Multi-objective-trust aware improved grey wolf optimization technique for uncovering adversarial attacks in WSNs

Venkatesh Prasad Bannikuppe Srinivasiah[1], Roopashree Hejjaji Ranganathasharma[2], Venkatesh Ramanna[3]
[1]Department of Computer Science and Engineering, Government Engineering College, Kushalnagar, India
[2]Department of Artificial Intelligence and Data Science, GSSS Institute of Engineering and Technology for Women, Mysuru, India
[3]Department of Computer Science and Engineering, University of Visvesvaraya College of Engineering, Bangalore, India

Article Info

Article history:

Received Mar 14, 2024
Revised May 15, 2024
Accepted Jun 5, 2024

Keywords:

Energy efficiency
Malicious attacks
M-TAIGWO
Secure cluster head
Wireless sensor networks

ABSTRACT

Wireless sensor network (WSN) is made of several sensor nodes (SN) that monitor various applications and collect environmental data. WSNs are essential for a wide range application, including healthcare, industrial automation, and environmental monitoring. However, these networks are susceptible to several security threats, underscoring the need for robust attack detection systems. Therefore, in this study, a multi-objective-trust aware improved grey wolf optimization (M-TAIGWO) is implemented to mitigate various attacks types. This implemented M-TAIGWO method is used to select secure cluster heads (CH) and routes to obtain secure communication through the network. The implemented M-TAIGWO provides improved security against malicious attacks by increasing the energy efficiency. The important aim of M-TAIGWO is to attain secured data transmission and maximize the WSN network lifetime. The M-TAIGWO method's performance is evaluated through energy consumption and delay. The implemented method obtains a high PDR of 98% for 500 nodes, which is superior to the quantum behavior and gaussian mutation Archimedes optimization algorithm (QGAOA), with a delay of 15 ms for 100 nodes which is lesser than fuzzy and secured clustering algorithms. In comparison to the trust-based routing protocol for WSNs utilizing an adaptive genetic algorithm (TAGA), this implemented method achieves defense hello fold, black hole, sinkhole, and selective forwarding attacks effectively.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Venkatesh Prasad Bannikuppe Srinivasiah
Department of Computer Science and Engineering, Government Engineering College
Kushalnagar, Karnataka, India
Email: venkyp25@gmail.com

1. INTRODUCTION

Wireless sensor network (WSN) consists of several low-power, low-processing sensor nodes (SN) that leverage their inherent ability to self-organize and create a small network for data processing, transmission, and collection [1], [2]. Road accidents, pollution, and traffic congestion are getting worse, as a consequence of the massive increase in the demand for various forms of transport, including pedestrian traffic and public transport. Other factors contributing to this problem include inadequate infrastructure and work zones, poor capacity management (i.e., poor traffic timing), and inadequate infrastructure [3]. Temperature, pressure, soil moisture content, and other physical factors are examples of data collection parameters. Data over wireless links are organized at a single location known as the base station (BS), all at a time [4]. A security attack is any activity that compromises the machine's security by creating an intellectual risk to the unit. There exist numerous types of threats categorized into two primary forms of defensive threats, active attacks and passive attacks. The attacks endure many security services such as access control authentication non-repudiation, and data completeness and encryption [5]. They are crucial to WSNs as they manage the path in which the data goes from SN to BSs, significantly affecting the network's quality of life, energy conception, and performance [6]. The primary problem is to develop an effective security strategy that protects the empirical data while using the least number of resources possible, because of the ignored environment of its deployment [7]. In a WSN, each SN is capable of sensing, processing, and sending data to other SNs or BS directly, or in response to a request [8]. Consequently, WSNs are viewed as a collection of resources that force SN to collect data from their surroundings, process the outputs into a prepared form, and then wirelessly transfer formatted data to the designated terminal [9]. Moreover, in WSNs, the stability of root selection, the security of data transfer, and the balance of energy consumption are all very crucial [10]. However, the extensive use of WSNs creates security issues, making the network vulnerable to a variety of criminal operations and assaults [11]. The network's lifespan is potentially reduced with energy gaps appearing if its nodes employ different power quantities [12]. Therefore, the connection between the source and destination has failed to transfer the data from source to destination [13]. Sensor data from the physical area is sent to a BS multi-hop or multi-path routing. Self-organizing networks or WSNs have a limited battery capacity [14]. The selection of rooting algorithms is a critical factor in the effective transport of sensor data from source to destination. Depending on the application domains and network architecture, several energy-efficient routing strategies have been devised for WSN [15].

Kranthikumar and Velusamy [16] presented a novel fuzzy and secured clustering algorithm which was utilized to increase cluster based secure routing in WSNs. This method employed a key generation method to generate public and private keys for the process of encryption and decryption. It had the benefits of increased security and good overall performance, alongside reducing the energy consumption and delay by utilizing trust-based fuzzy logic. Yet, the implemented method had difficulty in selecting the optimal clusters. Han *et al.* [17] implemented an energy-aware and trust-based routing protocol for WSNs utilizing an adaptive genetic algorithm (TAGA) to resist special trust and common routing attacks. This algorithm with a cluster heads (CH) selection threshold was applied to select the secure and high-energy nodes as CHs. As a result, the TAGA method effectively reduced the malicious nodes' impact, and also improved energy utilization in the network by using a novel threshold function. But this method was limited in countering sophisticated attacks targeting genetic algorithm parameters, affecting the overall security of the routing protocol. Kumar and Srimanchari [18] developed a quantum behavior and gaussian mutation archimedes optimization algorithm (QGAOA) method for energy-efficient clustering and routing protocol for WSN. The developed method had three stages formation of cluster, CH, and optimum route selection. Primarily, clusters were developed by utilizing the voronoi-included K-means clustering algorithm. Next, CHs and optimum routing were chosen by the QGAOA method. But the CH selection was majorly dependent on node distance, trust, and energy. Bangotra *et al.* [19] implemented a trust based secure intelligent opportunistic routing protocol (TBSIOP) method used to provide trust WSN security. This implemented method used three distinct WSN attributes to compute the node's likelihood of being malicious. This method used a trust-based relay selection algorithm to enhance the network's lifetime through low energy consumption, also highly securing black-hole and gray attacks. However, this implemented method analyzed only a small number of nodes. Pathak *et al.* [20] implemented a node trust optimization model-based detection algorithm (NTOMA-DA) to resist wormhole attacks and increase the performance of the network. This implemented NTOMA-DA was a localized detection algorithm, combining node trust and path hops for detected attach. As a result, this method effectively assured reliable and safe WSN operation and attained superior wormhole attack detection. Nonetheless, the implemented method consumed more energy.

Teng *et al.* [21] implemented a lightweight secure routing (LSR) algorithm which was used for managing WSNs that directly addressed the multi-objective WSN optimization issue. An adaptive quality of service (QoS) method was utilized in this method to enhance QoS and network energy efficiency by increasing the source node selection. This implemented algorithm assisted low node-density networks to overcome the energy-hole challenge and to increase network security by incorporating a trust model. However, this method was limited in indirect trust value to 1-hop neighbors due to energy consumption, and hence required to be extended to multi-hop scenarios for increasing indirect trust value. Sajan *et al.* [22] implemented a three-level weighted trust evaluation-based GWO (3LWT-GWO) method used for an energy-aware secure routing in a wireless ad hoc sensor network. To alert military commanders, this method gathered data from targets of interest in dangerous situations and sent it to ground surveillance systems. The 3LWT-GWO method performed an effective detection of misbehaving nodes and attained optimal secure routes through nodes for delivering the data securely to the destination. Due to less data aggregation, this method required methods like watermarking and digital signatures to secure data integrity and improve the process of data aggregation. There are several constraints associated with the aforementioned existing methods, which have been proven to be challenging due to limited processing time and high energy consumption. These limitations have adversely affected the security of overall routing protocols, particularly in their vulnerability to sophisticated attacks targeting the parameters of genetic algorithms. Factors such as node energy, trust, and distance are pivotal in the selection of CH. In order to overcome these issues, the M-TAIGWO method is implemented to select secure CH and routes for obtaining secure communication through the network. Current methods have limitations of limited processing time, energy consumption, and difficulty in countering sophisticated attacks. The M-TAIGWO method is implemented to select secure CH and routes for secure network communication. Security and energy consumption are two important problems because of limited energy resources and open resources. For the security of WSN, trust-based methods have are established which have high robustness against malicious attacks. In this research, IGWO is used over other metaheuristic algorithms because GWO imitates the collaborative hunting behavior of grey wolves, thereby improving energy efficiency and network coverage. The GWO algorithm causes simultaneous minimization of search space, while the decision variables are less, avoiding local optimum. The main contributions of this research are given as follows:

- GWO algorithm is enhanced to multi objective-trust aware improved grey wolf optimization (M-TAIGWO) to mitigate various types of attacks in WSN.
- Selecting SCHs effectively with M-TAIGWO improves security protection against malicious attacks like Hello flood attacks, sinkhole attacks, selective forwarding attacks, black hole attacks, and reduced energy consumption.
- Secure route path selection is performed by M-TAIGWO. The effectiveness of the implemented model is analyzed based on performance measures with less delay, energy consumption, high packet delivery ratio (PDR), and network lifetime.

This paper is structured as follows: the proposed method is detailed in section 2. The process of M-TAIGWO method is explained in section 3. Results and discussion are given in section 4, and conclusion of this paper is described in section 5.

2. PROPOSED METHOD

2.1. System model

This approach aims to accelerate the discovery of novel concepts in various scenarios. Numerous routing protocols have been implemented to boost WSN security. To increase security in WSN, M-TAIGWO methods are implemented in this research. The proposed method consists of four main steps: i) network setup and energy model, ii) determining safe nodes, iii) clustering and CHs selection, and iv) clustering-based routing.

2.2. Network setup

By grouping sensors into clusters, WSN clustering aims to reduce energy consumption. Sometimes, common nodes send sensory data to the CH and keep monitoring their surroundings. The CH node is always selected between the common nodes. The CH plays a crucial function in gathering data from every cluster node and sending it to the BS. Grouping helps to prevent direct connection between sensors and receivers [23]. Figure 1 shows the WSN system model.

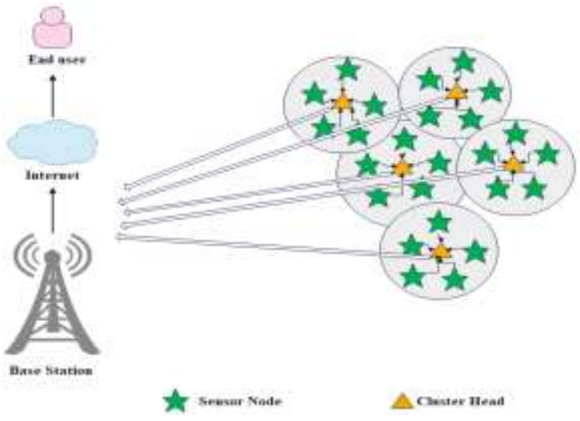

Figure 1. The WSN system model

2.3. Energy model

The architecture of the system comprises various SN connected to a single BS [24]. Two distinct channel models are used in a radio energy model of an SN, called the multipath propagation fading (d^4) model for multi-hop path communication and free space path loss (d^2) model for single-hop communication. As a result, the energy required to transport an n-bit packet over distance d is calculated in (1).

$$E_{TX}(n,d) = \begin{cases} n \times E_{elec} + n \times e_{fs}\, d^2 \ , & d < d_0 \\ n \times E_{elec} + n \times e_{mp}\, d^4 \ , & d \geq d_0 \end{cases} \tag{1}$$

Where, E_{TX} is the expected transmission count, n is the packet length, d is the distance between receiving and sender nodes, and E_{elec} is the energy required to receive/ transmit 1-bit data. The distance threshold is denoted as d_0, that is expressed in (2). In (3), the quantity of energy used to receive an n-bit packet size at R_x is determined.

$$d_0 = \sqrt{\frac{e_{fs}}{e_{mp}}} \tag{2}$$

$$E_{RX}(n) = n \times E_{elec} \tag{3}$$

3. MULTI-OBJECTIVE-TRUST AWARE IMPROVED GREY WOLF OPTIMIZATION

Normal, malicious, and sink nodes are the three kinds of nodes that form the network topology. Data from the environment is sensed by normal nodes and transmitted to the sink. Denial of service (DoS) attack is another kind of DoS attack on malicious nodes normal nodes. In brief, the M-TAIGWO is developed by the study's leadership behavior, encircling behavior, and hunting behavior, also summarising the algorithm's stages. Figure 2 shows the implemented M-TAIGWO method's block diagram. The proposed M-TAIGWO method has four stages of sensor initialization, M-TAIGWO-based SCH selection stage, clustering, and route discovery stage using M-TAIGWO. The secure CH and route path selection are utilized to avoid malicious attacks like Hello flood attacks, selective forwarding attacks, black hole attacks and sinkhole attacks when transmitting the data packets. So, unnecessary data packets and energy consumption are decreased by employing the proposed M-TAIGWO method. These malicious attacks are:

- Sinkhole attack: in this type of attack, a compromised node disrupts the neighboring traffic by establishing a sinkhole at the center, present as the attacking relay within the local area.
- Selective forwarding attack: a selective forwarding attack is a security threat in WSN where malicious nodes forward data packets while dropping others, compromising network integrity and availability.
- Black hole attacks: these attacks selectively drop control and data packets, causing partial or total data loss for any packet routed through an intermediate malicious node.
- Hello flood attack: this attack is a network layer attack where a high-powered node broadcasts a Hello packet, causing many nodes to choose it as the parent node, even from far away.

3.1. Sensor initialization

Initially, sensors are randomly placed in the WSN's interested area. The previous section contains the network and energy models utilized in this study. M-TAGWO is used to find SCHs and routes via SCHs to BS, which are discussed in the following sections.

3.2. M-TAIGWO based SCH selection stage

In this stage, optimum SCHs from the normal sensors are identified by utilizing the M-TAIGWO. Optimization is crucial for SCH selection in WSN to improve efficiency and strength. The process involves trade-offs between performance, energy consumption, and security. This helps mitigate vulnerabilities, resist attacks and adapt to changing conditions, ensuring a robust and secure basis for WSN operations. In WSN, IGWO provides a better CH selection process than GWO, optimizing the process of choosing the best nodes to act as CH. Better network performance and energy efficiency are ensured as a result. Through energy consumption optimization and network lifetime extension, IGWO improves the effectiveness of CH selection in WSN. In short, the study's inspiration for the M-TAIGWO is hunting behavior, encircling, and leadership behaviour. In this section, GWO is transformed into M-TAIGWO to discover the set of optimum SCHs.

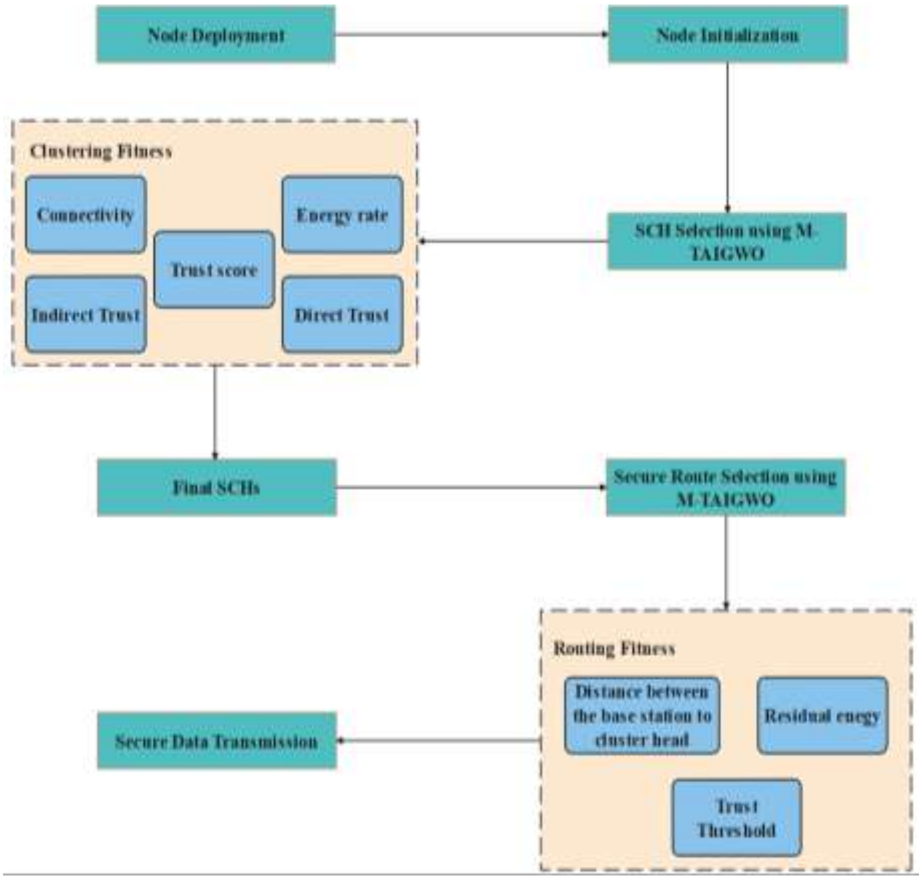

Figure 2. Implemented M-TAIGWO method's block diagram

3.3. Grey wolf optimization

3.3.1. Leadership behaviour

GWO is a metaheuristic search method with natural inspiration that makes it possible to identify the best solution in the problem area [25]. The process is similar to the way grey wolves hunt in terms of social behavior and technique to pinpoint the precise location. There are four subspecies of grey wolves: alpha (α), delta (δ) beta (β), and omega (ω) [26]. Usually, one or two of the team's alpha wolves are the most dominant. They are responsible for deciding what to hunt and how to pursue it. The alpha wolf's decision and other duties are supported by the beta wolves. Beta wolves are more common than alpha wolves, but less common than delta and omega wolves. Alpha and Beta are the two wolves on the teams with the most experience. While they rule omega, delta wolves protect alpha and beta wolves. Omega wolves, the least prominent type, primarily serve as babysitters. The most suitable candidate for describing the social behavior of grey wolves statistically is alpha (α), followed by the second and third most suitable candidates, beta (β), and delta (δ).

3.3.2. Encircling behavior

The process of encircle behavior is mathematically expressed in following formula in (4) and (5). Where, t denotes the iteration number of current, $\vec{H}, \vec{K}$ denote the coefficient vectors, $\overrightarrow{X_p}$ denotes the prey position, and $\vec{X}$ denotes the position of the grey wolf. $\vec{H}$ and $\vec{K}$ vectors are denoted in (6) and (7).

$$\vec{L} = \left|\vec{K}.\overrightarrow{X_p}(t) - \vec{X}(t)\right| \tag{4}$$

$$\vec{X}(t+1) = \overrightarrow{X_p}(t) - \vec{H}.\vec{L} \tag{5}$$

$$\vec{H} = 2.\vec{h}.\vec{r_1} - \vec{h} \tag{6}$$

$$\vec{K} = 2.\vec{r_2} \tag{7}$$

Where, $\vec{r_1}$ and $\vec{r_2}$ are uniformly random numbers in interval [0, 1]. $\vec{h}$ is linearly decremented from 2 to 0 with a number of iterations and represented in (8), where the maximum iteration number is denoted as $Maxiter$.

$$\vec{h} = 2 - 2\left(\frac{t}{Maxiter}\right) \tag{8}$$

3.2.3. Hunting behavior

It is believed that gamma, alpha, and beta candidates have a better grasp of prey regions and guide the process of the whole search towards the best option. Every iteration updates the applicants' positions according to their top three places. If the values are outside of solution space or if the window size is changed to a negative integer, the values are updated using the evolution approach, and the formula for updating wolves' positions is given in (9)-(15).

$$\overrightarrow{L_\alpha} = \left|\overrightarrow{K_1}.\overrightarrow{X_\alpha} - \vec{X}\right| \tag{9}$$

$$\overrightarrow{L_\beta} = \left|\overrightarrow{K_2}.\overrightarrow{X_\beta} - \vec{X}\right| \tag{10}$$

$$\overrightarrow{L_\delta} = \left|\overrightarrow{K_3}.\overrightarrow{X_\delta} - \vec{X}\right| \tag{11}$$

$$\overrightarrow{X_1} = \overrightarrow{X_\alpha} - \overrightarrow{H_1}.(\overrightarrow{L_\alpha}) \tag{12}$$

$$\overrightarrow{X_2} = \overrightarrow{X_\beta} - \overrightarrow{H_2}.(\overrightarrow{L_\beta}) \tag{13}$$

$$\overrightarrow{X_3} = \overrightarrow{X_\delta} - \overrightarrow{H_3}.(\overrightarrow{L_\delta}) \tag{14}$$

$$\vec{X}(t+1) = \frac{\overrightarrow{X_1}+\overrightarrow{X_2}+\overrightarrow{X_3}}{3} \tag{15}$$

For the values of $r_1, and\ r_2$, random selections are taken within the range (0.1). Because of this, the wolves can approach the prey from any angle. Values for H come from the interval [-h, h] and values for h are chosen from [0,2]. When $|H|$ <1, the wolves make use of the space solution, allowing them to approach the prey more closely. When $|H|$ >1, it indicates that they move their prey and explore search space as wolves are capable of studying the space of solution. Leaving wolves at their local minimum or maximum is likewise permitted by K and H. Ultimately after the final iteration, the best answer for the most suitable candidate is given back.

3.4. Improved GWO

In GWO, $\alpha, \beta,$ and δ guide ω wolves to search space areas that are probably related to the best solution. This strategy leads to enlargement in a locally optimal solution. Another drawback is that a decrease in population diversity causes GWO closer to local optimum. The implemented IGWO deals with these issues. This model is improved by the use of a novel search method that combines a phase for selection and upgrading. In addition, IGWO contains two steps as mentioned below.

3.5. Movement phase

A different mobility strategy included in the implemented IGWO is called as dimension learning-based hunting (DLH) technique. Using this approach, every wolf is instructed by its neighbors to be a distinct candidate for novel position, $X_i(t)$. Euclidean distance among current position $X_{i-GWO}(t+1)$ is utilized for evaluating a radius $R_i(t)$, as represented in (16). The neighbors of $X_i(t)$ indicated by $N_i(t)$ are then built using (17) to the radius $R_i(t)$, where Euclidean distance among $X_i(t)$ and $X_j(t)$ is represented D_i.

$$R_i(t) = ||X_i(\mathrm{t}) - X_{i-GWO}(t+1)|| \tag{16}$$

$$N_i(t) = \{X_j(t)|D_i(X_i(t), X_j(t)) \leq R_i(t), X_j(t) \in position\} \tag{17}$$

Once the neighborhood $X_i(t)$ has been built, multi-neighbour express in (18), where $X_{i-DLH,d}(t+1)$ is d-th dimension is evaluated utilizing the d-th dimension of a random wolf $X_{r,d}(t)$ from the position, and a random neighbour $X_{n,d}(t)$ chosen from $N_i(t)$. After this movement phase, the selecting and updating phase is performed for selecting a shorter route based on these factors, M-TAIGWO aims to improve security and save energy.

$$X_{i-DLH,d}(t+1) = X_{i,d}(t) + rand \times (X_{n,d}(t) - X_{r,d}(t)) \tag{18}$$

3.6. Selecting and updating phase:

To choose the ideal candidate at this step, the fitness ratings of two candidates, $X_{i-GWO}(t+1)$ and $X_{i-DLH}(t+1)$ are compared in (19). Next, to the update position of $X_i(t+1)$, if their fitness is lower than $X_i(t)$, then the selected candidate updates $X_i(t)$. If not, $X_i(t)$ stays the same. Following the process, the number of iterations is improved by 1, and the search is continued again until the target number of epochs is reached.

$$X_i(t+1) = \begin{cases} X_{i-GWO}(t+1) & ,if\ fX_{i-GWO} < fX_{i-DLH} \\ X_{i-DLH}(t+1) & otherwise \end{cases} \tag{19}$$

Every software's fitness is determined using a multi-objective function. These goals consist of the following: (i) decreasing the cluster numbers, (ii) higher intra-cluster density, (iii) energy balance of clusters, (iv) node balancing inside clusters, and (v) a smaller distance between candidate nodes and sink. Safety nodes that are within range of every member in their cluster are referred to as candidate nodes. In actuality, a single hop can be used to send data among candidate nodes and other members. The selection of nodes as CH is hence done effectively. The node with the highest safety level among the candidates is chosen as the CH for each cluster. These CH assignments are updated regularly at every θ_{CH} routing round. In (20) is utilized to calculate the fitness function by utilizing the specified objectives.

$$min\ w_1.K + w_2.D_v + w_3.\sigma_e + w_4.\sigma_c + w_5.D_C \tag{20}$$

Where, intra-cluster distance's sum denotes D_v, which is taken as the average across all clusters. The total number of i^{th} software's clusters shows K, while the average distance between each candidate node and the sink is known D_C. Standard deviation of total number of candidate nodes across all clusters is represented as σ_c, and minimizing it aids in the best possible selection of CH. σ_e denotes standard deviation of clusters' energy and reducing it causes a high energy balance among clusters. The influence of each object is applied using the total weight technique as the intended objectives differ. In the fitness function, where $w_1 + w_2 + w_3 + w_4 + w_5 = 1$, w denotes the weight coefficient of each object.

By selecting a shorter route based on these factors, M-TAIGWO aims to improve security and save energy. Therefore, only secure nodes and an energy-aware trust mechanism are used by the M-TAIGWO routing algorithm. In (21) is used to build the fitness function and choose the route. Every route has this function calculated and routing is based on the route with the highest value.

$$max\ \xi_1.E_r + \xi_2.T_r - \xi_3.HC_r - \xi_4.D_r \tag{21}$$

Where, the sum of distance, energies, and trust scores of nodes incorporated in route r is represented by D_r, E_r, and T_r. In this route, the hop count is denoted by HC_r. $\xi_1 + \xi_2 + \xi_3 + \xi_4 = 1$, where ξ is the weight coefficient to demonstrate each parameter's effect, and this algorithm runs until the 100 iterations.

3.7. Fitness for SCH selection

The following explains multi-objective functions utilized in cluster routing path selection optimization technique; the energy, connection, and trust score characteristics in the implemented method are used to identify the safe nodes, and the routing operation is executed accordingly. The neighbors and routing tables provide connectivity and energy respectively, while each node's distribution of the trust score determines the total trust score. Specific timeslots (for instance, every θ_{SN} routing round) are updated/detected in safe nodes, and node j's safety level is denoted as SV_j. In the first round, all nodes are safe because all node's trust scores are initially set to 1. However, after examining nodes' behavior, the nodes' energy and change of trust score, a threshold needs to be used to identify the safe nodes. The approach that is adopted divides safe and malicious nodes by θ_{MN} applying the threshold. Consequently, the routing table's "safe" field is determined using (22).

$$Safe_j = \{0\ SV_j < \theta_{MN}\ 1\ otherwise \tag{22}$$

Where, the trust score, energy, and connectivity parameters are calculated using SV_j, as represented in (23). Because of the variations in parameter types, all parameters' scales are normalized with values between 0 and 1. Furthermore, the node only determines its neighboring nodes' safety level, and it is not allowed for any node to assess its safety level. Where the connectivity, energy rate, and trust score of s_j are respectively denoted as C_j, E_j, and T_j, as described below.

$$SV_j = \frac{1}{3}[E_j + C_j + T_j] \tag{23}$$

- Energy rate: a malicious node appears as a node with large resources (energy, memory, etc.) in the majority of attacks including Sinkhole, Black-hole, Hello flood, selective forwarding, and Sink-hole. Consequently, energy must be considered when identifying safe nodes. The energy rate parameter can be computed as the difference between node with highest energy and node with leftover energy. Given that malicious nodes are thought to declare their resources in large quantities, a node with a modest energy differential is probably malicious. This considers the energy rate depending on the initial energy to compute it more accurately. Therefore, E_j is computed in (24). Where, the node with maximum energy is represented as e_{max}, the j-th node energy is shown as e_j, and the initial energy of nodes is denoted as E_0.

$$E_j = E_0 - [e_{max} - e_j] \tag{24}$$

- Connectivity: safe data flow is ensured by a network that is fully connected. Every node must have at least one route sink, which is available for connecting with a WSN. In general, the nodes' positions have a big impact on connection. In this situation, nodes with bi-directional links ensure a fully connected network which is used to calculate connectivity parameter. C_j is represented in (25), whereas the network's total number of connections is shown as L, and j-th node's number of links denoted nc_j.

$$C_j = \frac{nc_j}{L} \tag{25}$$

- Trust score: as demonstrated in (26), this metric is defined as the total of direct and indirect trust. T_j is trust score of j^{th} node and utilized to infuse neighboring table's 'Trust' field. Here, the impact coefficient for trust score is represented as α, and indirect and direct trust applied to j^{th} node is denoted IT_j and DT_j.

$$T_j = \alpha.DT_j + (1-\alpha).IT_j \tag{26}$$

- Direct trust: the interactions between the two nodes determine the direct trust score. Every node in the network additionally calculates the trustworthiness of its neighbors. Therefore, DT_j is computed using (27).

$$DT_j = \beta\frac{ar_j}{nr_j} + (1-\beta).\frac{at_j}{nt_j} \tag{27}$$

  Where, the received total number of packets is represented nr_j, and the received acknowledgment packet number by j^{th} node is denoted as ar_j. Likewise, packets sent from the j^{th} node show at_j and nt_j. Additionally, the direct trust score is measured by the β effect coefficient among received and sent packets.
- Indirect trust: the neighboring table's data is used to measure indirect trust, based on the node's behavior towards its neighbours. Therefore, IT_j is calculated by (28). Where, the neighboring nodes are set and their number denotes nn_j and $|nn_j|$. In addition, the trust score of s_k is represented as T_k, and the recommended trust to s_j by s_k denotes T_k^j.

$$IT_j = \frac{\sum_{k \in nn_j}[T_k + T_k^j]}{|nn_j|} \tag{28}$$

3.8. Clustering

This section divides the network into several clusters according to the member nodes' time division multiple access (TDMA) schedules. It consists of r rounds with the steady-state phase and set-up phase being two phases of each round. CH selection occurs in the first phase or setup phase, and is determined by two criteria. Percentage p of nodes in network is the first factor, and the total number of nodes that have functioned as CH is the second phase. Based on a random number selected between 0 and 1, each node n determines a threshold value $T(n)$, which is shown in (29). Based on a random number chosen between 0 and 1, each node n determines a threshold value $T(n)$.

$$T(n) = \begin{cases} \frac{p}{1-p\left[r \bmod\left(\frac{1}{p}\right)\right]} & if\ n \in G \\ 0, & else \end{cases} \tag{29}$$

At each round, a node receives CH if the random number generated is lesser than the threshold value. A similar probability $\frac{1}{p}$ is assigned to each SN to become a CH in a given round. SN use the TDMA slot they have been assigned to transmit the data they have gathered to the CH during the second phase, also known as the steady state phase. The BS receives the combined data that the CH has collected.

3.9. Route discovery stage using M-TAIGWO

The distance, energy, and trust parameters are used in the M-TAIGWO based secure multi-hop discovery process. An M-TAIGWO technique increases the overall effectiveness, and security of WSNs by combining path optimization and CH selection within a unified optimization method. The M-TAIGWO method is used to optimize CH selection and routing paths in WSN, aiming to minimize energy consumption and enhance security, resulting in a more robust and efficient WSN. The following are the steps for route discovery using M-TAIGWO:

- Grey wolf solutions frequently utilize paths with dimensions equal to the number of relays SCHs, connecting the transmitter SCHs to the BS.
- The position update for the potable paths initialized in grey wolf is comparable to the iterative approach outlined in the preceding section. The fitness considered in the M-TAIGWO for determining the route is specified in (30).

$$f = \mu_1 \times (DT + IT + RT) + \mu_2 \times \sum_{i=1}^{d} E_{CH_i} + \mu_3 \times \sum_{i=1}^{d} dis(SCH_i, BS) \tag{30}$$

The fitness function that is previously mentioned determines the secure path that is used to avoid malicious attacks such as Hello flood attacks, selective forwarding attacks, and black hole attacks, sinkhole attacks during data transfer. Malicious node mitigation aids in preventing underside network energy usage and packet loss. IGWO can be seen in Algorithm 1.

Algorithm 1. Improved grey wolf optimization (IGWO)

```
Input: N, D, Maxiter
Output: The global optimum
Start
Initialize (N wolves are distributed at random around the search area, and their fitness is determined)
For iter = 2 to Maxiter
      Find $\overrightarrow{X_\alpha}$, $\overrightarrow{X_\beta}$, and $\overrightarrow{X_\delta}$.
      For i = 1 to N
             Calculating $\overrightarrow{X_1}$, $\overrightarrow{X_2}$, $\overrightarrow{X_3}$ by utilizing (12), (13), (14). // updating positions
             Calculating $X_{i-GWO}(t+1)$ by utilizing (15).
             Calculating $R_i(t)$ by (16).
             Establishing neighborhood $X_i(t)$ with radius $R_i$ by (17). // exploration
             For l = 1 to D
                   $X_{i-DLH,d}(t+1) = X_{i,d}(t) + rand \times (X_{n,d}(t) - X_{r,d}(t))$ // exploitation
             End for
             Choosing best $(X_{i-GWO}(t+1), X_{i-DLH}(t+1))$.
             Updating positing
      End for
End for
Return the global optimum.
End
```

4. RESULTS AND DISCUSSION

The results and evaluation studies of the M-TAIGWO approach are described in this section. MATLAB R2020b is utilized to implement and simulate the M-TAIGWO technique. The system specifications include an i7 processor, 16 GB RAM, and Windows 10 OS. The estimation of the M-TAIGWO algorithm is performed through varying numbers of nodes. The SCHs and secure route path selection are performed by M-TAIGWO to attain secure communication. Table 1 shows the simulation parameters considered to analyze the M-TAIGWO. Variable nodes are considered because node density is one of the primary characteristics for assessing the performance of WSN.

Table 1. Simulation parameters

Parameter	Value
Number of nodes	5, 10, 15, 20, 25, 30, 100, 200, 300, 400, and 500
Network size	$1500 \times 1500m$
Initial energy	1J
Size of packet	s

4.1. Quantitative and qualitative analysis

In this section, quantitative and qualitative analyses of the implemented M-TAIGWO approach concerning energy consumption, delay, and network lifetime are presented in Tables 2 to 5. Table 2 shows performance analysis of the under-hello flood attacks with varying 5 nodes. The performances of the black widow (BW), particle swarm optimization (PSO), and artificial bee colony (ABC) are compared with that of the implemented M-TAIGWO approach. Figure 3 illustrates the graphical representation of under hello flood attacks with varying 5 nodes. Figure 3 shows how the quantity of packets that malicious nodes in the network discards increases corresponding to the number of malicious nodes initiating hello flood attacks. In a hello flood attack, a malicious node broadcasts hello packets with sufficient energy to confuse other distant nodes into believing it to be its immediate neighbor. This suggests that the malicious node rejects a large number of packets. The quantity of rejected packets in M-TAIGWO is significantly lesser than that of BW, ABC, and PSO as seen in Figure 4. When compared to the M-TAIGWO to BW, ADC, and PSO, the average number of lost packets is lower by 17.62%, and 30.97%, respectively.

Table 2. Performance analysis of under hello flood attacks with varying 5 nodes

Proportion of malicious nodes/%	BW	ABC	PSO	Proposed M-TAIGWO
5	300	420	350	200
10	360	500	420	280
15	430	640	510	300
20	550	760	680	420
25	1,400	1,700	1,650	1,000
30	1,700	1,800	1,780	1,200

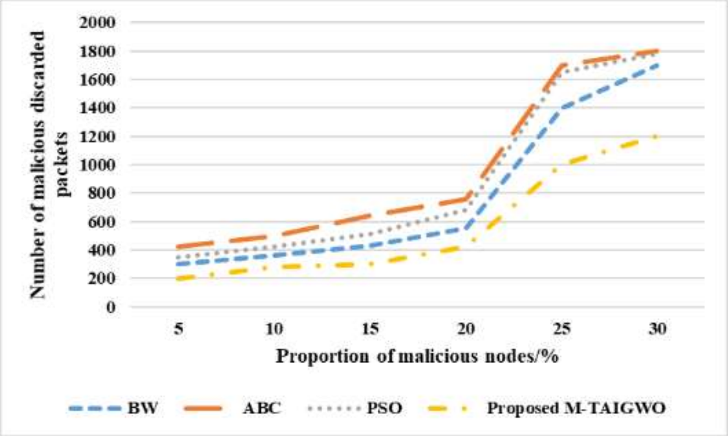

Figure 3. Graphical representation of under hello flood attacks with varying 5 nodes

Table 3 represents the performance analysis of under sinkhole attacks with varying 5 nodes. Figure 4 represents a graphical representation of under sinkhole attacks with varying 5 nodes. Figure 4 shows how the quantity of packets that malicious nodes in network gradually improves correspondingly with number of malicious nodes conducting sinkhole attacks. In a sinkhole attack, a malicious node forms a black hole around itself, attracting all other nodes in the area to transmit packets to it. In comparison to BW, ABC, and PSO, the average number of lost packets for M-TAIGWO decreases by 17.53% and 34.4%, respectively.

Table 3. Performance analysis of under sinkhole attacks with varying 5 nodes

Proportion of malicious nodes/%	BW	ABC	PSO	Proposed M-TAIGWO
5	150	130	110	80
10	280	200	250	110
15	295	240	265	115
20	320	255	280	135
25	375	290	330	180
30	400	350	370	200

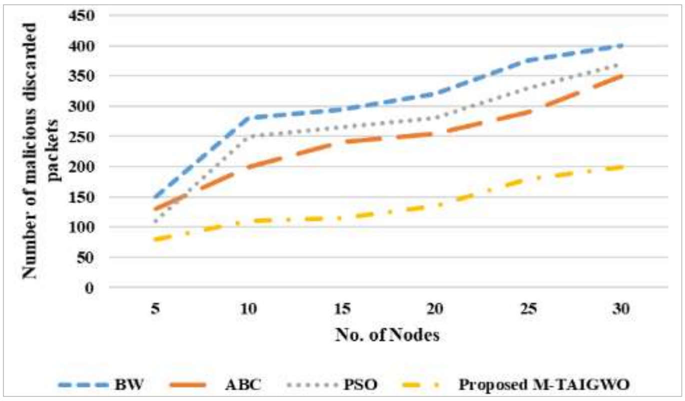

Figure 4. Graphical representation of under sinkhole attacks with varying 5 nodes

Table 4 shows under-hello flood attacks performance analysis with varying 5 nodes. Figure 5 illustrates the graphical representation of under hello flood attacks with varying 5 nodes. A malicious node performs a black hole attack by confusing another node in the network into establishing routing connections with it, resulting in malicious loss of packets intended for forwarding. All of the packets that are received are discarded by the malicious nodes. As a result, the malicious node's trust value rapidly drops below the trust threshold as compared to BW, ABC, and PSO. It minimizes the quality of harmful dropped packets and speeds up the identification of malicious nodes. In comparison to BW, ABC, and PSO, the average number of packet losses for M-TAIGWO is decreased by 15.75% and 23.32%, respectively.

Table 5 shows under-selective forwarding attacks with varying 5 nodes performance analysis. Figure 6 illustrates graphical representation of under-selective forwarding attacks with varying 5 nodes. Figure 6 shows how the quantity of packets discarded by malicious nodes in the network progressively improves the number of malicious nodes and increases selective forwarding attacks. Black hole attack arises when packets have a 100% probability, but selective forwarding attack occurs when a malicious node forwards or discards essential packets with a certain probability. This study has a 70% probability that the packets received are discarded by the malicious node. Drawing from Figures 5 and 6, it is seen that malicious nodes establishing selective forwarding attacks have a greater number of packets than malicious nodes initiating black hole attacks. The average number of lost packets for M-TAIGWO is lower than that of BW, ABC, and PSO by 9.21% and 9.62% as shown in Figure 6.

Table 4. Performance analysis of under black hole attacks with varying 5 nodes

Proportion of malicious nodes/%	BW	ABC	PSO	Proposed M-TAIGWO
5	180	200	155	100
10	240	265	210	190
15	360	390	350	310
20	430	475	480	400
25	730	740	710	615
30	815	850	875	730

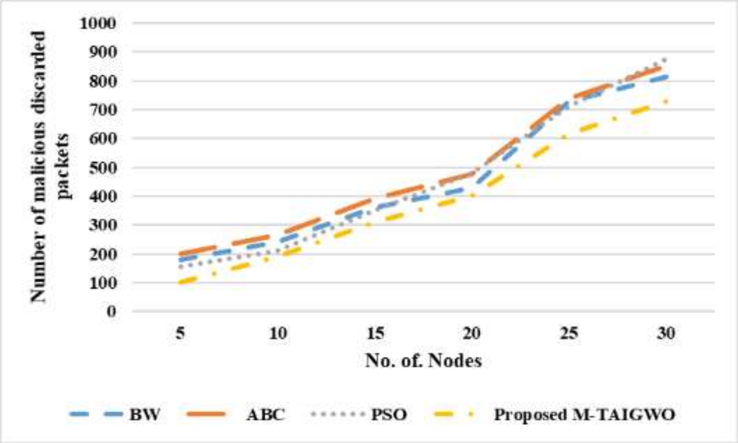

Figure 5. Graphical representation of under black hole attacks with varying 5 nodes

Table 5. Performance analysis of under selective forwarding attacks with varying 5 nodes

Proportion of malicious nodes/%	BW	ABC	PSO	Proposed M-TAIGWO
5	470	380	450	350
10	500	530	580	440
15	740	790	810	610
20	1,000	1,090	1,075	980
25	1,280	1,300	1,310	1,150
30	1,490	1,500	1,465	1,300

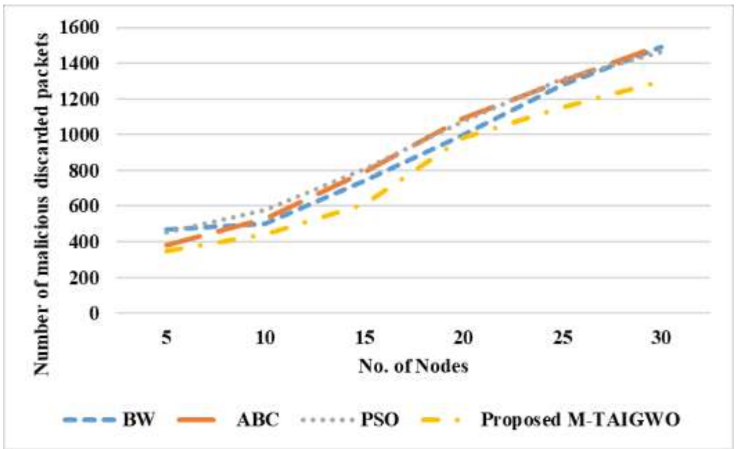

Figure 6. Graphical representation of under selective forwarding attacks with varying 5 nodes

Table 6 represents energy consumption performance analysis in Joule (J) with varying 100 nodes. The performances of the BW, ABC, and PSO are compared with the M-TAIGWO approach. Figure 7 shows the graphical representation of energy consumption with varying 100 nodes. The obtained result shows that the implemented M-TAIGWO demands lesser energy consumption of 75 J in 100 nodes, 78 J in 200 nodes, and 79 J in 300 nodes, respectively.

Table 6. Performance analysis of energy consumption (J) with varying 100 nodes

Number of nodes	BW	ABC	PSO	Proposed M-TAIGWO
100	75	89	87	64
200	80	85	92	70
300	83	90	95	73

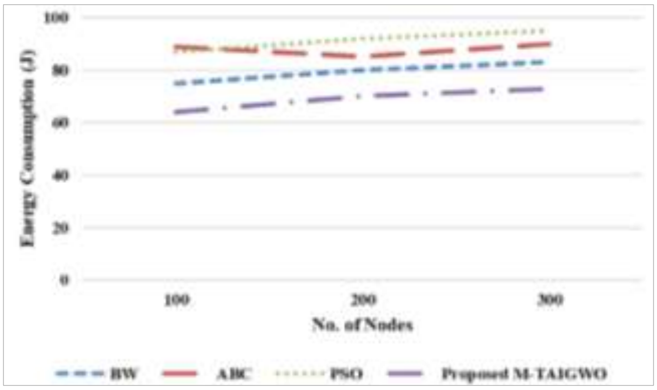

Figure 7. Graphical representation of energy consumption (J) with varying 100 nodes

Table 7 represents the performance analysis of delay in milli seconds (ms) with varying 100 nodes. The delay refers to the time taken for transmitting data packets from source to BS. The outcomes of the BW, ABC, and PSO are compared with the M-TAIGWO approach. Figure 8 shows the graphical representation of delay with varying 100 nodes. The obtained result shows that the implemented M-TAIGWO provides less delay of 15 ms in 100 nodes, 46 ms in 200 nodes, and 52 ms in 300 nodes, respectively.

Table 7. Performance analysis of delay (ms) with varying 100 nodes

Number of nodes	BW	ABC	PSO	Proposed M-TAIGWO
100	40	56	47	15
200	52	63	59	46
300	65	70	68	52

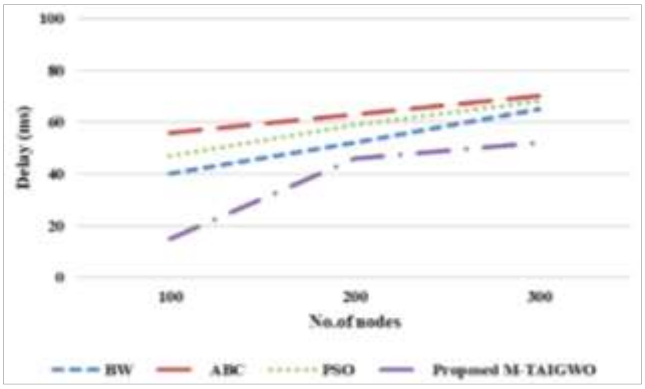

Figure 8. Graphical representation of delay (ms) with varying 100 nodes

Table 8 represents the performance analysis of PDR in (%) with varying 100 nodes. The outcomes of the BW, ABC, and PSO are compared with the M-TAIGWO approach. Figure 9 shows the graphical representation of PDR with varying 100 nodes. The obtained result shows that the implemented M-TAIGWO provides a high PDR of 94% in 100 nodes, 97% in 200 nodes, 95% in 300 nodes, 96% in 400 nodes, 98% in 500 nodes.

Table 8. Performance analysis of PDR (%)

Number of nodes	BW	ABC	PSO	Proposed M-TAIGWO
100	75	89	90	94
200	80	93	85	97
300	92	87	89	95
400	89	79	92	96
500	82	90	93	98

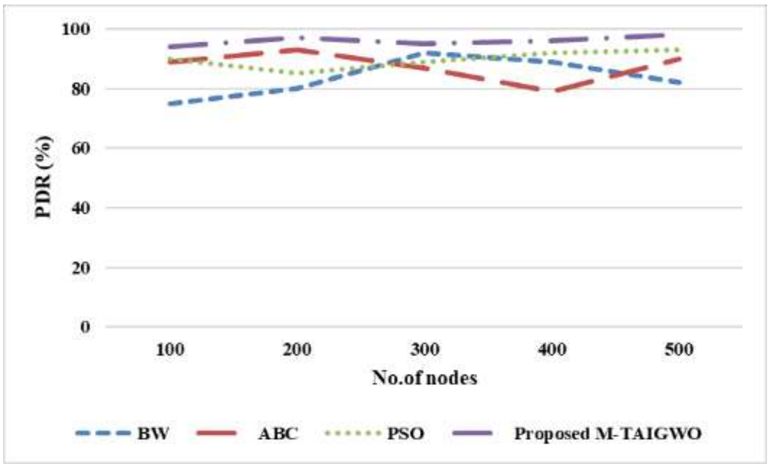

Figure 9. Graphical representation of PDR (%)

Table 9 displays the performance analysis of the network lifetime in rounds with varying 100 nodes. The results of the BW, ABC, and PSO are compared with the M-TAIGWO approach. Figure 10 shows the graphical representation of network lifetime with varying 100 nodes. The obtained result shows that the implemented M-TAIGWO provides a high network lifetime of 240 rounds in 100 nodes, 255 rounds in 200 nodes, 260 rounds in 300 nodes, 255 rounds in 400 nodes, and 270 rounds in 500 nodes.

Furthermore, by improved node load balancing, better CH selection and better clustering, the M-TAIGWO provides an improved network lifetime. Trust-based routing identifies malicious nodes like Hello flood attacks, sinkhole attacks, black hole attacks, and selective forwarding attacks, and sends out more packets as an outcome. Nodes' energy consumption is decreased due to an increase in packet delivery ratio and enhanced identification of malicious nodes, which has improved network lifetime.

Table 9. Performance analysis of network lifetime (rounds)

Number of nodes	BW	ABC	PSO	Proposed M-TAIGWO
100	210	200	190	240
200	185	210	235	255
300	220	245	250	260
400	215	195	230	255
500	200	230	245	270

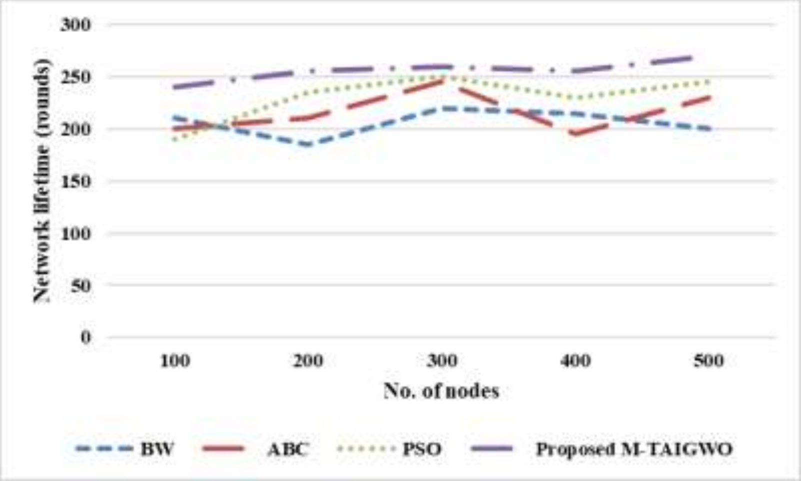

Figure 10. Graphical representation of network lifetime (rounds)

4.2. Comparative analysis

Table 10 represents simulation parameters considered to analyse M-TAIGWO. This section supplies a comparative analysis of implemented M-TAIGWO approach with evaluation metrics including energy consumption, delay, network lifetime, and PDR are shown in Tables 11 to 13. Table 11 shows the four types of attacks with varying 5 nodes compared with existing TAGA [17]. While the malicious nodes proportion increases, the number of malicious discarded packets also increases. Table 12 denoted the energy consumption (J) and delay (ms) varying 100 nodes compared with existing method of fuzzy and secured clustering algorithm. The number of nudes increases the energy consumption (J) and delay (ms) decreases. Table 13 illustrates the network lifetime (rounds), and PDR (%) varying 100 nodes compared with existing method of QGAOA. The network lifetime (rounds) and PDR (%) are increases when the number of nodes increases. The implemented M-TAIGWO method's performance is compared with existing methods such as the fuzzy and secured clustering algorithm [16], QGAOA [18], and TAGA [17]. The implemented M-TAIGWO algorithm is used to improve capacity against malicious attacks.

Table 10. Simulation parameters

Parameter	Value
Number of nodes	5, 10, 15, 20, 25, 30, 100, 200, 300, 400, and 500
Network size	$1500 \times 1500m$
Initial energy	1J
Size of packet	s

Table 11. Comparison of four types of attacks with varying 5 nodes for malicious discarded packets

Proportion of malicious nodes/%	TAGA [17]				Proposed M-TAIGWO			
	Hello Flood	Sinkhole	Black hole	Selective forwarding	Hello Flood	Sinkhole	Black hole	Selective forwarding
5	210	95	200	380	200	80	100	350
10	300	140	220	460	280	110	190	440
15	330	145	350	650	300	115	310	610
20	450	170	440	1,100	420	135	400	980
25	1,300	200	650	1,250	1,000	180	615	1,150
30	1,500	230	780	1,600	1,200	200	730	1,300

Table 12. Comparison of energy consumption (J) and delay (ms) varying 100 nodes with existing methods

Number of nodes	Fuzzy and secured clustering algorithm [16]		Proposed M-TAIGWO	
	Energy consumption (J)	Delay (ms)	Energy consumption (J)	Delay (ms)
100	85	25	64	15
200	86	58	70	46
300	88	60	73	52

Table 13. Comparison of network lifetime (rounds), and PDR (%) varying 100 nodes with existing methods

Number of nodes	QGAOA [18]		Proposed M-TAIGWO	
	Network lifetime (rounds)	PDR (%)	Network lifetime (rounds)	PDR (%)
100	230	93	240	94
200	240	96	255	97
300	250	93	260	95
400	245	94	255	96
500	255	97	270	98

5. CONCLUSION

In order to improve security against malicious attacks, M-TAIGWO implements the secure cluster-based routing protocol in this research. To avoid malicious attacks like Hello flood attacks, sinkhole attacks, black hole attacks, and selective forwarding attacks during communication, SCHs from regular sensors and route paths through SCHs are selected by using M-TAIGWO. Additionally, M-TAIGWO clustering increases the WSN network lifetime by improving energy efficiency and performing safe communication. The shortest route obtained from M-TAIGWO is employed to secrease delay over WSN, and hence, data transmission of M-TAIGWO is improved in WSN. From the experimental results, it is evident that the implemented method achieves superior performance to the Fuzzy and secured clustering algorithm, QGAOA, and TAGA. The implemented method obtains a PDR of 98% for 500 nodes which is superior to the QGAOA, with a delay of 15 ms for 100 nodes which is lesser than the fuzzy and secured clustering algorithm. In contrast to

TAGA, this implemented method achieves defense, hello flood, selective forwarding, sinkhole, and black hole attacks effectively. The simulation results demonstrate the effective performance of the M-TAIGWO method in mitigating the impact of malicious nodes. It not only decreases the incidence of lost packets, but also significantly improves the network energy efficiency. In the future, advanced WSN attributes can be explored for trust factors computation for secure routing, and also a novel robust protocol can be developed to manage more WSN critical attacks.

REFERENCES

[1] H. Wu, H. Zhu, X. Li, and M. J. V. Amuri, "Trust-based distributed set-membership filtering for target tracking under network attacks," *IEEE Access*, vol. 11, pp. 84468–84474, 2023, doi: 10.1109/ACCESS.2023.3303203.

[2] W. Osamy, A. M. Khedr, D. Vijayan, and A. Salim, "TACTIRSO: trust aware clustering technique based on improved rat swarm optimizer for WSN-enabled intelligent transportation system," *Journal of Supercomputing*, vol. 79, no. 6, pp. 5962–6016, Apr. 2023, doi: 10.1007/s11227-022-04889-3.

[3] T. Khan *et al.*, "An efficient trust-based decision-making approach for WSNs: machine learning oriented approach," *Computer Communications*, vol. 209, pp. 217–229, Sep. 2023, doi: 10.1016/j.comcom.2023.06.014.

[4] P. Srividya and L. N. Devi, "An optimal cluster & trusted path for routing formation and classification of intrusion using the machine learning classification approach in WSN," *Global Transitions Proceedings*, vol. 3, no. 1, pp. 317–325, Jun. 2022, doi: 10.1016/j.gltp.2022.03.018.

[5] Y. Xia *et al.*, "A trust-based reliable confident information coverage model of wireless sensor networks for intelligent transportation," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 7, pp. 9542–9554, Jul. 2023, doi: 10.1109/TVT.2023.3253131.

[6] A. V. Jatti and V. J. K. K. Sonti, "Optimizing optical network longevity via Q-learning-based routing protocol for energy efficiency and throughput enhancement," *Optical and Quantum Electronics*, vol. 56, no. 1, p. 32, Jan. 2024, doi: 10.1007/s11082-023-05658-z.

[7] K. Dinesh and S. V. N. Santhosh Kumar, "Energy-efficient trust-aware secured neuro-fuzzy clustering with sparrow search optimization in wireless sensor network," *International Journal of Information Security*, vol. 23, no. 1, pp. 199–223, Feb. 2024, doi: 10.1007/s10207-023-00737-4.

[8] S. L. Shah, Z. H. Abbas, G. Abbas, F. Muhammad, A. Hussien, and T. Baker, "An innovative clustering hierarchical protocol for data collection from remote wireless sensor networks based internet of things applications," *Sensors*, vol. 23, no. 12, p. 5728, Jun. 2023, doi: 10.3390/s23125728.

[9] H. Yin, H. Yang, and S. Shahmoradi, "EATMR: an energy-aware trust algorithm based the AODV protocol and multi-path routing approach in wireless sensor networks," *Telecommunication Systems*, vol. 81, no. 1, pp. 1–19, Sep. 2022, doi: 10.1007/s11235-022-00915-0.

[10] X. Yu, F. Li, T. Li, N. Wu, H. Wang, and H. Zhou, "Trust-based secure directed diffusion routing protocol in WSN," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 3, pp. 1405–1417, Mar. 2022, doi: 10.1007/s12652-020-02638-z.

[11] A. R. A. Moundounga and H. Satori, "Stochastic machine learning based attacks detection system in wireless sensor networks," *Journal of Network and Systems Management*, vol. 32, no. 1, p. 17, Jan. 2024, doi: 10.1007/s10922-023-09794-5.

[12] 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, Jul. 2023, doi: 10.1007/s11276-023-03288-7.

[13] A. Sharma, H. Babbar, S. Rani, D. K. Sah, S. Sehar, and G. Gianini, "MHSEER: a meta-heuristic secure and energy-efficient routing protocol for wireless sensor network-based industrial IoT," *Energies*, vol. 16, no. 10, p. 4198, May 2023, doi: 10.3390/en16104198.

[14] C. Li, Y. Liu, J. Xiao, and J. Zhou, "MCEAACO-QSRP: a novel QoS-secure routing protocol for industrial internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18760–18777, Oct. 2022, doi: 10.1109/JIOT.2022.3162106.

[15] K. Sathish *et al.*, "Reliable data transmission in underwater wireless sensor networks using a cluster-based routing protocol endorsed by member nodes," *Electronics (Switzerland)*, vol. 12, no. 6, p. 1287, Mar. 2023, doi: 10.3390/electronics12061287.

[16] B. Kranthikumar and R. L. Velusamy, "Trust aware secured energy efficient fuzzy clustering-based protocol in wireless sensor networks," *Soft Computing*, Apr. 2023, doi: 10.1007/s00500-023-08098-9.

[17] 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, doi: 10.1109/ACCESS.2022.3144015.

[18] 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*, vol. 15, no. 3, pp. 1057–1069, Mar. 2024, doi: 10.1007/s13198-023-02189-4.

[19] D. K. Bangotra, Y. Singh, A. Selwal, N. Kumar, and P. K. Singh, "A trust based secure intelligent opportunistic routing protocol for wireless sensor networks," *Wireless Personal Communications*, vol. 127, no. 2, pp. 1045–1066, Nov. 2022, doi: 10.1007/s11277-021-08564-3.

[20] A. Pathak, I. Al-Anbagi, and H. J. Hamilton, "An adaptive QoS and trust-based lightweight secure routing algorithm for WSNs," *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 23826–23840, Dec. 2022, doi: 10.1109/JIOT.2022.3189832.

[21] Z. Teng, C. Du, M. Li, H. Zhang, and W. Zhu, "A wormhole attack detection algorithm integrated with the node trust optimization model in WSNs," *IEEE Sensors Journal*, vol. 22, no. 7, pp. 7361–7370, Apr. 2022, doi: 10.1109/JSEN.2022.3152841.

[22] R. I. Sajan, V. B. Christopher, M. J. Kavitha, and T. S. Akhila, "An energy aware secure three-level weighted trust evaluation and grey wolf optimization based routing in wireless ad hoc sensor network," *Wireless Networks*, vol. 28, no. 4, pp. 1439–1455, May 2022, doi: 10.1007/s11276-022-02917-x.

[23] S. Al-Otaibi, V. Cherappa, T. Thangarajan, R. Shanmugam, P. Ananth, and S. Arulswamy, "Hybrid K-Medoids with energy-efficient sunflower optimization algorithm for wireless sensor networks," *Sustainability (Switzerland)*, vol. 15, no. 7, p. 5759, Mar. 2023, doi: 10.3390/su15075759.

[24] V. Pandiya Raj and M. Duraipandian, "Energy conservation using PISAE and cross-layer-based opportunistic routing protocol (CORP) for wireless sensor network," *Engineering Science and Technology, an International Journal*, vol. 42, p. 101411, Jun. 2023, doi: 10.1016/j.jestch.2023.101411.

[25] R. K. V. Penmatsa, S. K. R. Mallidi, and R. R. Muni, “A wrapper based feature selection using grey wolf optimization for botnet attack detection,” *International Journal of Sensors, Wireless Communications and Control*, vol. 11, no. 9, pp. 951–956, Nov. 2021, doi: 10.2174/2210327911666210120124340.

[26] M. Otair, O. T. Ibrahim, L. Abualigah, M. Altalhi, and P. Sumari, “An enhanced grey wolf optimizer based particle swarm optimizer for intrusion detection system in wireless sensor networks,” *Wireless Networks*, vol. 28, no. 2, pp. 721–744, Feb. 2022, doi: 10.1007/s11276-021-02866-x.

BIOGRAPHIES OF AUTHORS

Venkatesh Prasad Bannikuppe Srinivasiah received the B.E. degree in Computer Science and Master Degree in Information Technology from Bangalore University, Karnataka, India. He is presently working as Assistant professor in the Department of Computer Science and Engineering at Government Engineering College, Kushalnagar, Karnataka, India. His main research interests include computer networks, wireless sensor networks, and machine learning. He can be contacted at email: venkyp25@gmail.com.

Roopashree Hejjaji Ranganathasharma has completed B.E. (E&C) and M.Tech. (CS&E) from VTU, Belagavi, Karnataka, India and Ph.D. from CHRIST (Deemed to be University) Bengaluru, Karanataka, India. She has around 13 years of Industrial experience and 2 years of teaching experience. She is presently working as a Professor and Head of, the Department of Artificial Intelligence and Data Science at GSSSIETW, Mysuru. She can be contacted at email: roopashreehr@gsss.edu.in.

Venkatesh Ramanna is currently Associate Professor in department of Computer Science and engineering, University of Visvesvaraya College of Engineering, Bangalore, obtained his bachelor degree, master degree and Ph.D. degree in Computer Science and Engineering in the year 2000, 2004 and 2018 respectively. His area research includes segmentation techniques, cyber security, IoT wireless sensor network and OSN privacy preservation. He can be contacted at email: venkateshm.uvce@bub.ernet.in.