. From Figure 10, the S-MOWaOA obtains high throughput with varying numbers of nodes when compared to DEEC, LEACH, TDEEC, DDEEC and CLEACH. This improvement by S-MOWaOA enhances the load balancing and efficiency of data transmission in the network. The result analysis highlights the superior performance of S-MOWaOA in terms of key metrics such as energy consumption, network lifetime, and throughput compared to existing algorithms. These findings imply that S-MOWaOA is well-suited for real-world applications where energy efficiency and reliable data transmission are critical, such as IoT-based monitoring systems and smart agriculture. The inclusion of visual aids like comparative graphs and detailed tables in the analysis improves data interpretability and helps demonstrate the practical advantages of the proposed approach.

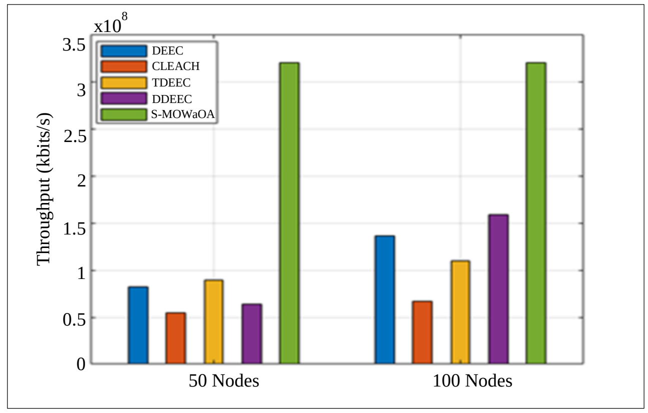

Fig. 10 Throughput vs Number of nodes

The performance metrics-energy consumption, Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), delay, and throughput-were selected because they directly reflect the critical aspects of a Wireless Sensor Network (WSN). Energy consumption is vital as it affects the network's lifetime, while PDR and PLR evaluate the reliability of data transmission. Delay assesses the efficiency of data communication, and throughput measures the system's capacity to handle high data loads. These metrics provide a comprehensive understanding of the network's performance, ensuring that the proposed S-MOWaOA approach effectively optimizes these key factors.

4.6. Comparative Analysis

The performance of S-MOWaOA is contrasted against that of the existing algorithms, TSFC [21], SFO and SHO [22] and HHOCFR [23] with different scenarios, and is tabulated in Table 2. In Table 2, the simulation parameters of TSFC [21] are represented as scenario 1, and these parameters are compared with S-MOWaOA, as described in Table 3. The simulation parameters of SFO and SHO [22] are represented as scenario 2, displaying a comparative analysis of S-MOWaOA in Table 4. The simulation parameters of HHOCFR [23] are represented as scenario 3 and are compared with S-MOWaOA, which is described in Table 5. The model, by considering the fitness functions of trust values, node degree, and distances, selects optimal, secure CHs with less energy consumption and avoids malicious nodes. Then, the optimal routes are chosen for data transmission with less delay and maximized network lifetime. The S-MOWaOA outperforms the existing algorithms TSFC [21], SFO and SHO [22] and HHOCFR [23] in terms of clustering and routing.

Table 2. Specification of different scenarios

Parameters	Scenario 1	Scenario 2	Scenario 3
Area	150m x 150 m	1000m x 1000m	100m x 100m
Initial energy	0.5J	1J	1J
Number of nodes	100, 200	1000	100
Packet size	4000 bits	4000 bits	4000 bits

Table 3. Comparing with TSFC [21]

Performance Metrics	Methods	Number of rounds				
		200	400	600	800	1000
Residual energy (J)	TSFC [21]	44.2	33.9	25.1	14.9	5.0
	Proposed S-MOWaOA	49.62	48.99	48.42	47.82	47.26
Energy consumption (J)	TSFC [21]	0.043	0.043	0.043	0.043	0.043
	Proposed S-MOWaOA	0.025	0.038	0.039	0.039	0.040
Alive nodes	TSFC [21]	100	100	100	100	100
	Proposed S-MOWaOA	100	100	100	100	100

Table 4. Comparing with SFO and SHO [22]

Performance Metrics	Methods	Number of rounds				
		1000	2000	3000	4000	5000
Residual energy (J)	SFO and SHO [22]	0.73	0.55	0.43	0.28	0.15
	Proposed S-MOWaOA	4.85	4.29	4.10	3.95	3.50
Alive nodes	SFO and SHO [22]	820	570	250	0	0
	Proposed S-MOWaOA	900	600	350	200	50

Table 5. Comparing with HHOCFR [23]

Performance Metrics	Methods	Number of rounds				
		200	400	600	800	1000
Alive nodes	HHOCFR [23]	100	100	100	100	100
	Proposed S-MOWaOA	100	100	100	100	100
Energy consumption (J)	HHOCFR [23]	12	23	34	46	58
	Proposed S-MOWaOA	1.13	2.27	3.43	4.58	5.75

4.7. Discussion

The outcomes of the S-MOWaOA algorithm are compared with those of the existing methods such as DEEC, LEACH, TDEEC, DDEEC and CLEACH. The S-MOWaOA has lesser energy of 3J for 1000 rounds, 6J for 2000 rounds, 8J for 3000 rounds, 12J for 4000 rounds and 16J for 5000 rounds when compared to the existing methods. The existing algorithms of TSFC [21], SFO and SHO [22] and HHOCFR [23] are compared with the S-MOWaOA, and these existing algorithms have drawbacks of lesser PDR, not considering the distance among the nodes and node degree, high packet loss and energy consumption. This research proposes the S-MOWaOA in dynamic networks, considering the fitness functions of distance among nodes, distance between BS and CH, node degree, trust value and integrity factor. By considering these fitness functions, the S-MOWaOA effectively minimizes energy consumption and selects the optimal secure CHs. Then, clusters are generated by using the potential function while the optimal routes are selected with a high network lifetime.Future work could focus on adapting the S-MOWaOA algorithm to dynamic environments with node mobility and fluctuating conditions, optimizing routing decisions for large-scale networks. Incorporating real-time factors like network congestion and machine learning techniques could further enhance efficiency and resilience for applications in IoT and smart cities.

5. Conclusion

This research proposes the S-MOWaOA for secure clustering and routing in WSN. The secure CHs are selected by using S-MOWaOA with less energy consumption while avoiding malicious nodes during CHs selection. Then, the clusters are generated using the potential function, and the routing is performed by S-MOWaOA. The optimum routes are chosen through S-MOWaOA with shorter distances and enhanced lifetime of the network. The S-MOWaOA is determined using different key metrics, including the alive nodes, energy consumption, delay, throughput, PDR, and PLR. The S-MOWaOA consumes less energy of 3J for 1000 rounds, 6J for 2000 rounds, 8J for 3000 rounds, 12J for 4000 rounds, and 16J for 5000 rounds, which is effective when compared to the TSFC. In the future, the hybrid optimization algorithm can be used for clustering and routing to further enhance network lifetime.

References

[1] Aljapur Vinitha, M.S.S. Rukmini, and Dhirajsunehra, "Secure and Energy Aware Multi-Hop Routing Protocol in WSN Using Taylor-Based Hybrid Optimization Algorithm," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 5, pp. 1857-1868, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] B.S. Venkatesh Prasad, and H.R. Roopashree, "Energy Aware and Secure Routing for Hierarchical Cluster through Trust Evaluation," *Measurement: Sensors*, vol. 33, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Anil Kumar Jemla Naik, Manjunatha Parameswarappa, and Mohan Naik Ramachandra, "Multiobjective, Trust-Aware, Artificial Hummingbird Algorithm-Based Secure Clustering and Routing with Mobile Sink for Wireless Sensor Networks," *Electronics and Telecommunications Research Institute Journal*, vol. 46, no. 6, pp. 950-964, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] A. Saravanaselvan, and B. Paramasivan, "FFBP Neural Network Optimized with Woodpecker Mating Algorithm for Dynamic Cluster-Based Secure Routing In WSN," *Institution of Electronics and Telecommunication Engineers Journal of Research*, vol. 70, no. 7, pp. 6515-6524, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Y.P. Makimaa, and R. Sudarmani, "Secured Routing Protocol for Improving the Energy Efficiency in WSN Applications," *Institution of Engineering and Technology Circuits, Devices and Systems*, vol. 2024, no. 1, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] G. Kiran Kumar et al., "An Optimized Meta-Heuristic Clustering-Based Routing Scheme for Secured Wireless Sensor Networks," *International Journal of Communication Systems*, vol. 37, no. 1, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] K. Dinesh, and, S.V.N. Santhose 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. [CrossRef] [Google Scholar] [Publisher Link]

[8] K. Dinesh, and, S.V.N. Santhose Kumar, "GWO-SMSLO: Grey Wolf Optimization-Based Clustering with Secured Modified Sea Lion Optimization Routing Algorithm in Wireless Sensor Networks," *Peer-to-Peer Networking and Applications*, vol. 17, no. 2, pp. 585-611, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Shashank Singh, Veena Anand, and Sonal Yadav, "Trust-Based Clustering and Routing in WSNs Using DST-WOA," *Peer-to-Peer Networking and Applications*, vol. 17, no. 3, pp. 1486-1498, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] S. Kishore Verma et al., "Energy Efficient Multi-Objective Cluster-Based Routing Protocol for WSN Using Interval Type-2 Fuzzy Logic Modified Dingo Optimization," *Peer-to-Peer Networking and Applications*, vol. 17, no. 4, pp. 1934-1962, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Mehdi Hosseinzadeh et al., "A Cluster-Based Trusted Routing Method Using Fire Hawk Optimizer (FHO) In Wireless Sensor Networks (Wsns)," *Scientific Reports*, vol. 13, no. 1, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] I. Adumbabu, and K. Selvakumar, "Energy Efficient Routing and Dynamic Cluster Head Selection Using Enhanced Optimization Algorithms for Wireless Sensor Networks," *Energies*, vol. 15, no. 21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] S.M. Udhaya Sankar, Mary Subaja Christo, and P.S. Uma Priyadarsini, "Secure and Energy Concise Route Revamp Technique in Wireless Sensor Networks," *Intelligent Automation and Soft Computing*, vol. 35, no. 2, pp. 2337-2351, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Maha Ebrahim Al-Sadoon, Ahmed Jedidi, and Hamed Al-Raweshidy, "Dual-Tier Cluster-Based Routing in Mobile Wireless Sensor Network for Iot Application," *IEEE Access*, vol. 11, pp. 4079-4094, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Deep Kumar Bangotra et al., "A Trust Based Secure Intelligent Opportunistic Routing Protocol for Wireless Sensor Networks," *Wireless Personal Communications*, vol. 127, no. 2, pp. 1045-1066, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Pawan Singh Mehra, "E-FUCA: Enhancement in Fuzzy Unequal Clustering and Routing for Sustainable Wireless Sensor Network," *Complex and Intelligent Systems*, vol. 8, no. 1, pp. 393-412, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] J. Paruvathavardhini, and B. Sargunam, "Stochastic Bat Optimization Model for Secured WSN with Energy-Aware Quantized Indexive Clustering," *Journal of Sensors*, vol. 2023, no. 1, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Aditya Pathak, Irfan Al-Anbagi, and Howard 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. [CrossRef] [Google Scholar] [Publisher Link]

[19] Pankaj Kumar Sharma, and Uma Shankar Modani, "Trusted Cluster-Based Communication for Wireless Sensor Network Using Meta-Heuristic Algorithms," *Computer Systems Science and Engineering*, vol. 45, no. 2, pp. 1935-1951, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Yuan Xiaogang, "Secure Low-Energy Routing Protocol Based on Dynamic Trust Awareness and Load Balancing in Wireless Sensor Networks," *Security and Communication Networks*, vol. 2023, no. 1, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Yin-Di Yao et al., "Clustering Routing Protocol Based on Tuna Swarm Optimization and Fuzzy Control Theory in Wireless Sensor Networks," *IEEE Sensors Journal*, vol. 24, no. 10, pp. 17102-17115, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] Michaelraj Kingston Roberts, Jayapratha Thangavel, and Hamad 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. [CrossRef] [Google Scholar] [Publisher Link]

[23] Di Jing, "Harris Harks Optimization Based Clustering with Fuzzy Routing for Lifetime Enhancing in Wireless Sensor Networks," *IEEE Access*, vol. 12, pp. 12149-12163, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[24] Youjia Han, Huangshui Hu, and Yuxin 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. [CrossRef] [Google Scholar] [Publisher Link]
[25] K. Dinesh, and S.V.N. Santhosh Kumar, "HBO-SROA: Honey Badger Optimization-Based Clustering with Secured Remora Optimization-Based Routing Algorithm in Wireless Sensor Networks," *Peer-to-Peer Networking and Applications*, vol. 17, no. 5, pp. 2609-2636, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[26] Abdullah Alghamdi et al., "Security and Energy Efficient Cyber-Physical Systems Using Predictive Modeling Approaches in Wireless Sensor Network. Wireless Networks," vol. 30, no. 6, pp. 5851-5866, 2024. [CrossRef] [Google Scholar] [Publisher Link]