Received: April 2, 2022. Revised: May 10, 2022.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Secure Optimized Routing and Data Transmission in Wireless Sensor Networks with Elliptic Curve Cryptography

Chada Sampath Reddy[1]* **G. Narsimha[2]**

[1]*Department of Computer Science Engineering,*
Sree Chaitanya Institute of Technological Sciences, Karimnagar, India
[2]*Department of Computer Science Engineering, JNTUH University College of Engineering, Sultanpur, India*
* Corresponding author's Email: sampath553@gmail.com

Abstract: Wireless sensor networking (WSN) is an important subject among the researchers in recent years and it is recognized as a familiar approach for upcoming applications like traffic monitoring in real time, battlefield, and eco-systems for surveillance. The network has receptive data and it is essential that the networks secure the several types of attacks like eavesdropping, capturing the node, rejection of service. Various sensor networks routing approach has been proposed to secure the networks. This work offers a secure routing scheme in WSN with deep learning approaches. Initially, trust verification is performed to select the non-malicious node, which is carried out through long short-term memory (LSTM), where the malicious nodes are removed. Secondly, data transmission is done through encrypting the data using elliptic curve cryptography (ECC) algorithm. This encrypted data is forwarded to the secured shortest paths, in which the secure shortest path is selected by dragonfly algorithm (DA) through solving the multi-objective function by incorporating the measures like distance, energy, delay, throughput, and trust. Evaluation of cost function of the proposed DA-LSTM model is correspondingly secured 22 %, 27 %, 31 %, and 18 % enriched performance than the PSO-LSTM, GWO-LSTM, WOA-LSTM, and CSA-LSTM at iteration 10th. Finally, the numerical simulations show that the suggested secure routing and data transmission in WSN is validated with other optimization algorithms and shows an advanced performance based on analysis with various performance measures by concerning with the number of sensor nodes and the maximum number of iterations.

Keywords: Secure optimized routing, Data transmission, Wireless sensor networks, Elliptic curve cryptography, Long short-term memory, Dragonfly algorithm.

1. Introduction

WSN is one of the most essential technologies used in network system. The sensor nodes present in WSN transfer the electric signals from the channel to the base station. The organization of sensor nodes in WSN is executed in ad hoc without proper engineering and planning. The WSN incorporates wireless communication, information technology, and sensor technology. The major aim of WSN is to gather the data from the monitored area and then, it converts the data into signals and the electrical signals are forwarded to the base station through wireless communication. WSN is suitable in all types of fields like medicine, military, and industries. The computing power and energy of WSN are limited and it is difficult to change the battery. The sensor nodes of WSN are out of energy in some situations, it results in changes in network topology. The presence of dead nodes in the WSN stops the functioning of the network and be paralyzed. The life span of network is maintained with energy-efficient routing protocols. The parameters of WSN measure the location, humidity, and temperature of the objects.

The challenges in WSN are trustworthiness and the localization of security. The application of telemedicine and localization suffers from security issues. The sensor nodes in WSN have limited capability of communication and energy efficiency,

Equation symbols and descriptions

S.no	Symbol	Description
1.	$\left[\mathrm{ITu}_{\mathrm{NN}_{\mathrm{nn}}}(\mathrm{No}_{\mathrm{nn}})\right]$	The indirect trust of neighbour nodes$\mathrm{NN}_{\mathrm{nn}}on\mathrm{No}_{\mathrm{nn}}$.
2.	$c(x, y) = 0$	The elliptic curve with non-singular cubic curve of two variables.
3.	$R * S$	The straight line joins points $R$and S.
4.	$R + S$	The reflection of $R * S$in the x-axis.
5.	$\mathrm{Fit} = \underset{\{\mathrm{pt}_{\mathrm{jk}}\}}{\mathrm{argmin}}(\mathrm{Obj})$	Fitness function.
6.	Eng	Residual energy
7.	$\mathrm{Eng} = \mathrm{Eng}_{\mathrm{nn}} - \left(\mathrm{eng}_{\mathrm{nn}}^{\mathrm{cs}} + \mathrm{eng}_{\mathrm{nn}}^{\mathrm{sh}}\right)$	Computation of residual energy.
8.	$\mathrm{Dis} = \sqrt{(m_u - n_v)^2 + (m_u - n_v)^2}$	The length of a line segment between the two nodes.
9.	$\mathrm{Dly} = \frac{\max \sum \mathrm{pt}_{\mathrm{jk}}}{N}$	Transmission Delay.
10.	$\max \sum \mathrm{pt}_{\mathrm{jk}}$	Data transmission from sensor node to base station.
11.	$\mathrm{Thr} = \frac{\sum(P_{\mathrm{sc}} * \mathrm{Ap}_s)}{\mathrm{tms}}$	Throughput.
12.	$\mathrm{SP}_n = -\sum_{i=1}^{K}(B_n - B_i)$	The distance among two adjacent dragonflies
13.	$\mathrm{AN}_n = \frac{\sum_{i=1}^{K} V_i}{K}$	The aligned position of the dragonflies.
14.	$\mathrm{CN}_n = \frac{\sum_{i=1}^{k} B_i}{K} - B_n$	Cohesion.

and therefore the limitations can overcome by adopting wireless sensor nodes. Security is more significant in all networks. A light weighted security scheme is necessary for the nodes of WSN. A cryptography approach moderates the issues in encryption phase which results in high energy efficiency. The electronic deceived with high energy are designed with conventional cryptography process. The secure management at base station requires steering data and encryption methods for securing the data. The sensor hubs are used to secure the networks. The multiple numbers of sensor hubs are gathered and verified in order to protect the trade information.

The symmetric key-based cryptography is an efficient method used in WSN. However, symmetric key-based cryptography model suffers from numerous problems such as low memory, low scalability, and requires key materials. Various techniques were incorporated to overcome the limitations of low energy efficiency in sensor nodes. The clustering technique is well known for WSN limitations. The lifetime of the sensor nodes is increased with optimization algorithm-based routing protocols. The ant colony optimization (ACO) algorithm is applied in solving all types of optimization problems especially in wireless routing protocols. The main advantage of this optimization algorithm is avoiding the local minima and obtaining the global optimization solution. A deep learning approach enhances the performance of WSN to estimate the energy to be produced within a time period. The locations of sensor nodes are changed due to the external and internal factors. The deep learning technique provides accurate localization and optimization. The transmitted data in WSN are secured with ECC and provide high security to the networks.

The designed framework has following contribution as given here. This proposed model aims to secure the networks from different type of attacks through a new heuristic algorithm along with deep learning strategy by adopting an encryption scheme. LSTM network is used for detecting the malicious nodes and the non-malicious nodes to ensure the trust in routing, where the detected non-malicious nodes are secured for routing whereas "malicious nodes are removed" from the network. Then, ECC is used for performing the secure routing among source to destination nodes, where the data transmission is carried out through the selected shortest path. Further, the shortest path communication is done through DA through deriving the multi-objective functions concerning to distance, energy, delay, throughput, and trust.

The remaining sections are discussed here. The existing works are discussed in section 2. The architectural view of secured routing and data

transmission in WSN is depicted in section 3. Section 4 provides the optimal shortest path data communication in WSN using DA. Section 5 shows the result visualization of offered method. At the end, the ending to the proposed model is shown in section 6.

2. Literature survey

2.1 Related works

In 2021, Rathee et al. [1] have suggested an "ACO-based Quality of Service (QoS) Aware Energy Balancing Secure Routing (QEBSR) algorithm" for securing the WSN. The enhanced heuristic algorithm has been used for determining the end-to-end delay of data transmission and proposed the trust factors on the routing path. The experimental results have confirmed that the proposed method has outperformed the other two algorithms.

In 2020, Haseeb et al. [2] have offered a routing protocol named "Secure and Energy-Aware Heuristic-Based Routing (SEHR) method for WSN" to identify and prevent the conciliation data with effective performance. Initially, the suggested protocol incorporated artificial intelligence (AI)-based heuristic model to analyze and accomplish intellectual and consistent learning framework. Then, this framework has protected the networks from opponent groups to obtain high security with low complexity. The network disconnection and link failures were reduced with route maintenance strategy.

In 2013, Ganesh et al. [3] have proposed a method for efficient and secured routing for WSN with "Signal-to-Noise Ratio (SNR)-Based Dynamic Clustering (SDC) model". In the inter clustering routing, the error recovery was adopted to avoid the end-to-end error recovery. The security of the network was accomplished by separating the malicious nodes with sink-based routing method.

In 2009, Le et al. [4] have suggested an energy efficiency control model-based ECC to conquer the issues in data transmission and secure routing, and to provide energy efficient network. With the process of simulation and analysis the results were evaluated and the proposed model has enhanced the security issues in networks and further, achieved high energy efficiency while compared to the current method.

In 2015, Senthil et al. [5] have developed an integrity method and secure authentication model to solve the reliability and security issues in WSN. The authentication was provided by shared keys. The sender and the recipient have shared the common key for authentication in the mutual authentication method. The noise corrupted signal was verified by both the sender and receiver according to the hamming weight. The integrity and authentication were improved with offline encryption models. This scheme has satisfied both the mechanism of public key encryption and digital signature in a single process.

In 2022, Halidoddi et al. [22] have suggested a "two-level security" to the data transformation with a help of WSN. A "Multi-Objective Trust-based Bat Optimization Algorithm (MOTBOA)" has introduced to employ a secure clustering and routing operation. The improved homomorphic cryptosystem (EHC) has created for the data security of the network. The effectiveness of the offered approach has validated using the diverse parameters of the network. At the end, the experimental results have confirmed that the offered approach has given accurate system performance.

In 2022, Veerabadrappa et al. [23] have offered "Multi Objective Trust Aware Hybridized Optimization (MOTAHO)" to employ a secure data transmission with the WSN. The optimization has done with the help of hybridized moth flame optimization (MFO) and chicken swarm optimization (CSO) using various different types of constraints. The suggested method has utilized for providing the security against the "Distributed Denial of Service (DDoS)" attack. At the end, the experimental findings have provided the optimal performance of the offered MOTAHO method.

In 2021, VenkataRao et al. [24] have introduced the hybrid optimization algorithm (HOA)-based secure cluster head (CH) selection for generating a routing path to secure the data transmission. The optimization has done by using the combination of the grey wolf optimization (GWO) and moth flame optimization (MFO) algorithms. The shamir secret sharing (SSS) method was utilized for providing mutual authentication among the nodes. The efficiency of the "HOA-IoT-WSN" was reviewed regarding packet loss ratio (PLR), packet delivery ratio (PDR), average "End to-End Delay (AEED)" and network overhead.

In 2021, Malligehalli et al. [25] have offered "Cost Centric Cuckoo Search Algorithm (CCCSA)" the energy and security issues in WSN. The "K-means clustering algorithm (KMC)" was utilized for employed the clustering functions. The offered method was used for selecting the adaptive cluster head (CH) among the normal nodes in the cluster. The suggested method has combined with "Ad hoc On-Demand Distance Vector (AODV)" routing

protocol. The adaptive routing path was generated using the AODV. The experimental findings have confirmed that the suggested approach has obtained advance security of the network.

In 2021, Halidoddi et al. [26] have suggested "Grasshopper Optimization Algorithm (GOA) and Elliptic Curve Cryptographic and Diffie Hellman (ECCDH)-based key exchange algorithm" for node selection and secure route path generation. The main scope of this suggested method was for selecting the accurate route path with lowest energy consumption and enhancing the system life time in WSN. The efficiency of the suggested method was validated and tested to the baseline "Secure and Energy-aware Heuristic-based Routing (SEHR) method and Secure Routing Protocol based on Multi-Objective Ant-colony-algorithm (SRPMA)" approach.

2.2 Problem statement

In WSN, when the nodes are used in "unattended and harsh" environment, the sensor nodes become damaged and defective. The consumption of energy while delivering the packets from the channel to the base station is considered as the main challenge in WSN. The adequate energy in the node causes the packet to drop while data transmissions. The features and challenges of secure routing and data transmission in WSN are illustrated in Table 1.

ACO [1] is used for end-to-end transmission of data without delay. However, it has limited storage capacity in sensor nodes that affects the efficiency. SEHR [2] advances the efficiency of system throughput and decreases the failures in networks. Moreover, the energy efficiency of the network needs to be improved. "Efficient and Secure Routing Protocol for WSN through SNR-based Dynamic Clustering (ESRPSDC)" [3] avoids the error in data transmissions and enhances the network lifespan. Moreover, it causes delay and also decreases network throughput rate. ECC [4] acts as a tool for real world function in optimizations. However, it cannot be applied in real time applications. "Secure Authentication and Integrity techniques for Randomized Secured Routing (SAIRSR)" [5] balance the system loads and it is used to avoid the path loss problems. Moreover, it causes packet loss among the networks. The data traffic issues are continuously repeated in network, because the nodes create similar data in sensing. The complexity in routing protocol can affect the performance of all wireless networks. The shortage of energy in the sensor nodes are the major challenges in WSN. Therefore, the challenges in the existing works have motivated the researchers to focus on introducing a novel secure optimized routing in WSN.

Table 1. Pros and cons of secure routing and data transmission in WSN

Author, Techniques	pros	Cons
Rathee *et al.* [1], ACO	• It is used for end to end transmission of data without delay.	• It has limited storage capacity in sensor nodes that influence the efficiency.
Haseeb *et al.* [2], SEHR	• It enhances the network throughput. • It reduces failures in networks.	• The network's energy efficiency needs to be improved.
Ganesh *et al.* [3], ESRPSDC	• It avoids errors in data transmissions. • It enhances the network lifespan.	• It causes delay and network throughput rate reduced.
Le *et al.* [4], ECC	• It acts as a tool for real world functions in optimizations.	• It cannot be applied in real time applications
Senthil *et al.* [5], SAIRSR	• It balances network loads and it is used for avoiding the path loss problems.	• It causes packet loss among the networks.

3. Architectural view of secured routing and data transmission in WSN

3.1 Developed system model

Routing is one of the most significant factors in WSN while it is dealing with data transmission among source to destination. The operation of WSNs can be considerably degraded due to the routing attacks. However, conventional security schemes like authentication and cryptography alone cannot adopt for solving some of the routing attacks. In recent years, trust mechanism is utilized for improving cooperation and security among nodes. Thus, trust-aware routing is required for avoiding the malicious nodes during routing operation by considering the evaluated trust values. "There is a need of avoiding" malicious nodes in the network as

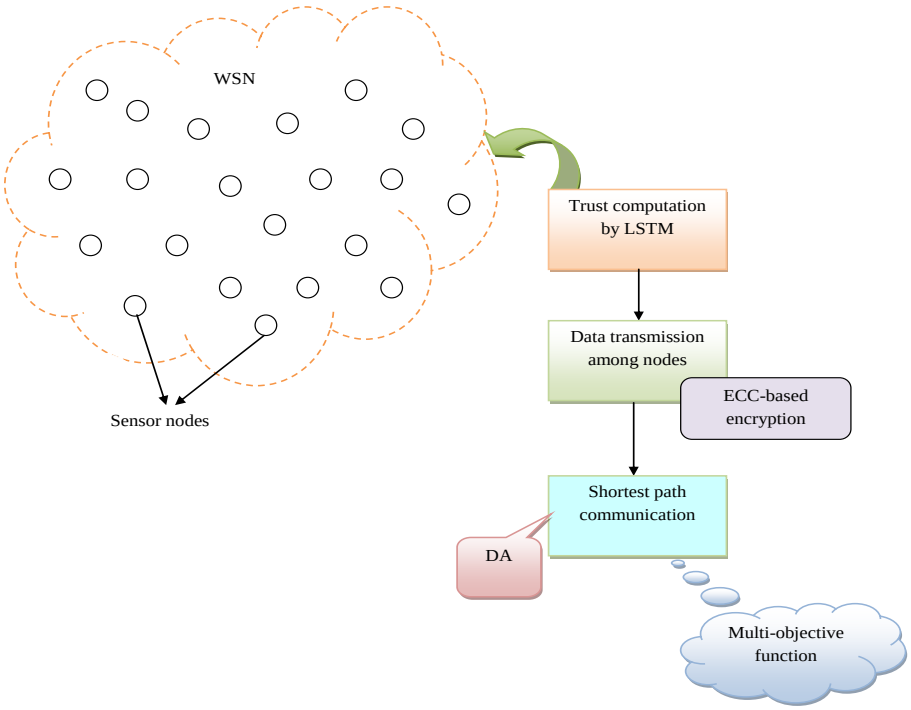


Figure. 1 Architectural representation of the designed secure "data transmission and routing" in WSN

it launches diverse attacks from the outside that must control or cripple the entire WSNs. After receiving the data, malicious nodes attract the data from other nodes, and then, it drops the received data that minimize the performance of the routing protocol. Thus, these kinds of nodes must be monitored and detected them. In recent works, various routing schemes are suggested and but, "there is no much research work on offering trust to secure routing". Hence, this work has offered a new secure optimized routing and data transmission in WSN with encryption scheme, which is diagrammatically represented in Fig. 1.

This work offers a new secure routing method in WSN with deep learning model. At first, the trust verification is performed to select and remove the malicious nodes, which are done with LSTM. Then, the data transmission is carried out with ECC algorithm by encrypting the data. Later, the encrypted data is passed through the secured shortest path. The shortest path communication is selected using DA through deriving the multi-objective functions regarding energy, distance, delay, trust, and throughput. Finally, the data is transmitted through the secured shortest path. Thus, secure data transmission is ensured by the designed model.

3.2 Trust computation by LSTM

This proposed secure routing model utilizes LSTM for computing the trust among the sensor nodes, where the non-trusted nodes will be avoided for transmission and the determined trust nodes are used for further performing secure routing.

LSTM [17] is a "specific type of recurrent neural network (RNN) architecture" that is highly preferable for learning the experiences for classifying, processing and predicting the data. This model has used LSTM for determining the trust among the nodes. It is shown here as it has used "temporal sequences and their long-range dependencies" for more accurate operational process while comparing to the traditional RNNs. LSTM is useful in converging at quicker manner, solving the vanishing and exploding grading issues of existing RNNs. thus, it has been utilized in various research fields. Generally, LSTM is consisted of several units named memory blocks, which includes "memory cells with self-connects for remembering the temporal state of the network" for offering functionalities along with multiplicative units also termed as gates, which is helpful in controlling the information flow. Here, the input gate is included in every memory block for controlling the "flow of input activations to the memory cell whereas the output flow of cell activations will be controlled by an output gate" that will be fed to a forget gate and also to the rest of the network. In addition, the "internal state of the cell is scaled by the forget gate before inserting it back to the cell as input via self recurrent connection" and so, the cells memory will be adaptively resettled or forgotten. Finally, LSTM includes peephole connects from their internal cells to the gates in the similar cell for learning accurate

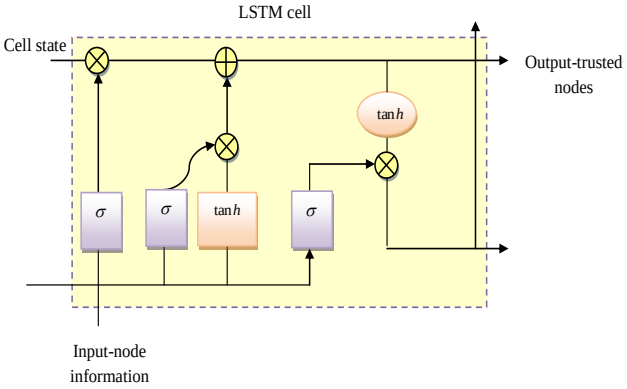


Figure. 2 Trust determination by LSTM in WSN

timing of the outcomes.

Thus, the LSTM is used for computing the trust among nodes to avoid malicious nodes in the WSN. The trust determination is specified here, where trust is explained as, the integrated characteristics of the model "for providing the security, reliability, privacy with respect to the mobility", which is termed as Tu as derived in Eq. (1).

$$\mathrm{Tu} = \sum_{\mathrm{nn}=1}^{\mathrm{NN}}\left(\sum_{\mathrm{nn}=1}^{\mathrm{NN}} \mathrm{DTu}_{\mathrm{NN}_{\mathrm{nn}}}(\mathrm{No}_{\mathrm{nn}})\right) + \sum_{\mathrm{nn}=1}^{\mathrm{NN}}\left(\sum_{\mathrm{nn}=1}^{\mathrm{NN}} \mathrm{ITu}_{\mathrm{NN}_{\mathrm{nn}}}(\mathrm{No}_{\mathrm{nn}})\right) \quad (1)$$

Here, the complete trust of node is formulated as Tu, the indirect trust of neighbour nodes $\mathrm{NN}_{\mathrm{nn}}$ on $\mathrm{No}_{\mathrm{nn}}$ is formulated by $\left[\mathrm{ITu}_{\mathrm{NN}_{\mathrm{nn}}}(\mathrm{No}_{\mathrm{nn}})\right]$, and the direct trust of neighbour nodes on $\mathrm{No}_{\mathrm{nn}}$ is equated as $\mathrm{DTu}_{\mathrm{NN}_{\mathrm{nn}}}(\mathrm{No}_{\mathrm{nn}})$. The proposed model finally determines the trust value regarding sensor nodes in the network for determining whether "the sensor node is a malicious or non-malicious one".

Therefore, the trusted nodes are utilized in the communication process. The proposed trust calculation with LSTM model is given in Fig. 2.

3.3 ECC-based data transmission between nodes

The ECC is a public key encryption method, where the smaller, faster, and efficient cryptographic keys are created. The keys are produced using the properties of elliptic curve equations. These keys are used to maintain the authentication and privacy of data. ECC [18] is applied in various mobile applications that offer privacy protection with high resource battery and low computing power. The encryption awareness of ECC helps to develop the cloud computing inside the cloud organizations. The combination of techniques is used for securing data that involves encryption, authentication and authorization techniques. In this encryption technique, the encryption key is used for decoding the encrypted files and the information using the complex algorithm. ECC secures the transmitted and received data during communication for maximizing the reliability and efficiency of each transmitted data. The data is encrypted before transmissions and initiates the communication.

The below equation defines plane algebraic curve form of elliptic curve.

$$y^2 = x^3 + \mathrm{ax} + b \quad (2)$$

The selection of private keys is done in ECC. The final computations may get incorrect results due to the selection of random values at the same time. The elliptic curve with non-singular cubic curve of two variables is in the form of $c(x, y) = 0$. The field of the elliptic curve is compiled of algebraic expressions, real, complex numbers, rational and finite field. The speed and accuracy are the main parts of the cryptography. The elliptic curve executes point operation such as point addition, point doubling and scalar multiplication that are mentioned below.

The point addition is performed by considering the straight line joins points R and S that are assumed to be selected in the elliptic curve$N$. This line joins Nwhich is known as $R * S$, which is the third point. However, the sum $R + S$is referred as the reflection of $R * S$in the x-axis, but not $R * S$itself. Assume $R(x_1, y_1)$ and $S(x_2, y_2)$ are the two points and the line form is denoted in Eq. (3).

$$y = \mathrm{tx} + f \quad (3)$$

At the same time, the two equations Eqs. (2) and (3) give the single variable equation that is explained from Eq. (4) to Eq. (6).

$$(\mathrm{tx} + f)^2 = x^3 + \mathrm{ax} + b \quad (4)$$

$$t^2x^2 + f^2 + 2\mathrm{txf} = x^3 + \mathrm{ax} + b \quad (5)$$

$$x^3 - t^2x^2 + (a - 2tf)x + b - f^2 = 0 \quad (6)$$

$$R.S = (x_3, y_3) \quad (7)$$

In Eq.(7) The point $R \cdot S$lies on the x-axis and gives the elliptic point addition values of R and S that is indicated in the Eq. (8).

$$R + S = (x_3, -y_3) \quad (8)$$

The elliptic curve is $N$and the sum $(R_1 + R_2)$ is derived as follows. The three coordinates on x-axis and y-axis are represented as R_1, $R_2$and R_3 that are

given here.

$$R_1 = (x_1, y_1) \tag{9}$$

$$R_2 = (x_2, y_2) \tag{10}$$

$$R_3 = (x_3, y_3) \tag{11}$$

$$t = \frac{(y_3 - y_1)}{(x_3 - x_1)} \tag{12}$$

The summation of the three roots is given below.

$$x_1 + x_2 + x_3 = -(-t)^2 \tag{13}$$

$$x_1 + x_2 + x_3 = t^2 \tag{14}$$

From this $x_3$can be attained in the Eq. (15).

$$x_3 = t^2 - x_1 - x_2 \tag{15}$$

The slope equation is essential to obtain y_3 that is shown in the Eqs. (16) and (17).

$$t(x_3 - x_1) = (y_3 - y_1) \tag{16}$$

$$y_3 = y_1 + t(x_3 - x_1) \tag{17}$$

The reflection point on y-axis can be computed as given in Eq. (18).

$$y_3 = -(y_1 + t(x_3 - x_1)) \tag{18}$$

The point doubling is essential to compose R and S to be equal which means by adding the values itself. The derivative can be calculated from the Eqs. (19) and (20).

$$2y\frac{\mathrm{dy}}{\mathrm{dx}} = 3x^2 + a \tag{19}$$

$$\frac{\mathrm{dy}}{\mathrm{dx}} = \frac{3x^2 + a}{2y} \tag{20}$$

The point doubling is explained in the Eqs. (21) and (22), respectively.

$$x_3 = t^2 - 2x_1 \tag{21}$$

$$y_3 = -(y_1 + t(x_3 - x_1)) \tag{22}$$

The most significant part in ECC is scalar point multiplication, which computes kR, in which the integer k is multiplied to kR and another point in the curve is obtained.

The easiest process for calculating kR is the binary method that works with the help of the binary representation as shown in Eq. (23) and it is used to establish $k_i \in q\{0, 1\}$ and kR based on the Eq. (24).

$$k = \sum_{i=0}^{e-1} k_i \, 2^i \tag{23}$$

$$\mathrm{kR} = \sum_{i=0}^{e-1} k_i \, 2^i R = 2(..2(2k_{e-1}R + k_{e-2}R) + ...) + k_0 R \tag{24}$$

The worst case requires 1-multiplying and 1-1 addition, where kR is calculated in the Eq. (25), if $k = 31$.

$$31R = 2(2(2(2R + 1) + R) + R) + R) \tag{25}$$

Finally, the data encryption is done and this encrypted data will be forwarded to the shortest paths.

4. Optimal shortest path data communication in WSN using dragonfly algorithm

4.1 Multi-objective function for shortest path communication

In this proposed secure data communication scheme, DA is used for selecting the optimal and shortest path among the source and destination nodes, which is done during computing the multi-objective functions concerning energy, distance, delay, trust and throughput. This multi-objective function is equated in Eq. (26).

$$\mathrm{Fit} = \underset{\{\mathrm{pt_{jk}}\}}{\arg\min}(\mathrm{Obj_4}) \tag{26}$$

In Eq. (26), the selected shortest path using DA is termed as $\mathrm{pt_{jk}}$, where $\mathrm{jk} = 1,2,\cdots,\mathrm{JK}$ and the total number of shortest paths selected in WSN is noted as JK. The range of selected shortest path $\mathrm{pt_{jk}}$ is derived among $[1, \mathrm{No}]$ and the total number of sensor nodes in the WSN is mentioned as No. The objective function $\mathrm{Obj_4}$ regarding several constraints is formulated here.

$$\mathrm{Obj_1} = (\alpha \times \mathrm{Dis}) + (1 - \alpha) \times \frac{1}{\mathrm{Eng}} \tag{27}$$

$$\mathrm{Obj_2} = (\beta \times \mathrm{Obj_1}) + (1 - \beta) \times \mathrm{Dly} \tag{28}$$

$$\mathrm{Obj_3} = (\gamma \times \mathrm{Obj_2}) + (1 - \gamma) \times \mathrm{Thr} \tag{29}$$

$$\mathrm{Obj_4} = (\delta \times \mathrm{Obj_3}) + (1 - \delta) \times \mathrm{Tu} \tag{30}$$

The values of α, β, γ and δ are assigned as 0.2, respectively. The "distance between two sensor nodes in same cluster or in other clusters" is determined for offering the optimal routing, where the distance is represented as Dis . "Euclidean distance Dis is determined among two nodes" is specified as "the length of a line segment between the two nodes" that is derived in Eq. (31).

$$\text{Dis} = \sqrt{(m_u - n_v)^2 + (m_u - n_v)^2} \quad (31)$$

In Eq. (31), the cluster heads taken for communication is formulated as m and n and the "corresponding coordinates to these nodes" are represented as u and v respectively.

The residual energy is termed as Eng that is explained as the "average remaining energy of the active sensor nodes at the end of each simulation experiment" as formulated in Eq. (32).

$$\text{Eng} = \text{Eng}_{\text{nn}} - \left(\text{eng}_{\text{nn}}^{\text{cs}} + \text{eng}_{\text{nn}}^{\text{sh}}\right) \quad (32)$$

In Eq. (32), the initial energy of any nodeNN_{nn} is derived as Eng_{nn} , the "energy consumption by collecting the number of data" unit is derived as $\text{eng}_{\text{nn}}^{\text{cs}}$, and the "energy consumption" by sending the number of data units is formulated as $\text{eng}_{\text{nn}}^{\text{sh}}$.

Delay is mentioned as Dly that is computed by performing the propagation delay and transmission delay during transmission of packets and formulated in Eq. (33).

$$\text{Dly} = \frac{\max \sum \text{pt}_{\text{jk}}}{NN} \quad (33)$$

In Eq. (33), the "data transmission from sensor node to base station" is noted as $\max \sum \text{pt}_{\text{jk}}$ and term NN denotes "the total number of nodes in sensor network".

Throughput is defined as, "how much data can be transferred from one location to another in a given amount of time. It is used to measure the performance of hard drives and RAM, as well as Internet and network connections", and it is represented by Thr and formulated in Eq. (34).

$$\text{Thr} = \frac{\sum(P_{\text{sc}} * \text{Ap}_s)}{\text{tms}} \quad (34)$$

Here, the variable Ap_s denotes the average packet size and P_{sc} denotes the successful packets count. Trust is defined in Eq. (1).

4.2 Dragonfly algorithm

DA [16] is motivated by the living behaviour of the dragonfly (solution). Generally, the solution has two phases that are "nymph and adult". The significant feature of the DA is it has the capacity for avoiding the real time optimization issues. It has the better "exploitation and exploration" phases and has high convergence rate. The DA is utilized in various areas to find optimal solutions and to reduce the error rate in optimization process. DA is applied in various applications such as network systems, image processing, machine learning [27, 28] and in wireless networks. Therefore, this method selects DA for secure data transmission. The solution hunts the small insects or small fishes as their food. DA utilizes the migration and hunting behaviour of the swarm to demonstrate their food resources and also to survive from their enemies. The position of the swarm is very important for the migration and hunting characteristic that is expressed in five stages that are mentioned below.

Separation: It is used to calculate the distance among two adjacent dragonflies as given in Eq. (35).

$$\text{SP}_n = -\sum_{i=1}^{K}(B_n - B_i) \quad (35)$$

Here, the term SP_n is denoted as the separation of n^{th} individual, B_n is defined as the location of n^{th} neighbouring individual, K indicates the number of neighbourhoods, and B_i represents the location of i^{th} individual.

Alignment: The aligned position of the dragonflies is computed using Eq. (36).

$$\text{AN}_n = \frac{\sum_{i=1}^{K} V_i}{K} \quad (36)$$

Here, the term V_i denotes the velocity of the i^{th} neighbouring individual and AN_n defines the alignment of n^{th}individual.

Cohesion: It is measured according to the Eq. (37).

$$\text{CN}_n = \frac{\sum_{i=1}^{k} B_i}{K} - B_n \quad (37)$$

The variable CN_n denotes the cohesion of n^{th} individual.

Attraction: The directions of food are attracted by dragonflies that are shown in the Eq. (38).

$$\text{FD}_n = B^{+} - B_n \quad (38)$$

Here, the term B^{+}shows the location of the food source, FD_n depicts the food source of the n^{th}individual.

Algorithm 1: DA [16]

Initialize the population with iteration
Compute the fitness solution
Determine the best solution
  Compute the fitness for all dragonflies
  Formulate Eq. (35) to Eq. (39) to calculate five position behaviour of the swarm.
Determine the neighbouring radius
  If the presence of neighbouring dragonfly occurs
    Formulate Eq. (40) to upgrade the step vector
    Formulate Eq. (41) to upgrade the solutions
  Else
    Formulate Eq. (42) to update the new position of vector
    Check the new positions using the variables in boundaries
  End if

Distraction: The dragonflies are distracted into various directions to escape from the enemies using the Eq. (39).

$$\mathrm{ED}_n = B^- - B_i \tag{39}$$

Here, the term ED_n represents "the position of an enemy of n^{th} individual" and B^- denotes "the position of the natural enemy". The location of "the dragonfly is upgraded in the search space and their movements" are examined through two vectors like, step vector ΔB and position vector B. The step vector initiates the movement of the dragonflies as given in Eq. (40).

$$\Delta \mathrm{B}_\mathrm{n}^{\mathrm{d}+1} = (\mathrm{spSP_n} + \mathrm{anAN_n} + \mathrm{cnCN_n} + \mathrm{fdFD_n} + \mathrm{edED_n}) + \mathrm{w}\Delta \mathrm{B}_\mathrm{n}^{\mathrm{d}} \tag{40}$$

Here, the term d is denoted as the iteration counter and the inertia weight is indicated as w, the terms $\mathrm{sp}, \mathrm{an}, \mathrm{cn}, \mathrm{fd}$ and ed correspondingly refers the weights of separation, alignment, attraction, cohesion and distraction. Then, the position vectors are updated based on Eq. (41).

$$B_n^{d+1} = B_n^d + \Delta B_n^{d+1} \tag{41}$$

If the lack of neighbouring solutions SN occurs, then the location vectors are given in Eq. (42).

$$B_n^{d+1} = B_n^d + \mathrm{lw(DN)} \times B_n^d \tag{42}$$

The dimensionality of the location vector is denoted as DN and the levy function is indicated as lw(DN) is computed based on Eq. (43).

$$\mathrm{lw(DN)} = 0.01 \times \frac{z_1 \times \sigma}{|z_2|^{\frac{1}{\beta}}} \tag{43}$$

$$\sigma = \left\{ \frac{\Gamma(1+\beta) \times \sin\left(\frac{\pi\beta}{2}\right)}{\Gamma\left(\frac{1+\beta}{2}\right) \times \beta \times 2^{\frac{(\beta-1)}{2}}} \right\}^{\frac{1}{\beta}} \tag{44}$$

The arbitrary numbers are termed as z_1 and z_2 that is ranging among $[0,1]$ and the constant is referred as β. The "pseudo code of the DA" is shown in Algorithm 1.

5. Results and discussions

5.1 Experimental evaluation

The offered "secure routing and data transmission" in WSN was developed in

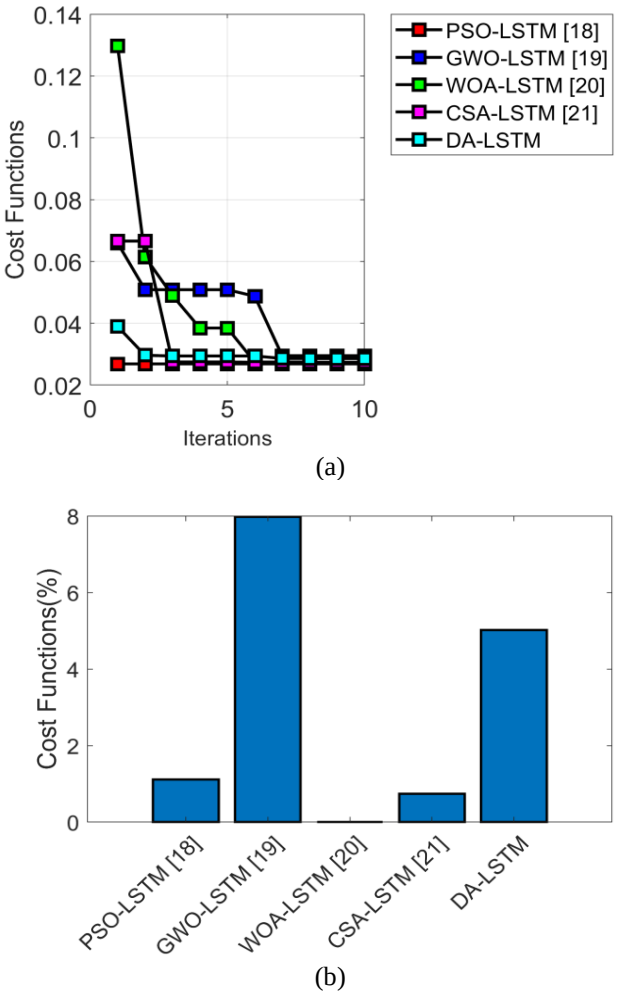
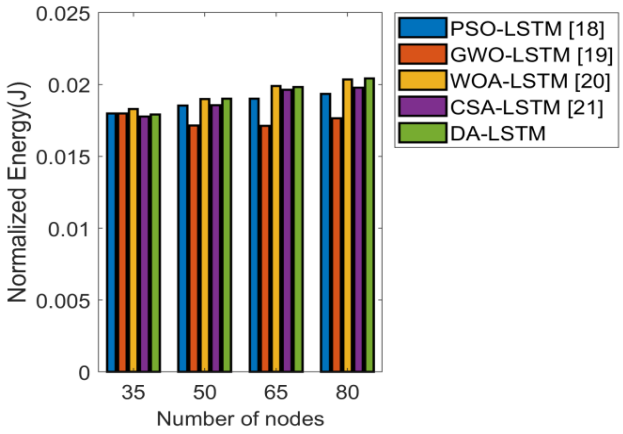


Figure. 3 Convergence evaluation of the offered "secure optimized routing and data transmission" in WSN regarding: (a) by varying the iterations and (b) by varying the algorithms

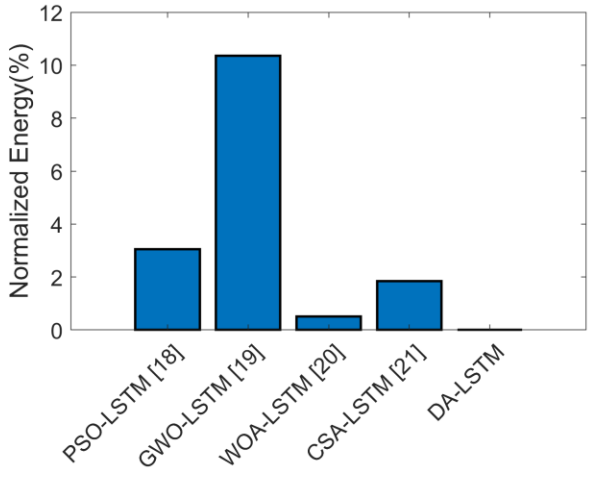
MATLAB2020a and the experimental results were validated. The offered method was tested with diverse algorithms such as "Particle Swarm Optimization (PSO) [18], Grey Wolf Optimization (GWO) [19], Whale Optimization Algorithm (WOA) [20], Crow Search Algorithm (CSA)" [21] and DA [16]. The performance measures were conducted regarding convergence analysis, latency, length of shortest path and normalized energy. The proposed method was validated by differing the number of sensor nodes as 35, 50, 65 and 80 and the maximum number of rounds as 800.

5.2 Convergence analysis

The convergence evaluation is carried out by varying the number of iterations and cost functions as given in Fig. 3. From the analysis, it is verified that the designed algorithm has shown the maximum convergence rate. The convergence evaluation of the



(a)



(b)

Figure. 4 Evaluation on normalized energy for the designed "secure optimized routing and data transmission" in WSN regarding: (a) by varying the iterations and (b) by varying the algorithms

Table 2. Analysis on shortest path length for the proposed "Secure Optimized Routing and Data Transmission" in WSN by using number of nodes as 80

Rounds	PSO-LSTM [18]	GWO-LSTM [19]	WOA-LSTM [20]	CSA-LSTM [21]	DA-LSTM
0	181.05	127.43	56.933	112.11	300.8
100	133.88	475.12	152.08	163.9	235.24
200	284.48	372.22	212.64	71.359	55.07
300	126.83	97.176	79.532	219.86	85.925
400	444.48	131.92	35.923	71.81	150.51
500	260.27	486.06	269.71	323.36	58.206
600	176.86	296.51	35.923	56.886	373.4
700	396.15	34.442	134.4	324.21	82.64
800	186.6	83.384	104.26	389.5	35.923

suggested DA-LSTM method is correspondingly secured 14 %, 11 %, 14 %, and 18 % enriched performance than the PSO-LSTM, GWO-LSTM, WOA-LSTM, and CSA-LSTM for the 5th iteration. Evaluation of cost function of the proposed DA-LSTM model is correspondingly secured 22 %, 27 %, 31 %, and 18 % enriched performance than the PSO-LSTM, GWO-LSTM, WOA-LSTM, and CSA-LSTM at iteration 10th. Therefore, the proposed method has obtained lowest convergence rate than other conventional models.

5.3 Energy analysis

The performance analysis in terms of energy is evaluated with energy by varying the number of nodes and heuristic algorithms as given in Fig. 4. This analysis has offered a superior performance using DA-LSTM when comparing with other heuristic algorithms.

5.4 Comparative analysis over shortest path length

The evaluation of efficiency regarding shortest path length for the proposed secure optimized routing and data transmission in WSN is shown in Table 2. From the experimental evaluation, it is verified that the designed model has ensured the optimal path selection while comparing with other heuristic algorithms.

5.5 Evaluation of energy using baseline routing protocols

The performance analysis regarding energy is evaluated with energy by varying the number of nodes and routing protocols as given in Fig. 5. This

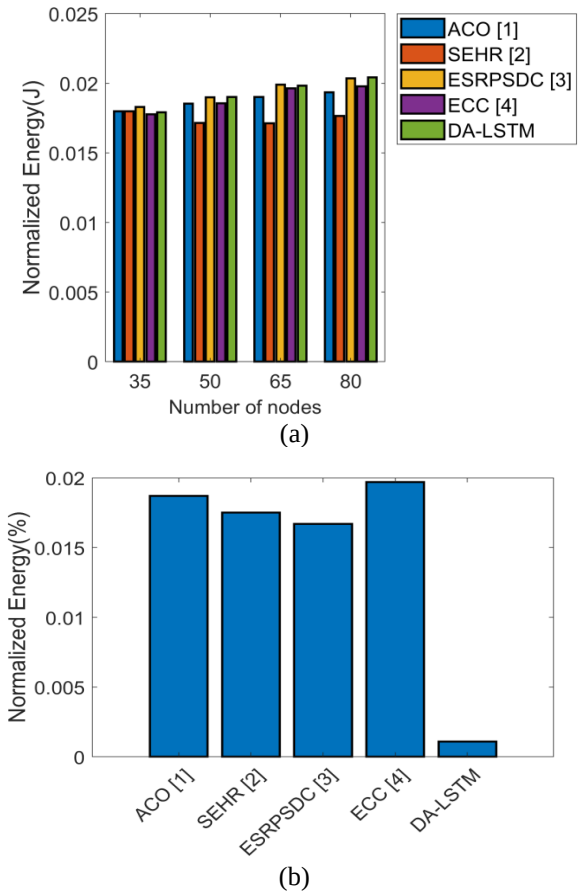


Figure. 5. Validation on normalized energy for the designed "secure optimized routing and data transmission" in WSN by varying with diverse baseline routing protocols regarding: (a) by varying the iterations and (b) by varying the routing protocols

analysis has offered a superior performance using DA-LSTM when comparing with other baseline routing protocols.

5.6 Discussion

Few of the drawbacks of optimization algorithms are given by, PSO takes more time for installation and it obtains lowest accuracy rate. GWO, WOA, and SFO algorithms maximize the fault rates and provide a low exploitation phase and they do not provide the accurate outcomes. The main obstacles of the baseline routing protocol are listed below, the storage limit is very low and it decreases the energy efficiency. It causes packet loss and delay for the number of nodes. Due to this it can affect the performance of the routing protocol. The suggested DA-LSTM method is more effective than other baseline optimization algorithms owing to the challenges of existing studies. This is according to the capability of DA-LSTM to get the accurate results with lowest errors. It has a better exploitation capacity and it attains highest accuracy rate. The experimental results reveal that the suggested DA-LSTM method achieves a better cost function based on the iterations and the comparison among baseline conventional algorithms which leads to a better convergence rate. Accordingly, it obtains better energy efficiency and the evaluation efficiency regarding shortest path length for the suggested method which is more secure for transmitting the data in WSN.

6. Conclusion

This work has proposed a secure routing scheme in WSN with the help of heuristic and deep learning approaches. At first, the LSTM was used for verifying the trust among the sensor nodes, where the malicious nodes are detected and removed from the system. Then the second phase, the secure data transmission was employed with the help of ECC algorithm during encrypting the data process. Then, the encrypted data was forwarded to the secured and selected optimal shortest paths, in which the secure shortest path selection was done through DA by deriving the multi-objective function regarding the several measures. The convergence evaluation of the suggested DA-LSTM method is correspondingly secured 14 %, 11 %, 14 %, and 18 % enriched performance than the PSO-LSTM, GWO-LSTM, WOA-LSTM, and CSA-LSTM for the 5th iteration. The energy efficiency is better than the other baseline routing protocols and algorithms. Finally, the proposed work has shown elevated performance regarding convergence and energy analysis. In future, the efficiency of the secured routing scheme in WSN can be further improved through the utilization of hybrid optimization techniques.

Author contributions

"The paper Conceptualization, methodology, software, validation, formal analysis, investigation, resources, data collection, 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".

Conflict of interest

The authors declare no conflict of interest.

References

[1] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy, and R. Patan, "Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm

for Wireless Sensor Networks", *IEEE Transactions on Engineering Management*, Vol. 68, No. 1, pp. 170-182, Feb. 2021.

[2] 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.

[3] S. Ganesh and R. Amutha, "Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms", *Journal of Communications and Networks*, Vol. 15, No. 4, pp. 422-429, Aug. 2013.

[4] X. H. Le, S. Lee, I. Butun, M. Khalid, R. Sankar, M. Kim, M. Han, and Y. K. Lee, "An energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography", *Journal of Communications and Networks*, Vol. 11, No. 6, pp. 599-606, Dec. 2009.

[5] U. S. kumaran and P. Ilango "Secure authentication and integrity techniques for randomized secured routing in WSN", *Wireless Networks*, Vol. 21, pp. 443–451, 2015.

[6] K. Haseeb, N. Islam, A. Almogren, I. U. Din, H. N. Almajed, and N. Guizani, "Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs", *IEEE Access*, Vol. 7, pp. 79980-79988, 2019.

[7] W. Feng, F. Wang, D. Xu, Y. Yao, X. Xu, X. Jiang, and M. Zhao, "Joint Energy-Saving Scheduling and Secure Routing for Critical Event Reporting in Wireless Sensor Networks", *IEEE Access*, Vol. 8, pp. 53281-53292, 2020.

[8] A. Liu, Z. Zheng, C. Zhang, Z. Chen, and X. Shen, "Secure and Energy-Efficient Disjoint Multipath Routing for WSNs", *IEEE Transactions on Vehicular Technology*, Vol. 61, No. 7, pp. 3255-3265, Sept. 2012.

[9] K. Haseeb, N. Islam, A. Almogren, and I. U. Din, "Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things", *IEEE Access*, Vol. 7, pp. 185496-185505, 2019.

[10] S. Li, S. Zhao, X. Wang, K. Zhang, and L. Li, "Adaptive and Secure Load-Balancing Routing Protocol for Service-Oriented Wireless Sensor Networks", *IEEE Systems Journal*, Vol. 8, No. 3, pp. 858-867, Sept. 2014.

[11] D. Qin, S. Yang, S. Jia, Y. Zhang, J. Ma, and Q. Ding, "Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network", IEEE Access, Vol. 5, pp. 9599-9609, 2017.

[12] G. Zhan, W. Shi, and J. Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs", *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 2, pp. 184-197, March-April 2012.

[13] X. Fu, Y. Yang, and O. Postolache, "Sustainable Multipath Routing Protocol for Multi-Sink Wireless Sensor Networks in Harsh Environments", *IEEE Transactions on Sustainable Computing*, Vol. 6, No. 1, pp. 168-181, 1 Jan.-March 2021.

[14] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks", *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 9, pp. 2013-2027, Sept. 2016.

[15] W. Gu, N. Dutta, S. Chellappan, and X. Bai, "Providing End-to-End Secure Communications in Wireless Sensor Networks", *IEEE Transactions on Network and Service Management*, Vol. 8, No. 3, pp. 205-218, September 2011.

[16] M. Jafari and M. H. B. Chaleshtari, "Using dragonfly algorithm for optimization of orthotropic infinite plates with a quasi-triangular cut-out", *European Journal of Mechanics A/Solids*, Vol. 66, pp. 1-14, 2017.

[17] A. Azzouni and G. Pujolle "A Long Short-Term Memory Recurrent Neural Network Framework for Network Traffic Matrix Prediction", *Networking and Internet Architecture*, 2017.

[18] A.Yadav, S. Kumar, and S. Vijendra, "Network Life Time Analysis of WSNs Using Particle Swarm Optimization", *Procedia Computer Science*, Vol. 132, pp. 805-815, 2018.

[19] N. A. A. Aboody and H. S. A. Raweshidy, "Grey wolf optimization-based energy-efficient routing protocol for heterogeneous wireless sensor networks", *International Symposium on Computational and Business Intelligence (ISCBI)*, pp. 101-107, 2016.

[20] A. R. Jadhav and T. Shankar "Whale Optimization Based Energy-Efficient Cluster Head Selection Algorithm for Wireless Sensor Networks", *Neural and Evolutionary Computing*, 2017.

[21] A. G. Hussien, M. Amin, M. Wang, G. Liang, A. Alsanad, A.Gumaei, and H. Chen, "Crow Search Algorithm: Theory, Recent Advances, and Applications", *IEEE Access*, Vol. 8, pp. 173548-173565, 2020.

[22] G. Halidoddi and R. Pandu "Secured Data Transmission Using Multi-Objective Trust

Based Bat Optimization Algorithm and Enhanced Homomorphic Cryptosystem for WSN", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 1, pp. 214-224, 2022, doi: 10.22266/ijies2022.0228.20.

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

[24] S. VenkataRao and V. Ananth "A Hybrid Optimization Algorithm and Shamir Secret Sharing Based Secure Data Transmission for IoT based WSN", *International Journal of Intelligent Engineering and Systems*, Vol. 14, No. 6, pp. 498-506, 2021, doi: 10.22266/ijies2021.1231.44.

[25] S. M. Shivakumaraswamy and C. S. Mala "Security and Energy Aware Adaptive Routing using Cost Centric Cuckoo Search Algorithm", *International Journal of Intelligent Engineering and Systems*, Vol. 14, No. 6, pp. 596-604, 2021, doi: 10.22266/ijies2021.1231.53.

[26] G. Halidoddi and R. Pandu "A GOA Based Secure Routing Algorithm for Improving Packet Delivery and Energy Efficiency in Wireless Sensor Networks", *International Journal of Intelligent Engineering and Systems*, Vol. 14, No. 6, pp. 311-320, 2021, doi: 10.22266/ijies2021.1231.53.

[27] J. Tabjula, S. Kalyani, P. Rajagopal, and B. Srinivasan "Statistics-based baseline-free approach for rapid inspection of delamination in composite structures using ultrasonic guided waves", *Structural Health Monitoring*, 2021.

[28] J. L. Tabjula, S. Kanakambaran, S. Kalyani, P. Rajagopal, and B. Srinivasan "Outlier analysis for defect detection using sparse sampling in guided wave structural health monitoring", *Structural control and Health Monitoring*, Vol. 28, Issue, March 2021.