SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I1P114

Volume 12 Issue 1, 151-162, January 2025

Original Article

Secure and Energy Efficient Clustering and Routing Scheme Using Multi-Objective Trust-Aware Golf Optimization Algorithm in Wireless Sensor Network

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: 10 November 2024 Revised: 12 December 2024 Accepted: 14 January 2025 Published: 25 January 2025

Abstract *- Wireless Sensor Networks (WSN) have become a vital technology for monitoring and tracking applications across various applications. It senses an environment, gathers data, and transmits it to the Base Station (BS) for analysis. However, energy efficiency and security are challenging because of an open environment and a limited battery source. This research proposes a Multi-objective Trust-Aware Golf Optimization Algorithm (M-TAGOA) to achieve a secure and energy-efficient clustering and routing process in WSN. M-TAGOA chooses a Secure Cluster Head (SCH) depending on the distance between the neighbor nodes, the distance between BS and CH, node degree, and trust threshold like direct, indirect, and recommendation trust are the multi-objective functions. Then, secure routing is determined by M-TAGOA with energy and distance. Hence, the M-TAGOA prevents malicious nodes, which enhances data delivery and avoids excessive energy consumption. M-TAGOA achieves less consumption of energy at 0.05 mJ compared to existing techniques like Neuro-Fuzzy-based clustering with Sparrow Search Optimization Algorithm (NF-SSOA)*

Keywords *- Base station, Multi-objective trust-aware golf optimization algorithm, Secure cluster head, Secure routing, Wireless Sensor Networks.*

1. Introduction

Wireless Sensor Network (WSN) has a huge number of spatial distributed microelectronic devices. These nodes enable components of their environments to communicate between their peers or transmit the data to the BS directly. Nodes normally consume energy commonly during the communication process [1]. Sensor nodes have limited battery power, communication capabilities, and electromagnetic frequency, but BS has higher energy and intellectual and data quality. The BS acts as a gateway between the end user and the sensor nodes [2]. The BS gathers the data, analyses it, and decides according to the application [3]. In a network, every node has limited energy and faces a primary challenging problem when constructing an energy-efficient routing approach. Therefore, energy-efficient approaches are required to extend the network lifetime and enhance the network performance [4]. Cluster-based techniques proved effective for energy balancing and scalability to handle WSN energy consumption [5]. The clustering process has a group of numerous nodes in a network for effective communication with BS and Cluster Head (CH) [6]. Equivalent CH and cluster selection are time-consuming and complicated tasks. Recently, different approaches have been utilized to obtain an appropriate CH [7]. The clustering approach is a significant role concern in WSN to provide an energy-efficient routing that makes their ability scalable and flexible [8, 9]. Each cluster has to select a CH to perform specialized tasks for retrieving the details or information from the nodes within integrated data clusters and transferring the integrated data directly to the BS [10, 11]. A cryptography-based security approach is required to resist malicious attacks on WSNs and operate them in a secure environment. However, the cryptography approach requires sophisticated computation and complex functions that obtain high memory space and more energy consumption. Therefore, trust-based security schemes determine and predict the node behavior depending on its past behavior, and they quantify the node behavior by constructing models [12, 13]. WSN performs certain forms of routing mechanisms. With the assistance of Energy-Optimized Secure Routing (EOSR), WSN balances their energy consumption and enhances security by determining trusted nodes and secure data sharing between them [14]. Routing is the most significant activity in the sensor node, and it consumes more energy than other activities [15]. The sensor network lifetime decreases when too much energy is consumed by a sensor node; therefore, the network security goals are not achieved in a full-fledged manner [16]. Optimizing the clustering process involves enhancing the data

aggregation performance, data communication, and cluster formation [17, 18]. However, security and energy efficiency are difficult due to a restricted battery source and open environment. To overcome this problem, an M-TAGOA is proposed to determine a secure data transmission by utilizing clustering and routing processes that minimize energy consumption and provide security in WSN.

The proposed M-TAGOA approach stands out by integrating multiple fitness functions for secure cluster head selection and routing, offering superior energy efficiency and security compared to existing methods. The primary contribution of this research is described below:

- M-TAGOA-based SCH selection enhances security and energy efficiency in sensor nodes by utilizing various fitness functions.
- Multiple fitness functions, including the distance between the neighbor nodes, the distance between BS and CH, node degree, and trust threshold, are used, which selects SCH from a normal sensor. This process ensures the reliable and effective operation of the sensor node.
- The secure routing process established by M-TAGOA optimizes routing in WSN by utilizing energy and distance as fitness functions. This approach reduces energy consumption and enhances security in data transmission.

The remaining part is structured as follows: Section 2 describes a literature survey of existing methods. Section 3 illustrates a proposed methodology. Section 4 indicates the results for the proposed and existing methods. Section 5 summarizes the conclusion.

The introduction section has been revised to highlight the research gap, emphasizing the challenges of achieving energy efficiency and security in WSNs due to limited battery resources and open environments. Additionally, the problem is introduced by stating the necessity for a robust clustering and routing approach, like M-TAGOA, to address these challenges effectively. Section 2 describes the literature review, and section 3 presents the proposed mechanism used. Section 4 describes the results, and section 5 concludes the work.

2. Literature Review

This section discussed the related work about secure and energy-efficient clustering and routing in WSN, along with its benefits and limitations.

K. Dinesh & S. V. N. Santhosh Kumar [19] presented a Neuro-Fuzzy-based clustering with Sparrow Search Optimization Algorithm (NF-SSOA) to generate secure, energy-efficient, trust-aware cluster-based data transmission in WSN. The NF was performed for effective node clustering, and SSOA was utilized for routing. During data transmission, the NF-SSOA approach utilizes pseudo-random identity generation to perform anonymous authentication in the network. The presented approach enhances the energy efficiency and reliability in WSN by using NF clustering. However, NF-SSOA faces scalability challenges in large-scale networks due to its dependence on specific neuro-fuzzy parameters, reducing its effectiveness as the network grows.

Shashank Singh et al. [20] implemented a Dempster-Shafer Theory-Whale Optimization Algorithm (DST-WOA) for trusted clustering and routing. The main aim of this approach was to increase the energy efficiency and reliability in WSN by including the considerations of trustworthiness in optimal cluster and routing selection. The DST-WOA enhances energy efficiency and reliability by incorporating trust management approaches into the routing protocol. However, determining accurate initial condition assignments for DST-WOA was challenging because network environments are inherently subjective and uncertain, making it difficult to assign initial conditions accurately.

R. Nandha Kumar and P. Srimanchari [21] developed a Quantum behavior and Gaussian Mutation based Archimedes Optimization Algorithm (QGAOA) to secure data aggregation and routing schemes in WSN. QGAOA contains three parts: CH, cluster formation, and optimal routing. The clusters were established utilizing the Voronoi k-means clustering technique. Then, the CH and routing were chosen by employing QGAOA. During the CH selection, malicious node activity was avoided, minimising packet drops and enhancing network security. However, QGAOA struggles to adapt to dynamic network conditions and topology changes due to its dependence on mutation strategies and quantum behavior.

A. Vinitha et al. [22] introduced a Taylor-based Cat Salp Swarm Algorithm (Taylor C-SSA) for energy-efficient multihop routing. The energy-efficient CH was chosen by utilizing the Low Energy Adaptive Clustering Hierarchy (LEACH) to transmit data effectively, and the sensor nodes send data over CH that transmits to BS via the selected optimal hop. Then, the optimal hop selection was performed by utilizing Taylor C-SSA. The Taylor series generates the accurate estimation of primary functions and achieves convergence easily. However, Taylor C-SSA lacks sufficient search space exploration because of its dependence on Taylor series expansion, which limits the algorithm's ability to explore diverse optimal solutions.

Perumalla Suman Prakash et al. [23] suggested a Fractional Artificial Lion Algorithm (FAL) to select the optimal paths in WSN during routing securely and effectively. The FAL evaluates the secure routing path by fitness parameter, and the route is maintained by network lifetime. The CH selection and routing approach was attained successfully in the FAL approach by integrating Fractional

calculus, Artificial Bee Colony (ABC), and Lion Optimization Algorithm (LOA). However, FAL suffers from slower convergence rates because it depends on iterative processes that take longer to find optimal paths, leading to potential inefficiencies in WSNs. Ibraheem et al. [24] proposed Security-Enhanced Energy Conservation with an Enhanced Random Forest Classifier for a Low Execution Time Framework (S-2EC-ERF). This framework leverages the Enhanced Consumed Energy LEACH (ECP-LEACH) protocol and the Enhanced Random Forest Classifier for Low Execution Time (ERF-LET) algorithm to address attack detection and energy efficiency.

The SEE2PK algorithm [25] improves WSNs by balancing security and energy efficiency through pairwise key establishment, reducing communication, computation, and storage costs while enhancing performance. By utilizing adjacency matrices and mesh routers as Cluster Heads, it achieves efficiency; however, its dependence on adjacency matrices may limit scalability in dynamic and large-scale networks. In the overall analysis, the existing technique has limitations like struggles with scalability in large-scale networks, suffering from slower convergence rates due to its dependence on iterative processes and difficulties in energy efficiency and security. To solve these issues, the M-TAGOA is proposed to achieve secure data transmission in WSN by using multiple fitness functions that achieve reliable and reduced energy consumption.

2.1. Proposed System

The M-TAGOA is proposed to secure and energy-efficient clustering and routing in WSN. It contains trust-based clustering, SCH and an energy-efficient routing scheme. Nodes with identical energy are utilized arbitrarily in a system model. Figure 1 determines the WSN's system model.

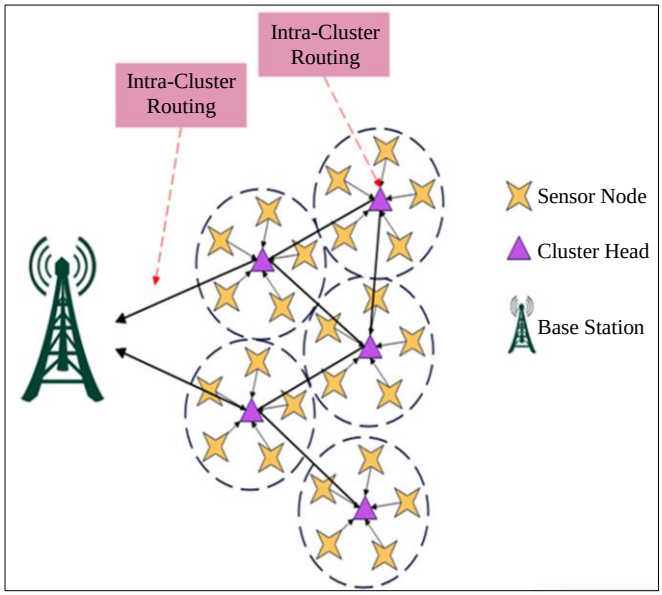


Fig. 1 Architecture of proposed model

3. System Model

Initially, the nodes are collected from different clusters, and each CH is connected to an individual BS or sink in WSN. It provides certain assumptions regarding the WSN model and describes the energy consumption model utilized in this research. Wireless connection among Sensor Node (SN) in the transmission range indicates direct transmission. Once the cluster has been established, the nodes utilize their consistent CH to communicate the bytes.

3.1. Network Model

This section enables the following considerations regarding a network model, which are described below:

- The area WSN manages is a flat regular graph in that SN is distributed randomly. The locations of every node are fixed, and no human intervention is utilized after a network. Also, every node has a globally unique network identifier.
- Each SN is isomorphic; each node has identical communication ability, the same initial energy, and equal computing power. A battery with limited energy powers SN and does not recharge.
- The node identifies its position and calculates the distance from itself to a transmitter based on the received signal strength. According to the communication distance, the power of wireless transmission is self-regulated and transmission power is chosen independently.
- BS is situated inside or outside a monitoring area, and its computing power and energy are unlimited.

3.2. Energy Consumption Model

According to the distance between transmitter and receiver, multi-path fading or free-space (d^4 or d^2 energy consumption) channel approach is utilized. Over a distance d, the energy required to transmit m-bit packet data is expressed in Equation (1),

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

The energy needed for a node to obtain an m-bit message is formulated in Equation (2),

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

The energy needed for CH to fuse an m-bit packet of data is represented in Equation (3),

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

Where E_{elec} represents the energy required for transmitting per-bit data, $d_0 = \sqrt{\varepsilon_{fs}/\varepsilon_{mp}}$ indicates distance

threshold, ε_{fs} and ε_{mp} denotes the transmitting circuit's amplification factor of free space and multi-path fading approach. A free space model is employed if a distance exceeds d_0 a threshold; otherwise, the multi-path approach is utilized.

3.3. Secure CH Discovery Using M-TAGOA

In M-TAGOA, an efficient secure CH and route discovery is generated to attain a reliable and secure data transmission by avoiding malicious nodes. Initially, SCH is determined from normal sensors utilizing the distance between neighbor nodes, the distance between BS to CH, node degree, and trust thresholds like direct trust, indirect trust, and recommendation trust. Then, the M-TAGOA is employed to determine the secure path from a transmitter by employing a fitness function as energy and distance. Figure 2 represents the block diagram for the MGWO approach.

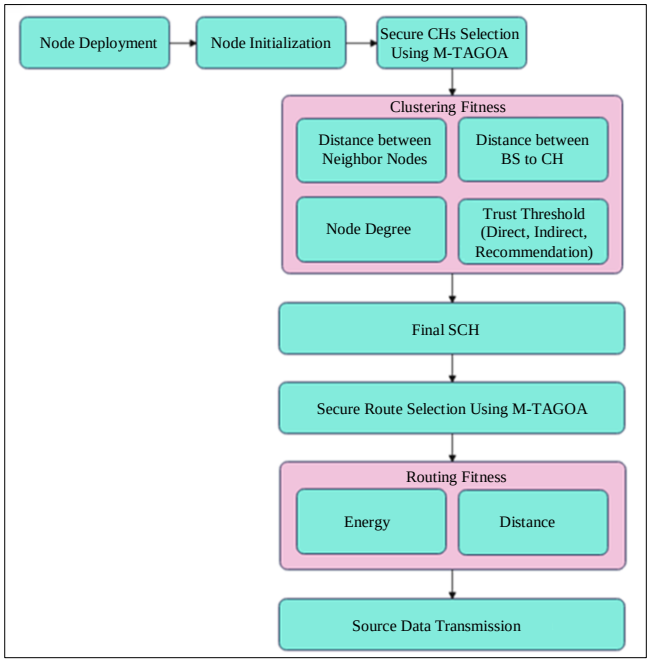


Fig. 2 Block diagram for the M-TAGOA approach

3.3.1. Sensor Initialization

Initially, the sensors are utilized randomly in the WSN area. The energy and network models are provided in the previous section. A SCH and route discovery are performed by utilizing M-TAGOA, which will be discussed in the upcoming sections. After initializing the sensor, the SCH is established using M-TAGOA.

3.3.2. SCH Using M-TAGOA

In this phase, optimum SCH from normal sensors is determined by utilizing the M-TAGOA technique. GOA is a population-based technique that generates relevant solutions to optimization issues via a random search of its members in the space of problem-solving. It is divided into two stages: exploration and exploitation. The GOA can balance exploitation and exploration effectively, leading to better convergence rates. It mimics the strategies utilized in golf to reach a target with reduced strokes, which makes for effective energy usage and a robust network lifetime. In this stage, the GOA is converted into M-TAGOA to determine the optimum SCH selection.

3.3.3. Initialization

The M-TAGOA's member position in the problem space evaluates the value of problem variables, and their population is formulated. The population members are distributed randomly over the problem space by utilizing a uniform distribution. The M-TAGOA's position is initialized randomly in search space, which is expressed in Equation (4)

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix}_{N\times m} = \begin{bmatrix} x_{1,1} \dots x_{1,d} \dots x_{1,m} \\ \vdots \quad \ddots \quad \vdots \quad \iddots \quad \vdots \\ x_{i,1} \cdots x_{i,d} \cdots x_{i,m} \\ \vdots \quad \iddots \quad \vdots \quad \ddots \quad \vdots \\ x_{N,1} \cdots x_{N,d} \cdots x_{N,m} \end{bmatrix}_{N\times m} \tag{4}$$

$$X_i : x_{1,d} = lb_d + r \times (ub_d - lb_d) \tag{5}$$

Where X represents M-TAGOA's population matrix, X_i indicates i^{th} member, $x_{i,d}$ denotes d^{th} variable produced by i^{th} member, N determines the number of M-TAGOA's members, m shows the number of variables, r represents the random number in [0-1] interval, lb_d and ub_d indicates a d^{th} variable lower and upper bound. The computed values for the objective function are denoted by utilizing a vector, which is represented in Equation (6)

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N\times 1} = X = \begin{bmatrix} F(X_1) \\ \vdots \\ F(X_i) \\ \vdots \\ F(X_N) \end{bmatrix}_{N\times 1} \tag{6}$$

Where F indicates objective function vector values and F_i denotes acquired value for objective function depending on i^{th} M-TAGOA member. Then, the M-TAGOA fed into the process of updating the population members.

3.3.4. Exploration

Once the M-TAGOA's initialization stage is performed, it passes through the updating process for population members. It is updated into two stages: exploration and exploitation. The initial swing in a golf game is struck in a playground area known as the grip. The best member position is considered a hole, and this technique scans various search space areas, representing the M-TAGOA's ability to explore global search. The updating process of M-TAGOA's

exploration stage is formulated in Equations (7) and (8). A new position is computed by utilizing Equation (6) based on the player's strongest ball shot. Next, if the objective function value enhances in this newly computed position, it replaces the prior position of the respective member-based, which is expressed in Equation (8). The ball approaches the hole if the parameter I is equal to 1. If the parameter I is equal to 2, the exploration ability is enhanced in global search by increasing the possibility of moving the ball to scan various areas of search space.

$$X_i^{P1}: x_{i,d}^{P1} = x_{i,d} + r \times (B_d - I \times x_{i,d}) \tag{7}$$

$$X_i = \begin{cases} X_i^{P1}, & F_i^{P1} < F_i \\ x_i, & else \end{cases} \tag{8}$$

Where X_i^{P1} represents new calculated status of i^{th} M-TAGOA member depending on exploration stage, $x_{i,d}^{P1}$ and B_d denotes d^{th} dimension, F_i^{P1} indicates value of objective function, B determines best member of M-TAGOA, I denotes random number which is randomly chosen from the $\{1, 2\}$ set.

3.3.5. Exploitation

The area where the hole is situated on the playground is called green. The players try to put golf balls into holes with kicks in this area, which is putt. These kicks are presented with low power; hence, golf balls cannot move away from holes and green areas. This strategy enables the area where the M-TAGOA member is situated to scan, representing the M-TAGOA's exploration ability in local search. The updating process of M-TAGOA depends on the exploitation stage, which is formulated in Equations (9) and (10). A new position is computed for each M-TAGOA member by utilizing Equation (9) based on the player's low power shots to balls. If the objective function value is improved, the prior position of a respective member is replaced, which is shown in Equation (10),

$$X_i^{P2}: x_{i,d}^{P2} = x_{i,d} + (1 - 2r) \times \frac{lb_d + r \times (ub_d - lb_d)}{t} \tag{10}$$

$$X_i = \begin{cases} X_i^{P2}, & F_i^{P2} < F_i \\ X_i, & else \end{cases} \tag{11}$$

Where X_i^{P2} determines new calculated M-TAGOA members based on exploitation stage, $x_{i,d}^{P2}$ denotes d^{th} dimension, F_i^{P12} indicates value of an objective function, and t refers to iteration counter. After each stage of updating the position of population members, it checks if the new solutions belong to feasible solutions or not. The initial constraint group is associated with the decision variable's acceptable range. Its value is considered borderline if the decision variable value exceeds the lower or upper bound. This restriction lower and upper bands for decision variables are checked and, if it is required, solved by employing Equations (12) and (13).

$$x_{i,d}^{P1} = \begin{cases} x_{i,d}^{P1}, & lb_d \le x_{i,d}^{P1} \le ub_d \\ ub_d, & x_{i,d}^{P1} > ub_d \\ lb_d, & x_{i,d}^{P1} < lb_d \end{cases} \tag{12}$$

$$x_{i,d}^{P2} = \begin{cases} x_{i,d}^{P2}, & lb_d \le x_{i,d}^{P2} \le ub_d \\ ub_d, & x_{i,d}^{P2} > ub_d \\ lb_d, & x_{i,d}^{P2} < lb_d \end{cases} \tag{13}$$

By incorporating the penalty coefficient into the objective function value of the issue, a new solution is identified as an irrelevant solution, and it is impossible to select the solutions to the issue. This constraint group is determined by utilizing Equation (14),

$$F_i = F_i + n_q \times PF_i \tag{14}$$

Where n_q denotes number of constraints of issue which is not established and PF_i represents penalty factor $PF_i = 10^5 \times |F_i|$. M-TAGOA lies in their ability to manage complex optimization issues effectively. It provides robust clustering and routing solutions, enhancing network security by optimizing energy consumption. Their adaptive nature makes them appropriate for dynamic WSN environments and makes secure and reliable data transmission while enhancing network lifetime through effective resource allocation.

3.3.6. Fitness for SCH Selection

The multi-objective fitness is determined to acquire the best solutions in SCH selection. The four fitness functions like the distance between BS and CH, the distance between the neighbor nodes, node degree, and trust threshold (direct, indirect, and recommendation trust), are utilized for SCH, which are explained below:

Distance between Neighbor Nodes

Every CH recognizes a neighbor CH, and it sends an acknowledgement message to distance the BS and node degree after the node is selected. Equation (15) represents the distance between neighbor nodes.

$$f1 = \sum_{i=1}^{n} f(XCH_i) \quad \forall i \in N \tag{15}$$

Where, n represents total number of elements or nodes and X denotes vector or specific data points respectively.

Distance between BS and CH

It computes the distance between BS and CH, and the space via the transmission path evaluates the energy consumption of the node. More energy is required for data transmission if the BS is located far from CH. The CHs have failed suddenly due to the large energy consumption. Hence, the transmission of data prefers short-distance node from BS and its fitness function is calculated in Equation (16),

$$f2 = \sum_{i=1}^{m} d(CH_{j,}BS) \quad (16)$$

Where m indicates total number of CH and $d(CH_{j,}BS)$ represents distance between CH and BS.

Node Degree

After sensor node deployment, certain clusters have a huge number of members, and some have fewer members. It is based on neighbor node's load, which is expressed in Equation (17),

$$f3 = ND_{min} = \sum_{i=1}^{h^T} CM_i \quad (17)$$

Where ND_{min} indicates minimum node degree, h^T represents the number of CH, and CM_i denotes total neighbors of chosen CH.

Trust

The primary fitness employed in M-TAGOA is trust value, where it has 3 various trust measures such as direct, indirect, and recommendation trust. Direct Trust (DT) is determined by considering sending and receiving neighbor packets, expressed in Equation (18). Indirect Trust (IDT) generates the trust value between node and target nodes through primary nodes as calculated in Equation (19).

Recommendation Trust Score (RTS) calculates the trusted node based on neighbor data. If more than 1 recommendation values are chosen, then the node of trust considers the maximum RTS value formulated in Equation (20). The overall trust node value is represented in Equation (21). The minimum fitness for the clustering process is represented in Equation (22).

$$DT = \frac{Received\ packets_{a,b}(t)}{Sent\ packets_{a,b}(t)} \quad (18)$$

$$IDT = \frac{1}{NN}\sum_{u=1}^{NN} DT_{u,a} \quad (19)$$

$$RTS_{ij} = \max\{RTS_{wj}\} \quad (20)$$

$$f4 = DT + IDT + RTS_{ij} \quad (21)$$

$$Minimum\ fitnes = \propto_1 f1 + \propto_2 f2 + \propto_3 f3 + \propto_4 f4 \quad (22)$$

Where $\sum_{i=1}^{4} \propto_i = 1$; and $\propto_i \epsilon(0,1)$, a, b denotes sensors, NN represents a number of neighbor nodes, and w determines neighbor of j.

3.4. Cluster Formation

Once the SCHs are selected by utilizing M-TAGOA, a possible function is presented, which is represented in Equation (23). SN with fewer transmission distances and more remaining energy is provided to CH. Therefore, the quantity of energy consumption during data transmission is lower.

$$\text{Potential function } (\mathrm{Sn_p}) = \frac{\mathrm{z} \times \mathrm{E(SCH_j)}}{\mathrm{D(S_i, SCH_j)}} \quad (23)$$

Where z indicates proportionality constant, Sn_p represents potential of SN and $D(S_i, SCH_j)$ defines distance among SCH_j and sensor S_i. The sensor is generated to SCH with high potential and $E(SCH_j)$ determines the residual energy of CH. While the distance among 2 different SCHs and SN is equal, the SN is associated with CH with high energy. The discovery of the routing stage using M-TAGOA is constructed after the clustering stage to determine a data transmission of SCH to BS.

3.5. Secure Routing Discovery Using M-TAGOA

The routing process is generated by 2 phases: initialization and routing selection. T-MAWOA indicates the data transmission path among CH and BS. The route discovery is transmitted from source to BS, updated by each golf, and the CH quantity in the relevant transmission is identical to every golf measurement. To evaluate the data transmission path, T-MAWOA employs the identical fitness function as energy and distance.

3.5.1. Energy

The residual energy of the sensor node is computed by incorporating energy depleted when a node is in every state, which is determined utilizing Equation (24),

$$f5 = E''_{xenr} = \frac{1}{T_{tch}}\sum_{n=1}^{T_{tch}} (E''_{xenr})_n \quad (24)$$

Where T_{tch} represents the overall number of CHs.

3.5.2. Distance

According to CH distance, the distance among two nodes is called the node's distance. This distance is very short to communicate efficiently. Distance among n^{-th} CH and o^{-th} the neighboring node is formulated in Equation (25),

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

Where N_{nch} determines total neighboring nodes. With respect to the normalization process $F(x))$ is determined to every function $\propto_1, \propto_2, \propto_3, \propto_4, \propto_5$, and $\propto_6$ which is expressed in Equation (26),

$$F(x)) = \frac{f_i - f_{min}}{f_{max} - f_{min}} \quad (26)$$

Where f_{min} and f_{max} represents minimum and maximum values, which is formulated in Equation (27),

$$Minimum\ fitnes = \propto_5 f5 + \propto_6 f6 \quad (27)$$

Where, $\sum_{i=1}^{2} \propto_i = 1$; and $\propto_i \epsilon(0,1)$. In the routing process, every inhabitant's measurement is identical to the number of CH (m). A route request data transmission is sent from a source node to neighbor nodes for adjusting the route identification procedure. At that point, the next node with a greater fitness rating transmits data back to source CH via the reverse path. Once a routing path is established, the source CH receives the data from nearby nodes. After creating a routing path, data transmission is initiated through a network.

3.6. CH Maintenance

To balance a load between clusters, cluster management is significant to avoid node failure. CH handles communication among SN and BS, optimizing network energy efficiency by minimizing redundant transmissions. It performs data aggregation and reduces the amount of transmission data, which preserves energy. CH maintenance ensures balanced energy consumption across the network and extends the overall network lifetime. Also, it increases network stability and reliability by preventing a single node from a point of failure.

4. Experimental Results

In this section, the outcomes and comparative analysis of the M-TAGOA approach are determined. The M-TAGOA is proposed and simulated by utilizing MATLAB R2020b with Windows 10 Operating System, i5 intel processor, and 64 GB RAM. M-TAGOA is employed to achieve reliable and secure data transmission over the WSN. Table 1 represents the simulation parameters to determine M-TAGOA.

Table 1. Simulation parameters

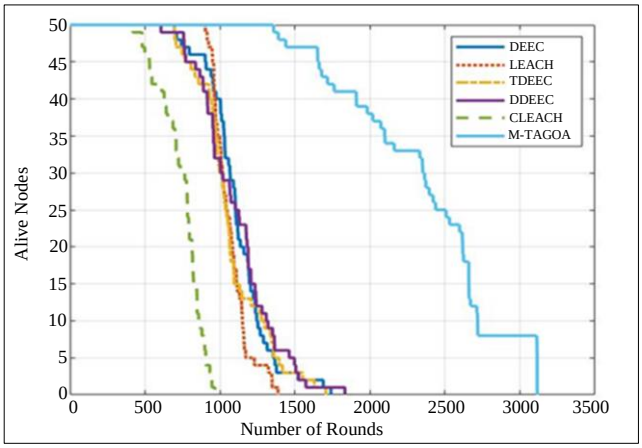
Parameter	Values
Initial energy	0.55 J
Number of nodes	50, 100
Network size	$200m \times 200m$
Packet size	4000 bits
E_{elec}	$50nJ/bit/m^2$
ε_{mp}	$0.0013pJ/bit/m^2$
ε_{fs}	$10pJ/bit/m^2$

4.1. Performance Analysis

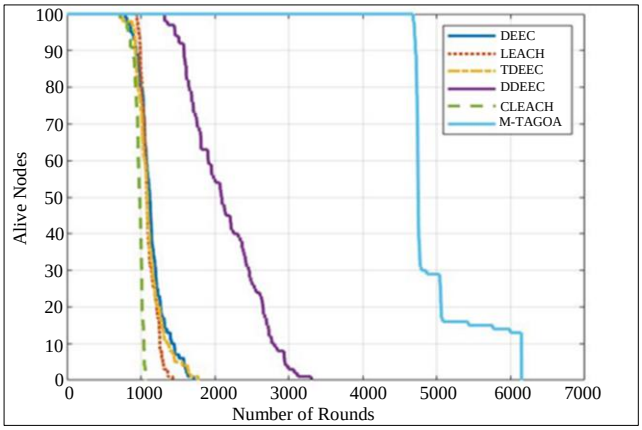
The proposed M-TAGOA is determined with different performance measures such as alive nodes, energy consumption, dead nodes, First Node Dead (FND), Half Node Dead (HND), Last Node Dead (LND), delay, throughput, and Packet Loss Ratio (PLR). The proposed M-TAGOA is analyzed with Distributed Energy-Efficient Clustering (DEEC), LEACH, Developed DEEC (DDEEC), Threshold DEEC (TDEEC), and Centralized LEACH (CLEACH) because these existing approaches are determined by utilizing similar specifications which are presented in Table 1.

4.2. Alive Nodes

Figure 3 represents the performance of alive nodes analysis for 50 and 100 nodes. In WSN, alive nodes are the nodes that have the energy to establish data transfer. The analysis compares DEEC, LEACH, TDEEC, DDEEC, CLEACH, and M-TAGOA. The result shows that M-TAGOA's alive nodes sustained longer than DEEC, LEACH, TDEEC, DDEEC, and CLEACH due to energy existing in M-TAGOA's nodes is preserved by avoiding malicious nodes during SCH and routing selection. Also, energy is balanced by CH maintenance, which allows the nodes to select the next best node. Therefore, nodes remain active for up to 3200 and 8100 rounds for 50 and 100 nodes.



(a) 50 nodes

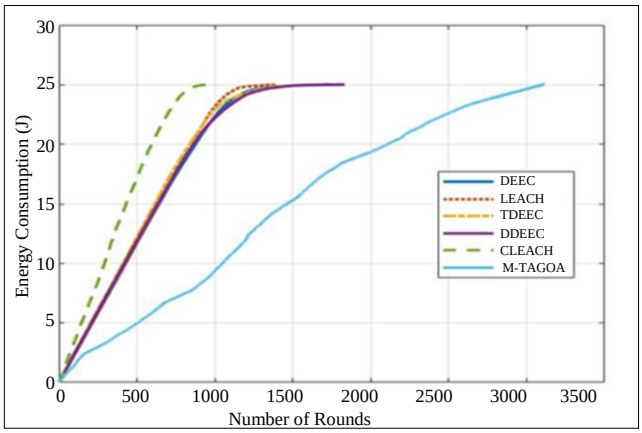


(b) 100 nodes

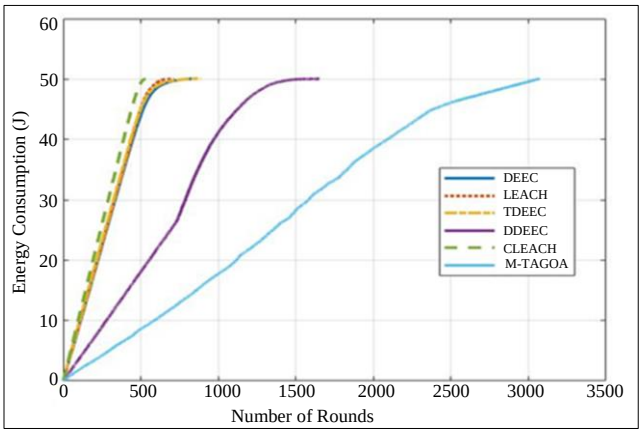
Fig. 3 Performance of alive nodes

4.3. Energy Consumption

Figure 4 denotes the energy consumption performance for 50 nodes and 100 nodes. M-TAGOA is determined with different numbers of rounds, such as 0 to 3500 for 50 nodes and 0 to 7000 rounds for 100 nodes. The outcomes show that M-TAGOA attains less energy consumption due to golf optimization, which adjusts clustering and routing decisions based on present network conditions, preserves energy depletion in certain areas, and distributes the load more evenly.

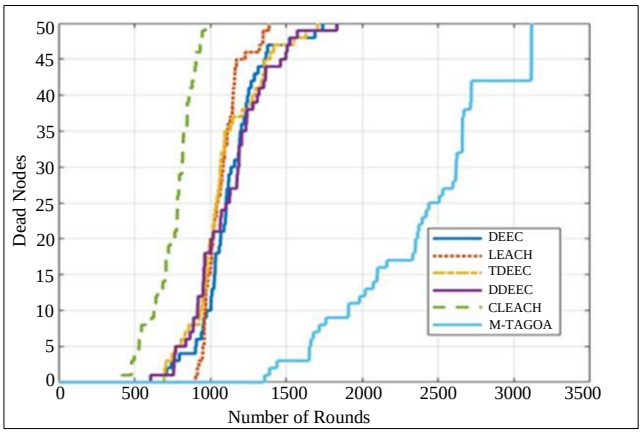


(a) 50 nodes

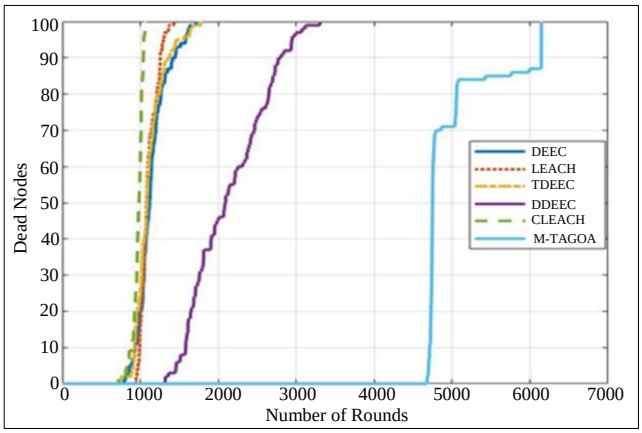


(b) 100 nodes

Fig. 4 Performance of energy consumption



(a) 50 nodes



(b) 100 nodes

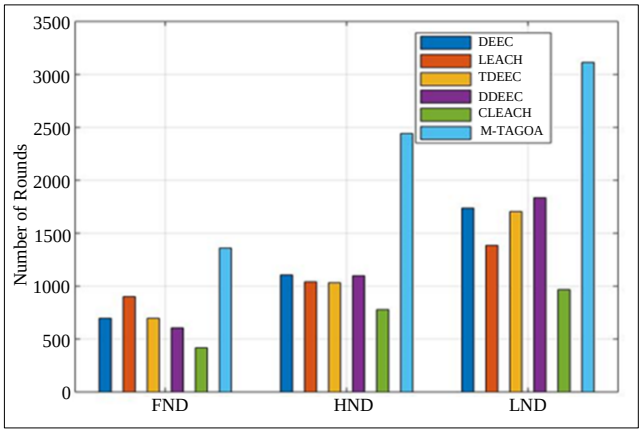
Fig. 5 Performance of dead nodes

4.4. Dead Nodes

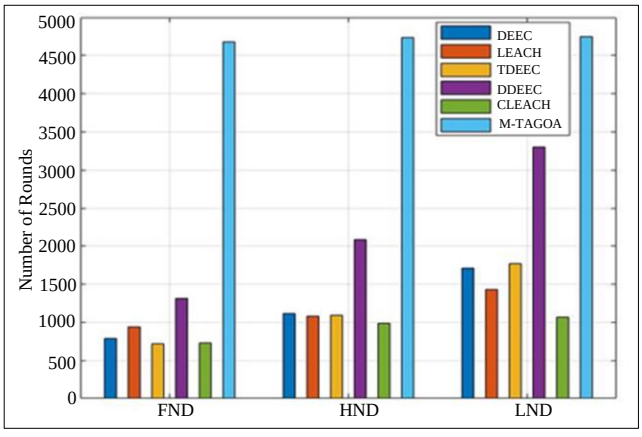
Figure 5 determines the analysis of dead node performance. M-TAGOA is estimated with various numbers of rounds like 0 to 3500 for 50 nodes and 0 to 7000 rounds for 100 nodes. When analyzed with DEEC, LEACH, TDEEC, DDEEC, and CLEACH, M-TAGOA achieves fewer dead nodes due to it ensures balanced energy consumption using CH maintenance across nodes and its trust mechanism prevents unreliable node selection.

4.5. FND, HND, and LND

Figure 6 illustrates the performance analysis of FND, HND, and LND. The number of rounds employed for 50 nodes varies from 0 to 3500 and 0 to 5000 for 100 nodes. M-TAGOA achieves a high FND, HND, and LND because of M-TAGOA's available energy in the nodes, which is enhanced by balancing the energy usage via the selection of SCH and routing process without malicious node interferences.



(a) 50 nodes



(b) 100 nodes

Fig. 6 Performance of FND, HND, and LND

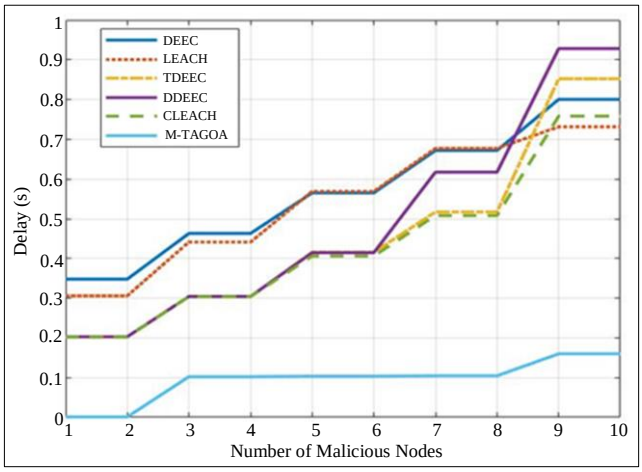


Fig. 7 Performance of malicious nodes for 50 nodes

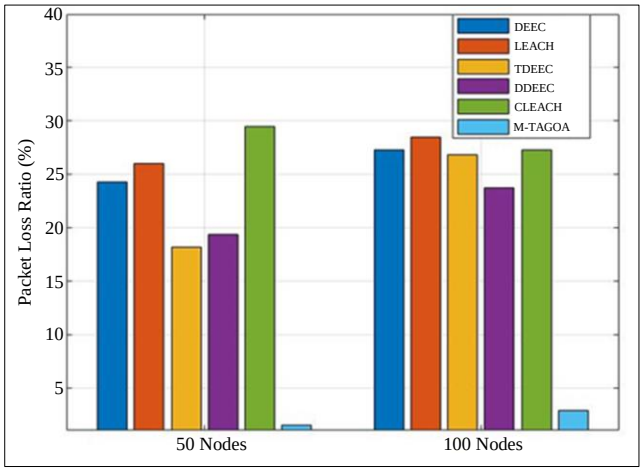


Fig. 8 Analysis of PLR for 50 and 100 nodes

4.6. Delay Analysis

Figure 7 indicates the performance of malicious node analysis for 50 nodes. Delay represents duration of time required to transmit data packets from source to destination. The results show that delay of M-TAGOA is less than existing approaches due to M-TAGOA accomplishes identification of a secure routing path with reduced broadcasting distance which effectively minimizes delay in the transmission of data.

4.7. PLR

Figure 8 denotes the analysis of PLR performance for 50 nodes and 100 nodes. PLR analysis observes that M-TAGOA provides enhanced data delivery than DEEC, LEACH, TDEEC, DDEEC, and CLEACH due to failure nodes and malicious nodes are prevented in M-TAGOA, which assists in reducing the packet loss in the routing procedure.

4.8. Throughput

The performance of throughput analysis for 50 and 100 is determined in Figure 9. Throughput refers to the total packet that is transmitted successfully from transmitter SCH. The outcome reveals that M-TAGOA achieves high throughput due to its effective clustering and routing mechanisms that optimize the data transmission path and minimize interference. It ensures that data is transmitted reliably and with minimal delay, which increases overall network throughput.

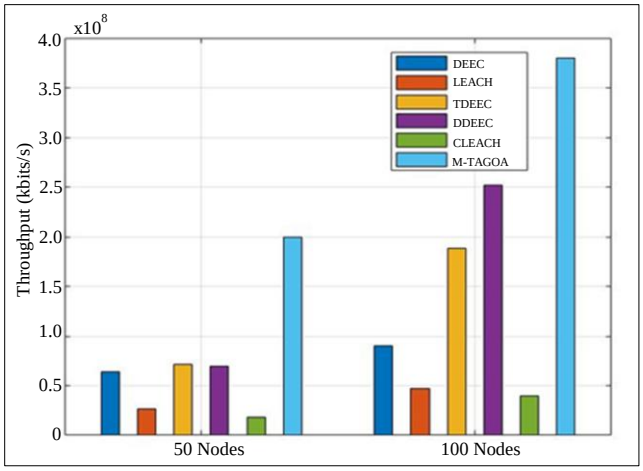


Fig. 9 Throughput analysis for 50 and 100 nodes

4.9. Comparative Analysis

Table 2 demonstrates the different scenario specifications based on different metrics. In the different scenarios, scenario 1 is for NF-SSOA [19], scenario 2 is for QGAOA [21], and scenario 3 is for FAL [23] in comparison with M-TAGOA. The M-TAGOA is configured to evaluate the performance for the specifications mentioned in Table 2. Tables 3, 4, and 5 represent the comparison of M-TAGOA with NF-SSOA [19], QGAOA [21], and FAL [23].

It shows that M-TAGOA outperforms existing techniques. For instance, alive nodes in M-TAGOA for 100 nodes is 39 while FAL [20] has 32 alive nodes. Mitigating malicious nodes by utilizing the trust metric in M-TAGOA assists in avoiding unnecessary energy usage and packet loss in WSN. Hence, the alive nodes of M-TAGOA are increased when reducing the packet drop respectively.

Table 2. Different scenario specifications

Parameters	Scenarios		
	1	2	3
Area	1000 x 1000m^2	1500 x 1500m	100 x 100m^2
No. of Nodes	100, 200, 300, 400, 500	100, 200, 300, 400, 500	100, 150, 200
Initial Energy	1J	1J	0.5J

Table 3. Comparative analysis of M-TAGOA with NF-SSOA

Methods	Performance Measures	Number of Nodes				
		100	200	300	400	500
NF-SSOA [19]	Energy Consumption (mJ)	0.1	0.21	0.27	0.31	0.35
	Throughput (mbps)	95	95	94	94	93
	Delay (ms)	12	13	13	15	18
Proposed M-TAGOA	Energy Consumption (mJ)	0.05	0.15	0.10	0.22	0.26
	Throughput (mbps)	98	99	96	96	97
	Delay (ms)	9	10	10	12	15

Table 4. Comparative analysis of M-TAGOA with QGAOA

Methods	Performance Measures	Number of Nodes				
		100	200	300	400	500
QGAOA [21]	Delay (ms)	11.34	13.24	14.56	16.21	18.86
	Throughput (%)	96	97	94	96	95
Proposed M-TAGOA	Delay (ms)	10.59	10.24	11.30	13.55	14.39
	Throughput (%)	99	98	96	97	98

Table 5. Comparative analysis of M-TAGOA with FAL

Methods	Performance Measures	Number of Nodes		
		100	150	200
FAL [23]	Alive node	32	44	45
	Energy (J)	0.14	0.108	0.091
	Throughput (%)	91.10	90.08	92.25
Proposed M-TAGOA	Alive Node	39	48	49
	Energy (J)	0.25	0.364	0.267
	Throughput (%)	98.15	96.32	96.14

4.10. Discussion

The advantages of the proposed M-TAGOA and the limitations of existing techniques are discussed briefly in this section. The limitation of existing techniques like NF-SSOA [19] faces scalability challenges in large-scale networks due to its dependence on specific neuro-fuzzy parameters, which reduces its effectiveness as network size grows. Determining accurate initial condition assignments for DST-WOA [20] was challenging because network environments are inherently subjective and uncertain, making it difficult to assign initial conditions accurately. QGAOA [21] struggles to adapt to dynamic network conditions and topology changes due to its dependence on mutation strategies and quantum behavior.

Taylor C-SSA [22] lacks sufficient search space exploration because of its dependence on Taylor series expansion, which limits the algorithm's ability to explore diverse optimal solutions. FAL [23] suffers from slower convergence rates because it depends on iterative processes that take longer to find optimal paths, which leads to potential inefficiencies in WSNs. The proposed M-TAGOA overcomes these existing techniques' limitations. The M-TAGOA in attaining secure and energy-efficient clustering and routing in WSN is its multi-fitness approach, which optimizes node selection and routing paths. This improves security through trust thresholds by minimizing energy consumption. Therefore, it enhances overall network performance and reliability. M-TAGOA addresses the limitations of existing methods by ensuring scalability, adaptability, and energy efficiency in dynamic WSN environments. Its multi-fitness approach enhances security through trust thresholds and minimizes energy consumption, extending network lifetime. These advancements make M-TAGOA a robust solution for practical applications like environmental monitoring and smart cities.

5. Conclusion

In this research, the M-TAGOA is proposed to achieve a secure and energy-efficient based clustering and routing process in WSN. M-TAGOA selects a normal node as CH depending on the trust, which has high energy, less transmission distance, and equal balancing among clusters. The balancing between clusters is performed to enhance the energy in nodes. The secure routing path is generated using M-TAGOA, which leads to reduced energy consumption and enhanced data transmission security.

By performing this operation, the proposed M-TAGOA achieves better performance. Compared to existing techniques like NF-SSOA, the M-TAGOA obtains a lower energy consumption of 0.05 mJ. In the future, advanced optimization approaches will be considered for energy-efficient processes

to prevent the network from other types of attacks. In this research, the M-TAGOA is proposed to achieve a secure and energy-efficient based clustering and routing process in WSN. M-TAGOA selects a normal node as CH depending on thetrust, which has high energy, less transmission distance, and equal balancing among clusters. The balancing between clusters is performed to enhance the energy that exists in nodes. The secure routing path is generated using M-TAGOA, which leads to reduced energy consumption and enhanced data transmission security. Already discusses future improvements, including integrating advanced optimization techniques for energy efficiency and enhanced security measures to prevent various network attacks. However, per the reviewer's suggestion, these points will be consolidated into a dedicated "Future Work" section for better clarity and emphasis.

References

[1] Mei Wu et al., "A Dual Cluster-Head Energy-Efficient Routing Algorithm Based on Canopy Optimization and K-Means for WSN," *Sensors*, vol. 22, no. 24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Kantharaju Veerabadrappa, and Sanjeev Channaabasappa Lingareddy, "Trust and Energy Based Multi-Objective Hybrid Optimization Algorithm for Wireless Sensor Network," *International Journal of Intelligent Engineering and Systems*, vol. 15, no. 5, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Rashmi Mishra, and Rajesh K. Yadav, "Energy Efficient Cluster-Based Routing Protocol for WSN Using Nature Inspired Algorithm," *Wireless Personal Communications*, vol. 130, no. 4, pp. 2407-2440, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] 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]

[5] Sanjeev Kumar, and Richa Agrawal, "A Hybrid C-GSA Optimization Routing Algorithm for Energy-Efficient Wireless Sensor Network," *Wireless Networks*, vol. 29, no. 5, pp. 2279-2292, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Ushus Elizebeth Zachariah, and Lakshmanan Kuppusamy, "A Hybrid Approach to Energy Efficient Clustering and Routing in Wireless Sensor Networks," *Evolutionary Intelligence*, vol. 15, no. 1, pp. 593-605, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Nageswararao Malisetti, and Vinay Kumar Pamula, "Energy Efficient Cluster Based Routing for Wireless Sensor Networks Using Moth Levy Adopted Artificial Electric Field Algorithm and Customized Grey Wolf Optimization Algorithm," *Microprocessors and Microsystems*, vol. 93, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Robin Abraham, and M. Vadivel, "An Energy Efficient Wireless Sensor Network with Flamingo Search Algorithm Based Cluster Head Selection," *Wireless Personal Communications*, vol. 130, no. 3, pp. 1503-1525, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Y. Alekya Rani, and E. Sreenivasa Reddy, "A Novel Energy-Efficient Clustering Protocol in Wireless Sensor Network: Multi-Objective Analysis Based on Hybrid Meta-Heuristic Algorithm," *Journal of Reliable Intelligent Environments*, vol. 8, no. 4, pp. 415-432, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] R. Sheeja, M. Mohamed Iqbal, and C. Sivasankar, "Multi-Objective-Derived Energy Efficient Routing in Wireless Sensor Network Using Adaptive Black Hole-Tuna Swarm Optimization Strategy," *Ad Hoc Networks*, vol. 144, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] R. Suresh Kumar et al., "Cluster Head Selection and Energy Efficient Multicast Routing Protocol-Based Optimal Route Selection for Mobile Ad Hoc Networks," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] 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]

[13] Anil Kumar et al., "Optimal Cluster Head Selection for Energy Efficient Wireless Sensor Network Using Hybrid Competitive Swarm Optimization and Harmony Search Algorithm," *Sustainable Energy Technologies and Assessments*, vol. 52, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Neelakandan Subramani et al., "Controlling Energy Aware Clustering and Multihop Routing Protocol for IoT Assisted Wireless Sensor Networks," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] V. Kavitha, and Kirupa Ganapathy, "Galactic Swarm Optimized Convolute Network and Cluster Head Elected Energy-Efficient Routing Protocol in WSN," *Sustainable Energy Technologies and Assessments*, vol. 52, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Walid Osamy et al., "TACTIRSO: Trust Aware Clustering Technique Based on Improved Rat Swarm Optimizer for WSN-Enabled Intelligent Transportation System," *The Journal of Supercomputing*, vol. 79, no. 6, pp. 5962-6016, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Sengathir Janakiraman, "Energy Efficient Clustering Protocol Using Hybrid Bald Eagle Search Optimization Algorithm for Improving Network Longevity in WSNs," *Multimedia Tools and Applications*, pp. 1-23, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Zongshan Wang et al., "Energy Efficient Cluster Based Routing Protocol for WSN Using Firefly Algorithm and Ant Colony Optimization," *Wireless Personal Communications*, vol. 125, no. 3, pp. 2167-2200, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] K. Dinesh, and S.V.N. Santhosh 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]

[20] 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, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] R. Nandha Kumar, and P. Srimanchari, "A Trust and Optimal Energy Efficient Data Aggregation Scheme for Wireless Sensor Networks using QGAOA," *International Journal of System Assurance Engineering and Management*, vol. 15, no. 3, pp. 1057-1069, 2024. [CrossRef] [Google Scholar] [Publisher Link]

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

[23] Perumalla Suman Prakash, Dwaram Kavitha, and Pakanati Chenna Reddy, "Safe and Secured Routing Using Multi-Objective Fractional Artificial Lion Algorithm in WSN," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Manar Khalid Ibraheem Ibraheem et al., "A Security-Enhanced Energy Conservation with Enhanced Random Forest Classifier for Low Execution Time Framework (S-2EC-ERF) for Wireless Sensor Networks," *Applied Sciences*, vol. 14, no. 6, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Anurag Shukla et al., "SEE2PK: Secure and Energy Efficient Protocol Based on Pairwise Key for Hierarchical Wireless Sensor Network," *Peer-to-Peer Networking and Applications*, vol. 17, no. 2, pp. 701-721, 2024. [CrossRef] [Google Scholar] [Publisher Link]