Journal of Harbin Engineering University Vol 44 No. 7

ISSN: 1006-7043 July 2023

An Energy – Aware and Trust based Secure Routing Protocol using OEHO and CDFPCC Approaches in WSN Environment

S. Kalaivani
Research Scholar
Dept. of Computer Science and Engineering
Annamalai University
Annamalainagar – 608002
Tamilnadu, India
Email: kvani89.mec@gmail.com
Dr. G. Ramachandran
Associate Professor
Dept. of Computer Science and Engineering
Annamalai University
Annamalainagar – 608002
Tamilnadu, India
Email: gmrama1975@gmail.com
Dr.T.Priyaradhikadevi
Professor & Head
Dept. of Computer Science and Engineering
Mailam Engineering College
Mailam – 604304
Tindivanam
Tamilnadu, India
Email: prdcsehodmec@gmail.com

ABSTRACT

A wireless sensor network (WSN) is a group of sensor nodes that dynamically organizes itself into a wireless network without using any pre-existing infrastructure. The energy consumption of WSNs is one of the main issues, and it affects the lifespan of the network. This research proposes ETHOEHO, a hybrid Osprey-Elephant herding optimizer (ETHOEHO) algorithm, as an energy-aware and trust-based routing protocol for wireless sensor networks as a result of the need for improvement. In this study, the initialized nodes' direct and indirect trust values are computed based on threshold calculation. The cluster is then generated using HWF-SS based on the factors, and the cluster head is chosen using OEHO. Then, among the discovered pathways, the best paths are chosen using the ATSO after the CH paths are chosen using the SFDENN. The detected data are safely transferred to the BS via CDFPCC from the chosen route. When conducting an experimental assessment, the planned research's performance is analyzed using the currently used methods. The suggested achieves superior results.

Keywords - Wireless Sensor Network (WSN), Weighted Function based Stratified Sampling (HWF-SS), Swish Functional Deep Elman Neural Network (SFDENN), Adjusted Tunicate Swarm Optimization (ATSO), and Cumulative Distributed Four Point Curve Cryptographic (CDFPCC)

1. INTRODUCTION

In a typical WSN, several sensor nodes gather data by using self-organizing methods with the sink, and sensor nodes transfer the data to the sink for processing [1]. The sink is then in charge of integrating, processing, and uploading the data to the server. Since sensor nodes in WSNs are often unattended, nodes run on batteries with limited power and cannot be quickly recharged or replaced. As a result, the majority of earlier research projects have concentrated on increasing node longevity while attaining peak throughput [2]. Data transmission consumes more energy than

sensing, as shown by the fact that a node may do 800 internal operations with the same amount of energy as a single transmission [3]. Nodes are also susceptible to a range of threats since they operate in unattended settings. To safeguard WSN, secure routing techniques have been created [4]. When sending communications from source to destination, choosing the best route is essential. A significant quantity of energy is used up when transmitting data. The issue of high energy usage has been effectively solved by hierarchical routing design. One of the most efficient methods for preserving sensor node energy is to cluster the nodes together. The network is partitioned into several groups, or clusters, during the clustering phase. Each cluster is headed by a leader known as the Cluster Head (CH). The local data must be gathered by CHs from their member sensor nodes inside the clusters, aggregated, and sent either directly or indirectly via other CHs to a distant Base Station (BS) [5][6]. Multi-hop WSNs provide routing at the network layer, which is where intermediary Sensor Nodes (SNs) receive and deliver data packets. Under these conditions, trustworthy intermediate SNs along the shortest path to the sink are necessary for efficient data transfer. In order to confuse other SNs and jeopardize the reliability of WSNs, malicious SNs may engage in any unexpected action with data packets and forwarding routes [7]. The trust management technique has to be used in the routing process for data packet deliveries at the base station to be successful. The routing method should not include sensor nodes with low trust scores [8]. Wireless sensor networks include a variety of safe routing protocols, but they all need some kind of conventional cryptography and authentication, which raises processing requirements and increases routing costs [9]. Furthermore for the CH choice the most effective approach to increase the network's lifetime is to use meta-heuristic optimization methods. Heuristics have a wide range of fascinating uses in a variety of technological disciplines, including remote sensing models and electric system optimization. The algorithms do, however, encounter a number of typical issues, including rapid convergence, local search issues with the fitness function, and increasing cost [10]. This study offered a unique strategy to create trustworthy nodes and improved CH selection for reducing node energy usage.

Problem Definition

Existing research works develops many methods for energy efficient routing but still the challenges are presented that are,

- Convergence problem was occurred during efficient CH management.
- Trust level was not considered based on most important metrics.
- Efficient path strategy was not fully focused with advanced approaches.

To mitigate those problems this research methodology proposed an advanced approach with considering most important metrics for the path generation and data transmission process.

The proposed research methodology is structured as follows: in section 2, the existing research methodologies related to energy-aware routing in WSN are explained; in section 3, the proposed methodology has been explained; in section 4, the experimental analysis of the proposed methodology is given; and in section 5, the proposed research is concluded with the possibility of future improvement.

2. RELATED WORK

Youjia Han *et al*. [11] proposed a trust-based routing protocol for wireless sensor networks [11], aiming to protect against standard and unique attacks, as well as reduce energy expenditure due to data transmission. An adaptive evolutionary algorithm known as TAGA was employed in order to select strong cluster heads through the introduction of a threshold function that considers changes in composite trust ratings and residual energy levels.

M. Selvi *et al*. [12] recently unveiled an innovative secure routing system known as energy conscious trust-based routing algorithm. This method capitalizes on the combination of trust score assessment, decision tree technique and spatio temporal constraints to accurately distinguish illegitimate users in Wireless Sensor

Networks (WSN). Abdulhamid Zahedi and Faryad Parma [13], the gravitational search approach was applied to improve the routing process with special regard to energy conservation and node trusts, both direct and indirect. The combination of these components resulted in the introduction of an algorithm known as the Energy-aware, Trusted-based Gravitational Search Approach (ETGSA).

Maryam Hajiee *et al*. [14] designed the Energy-aware Trust and Opportunity-based Routing (ETOR) algorithm; they crafted an exclusive hybrid fitness function to evaluate it. This hybrid approach weighed factors such as energy conservation, trustworthiness, Quality of Service (QoS), connection strength, distance traveled, hop count, and network traffic in order to choose the most effective and secure path. In addition, ETOR utilizes the multipath route strategy with both intra-cluster and inter-cluster multi-hop communication systems.

M. Udhayavani and M. Chandrasekaran [15] are the architects behind a trust-aware routing framework and energy-efficient network protocol with minimal overhead. The purpose of these combined initiatives is to reduce assaults on the network, thereby ensuring a higher quality of service as well as more reliable, energy-efficient routes which can prolong the lifespan of the network.

To establish an efficient WSN routing protocol, D. Laxma Reddy *et al.* [16] sought to find an optimal cluster head. As a result, they proposed a novel hybrid algorithm known as Ant Colony Optimization (ACO) integrated Glowworm Swarm Optimization (GSO) method (ACI-GSO). This algorithm seeks to maximize several objectives such as distance, delay, and energy. Eventually, its efficiency was evaluated in comparison with existing works and it was proven to be successful.

Thangaramya Kalidoss *et al*. [17] proposed a trust modeling method which amalgamates an authentication approach with a key-based security mechanism to create trust scores. These process results three categories of direct, indirect, and total trust ratings and the final route is then selected on basis of path-trust, energy, and hop count for successful completion of the safe routing procedure. The experimental outcomes suggest that their proposed algorithm presents improved performance when evaluated against packet delivery ratio, network life, and security. Comparatively speaking, Fuzzy Rule technique was less effective since it solely depends on human understanding.

In an effort to maximize network lifespan and achieve load balancing, S. Balaji *et al*. [18] proposed using three criteria – energy, weight and distance to base station – to select a Cluster Head (CH) from each individual cluster of nodes. This CH was responsible for transmitting data packets from source node to base station, with all nodes in a chain format connected via fuzzy logic type 1 method. A major benefit of this approach is that it leads to conserved energy as well as prolonged network lifespan; however, its downside is that it relies on pre-defined rules based solely on experience.

In their aim of bolstering trust and thus enhancing network lifetime, Nitin Mittal *et al*. [19] proposed a Cuckoo search optimization technique using fuzzy type-2 logic-based clustering. Multi-hop routing instead of the threshold-based data transmission algorithm was utilized for intra-cluster communications in order lessen energy loss from CHs which were far away from the Base Station (BS). Simulation results revealed that this approach is more effective than other communication methods regarding energy consumption, stability time, and lifespan of the network as well as successfully removing malicious nodes. Sadly, there exists an issue with its low convergence accuracy and slow search speed.

Manisha Rathee *et al*. [20] suggested a novel QoS aware Energy Balancing Secure Routing (QEBSR) technique based on ant colony optimization for WSNs. This heuristic was enhanced to consider route node trust levels and end-to-end latency. To assess its performance, the proposed approach was compared to distributed energy balanced routing and energy efficient routing with compromised resistance algorithms. According

to simulation results, QEBSR proved superior to the other two methods.

3. PROPOSED METHODOLOGY

3.1 Energy-Aware and Trust-based Secure Routing Protocol using Hybrid Technique

Secure communication is a major issue that must be addressed in Wireless Sensor Networks (WSNs). Attackers may be able to repeat routing data through malicious nodes, thus stealing the identities of legitimate ones. This can lead to disastrous outcomes, such as wasted energy from excessive packet loss and slower overall performance. To combat this, researchers are proposing an energy-efficient trust-based routing protocol for WSNs known as ETHOEHO, which is based on the Osprey-Elephant Herding Optimizer algorithm. As shown in Figure 1, block diagram consists of a variety of components.

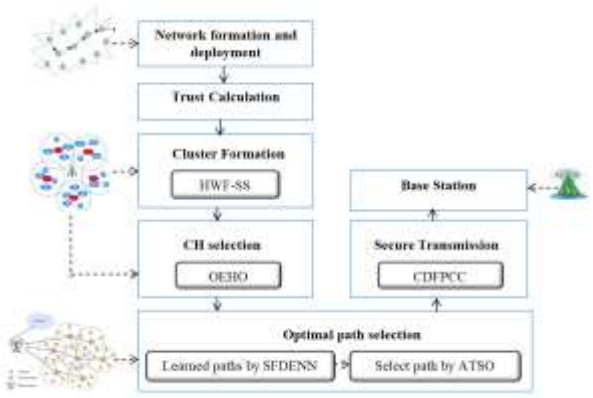


Figure 1 Block Diagram for the Proposed Research Methodology

3.2 Network Formation

At first, numerous sensor nodes are set up in a network. These nodes can then identify and broadcast a value to a base station. As part of network deployment, it is essential to gauge node performance. This is expressed in an initialized node as explained in Equation (1):

$$\varpi_y = \{\varpi_1, \varpi_2, ..., \varpi_n\} \ (or) \ \varpi_i, i = 1,2,...., n \quad (1)$$

Where, ϖ_y defines the initialized node set and ϖ_n specifies the n-number of initialized nodes.

3.3 Trust Calculation

Once the network has been established, a trust value is then determined. In this particular research process, various factors are taken into consideration when computing a direct and indirect level of trust. Residual energy (λ_1), degree difference (λ_2), sum of the distances betwixt nodes with all its neighbor's cumulative time (λ_3), initial energy (λ_4), signal to inferences plus noise ratio (λ_5), network load (λ_6), distance as of source node to base station (λ_7), time factor (λ_8), collision factor (λ_9), packet forwarding rate (λ_{10}), and loss factor (λ_{11}). Thus, the calculated trust factors are mentioned as in equation formation in equation (2),

$$\lambda_i = \{\lambda_1, \lambda_2, \lambda_3, ..., \lambda_{11}\} \quad (2)$$

In this step, λ_i the trustworthiness of a node is determined by evaluating its trust value against a predetermined threshold. When the obtained value meets or surpasses the specified limit, it is labeled as a trusted node; otherwise, rule conditions distinguish it as an untrusted one.

3.4 Cluster Formation

This section centres around the use of trust values to group nodes into clusters. To facilitate this clustering, the trust factor of each node λ_i is implemented as a weight value (ω_i) The Haversine with Weighted Function based Stratified Sampling (HWF-SS) approach is employed for this purpose and replaces Euclidean distance which can be inefficient when dealing with large numbers. This method consists of three stages: stratification, sample allocation and sample extension. During stratification, η centroids are established according to maximum and minimum range

heuristics then data points are assigned to a η stratum using the Haversine distance between them and the η centroid of data.

The sample allocation procedure is next implemented. Optimum sample allocation is a type of sample allocation method that takes into account the stratum size and variability, with the lowest price tag. This technique permits one to establish the desired number of sampling units q^{th} for the stratum based on equation (3),

$$n_q = \frac{n\,\omega_i\,\sigma_q}{\sum \omega_i \sigma_q^2} \tag{3}$$

In the process of expanding a sample n, D_{tt} the Euclidean distance between the centroid and other sensor node values can be determined with being n the total sample size, σ_q specifying standard deviation and σ_q^2 representing variance q^{th} based on N_q individual units. By calculating these metrics, this distance is represented in Equation (4):

$$D_{tt} = \sqrt{\sum \left| cen_i - \lambda_i \right|^2} \tag{4}$$

Utilizing the distance values that have been calculated, a grouping of nodes is created.

3.5 Cluster Head Selection

Using the Osprey Elephant Herding Optimization (OEHO) algorithm, a cluster head is determined based on the minimum transmission energy of sensor nodes. The osprey, alternatively known as a fish hawk, river hawk or sea hawk and found worldwide, are observed to have intelligent strategies when hunting for fish and taking them to an optimal eating position. However, this process can suffer convergence issues; thus necessitating an updation procedure in order to rectify this problem. To start the procedure, each osprey within the OOA population is initialized. This requires that the variables for the problem be first set according to their respective positions inside of the search space. Equation (5) assigns random coordinates to these ospreys, defining their exact location inside of this search space.

$$w_{i,j} = v_j + \alpha_{i,j} . \left(u_j - v_j \right),\ i = 1,2,\ldots,N,\ j = 1,2,\ldots,m \tag{5}$$

In order to W identify the population matrix of ospreys' locations, W_i it $w_{i,j}$ is important to consider the characteristics and j^{th} dimensions of the i^{th} osprey. Specifically, it is needed to consider the number of ospreys as well as the number of problem variables. Furthermore, random numbers in interval [0, 1] are also essential for establishing a fitness value for each population. Finally, v_j, and u_j are lower bound and upper bounds of problem variables will be taken into account too Equation (6).

$$R = \begin{bmatrix} R(W_1) \\ . \\ R(W_i) \\ . \\ R(W_N) \end{bmatrix}_{N \times 1} \tag{6}$$

The osprey's trajectory is determined by R th the vector of the objective function values. Through fitness evaluation, a suitable spot for hunting fish is identified. Then, with random chance, the osprey finds one of these schools of fish and launches an attack. Utilizing Equation (7) & (8), a new position is calculated based on the simulation of its movements toward the prey. Ultimately, this replacement position will improve upon its desired outcome according to Equation (9).

$$w_{i,j}^{O1} = w_{i,j} + \alpha_{i,j} . \left(E_{i,j} - D_{i,j} . w_{i,j} \right) \tag{7}$$

$$w_{i,j}^{O1}=\begin{cases} w_{i,j}^{O1}, & v_j \le w_{i,j}^{O1} \le u_j; \\ v_j, & w_{i,j}^{O1} < v_j; \\ u_j, & w_{i,j}^{O1} > u_j. \end{cases}$$

(8)

$$W_i=\begin{cases} W_i^{O1}, & R_i^{O1} < R_i; \\ W_i, & else. \end{cases}$$

(9)

After analyzing the details of the W_i^{O1} first phase of i^{th} osprey, such as its dimension, R_i^{O1} objective function value and food selection, $\alpha_{i,j}$ and $D_{i,j}$ are random numbers were assigned to both the interval [0 , 1] and set {1, 2}. Then an elephant herding updating procedure was applied in order to locate a secure position according to Equation (10).

$$w_{i,j}^{O1}=w_{i,j}+\delta\times\left(w_{i,j}^{O1}-w_{i,j}\right)\times\alpha$$

(10)

Where, $\delta\in[0,1]$ is the scaling factor that determines the influence of matrix of the population.

Input: Obtained cluster sets

Output: Selected cluster head ζ_i

Begin

Initialize population, fitness, iteration rr_t and maximum iteration x_{ma}

Compute fitness

Set iteration $rr_t=1$

While $\left(rr_t \le x_{ma}\right)$ **do**

Movements of the osprey by, $w_{i,j}^{O1}=w_{i,j}+\alpha_{i,j}.\left(E_{i,j}-D_{i,j}.w_{i,j}\right)$

Update the new position

If $R_i^{O1} < R_i$ **{**

$$W_i=W_i^{O1}$$

} else {

$$W_i=W_i$$

} end if

Obtain the safe position for eat prey using, $w_{i,j}^{O1}=w_{i,j}+\delta\times\left(w_{i,j}^{O1}-w_{i,j}\right)\times\alpha$

Calculate fitness

Set $rr_t=rr_t+1$

End while

Return Cluster head

End

The selected cluster heads are specified in Equation (11),

$$\zeta_i=\{\zeta_1,\zeta_2,.....,\zeta_n\}$$

(11)

Where, ζ_i defines the cluster head set and ζ_n specifies the n-number of cluster set.

3.6 Optimal Path Selection

After selection of the cluster head the optimal path is detected. For that detection the path is learned by using Swish Functional Deep Elman Neural Network (SFDENN). The vanishing gradient problem is presented in the neural network in order to solve that problem this research methodology considers the Swish activation functions. Based on the learning the elements are updated in the routing table which will helpful to know the available paths. From the available paths the best path is chosen by using Adjusted Tunicate Swarm Optimization (ATSO) algorithm.

Elman Neural Networks are usually comprised of four layers - input, hidden, undertake and output - with their recurrent connections fixed and their feedback connections alterable. The purpose of the undertaking layer is to retain the output from the hidden layer, operating like a

step-delay operator. Finally, these Elman networks can operate on deep layers for more sophisticated learning of the inputs.

Given n inputs and m outputs, along with a certain number of hidden and undertake neurons (denoted as r), the weight from input layer to hidden layer is known as $w1$, from undertake layer to hidden layer as $w2$, and from hidden layer to output layer as $w3$; For this neural network system, the input value can be defined as (k – 1), the output of the hidden layer as (k).

$$h(l) = f\left(\tau_2 \zeta_i + \tau_1(e_t)\right) \tag{12}$$

$$t(l) = h(l-1) \tag{13}$$

Where in Equation (12), f denotes the activation function which is based on swish activation which is derived in Equation (13),

$$f = e_t . sg_d(e_t) \tag{14}$$

From Equation (14), $sg_d(e_t)$ specifies the sigmoid function of the input value. The output layer function $p(l)$ is given in Equation (15),

$$p(l) = f\left(\tau_3 h(l)\right) \tag{15}$$

The final error of the process is derived in Equation (16),

$$l_s = \sum (g(l) - p(l))^2 \tag{16}$$

Where, l_s indicates the error function and $g(l)$ specifies the target output value. Thus, the learned paths are updated in the table. From the path the optimal one is selected using ATSO and the minimum distance and less energy consumption is considered as fitness function. The Tunicate Swarm Algorithm (TSA) is an intelligently designed meta-heuristic optimizer that emulates the behaviour of marine tunicates and their jet propulsion systems. For the system to faithfully replicate nature, three conditions have been established: no conflicts between search agents, movement in the direction of a better-performing agent, and remaining close to the most successful searcher. To begin with, tunicates are initialized according to ascending order, aiming to prevent convergence problems as described by Equation (17).

$$C_N = \{c_1, c_2, ..., c_n\} \tag{17}$$

Where, C_N defines the initialized tunicates based on ascending order, and c_n denotes the n-number of tunicates. The position of the initialized population is expressed in Equation (18),

$$C_N^p = C_N^{p_{\min}} + r_d \times \left(C_N^{p_{\max}} - C_N^{p_{\min}}\right) \tag{18}$$

In order to find optimal position, the tunicates utilize a formula that allows them to adjust their location at various stages in the process. Here, C_N^p is their location on the spectrum and r_d is a random value between 0 and 1. The design variables' lower bound is denoted by $C_N^{p_{\min}}$ and their upper limit by $C_N^{p_{\max}}$. This Equation (19) reads as follows:

$$C_N^p(d+1) = \frac{C_N^p(d) + C_N^p(d+1)}{2 + r_d} \tag{19}$$

Where, $C_N^p(d)$ refers to the updated position of the tunicate with respect to the position of the food source based on equation (20),

$$C_N^p(d) = \begin{cases} F_s + R_C \times \left|F_s - r_d \times C_N^p\right|, & if \quad r_d \geq 0.5 \\ F_s - R_C \times \left|F_s - r_d \times C_N^p\right|, & if \quad r_d < 0.5 \end{cases} \tag{20}$$

Food source F_s is an essential factor in determining the optimal position of a

population's tunicates. To prevent them from bumping into each other, randomized vector R_C were modelled, which is stated in Equation (21):

$$R_C = \frac{r_{d(2)} + r_{d(3)} - 2r_{d(1)}}{SD_{\min} + r_{d(1)}\left(SD_{\max} - SD_{\min}\right)} \quad (21)$$

Where, $r_{d(1)}$, $r_{d(2)}$ and $r_{d(3)}$ are random numbers within range [0, 1]; $SD_{\min}$ and $SD_{\max}$ reflect the minimum and maximum speeds that are used to create social interaction. Thus, the selected path is denoted as β_i.

3.7 Secure Data Transmission

The sensed data are securely transferred to the base station via selected optimal path using Cumulative Distributed Four Point Curve Cryptographic (CDFPCC). For the encryption the four points based curve is considered. Four point curves mean the Edward curve. Thus, the Edward curve is a new form for elliptic curves over fields of characteristics. The Edward curves satisfy the following form in Equation (22),

$$g^2 + h^2 = b^2 + b^2 g^2 h^2 \quad (22)$$

Where, g and h defines the neutral element and b represents the non-zero value. The operation of the Edward curve is more efficient than most of the other forms of elliptic curves. First the private key is generated randomly. To generate a private key, the cumulative distribution function is utilized. The formula for this is stated in Equation (23)

$$p_{vt} = \int nu_x \, dx \quad (23)$$

Here, p_{vt} indicates the private key, nu_x defines all the values. Finally, based on the private key and four points of the curve, a public key is generated. This process can be expressed as follows:

$$p_{lc} = p_{vt} * p_{ot} \quad (24)$$

Where in Equation (24), p_{ot} defines the point on curve of the four points. After initialization of points the data is encrypted using equation (25) and (26),

$$Ex_1 = p_{ot} * \chi \quad (25)$$

$$Ex_2 = \beta_i + \chi * Ex_1 \quad (26)$$

Where, Ex_1 and Ex_2 represents the two cipher texts, χ denotes the random number and β_i denotes the sensed data. At the base station the data is decrypted by using Equation (26),

$$\beta_i = \left(Ex_2 - p_{vt}\right) * Ex_1 \quad (26)$$

Based on those procedures the data is forwarded to the base station.

4. RESULTS AND DISCUSSION

In order to further examine the effectiveness of ETHOEHO, several well-established research methodologies have been utilized. To carry out the implementation, MATLAB was selected as the working platform.

4.1 Performance of Optimal Path Detection

Here, the accuracy, F-Measure, precision, recall, specificity, and sensitivity of the proposed SFDENN-based optimal path learning are compared to those of the existing Beta Distribution and Scaled Activation Function-based Deep Learning Neural Network (BDSAF-DLNN), Artificial Neural Network (ANN), and Support Vector Machine (SVM).

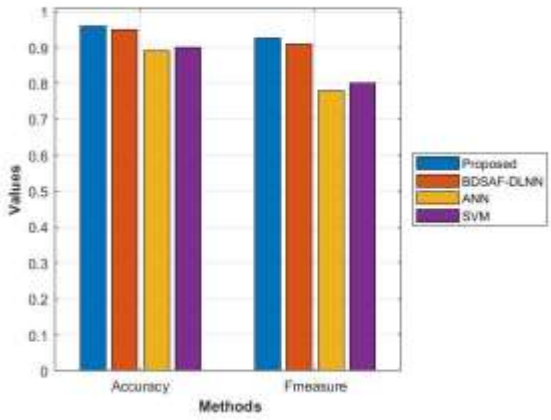


Figure 2 Performance Analysis Based on Accuracy and F-Measure Metric

The accuracy and F-measure values of the proposed and current research approaches are shown in Figure 2. The percentage of accurate forecasts and total predictions determine the accuracy value. The accuracy and recall metrics are combined to create the F-Measure. The suggested technique outperforms current methods in terms of accuracy, which is above 0.95, and F-measure. Due to the proposed ability to resolve the vanishing gradient issue, it achieves greater F-measure values and accuracy.

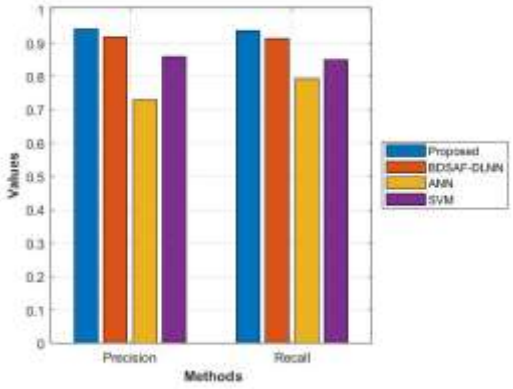


Figure 3 Precision and Recall Analysis

The suggested algorithm's recall and precision values are contrasted with those of the current methods, which are shown in Figure 3. Recall measures the amount of performance, whereas precision assesses the quality of performance. Here, the suggested strategy outperforms the current methods based on the two measures.

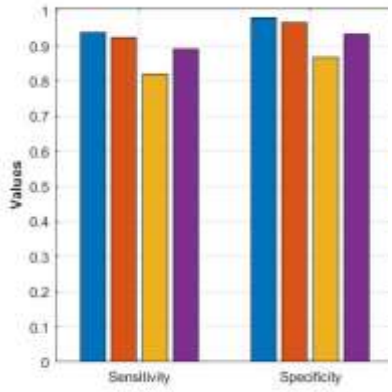
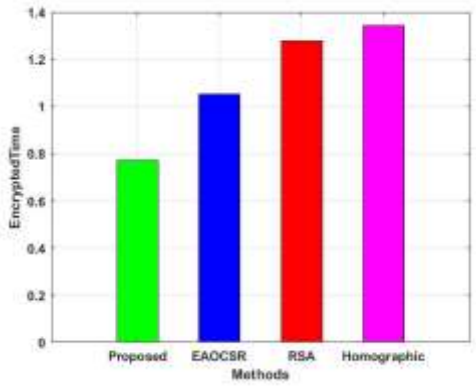


Figure 4 Sensitivity and Specificity Analysis

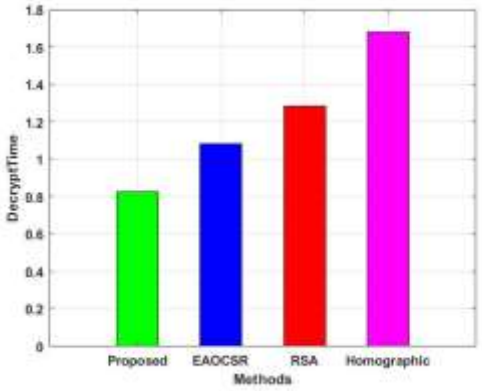
The sensitivity and specificity analysis of the suggested and current algorithms is shown in Figure 4. The statistic known as sensitivity assesses a model's capacity to forecast true positives for each accessible category. The statistic known as specificity assesses a model's capacity to forecast true negatives for each accessible category. Here, compared to other current approaches and the suggested methodology, the performance of the present ANN is very poor. However, the suggested strategy outperforms the current research approaches in terms of both measures.

4.2 Performance Analysis for Secure Data Transmission

According to encryption time and decryption time, the proposed CDFPCC is compared in this section to the existing Energy-Aware Optimal Clustering and Securing Routing (EAOCSR) approach, which uses Log-based Improved Elliptic Curve Cryptography (LIECC), Rivest, Shamir, Adleman (RSA), and Homographic algorithms.



(a)



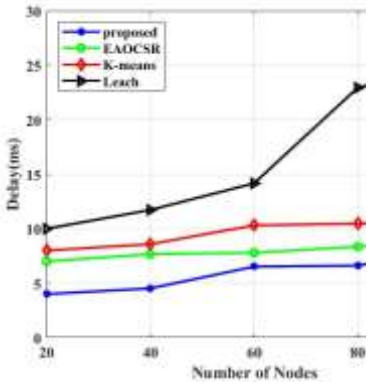
(b)

Figure 5 (a) Encryption Time (b) Decryption Time Analysis of the Proposed and Existing Algorithms

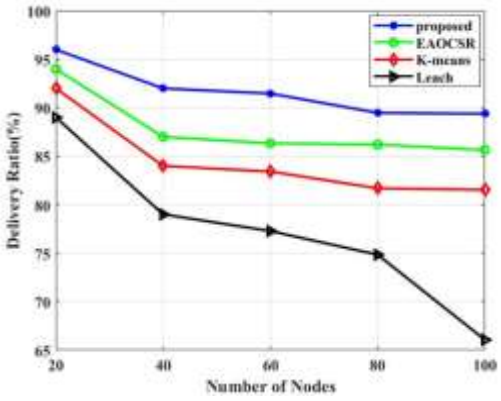
Figure 5 analyzes the secure data transfer to the BS using a cryptographic technique. The encryption time is examined in Figure 5(a). The encryption time indicates how long it takes to convert plaintext to cipher text, while the decryption time indicates how long it takes to reverse the process. The system is referred to as being efficient if it requires less time. On this basis, the conventional technique takes longer than the suggested method to encrypt the data, which is less than 0.8 seconds. Similar to Figure 5(a), Figure 5(b) shows the decryption time. The suggested method takes less time than the current study methodologies.

4.3 Performance Analysis for the Overall System

Here, the delay, delivery ratio, energy consumption, residual energy, and throughput of the proposed ETHOEHO are compared with those of the current EAOCSR, K-Means method, and LEACH.



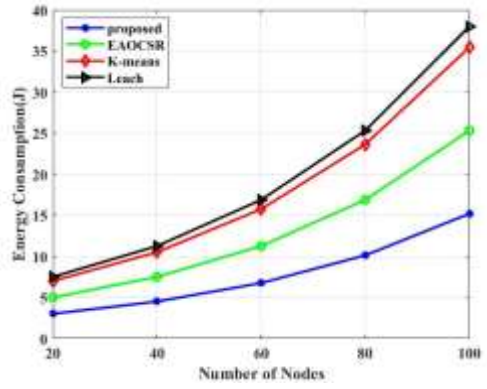
(a)



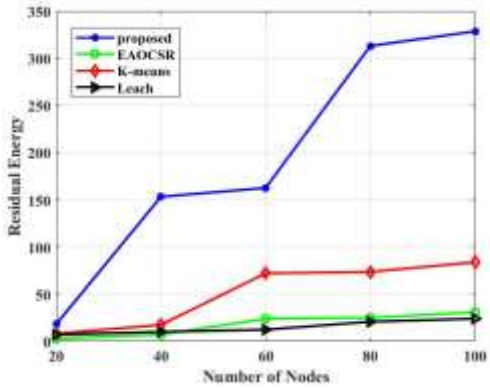
(b)

Figure 6 (a) Delay and (b) Delivery Ratio

With regard to Figure 6(a) delay and Figure 6(b) delivery ratio, the performance of the suggested technique is compared to the present approach-based transmission. In terms of node count, both metrics are analyzed. The performance varies depending on the number of nodes. The suggested solution and the current approaches both saw an increase in latency as the node count rows. Based on the delay measure, the LEACH performs worse than the currently used techniques and the suggested method. The suggested approach has a greater delivery ratio. The suggested system performs better as a result of the approach's consideration of trust metrics.



(a)



(b)

Figure 7 (a) Energy Consumption and (b) Residual Energy

The comparison between the suggested technique and the current strategy is shown in Figure 7. The analysis of the energy usage during data transmission may be seen in Figure 7(a). The suggested solution has a very low energy need. The residual energy of the suggested and current approaches is analyzed in Figure 7(b). Based on this parameter, the suggested technique has more residual energy than the current methods.

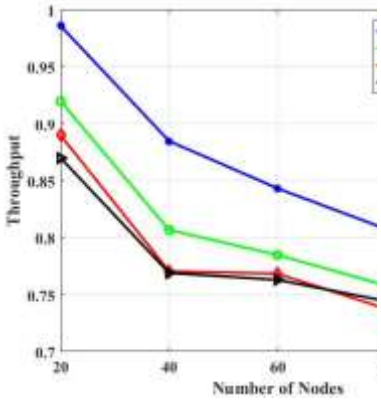


Figure 8 Throughput Analysis

The throughput comparison between the suggested technique and the currently used research approaches is shown in Figure 8. Network throughput in data transmission refers to the volume of data successfully sent from one location to another in a certain length of time. Here, additional data is provided to the base station depending on the suggested technique. However, the suggested technique is more efficient than the current strategy based on data transfer.

5. CONCLUSION

In this study, ETHOEHO, a hybrid Osprey-Elephant Herding Optimizer algorithm, an energy-conscious and trust-based routing protocol for wireless sensor networks, is developed. Here, both the direct and indirect trust assessments are taken into account, and the cluster formation, cluster head selection, and best route are chosen based on the trust values. Finally, an improved technique is used to securely communicate the detected data to the BS. The effectiveness of the suggested methodology is evaluated using the current research methodologies. On the basis of precision, recall, accuracy, F-Measure, sensitivity, and specificity metrics, the suggested technique is contrasted with the current BDSAF-DLNN, ANN, and SVM during the optimum route selection phase. The suggested achieves about 0.95 accuracy and performs better than the previous proposal based on all measures. Additionally, the suggested algorithm achieves a superior result than the current research techniques when the secure data transmission utilizing the proposed cryptographic algorithm

is compared to the existing algorithms. The study then yields improved results based on the whole system analysis. However, this study does not automatically identify the malicious nodes. Future study may be expanded to take malicious node identification into account.

REFERENCES

1. Qianao Ding, Rongbo Zhu, Hao Liu, and Maode Ma, "An overview of machine learning-based energy-efficient routing algorithms in wireless sensor networks", Electronics, vol. 10, no. 13, pp. 1539, 2021.
2. Wooseong Kim, Muhammad Muneer Umar, Shafiullah Khan, and Muhammad Altaf Khan, "Novel Scoring for Energy-Efficient Routing in Multi-Sensored Networks", Sensors, vol. 22, no. 4, pp. 1673, 2022.
3. Zain ul Abidin Jaffri, Muhammad Asif, Wali Ullah Khan, Zeeshan Ahmad, Zain ul Abiden Akhtar, Kalim Ullah, and Md Sadek Ali, "TEZEM: A new energy-efficient routing protocol for next-generation wireless sensor networks", International Journal of Distributed Sensor Networks, vol. 18, no. 6, pp. 15501329221107246, 2022.
4. Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb, and Abdul Waheed Khan, "A trust aware routing protocol for energy constrained wireless sensor network", Telecommunication Systems, vol. 61, pp. 123-140, 2016.
5. PC Srinivasa Rao, Prasanta K. Jana, and Haider Banka, "A particle swarm optimization based energy efficient cluster head selection algorithm for wireless sensor networks", Wireless networks, vol. 23, pp. 2005-2020, 2017.
6. Kalpna Guleria, and Anil Kumar Verma, "Comprehensive review for energy efficient hierarchical routing protocols on wireless sensor networks", Wireless Networks, vol. 25, pp. 1159-1183, 2019.
7. Tayyab Khan, Karan Singh, Mohd Hilmi Hasan, Khaleel Ahmad, G. Thippa Reddy, Senthilkumar Mohan, and Ali Ahmadian, "ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs", Future Generation Computer Systems, vol. 125, pp. 921-943, 2021.
8. Nagesh Kumar, and Yashwant Singh, "An energy efficient and trust management based opportunistic routing metric for wireless sensor networks", In 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), IEEE, pp. 611-616, 2016.
9. Khalid Haseeb, Naveed Islam, Ahmad Almogren, Ikram Ud Din, Hisham N. Almajed, and Nadra Guizani, "Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs", IEEE Access, vol. 7, pp. 79980-79988, 2019.
10. Gobi Natesan, Srinivas Konda, Rocío Pérez de Prado, and Marcin Wozniak, "A Hybrid Mayfly-Aquila Optimization Algorithm Based Energy-Efficient Clustering Routing Protocol for Wireless Sensor Networks", Sensors, vol. 22, no. 17, pp. 6405, 2022.
11. Youjia Han, Huangshui Hu, and Yuxin 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.
12. Munuswamy Selvi, K. Thangaramya, Sannasi Ganapathy, Kanagasabai Kulothungan, H. Khannah Nehemiah, and Arputharaj Kannan, "An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks", Wireless Personal Communications, vol. 105, pp. 1475-1490, 2019.
13. Abdulhamid Zahedi, and Faryad Parma, "An energy-aware trust-based routing algorithm using gravitational search approach in wireless sensor networks", Peer-to-Peer Networking and Applications, vol. 12, no. 1, pp. 167-176, 2019.
14. Maryam Hajiee, Mehdi Fartash, and NaisehOsatiEraghi, "An energy-aware trust and opportunity based routing algorithm in wireless sensor networks using multipath

routes technique", Neural Processing Letters, vol. 53, no. 4, pp. 2829-2852, 2021.

15. M. Udhayavani, and M. Chandrasekaran, "Design of TAREEN (trust aware routing with energy efficient network) and enactment of TARF: A trust-aware routing framework for wireless sensor networks", Cluster Computing, vol. 22, no. Suppl 5, pp. 11919-11927, 2019.
16. D. Laxma Reddy, C. Puttamadappa, and H. N. Suresh, "Merged glowworm swarm with ant colony optimization for energy efficient clustering and routing in wireless sensor network", Pervasive and Mobile Computing, vol. 71, pp. 101338, 2021.
17. ThangaramyaKalidoss, Logambigai Rajasekaran, Kulothungan Kanagasabai, Ganapathy Sannasi, and Arputharaj Kannan, "QoS aware trust based routing algorithm for wireless sensor networks", Wireless Personal Communications, vol. 110, pp. 1637-1658, 2020.
18. Subramanian Balaji, E. Golden Julie, and Y. Harold Robinson, "Development of fuzzy based energy efficient cluster routing protocol to increase the lifetime of wireless sensor networks", Mobile Networks and Applications, vol. 24, pp. 394-406, 2019.
19. Nitin Mittal, Simrandeep Singh, Urvinder Singh, and Rohit Salgotra, "Trust-aware energy-efficient stable clustering approach using fuzzy type-2 Cuckoo search optimization algorithm for wireless sensor networks", Wireless Networks, vol. 27, pp. 151-174, 2021.
20. Manisha Rathee, Sushil Kumar, Amir H. Gandomi, Kumar Dilip, Balamurugan Balusamy, and Rizwan 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, 2019.