Received: January 2, 2024. Revised: March 11, 2024.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Secure Cluster Based Routing Using Trust-based Modified Moth Flame Optimization Algorithm for WSN

Sowmyashree Malligehalli Shivakumaraswamy[1]* **Saritha Ibakkanavar Guddappa**[1]
Naveen Ibakkanavar Guddappa[2]

[1]*Department of Electronics and Telecommunication Engineering,*
BMS Institute of Technology and Management Bengaluru-56064, India
[2]*Department of Electronics and Communication Engineering,*
Nitte Meenakshi Institute of Technology, Bengaluru, India
* Corresponding author's Email: sowmyashree.m.s@bmsit.in

Abstract: Wireless sensor networks (WSN) is a self-organization network that contains many small sensor nodes utilized to track and monitor the application in a wide range. However, energy consumption and security are two vital problems in WSN due to open resources and limited energy resources. In this research, a Trust-based Modified Moth Flame Optimization (T-MMFO) algorithm is proposed for secure cluster-based routing in WSN. The proposed T-MMFO is utilized to select Secure CHs and routes to attain secure communication over the network. The proposed T-MMFOA gives enhanced security against malicious attacks by improving energy efficiency. The important aim of T-MMFOA is to attain secured data transmission and maximize WSN life expectancy. The Performance of T-MMFOA is estimate through packet delivery ratio (PDR), Energy consumption, Delay, and Throughput. The proposed T-MMFO algorithm attained high PDR of 98.5% and 95.7% for 200 and 400 nodes which is superior to other 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 behavior and gaussian mutation archimedes optimization algorithm (QGAOA).

Keywords: Cluster-based routing, Malicious attacks, Security, Trust-based modified moth flame optimization, Wireless sensor network.

1. Introduction

A wireless sensor network (WSN) is interconnected with sensor nodes (SN) which are combined in the network through wireless [1]. WSN finds regions of applications for observing the external and environmental positions of remote locations [2]. Commonly, WSNs are taken as heterogeneous executing applications which has small network, less power, advanced sensor hubs, and many base stations [3]. SN gathers information in various locations including natural ecosystems, battlefields, and man-made environments, and communicates it with many base stations [4]. The SNs have limited battery power, memory, electromagnetic frequency, and capability of communication but the base station has huge intellectual, energy, and data regarding quality. Between SNs and end users, a base station helps as a gateway [5, 6]. The trust-based security approaches have predicted the node behavior in further moments depending on their historical behavior [7]. The good node behavior has high trust values and security, however, classical trust-based security approaches have limitations like can't able to defend against multiple attack types, not being fast enough to find malicious nodes, and high energy consumption [8].

The main problem of WSN is the limited energy of sensors. The sensor receives energy from the involved battery that is irreplaceable [9, 10]. The sensor's life expectancy is represented through battery power; hence energy is needed to be efficiently used in the whole network [11]. The energy-efficient method such as the clustering-based technique is utilized to resolve the problem related to battery lifetime [12]. The sensors clustering, selection of CH, and routing are utilized to reduce the amount of participating sensors in the path which helps to reduce energy consumption [13, 14]. Though, separately increasing life expectancy, various real-time and mission-crucial application requires assurance of quality of service (QoS) [15]. Simultaneously, security is a crucial issue in WSN due to unreliable channels and unattended operation disclosures the vulnerability of sensors to malicious attacks [16]. Energy consumption and security are two essential problems due to open resources and limited energy resources. For the security of WSN, trust-based methods have been established which have high robustness against malicious attacks. In this research, moth flame optimization (MFO) is used over other metaheuristic algorithms because MFO has a high convergence rate. The MFO algorithm causes simultaneous minimization of search space and also decision variables are less and avoided local optimum. To ensure the security of WSN, trust based methods has to include to be hugely robustness against malicious nodes.

The major contributions of the research are described below:

- The moth flame optimization (MFO) algorithm is modified to T-MMFOA for secure communication in WSN. The MFO is chosen because of their high convergence rate and avoided local optimal.
- Trust-based MMFOA is utilized for performing SCHs selection that enhanced the security against malicious attacks and minimized the energy efficiency.
- The Secure route path selection is performed by T-MMFOA. Hence, the proposed algorithm reduced the packet loss and unnecessary energy consumption caused by malicious attacks.

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

2. Literature review

Singh [17] implemented a fuzzy grey wolf optimization (F-GWO) algorithm for energy-efficient clustering and routing protocol for WSN. The F-GWO algorithm was utilized for the cluster head selection. A new parameter was utilized in F-GWO to choose the CHs and the terminology used was fitness function. The opportunistic routing method was utilized which minimizes power usage and balances the energy consumption among nodes in WSN. The fuzzy parameters were evaluated with an algorithm that produced an enhanced route. However, the implemented algorithm failed to consider the fitness function of energy and distance that cause packet drop in the network.

Mohanadevi and Selvakumar [18] introduced a quality of service-aware multipath routing (QMR) method for energy-efficient clustering and routing protocol for WSN. In the introduced protocol, a hybrid Cuckoo search and particle swarm optimization algorithm was utilized for clustering sensor nodes and choosing CHs to ensure sure reliability of data delivery. The introduced protocol utilized various paths to deliver data packets and contained highly manageable over-data traffic in a network. The introduced protocol minimized the consumption of energy with a network. However, the introduced method analyzed only with a smaller number of nodes.

Meenakshi and Karunkuzhali [19] presented a cluster head-enhanced elman spike neural network optimized with hybrid wild horse optimization and chameleon swarm algorithm-WSN (CH-EESNN-Hyb-WH-CSOA-WSN) protocol for energy efficient clustering and routing protocol for WSN. Initially, the EESNN method was used to select CHs and after CHs selection, data was sent through a trusted route path. Next, hybrid WH-CSOA was implemented to identify the optimal path with less delay. The presented method provided high throughput. However, the presented algorithm failed to consider security issues in the WSN network.

Asiri [20] suggested improved duck and traveller optimization (IDTO) enabled cluster-based multi-hop routing (IDTOMHR) protocol for energy-efficient clustering and routing protocol for WSN. Initially, the IDTO algorithm was used to choose cluster heads (CHs) and cluster constructions. The artificial gorilla troops optimization (ATGO) method was utilized to originate an optimum group of routes for an endpoint. The clustering and routing methods utilized fitness function with the presence of multi-input parameters. However, the suggested method utilized a huge number of control packets in route path selection which caused to maximized the delay.

Kumar and Srimanchari [21] developed a quantum behavior and gaussian mutation archimedes optimization algorithm (QGAOA) method for energy-efficient clustering and routing protocol for

Received: January 2, 2024. Revised: March 11, 2024.

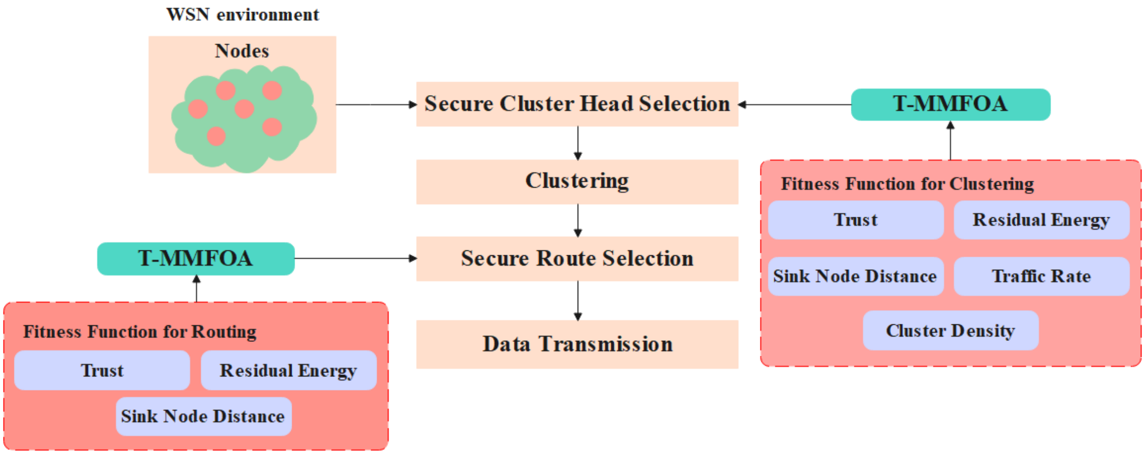

Figure. 1 Process of the T-MMFOA method for secure CHs and routing in WSN

WSN. The developed method has three stages formation of cluster, cluster heads, and optimum route selection. Primarily, clusters were developed by utilizing the Voronoi-included K-means clustering algorithm. Next, CHs were chosen and optimum routing was chosen by the QGAOA method. However, the CH selection was majorly dependent on node distance, trust, and energy.

Veerabadrappa and Lingareddy [22] introduced a trust and energy multi-objective hybrid optimization algorithm (TE-MHOA) method for energy-efficient clustering and routing protocol for WSN. The introduced method has several fitness functions to enhance the lifetime of the network. Hybrid optimization methods have adaptive particle swarm optimization and monarch butterfly optimization (APSO-MBO) algorithms. Multiple route algorithms were utilized in combination with multiple hop intra and inter-cluster broadcasts. However, the introduced method does not consider distance when data broadcasting.

Seresane Venkata Krishna Reddy [23] implemented a multiobjective-trust centric reptile search algorithm (M-TCRSA) for secure cluster-based routing. The implemented method was utilized for ensuring SCH and secure route selection for attaining reliable communication across WSN. The implemented method provided highest security against malicious nodes when improving energy efficiency.

The existing methods have limitations like failing to consider the fitness function of energy and distance that cause packet drop in the network. Analyzed only with a smaller number of nodes and failed to consider security issues. Utilized a huge number of control packets in route path selection which caused to maximized the delay.

3. Proposed method

In this research, secure and reliable communication is made by utilizing the trust-based modified moth flame optimization algorithm (T-MMFOA). The proposed T-MMFOA method has four stages sensor deployment, selection of secure cluster heads, cluster formation and secure route path selection. The secure cluster head and route path selection are utilized to avoid malicious attacks when transmitting the data packets. Hence, unnecessary data packets and energy consumption are reduced by utilizing the proposed T-MMFOA method. The overall process of the T-MMFOA method is given in Fig. 1.

3.1 Sensor deployment

Primarily, nodes are randomly located in WSN followed by optimum secure cluster head and secure routes are selected by utilizing T-MMFOA which supports attaining secure reliable data transmission in a network.

3.2 Secure CH selection using the T-MMFOA method

The optimum secure CHs from normal nodes are selected by utilizing a T-MMFOA method with different fitness metrics. The MFOA is one of the metaheuristic algorithms that replicates the moth's global exploration and local exploitation behavior. The MFOA is a population-based metaheuristic algorithms, it is initialized by producing moths randomly in solution space. The T-MMFOA method-based secure CH selection is described in the next sections.

3.2.1. Representation and initialization

The set of nodes is considered as secure CHs at the time of solution initialization when the dimension of every solution is the same as to number of secure CHs. In that stage, every solution is set with sensor ID among 1 and N, where N represents the total sensors initialized in WSN. Consider ith solution of T-MMFOA is represented as $y_i = (y_{i,1}, y_{i,2}, \dots, y_{i,D})$, where D represents the solution's dimension. The position of the solution is $y_{i,rs}, 1 \leq rs \leq D$ that described random senor among entire sensors.

3.2.2. T-MMFOA algorithm

The moth-flame optimization (MFO) algorithm is the population-based metaheuristic algorithm. MFO algorithm produced moths randomly in solution space, next calculated fitness values (which is position) of every moth and tagging superior location through flame. After, updating the position of the moth based on the spiral movement function to attain superior locations tagged through the flame, updating new good individual positions and repeating the prior process till the stopping criteria are reached. The MFO algorithm contains three major stages such as producing the moth's initial population, updating the position of the moth, and updating the number of flames.

- **Generating the moth's initial population:**

Let's consider that every moth will fly in $1 - D, 2 - D, 3 - D,$ or hyperdimensional space. The mathematical formula for a group of moths is given as Eq. (1),

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

Where n represents the number of moths, d represents the count of dimensions in solution space. The mathematical formula of fitness value for entire moths is given in array and represented as Eq. (2),

$$OM = \begin{bmatrix} OM_1 \\ OM_2 \\ \dots \\ OM_n \end{bmatrix} \tag{2}$$

The rest components in the MFO algorithm are flames. The next matrix formula represents flames in D −dimensional space through its fitness value and represented as Eq. (3) and (4),

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

$$OF = \begin{bmatrix} OF_1 \\ OF_2 \\ \dots \\ OF_n \end{bmatrix} \tag{4}$$

The moths and flames are the solutions and the only difference between them is how position is updated in every iteration. Moths are searching agent that moves around search space and flames are the superior location of moths which attained so far. The flames are taken as flags that are dropped through moths while searching to search space. Hence, every moth searches around flag and updated it in identifying superior solution. With this algorithm moth can't loses their superior solution.

- **Updating positions of moth:**

The MFO assigns 3 variant functions to converge global optimum of optimization issues. The mathematical formula for these functions is represented as Eq. (5),

$$MFO = (I, P, T) \tag{5}$$

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

$$M(i,j) = \big(ub(i) - lb(j)\big) \times rand() + lb(i) \tag{6}$$

Where lb represents the lower bounds of variables, ub represents the upper bounds of variables. Moths fly in search space utilizing a transverse location. 3 circumstances must be while using a logarithmic spiral and the procedure is represented as follows:

- The early point of the spiral should begin from moth
- The last point of the spiral should be the location of the flame
- Fluctuation of the spiral range must not extend a search space.

Hence, a logarithmic spiral for MFO algorithm is measured by Eq. (7),

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

Where, D_i represents space among ith and jth flame, b represents a fix to determine logarithmic spiral shape and t represents random number among $[-1,1]$. In MFO algorithm balancing between exploration and exploitation is assured through the spiral motion of moth nearby flame within the search space. To avoid falling in traps to local optimum, optimum solutions have been saved in every recurrence and moths fly around flames (that is every moth flies near the nearest flame by utilizing OF and OM matrices).

- **Updating number of flames**

The exploitation stage of the MFO algorithm is enhanced, which means the position of the moth is updated in n different positions in the search space may minimize the exploitation chance of superior results. Hence, minimizing the number of flames supports to resolve the problem based on Eq. (8),

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

Where N represents the maximum no. of flames, l represents a present number of iterations and T represents the maximum no. 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),

$$F = \delta_1 \times ff_1 + \delta_2 \times ff_2 + \delta_3 \times ff_3 + \delta_4 \times ff_4 + \delta_5 \times ff_5 \tag{9}$$

Where, F represents the overall fitness function, $\delta_1 - \delta_5$ represents weight metrics employed for every fitness function. The description of the fitness function utilized in T-MMFOA is represented below:

- **Trust**

Trust is an essential component in fitness function to strengthen the security against malicious activities in CHs selection. The trust measures depended on the behavior of packet forwarding that is the relationship between transmitted (TDP_{ij}) and received (RDP_{ij}) data. The evaluated trust value (g_1) is represented as Eq. (10) and utilized to mitigate DDoS attacks while transmitting data packets.

$$ff_1 = g_1 = \frac{TDP_{ij}}{RDP_{ij}} \tag{10}$$

- **Residual energy**

The SCHs are needed to receive, collect, and broadcast data to the Base Station. A sensor with more energy is considered for following hop SCH and the energy execution is described as Eq. (11),

$$ff_2 = \sum_{i=1}^{D} \frac{1}{E_{SCH_i}} \tag{11}$$

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

- **Sink node distance**

Sensors in WSNs consumed energy when broadcast data from transmitter SCHs and BS. The energy consumption of the sensor is directly proportional to the transmitted distance. Hence, it is needed to select SCH that has less distance from CMs and BS. The mathematical formula for distance is given as Eq. (12),

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

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

- **Traffic rate**

Traffic rate is the less efficient network that includes traffic density which is based on channel load network, packet drop, buffer usage, and scaling of traffic density is based on a mean of 3 parameters. The mathematical formula for traffic rate is given as Eq. (13),

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

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

- **Cluster density**

Cluster density is referred to as node which specifies how to communicate less in an easy path.

while high density raises congestion with packet drop. Density is the proportion of the entire cluster to entire nodes. The mathematical formula for cluster density is given as Eq. (14),

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

Where, $|Y_i|$ represents ith cluster nodes, M represents the total node in the network and A represents the total number of SCHs. The trust calculates taken in SCH selection avoid attacker nodes that support to reduce the packet drop and unnecessary consumption of energy. The node failure is avoided by utilizing residual energy and transmission distance is reduced through utilizing distance between two nodes. Additionally, cluster density and traffic rate are utilized to enhance energy efficiency when improving network security against malicious attacks.

3.3 Cluster generation

In the process of cluster generation, normal sensors are assigned to SCHs. Residual energy and distance are considered in potential function which is represented as Eq. (15) that is utilized to employ normal sensors to selected SCHs.

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

3.4 Route path selection using the T-MMFOA method

The T-MMFOA method is utilized to process the route path selection. The steps utilized to route path selection are given below:

- The probable paths from transmitter SCHs to BS are taken as early solutions to select route paths. The dimension of every result is the same as the amount of SCHs present in the route.
- Moreover, the fitness function executed by trust, energy, and distance is given as Eq. (16) and is utilized to update the position of the solution. The position update of route path selection is performed depending on the iteration process of T-MMFOA.

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

Where, $\tau_1, \tau_2\ and\ \tau_3$ are represented as weight parameters employed for the fitness function of route path selection. Therefore, an optimum secure route is chosen to improve the WSN security that improves data delivery.

4. Experimental results

Table 2 and Fig. 2 represent the performance of the proposed algorithm with performance metrics of PDR. The PDR is referred to as the ratio between the number of packets received by the base station and the number of packets broadcast through the transmitter node. The proposed algorithm attained the high PDR of 99.1%, 98.5%, 96.9% 95.7% and 94.3% for 100, 200, 300, 400 and 500 nodes which is superior to other existing algorithms like GWO, WOA, PSO and MFO.

The performance of the proposed T-MMFOA algorithm is simulated with MATLAB R2018a with system requirements of the processor – intel core i6, operating system – windows 10, and RAM – 6 GB. The estimation of the T-MMFOA algorithm is performed through varying numbers of nodes. The SCHs and secure route path selection are performed by T-MMFOA to attain secure communication. The simulation parameters of the T-MMFOA method are represented in Table 1.

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 estimated by packet delivery ratio (PDR), energy consumption, throughput, and delay. The existing algorithms utilized to evaluate the proposed algorithm are grey wolf optimization (GWO), whale optimization algorithm (WOA), particle swarm optimization (PSO), and moth flame optimization (MFO) which were developed for similar specifications to the proposed T-MMFOA.

Table 3 and Fig. 3 represent the performance of the proposed algorithm with performance metrics of throughput. The throughput is referred to as number of data packets received at BS and throughput is evaluated in percentage. The proposed algorithm attained a high throughput of 95.2%, 96.7%, 97.4%

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

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

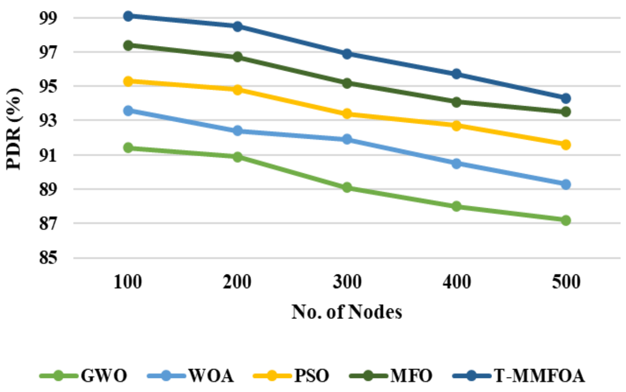

Figure. 2 Packet delivery ratio (%) vs number of nodes

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

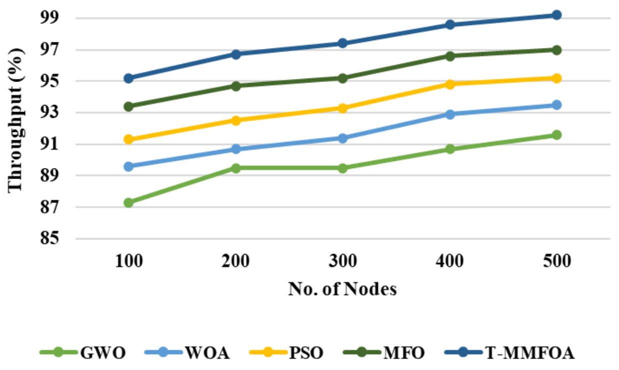

Figure. 3 Throughput (%) vs number of nodes

98.6% and 99.2% for 100, 200, 300, 400 and 500 nodes which is superior to other existing algorithms like GWO, WOA, PSO and MFO.

Table 4 and Fig. 4 represent the performance of the proposed algorithm with performance metrics of delay. The delay refers to the quantity of time taken for transmitting data packets from source to BS. The proposed algorithm attained less delay 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 which is superior to other existing algorithms like GWO, WOA, PSO and MFO.

Table 5 and Fig. 5 represent the performance of the proposed algorithm with performance metrics of energy consumption. The delay is referred to as the amount of energy spent by every node in WSN and is evaluated by J. The proposed algorithm attained less energy consumption 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 which is superior to other existing algorithms like GWO, WOA, PSO and MFO.

4.2 Comparative analysis

The performance of the proposed T-MMFOA algorithm is compared with existing algorithms like F-GWO [17], QMR [18], CH-EESNN-Hyb-WH-CSOA-WSN [19], IDTOMHR [20], QGAOA [21], TE-MHOA [22] and M-TCRSA [23]. Table 6 represents a comparative analysis of the proposed algorithm; it is clear that the T-MMFOA algorithm attained superior performance than other existing algorithms. The proposed T-MMFOA algorithm is utilized to enhance the robustness against malicious attacks to improve the data delivery and life expectancy of WSN.

Received: January 2, 2024. Revised: March 11, 2024.

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
	M-TCRSA [23]	N/A	99.27
	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
	M-TCRSA [23]	N/A	12.07
	Proposed T-MMFOA	3.3	6.7
Energy Consumption (J)	QMR [18]	7	-
	IDTOMHR [20]	7.6	-
	Proposed T-MMFOA	6.6	8.2
Throughput (%)	QGAOA [21]	96	97
	Proposed T-MMFOA	97	98
Network Lifetime (s)	TE-MHOA [22]	936,51	N/A
	M-TCRSA [23]	63.17	N/A
	Proposed T-MMFOA	955.21	1034.03

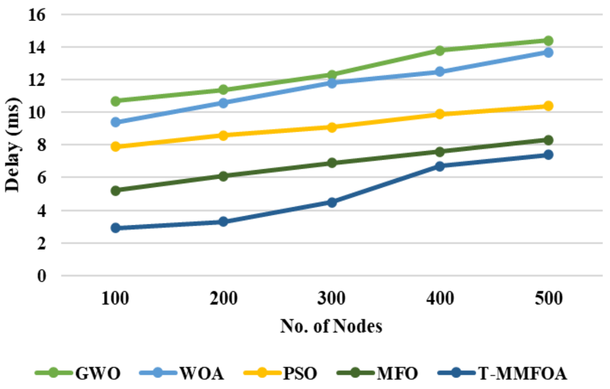

Figure. 4 Delay (ms) vs number of nodes

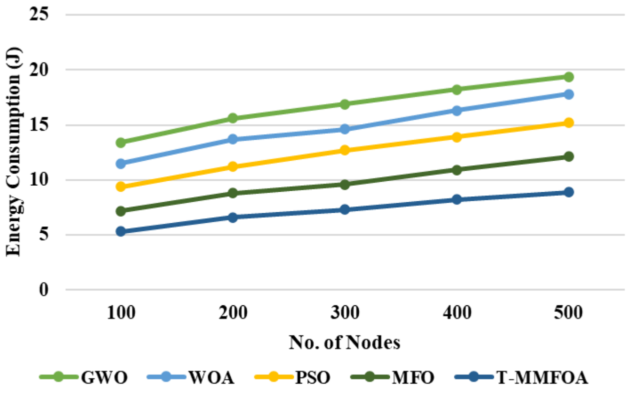

Figure. 5 Energy consumption (J) vs number of nodes

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

4.3 Discussion

The limitations of the existing algorithms and the advantages of the proposed algorithm in secure CH and route path selection are described in this section. The F-GWO [17] and QMR [18] methods have limitations that fail to consider the fitness function of energy and distance that cause packet drop in the network. In proposed T-MMFOA considered the residual energy that supports to removal of node failure and unnecessary packet drop. The CH-EESNN-Hyb-WH-CSOA-WSN [19] technique failed to consider security issues in the WSN network. In proposed T-MMFOA considered the fitness function of trust which enhanced the security and avoided malicious attacks. The IDTOMHR [20], QGAOA [21], TE-MHOA [22] and M-TCRSA [23] methods have limitations such as utilizing the huge number of control packets in route path selection which caused maximized delay. In proposed T-MMFOA attained less delay due to the generation of the shortest path and less utilization of the control packet in route path selection.

5. Conclusion

In this research, the secure cluster-based routing protocol is developed by T-MMFOA to enhance security against malicious attacks. SCH from normal sensors and route paths through SCHs are chosen to utilize T-MMFOA which avoids malicious attacks in communication. Moreover, clustering by T-MMFOA enhanced the WSN energy efficiency and performed secure and reliable communication when enhancing WSN life expectancy. The shortest route acquired from T-MMFOA is utilized to reduce delay over WSN. Hence, data transmission of T-MMFOA is enhanced in WSN. From the experimental results, it is clear that T-MMFOA performed superior to F-GWO, QMR, IDTOMHR and QGAOA. The proposed T-MMFO algorithm attained high PDR of 98.5% and 95.7% for 200 and 400 nodes which is superior to F-GWO, QMR, IDTOMHR and QGAOA. In the future, a hybrid optimization algorithm can be utilized to improve the performance of WSN.

Notation

Notations	Description
n	Number of moths
d	Count of dimensions in solution space
D	Solution's dimension
I	Initial random position
P	Moth's motion in search space
T	End search process
lb	Lower bounds of variables
ub	Upper bounds of variables
D_i	Space among ith and jth flame
b	Fix to determine logarithmic spiral shape
t	Random number among $[-1,1]$
N	Maximum no. of flames
l	Present number of iterations
ff_1	Trust
ff_2	Residual energy
ff_3	Distance between nodes
ff_4	Traffic rate
ff_5	Cluster density
F	Overall fitness function
$\delta_1 - \delta_5$	Weight metrics
TDP_{ij}	Transmitted Data
RDP_{ij}	Received Data
g_1	Trust value
E_{SCH_i}	Remaining energy of ith SCH
$dis(SCH_i, BS)$	Distance between ith SCHs and BS
$B_{utilization}$	Buffer usage
P_{drop}	Packet drop
C_{load}	Channel load
$\lvert Y_i \rvert$	ith cluster nodes
τ_1, τ_2 and τ_3	Weight parameters

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 1st author. The supervision and project administration, have been done by 2nd and 3rd author.

References

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

[2] S. Kumar and R. Agrawal, "A hybrid C-GSA optimization routing algorithm for energy-efficient wireless sensor network", *Wireless Networks*, Vol. 29, No. 5, pp. 2279-2292, 2023.

[3] Z. Wang, H. Ding, B. Li, L. Bao, Z. Yang, and Q. Liu, "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.

[4] R. Mishra and R. 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.

[5] M. Supriya and T. Adilakshmi, "Security Aware Cluster-Based Routing Using MTCSA and HEA for Wireless Sensor Networks", *International Journal of Intelligent Systems and Applications in Engineering*, Vol. 11, No. 2, pp. 663-669, 2023.

[6] B. Ramachandra and T. P. Surekha, "Secure Cluster based Routing Using Improved Moth Flame Optimization for Wireless Sensor Networks", *International Journal of Intelligent Engineering & Systems*, Vol. 15, No. 4, pp. 116-124, 2022, doi: 10.22266/ijies2022.0831.12.

[7] S. S. Rao, and K. C. K. Reddy, "An Energy Efficient Clustering based Optimal Routing Mechanism using IBMFO in Wireless Sensor Networks", *International Journal of Intelligent Systems and Applications in Engineering*, Vol. 10, No. 4, pp. 641-651, 2022.

[8] F. S. Alrayes, J. S. Alzahrani, K. A. Alissa, A. Alharbi, H. Alshahrani, M. A. Elfaki, A. Yafoz, A. Mohamed, and A. M. Hilal, "Dwarf Mongoose Optimization-Based Secure Clustering with Routing Technique in Internet of Drones", *Drones*, Vol. 6, p. 247, 2022.

[9] Y. Han, H. Hu, and Y. Guo, "Energy-Aware and Trust-Based Secure Routing Protocol for Wireless Sensor Networks Using Adaptive Genetic Algorithm", *IEEE Access*, Vol. 10, pp. 11538-11550, 2022.

[10] K. Veerabadrappa, and S. C. Lingareddy, "Secure Routing using Multi-Objective Trust Aware Hybrid Optimization for Wireless Sensor Networks", *International Journal of Intelligent Engineering & Systems*, Vol. 15, No. 1, pp. 540-548, 2022, doi: 10.22266/ijies2022.0228.49.

[11] P. D. Kumar and K. Valarmathi, "Fuzzy based hybrid BAT and firefly algorithm for optimal path selection and security in wireless sensor network", *Automatika*, Vol. 64, No. 2, pp. 199-210, 2023.

[12] P. Gulganwa and S. Jain, "EES-WCA: energy efficient and secure weighted clustering for WSN using machine learning approach", *International Journal of Information Technology*, Vol. 14, No. 1, pp. 135-144, 2022.

[13] A. Balamurugan, S. Janakiraman, M. D. Priya, and A. C. J. Malar, "Hybrid Marine predators optimization and improved particle swarm optimization-based optimal cluster routing in wireless sensor networks (WSNs)", *China Communications*, Vol. 19, No. 6, pp. 219-247, 2022.

[14] A. Asha, A. Rajesh, N. Verma, and I. Poonguzhali, "Multi-objective-derived energy efficient routing in wireless sensor networks using hybrid African vultures-cuckoo search optimization", *International Journal of Communication Systems*, Vol. 36, No. 6, p. e5438, 2023.

[15] M. K. Roberts and J. Thangavel, "An improved optimal energy aware data availability approach for secure clustering and routing in wireless sensor networks", *Transactions on Emerging Telecommunications Technologies*, Vol. 34, No. 3, p. e4711, 2023.

[16] G. Sudha and C. Tharini, "Trust-based clustering and best route selection strategy for energy efficient wireless sensor networks", *Automatika*, Vol. 64, No. 3, pp. 634-641, 2023.

[17] J. Singh, J. Deepika, Zaheeruddin, J. S. Bhat, V. Kumararaja, R. Vikram, J. J. Amalraj, V. Saravanan, and S. Sakthivel, "Energy-efficient clustering and routing algorithm using hybrid fuzzy with grey wolf optimization in wireless sensor networks", *Security and Communication Networks*, Vol. 2022, p. 9846601, 2022.

[18] C. Mohanadevi and S. Selvakumar, "A qos-aware, hybrid particle swarm optimization-cuckoo search clustering based multipath routing in wireless sensor networks", *Wireless Personal Communications*, Vol. 127, No. 3, pp. 1985-2001, 2022.

[19] B. Meenakshi and D. Karunkuzhali, "Enhanced Elman spike neural network for cluster head based energy aware routing in WSN", *Transactions on Emerging Telecommunications Technologies*, Vol. 34, No. 3, p. e4708, 2023.

[20] M. M. Asiri, S. S. Alotaibi, D. H. Elkamchouchi, A. S. A. Aziz, M. A. Hamza, A. Motwakel, A. S. Zamani, and I. Yaseen, "Metaheuristics Enabled Clustering with Routing Scheme for Wireless Sensor Networks", *CMC-Computers Materials & Continua*, Vol. 73, No. 3, pp. 5491-5507, 2022.

[21] R. N. 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*, 2023.

[22] K. Veerabadrappa and S. C. Lingareddy, "Trust and Energy Based Multi-Objective Hybrid Optimization Algorithm for Wireless Sensor Network", *International Journal of Intelligent Engineering & Systems*, Vol. 15, No. 5, pp. 71-80, 2022, doi: 10.22266/ijies2022.1031.07.

[23] S. V. K. Reddy and J. K. Murthy, "Secure Cluster based Routing Using Multiobjective Trust Centric Reptile Search Algorithm for WSN", *International Journal of Intelligent Engineering & Systems*, Vol. 16, No. 2, pp. 526-535, 2023, doi: 10.22266/ijies2023.0430.43.