Received: March 25, 2022. Revised: May 14, 2022.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Trust and Energy Based Multi-Objective Hybrid Optimization Algorithm for Wireless Sensor Network

Kantharaju Veerabadrappa[1]* **Sanjeev Channaabasappa Lingareddy**[2]

[1]*Visvesvaraya Technological University-Belagavi, Karnataka, India*
[2]*Sri Venkateshwara College of Engineering, Vidyanagar, Bangalore, India*
* Corresponding author's Email: kantharajv@gmail.com

Abstract: In recent days, nodes communicating in sensor networks have emerged as a result of recent growth in CPUs and wireless sensor networks (WSNs). Generally, WSN nodes utilize multi-hop routing and work with one another to send the data efficiently. While transmitting the data packets, these communicating systems are interfered with by a variety of threats (attacks). An effective trust based method must be designed to estimate the trustworthiness of each node while differentiating the remaining hostile nodes. Trust-based communication networks and dynamic routing have emerged as essential techniques for improving WSN availability and energy efficiency in recent years. Here, trust and energy based multi-objective hybrid optimization algorithm (TE-MHOA) is proposed with various fitness functions to improve the network lifetime. The hybrid optimization algorithm consists of adaptive particle swarm optimization and monarch butterfly optimization (APSO-MBO) techniques. The multipath routes methodology is used in conjunction with a multi-hop intra-cluster and inter-cluster transmission medium in this technique. The simulation results show that the evaluation criteria in the proposed TE-MHOA have enhanced in terms of throughput (1089.97 Kbps), delay (0.014 ms), PDR (99.96 %), routing overhead (0.017), energy consumption (0.34 J), and extended the network lifetime up to 1177.56 s which is better when related to existing energy-aware trust and opportunity-based routing (ETOR) algorithm and trust aware secure routing protocol (TASRP).

Keywords: Adaptive particle swarm optimization, Energy-aware trust and opportunity-based routing, Energy efficiency, Monarch butterfly optimization, Wireless sensor networks.

1. Introduction

Generally, WSNs are considered as new heterogeneous computing applications that consist of a network of small, low-power, advanced sensor hubs and one or even more base stations [1]. Sensor nodes collect data in a variety of locations, including natural ecosystems, battlefields, and man-made environments, and communicate it to one or more base stations [2]. Sensor nodes have limited battery power, computer power, memory, electromagnetic frequency, and communication capabilities, but the base station has higher intellectual, energy, and information about the quality [3, 4]. Among the sensor nodes and the end user, the base station serves as a gateway. WSN gathers data about the surroundings using sensor modules and analyses the data with potential fields [5]. Unfortunately, the resource, computing capabilities, communication radius, and storage memory of sensor nodes in sensor networks are reserved [6]. As a result, all wireless sensor network methods have been analyzed to reduce energy consumption by utilizing energy efficiently and taking into account the limiting capability of sensor nodes [7, 8].

WSNs are usually built-in unsupervised surroundings to evaluate the environmental data or warfare areas by connecting wireless connections (relay recorded information) to base stations [9]. Records can be quickly revealed throughout packet forwarding because of these qualities. This can be a severe issue in the application that deal with military data or personal information [10]. Investigations on security applications have been conducted to address these issues. Generally, wireless sensor networks are exposed to a variety of threats, so, security is considered a key issue [11]. The restricted capacity of sensor nodes is one motivation to attack sensor networks [12]. The most important applications in the WSNs field, such as military surveillance, traffic monitoring, and healthcare, could be harmed by security assaults [13]. As a result, there are many sorts of detection mechanisms are introduced for security in WSN [14]. Furthermore, severe limits on sensor nodes, such as dependability, scalability and energy efficiency, have an impact on WSN security. A framework will be developed in this study to defend the wireless sensor network against malicious assault [15]. In this paper, the adaptive PSO is integrated through monarch butterfly algorithm for enhancing the performance parameters present in the network. However, in certain situation, for the period of exploration, PSO gets trapped within the primary targets. For that reason, monarch butterfly is integrated next to PSO in the direction of developing the exploration possibility in both the local and global situations. Moreover, by using the proposed TE-MHOA, the secure routing from source CH towards BS is identified. As a result, TE-MHOA is exploited for security enhancement whereas reducing the nodes energy consumption. The major contribution of this research is mentioned as follows,

- Using TE-MHOA, the energy consumption of sensors must be decreased as much as feasible to extend the total network operating lifetime.
- TE-MHOA protocol is used to investigate the node selection process in WSN.
- To provide a TE-MHOA protocol that takes into account energy usage, reliability, and privacy protection in both homogeneous and heterogeneous situations.
- To compare TE-MHOA protocol to current protocols to assess its performance.

The organization of this research are mentioned as follows; section 2 stated the literature review of previous papers related with secure routing. The problem statement of this research is described in section 3. Section 4 explained the process, equations and working procedure of proposed methodology. Section 5 represents the result and discussion along with the comparative analysis. Finally, the conclusions are declared at section 6.

2. Literature review

Reddy, D.L., Puttamadappa, C.G. and Suresh, H.N.G [16] demonstrated the hybrid method name called grey wolf updated whale optimization algorithm (GU-WOA) for selecting the best CH. The suggested GU-WOA method was applied to reduce the distance between the selected CH and node. Uncertainty, the system was executed in a single hop transmission only, and unsuccessful to implement in the process of multi hop routing. Also, these systems are vulnerable to a variety of security risks, which can negatively impact their performance.

Sundararajan and Premkumar [17] provided deep learning-based defense mechanism (DLDM) system to recognize and separate DoS attacks in the data forwarding phase (DFP). The DLDM case formulation has the best results for identifying DoS threats. This approach is correspondingly suitable to nodes with minimal count or mobility state. However, this method is ineffective while the nodes were moving in a considerable location.

OHIDA RUFAI AHUTU AND HOSAM EL-OCLA [18] suggested a lightweight multi-hop routing protocol (MAC centralized routing protocol (MCRP) to decrease energy usage and identify wormhole attacks. The deployment of centralized network information in one element through the BS to improve energy efficiency while increasing routing performance and usage of the convergence among sensor nodes and BS were the primary ideas in MCRP. However, this clustering algorithm does not improve network longevity because it considers the CH as an elevated node.

Chen Hongsong [19] proposed a spark-assisted correlation analysis for low rate attackers in WSN. The use of spark-assisted correlation coefficient examination approaches to distinguish LDoS attacks in the WSN was quite effective. The established approach improves the accuracy of LDoS recognition. The amount of routing messages in the attack scenario does not differ substantially from that at the reasonable level. As a result, it's impossible to communicate the difference between a DoS attack and normal routine.

Tayyab Khan and Karan Singh [20], presents a trust aware secure routing protocol (TASRP) for sensor networks while avoiding network layer attacks. TASRP is a multifactor method which applies nodes remaining energy, trust score and route distance to deliver consistent paths over and done with minimized consumption. This approach supports in choosing trusted nodes for data transmission and reduce the routing distance. The method's complexity,

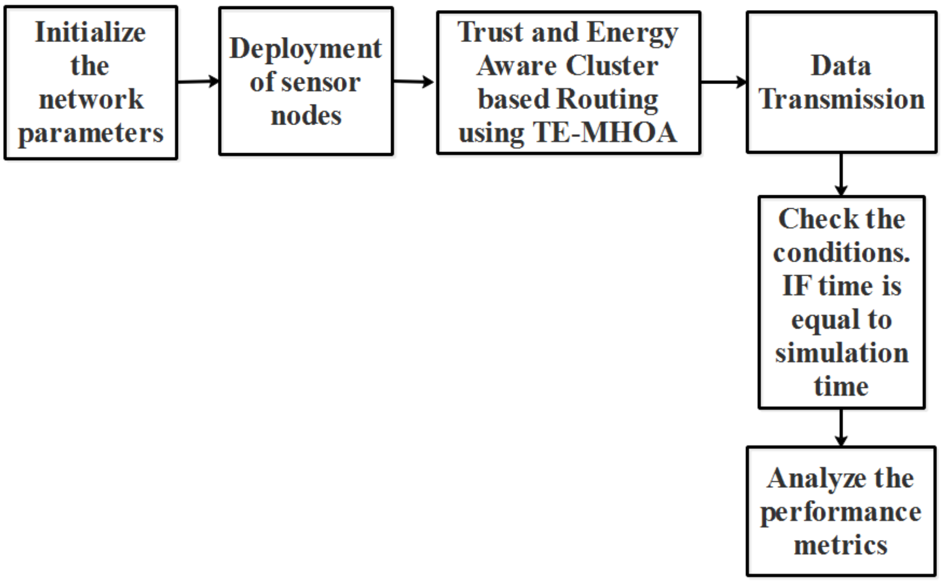
Initialize the network parameters
Deployment of sensor nodes
Trust and Energy Aware Cluster based Routing using TE-MHOA
Data Transmission
Check the conditions. IF time is equal to simulation time
Analyze the performance metrics

Figure. 1 Block diagram for the proposed method

low energy loss, and ability to offset the impacts of network attacks are all notable aspects. On the other hand, the trust value based method does not consider the collision attacks.

The energy-aware trust and opportunity-based routing (ETOR) with composite fitness function were presented by Hajiee, Fartash, and Eraghi [21]. ETOR-MN was the name given to the ETOR that ran on mobile nodes (MN). Network activity, bandwidth, hop-count, latency, resource, trust, and QoS were the fitness functions examined in this ETOR. There were two crucial phases in this ETOR. The endurance factor was used to choose the safe nodes, which were then followed by the opportunistic nodes for routing. Using this ETOR, the likelihood of a transition error was reduced. However, the packet delivery ratio was high once the system integrated with a large number of devices.

3. Problem statement

- One of the most important issues in WSN is energy efficiency. During transmission, sensing, and data analysis, WSNs use a tremendous amount of energy.
- The selection of CH is critical in WSNs since it affects the network lifespan and efficiency.
- Another significant factor to consider when developing wireless sensor networks is data security, as WSNs may be implemented in hostile environments.
- In ordinary networks, current sensing hubs have no protection, and safeguarding WSN connections from malicious attacks provides various issues.

4. Proposed methodology

The goal of this study is to develop a TE-MHOA architecture for establishing safe, energy-efficient data transmission from the source node to the destination node. As a result, data can be transmitted securely while using less energy. This concept ensures secure data exchange while also extending the sensor network's lifespan. The goal of data routing methods is to eliminate redundant data transmission and extend the life of energy-constrained wireless sensor networks. In this paper, the TE-MHOA algorithm achieves secure data routing using a clustering method with a resource-rich dynamic cluster head. As a result, routing at cluster-head expressed dissatisfaction over head and reduces the burden of re-clustering to improve energy efficiency and maximize network longevity. The recommended technique's block diagram shown in Fig. 1.

Step 1: At first, the sensor nodes are placed at random in the area of interest. The source node and BS are fixed and are dependent on the position of the sensor nodes.

Step 2: The presence of a malicious assault in a network is detected using an effective routing technique.

Step 3: The malicious attack's location will be presented as an input to a routing-based algorithm.

Step 4: For the routing mechanism, the TE-MHOA algorithm was designed in this research work.

- A fitness function is used to calculate the communication cost and residual energy of the nodes.

- An optimum node is chosen from the routing algorithm to build the path from the source node to the destination.
- The source node transfers the data to the destination after building the path from source to destination.

Step 5: To reduce sensor node energy consumption, efficient routing is premised on the communication cost and energy of the nodes.

Step 6: If a malicious attack is discovered in the routing path, re-routing is enabled, with re-routing dependent on the identical fitness function.

Step 7: During the transmission phase, the quality of service (QoS) parameters are increased by utilizing an efficient routing scheme.

For data transmission from the internet region, the TE-MHOA approach prevents hostile attacks. The proposed method's major goal is to increase the network's reliability and lifespan.

4.1 Particle swarm optimization (PSO)

The PSO has been used to resolve a variety of discrete optimization problems successfully and one version of PSO is known as adaptive PSO which provides better advancements for resolving optimization concerns. As a result of the changes, the PSO algorithm now works for these diverse types of issues. Velocity is defined as a bit's ability to reach a value of one. PSO looks to be a better option for increasing distribution system efficiency. As a result, a unique APSO method is developed and tested to improve system stability by lowering power losses.

In PSO, the position and the velocity of each particle at the reiteration k in the exploration interplanetary are labeled by ${X^i}_k$ and ${V^i}_k$. The particle velocity I in the iteration $k+1$ ${P^i}_{lbest}$ is attained after the subsequent Eq. (1).

$$ {V^i}_{k+1}= \omega. {V^i}_k + C_1.R_1\ ({P^i}_{lbest} - {X^i}_k) \\ +C_2.R_2\ ({P^i}_{global} - {X^i}_k) \quad (1) $$

Where random functions are declared as $R_1.R_2$; training coefficients are stated as $C_1.C_2$. ω is the inertia weight factor and attained on or after the next Eq. (2).

$$ \omega = \omega_{max} - \{(\omega_{max} - \omega_{min}) - \mathrm{k}_{max})\} \times k \quad (2) $$

Where a maximum number of iterations is stated as k_{max}. After each iteration, a new position for each particle is achieved through the addition of the previous position and new velocity as shown in Eq. (3)

$$ {X^i}_{k+1} = {X^i}_k + {V^i}_{k+1} \quad (3) $$

4.2 Adaptive control of PSO parameters

Many swarm intelligences have confronted that the value of population should be high in the exploration state; while processing the exploitation state, the population should be low. Correspondingly, the inertia weight is relatively large during the research phase and that became small during the converged state. From now, it could be advantageous to permit ω to monitor the evolutionary situations using a sigmoid planning $\omega(f): \mathrm{R}^+ \to \mathrm{R}^+$ which is represented as Eq. (4).

$$ \omega(f) = \frac{1}{1+1.5e^{2.6f}} \in [0.4,0.9] \quad \forall f \in [0.1] \quad (4) $$

Where ω is initialized to 0.9, and familiarize to exploration setting which is considered as f. Based on the following concept, adaptive control for acceleration coefficients can be designed. The parameters C_1 and C_2 indicate "self-cognition" and "peer acceptance," respectively, which push the crowd to diverge to the existing globally optimal area, assisting with quick convergence. As previously stated, the above acceleration coefficient modifications should not be too disruptive. As a result, the maximum increase or decrease in value between two generations is constrained by Eq. (5).

$$ |C_i(g+1) - C_i(g)| \le \delta \qquad i = 1,2. \quad (5) $$

The constriction factor is determined as, $C_i = \frac{C_i}{C_1+C_2}$

where δ is labelled as the "acceleration rate" in the range of [0.05, 0.1].

4.3 Monarch butterfly optimization (MBO)

Butterfly movement behavior can be idealized to solve a variety of optimization challenges. The following Eq. (6) is a process of the migration

$$ x_{i,k}^{t+i} = x_{r_{1,k}}^{t} \quad (6) $$

where $x_{i,k}^{t+i}$ designates the k^{th} component of x_i at iteration $t+1$ which offerings the butterfly position as i . t is represented as the existing generation count; Correspondingly, $x_{r_{1,k}}^{t}$ designates the k^{th} component of x_{r_1} is freshly produced location of the butterfly r_1. Monarch butterfly r_1 is arbitrarily nominated on or after subpopulation 1. While $r \leq p$, the portion k in the freshly created butterfly is produced through Eq. (7). Here, r can be designed as

$$r = rand \times peri \quad (7)$$

Where migration period is stated as $peri$ and fixed to 1.2. $rand$ is a random quantity drained from constant dissemination. If $r > p$, the part k in the recently produced butterfly is made by Eq. (8).

$$x_{i,k}^{t+1} = x_{r_{2,k}}^{t} \quad (8)$$

where $x_{r_{2,k}}^{t}$ designates the k^{th} part of x_{r_2} which is recently produced location of the butterfly r_2. Monarch butterfly r_2 is arbitrarily designated on or after subpopulation 2. If an arbitrarily produced integer rand is lesser or equivalent to p, it is written as Eq. (9).

$$x_{j,k}^{t+1} = x_{best,k}^{t} \quad (9)$$

where $x_{j,k}^{t+1}$ specifies the k^{th} part of x_j at iteration $t + 1$ which offerings the butterfly location as j. t is represented as existing generation count. Correspondingly, $x_{best,k}^{t}$ designates the k^{th} portion of x_{best} as finest position. On the dissimilarity, if rand is superior over p, it is modernized as Eq. (10).

$$x_{j,k}^{t+1} = x_{r_{3,k}}^{t} \quad (10)$$

where $x_{r_{3,k}}^{t}$ designates the k^{th} portion of x_{r_3}. if $rand > BAR$, the above equation is modified and represented as Eq. (11).

$$x_{j,k}^{t+1} = x_{j,k}^{t+1} + \left(\alpha \times \left(d_{x_k} - 0.5\right)\right) \quad (11)$$

where the adjusting rate of a butterfly is signified as BAR. d_x is the walk step of butterfly j which is used to compute levy flight performance using Eq. (12).

$$d_x = Levy(x_j^t) \quad (12)$$

In Eq. (11), a weighting factor is stated as α which is prearranged as Eq. (13).

$$\alpha = \frac{S_{max}}{t^2} \quad (13)$$

where maximum step walk is represented as S_{max}; existing generation is stated as t. The greater α suggesting lengthy period of exploration rises the impact of d_x on $x_{j,k}^{t+1}$; And minor α, signifying a small period of exploration reduces the impact of d_x on $x_{j,k}^{t+1}$.

4.4 TE-MHOA based clustering

4.4.1 Fitness function derivation

The main function of TE-MHOA based clustering process is to choose the nearby finest number of nodes such as CHs. The major aim is to achieve suitable fitness by expressing residual energy, communication cost, trust, and node degree.

a) Residual energy

The first objective is f_1 (residual energy) which is condensed and characterized in Eq. (14).

$$Minimize\ f_1 = \sum_{i=1}^{m} \frac{1}{E_{CHi}} \quad (14)$$

b) Communication cost

The communicating cost with the neighbor node is labeled as shown in Eq. (15).

$$C_{com} = \frac{d_{avg}^2}{d_0^2} \quad (15)$$

Where, d_{avg}^2 quantified as distance amongst the nodes and neighbor; d_0^2 is stated as the radius of a node.

The second objective is characterized as

Minimize $\mathrm{f}_2 = \frac{1}{N_T} \sum_{\mathrm{i}=1}^{\mathrm{N}} N_{prox}(N_i)$, where a number of nodes are stated as N

c) Trust

Trust is a significant element in the fitness function for strengthening security against malicious assaults in this CH selection. The conversation is carried out using the mutual trust established over a while. The trust is calculated based on the packet forwarding behavior, which is the relationship between the transmitted (TDP_{ij}) and received (RDP_{ij}) data. The estimated trust value (g_1) is shown in Eq. (16) and is used to mitigate DDoS attacks when transmitting packets of data. The third goal is expressed as Eq. (16)

$$f_3 = g_1 = \frac{TDP_{ij}}{RDP_{ij}} \quad (16)$$

d) Degree of nodes

It is demarcated as the amount of non-CH contributors who drives into the specific mobile node. Therefore, the objective f_3 is expressed in Eq. (17).

$$Minimize\ f_4 = \sum_{i=1}^{m} I_i \qquad (17)$$

Accordingly, the process of normalization $(F(x))$ is subjugated to each function $\alpha_1, \alpha_2,\ \alpha_{3,}\alpha_4$ that is revealed in Eq. (18).

$$F(x) = \frac{f_i - f_{min}}{f_{max} - f_{min}} \qquad (18)$$

Where minimum and maximum fitness values are stated as f_{min} and f_{max} which is assumed in Eq. (19).

$$Minimum\ fitness = \alpha_1 f1 + \alpha_2 f2 + \alpha_3 f3 + \alpha_4 f4 \qquad (19)$$

Where, $\sum_{i=1}^{4} \alpha_i = 1; and\ \alpha_i \in (0,1)$

In the routing procedure, each inhabitant's measurement is equal to the amount of CH (m). Let $P_i = P_i^1, P_i^2, \dots P_i^m$) be i^{th} population, wherever population measurement is stated as $P_i^1 = (0,1)$, which are modified arbitrarily.

4.5 TE-MHOA based routing

The primary goal of this study is to find a neighbouring optimum path from each cluster head to the appropriate BS. The routing path between the source CH and the BS is constructed in TE-MHOA using the same fitness function that was used to pick the CH.

4.5.1. Initialization

Each TE-MHOA represents the data forwarding path from the CH to the BS in routing. Each TE-MHOA has the same dimensions as the total number of CH'S in the network, plus one extra slot for the BS. The proposed transmission route between the source node and the BS is updated every butterfly in the routing process. The quantity of CHs in the relevant transmission is equal to the measurement of each butterfly.

4.5.2. Route selection

To determine the data transmission path, TE-MHOA uses the identical fitness value that was previously defined in section 4.4.1. The route request (RREQ) message is sent from the source node to neighbour nodes to adjust the route identification process. At that point, the next node with a higher fitness rating transmits the message back to source CH through the reverse path. Source CH receives the information from the nearby nodes once the routing path has been created. The data transmission is initiated through the network after the routing path has been generated.

Table 1. Specification parameters

Constraint	Proportion
Wireless propagation protocol	Two Ray Ground
Simulation time	100 s
Queue type	Pri-Queue
Number of nodes	100
Network interface type	WirelessPhy
Malicious attacks	2, 4, 6, 8 & 10
MAC protocol	Mac/802.11
Initial energy	50 J
Area	1200m × 1200m
Antenna pattern	Omni-Antenna

5. Results and discussion

This section represents the results and analysis for the TE-MHOA approach. The network simulation (NS2) software is used to create and simulate this TE-MHOA approach, which runs on a system with 6-GB RAM and an intel core processor. While analysing the performance of TE-MHOA, the network is examined with CH node, malicious attacks, and nodes positioned in the region of 1200m × 1200m. In addition, the WSN's sensors are set at a detailed energy level of 50 J. The TE-MHOA specification parameters are listed in Table 1.

The throughput, latency, normalized routing overhead, PDR, average energy consumption, and a lifetime of the network of such TE-MHOA approach are all examined. The detailed comparison of the TE-MHOA approach is evaluated using an existing method termed ETOR-MN [21].

5.1 Performance of throughput

Fig. 2 depicts the results of the throughout performance for suggested and current approaches. The main considerations for the suggested TE-MHOA achieve better throughput than TASRP [20] and ETOR-MN [21]. The proposed TE-MHOA contains a long network lifetime, therefore the base station receives more data packets. The comparison of results for throughput is shown in Table 2. From the Table 2, it clearly illustrates that the suggested TE-MHOA achieves a maximum throughput of

Table 2. Performances of throughput

Number of nodes	Throughput (Kbps)		
	TASRP [20]	ETOR-MN [21]	Proposed TE-MHOA
20	NA	300.13	1089.97
40	NA	304.55	1089.54
60	164.92	308.27	1090.52
80	173.55	315.73	1089.54
100	180.11	323.29	1089.81

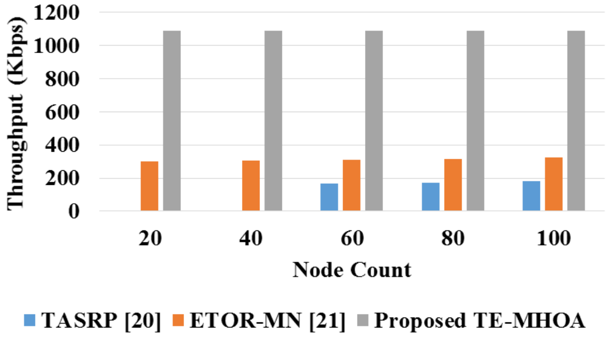

Figure. 2 Performance analysis of throughput

Table 3. Performances of end-to-end delay

Number of nodes	End-to-End Delay (ms)	
	ETOR-MN [21]	Proposed TE-MHOA
20	6.6	0.014
40	6.8	0.019
60	7.4	0.024
80	9.3	0.015
100	10.4	0.037

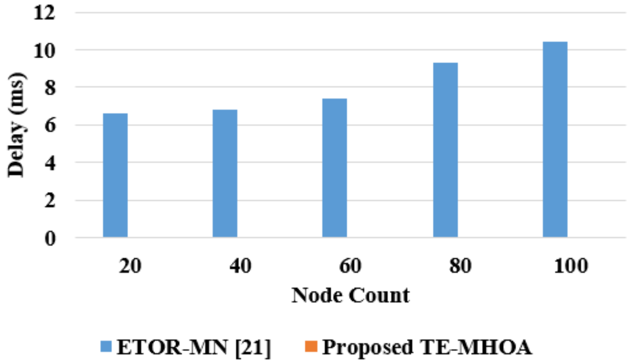

Figure. 3 Performance of end-to-end- delay

Table 4. Performances of packet delivery ratio

Number of nodes	Packet delivery ratio (%)	
	ETOR-MN [21]	Proposed TE-MHOA
20	44.13	99.96
40	52.46	99.8999
60	58.28	99.9699
80	62.92	99.9199
100	66.36	99.9246

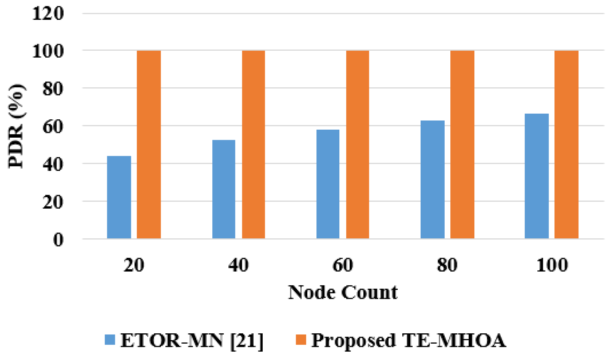

Figure. 4 Performance of PDR

1089.97 Kbps, whereas TASRP [20] attains only 180.11 Kpbs and ETOR-MN [21] only managed to obtain 323.29 Kbps.

5.1 Performance of end-to-end delay:

The node count is varied from 50 to 200 to study the consequence of mobile nodes and node density. The results of end-to-end delay for suggested and existing approaches are depicted in Fig. 3. Whenever the number of nodes increases, so does the size of the route request, increasing delay. The end-to-end delayed comparison of results is shown in Table 3. Table 3 reveals that the suggested TE-MHOA has a delay of 0.014 ms to 0.037 ms, while ETOR-MN [21] has a delay of 6.6 ms to 10.4 ms.

5.2 Performance of PDR

Fig. 4 shows the results of the packet delivery ratio for proposed and existing technologies. The comparative evaluation for the PDR is shown in Table 4. It simply proves that the planned TE-MHOA has a PDR ranging from 99.91 to 99.96 %, while ETOR-MN [21] has a PDR ranging from 44.13 to 66.36.

5.3 Performance of normalized routing overhead

Fig. 5 depicts the results of the normalized routing overhead for existing and proposed approaches. When the number of nodes increases, the size of the routing path and delay gets increases. The comparative evaluation for normalized routing overhead is shown in Table 5. From Table 5, it proves that the proposed TE-MHOA routing overhead ranges from 0.017 to 0.154, while ETOR-MN [21] improved from 7.01 to 13.25.

5.1 Performance of energy consumption

The mobility of the nodes leads to link disruption and extra energy utilization. Fig. 6 depicts the results

Table 5. Performances of Normalized routing overhead

Number of nodes	Normalized Routing Overhead	
	ETOR-MN [21]	Proposed TE-MHOA
20	7.01	0.017
40	7.24	0.042
60	8.38	0.092
80	10.48	0.082
100	13.25	0.154

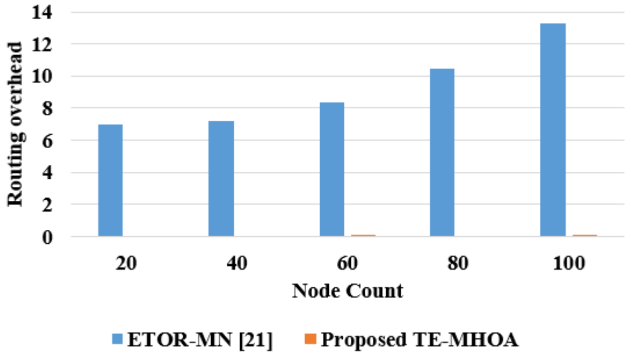

Figure 5. Performance Analysis of Normalized routing overhead

Table 6. Performances of energy consumption

Number of nodes	Energy Consumption (J)		
	TASRP [20]	ETOR-MN [21]	Proposed TE-MHOA
20	NA	1.67	1.32742
40	NA	1.75	0.793975
60	NA	1.79	0.624003
80	NA	1.87	0.349989
100	30.00	1.93	0.382304

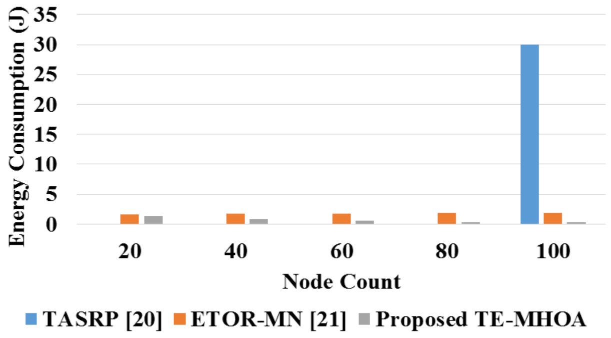

Figure 6. Performance Analysis of energy consumption

of the energy requirement analysis for the algorithms under consideration. As the number of nodes grows, so does the amount of energy consumed by the network. Delivering packets down less-traffic paths has been used in the suggested TE-MHOA algorithm, which has resulted in a reduction in collisions when compared to the existing algorithm. From the results, clearly shows that the suggested TE-MHOA consumes less energy in the case of both stationary node and dynamic node conditions. The comparative analysis of energy use is shown in Table 6. The proposed TE-MHOA achieves less energy consumption of 0.34 J, whereas the existing ETOR-MN [21] consumes up to 1.67 J and existing TASRP [20] consumes 30 J. The energy consumption is reduced by proposed TE-MHOA which eliminating malicious nodes and recognize the shortest distance. But, on the other hand, existing TASRP [20] doesn’t deliberate the energy whereas producing the route that causes excessive consumption of energy.

Table 7. Performances of network lifetime

Number of nodes	Network Lifetime (s)		
	GU-WOA [16]	ETOR-MN [21]	Proposed TE-MHOA
20	98	183	1177.56
40	99	191	939.58
60	101	213	782.58
80	102	230	1173.57
100	104	264	936.57

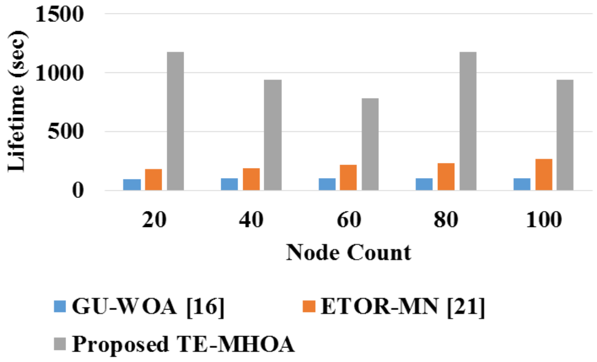

Figure 7. Performance analysis of network lifetime

5.1. Performance of network lifetime

The number of distinct routings completed by CHs to the sink before releasing the energies of the very first node which is referred to as network lifespan. Fig. 7 depicts the network lifetime analysis for the methods under consideration. The proposed algorithm has a lifetime of the network of 327 rounds, which means that the energy of the initial node is discharged in this round of routing. Those TE-MHOA findings indicate a clear advantage over GU-WOA [16] and ETOR-MN [21]. At the process of routing, the energy consumption gets minimized which will automatically improve the lifetime of the network. The network lifespan comparison is shown in Table 7.

By comparing the new TE-MHOA to the conventional GU-WOA [16] and ETOR-MN [21] approaches, the cumulative simulations show that the suggested TE-MHOA gives improved results across all node counts (20-100).

6. Conclusion

In this study, malicious attack nodes in the cluster are considered along with trust and energy based multi-objective hybrid optimization algorithm (TE-MHOA) employing a fitness function for identifying optimal routes in WSNs is provided. The proposed TE-MHOA algorithm increases the reliability of malicious node target identification by avoiding the usage of malicious nodes and enhancing the performance of multipath routing. WSN simulation with various numbers of nodes in the case of an external attack is used to test the effectiveness of the suggested TE-MHOA routing protocol. The simulation shows the improvement in terms of throughput (1089.97 Kbps), delay (0.014 ms), PDR (99.96 %), routing overhead (0.017), energy consumption (0.34 J), and extended the network lifetime up to 1177.56 s. This analysis shows the overall effectiveness of TE-MHOA, especially in comparison to the existing GU-WOA, TASRP and ETOR-MN routing protocols. The suggested approach is also extensible since each throughput of the complete routing cycles is nearly identical despite the number of distinct nodes. In future research, this research can be further extended with the movement of many sources through novel optimization algorithms.

Notation list

Notation	Description
$X^{i}{}_{k}$	Position of particle
$V^{i}{}_{k}$	Velocity of particle
$P^{i}{}_{lbest}$	Local Best position
R_1, R_2	Random functions
C_1, C_2	Training coefficients
ω	Inertia weight factor
k_{max}	Maximum number of iteration
$X^{i}{}_{k+1}$	New position of particle
ω(f)	Sigmoid planning
f	Exploration setting
C_i	Constriction factor
δ	Acceleration rate
$x_{i,k}^{t+i}$	Butterfly position
$peri$	Migration period
$rand$	Random value
r_1, r_2	Monarch butterfly
t	Existing generation count
x_{best}	Best Position
BAR	Adjusting rate of butterfly
α	Weighting factor
S_{max}	Maximum step walk
d_x	Butterfly walk step
C_{com}	Communication cost
d_{avg}^2	distance
d_0^2	Radius of a node
N	Number of nodes
TDP_{ij}	Transmitted data packet
RDP_{ij}	Received data packet
g_1	Estimated trust value
$F(x)$	Normalization process
f_{min} and f_{max}	Minimum and Maximum fitness
P_i	Population

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

The paper background work, conceptualization, methodology, dataset collection, implementation, result analysis and comparison, preparing and editing draft, visualization have been done by first author. The supervision, review of work and project administration, have been done by second author.

References

[1] T. Gaber, S. Abdelwahab, M. Elhoseny, and A. E. Hassanien, “Trust-based secure clustering in WSN-based intelligent transportation systems”, *Computer Networks*, Vol. 146, pp. 151-158, 2018.

[2] D. Qin, S. Yang, S. Jia, Y. Zhang, J. Ma, and Q. Ding, “Research on trust sensing based secure routing mechanism for wireless sensor network”, *IEEE Access*, Vol. 5, pp. 9599-9609, 2017.

[3] A. Miglani, T. Bhatia, G. Sharma, and G. Shrivastava, “An energy efficient and trust aware framework for secure routing in LEACH for wireless sensor networks”, *Scalable Computing: Practice and Experience*, Vol. 18, No. 3, pp. 207-218, 2017.

[4] A. Ahmed, K. A. Bakar, M. I. Channa, A. W. Khan, and K. Haseeb, “Energy-aware and secure routing with trust for disaster response wireless sensor network”, *Peer-to-Peer Networking and Applications*, Vol. 10, No. 1, pp. 216-237, 2017.

[5] A. Alghamdi, “Secure and energy efficient path optimization technique in wireless sensor networks using DH method”, *IEEE Access*, Vol. 6, pp. 53576-53582, 2018.

[6] F. Ishmanov, and Y. B. Zikria, "Trust mechanisms to secure routing in wireless sensor networks: Current state of the research and open research issues", *Journal of Sensors*, 2017.

[7] A. A. Mugheri, M. A. Siddiqui, and M. Khoso, "Analysis on security methods of wireless sensor network (WSN)", *Sukkur IBA Journal of Computing and Mathematical Sciences*, Vol. 2, No. 1, pp. 52-60, 2018.

[8] A. Mehmood, A. Khanan, M. M. Umar, S. Abdullah, K. A. Z. Ariffin, and H. Song, "Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks", *IEEE Access*, Vol. 6, pp. 5688-5694, 2017.

[9] K. Selvakumar, L. Sairamesh, and A. Kannan, "An intelligent energy aware secured algorithm for routing in wireless sensor networks", *Wireless Personal Communications*, Vol. 96, No. 3, pp. 4781-4798, 2017.

[10] S. Tanwar, K. Thakkar, R. Thakor, and P. K. Singh, "M-Tesla-based security assessment in wireless sensor network", In: *Proc. of Procedia Computer Science*, Vol. 132, pp.1154-1162, 2018.

[11] C. Kavitha, "Secure cluster-based data integrity routing for wireless sensor networks", In: *Proc. of Sensors and Image Processing*, pp. 157-167, 2018.

[12] S. Jabbar, M. A. Habib, A. A. Minhas, M. Ahmad, R. Ashraf, S. Khalid, and K. Han, "Analysis of factors affecting energy aware routing in wireless sensor network", *Wireless Communications and Mobile Computing*, Vol. 2018, 2018.

[13] A. Mehmood, M. M. Umar, and H. Song, "ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks", *Ad Hoc Networks*, Vol. 55, pp.97-106, 2017.

[14] T. Jamal, and S. A. Butt, "Low-energy adaptive clustering hierarchy (LEACH) enhancement for military security operations", In: *Proc. of Journal of Basic and Applied Scientific Research*, pp. 2090-4304, 2017.

[15] E. Rehman, M. Sher, S. H. A. Naqvi, K. B. Khan, and K. Ullah, "Energy efficient secure trust based clustering algorithm for mobile wireless sensor network", *Journal of Computer Networks and Communications*, Vol. 2017, 2017.

[16] D. L. Reddy, C. G. Puttamadappa, and H. N. G. Suresh, "Hybrid optimization algorithm for security aware cluster head selection process to aid hierarchical routing in wireless sensor network", *IET Communications*, Vol. 15, No. 12, pp. 1561-1575, 2021.

[17] M. Premkumar, and T. V. P. Sundararajan, "DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks", *Microprocessors and Microsystems*, Vol. 79, p. 103278. 2020.

[18] O. R. Ahutu, and H. E. Ocla, "Centralized routing protocol for detecting wormhole attacks in wireless sensor networks", *IEEE Access*, Vol. 8, pp. 63270-63282, 2020.

[19] C. Hongsong, M. Caixia, F. Zhongchuan, and C. Lee, "Novel LDoS attack detection by Spark-assisted correlation analysis approach in wireless sensor network", *IET Information Security*, Vol. 14, No. 4, pp. 452-458, 2020.

[20] T. Khan, and K. Singh, "TASRP: a trust aware secure routing protocol for wireless sensor networks", *International Journal of Innovative Computing and Applications*, Vol. 12, Nos. 2-3, pp. 108-122, 2021.

[21] M. Hajiee, M. Fartash, and N. O. Eraghi, "An Energy-Aware Trust and Opportunity Based Routing Algorithm in Wireless Sensor Networks Using Multipath Routes Technique", *Neural Processing Letters*, Vol. 53, pp. 2829-2852, 2021.