Received: June 13, 2021. Revised: August 25, 2021.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A GOA Based Secure Routing Algorithm for Improving Packet Delivery and Energy Efficiency in Wireless Sensor Networks

Gouramma Halidoddi[1]* Rubini Pandu[2]

[1]*Department of Computer Science and Engineering, Guru Nanak Dev Engineering College, Bidar, India*
[2]*School of Engineering and Technology, CMR University, Bengaluru, India*
* Corresponding author's Email: gouramma.16phd@cmr.edu.in

Abstract: Wireless Sensor Networks (WSNs) attain much attention in different areas due to their self-configurability, easy maintenance and scalability feature. WSN is configured with more nodes to transfer the data inside the network. The sensor networks are usually characterized based on low bandwidth, limited energy, limited power supplies and small size memory, which leads to demand for the environment to provide security. Recently, the objective is to accomplish network security with low energy utilization is a challenging task in WSN. In this paper, an appropriated node selection and secure route path generation are achieved by using Grasshopper Optimization Algorithm (GOA) and Elliptic Curve Cryptographic and Diffie Hellman (ECCDH) based key exchange algorithm. The main aim of using the GOA-ECCDH method is to select the optimal route path with minimum energy consumption and improving the network lifespan in WSN. The performances of the GOA-ECCDH method are evaluated and compared to the existing Secure and Energy-aware Heuristic-based Routing (SEHR) method and Secure Routing Protocol based on Multi-Objective Ant-colony-algorithm (SRPMA) method in terms of packet delivery ratio, average energy consumption, packet loss rate, and routing load. The packet loss rate of the GOA-ECCDH method is 7.2% for the network with 8 black hole nodes, which is lesser when compared to the SEHR method and SRPMA method.

Keywords: Diffie-hellman key exchange, Energy consumption, Elliptic curve cryptography, Grasshopper optimization algorithm, Network lifespan, Wireless sensor network.

1. Introduction

WSNs are composed of a large number of smart sensor nodes, which are of strictly limited power, capabilities of computation, storage, and communication. Recently, WSNs have been widely used in many fields such as wild animal monitoring, military surveillance, target tracking, forest fire detection, and industry security. [1]. The WSN is a self-organization network with numerous sensor nodes, which determine the life span of the network [2, 3]. The sensor nodes are denoted as hubs and observed physical data such as relative humidity, pressure, temperature, etc., [4] where the sensing data was forward to the Base Station (BS), which is acts as a sink. The sensor node consists of four main units' transceiver, power unit, sensor, and processor [5, 6]. Energy is the main constrain while designing the WSN due to its battery-powered sensor nodes. [7, 8].

Security is one of the essential requirements in WSN. Generally, WSN is vulnerable to various kinds of threats [9-11]. The several attacks in WSN are Sybil attacks, wormhole attacks, black hole attacks, and hello flood attacks [12, 13]. The WSN has some security goals such as primary and secondary. The primary goal includes confidentiality, integrity, and authentication and the secondary goal includes data freshness, self-organization, secure localization, and self-organization [14, 15]. The encryption has done using three keys: such as hash, private and public keys. The public key (asymmetric) affords the similar key encryption and decryption whereas private key (symmetric) afford different key for encryption and decryption. The authorized operator has the key to access the data where the unauthorized operator not able to access the data. The data or information was transmitted securely in WSN using the encryption key, [16]. The major critical issue for many other existing techniques is to improve the energy efficiency for WSN with timely delivered data [17]. Hence, this paper proposed a secured route path and key exchange method based on GOA-ECCDH. Furthermore, the main contribution of this research work by using the GOA-ECCDH method is given as follows.

- In GOA-ECCDH, the selection of route path is considered using four fitness function values like trust values, residual energy of node, distance from a node to BS, and node degree.
- Next, ECCDH is used to authorize the node path in the network communication.
- Therefore, the route path generation and key exchange process are used to minimize the packet loss rate to increase the packet delivery ratio and less energy consumption which results in a better network lifespan.

The structure of this research paper is organized as follows. Section 2 describes the outline of the related work. Section 3 discussed about the proposed approach of the GOA-ECCDH method. Section 4 describes the experimental simulation and results. And the conclusion of the paper is given in Section 5.

2. Related work

Khalid Haseeb [18] developed a SEHR protocol for WSN to identify and avoid compromising data with systematic performance. In SEHR protocol, the information was more authentic and secure among each data packets depending on the previous encryption data packets. The SHER protocols were accomplished by a secure routing based on counter mode encryption while using the secret key function. Moreover, the protocol affords data security which depends upon random features of the counter mode encrypt algorithm, simple and lightweight. However, the integrity of the link was overlooked in the routing decision and it lacks security consideration.

Elhoseny and Yuan [19] utilized an Energy Efficient encryption method to secure dynamic in WSN. The developed method influences the Elliptic Curve Cryptographic (ECC) algorithm to produce binary strings for every sensor node to combine with the distance between the Cluster Head (CH), round index, and node ID for an exclusive 176-bit encryption operation. In this work, the data encryption and decryption are protected using three simple operations like OR, substitution, and permutation operation. Moreover, these three operations make encryption more efficient and most prominent. This developed model prevented the network from some attacks including selective forwarding attack, HEELO flood attack, and brute-force attack. However, the developed model required more energy that connects directly to the BS.

Hosam [20] implemented to detect the wormhole attack in WSN using a centralized routing protocol. The developed model minimizes the energy utilization to identify the wormhole attack by a lightweight multi-hop routing protocol. The basis of the Medium Access Control (MAC) centralized routing protocol (MCRP) depends on a single BS, which has a limitless amount of energy supply for energy nodes. The process of creating a route path from a source node to sink was improved to facilitate network management using the MCRP base station. However, the performance of LEACH and LEACH-C was negatively affected that increases the number of nodes.

Wateen [21] developed energy preserve secure techniques in Ad-hoc On-demand Distance Vector (AODV) protocol to detect the wormhole attack in WSN. The developed method presented wormhole detection with energy-efficient in two stages. The two stages of wormhole detection are based on the connection between two nodes or adjacent information. In the first stage, the sensor nodes are applied on the selected path in the transmission. In the second stage, the stage passed was relieved by the protocol to check the later stage. The developed method was achieved 100% accuracy to detect the wormhole attack with the end-to-end delay that is more efficient in packet delivery ratio. However, the developed method focused on throughput.

Min Wei [22] implemented the SRPMA for WSN. The developed method was mainly considered as two objective functions. The first objective function was considered as the average residual energy of the routing path, which is utilized to minimize the energy utilization. The second objective function was considered as the typical trust value of the routing path, which ensures the route nodes being trusted. The SRPMA method achieved better performance against blackhole attacks in WSN. However, the SRPMA method consumes more time to predict the energy consumption level in the network.

3. GOA-ECCDH method

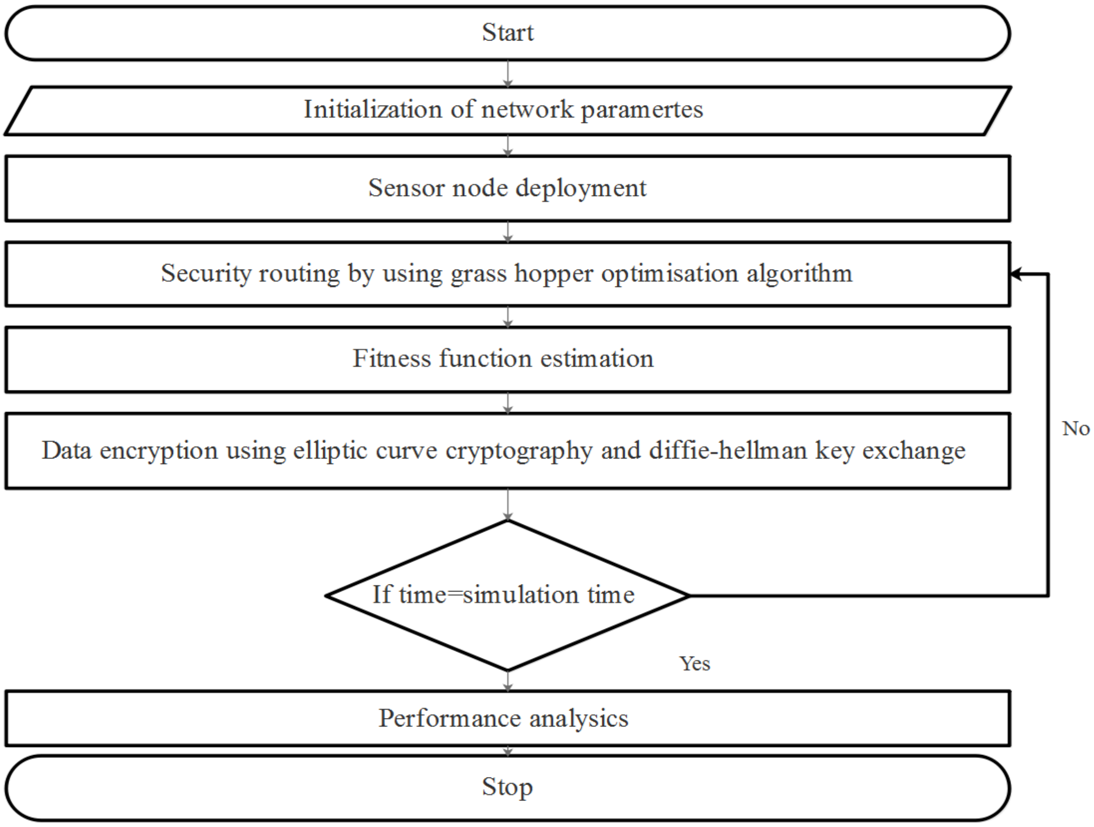
Start
Initialization of network paramertes
Sensor node deployment
Security routing by using grass hopper optimisation algorithm
Fitness function estimation
Data encryption using elliptic curve cryptography and diffie-hellman key exchange
If time=simulation time
No
Yes
Performance analysics
Stop

Figure. 1 Flowchart of the GOA-ECCDH method

The proposed GOA-ECCDH method has two main phases such as node selection and routing path generation. In the node selection process, the optimal node from the network is selected by using a Grasshopper Optimization Algorithm (GOA). Additionally, the routing paths are selected by various fitness functions like trust values, residual energy of node, the distance between a node to BS, and node degree. The main objective of the GOA-ECCDH method is to design energy efficiency in WSN to improve the network lifetime. The flowchart of the GOA-ECCDH method is shown in Fig. 1.

3.1 Sensor node deployment

Initially, the sensor node is randomly deployed in the network area. The routing path is identified using a grasshopper optimization algorithm of avoiding the malicious node while generated the secure routing path. Next, the encryption and decryption algorithm is used to transfer the secure data in network medium.

3.2 Secure routing using a Grasshopper optimization algorithm

Overview of the grasshopper algorithm:

GOA is the latest swarm algorithm with the population-based algorithm. Food source searching is the important attribute of the grasshopper swarms, which is considered in GOA. Therefore, the food searching process is divided into double categories such as exploration and exploitation. In exploration, the search agent encourages to move sharply, while they tend to travel locally during exploitation. The grasshopper natural is performed in these two categories such as exploration and exploitation. The GOA imitates the behavior of swarm grasshopper and social interaction. Moreover, the mathematical model is applied to stimulate the swarming behavior of the grasshopper which is described as follows: Each grasshopper position in the swarm is based on three forces. Where the three forces are expressed in the given mathematical Eq. (1):

$$X_i = S_i + G_i + A_i \tag{1}$$

where, X_i represents the location of the i^{th} grasshopper, S_i represents the social interaction, G_i represents the gravity of the i^{th} grasshopper, and A_i represents the wind advection.

The social interaction force between each grasshopper and other grasshopper is defined in Eq. (2).

$$S_i = \sum_{\substack{j=1 \\ j \neq i}}^{N} s(dij)\,\widehat{dij} \qquad (2)$$

Where, the distance among the i^{th} and j^{th} grasshopper is defined as dij, where, S is a function that represents a strength of the social force where it is calculated as $d_{ij} = |x_j - x_i|$, the,$\widehat{dij} = \frac{x_j - x_i}{d_{ij}}$ is a unit vector between i^{th} grasshopper to the j^{th} grasshopper.

The two social forces between the grasshopper such as repulsion and attraction are defined in Eq. (3).

$$S(r) = fe^{-r/l} - e^{-r} \qquad (3)$$

Where the intensity of attraction is denoted as f, and the attractive length scale is denoted as L.

The G_i element from Eq. (1) are identified in Eq. (4).

$$G_i = -g\widehat{e_g} \qquad (4)$$

Where, the gravitational force is denoted as G_i and center of earth unity vector is denoted as $\widehat{e_g}$.

The A_i element in Eq. (1) is identified in Eq. (5).

$$A_i = u\widehat{e_w} \qquad (5)$$

Where the drift constant is denoted as u and the wind direction of the unit vector is denoted as $\widehat{e_w}$.

The nymph grasshopper has no wings, so the movements are connected with wind direction by Substituting si, G_i and A_i in Eq. (1), the position of the grasshopper can be computed by using Eq. (6).

$$X_i = \sum_{\substack{J=1 \\ J \neq i}}^{N} s(|X_j - X_i|)\frac{X_j - X_i}{d_{ij}} - g\widehat{e_g} + u\widehat{e_w} \qquad (6)$$

The above equation is altered as Eq. (7) to solve the optimization problem.

$$X_i^d = c\left(\sum_{\substack{j=1 \\ j \neq i}}^{N} c\frac{ub_d - lb_d}{2} s(|X_j^d - X_i^d|)\frac{X_j - X_i}{d_{ij}}\right) + \widehat{T_d} \qquad (7)$$

Where the upper bound in the dth dimension is denoted as ub_d , the lower bound in the dth dimension is denoted as lb_d and the target value in the dth dimension is denoted as $\widehat{T_d}$. The coefficient that decreased is denoted as c and it is responsible for decreasing comfort zone, attraction zone and repulsion zone.

The coefficient c is proportional to some iteration to equity of exploration and exploitation in the grasshopper optimization algorithm, which is computed by using Eq. (8).

$$c = cmax - l\frac{cmax - cmin}{L} \qquad (8)$$

Where the maximum value is denoted as $cmax$, the minimum value is denoted as cmin ,the current iteration is denoted as l and the maximum amount of iteration is denoted as L.

3.2.1. Routing path generation using grasshopper algorithm

The routing path is created by considering the four various fitness functions like trust computation, the distance between the node to BS, residual energy of the node, and node degree. A detailed explanation is given as follows.

3.2.2. Representation of grasshopper swarm

In the representation stage, each grasshopper is represented as nodes. The dimension of each grasshopper in the routing is equal to the amount of the CHs in the network.

3.2.3. Grasshopper initialization

The dimension of each grasshopper is equal to the number of nodes. Let $x^i = x_1^i, x_2^i \dots\dots. x_j^i$, is considered as the ith grasshopper. Where j is denoted as a dimension that is similar to the number of nodes. The position of each grasshopper is x_j^i,$1 \leq a \leq j$ so that defines the next hop of the N_j towards the BS.

3.3 Formulation of fitness function for grasshopper algorithm

In the grasshopper algorithm, there are four types of fitness functions such as trust computation, the distance between the node to BS, residual energy of the node, and node degree. These four fitness functions are considered to choose a suitable path from a node to BS. Then these multiple objective functions are changed into a single objective function with the help of weighted sum approach as follows;

3.3.1. Computation of Trust

In the proposed method, the trust of an individual node is calculated and select an optimal path to secure data transmission by utilizing the grasshopper algorithm. The trust model of the node is computed by using Eq. (9).

$$Z_1 = T_{ij}^{direct} + T_{ij}^{indirect} + T_{ij}^{recent} + T_{ij}^{bytes} \quad (9)$$

The trust model computation is performed by using the Eq. (9). The sub-trust values used for the calculation of individual node trust are direct trust T_{ij}^{direct}, indirect trust $T_{ij}^{indirect}$, recent trust T_{ij}^{recent} and trust based on data bytes T_{ij}^{bytes}. The difference in the actual and estimation time is used in direct trust. The calculation of the direct trust is based on the witness factor that contributes much to increase the nodal trust. The calculation of indirect trust using a recommendation is received from a neighbouring agent which specific the trustworthiness of the node. The recent trust combines both the direct trust and the indirect trust that reflects the present experience and behaviour of the nodes. Additionally, the robustness of the routing improves through the trust factor. The trust factor is relying on the total number of bytes sent from the sensor node and the total amount of data bytes received via the destination node. The following Eqs. (10) to (13) represents direct trust, indirect trust, recent trust and trust based on data bytes respectively.

$$T_{ij}^{direct}(t) = \frac{1}{3}\left[T_{ij}^{direct}(t-1) - \left[\frac{T^{key} - E^{key}}{T^{key}}\right] + \omega\right] \quad (10)$$

Where the appropriated time required to send key is denoted as T^{key}, the witness factor of the jth destination is denoted as ω and the expecting time to receive the key is denoted as E^{key}.

$$T_{ij}^{indirect}(t) = \frac{1}{N}\sum_{i=1}^{N} T_{i,x}^{indirect}(x) \quad (11)$$

where the total number of the i node is denoted as N.

$$T_{ij}^{recent}(t) = \alpha \times T_{i.j}^{direct}(t) + (1-\alpha) \times T_{i,j}^{indirect}(t) \quad (12)$$

Where the weight of the trust is denoted as α

$$T_{i,j}^{\partial} = \frac{1}{2} \times \left[\frac{\partial_{i,j}^{i}}{d} + \frac{\partial_{i,j}^{j}}{d}\right] \quad (13)$$

The source node is used to forward the data bytes is denoted as $\partial_{i,j}^{i}$, the data byte received in the destination node is denoted as $\partial_{i,j}^{j}$ and d is denoted as the sending and receiving data packets are limited.

3.3.2. Residual energy of the node

In the stage of data transmission, the nodes choose the nearest next-hop to transmit the data from the source to the BS. i.e. proceed data from its node members after aggregation. Hence, the next-hop with high residual energy is the most desired choice. The residual energy Z_2 in the fitness function is presented in Eq. (14).

$$Z_2 = \sum_{i=1}^{m} E_{Ni} \quad (14)$$

Where the residual energy of the node in the network is denoted as E_{Ni}.

3.3.3. Distance calculation

The Euclidean distance is referred to as the distance between the node to the next-hop and the next-hop to the BS. Here the transmission distance is used to determine the energy consumption. If the transmission distance is minimum, it required less amount of energy. Hence, it minimizes both distances and increases the network lifetime. The distance Z_3 in fitness function is convey in Eq. (15)

$$Z_3 = \frac{1}{\sum_{i=1}^{m} dis(Ni,NH) + dis(NH,BS)} \quad (15)$$

3.3.4. Node degree

The node degree is the significant factor in next-hop selection. If the next- hop is chosen in low node degree, then the performance of the node lasts for a long duration and received low data from its member, so the next –hop mostly preferred low node degree. The node degree Z_4 in the fitness function is given in Eq. (16).

$$Z_4 = \frac{1}{\sum_{i=1}^{m} I_i} \quad (16)$$

Above-mentioned functions have dissimilar range value, so it is changed into same normalized function value, which is applied and denoted in Eq. (13). Further, all the Above-mentioned multiple objective functions are changed into a single objective function by utilizing the weighted–sum approach in Eq. (17). Here, the weights combined with each objective function is denoted as β_1, β_2, β_3 and β_4.

$$\text{Fitness function} = \beta_1(Z_1) + \beta_2(Z_2) + \beta_3(Z_3) + \beta_4(Z_4) \tag{17}$$

Where, $\sum_{i=1}^{3} \beta_i = 1, \beta_i \in (0,1)$.

3.4 Elliptic curve cryptography and diffie-hellman key exchange algorithm

ECCDH methods are executed in cryptography on the public keys which depends upon elliptic curve structure over the limited number of fields. The ECC gives equivalent security to smaller key values where the public keys and private keys are combined to utilize ECC methods, which makes the encryption data more secure. These keys were help to achieve the encryption and decryption process. After choosing the key value of the sender, the process of key exchange takes place to secure the data. For the key exchange process, the Diffie-hellman key exchange is utilized widely in the security protocols to protect information. The two users are agreed to exchange the cryptographic keys through public communication where it is used for a key agreement, not for encryption and decryption. The purpose of the algorithm is strongly secured in the communication between two users. By using the grasshopper protocol, the trust mechanism is performed. In key management, every node keep holds the public key of neighbor nodes and performs only as a router, which reduces the necessity of a centralized method of key management. Even-though, the requirement of every storage of nodes, the public key is decreased which reduced the overhead of storage on every node. Finally, all the encrypted data are sent back to the base with the key management process. Moreover, it is based on a mathematical principle where the ECC algorithm exposes key generation, encryption, and decryption, which is, characterized in step by step process.

Step 1: Global public elements

1. First, select an elliptic curve $E_q(a,b)$ with parameters a, b and q, where q is denoted as a prime number or an integer of the form 2^m.
2. Select G which is denoted as a global point on the elliptic curve whose order is a large value of n.

Step 2: Key generation of user A

1. Choose the private key, N_A is mentioned in Eq. (18);

where,

$$N_A < n \tag{18}$$

Where, n is denoted maximum value in the curve.

1. Compute public key,P_A is mentioned in Eq. (19).

$$P_A = N_A \times G \tag{19}$$

Step 3: Key generation of user B

1. Selects private key, N_B is mentioned in Eq. (20);

where

$$N_A = n \tag{20}$$

2. Compute public key,P_B is mentioned in Eq. (21)

$$P_B = N_B \times G \tag{21}$$

Step 4: Computation of secret key by user A

By combining, the Eqs. (18) and (21) to get the user secret key is represented in Eq. (22).

$$S_K = N_A \times P_B \tag{22}$$

Where, S_K is denoted as a secret key, P_B is denoted as a public key of user B.

Step 5: Computation of secret key by user B

Combining, the Eqs. (20) and (19) to get user B secret key is represented in Eq. (23).

$$S_K = N_B \times P_A \tag{23}$$

Where, P_A is denoted as a public key of user A.

Step 6: Encryption by user A using public key of user B

1. User A selects a message P_m and K is denoted random positive integer and $1 < K < q$.
2. The ciphertext, $C_m = K \times GP_m + K \times P_B$, this text is sent to the receiver. (24)

The ciphertext is mentioned in Eq. (24). Where, P_m is denoted as plain text and C_m is denoted as ciphertext.

Step 7: Decryption by user B using own private key

plain text =$(P_m + K \times P_B) - (K \times N_B \times G)$

Finally,

$$pt = P_m \tag{25}$$

The plain text equation is given in Eq. (25). Here, the coordination of C_m is multiplied with user B's private key i.e. N_B , which turns to be-comes

Table 1. Specification parameters

Parameters	Values
Network interface type	Wireless phy
Communication radius	250mm
Number of connections	20
Number malicious nodes	10
Mac protocol	Mac/802.11
Antenna pattern	Omni antenna
Wireless propagation protocol	Two ray ground
Initial energy	50J
Queue type	Pri Queue
Speed of the data flow	448kbits/s
Size of packets	210Byte
Simulation time	100s

identical to the user B public key. finally, the subtraction of results are coordinated with the second coordination of the ciphertext C_m, to get dropped and only P_m gets left. Hence, the overall system discussed the proper routing path and key exchange is achieved using GOA-ECCDH algorithm in WSN which is improves the security to reduce the loss. Moreover, the performance analysis and efficient performance of the proposed GOA-ECCGH method are calculated in Section 4.

4. Result and discussions

In this section, the network simulator 2.35 platform is used to simulate the result where the 100 nodes are randomly arranged in the area of 1200m × 1200m to simulate GOA-ECCDH. The various number of nodes is presented as a malignant node, to simulate a black hole attack. The sink node's energy is limitless and the starter energy of every sensor node is steady. The simulation results and parameter settings of nodes are shown in Table 1.

4.1 Performance evaluation

The simulation results of the GOA-ECCDH method, SRPMA method [22] and SEHR method [18] are generated by using aforementioned parameter settings. The evaluation of the GOA-ECCDH method's performance is calculated using packet delivery ratio, packet loss rate, routing load, and average energy consumption.

4.1.1. Packet delivery ratio

Packet Delivery Ratio (PDR) is characterized as the aggregate sum of packets received at the destination is partitioned by the aggregate sum of packets sent by the source node. The mathematical form of PDR is given in Eq. (26).

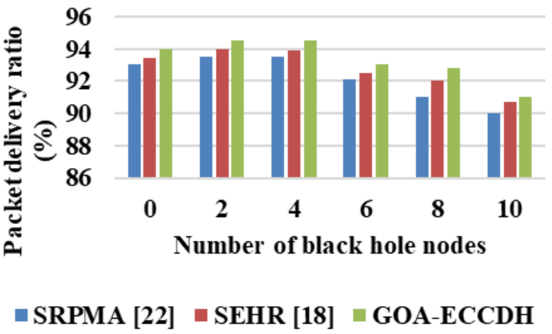

Figure. 2 Packet delivery ratio

$$PDR = \frac{\sum_{i=1}^{n} X_i}{\sum_{i=1}^{n} Y_i} \times 100\% \tag{26}$$

where, X is denoted as some packets received, Y is denoted as some packets send, i is denoted as a number of the destination node and n is denoted as the amount of source nodes. Fig 2. Illustrates the packet delivery ratio of comparison between GOA-ECCDH algorithm, SEHR method [18] and SRPMA algorithm [22]. Here, the GOA-ECCDH algorithm gives a better performance when compared to the SEHR method [18] and SRPMA algorithm [22]. The GOA-ECCDH algorithm achieved secure routing by considering the trust behavior value. Hence, the GOA-ECCDH algorithm increases the packet delivery ratio.

4.1.2. Packet loss rate

Packet Loss Rate (PLR) is defined as the total number of packet dropped is divided by the total number of packet send by source node ×100% is given in Eq. (27).

$$PLR = \frac{\sum_{i=1}^{n} Y_i - \sum_{i=1}^{n} X_i}{\sum_{i=1}^{n} Y_i} \times 100\% \tag{27}$$

Where, X is denoted as the number of packets received, Y is denoted as the number of packets send, i is denoted as the number of the destination node and n is denoted as the number of source nodes.

Fig. 3 shows the packet loss rate which is compared between the GOA-ECCDH algorithm, SEHR method [18] and SRPMA algorithm [22]. Here, the packet loss rate in the GOA-ECCDH algorithm is lower when compared to the SEHR method [18] and SRPMA algorithm [22]. Due to the malicious nodes present in the network, the data packet loss occurs during data transmission through the routing path. Hence, the packet loss rate of the GOA-ECCDH algorithm is minimized by considering the trust value in the fitness function.

Received: June 13, 2021. Revised: August 25, 2021.

Moreover, the trust values act as the optimization objectives which means to select the higher trust value nodes and help to identify the normal node to prevent the malicious node. Next, the GOA-ECCDH algorithm is mainly considered as energy and distance which is used to eliminate a failure node in the routing path. Therefore, it minimized the packet loss in the network.

4.1.3. Routing load

Routing load is explained as the ratio of the amount of routing message created by the node to the number of data packets delivered successfully to all destination nodes, which is expressed in Eq. (28).

$$Routing\ load = \frac{Y}{X} \tag{28}$$

Fig. 4 shows the routing load of comparison between the GOA-ECCDH algorithm, SEHR method [18] and SRPMA algorithm [22]. Here, the routing load in GOA-ECCDH has a lower range when compared to the SEHR method [18] and SRPMA algorithm [22]. Hence, the GOA-ECCDH algorithm has a smaller routing load to forward more packets that are delivered successfully in destination load, which is a reduced routing load in the GOA-ECCDH algorithm.

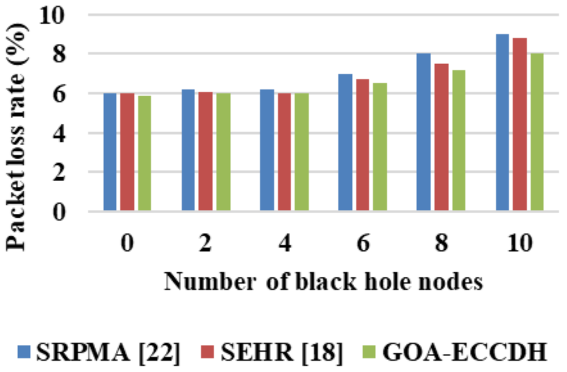

Figure. 3 Packet loss rate comparison

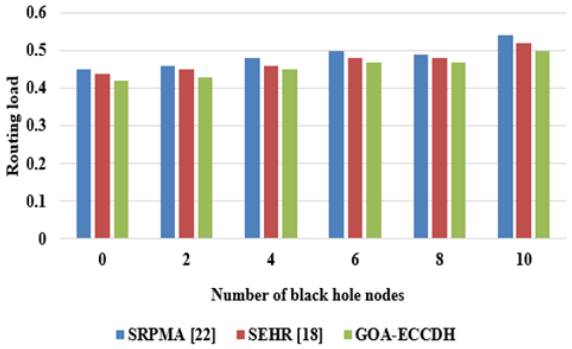

Figure. 4 Routing load comparison

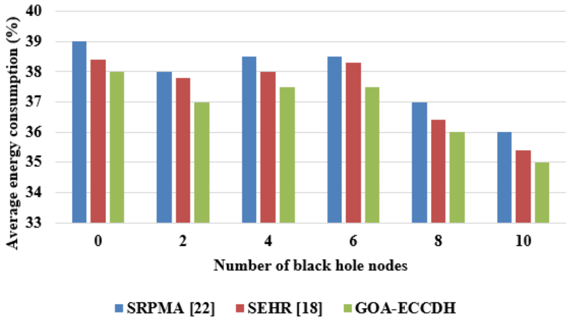

Figure. 5 Average energy consumption

4.1.4. Average energy consumption

Average energy consumption is measured between the preliminary energy level of the node and the ending energy level that is left in each node is mentioned in Eq. (29).

$$E_a = \frac{\sum_{K=1}^{n}[E_{ik} - E_{fk}]}{N} \tag{29}$$

Where the $n = N$ is an important metric among the lifespan of the network which is inversely proportional to the energy level of the network. The initial energy level of the node is denoted as E_i, the number of nodes in the simulation is denoted as N and the final energy level left in a node is denoted as E_f.

Table 2. Comparison of SEHR [18], SRPMA [22] and GOA-ECCDH methods in terms of packet delivery ratio and packet loss rate

Number of black hole nodes	PDR (%)			PLR (%)		
	SRPMA [22]	SEHR [18]	GOA-ECCDH	SRPMA [22]	SEHR [18]	GOA-ECCDH
0	93	93.4	94	6	6	5.9
2	93.5	94	94.5	6.2	6.1	6
4	93.5	93.9	94.5	6.2	6	6
6	92.1	92.5	93	7	6.7	6.5
8	91	92	92.8	8	7.5	7.2
10	90	90.7	91	9	8.8	8

Table 3. Comparison of SEHR [18], SRPMA [22] and ECCDH methods in terms of routing load and average energy consumption (J)

Number of black hole nodes	**Routing load**			**Average energy consumption (%)**		
	SRPMA [22]	**SEHR [18]**	**GOA-ECCDH**	**SRPMA [22]**	**SEHR [18]**	**GOA-ECCDH**
0	0.45	0.44	0.42	39	38.4	38
2	0.46	0.45	0.43	38	37.8	37
4	0.48	0.46	0.45	38.5	38	37.5
6	0.5	0.48	0.47	38.5	38.3	37.5
8	0.49	0.48	0.47	37	36.4	36
10	0.54	0.52	0.5	36	35.4	35

The average energy utilization is compared between the GOA-ECCDH algorithm, SEHR method [18] and SRPMA algorithm [22] is given in Fig.5. The GOA-ECCDH algorithm gives a better performance in average energy consumption when compared to the SEHR method [18] and SRPMA algorithm [22]. The GOA-ECCDH algorithm is mainly considered as the distance, which is helpful to identify the shortest path, and reduced the energy consumption. Table 2 shows the comparison of SEHR [18], SRPMA [22] and GOA-ECCDH methods in terms of packet delivery ratio and packet loss rate.

Table 3 provides the comparison results between the SEHR [18], SRPMA [22] and ECCDH methods in terms of routing load and average energy consumption (J). The above Fig. 2 to 5 indicates the packet delivery ratio, packet loss rate, average energy consumption, and routing load to the proposed GOA-ECCDH method, SEHR method [18] and SRPMA method [22] with attacks. While analysing the above graphs that distinctly shows that the proposed GOA-ECCDH method achieved higher security with better performance when compared to the existing SEHR method [18] and SRPMA method [22].

5. Conclusion

In WSN, identification of the secure path and routing generation is a challenging task due to the lack of security and limited energy. In this paper, a GOA is utilized which is used to detect the secure path in the network. Next, the ECCDH method is proposed which is used to secure the data transmission path. In ECCDH, the Diffie hellman key exchange is considered that makes the information more secure. The key exchange method is utilized in the ECCDH algorithm, which is used to achieve security and energy efficiency in this paper. Moreover, the packet delivery ratio is increased in the proposed GOA-ECCDH method by considering trust value in the fitness function. The energy consumption of the proposed GOA-ECCDH method is minimized by using the distance fitness function. The simulation results showed that the ECCDH method achieved better performance in routing load, energy consumption, and packet delivery ratio when compared to the SEHR method and SRPMA method. The packet loss rate of the GOA-ECCDH method is 7.2% for the network with 8 black hole nodes, it is less when compared to the SEHR method and SRPMA method. In the future, the energy-efficiency can be improved using an optimization algorithm in WSN.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

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

References

[1] N. Wang and J. Li, “Shortest path routing with risk control for compromised wireless sensor networks”, *IEEE Access*, Vol. 7, pp. 19303-19311, 2019.

[2] V. Srivastava, S. Tripathi, and K. Singh, “Energy-efficient optimized rate based congestion control routing in wireless sensor network”, *Journal of Ambient Intelligence and Humanized Computing*, Vol. 11, No. 3, pp. 1325-1338, 2020.

[3] L. Li and D. Li, “An energy-balanced routing protocol for a wireless sensor network”, *Journal of Sensors*, Vol. 2018, 2018.

[4] S. Karthick, “TDP: A novel secure and energy aware routing protocol for wireless sensor networks”, *International Journal of Intelligent*

Engineering and Systems, Vol. 11, No. 2, pp. 76-84, 2018.

[5] R. Baskar, K. Raja, C. Joseph, and M. Reji, "Sinkhole Attack in Wireless Sensor Networks-Performance Analysis and Detection Methods", *Indian Journal of Science and Technology*, Vol. 10, No. 12, pp. 1-8, 2018.

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

[7] A. Sarkar and T. S. Murugan, "Cluster head selection for energy efficient and delay-less routing in wireless sensor network", *Wireless Networks*, Vol. 25, No. 1, pp. 303-320, 2018.

[8] A. S. Toor and A. K. Jain, "Energy aware cluster based multi-hop energy efficient routing protocol using multiple mobile nodes (MEACBM) in wireless sensor networks", *AEU-International Journal of Electronics and Communications*, Vol. 102, pp. 41-53, 2019.

[9] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks", *IEEE Transactions on Industrial Electronics*, Vol. 63, No. 11, pp. 7124-7132, 2016.

[10] M. Sabet and H. R. Naji, "A decentralized energy efficient hierarchical cluster-based routing algorithm for wireless sensor networks", *AEU-International Journal of Electronics and Communications,* Vol. 69, No. 5, pp. 790-799, 2015.

[11] D. N. Biradar and T. S. Vishanath, "Mitigation of Selective Forwarding attacks in Wireless Sensor Network", *International Journal of Engineering and Advanced Technology*, Vol. 8, No. 6, pp. 4354-4358, 2019.

[12] D. N. Biradar and T. S. Vishanath, "Secured Data Transmission and Malicious Node Detection in Wireless Sensor Network", *International Journal of Engineering and Advanced Technology*, Vol. 8, No. 6, pp. 1062-1069, 2019.

[13] X. Luo, Y. Chen, M. Li, Q. Luo, K. Xue, S. Liu, and L. Chen, "CREDND: A novel secure neighbor discovery algorithm for wormhole attack", *IEEE Access*, Vol. 7, pp. 18194-18205, 2019.

[14] H. A. Babaeer and S. A. A. Ahmadi, "Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking", *IEEE Access*, Vol. 8, pp. 92098-92109, 2020.

[15] J. Choi, J. Bang, L. Kim, M. Ahn, and T. Kwon, "Location-based key management strong against insider threats in wireless sensor networks", *IEEE Systems Journal*, Vol. 11, No. 2, pp. 494-502, 2018.

[16] X. Liu, J. Yu, F. Li, W. Lv, Y. Wang, and X. Cheng, "Data aggregation in wireless sensor networks: from the perspective of security", *IEEE Internet of Things Journal*, Vol. 7, No. 7, pp. 6495-6513, 2019.

[17] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal, and A. Arshad, "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks", *Journal of Ambient Intelligence and Humanized Computing,* Vol. 12, No. 1, pp. 547-566, 2021.

[18] K. Haseeb, K. M. Almustafa, Z. Jan, T. Saba, and U. Tariq, "Secure and energy-aware heuristic routing protocol for wireless sensor network", *IEEE Access*, Vol. 8, pp. 163962-163974, 2020.

[19] M. Elhoseny, X. Yuan, H. K. E. Minir, and A. M. Riad, "An energy efficient encryption method for secure dynamic WSN", *Security and Communication Networks*, Vol. 9, No. 13, pp. 2024-2031, 2018.

[20] O. R. Ahutu and H. E. Ocla, "Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks", *IEEE Access*, Vol. 8, pp. 63270-63282, 2020.

[21] W. A. Aliady and S. A. A. Ahmadi, "Energy preserving secure measure against wormhole attack in wireless sensor networks", *IEEE Access*, Vol. 7, pp. 84132-84141, 2018.

[22] Z. Sun, M. Wei, Z. Zhang, and G. Qu, "Secure Routing Protocol based on Multi-Objective Ant-colony-optimization for wireless sensor networks", *Applied Soft Computing*, Vol. 77, pp. 366-375, 2019.