Journal of Theoretical and Applied Information Technology
15th February 2025. Vol.103. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TRUST-ENHANCED SECURE CLUSTER ROUTING IN WIRELESS SENSOR NETWORKS USING A MODIFIED MOTH FLAME OPTIMIZATION ALGORITHM

SOWMYASHREE M S[1],SARITHA I G[2], NAVEEN I G[3], SHASHIBHUSHAN G[4]

[1]Assistant Professor, Department of Electronics and Telecommunication Engineering, BMS Institute of Technology and Management, Karnataka, India
[2]Assistant Professor, Department of Electronics and Telecommunication Engineering, BMS Institute of Technology and Management, Karnataka, India
[3]Associate Professor, Department of Electronics and Communication Engineering, NITTE Meenakshi Institute of Technology, Karnataka,India
[4]Assistant Professor, Department of Electronics and Communication Engineering, Sir M Visveswaraya Institute of Technology, Karnataka, India

E-mail: [1]sowmyashree.m.s@bmsit.in ,[2]saritha.i.g@bmsit.in, [3]naveen.ig@nmit.ac.in, [4]sashibhushan_ec@sirmvit.edu

ABSTRACT

Wireless Sensor Networks (WSNs) are self-organizing systems composed of numerous small sensor nodes used to monitor and track various applications across extensive areas. In the context of healthcare, wireless sensor networks can play a crucial role by continuously monitoring patients' vital signs and ensuring timely data transmission to medical professionals. Despite their usefulness, WSNs face significant challenges related to energy consumption and security due to their open and limited resources. Implementing a Trust-based Modified Moth Flame Optimization (T-MMFO) algorithm in healthcare WSNs can help select secure and efficient routes for data transmission, thereby improving the overall reliability and longevity of the network. This enhanced security and energy efficiency ensure that critical health data is transmitted accurately and promptly, supporting better patient outcomes and more efficient healthcare delivery. The algorithm's performance was evaluated based on Packet Delivery Ratio (PDR), energy consumption, delay, and throughput. The results showed that T-MMFOA achieved a high PDR of 98.5% and 95.7% for networks with 200 and 400 nodes, respectively, outperforming existing methods like Fuzzy Grey Wolf Optimization (F-GWO), Quality of Service-aware Multipath Routing (QMR), Improved Duck and Traveller Optimization Multi-Hop Routing (IDTOMHR), and Quantum Behaviour and Gaussian Mutation Archimedes Optimization Algorithm (QGAOA)

Keywords: *Wireless Cluster-based Sensor Routing, Network Trust-based Modified Moth Flame Optimization, Malicious Attacks, Security.*

1. INTRODUCTION

A Wireless Sensor Network (WSN) is composed of interconnected Sensor Nodes (SNs) that communicate wirelessly [1]. WSNs are widely used in applications monitoring external and environmental conditions in remote areas [2]. Typically, WSNs are heterogeneous systems with small networks, low power consumption, advanced sensor hubs, and multiple base stations [3]. Sensor Nodes collect data from various locations, such as natural ecosystems, battlefields, and man-made environments, and relay this information to multiple base stations [4]. While SNs are constrained by limited battery power, memory, electromagnetic frequency, and communication capabilities, the base stations possess substantial processing power, energy resources, and data handling capacity. The base station acts as a gateway between the SNs and end users [5, 6]. Trust-based security approaches predict node behavior based on their historical

actions, assigning higher trust values to nodes with good behavior, thereby enhancing security [7]. However, traditional trust-based security methods face challenges such as inability to defend against multiple types of attacks, slow detection of malicious nodes, and high energy consumption [8].

The primary challenge in Wireless Sensor Networks (WSNs) is the limited energy supply of the sensors, which rely on non-replaceable batteries for power [9,10]. The lifespan of these sensors is directly tied to their battery life, making efficient energy use critical across the entire network [11]. To address this issue, energy-efficient methods like clustering techniques are employed to extend battery life [12]. By grouping sensors into clusters, selecting cluster heads (CHs), and optimizing routing paths, the number of active sensors in a transmission path is minimized, thereby reducing overall energy consumption [13,14].

However, beyond simply extending sensor life, many real-time and mission-critical applications demand guaranteed Quality of Service (QoS) [15]. At the same time, security remains a significant concern in WSNs due to the susceptibility of sensors to malicious attacks, stemming from their use of unreliable channels and unattended operation [16].

Given the dual challenges of energy consumption and security, robust trust-based methods have been developed to enhance the security of WSNs against malicious attacks. This research leverages the Moth Flame Optimization (MFO) algorithm, which outperforms other metaheuristic algorithms due to its high convergence rate. The MFO algorithm effectively minimizes the search space while reducing decision variables and avoiding local optima.

The major contributions of this research are outlined as follows:

- The Moth Flame Optimization (MFO) algorithm has been modified to T-MMFOA to enhance secure communication in WSNs, chosen for its high convergence rate and capability to avoid local optima.
- Trust-based MMFOA is employed for selecting secondary cluster heads (SCHs), enhancing security against malicious attacks while minimizing energy consumption.
- Secure route path selection is carried out using T-MMFOA, resulting in reduced packet loss and unnecessary energy consumption due to malicious attacks.

The research manuscript is organized as follows: Section 2 provides a literature review. Section 3 details the proposed T-MMFOA for secure communication. Section 4 presents the results and discussion of T-MMFOA. Section 5 concludes the research.

2. LITERATURE SURVEY

Jainendra Singh and colleagues [17] developed a Fuzzy Grey Wolf Optimization (F-GWO) algorithm aimed at enhancing energy efficiency in clustering and routing within Wireless Sensor Networks (WSNs). This innovative approach applied the F-GWO algorithm specifically for selecting Cluster Heads (CHs), incorporating a novel parameter into the fitness function for this purpose. By leveraging an opportunistic routing technique, the algorithm sought to reduce power consumption and achieve a more balanced distribution of energy usage among network nodes. Despite these advancements, the algorithm did not fully address the fitness function concerning both energy and distance, which led to packet loss issues in the network.

C. Mohanadevi and S. Selvakumar [18] proposed a Quality of Service-aware Multipath Routing (QMR) protocol designed to enhance energy efficiency in clustering and routing for Wireless Sensor Networks (WSNs). Their approach employed a hybrid algorithm combining Cuckoo Search and Particle Swarm Optimization to effectively cluster sensor nodes and select Cluster Heads (CHs), ensuring reliable data delivery. The protocol utilized multiple paths for transmitting data packets, thereby managing data traffic efficiently within the network and reducing overall energy consumption. However, it is worth noting that the effectiveness of the proposed method was evaluated only with a limited number of nodes.

B. Meenakshi and D. Karunkuzhali [19] introduced a Cluster Head-Enhanced Elman Spike Neural Network, optimized with a Hybrid Wild Horse and Chameleon Swarm Algorithm (CH-EESNN-Hyb-WH-CSOA-WSN), designed for energy-efficient clustering and routing in Wireless Sensor Networks (WSNs). The protocol initially employed the EESNN method to select Cluster Heads (CHs), followed by routing data through a trusted path. Subsequently, the hybrid WH-CSOA algorithm was used to determine the optimal path with minimal delay, resulting in high throughput. Despite these benefits, the method did not address security concerns within the network.

Mashael M. Asiri et al. [20] proposed the Improved Duck and Traveller Optimization (IDTO) protocol for cluster-based Multi-Hop Routing (IDTOMHR) to enhance energy efficiency in WSNs. The IDTO algorithm was initially used for selecting

Cluster Heads (CHs) and forming clusters. For optimal route selection, the Artificial Gorilla Troops Optimization (ATGO) method was applied. This approach utilized a fitness function with multiple input parameters for clustering and routing. However, the protocol's reliance on a large number of control packets for route path selection led to increased delays.

R. Nandha Kumar and P. Srimanchari [21] devised the Quantum Behavior and Gaussian Mutation Archimedes Optimization Algorithm (QGAOA) for energy-efficient clustering and routing in Wireless Sensor Networks (WSNs). This method involves three main stages: forming clusters, selecting Cluster Heads (CHs), and determining optimal routing paths. Initially, clusters are formed using the Voronoi-included K-means clustering algorithm. Following this, CHs are selected, and optimal routes are identified through the QGAOA method. However, the CH selection process heavily relies on node distance, trust, and energy levels.

S. Kantharaju Veerabadrappa et al. [22] proposed the Trust and Energy Multi-objective Hybrid Optimization Algorithm (TE-MHOA) for improving energy efficiency in WSN clustering and routing. This approach uses several fitness functions aimed at extending network lifespan, integrating Adaptive Particle Swarm Optimization and Monarch Butterfly Optimization (APSO-MBO) algorithms. It employs multiple route algorithms combined with intra and inter-cluster broadcasts. Nonetheless, this method does not account for distance when broadcasting data.

Overall, existing methods exhibit several limitations: they often neglect the fitness functions related to energy and distance, which can lead to packet loss; they are typically tested with a limited number of nodes; they overlook security issues; and they may use an excessive number of control packets, resulting in increased delays.

3. PROPOSED MODEL

In this study, the Trust-based Modified Moth Flame Optimization Algorithm (T-MMFOA) is employed to ensure secure and reliable communication. The T-MMFOA approach is structured into four key stages: sensor deployment, secure Cluster Head (CH) selection, cluster formation, and secure route path identification. By focusing on selecting secure CHs and routing paths, the method aims to mitigate the risk of malicious attacks during data transmission. This strategy effectively reduces both unnecessary data packets and energy consumption. The complete workflow of the T-MMFOA method is illustrated in Figure 1.

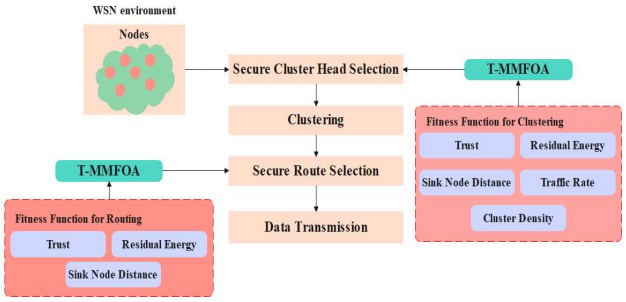

Figure 1 Process of the T-MMFOA method for Secure CHs and Routing in WSN

3.1 Sensor Deployment

In a Wireless Sensor Network (WSN), nodes are initially placed at random locations. Subsequently, the optimal secure cluster head and secure routes are chosen using the T-MMFOA (Trust-based Modified Multi-Factor Optimization Algorithm). This approach ensures secure and reliable data transmission within the network.

3.2 Secure CH Selection using the T-MMFOA method

Optimal secure Cluster Heads (CHs) from normal nodes are selected using the T-MMFOA method, which incorporates various fitness metrics. The Modified Firefly Optimization Algorithm (MFOA) is a metaheuristic approach that mimics the global exploration and local exploitation behaviors of moths. As a population-based metaheuristic algorithm, MFOA begins by randomly generating moths within the solution space. The process of secure CH selection based on the T-MMFOA method is detailed in the following sections.

3.2.1 Representation and Initialization

At the time of solution initialization, the set of nodes is considered secure Cluster Heads (CHs) when the dimension of each solution corresponds to the number of secure CHs. During this stage, each solution is assigned a sensor ID between 1 and N, where N represents the total number of sensors initialized in the WSN. The ith solution of T-MMFOA is denoted as $y_i=(y_{i,1},y_{i,2},\ldots,y_{i,D})$ where D represents the solution's dimension. The position of the solution $y_{i,rs}$, $1\leq rs\leq D$, describes a random sensor among all the sensors.

3.2.2 T-MMFOA Algorithm

The Moth-Flame Optimization (MFO) algorithm is a population-based metaheuristic technique. Initially, the MFO algorithm generates moths randomly within the solution space and then calculates the fitness values (positions) for each moth, marking the best positions with flames. Following this, the algorithm updates the moths' positions using a spiral movement function to move towards these superior locations. This process involves continuously updating the positions of the moths and marking new optimal locations, repeating until the stopping criteria are met. The MFO algorithm operates in three main stages: generating the initial population of moths, updating the moths' positions, and adjusting the number of flames.

- Generating the moth's initial population:

Let every moth fly in $1-\mathrm{D}, 2-\mathrm{D}, 3-\mathrm{D},$ or hyperdimensional space. For the moths group the formula is given in eq (1),

$$M\ is \begin{bmatrix} m_{1,1} & m_{1,2} & \dots & m_{1,d} \\ m_{2,1} & m_{2,2} & \dots & m_{2,d} \\ \dots & \dots & \dots & \dots \\ m_{n,1} & m_{n,2} & \dots & m_{n,d} \end{bmatrix}$$

Here, n represents the number of moths, and d denotes the number of dimensions in the solution space. The mathematical formula for calculating the fitness values of all moths is given in an array, represented as Equation (2).

$$OM = \begin{bmatrix} OM_1 \\ OM_2 \\ \dots \\ OM_n \end{bmatrix} \quad (2)$$

The remaining components in the MFO algorithm are the flames. The matrix formulas representing the flames in a D-dimensional space, based on their fitness values, are provided in Equations (3) and (4).

$$F = \begin{bmatrix} F_{1,1} & F_{1,2} & \dots & F_{1,d} \\ F_{2,1} & F_{2,2} & \dots & F_{2,d} \\ \dots & \dots & \dots & \dots \\ F_{n,1} & F_{n,2} & \dots & F_{n,d} \end{bmatrix} \quad (3)$$

$$OF = \begin{bmatrix} OF_1 \\ OF_2 \\ \dots \\ OF_n \end{bmatrix} \quad (4)$$

- In the MFO algorithm, both moths and flames represent solutions, but they differ in how their positions are updated in each iteration. Moths act as search agents, exploring the search space, while flames represent the best locations discovered by the moths so far. Flames serve as markers or flags placed by the moths during the search, guiding the moths to explore around these flags. As a result, each moth refines its search based on the positions of these flags, ensuring that the moths do not lose track of their best solutions.

- Updating Positions of Moth:

The MFO algorithm employs three variant functions to achieve global convergence in optimization problems. The mathematical formulas for these functions are provided in Equation (5).

$$MFO = (I, P, T) \quad (5)$$

where, I represents the initial random position of moths $(\mathrm{I}: \emptyset \rightarrow \{\mathrm{M}, \mathrm{OM}\})$, P represents moth's motion in search space $(\mathrm{P}: \mathrm{M} \rightarrow \mathrm{M})$ and T represents to end search process $(\mathrm{T}: \mathrm{M} \rightarrow \mathrm{true}; \mathrm{false})$. The next mathematical formula represents I function that is utilized to implement the random distribution and represented as eq (6),

Here, I represents the initial random position of moths, where I maps from the empty set $\emptyset$ to the set of moths M and optimal moths OM. P denotes the motion of the moths within the search space, mapping from M to M.T signifies the termination of the search process, mapping from M to a Boolean value (true or false). The mathematical formula for the I function, which implements the random distribution of moths, is provided in Equation (6).

$$M(i,j) = \big(ub(i) - lb(j)\big) * rand() + lb(i) \quad (6)$$

Here, lb represents the lower bounds of the variables, and ub denotes the upper bounds of the variables. Moths navigate the search space using a transverse location. There are three conditions that must be met when employing a logarithmic spiral, and the procedure for this is as follows:

- The initial point of the spiral must start from the moth's current position.
- The final point of the spiral must be at the location of the flame.

- Fluctuation of the spiral range must not extend a search space.

Thus, the logarithmic spiral for the MFO algorithm is defined by Equation (7)

$$S(M_i, F_j) = D_i \cdot e^{bt}.\cos(2\pi t) + F_j \quad (7)$$

Here, Di represents the distance between the i-th moth and the j-th flame, b is a constant that determines the shape of the logarithmic spiral, and t is a random number within the range [−1,1]. In the MFO algorithm, the balance between exploration and exploitation is maintained through the spiral motion of moths around flames within the search space. To prevent falling into local optima, the optimal solutions are saved in each iteration. Moths fly around flames, meaning each moth flies near the nearest flame using the OF and OM matrices.

- Updating number of flames

The exploitation stage of the MFO algorithm is enhanced by updating the position of the moth to n different positions in the search space, which helps minimize the chance of over-exploitation of superior results. Consequently, reducing the number of flames aids in addressing this issue, as represented by Equation (8).

$$flame\ no = round\left(N - l * \frac{N-l}{T}\right) \quad (8)$$

Here, N represents the maximum number of flames, l denotes the current number of iterations, and T stands for the maximum number of iterations. and T stands for the maximum number of iterations.

3.2.3 Fitness function for secure CHs selection

The fitness function utilized to select secure CHs by T-MMFOA is trust (ff_1), residual energy (ff_2), distance between nodes (ff_3), traffic rate (ff_4) and cluster density (ff_5). Mathematical formula for fitness function which is converted to one objective function (F) and represented as eq (9),

The fitness function used to select secure Cluster Heads (CHs) by T-MMFOA includes several metrics: trust (ff1), residual energy (ff2), distance between nodes (ff3), traffic rate (ff4), and cluster density (ff5). The mathematical formula for the fitness function, which is converted into a single objective function F, is represented as Equation (9),

$$F = \delta_1 \times ff_1 + \delta_2 \times ff_2 + \delta_3 \times ff_3 + \delta_4 \times ff_4 + \delta_5 \times ff_5 \quad (9)$$

Here, F represents the overall fitness function, while δ1 through δ5 are the weight metrics applied to each individual fitness function. The description of the fitness function used in T-MMFOA is detailed below:

- Trust

Trust is a crucial component of the fitness function for enhancing security against malicious activities in the selection of Cluster Heads (CHs). The trust measurement is based on the behavior of packet forwarding, specifically the relationship between the transmitted data (TDPij) and the received data (RDPij). The evaluated trust value (g1) is represented by Equation (10) and is used to mitigate Distributed Denial of Service (DDoS) attacks during data packet transmission.

$$ff_1 = g_1 = \frac{TDP_{ij}}{RDP_{ij}} \quad (10)$$

- Residual Energy

Secure Cluster Heads (SCHs) are responsible for receiving, collecting, and broadcasting data to the Base Station. Sensors with higher energy levels are preferred for subsequent hop SCHs. The energy utilization or execution is described by Equation (11).

$$ff_2 = \sum_{i=1}^{D} \frac{1}{E_{SCH_i}} \quad (11)$$

Where, E_{SCH_i} represents the remaining energy of ith SCH

- **Sink Node Distance**

In Wireless Sensor Networks (WSNs), sensors consume energy when broadcasting data from the transmitter SCHs to the Base Station (BS). The energy consumption of a sensor is directly proportional to the distance it transmits. Therefore, it is essential to select SCHs that are closer to Cluster Members (CMs) and the BS. The mathematical formula for calculating this distance is provided in Equation (12).

$$ff_4 = \sum_{i=1}^{D} dis(SCH_i, BS) \quad (12)$$

Where, $dis(SCH_i, BS)$ represents the distance between ith SCHs and BS

- Traffic Rate

Traffic rate is a measure of network efficiency, incorporating factors such as channel load, packet drop, and buffer usage. Traffic density is scaled based on the mean of these three parameters. The mathematical formula for calculating the traffic rate is provided in Equation (13).

$$ff_4 = \frac{1}{3}\left[B_{utilization} + P_{drop} + C_{load}\right] \quad (13)$$

Where, $B_{utilization}$ represents buffer usage, P_{drop} represents packet drop and C_{load} represents channel load.

- Cluster Density

Cluster density refers to the number of nodes within a cluster and affects communication efficiency. Higher density can lead to increased congestion and packet drops, while lower density typically results in more straightforward communication paths. Cluster density is calculated as the ratio of the number of nodes in a cluster to the total number of nodes. The mathematical formula for cluster density is given in Equation (14).

$$ff_5 = \frac{1}{M}\sum_{i=1}^{A}|Y_i| \quad (14)$$

Here, |Y_i| represents the number of nodes in the i-th cluster, M denotes the total number of nodes in the network, and A represents the total number of SCHs. Trust calculations in SCH selection help avoid attacker nodes, thereby reducing packet drops and unnecessary energy consumption. Node failures are mitigated by considering residual energy, and transmission distance is minimized by using the distance between nodes. Additionally, cluster density and traffic rate are used to enhance energy efficiency and improve network security against malicious attacks.

3.3 Cluster Generation

In the cluster generation process, normal sensors are assigned to selected SCHs. The potential function, which takes into account residual energy and distance, is represented by Equation (15). This function is used to assign normal sensors to the chosen SCHs.

$$Potential\ function\ (N_i) = \frac{E_{SCH}}{dis(N_i, SCH)} \quad (15)$$

3.4 Route Path Selection Using the T-MMFOA method

The T-MMFOA method is employed for route path selection. The steps for selecting route paths are as follows:

- Initial paths from transmitter SCHs to the Base Station (BS) are considered as early solutions for route path selection. The dimension of each solution corresponds to the number of SCHs in the route.
- The fitness function, which incorporates trust, energy, and distance, is given by Equation (16) and is used to update the position of the solution. The position update for route path selection is carried out based on the iteration process of T-MMFOA.

$$Routing\ fitness = \tau_1 \times \frac{TDP_{ij}}{RDP_{ij}} + \tau_2 \times \sum_{i=1}^{D}\frac{1}{E_{SCH_i}} + \tau_3 \times distance \quad (16)$$

Here, τ1, τ2 and τ3 are weight parameters used in the fitness function for route path selection. Consequently, an optimal secure route is selected to enhance WSN security and improve data delivery.

4. RESULTS AND DISCUSSION

The performance of the proposed T-MMFOA algorithm was simulated using MATLAB R2018a, with the following system specifications: Intel Core i6 processor, Windows 10 operating system, and 6 GB RAM. The evaluation of the T-MMFOA algorithm was conducted with varying numbers of nodes. The selection of SCHs and secure route paths was performed by T-MMFOA to achieve secure communication. The simulation parameters for the T-MMFOA method are detailed in Table 1.

Journal of Theoretical and Applied Information Technology
15th February 2025. Vol.103. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1 Simulation Parameters

Parameters	Values
Cluster based routing method	T-MMFOA
Area	1000m x 1000m
Number of Nodes	100, 200, 300, 400 and 500
Packet size	512 bytes

4.1 Quantitative and Qualitative Analysis

The performance of the proposed T-MMFOA algorithm is evaluated based on Packet Delivery Ratio (PDR), energy consumption, throughput, and delay. To assess its effectiveness, the T-MMFOA algorithm is compared with existing algorithms such as Grey Wolf Optimization (GWO), Whale Optimization Algorithm (WOA), Particle Swarm Optimization (PSO), and Moth Flame Optimization (MFO), which were developed for similar specifications.

Table 2 Packet Delivery Ratio (%) vs Number of Nodes

No. of Nodes	Packet Delivery Ratio (%)				
	GWO	WOA	PSO	MFO	T-MMFOA
100	91.4	93.6	95.3	97.4	99.1
200	90.9	92.4	94.8	96.7	98.5
300	89.1	91.9	93.4	95.2	96.9
400	88.0	90.5	92.7	94.1	95.7
500	87.2	89.3	91.6	93.5	94.3

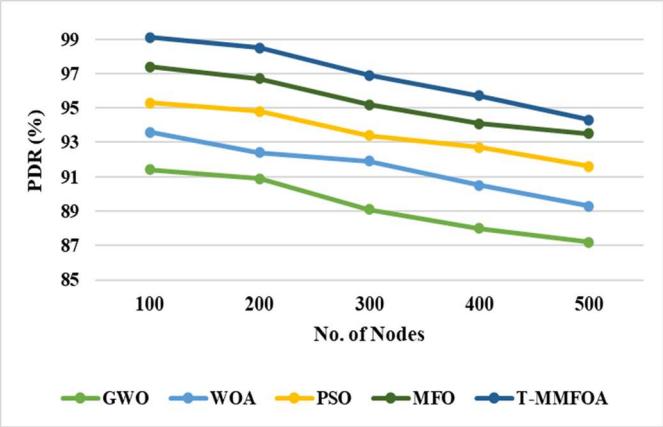

Figure 2 Packet Delivery Ratio (%) vs Number of Nodes

Table 2 and Figure 2 illustrate the performance of the proposed algorithm in terms of Packet Delivery Ratio (PDR). PDR is defined as the ratio of the number of packets received by the base station to the number of packets transmitted by the transmitter node. The proposed algorithm achieved high PDR values of 99.1%, 98.5%, 96.9%, 95.7%, and 94.3% for 100, 200, 300, 400, and 500 nodes, respectively. These results demonstrate the superior performance of the proposed algorithm compared to existing algorithms such as GWO, WOA, PSO, and MFO.

Table 3 Throughput (%) vs Number of Nodes

No. of Nodes	Throughput (%)				
	GWO	WOA	PSO	MFO	T-MMFOA
100	87.3	89.6	91.3	93.4	95.2
200	88.9	90.7	92.5	94.7	96.7
300	89.5	91.4	93.3	95.2	97.4
400	90.7	92.9	94.8	96.6	98.6
500	91.6	93.5	95.2	97.0	99.2

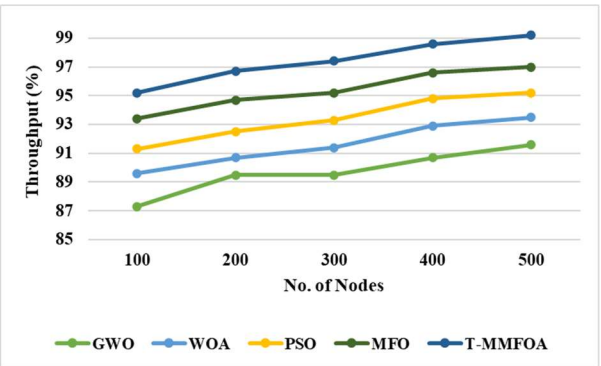

Figure 3 Throughput (%) vs Number of Nodes

Table 3 and Figure 3 present the performance of the proposed algorithm in terms of throughput. Throughput is defined as the percentage of data packets successfully received at the Base Station (BS). The proposed algorithm achieved high throughput rates of 95.2%, 96.7%, 97.4%, 98.6%, and 99.2% for 100, 200, 300, 400, and 500 nodes, respectively. These results indicate that the proposed algorithm outperforms existing algorithms such as GWO, WOA, PSO, and MFO.

Table 4 Delay (ms) vs Number of Nodes

No. of Nodes	Delay (ms)				
	GWO	WOA	PSO	MFO	T-MMFOA
100	10.7	9.4	7.9	5.2	2.9
200	11.4	10.6	8.6	6.1	3.3
300	12.3	11.8	9.1	6.9	4.5
400	13.8	12.5	9.9	7.6	6.7
500	14.4	13.7	10.4	8.3	7.4

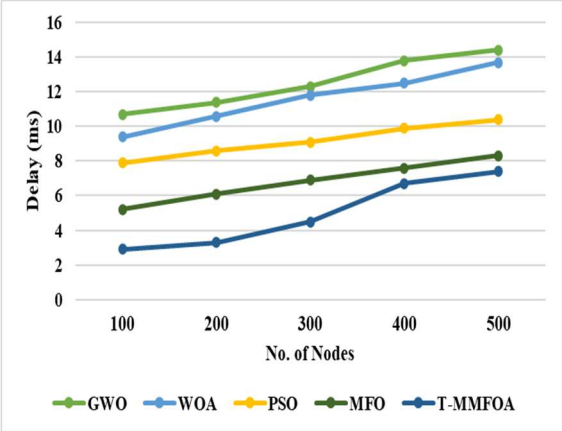

Figure 4 Delay (ms) vs Number of Nodes

Table 4 and Figure 4 showcase the performance of the proposed algorithm in terms of delay. Delay is defined as the amount of time required to transmit data packets from the source to the Base Station (BS). The proposed algorithm achieved lower delays of 2.9 ms, 3.3 ms, 4.5 ms, 6.7 ms, and 7.4 ms for 100, 200, 300, 400, and 500 nodes, respectively. These results demonstrate that the proposed algorithm outperforms existing algorithms such as GWO, WOA, PSO, and MFO in terms of reducing transmission delay.

Table 5 Energy Consumption (J) vs Number of Nodes

No. of Nodes	Energy Consumption (J)				
	GWO	WOA	PSO	MFO	T-MMFOA
100	13.4	11.5	9.4	7.2	5.3
200	15.6	13.7	11.2	8.8	6.6
300	16.9	14.6	12.7	9.6	7.3
400	18.2	16.3	13.9	10.9	8.2
500	19.4	17.8	15.2	12.1	8.9

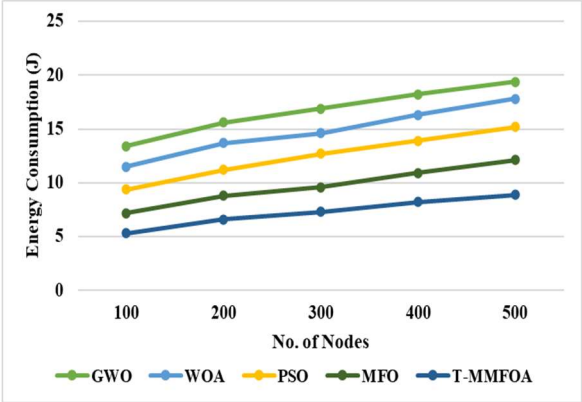

Figure 5 Energy Consumption (J) vs Number of Nodes

Table 5 and Figure 5 illustrate the performance of the proposed algorithm in terms of energy consumption. Energy consumption is defined as the amount of energy expended by each node in the Wireless Sensor Network (WSN), measured in joules (J). The proposed algorithm achieved lower energy consumption values of 5.3 J, 6.6 J, 7.3 J, 8.2 J, and 8.9 J for 100, 200, 300, 400, and 500 nodes, respectively. These results indicate that the proposed algorithm is more efficient in terms of energy consumption compared to existing algorithms such as GWO, WOA, PSO, and MFO.

4.2 Comparative Analysis

The performance of the proposed T-MMFOA algorithm is compared with existing algorithms such as F-GWO [17], QMR [18], IDTOMHR [20], and QGAOA [21]. Table 6 provides a comparative analysis, showing that the T-MMFOA algorithm outperforms these existing algorithms. As demonstrated in Table 2, the T-MMFOA algorithm achieves superior performance across various metrics. The proposed T-MMFOA algorithm enhances robustness against malicious attacks, thereby improving data delivery and extending the life expectancy of the Wireless Sensor Network (WSN).

Table 6 Comparative Analysis Of The T-MMFOA Method

Performance Measures	Methods	No. of Nodes	
		200	400
Packet Delivery Ratio (%)	F-GWO [17]	98	96
	QGAOA [21]	95.2	95
	Proposed T-MMFOA	98.5	95.7
Delay (ms)	F-GWO [17]	4	7
	CH-EESNN-Hyb-WH-CSOA-WSN [19]	17.5	-
	QGAOA [21]	13.24	16.21
	Proposed T-MMFOA	3.3	6.7
Energy Consumption (J)	QMR [18]	7	-
	IDTOMHR [20]	7.6	-
	Proposed T-MMFOA	6.6	8.2

4.3 Discussion

This section outlines the limitations of existing algorithms and highlights the advantages of the proposed algorithm in secure Cluster Head (CH) and route path selection.

- F-GWO [17] and QMR [18]: These methods do not account for the fitness functions related to energy and distance, leading to packet drops within the network. In contrast, the proposed T-MMFOA considers residual energy, which helps prevent node failures and reduces unnecessary packet drops.
- CH-EESNN-Hyb-WH-CSOA-WSN [19]: This technique does not address security issues in the WSN. The proposed T-MMFOA incorporates a trust-based fitness function, enhancing security and mitigating malicious attacks.
- IDTOMHR [20] and QGAOA [21]: These methods suffer from limitations due to the high number of control packets used in route path selection, which results in increased delay. The proposed T-MMFOA achieves lower delay by generating shorter paths and minimizing the use of control packets during route path selection.

5. CONCLUSION

In this research, a secure cluster-based routing protocol has been developed using T-MMFOA to improve security against malicious attacks which avoids snooping of patient's data through remote monitoring in healthcare applications. T-MMFOA is employed to select Cluster Heads (SCHs) from normal sensors and determine route paths through SCHs, effectively mitigating malicious attacks during communication. Additionally, T-MMFOA enhances WSN energy efficiency and supports secure and reliable communication, contributing to the overall life expectancy of the network. By utilizing the shortest route obtained from T-MMFOA, delay is reduced across the WSN, leading to improved data transmission. Experimental results demonstrate that T-MMFOA outperforms existing algorithms such as F-GWO, QMR, IDTOMHR, and QGAOA. Specifically, T-MMFOA achieved high Packet Delivery Ratios (PDR) of 98.5% and 95.7% for 200 and 400 nodes, respectively, surpassing the performance of the aforementioned algorithms. Future work could explore hybrid optimization algorithms to further enhance WSN performance.

REFERENCES

[1]. Dinesh, K. and Santhosh Kumar, S.V.N., 2023. Energy-efficient trust-aware secured neuro-fuzzy clustering with sparrow search optimization in wireless sensor network. International Journal of Information Security, pp.1-25.

[2]. Kumar, S. and Agrawal, R., 2023. A hybrid C-GSA optimization routing algorithm for energy-efficient wireless sensor network. Wireless Networks, pp.1-14.

[3]. Wang, Z., Ding, H., Li, B., Bao, L., Yang, Z. and Liu, Q., 2022. Energy efficient cluster based routing protocol for WSN using firefly algorithm and ant colony optimization. Wireless Personal Communications, 125(3), pp.2167-2200.

[4]. Mishra, R. and Yadav, R.K., 2023. Energy Efficient Cluster-Based Routing Protocol for WSN Using Nature Inspired Algorithm. Wireless Personal Communications, 130(4), pp.2407-2440.

[5]. Supriya, M. and Adilakshmi, T., 2023. Security Aware Cluster-Based Routing Using MTCSA and HEA for Wireless Sensor

Networks. International Journal of Intelligent Systems and Applications in Engineering, 11(2), pp.663-669.
[6]. Ramachandra, B. and Surekha, T.P., 2022. Secure Cluster based Routing Using Improved Moth Flame Optimization for Wireless Sensor Networks. International Journal of Intelligent Engineering & Systems, 15(4).
[7]. Rao, S.S. and Reddy, K.C.K., 2022. An Energy Efficient Clustering based Optimal Routing Mechanism using IBMFO in Wireless Sensor Networks. International Journal of Intelligent Systems and Applications in Engineering, 10(4), pp.641-651.
[8]. Alrayes, F.S., Alzahrani, J.S., Alissa, K.A., Alharbi, A., Alshahrani, H., Elfaki, M.A., Yafoz, A., Mohamed, A. and Hilal, A.M., 2022. Dwarf mongoose optimization-based secure clustering with routing technique in internet of drones. Drones, 6(9), p.247.
[9]. Han, Y., Hu, H. and Guo, Y., 2022. Energy-aware and trust-based secure routing protocol for wireless sensor networks using adaptive genetic algorithm. IEEE Access, 10, pp.11538-11550.
[10]. Veerabadrappa, K. and Lingareddy, S.C., 2022. Secure Routing using Multi-Objective Trust Aware Hybrid Optimization for Wireless Sensor Networks. International Journal of Intelligent Engineering & Systems, 15(1).
[11]. Dinesh Kumar, P. and Valarmathi, K., 2023. Fuzzy based hybrid BAT and firefly algorithm for optimal path selection and security in wireless sensor network. Automatika, 64(2), pp.199-210.
[12]. Gulganwa, P. and Jain, S., 2022. EES-WCA: energy efficient and secure weighted clustering for WSN using machine learning approach. International Journal of Information Technology, 14(1), pp.135-144.
[13]. Balamurugan, A., Janakiraman, S., Priya, M.D. and Malar, A.C.J., 2022. Hybrid Marine predators optimization and improved particle swarm optimization-based optimal cluster routing in wireless sensor networks (WSNs). China Communications, 19(6), pp.219-247.
[14]. Asha, A., Verma, N. and Poonguzhali, I., 2023. Multi-objective-derived energy efficient routing in wireless sensor networks using hybrid African vultures-cuckoo search optimization. International Journal of Communication Systems, 36(6), p.e5438.
[15]. Kingston Roberts, M. and Thangavel, J., 2023. An improved optimal energy aware data availability approach for secure clustering and routing in wireless sensor networks. Transactions on Emerging Telecommunications Technologies, 34(3), p.e4711.
[16]. Sudha, G. and Tharini, C., 2023. Trust-based clustering and best route selection strategy for energy efficient wireless sensor networks. Automatika, 64(3), pp.634-641.
[17]. Singh, J., Deepika, J., Sathyendra Bhat, J., Kumararaja, V., Vikram, R., Jegathesh Amalraj, J., Saravanan, V. and Sakthivel, S., 2022. Energy-efficient clustering and routing algorithm using hybrid fuzzy with grey wolf optimization in wireless sensor networks. Security and Communication Networks, 2022.
[18]. Mohanadevi, C. and Selvakumar, S., 2022. A qos-aware, hybrid particle swarm optimization-cuckoo search clustering based multipath routing in wireless sensor networks. Wireless Personal Communications, 127(3), pp.1985-2001.
[19]. Meenakshi, B. and Karunkuzhali, D., 2023. Enhanced Elman spike neural network for cluster head based energy aware routing in WSN. Transactions on Emerging Telecommunications Technologies, 34(3), p.e4708.
[20]. Asiri, M.M., Alotaibi, S.S., Elkamchouchi, D.H., Aziz, A.S.A., Hamza, M.A., Motwakel, A., Zamani, A.S. and Yaseen, I., 2022. Metaheuristics Enabled Clustering with Routing Scheme for Wireless Sensor Networks. CMC-COMPUTERS MATERIALS & CONTINUA, 73(3), pp.5491-5507.
[21]. Kumar, R.N. and Srimanchari, P., 2023. A trust and optimal energy efficient data aggregation scheme for wireless sensor networks using QGAOA. International Journal of System Assurance Engineering and Management, pp.1-13.
[22]. Veerabadrappa, K. and Lingareddy, S.C., 2022. Trust and Energy Based Multi-Objective Hybrid Optimization Algorithm for Wireless Sensor Network. International Journal of Intelligent Engineering & Systems, 15(5).