Received: October 23, 2024. Revised: November 18, 2024. 596

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Spiral Elite Learning with Gazelle Optimization Algorithm Based Secure Clustering and Routing in Wireless Sensor Network

Sumathi Manjari Suryanarayana[1]* Hemantaraj Mohan Kelagadi[2]
Soumya Lokeshappa Nagarathna[3] Raju Hajare[1]

[1]Department of Electronics and Telecommunication Engineering,
BMS Institute of Technology and Management, Bengaluru, India
[2]Department of Electronics and Communication Engineering,
Dr. Ambedkar Institute of Technology, Bangalore, India
[3]Department of Computer Science and Engineering (AI & ML), Sai Vidya Institute of Technology, Bengaluru, India
* Corresponding author's Email: sumathi.m@bmsit.in

Abstract: Wireless Sensor Networks (WSNs) are a dispersed group of sensor nodes that are deployed in an open and hostile environment for data transmission. Sensor data is transmitted by each node in the network using multi-hop communication until it reaches the Base Station (BS). However, the resource-constrained nature of devices and their operation in potentially hostile and dynamic environments makes it difficult to ensure and maintain secure communication in WSN which is one of the major challenges. To address this issue, a Spiral Elite Learning based Gazelle Optimization Algorithm (SEL-GOA) is proposed for secure Cluster Head (CH) selection and routing in the WSNs without compromising the nodes. In secure CH selection and routing, to avoid node compromising and malicious attacks, the GOA model optimizes the selection process by security parameters (Fitness Functions) and ensures that selected CH and routing paths are in the secure area of the network. The experimental results of the proposed SEL-GOA show that the algorithm has achieved energy consumption of 0.31 J, delay of 16 ms and Throughput of 94 mbps for 500 nodes. These results are better when compared to existing clustering and routing methods such as Neuro Fuzzy Clustering with Sparrow Search Optimization Algorithm (NF-SSOA).

Keywords: Base station, Cluster head, Secure cluster head selection and routing, Spiral elite learning based Gazelle optimization algorithm, Wireless sensor networks.

1. Introduction

Wireless Sensor Network (WSN) is a system of tiny, numerous and low power sensor nodes that are used to communicate with one another and with their surroundings. The WSN comprises several wireless sensor nodes that perform sensing, computation, and secure communication, which is used in several applications like military, aerospace, etc., [1–3]. The nodes are positioned randomly in specific areas forming wireless networks to perform specific tasks such as collecting relevant data and transmitting the information to the Base Station (BS) in a single or multi-hop transmissions [4]. Due to the limited resource nature of sensor networks and hostile environments, energy efficiency and security are considered two key factors in designing secure routing protocols [5]. A cluster in WSN refers to a group of sensor nodes that are deployed randomly and are organized to manage network operations efficiently in clustering and routing [6-8]. The clustering is a process of grouping sensor nodes that are organized to efficiently manage network operations and resource allocation [9].

Every cluster in WSNs contains CH to gather all data from neighbor nodes and then communicate with the BS for further processing [10]. An advantage of clustering is that it removes redundant data transmission in the network leads to minimizing communication overhead and reduced the Energy Consumption (EC) in WSN [11]. Several researchers

utilize different optimization algorithms in WSNs to optimize EC during clustering and routing as well as increase the network lifetime of nodes [12]. The data communication in WSNs is vulnerable to various attacks because the nodes in the network are deployed in open and unfriendly environments that leads to insecure data transmission [13]. Due to the dynamic and hostile environment of WSN networks, the sensor nodes are vulnerable to malicious attacks, thus security is crucial for efficient data transmission in WSN applications [14,15]. However, much research has focused only on energy-efficient clustering and routing since several factors lead to insecure communication in WSN. To overcome these limitations, a Spiral Elite Learning Strategy-Gazelle Optimization Algorithm (SEL-GOA) algorithm is proposed to perform secure Cluster Head (CH) selection and routing in WSN. The main contributions of the proposed method are:

- The SEL-GOA algorithm is proposed for secure clustering and routing in WSN which enhances secure communication with less energy consumption. The SEL strategy selects the elite solutions (CHs) based on the fitness functions to avoid node compromising.
- The SEL strategy improves secure clustering and routing by adapting the changes in dynamic network conditions and node behaviour that prevent node compromising in WSN.
- The GOA mitigates the impact of the compromised nodes by selecting only elite CH and routes that enhance secure data communication through an SEL strategy that minimizes the risk of security threats.

This research paper is structured as follows: Section 2 describes a literature review of existing clustering and routing methods. Section 3 presents an explanation of the proposed SEL-GOA algorithm. Section 4 illustrates the result and discussion. The conclusion of this research is given in Section 5.

2. Literature review

In this section, the advantages and limitations of existing clustering and routing algorithms in WSN are described.

Dinesh and Kumar [16] designed an energy-efficient secured clustering model in WSN based on Neuro Fuzzy Clustering with Sparrow Search Optimization Algorithm (NF-SSOA). The designed NF-SSOA optimization model was utilized for trust-aware clustering and routing, to provide lightweight key generation and ensure hop-to-hop authentication of nodes in WSN. An advantage of the NF-SSOA algorithm was improved energy consumption and throughput of the network by selecting optimal CH by SSO algorithm. However, the designed NF-SSOA model failed to adapt to evaluating attack patterns and thus selected the compromised nodes as CH and introduced delay while selecting of secure path that impacts data transmission.

Kumar and Srimanchari [17] developed a trust and energy-efficient data aggregation scheme based on Quantum behavior and Gaussian Mutation based Archimedes Optimization Algorithm (QGAOA). The developed QGAOA model was employed to select reliable and energy efficient CH and to avoid malicious activity of nodes. An advantage of the developed QGAOA clustering and routing model is decreased packet drops in data transmission due to a reliable routing path. However, the clustering and routing based on the QGAOA model focused only on energy efficiency and trust which does not prioritize the security aspects that lead to potential node compromising.

Kranthikumar and Velusamy [18] explored a trust-aware and secure energy-efficient clustering model in WSN. The explored trust-based fuzzy logic-based clustering model was used to identify malicious nodes and select reliable routes for data communication. A five-level rule-based mechanism by fuzzy logic was utilized to reduce energy consumption in CH selection and improve the clustering process by selecting an optimal CH. However, the explored fuzzy clustering model was sensitive to parameters that failed to select secure CH and routing due to the dynamic nature of the WSN environment.

Rajkumar [19] presented a secured energy-efficient routing model for WSN based on hierarchical protocol. The presented Hierarchical Secured Energy Efficient Routing Protocol (HSEERP) utilized well-organized path maintenance with a low overhead path discovery technique to reduce the energy consumption for clustering and routing. An advantage of the presented HSEERP model was that selected CH collects data from other sensor nodes which reduced the energy consumption efficiently by minimizing multiple data transmissions before forwarding them to the base station. However, the presented HSEERP protocol has the drawback of CH node compromise due to inherent vulnerabilities that affect the secure clustering and routing in WSN.

Biswas [20] represented the Energy Efficient Secure Multipath Routing (EESMR) model for secure and energy efficient communication in WSN based on lightweight mechanisms. The represented EESMR model utilized several techniques such as a one-way hash chain, message authentication code,

and a clique-based coordinator selection technique to improve the routing process in WSN. The main advantage of the presented multipath routing model was that enhanced secure routing by distributing the data packets to multiple routes. However, the represented EESMR model has limitations such as high energy consumption for path maintenance and the vulnerability of attack surface was increased due to multiple paths because all paths in the network are not secure uniformly.

Nageswararao Malisetti and Vinay Kumar Pamula [21] explored an energy efficient clusterbased routing model by hybrid optimization algorithm for WSN. The explored hybrid optimization model was a combination of Moth Levy Adopted Artificial Electric Field Algorithm (ML-AAEF) was employed to select the efficient cluster based routing and Customized Grey Wolf Optimization Algorithm (CGWO) for data transmission. The main advantage of the explored hybrid model was that determines an energy efficient cluster and routing path for efficient data transmission. However, the explored ML-AAEF and CGWO model only focused on energy efficient routing, where the model has limitation that node compromission.

There are some limitations from the above-mentioned existing clustering and routing approaches in WSN such as secure communication being difficult due to the dynamic environment, node compromising in the cluster, and increase in energy consumption. To overcome these drawbacks, a SEL-GOA algorithm is proposed for secure clustering and routing as well as to improve secure communication in WSN. The SEL strategy adapts to the dynamic environment efficiently and selects elite solutions (CH and routing path) and the quick agile nature of GOA prevents the node comprising those results in effective communication in the WSN.

3. Methodology

The proposed secure clustering and routing in WSN includes four phases: Node deployment and initialization, secure CH selection, cluster formation and secure routing. The flowchart of secure clustering and routing in WSN is illustrated in Fig. 1. Initially, the nodes in WSN are deployed and initialized for data transmission. Then CH is selected securely based on the proposed SEL-GOA algorithm.

After that, clusters are formed by potential functions and finally, a secure routing path to avoid malicious attacks effectively.

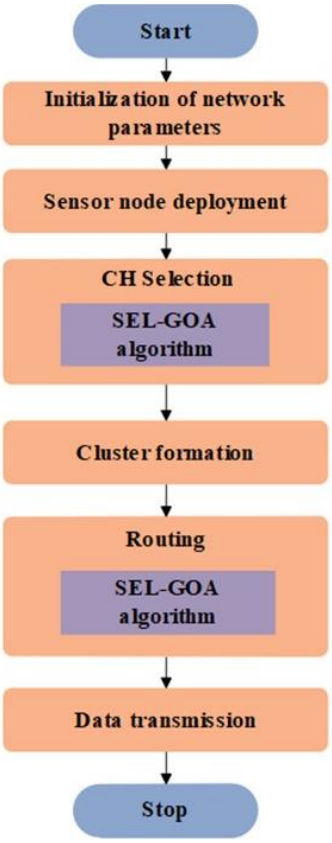

Figure. 1 The flowchart of proposed SEL-GOA model

3.1 Node deployment

The sensor node deployment is a process of distribution of nodes within the WSN that ensures the security and network coverage and energy efficiency of the network [22]. Here, the nodes are deployed randomly in WSN to ensure effective data transmission throughout the network.

3.2 SEL-GOA based secure CH selection

The CH selection is a process of selecting specific nodes that represent the leaders and coordinators of clusters of sensor nodes in WSN. A CH is responsible for managing the nodes utilized for different tasks like communication with other CHs or with the base station. The CH selection is most important to optimize the network's energy efficiency and secure data transmission. The gazelle optimization is a population-based algorithm that performs better in selecting optimal CH and routing in WSN. However, the limitations of GOA are sensitivity to initial conditions and less adaptability nature in dynamic environments that lead to node compromising, sub-optimal selection of CH and routing path which impact on risk of losing important information. To overcome these limitations, a SEL strategy based-

GOA is proposed is for secure CH selection which is explained below:

3.2.1. Initialization

The Gazelles are prey animals that are popularly known for their agility, speed, and acute senses to escape from predator (like cheetahs). This is a population-based optimization algorithm [23] where, each gazelles (X) is represented as a search agent to identify the best solutions. The position of each gazelle is initialized with a random node_id between 1 and n.

Let $x_{ij} = \left(x_{i,1}(t), x_{i,1}(t), \dots, x_{i,1}(t)\right)$ be the candidate solution j^{th} randomly induced in i^{th} solution, where the position $x_{i,d,}1 \le d \le m$ that determines the node_id and m represents amount of CHs in the WSN network. The mathematical representation of initialization and GOA population is expressed in Eq. (1) and Eq. (2).

$$X = \begin{bmatrix} x_{1,1} & x_{1,2} & \dots & x_{1,d-1} & x_{1,d} \\ x_{2,1} & x_{2,1} & \dots & x_{2,d-1} & x_{2,d} \\ \vdots & \vdots & x_{i,j} & \vdots & \vdots \\ x_{n,1} & x_{n,1} & \cdots & x_{n,d-1} & x_{n,d} \end{bmatrix} \quad (1)$$

$$x_{ij} = rand \times \left(UB_j - LB_j\right) + LB_j \quad (2)$$

Where, $rand$ represents random value; LB_j and UB_j denotes lower bound and upper bound ; x_{ij} indicates position vector of top gazelle; d and n stands for search space dimension and number of gazelles. After initialization, candidate solution for x_{ij}, n and d are estimated by the fitness function utilized for CH selection.

In SEL-GOA, the best solutions are updated based on two phases exploitation and exploration phases. For secure CH selection and routing in this research, Grazing, Stotting and Evasive running are the three strategic behaviours of gazelles are utilized in the above-mentioned two phases for finding the best solutions.

3.2.2. Exploitation stage

In the exploitation stage, the behaviour of gazelle known as "Grazing" technique which is used to search a specific area or region to obtain the best solution. To enhance convergence within the search space, a Brownian motion is employed in grazing technique which is represented in Eq. (3).

$$f_B(x, \mu, \sigma) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)} = \frac{1}{\sqrt{2\pi}} e^{\left(-\frac{x^2}{2}\right)} \quad (3)$$

Where, f_B denotes standard Brownian motion; μ, x, and σ^2 represents mean, given point, and unit variance. The grazing strategy by gazelles helps to select optimal CH by evaluating the fitness function of nodes based on historical data and potential vulnerability. The mathematical formulation for the exploitation of gazelles is formulated in Eq. (4).

$$\overrightarrow{g_{\iota+1}} = \overrightarrow{g_\iota} + \text{s}.\ \overrightarrow{R}.* \overrightarrow{R_B}.* \left(\overrightarrow{Elite_\iota} - \overrightarrow{R_B}.* \overrightarrow{g_\iota}\right) \quad (4)$$

Where, $\overrightarrow{g_{\iota+1}}$ and $\overrightarrow{g_\iota}$ represents next and current solutions; s denotes grazing speed of gazelles; $\overrightarrow{R}$ and $\overrightarrow{R_B}$ indicates a vector of uniform numbers and random numbers that represent Brownian motion. $\overrightarrow{Elite_\iota}$ stands for top gazelle vector. After searching (exploitation) for a suitable region the best solution space is identified to select the best solution performed by the exploration phase which is as follows

3.2.3. Exploration stage

The exploration process of GOA is divided into two subprocesses: Stotting and Evasive running for best CH selection. When the gazelles detect or sense a predator (attacks) near to them, it leaps into the air quickly which is called stotting. This is a behavior of the gazelle performed to escape from predators and a secret signal used to make other gazelles alert. The stotting of a gazelle is denoted by a scaled value which ranges between 0 and 1 which are small steps. To enhance exploration, Levy Flight method is used to combine the small steps of leaping in the stotting technique with occasional continuous steps. The Levy based movements in stotting are given in Eq. (5):

$$\overrightarrow{g_{\iota+1}} = \overrightarrow{g_\iota} + \text{S}.\,\mu.\,\overrightarrow{\text{R}}.* \overrightarrow{R_L} * \left(\overrightarrow{Elite_\iota} - \overrightarrow{R_L} * \overrightarrow{g_\iota}\right) \quad (5)$$

Where, μ denotes sudden directional changes by controlled steps; $\overrightarrow{R_L}$ represents Levy based movements. The behavior of the predator when gazelles change their direction suddenly by changing step lengths and random influences. The predator behavior and the sudden change are represented in Eqs. (6) and (7).

$$\overrightarrow{g_{\iota+1}} = \overrightarrow{g_\iota} + \text{S}..\,\mu.\,\text{CF}.* \overrightarrow{\text{R}_\text{B}}.* \left(\overrightarrow{Elite_\iota} - \overrightarrow{R_L}.* \overrightarrow{g_\iota}\right) \quad (6)$$

$$\overrightarrow{g_{\iota+1}} = \begin{cases} \overrightarrow{g_\iota} + CF[\overrightarrow{LB} + \vec{R}.* (\overrightarrow{UB} - \overrightarrow{LB})].* \vec{U}, if\ r \le PSRs \\ \overrightarrow{g_\iota} + [PSRs(1-r) + r](\overrightarrow{g_{r1}} - \overrightarrow{g_{r2}}), \quad otherwise \end{cases} \quad (7)$$

In an optimization process, the balance between the utilization of search space's exploration and exploitation is essential for achieving a global optimal solution. However, the performance of GOA algorithm negatively impacts on secure CH selection due to limitations such as dynamic re-routing, sensitivity at initial conditions that results in solving the issues of node compromise and dynamic environment. The gazelle's reactive nature, which relies on initial conditions that lead to inconsistent CH selection and routing in WSN. This results in increasing delay in adapting to the new network changes. The increase in learning time causes delays in adapting the network which makes it more susceptible to malicious attacks like Sybil attacks and DOS attacks.

3.2.4. Proposed spiral elite learning – Gazelle optimization algorithm

To improve secure CH selection and routing in WSN SEL strategy is employed with GOA for solving the limitations of GOA to make secure and reliable node selection as well as path selection. By selecting an Elite CH node using refinement selection reduces the need for frequent re-routing and improves secure CH selection.

- **Spiral elite learning strategy:**

Since GOA updates positions based on two randomly generated solutions that leads to the risk of losing promising regions. To address this, a SEL technique is proposed to obtain the best solution which utilizes a Logarithmic Spiral Step (LSS) that is designed to gradually decrease as iterations progress. The mathematical representation of LSS in GOA is given in Eqs. (8) to (10).

$$LSS = Ae^{-b.t}cos(2c\pi t) \tag{8}$$

$$A = \left(\frac{U_i - L_i}{2}\right) * \left(\frac{T-t}{T}\right)^2, U_i = max(X_i), \quad L_i = min(X_i) \tag{9}$$

$$x_i^{LSS} = x_{best} + LSS \tag{10}$$

Where, x_i^{LSS} represents new position utilizing LSS; A refers to shrinking radius; b indicates a constant that determines LSS; t denotes parameter that defines how much the next position should be near to best solution; c stands for number of spirals. Since the GOA model is a combination of random and linear search patterns it relies more on initial parameters. If the CH is selected based only on the initial condition it leads to less security and is prone to data breaches due to the chance of selecting sub-optimal CH and paths.

Hence, SEL strategy utilizes a spiral search pattern to minimize the dependency on initial conditions and reduce energy consumption for selection, by narrowing down the search technique in the most promising region. The main advantage of the SEL strategy is continuous learning and stable adoption which makes GOA learn and refine solutions quickly. The continuous and stable learning by SEL allows the GOA model to remain efficient in a dynamic environment and reduces the delay in adapting to the change.

3.3 Fitness function for secure CH selection

The proposed SEL-GOA enhanced the secure CH selection and reduced energy consumption in WSN by utilizing fitness functions such as Trust, distance, energy, node degree and hop count. The fitness value (f) of secure CH is evaluated as follows:

- **Trust:**

The trust value is a node's degree of trust receiving services which are compared to neighboring nodes. To select optimal and secure CH, the trust factor is the most important fitness function where the CH with a high trust value is selected for CH in WSN. The trust value of a cluster node should be high for that node to be selected as CH. The trust factor (f_1) for CH selection is expressed as in Eq. (11):

$$f_1 = \frac{1}{T_{tch} * N_{nch}} \sum_{n=1}^{T_{tch}} \sum_{o=1}^{N_{nch}} \left(T_{xtst}^{"}\right)_{no} \tag{11}$$

Where, $\left(T_{xtst}^{"}\right)$ represents average of three trust factors (T_{xtst}^{recent}), $\left(T_{xtst}^{direct}\right)$ and $\left(T_{xtst}^{indirect}\right)$ trust for n^{-th} CH and o^{-th} neighboring node of CH.

- **Distance:**

The distance is referred as the distance between every CH to the base station. The CH with minimum distance from the base station is the preferable decision for efficient data transmission in the WSN. Distance between n^{th} CH and o^{th} neighboring node f_2 is expressed in Eq. (12).

$$f_2 = \frac{1}{T_{tch} * N_{nch}} \sum_{n=1}^{T_{tch}} \sum_{o=1}^{N_{nch}} \left[\frac{\left(D_{xdis}^{"}\right)_{no}}{N_{nch}}\right] \tag{12}$$

Where, $D_{xdis}^{"}$ denotes distance between nodes; N_{nch} represents total neighboring nodes.

- **Energy:**

If the CH node's energy is less while receiving data from its perspective CH nodes, then the aggregation of nodes while transmitting the data to the base station helps for effective communication in WSN. The energy consumption of the selected CH is estimated by the Energy constraint f_3 which is evaluated by Eq. (13).

$$f_3 = \frac{1}{T_{tch}} \sum_{n=1}^{T_{tch}} \left(E_{xenr}^{"}\right)_n \quad (13)$$

Where, $E_{xenr}^{"}$ denotes energy of sensor nodes; T_{tch} represents the total number of CHs.

- **Minimum node degree:**

The minimum node degree is referred to number of cluster members in the network that are related to CH. The estimation of minimum node degree (f_4) in the cluster is expressed in Eq. (14).

$$f_4 = \sum_{i=1}^{n} \min\left(Nd\_degree\ (XCH_i, BS)\right) \quad (14)$$

Where, Nd_degree represents node degree; BS denotes base station. This node degree is crucial for selecting optimal CH where the node degree of the CH should be minimum.

- **Minimum hop count:**

The hop count refers to many intermediate devices such as routers, switches, or gateways that a data packet passes through a network from source to destination. The minimum hop count (f_5) is estimated by the Eq. (15).

$$f_5 = \sum_{i=1}^{n} \min\left(hop\_count\ (XCH_i, BS)\right) \quad (15)$$

The overall fitness function is estimated by the normalization process $\left(F(x)\right)$ which is subjugated to each function α_1, α_2, α_3, α_4 and $\alpha_5$is formulated as shown in Eq. (16).

$$F(x) = \frac{f_i - f_{min}}{f_{max} - f_{min}} \quad (16)$$

Where, f_{min} and f_{max} represents minimum and maximum fitness values. The minimum fitness value is estimated by the given Eq. (17).

$$F = \alpha_1 f_1 + \alpha_2 f_2 + \alpha_3 f_3 + \alpha_4 f_4 + \alpha_5 f_5 \quad where, \sum_{i=1}^{4} \alpha_i ; and\ \alpha_i \epsilon (0,1) \quad (17)$$

Where, F denotes the overall fitness function; α_1, α_2, α_3, α_4 and α_5 represents weighted coefficients, f_1, f_2, f_3, f_4, and f_5 refers to trust, distance, energy, minimum node degree and minimum hop count.

3.4 Cluster formation

According to the optimal CH selected by GOA, the nodes are further clustered to improve the effectiveness of the WSN. The sensor nodes are grouped to CH with high residual energy and less transmission distance. The cluster formation in WSN is represented in Eq. (18).

$$SN_p = \frac{Z \times Energy\ (CH_j)}{Distance(s_i, CH_j)} \quad (18)$$

Where, SN_p denotes sensor node potential; Z indicates proportionality constant; $Energy\ (CH_j)$ denotes residual energy of the respective CH; $Distance(s_i, CH_j)$ represents the distance between the CH_j and sensor s_i; This cluster formation in WSN reduced the energy consumption of several nodes in data transmission and minimizes intra-cluster distance between nodes effectively.

3.5 Routing

After selecting a secure CH in WSN, the suitable secure paths are identified for data transmission from cluster members (sensor nodes) to the BS through the selected CHs. The proposed SEL-GOA model is used to select an optimal and secure route for reliable data transmission. To ensure secure data transmission, the model estimates two important parameters in fitness estimation: trust, energy, and distance.

- **Trust:**

The trust value is a node's degree of trust receiving services which are compared to neighboring nodes. The value of trust of a cluster node should be high for the node for selection of routing. The trust factor (f_1) for optimal route selection is expressed as in Eq. (19).

$$f_1 = \frac{1}{T_{tch} * N_{nch}} \sum_{n=1}^{T_{tch}} \sum_{o=1}^{N_{nch}} \left(T_{xtst}^{"}\right)_{no} \quad (19)$$

- **Distance:**

The distance is referred to as the distance between CH to the hop node and from the hop node to the base station. The distance between nodes and base station should be less and consume less energy for effective communication in WSN. Therefore, distance between n^{th} CH to the base station f_2 is expressed in Eq. (20).

$$f_2 = \frac{1}{T_{tch} * N_{nch}} \sum_{n=1}^{T_{tch}} \sum_{o=1}^{N_{nch}} \left[\frac{\left(D_{xdis}^{"}\right)_{no}}{N_{nch}} \right] \quad (20)$$

- **Energy:**

The energy consumption of the hop nodes should be less for effective data transmission from the hop node to the base station in WSN. The routing path with less energy consumption is a preferable choice for data to receive, integrate, and transmit to the next CH or to the base station. The Energy constraint f_3 for routing is evaluated by Eq. (21).

$$f_3 = \frac{1}{T_{tch}} \sum_{n=1}^{T_{tch}} \left(E_{xenr}^{"}\right)_n \quad (21)$$

Due to the contrast of each fitness function values, a weighted sum technique is employed to normalize the values and this weighted value is assigned for each function. By utilizing this technique, the multi-objective function is converted into a single objective function. The values obtained from all fitness functions have distinct units, thus, the normalization method is applied for every fitness function which is represented in the Eq. (22).

$$F = \beta_1 \times f_1 + \beta_2 \times f_2 + \beta_3 \times f_3 \quad (22)$$

Where, β_1 , β_2 and β_3 denotes weighted coefficients; f_1 , f_2 and f_3 represents the fitness functions trust, distance and energy respectively. A reliable and secure route for efficient data transmission is identified by the position update Eq. (15) with the fitness function which have mentioned above. The agile nature and adaptive nature of gazelles search the optimal routes quickly between the sensor nodes. The proposed GOA algorithm identify multiple routing paths by avoiding vulnerable and congested nodes which lead to data packet loss and security threats. The proposed SEL-GOA model ensures that the sensitive information is transmitted by secure and reliable routes by adapting search mechanism according to dynamic network conditions. The proposed SEL-GOA algorithm focused on searching around the elite solutions, that ensure more secure and reliable routes by stotting and evasive running behaviour and optimize the factors like trust, energy and distance, which are critical for secure data transmission in WSNs.

4. Results and discussion

The performance analysis of the proposed SEL-GOA method is used in secure CH selection and routing in WSN is evaluated by different performance metrics. In this research, the proposed SEL-GOA model is simulated using MATLAB R2020b software tool with a system configuration of i7 processor, 16 GB RAM and Windows 10 OS. Performance measures used for evaluation are Throughput, Delay, Packet Delivery Ratio (PDR), energy consumption and residual energy. Table 1 represents the simulation parameter settings of the proposed method.

4.1 Quantitative and qualitative analysis

The performance analysis of the proposed SEL-GOA for secure clustering and routing in WSN is illustrated in Tables 2 to 6. The quantitative results of Throughput utilizing the number of nodes is illustrated in Table 2. The proposed SEL-GOA algorithm is evaluated and compared with existing optimization algorithms such as Particle Swarm Optimization (PSO), Salp Swarm Optimization (SSO), Ant Colony Optimization (ACO) and GOA. The SEL-GOA attains a superior throughput scoring of 98mbps, 97mbps, 96mbps, 95mbps, and 94mbps at the number of nodes of 100, 200, 300, 400, 500 respectively. The proposed GOA model ensured the utilization of network resources efficiently by selecting secure and energy-efficient routes through its agile nature that minimized node failure, and energy depletion results in enhanced throughput than existing approaches.

The quantitative results of delay utilizing the number of nodes is illustrated in Table 3. The proposed SEL-GOA algorithm is evaluated and compared with existing optimization algorithms such

Table 1. Simulation parameters of proposed method

Parameter	Value
Area	1000×1000
Number of Nodes	100-500
Initial Energy	1J

Table 2. Performance analysis of proposed SEL-GOA for Throughput

Methods	Metric	Number of Nodes				
		100	200	300	400	500
PSO	Throughput (mbps)	92	92	91	90	90
SSO		93	93	92	91	91
ACO		94	93	93	92	92
GOA		96	95	94	94	93
Proposed SEL-GOA		98	97	96	95	94

Table 3. Performance analysis of proposed SEL-GOA for Delay.

Methods	Metric	Number of Nodes				
		100	**200**	**300**	**400**	**500**
PSO	Delay (ms)	18	20	21	23	23
SSO		16	18	19	19	21
ACO		15	17	17	18	19
GOA		13	14	14	16	17
Proposed SEL-GOA		11	13	13	14	16

Table 4. Performance analysis of proposed SEL-GOA for PDR

Methods	Number of Nodes				
	100	200	300	400	500
PSO	0.92	0.91	0.90	0.90	0.89
SSO	0.93	0.92	0.91	0.91	0.90
ACO	0.94	0.93	0.93	0.92	0.91
GOA	0.96	0.95	0.95	0.93	0.92
Proposed SEL-GOA	0.98	0.97	0.97	0.94	0.92

Table 5. Performance analysis of proposed SEL-GOA for alive nodes

Methods	Number of Nodes				
	100	**200**	**300**	**400**	**500**
PSO	94	107	213	325	413
SSO	95	120	228	340	422
ACO	96	136	242	364	428
GOA	97	142	259	383	446
Proposed SEL-GOA	99	178	286	390	477

as PSO, SSO, ACO and GOA. The SEL-GOA attains less delay of 11 ms, 13 ms, 13, ms, 14 ms, 16 ms at number of nodes of 100, 200, 300, 400, and 500 respectively. The proposed GOA focused only on shorter and less congested routing paths to confirm that data packets are transmitted with minimum delays. The advantage of GOA which adopts and adjusts dynamic network conditions for the selection of optimal routing paths to reduce delay.

The quantitative results of PDR utilizing the number of nodes is illustrated in Table 4. The proposed SEL-GOA algorithm is evaluated and compared with existing optimization algorithms such as PSO, SSO, ACO and GOA. The SEL-GOA attains a high PDR of 0.98, 0.97, 0.97, 0.94, 0.92 at the number of nodes of 100, 200, 300, 400, 500 respectively. The SEL strategy incorporated with GOA selects the most reliable and secure routes for data transmission that reduces packet loss by compromised routes and improved PDR than previous routing approaches.

Table 6. Performance analysis of proposed SEL-GOA for energy consumption

Methods	Metric	Number of Nodes				
		100	**200**	**300**	**400**	**500**
PSO	Energy Consumption (J)	62	64	69	72	75
SSO		61	64	66	69	73
ACO		57	60	63	67	70
GOA		54	56	57	59	60
Proposed SEL-GOA		48	49	51	53	54

The quantitative results of alive nodes based on number of rounds are illustrated in Table 5. The proposed SEL-GOA algorithm is evaluated at 1000 th iteration and compared with existing optimization algorithms such as PSO, SSO, ACO and GOA.

The quantitative results of energy consumption utilizing number of nodes are illustrated in Table 6. The proposed SEL-GOA algorithm is evaluated and compared with existing optimization algorithms such as PSO, SSO, ACO and GOA. The SEL-GOA reduced the energy consumption of 48, 49, 51, 53, and 54 for nodes of 100, 200, 300, 400, and 500 respectively. The proposed SEL strategy optimizes the positioning and movement of CHs in a spiral search pattern which reflects the natural foraging behavior of elite gazelles in the algorithm. This balances the identifying of new CH nodes and optimizing existing CHs, which ensure energy-efficient nodes with optimal positions as CH.

4.2 Comparative analysis

The comparative analysis of proposed SEL-GOA with CH selection and routing techniques such as NF-SSOA [16], QGAOA [17], Fuzzy Clustering [18], HSEERP [19], EESMR [20] and ML-AAEF and CGWO [21] is depicted in this section. The comparison results for the proposed algorithm are performed under different scenarios with parameters like area, number of nodes and initial energy.

The existing models SSOA [16] and HSEERP [19] in scenario 1 involves area of $1000 \times 1000m^2$, 100-500 nodes, with initial energy of 1J. The QGAOA [17] in scenario 2 involves area of $1500 \times 1500m^2$, 100-500 nodes, with initial energy of 1J. The Fuzzy Clustering [18] model in scenario 3 involves area of $1000 \times 1000m^2$, 100-300 nodes, with initial energy of 1J. The EESMR [20] model in scenario 4 involves area of $100 \times 100m^2$, 100-500 nodes, with initial energy of 2J. The ML-AAEF and CGWO [21] model in scenario 5 involves area of

Table 7. Comparative analysis of proposed SEL-GOA vs NF-SSOA [16]

Methods	Metrics	Number of Nodes				
		100	200	300	400	500
NF-SSOA [16]	Energy Consumption (J)	0.1	0.21	0.27	0.31	0.35
	Delay (ms)	12	13	13	15	18
	Throughput (mbps)	95	95	94	94	93
Proposed SEL-GOA	Energy Consumption (J)	0.1	0.18	0.24	0.27	0.31
	Delay (ms)	10	11	11	13	16
	Throughput (mbps)	97	96	96	95	94

Table 8. Comparative analysis of proposed SEL-GOA vs QGAOA [17]

Methods	Metrics	Number of Nodes				
		100	200	300	400	500
QGAOA [17]	Energy Consumption (J)	3897.25	4312.93	4901.32	5292.01	5921.91
	Delay (ms)	11.34	13.84	14.56	16.21	18.86
	Throughput (%)	96	97	94	96	95
Proposed SEL-GOA	Energy Consumption (J)	3451.19	4198.47	4467.82	4896.34	5466.38
	Delay (ms)	10.27	12.44	13.19	14.86	16.92
	Throughput (%)	98	97	97	96	96

Table 9. Comparative analysis of proposed SEL-GOA vs Fuzzy Clustering [18]

Methods	Metrics	Number of Nodes		
		100	200	300
Fuzzy Clustering [18]	Delay (ms)	25	55	60
	Energy Consumption (J)	85	87	88
Proposed SEL-GOA	Delay (ms)	18	48	54
	Energy Consumption (J)	77	84	86

Table 10. Comparative analysis of proposed SEL-GOA vs HSEERP [19]

Methods	Metrics	Number of nodes				
		100	200	300	400	500
HSEERP [19]	PDR	98	96	95.5	95	93
Proposed SEL-GOA		100	98	96	95.5	94

Table 11. Comparative analysis of proposed SEL-GOA vs EESMR [20]

Methods	Metrics	Number of nodes				
		100	200	300	400	500
EESMR [20]	PDR	91	92	94	96	98
Proposed SEL-GOA		93	95	97	98	100

Table 12. Comparative analysis of proposed SEL-GOA vs ML-AAEF and CGWO [21]

Methods	Metrics	Number of nodes	
		100	200
ML-AAEF and CGWO [21]	Throughput	3.9×10^8	3×10^8
Proposed SEL-GOA		4×10^8	3.5×10^8

$100 \times 100m^2$, 100-200 nodes, with initial energy of 0.5J. The end condition for all scenarios is stop until the energy exhaust for every node.

The comparative analysis with existing methods in different scenarios is illustrated in Tables 7 to 12 using various performance metrics of delay, energy consumption, and throughput. From the comparative analysis results, it is clear that the proposed SEL-GOA is most suitable from smaller node level to high node level which perform efficiently in WSN.

4.3 Discussion

The proposed SEL-GOA model achieved better results for secure clustering and routing in WSN by selecting an optimal CH and reliable routing path. However, the existing methods used for CH selection and routing in WSN have drawbacks such as the dynamic nature of trust calculations and their integration with clustering in the NF-SSOA [16] model that leads to performance degradation in terms

of security. The clustering and routing by QGAOA model [17] focused on energy efficiency and trust which does not address security aspects which lead to potential security vulnerabilities. The fuzzy clustering [18] model failed to select the CH and path correctly due to the dynamic nature of the WSN environment and compromise in the node. HSEERP [19] protocol has the drawback of CH node compromise due to inherent vulnerabilities that affect the secure clustering and routing in WSN. EESMR model [20] has limitations such as high energy consumption for path maintenance and the vulnerability of attack surface was increased due to multiple paths because all paths in the network are not secure uniformly. ML-AAEF and CGWO model [21] only focused on energy efficient routing, where the model has limitation that node compromising.

To overcome these problems, a SEL-GOA algorithm is proposed to provide secure clustering and routing in WSN and for selecting optimal CH. The main advantage of the proposed SEL-GOA model can remove compromised nodes by selecting elite solutions and re-evaluate the search process to select optimal CH and route path by a spiral search pattern. The continuous learning in SEL make GOA to adapt the dynamic changes in the WSN environment quickly and make refined elite solutions for secure data transmission.

5. Conclusion

The SEL-GOA is proposed to enable secure clustering and routing in WSN by selecting optimal CH without compromising the network nodes. In secure clustering and routing, the SEL strategy in GOA helps to optimize the selection of CH and secure paths by integrating security parameters (Fitness Functions) such as trust, energy, distance, minimum node degree and minimum hop count. The learning process of the SEL strategy is integrated with the GOA model that adapts to dynamic security requirements efficiently and enhances the CH selection and routing which leads to secure and energy-efficient data transmission in WSN. The experimental results of the proposed SEL-GOA represent that the algorithm achieved energy consumption of 0.31 J, delay of 16 ms and Throughput of 94 mbps for 500 nodes which is better results when compared to existing clustering and routing methods such as NF-SSOA, QGAOA and Fuzzy clustering. In future, an improved metaheuristic optimization algorithm will be implemented to enhance CH selection and secure routing in WSN.

Notation

Notation	Description
$rand$	Random value
LB_j and UB_j	Lower bound and upper bound
x_{ij}	Position vector of top gazelle
d and n	Search space dimension and number of gazelles
f_B	Standard Brownian motion
μ, x, and σ^2	Mean, given point, and unit variance
$\overrightarrow{g_{i+1}}$ and $\overrightarrow{g_i}$	Next and current solutions
s	Grazing speed of gazelles
$\overrightarrow{R}$ and $\overrightarrow{R_B}$	A vector of uniform numbers and random numbers that represent Brownian motion
$\overrightarrow{Elite_i}$	Top gazelle vector
μ	Sudden directional changes by controlled steps
$\overrightarrow{R_L}$	Levy based movements
x_i^{LSS}	New position utilizing Logarithmic Spiral Step (LSS)
A	Shrinking radius
b	A constant that determines LSS
t	Parameter that defines how much the next position should be near to best solution
c	Number of spirals
$\left(T_{xtst}^{"}\right)$	Average of three trust factors $\left(T_{xtst}^{recent}\right)$, $\left(T_{xtst}^{direct}\right)$ and $\left(T_{xtst}^{indirect}\right)$ trust for n^{-th} CH and o^{-th} neighboring node of CH
$\left(T_{xtst}^{recent}\right)$	Recent trust
$\left(T_{xtst}^{direct}\right)$	Direct trust
$\left(T_{xtst}^{indirect}\right)$	Indirect trust
$D_{xdis}^{"}$	Distance between nodes
N_{nch}	Total neighboring nodes
$E_{xenr}^{"}$	Energy of sensor nodes
T_{tch}	The total number of CHs
Nd_degree	Node degree
BS	Base station
f_5	Minimum hop count
$\left(F(x)\right)$	Fitness function is estimated by the normalization process
f_{min} and f_{max}	Minimum and maximum fitness values
F	The overall fitness function
α_1, α_2, α_3, α_4 and α_5	Weighted coefficients
f_1, f_2, f_3, f_4, and f_5	Trust, distance, energy, minimum node degree and minimum hop count
SN_p	Sensor node potential
Z;	Proportionality constant
$Energy\ (CH_j)$	Residual energy of the respective CH

$Distance(s_i, CH_j)$	Distance between the CH_j and sensor s_i
β_1, β_2 and β_3	Weighted coefficients
f_1, f_2 and f_3	Fitness functions trust, distance and energy respectively

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 3rd and 4th author. The supervision and project administration, have been done by 1st and 2nd author.

References

[1] V.B.S. Prasad, and H.R. Roopashree, "Energy aware and secure routing for hierarchical cluster through trust evaluation", *Measurement: Sensors*, Vol. 33, p. 101132, 2024.

[2] A. Ali, A. Ali, F. Masud, M.K. Bashir, A.H. Zahid, G. Mustafa, and Z. Ali, "Enhanced fuzzy logic zone stable election protocol for cluster head election (E-FLZSEPFCH) and multipath routing in wireless sensor networks", *Ain Shams Engineering Journal*, Vol. 15, No. 2, p. 102356, 2024.

[3] T.A. Abose, V. Tekulapally, D.C. Kejela, K.T. Megersa, S.T. Daka, and K.A. Jember, "Optimized Cluster Routing Protocol with Energy-Sustainable Mechanisms for Wireless Sensor Networks", *IEEE Access*, Vol. 12, pp. 99661-99671, 2024.

[4] S. Anitha, S. Saravanan, and A. Chandrasekar, "Trust management based multidimensional secure cluster with RSA cryptography algorithm in WSN for secure data transmission", *Measurement: Sensors*, Vol. 29, p. 100889, 2023.

[5] E.P. Roja, and D.S. Misbha, "Lightweight key distribution for secured and energy efficient communication in wireless sensor network: An optimization assisted model", *High-Confidence Computing*, Vol. 3, No. 2, p. 100126, 2023.

[6] M.S. Sumathi, and G.S. Anitha, "WSN to detect real time terrain slides using Wi-GIM instrument", *Materials Today: Proceedings*, Vol. 80, No. 3, pp. 2888-2894, 2023.

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

[8] R.F. Mansour, S.A. Alsuhibany, S. Abdel-Khalek, R. Alharbi, T. Vaiyapuri, A.J. Obaid, and D. Gupta, "Energy aware fault tolerant clustering with routing protocol for improved survivability in wireless sensor networks", *Computer Networks*, Vol. 212, p. 109049, 2022.

[9] M.K. Roberts, and P. Ramasamy, "Optimized hybrid routing protocol for energy-aware cluster head selection in wireless sensor networks", *Digital Signal Processing*, Vol. 130, p. 103737, 2022.

[10] L. Yuebo, Y. Haitao, L. Hongyan, and L. Qingxue, "Fuzzy clustering and routing protocol with rules tuned by improved particle swarm optimization for wireless sensor networks", *IEEE Access*, Vol. 11, pp. 128784-128800, 2023.

[11] M. Selvi, G. Kalaiarasi, S.C. Mana, R. Yogitha, and R. Padmavathy, "Energy and Security Aware Hybrid Optimal Cluster-based Routing in Wireless Sensor Network", *Wireless Personal Communications*, Vol. 137, No. 3, pp. 1395-1422, 2024.

[12] K. Yesodha, M. Krishnamurthy, K. Thangaramya, and A. Kannan, "Elliptic curve encryption-based energy-efficient secured ACO routing protocol for wireless sensor networks", *The Journal of Supercomputing*, Vol. 80, pp. 18866-18899, 2024.

[13] 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, 2022.

[14] P. Mohan, N. Subramani, Y. Alotaibi, S. Alghamdi, O.I. Khalaf, and S. Ulaganathan, "Improved metaheuristics-based clustering with multihop routing protocol for underwater wireless sensor networks", *Sensors*, Vol. 22, No. 4, p. 1618, 2022.

[15] G. Santhosh, and K.V. Prasad, "Energy optimization routing for hierarchical cluster based WSN using artificial bee colony", *Measurement: Sensors*, Vol. 29, p. 100848, 2023.

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

of Information Security, Vol. 23, pp. 199-223, 2024.

[17] 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, 2024.

[18] B. Kranthikumar, and R.L. Velusamy, "Trust aware secured energy efficient fuzzy clustering-based protocol in wireless sensor networks", *Soft Computing*, 2023.

[19] U.S.D. Rajkumar, P. Shanmugaraja, K. Arunkumar, R. Sathiyaraj, and P. Manivannan, "A HSEERP—Hierarchical secured energy efficient routing protocol for wireless sensor networks", *Peer-to-Peer Networking and Applications*, Vol. 17, No. 1, pp. 163-175, 2024.

[20] K. Biswas, V. Muthukkumarasamy, M.J.M. Chowdhury, X.W. Wu, and K. Singh, "A multipath routing protocol for secure energy efficient communication in Wireless Sensor Networks", *Computer Networks*, Vol. 232, p. 109842, 2023.

[21] N. Malisetti, and V.K. Pamula, "Energy efficient cluster-based routing for wireless sensor networks using moth levy adopted artificial electric field algorithm and customized grey wolf optimization algorithm", *Microprocessors and Microsystems*, Vol. 93, p.104593, 2022.

[22] 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.

[23] S. Ekinci, and D. Izci, "Enhancing IIR system identification: Harnessing the synergy of gazelle optimization and simulated annealing algorithms", *e-Prime-Advances in Electrical Engineering, Electronics and Energy*, Vol. 5, p. 100225, 2023.