Journal of
Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777817

AN ENERGY EFFICIENT SECURE ROUTING SCHEME IN WSN USING LEVO AND LIECC APPROACHES

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

Wireless Sensor Networks (WSNs) are emerging as a new area of research in wireless technology. WSN is constructed with more number of inexpensive, tiny sized and battery powered sensor nodes. One of the fundamental challenges for WSN is to achieve reliability with the security of transmitted data in a vulnerable environment against malicious nodes. Many methods are developed by the existing research works but still it has research gap with respect to data transmission and energy consumption. To solve that problem this research methodology proposed Energy - Aware Optimal Clustering and Secure Routing (EAOCSR) approach. Here, the network deployment process is initially carried out and then the cluster is formed by SDM - FCM. From the clustered sensor nodes the cluster head is selected using LEVO approach. Then, nodes attributes are extracted; based on the extracted attributes the best path is selected using BDSAF - DLNN and by the selected path the data is securely transferred to the base station using LIECC algorithm. In experimental analysis, the proposed approach attains better performance than the existing research approaches.

Keywords - Energy-Aware Optimal Clustering and Securing Routing (EAOCSR), Standard Deviation and Manhattan based Fuzzy C - Means Clustering (SDM-FCM), Lion - Energy Valley Optimizer (LEVO), Beta Distribution and Scaled Activation Function based Deep Learning Neural Network (BDSAF - DLNN), and Log based Improved Elliptic Curve Cryptography (LIECC).

1. INTRODUCTION

Over the decades, WSNs become more attentive in the community of the real - world mobile computing environment. In general, WSN is made up of huge count of smaller and cheaper nodes that are capable of sensing, processing and communication [1]. It has widely used in enormous application fields such as military application, tracking and data acquisition in hazardous environments [2]. In WSN, multiple sensor nodes continuously record values to share with sink node via either node-to-node communication or cluster heads. The data is sent from sensor node to cluster head node which are then forwarded to Base Stations (BS) for further communication [3]. A WSN may contain one or more BS's along with some hundreds or even thousands of sensor nodes. The combined use of such a quantity of nodes enables the concurrent acquisition of data related to the ambient conditions at wide areas of interest [4]. Since, the WSNs are expanding drastically, there are many security violations possible in the network during the routing processes such as Sybil attacks, black hole attacks, and selective packet forwarding attacks. The currently available routing algorithm increases the performance of the network with reduced energy, less time and computational cost [5]. On the other hand, there are some fundamental issues, i.e., energy, security, and computational resources preservation. Therefore, WSN needs efficiency as well as security to enable more acceptable applications. In this context, several solutions are available; among them, most of the work suggests the use of network clustering [6]. Many protocols have been designed for WSNs according to the diverse requirements of applications and the multitude of WSNs characteristics. Several surveys that have sought to analyse and classify these routing protocols according to different parameters have been published [7]. There are three basic subsystems of WSN node i.e. processing subsystem for data processing, sensing subsystem for acquiring data and wireless communication subsystem for packet transmission. Including this, energy source is attached to sensor nodes to energy up the sensor node for doing the specific actions [8]. To gather the information from the remote location using a sensing node, WSN uses the various routing methodologies and protocols either in a distributed or coherent fashion, the WSN requires a unique path selection for data forwarding which requires special attention to address the path problems and maintain the same. The importance of maintaining the information in the hard environment is much more needed in the industrial prospective to retain the trust of its stake holders [9]. In order to guarantee the routing security of wireless sensor networks, many researchers have proposed different kinds of secure routing protocols based on cryptography and authentication [10]. But still the challenges are presented.

Problem Statement

Many existing research works are presented for the efficient routing and secure data transmission but still the challenges are not fully resolved. The drawbacks of the existing research work is described as follows,

- The clustering process is done based on single factor in existing research works. The efficiency is based on many factors such as, residual energy, throughput, delay, energy consumption, etc.
- Random distribution of nodes is considered by the existing research works. It leads to an insecure data transmission process.
- Shortest path was not automatic in the existing research so it takes time and may provide error outcome.

To solve those problems of the existing research works, this work proposed an energy efficient secure routing system. The contribution of the research work is described as follows,

- Many factors are considered for the cluster head selection by using LEVO algorithm.
- Security is maintained by the LIECC algorithm during data transmission.
- To select the shortest path by automatic manner using the proposed BDSAF-DLNN approach.

The structure of the presented research is organized as follows: in section 2, the existing research works related with routing is explained, in section 3, the proposed part is explained, in section 4, the experimental analysis of the proposed research is carried out and in section 5 it was concluded with the future enhancement.

2. RELATED WORK

V. Kavidha and S. Ananthakumaran [11] suggested an efficient Enhanced Fuzzy C means and Adaptive TDMA Scheduling (ECATS) method as a protocol to facilitate communication within the network. The Cluster Head (CH) selection was done on the basis of energy to manage the data aggregation among a number of nodes in the network. Here, hybridization of Time Division Multiple Access (TDMA) based Ant Lion Optimization scheduling is introduced for optimal CH selection which is used for better energy efficiency. Finally, ECATS can be done with optimized WSN performance metrics such as packet delivery ratio, throughput, minimum energy consumptions, communication overheads and end to end delay. The execution time was not fully solved because the Ant Lion algorithm had slow convergence speed.

Dongwan Kim *et al.* [12] presented an energy-efficient secure forwarding method that minimizes energy consumption while meeting both security and Quality of Service (QoS) requirements at the same time. To accomplish the goal, the research methodology alternatively uses hop-by-hop security for conserving energy through data aggregation and end-to-end security to satisfy the QoS requirement. The simulation result shows that the method outperforms other scheme in terms of energy efficiency while meeting both QoS and security. Average transmission time was needed to be improved.

R. Hajian and S. H. Erfani [13] developed a Continuous Hybrid and Energy-efficient Secure Data Aggregation (CHESDA) algorithm that trades of between privacy preserving, data integrity, communication overload, delay and accuracy and then chooses the best scenario based on application and importance of the parameters. Here, privacy preserving was maintained by slice-mixing technique. Results of analysis and simulations indicate that CHESDA was more energy-efficient and highly secure with lower communication overhead. The research may be an inefficient because it considered the random distribution of nodes.

Dhanashri Narayan Wategaonkar *et al.* [14] presented a novel approach to Sector Head (SH) selection called Energy-Efficient Reliable Sectoring-Scheme (EERSS). The Cat Swarm Optimization (CSO) based EERSS algorithm was implemented to rank Quality of Service (QoS) parameters, such as network lifetime maximization, with reliability and to minimize energy consumption. A path reliability prediction-based Markov chain model was applied to the CSO-based-EERSS algorithm to achieve results that were superior to that of traditional models. More parameters were not considered so it may be unreliable one.

Liangrui Tang *et al.* [15] recommended Energy Efficient and Reliable routing Algorithm (EERA) based on Dempster–Shafer (DS) evidence theory (DS-EERA). First, DS-EERA establishes three attribute indexes as the evidence under considering the neighboring nodes' residual energy, traffic, the closeness of its path to the shortest path, etc. After establishing the Basic Probability Assignment (BPA) function, the fusion rule of DS evidence theory was applied to fuse the BPA function of each index value to select the next hop. Theoretical analysis and simulation results show that DS-EERA was promising approach, which was effectively prolong the network lifetime.

Fatma H. El-Fouly *et al.* [16] introduced an Efficient Environment-Aware Fusion (E3AF) based reliable routing algorithm named E3AF. The algorithm takes different parameters into consideration, including environmental metrics, energy consumption balance among sensor nodes, and network and data reliability. With extensive experiments, the algorithm was evaluated and proved its efficiency. One of the algorithm drawbacks was the time complexity where it takes more time than the other two algorithms that were compared with.

Sheng Hao *et al.* [17] recommended a Learning Automata (LA) theory based stable and energy-efficient routing algorithm. Firstly, it construct a multi-factors measurement model for sensor nodes, which contains node stability model, energy ratio function, expected harvesting energy model (using Markov decision process method) and direction judgement model. Secondly, with the help of LA theory, it constructs a feedback mechanism to adjust the optimal path. As demonstrated in simulation experiments, the presented approach achieved the best performance in route survival time, energy consumption, energy balance and acceptable performance in end-to-end delay and packets delivery ratio. The congestion problem was occurred during the process of approach.

Wei Feng *et al.* [18] developed a Joint Power Allocation and Secure Routing Strategy (JPASR) to maximize the Routing Secure Connection Probability (RSCP) under the constraint of power. In the downlink, an Energy-First Multi-point relays Set Selection mechanism (EFMSS) was designed to choose the backbone nodes to broadcast messages, and the backbone nodes were taken up by the same level-by-level sleeping scheduling method as the uplink transmission. Extensive simulations results demonstrate that the energy saving and security performances of the method were superior to the existing ones.

Farman Ullah *et al.* [19] recommended a new Energy Efficient and Reliable Routing Scheme (ERRS) to enhance the stability period and reliability for resource-constrained Wireless Body Area Network (WBAN). ERRS comprises two novel solutions, namely, the Forwarder Node Selection and Forwarder Node Rotation techniques. The ERRS showed an improvement of 26% over the benchmark protocol in terms of network stability and throughput. Whereas, the end-to-end delay of the proposed ERRS was improved by 17% and 40% than by other protocols, respectively, which proves ERRS to be an efficient and reliable routing solution for WBANs. Scalability and mobility issues were presented in this approach.

S. Prithi and S. Sumathi [20] presented a novel Learning Dynamic Deterministic Finite Automata (LD^2FA). The data transmission was done in an energy efficient manner through the optimal path. Routing through optimal path improves the overall performance of the sensor network and it was examined through various metrics such as energy consumption, throughput, network lifetime, alive and dead nodes. The performance is evaluation shows that the approach attains better performance than the existing research methodologies.

3. PROPOSED ENERGY - AWARE OPTIMAL CLUSTERING AND SECURE ROUTING (EAOCSR) SYSTEM FOR WSN

There has been plenty of interest in building and deploying sensor networks. WSN is a collection of a large number of small nodes which acts as routers also. These nodes carry very limited power source which is non-rechargeable and non-replaceable which makes energy consumption a significant issue. Energy conservation is a very important issue for prolonging the lifetime of the network. As the sensor nodes act like routers as well, the determination of routing technique plays a key role in controlling the consumption of energy. Existing research works focus on the energy efficient routing system for WSN. But still many challenges are presented. To solve those research problems this research methodology proposed Energy - Aware Optimal Clustering and Secure Routing (EAOCSR) system for WSN. The proposed methodology consists of six phases that are network formation and node deployment, cluster formation by SDM-FCM, cluster head selection by LEVO, node attribute extraction, path selection using BDSAF-DLNN, secure data using LIECC. The block diagram for the proposed research methodology is shown in Figure 1.

3.1 Network Formation and Node Deployment

Initially, the network is formed which is composed of a finite set of sensor devices geographically distributed in a given indoor or outdoor environment. Then, the node deployment process is carried out. Node deployment means sample data communication between each nodes before real-time data transmission for gathering detail about the node information. The sensor nodes are expressed as follows,

$$\alpha_S = \{\alpha_1, \alpha_2, \alpha_3, ..., \alpha_n\} \text{(or) } \alpha_S = \alpha_i,\ i = 1,2,.....n \tag{1}$$

Here, α_S specifies the set of sensor nodes, and α_n indicates the n-number of sensor nodes presented in the network.

3.2 Cluster Formation

After network formation, the cluster is formed by using the Standard Deviation and Manhattan based Fuzzy C-Means Clustering (SDM-FCM). FCM is an unsupervised clustering algorithm. The clusters are formed according to the distance between data points and the cluster centres are formed for each cluster. The main reason for choosing FCM is it gives flexibility. But it has random centroid selection which may provide an inaccurate clustering output and it uses the Euclidean distance which is not support for the large amount of data. So, here the centroid is selected by calculating standard deviation between each data point and maximum deviated input node is considered as the centroid and this research uses the Manhattan distance instead of Euclidean distance.

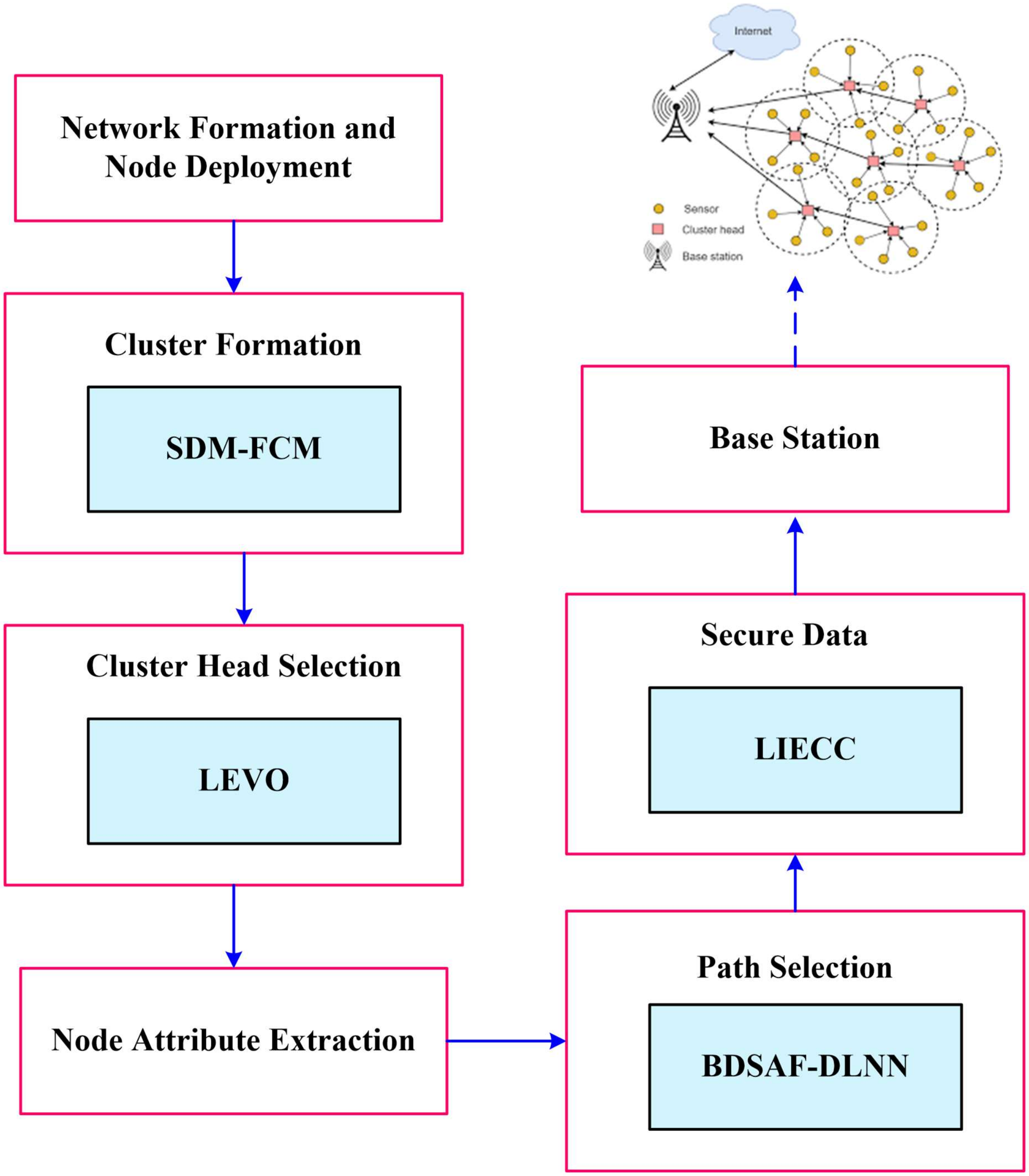


Figure 1 Block Diagram for the Proposed Methodology

The purpose of the cluster formation in this protocol is to minimize the following objective function (F_o):

$$F_o = \sum\sum D_{uv}^{l} T_{uv} \tag{2}$$

Where, D_{uv}^{l} is node v's degree of belonging to cluster u, l is the any real number greater and T_{uv} is the distance between node. First, the centroid point is selected by calculating standard deviation between nodes which expressed as follows,

$$G_i = \sqrt{\frac{\sum \alpha_S - \mu}{\alpha_n}} \tag{3}$$

Where, G_i specifies the cluster centre, and μ indicates the mean value. After the calculation of centre vector the distance matrix is calculated based on Manhattan distance calculation this is given as follows,

$$T_{uv} = |G_{i+1} - G_i| + |\alpha_{i+1} - \alpha_i| \tag{4}$$

Then, update the partition matrix for the j^{th} step is derived as follows,

$$D_{uv}^{l} = \left(1 \Big/ \sum (T_{uv}/T_{sv})^{2/l-1} \right) \tag{5}$$

Where, s denotes the iteration step. The FCM process is repeated until it converges. In this way the cluster is formed. The formed cluster is denoted as,

$$H_S = \{h_1, h_2, h_3, ...h_n\} \text{ (or) } H_S = h_i, \;\; i = 1,2,.....,n \tag{6}$$

Where, H_S indicates the formed cluster sets and h_n defines the n-number of clusters.

3.3 Cluster Head Selection

Here, the cluster head is selected from the formed cluster using Lion-Energy Valley Optimizer (LEVO). The lion optimization algorithm is developed based on the lions' social behaviour, which is to be the strongest in every generation. It searches an optimal solution based on two unique lions' behaviours, namely territorial defence and territorial takeover. Territorial defence happens between the occupant males and wandering males while, the territorial takeover happens between the old resident male and new mature resident male. But, it has the local optimum problem for complex data which may increase the poor searching capability. To solve that problem, this research methodology updates the position by using the energy valley optimization process. The proposed algorithm provides a global search with quick convergence rate. The proposed method has a high LOA search efficiency and a dynamic EVO capability that extends the life of sensor nodes. Here, sensor nodes of each cluster are considered as the lion. The first step of the lion optimization algorithm is to randomly generate population over the solution space. Every solution is represented by:

$$I_p = \{e_1, e_2, ..., e_n\} \tag{7}$$

Where, e_n specifies the dimensional space. The ratio of nomad lions is $\%n$ generated randomly and the rest of the population is resident lions. Then, the fitness is evaluated for the proposed research methodology which considers the maximum amount residual energy (r_e) and throughput (t_p).The fitness function (F_t) is mathematically defined as follows,

$$F_t = \max (r_e, t_p) \tag{8}$$

After that the hunters are divided into three sub groups randomly. Group with highest cumulative members' finesses is considered as Center and the other two groups consider as two wings. Best 6 prides are taken as the centre wing, and the rest of the prides are divided for the other two wings. A dummy prey is considered in centre of hunters in the following equation:

$$D_p = \frac{\sum_{i=1}^{n} O_i}{N(O_i)} \tag{9}$$

Where, D_p denotes dummy prey, and $N(O_i)$ indicates the total nodes. Throughout hunting, if a hunter improves its own finesses, D_p will escape from hunter and new position of D_p^{new} is obtained by the help of updation procedure of the energy valley optimization which is expressed as follows:

$$D_p^{new} = D_p + \left(\eta_d \times VV_s - \eta_d \times VV_{ng}\right) \tag{10}$$

Where, D_p is the current position, VV_s is the position vector of the particle with the best stability level, η_d denotes the random value which ranges from 0 to 1, and VV_{ng} is the position vector of the neighbouring particle. The new positions of hunters which are belonging both left and right wing are generated as follows:

$$P(O_i)^{new} = \begin{cases} \eta_d\left(\left(2 * D_p - P(O_i)\right), D_p\right), & \left(2 * D_p - P(O_i)\right) < D_p \\ \eta_d\left(D_p, \left(2 * D_p - P(O_i)\right)\right), & \left(2 * D_p - P(O_i)\right) > D_p \end{cases} \tag{11}$$

After that the prey position is presented at centre wing then the new position of the hunters is derived as follows,

$$P(O_i)^{new} = \begin{cases} \eta_d\left(P(O_i), D_p\right), & P(O_i) < D_p \\ \eta_d\left(D_p, P(O_i)\right), & P(O_i) > D_p \end{cases} \tag{12}$$

The suggested technique can be used to accomplish a variety of goals, including delay reduction and energy maximisation, depending on the intra- and inter-distances between cluster heads and nodes. As was previously mentioned, the suggested method combines the LOA and EVO searching behaviours. In other words, the suggested method can remove negative search ability while taking use of increased search ability for convergence. A female lion's new position may thus be described as follows:

$$FL' = FL + 2G \times \eta_d \{S_1\} + w(-1,1) \times \tan(\theta) \times G \times \{S_2\} \tag{13}$$

Where, FL' represents the new position of the female lion, FL specifies the female lion, G shows the distance between the female lion's position and the selected point chosen by tournament selection among the pride's territory, $\{S_1\}$ is a vector which its start point is the previous location of the female lion, and its direction is toward the selected position, and $\{S_1\}$ which is perpendicular to $\{S_1\}$. Then, the nomad lions are also hunting the prey. The nomad lions are generated as follows,

$$N_d(O_{ij}) = \begin{cases} O_{ij} & \text{if } \left(\eta_d\right)_j > \left(p_b\right)_i \\ \left(\eta_d\right)_j & \text{otherwise} \end{cases} \tag{14}$$

Where, $N_d(O_{ij})$ is the current position of i^{th} nomad lion, j is the dimension, $(\eta_d)_j$ is a uniform random number within [0, 1], and $(p_b)_i$ is a probability that is calculated for each nomad lion independently.

Then, mating process is carried out. Mating is an essential process that assures the lions' survival, as well as providing an opportunity for information exchange among members. The mating operator is a linear combination of parents for producing two new offspring. For the mating process two offspring process is derived which is given as follows,

$$og_j^1 = \tau * FL_j + \sum \frac{1-\tau}{\sum Z_i} * ML_j * Z_i \tag{15}$$

$$og_j^2 = (1-\tau) * FL_j + \sum \frac{\tau}{\sum Z_i} * ML_j * Z_i \tag{16}$$

Where, j is the dimension, Z_i equals 1 if Lions are selected for mating, otherwise it equals 0, ML_j indicates the male lion and τ is a randomly generated number with a normal distribution with mean value 0.5 and standard deviation 0.1. The pseudocode for the proposed LEVO is given as follows,

Input: Obtained cluster sets h_i

Output: Selected cluster head l_j

Begin

Initialize population, fitness, iteration Itr and maximum iteration $\max$

Compute fitness

Set iteration $Itr = 1$

While $(Itr \le \max)$ **do**

Update the new position by, $D_p^{new} = D_p + (\eta_d \times VV_s - \eta_d \times VV_{ng})$

Update the position of hunter by left and right side

If $(2 * D_p - P(O_i)) < D_p$ {

$P(O_i)^{new} = \eta_d((2 * D_p - P(O_i)), D_p)$

} **else** {

$P(O_i)^{new} = \eta_d(D_p, (2 * D_p - P(O_i)))$

} **end if**

Update the position by centre wing

Calculate fitness

Set $Itr = Itr + 1$

End while

Return Cluster head

End

Finally, the obtained cluster heads are expressed as in equation (17):

$$L_D = \{l_1, l_2, \ldots.., l_d\} \text{ (Or) } L_D = l_j \tag{17}$$

Where, L_D defines the obtained cluster head set, and l_d denotes the d-number of cluster heads.

3.4 Node Attributes Extraction

After selection of the cluster head the attributes such as maximum residual energy, minimum distance, mobility of node and hop count of the data transmission between the nodes are extracted which is derived as follows,

$$NA_A = \{NA_1, NA_2, ..., NA_n\} \text{ (or) } NA_i, i = 1,2,....., n \tag{18}$$

Here, NA_A defines the extracted attribute sets.

3.5 Optimal Path Selection

Thus, the extracted attributes are given as input to the Beta Distribution and Scaled Activation Function based Deep Learning Neural Network (BDSAF-DLNN) classifier which predicts the optimal paths. The deep learning neural network learns the attributes better than the other algorithms so that the deep learning neural network is considered. But it has the random dropout layer function thus the random dropout may drop the important layers so that the beta distribution function is used and it has the vanishing gradient problem. To solve that problem this research methodology uses the scaled activation function instead of using normal activation function. In this research approach, the target value is fixed based on the fuzzy logic condition. The structure of the proposed BDSAF-DLNN is shown in Figure 2.

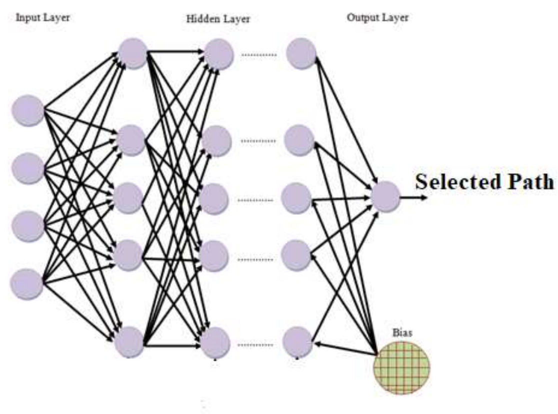


Figure 2 Structure for BDSAF-DLNN

Initially, the input values are given as input to the input layer. Thus, the input layer makes the input for the further processes. Then, the outcome of the input layer is given as input to the hidden layer. The hidden layer unit is calculated as follows,

$$\delta_i = \omega + \sum_{i=1}^{n} NA_i \cdot \rho_i \tag{19}$$

Where, δ_i specifies the hidden layer, ρ_i represents the weight value, and ω indicates the bias value. Here, the dropout layer is performed by calculating the beta distribution function (D_{oo}) which is derived as follows,

$$D_{oo} = \frac{y^{\gamma-1}(1-y)^{\beta-1}}{A(\gamma,\beta)} \tag{20}$$

Where, y defines the variable, γ and β denotes the parameters, and A denotes the gamma function. Then, Compute the output unit O_u which is derived as follows,

$$O_u = \begin{cases} \lambda \delta_i, & \delta_i > 0 \\ \lambda \psi \left(e^{\delta_i} - 1 \right) & \delta_i \leq 0 \end{cases} \tag{21}$$

Where, λ, ψ is the scaled parameters by the help of the fuzzy rule creation the optimal path is selected.

3.6 Secure Data

Here, the sensed data from the sensor nodes are transferred to the base station by the help of secure algorithm. This research methodology uses the Log based Improved Elliptic Curve Cryptography (LIECC) algorithm for secure the sensed data. Elliptic Curve Cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. An elliptic curve is a plane curve defined by an equation of the form,

$$q^2 = p^3 + cp + d \tag{22}$$

Where, c and d are the integers. In a cryptographic process, the strength of the encryption technique depends purely on the mechanism that is employed for the generation of the key. In this research methodology two keys are generated. The private keys are randomly generated which may be provide an insecure output, to solve that problem this research uses the log function for the selected value. Consider the following equation that can generate the public key.

$$CL_c = \log\left(PL_c \right) * R_d \tag{23}$$

Here, CL_c represents the public key, PL_c denotes the private key, and R_d represents the point on the curve. By the help of the those keys the sensed values encrypted which is mathematically defined as follows,

$$CT_1 = r_{num} * R_d \tag{24}$$

$$CT_2 = SD + r_{num} * CT_1 \tag{25}$$

Where, C_1 and C_2 represents the two cipher texts, r_{num} denotes the random number and SD denotes the sensed data. From the obtained path the encrypted sensed values are transmitted to the base station. In the base station side the encrypted values are decrypted which is shown in below equation (26),

$$SD = \left(CT_2 - PL_c \right) * CT_1 \tag{26}$$

With the help of these processes the secure routing in optimal clustering process is carried out. In the further section the performance of the proposed research methodology is analysed.

4. RESULTS AND DISCUSSION

Here, the performance of the proposed energy-aware optimal clustering and secure routing system for WSN is analyzed with the existing research methodology. The proposed research methodology is implemented in the working platform of MATLAB. In Table 1 show that the simulation parameters of proposed system have been determined. The cluster simulation diagram is shown in Figure 3.

Table 1 Simulation of System Parameters

Parameters	Value
Number of nodes	100
Number of rounds	1000
Eo	0.5
Net size	300
Sink x	100
Sink y	100

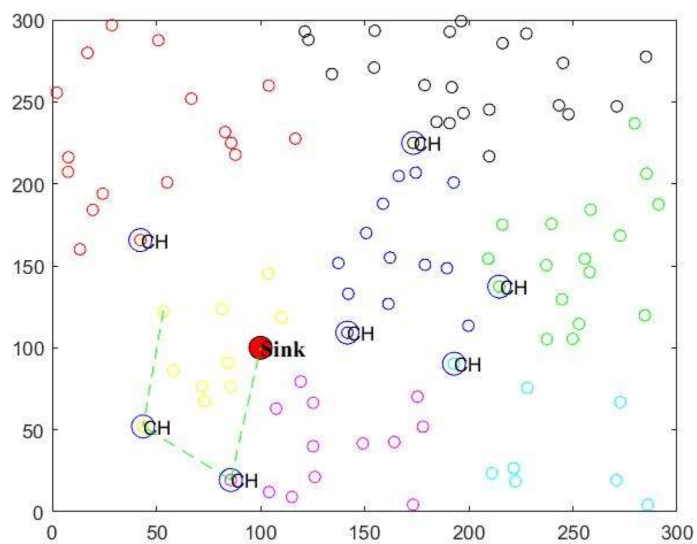


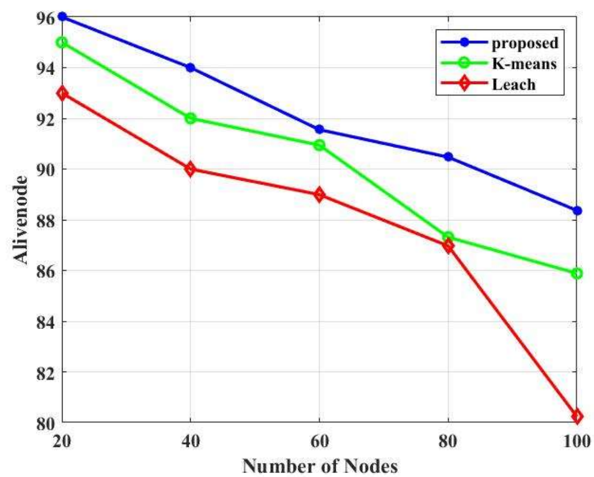
Figure 3 Simulation Diagram for Clustering and Cluster Head Selection Process

4.1 Performance Analysis

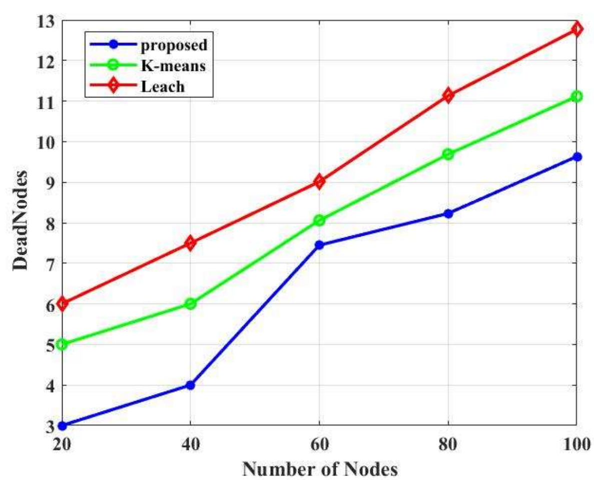
Here, the performance of the proposed research methodology is analysed with the existing research methodologies for the three phases that are, analysis for the cluster formation and cluster head selection, analysis for optimal path selection, and analysis for secure data.

(a) Performance Analysis for the Clustering Process

In this section, the performance of the proposed clustering process based on cluster formation and clustering head selection is analyzed with the existing K-Means algorithm with the LEACH in terms of alive nodes, dead nodes, delay, energy consumption, residual energy, and throughput.



(a)



(b)

Figure 4 Analysis of the Proposed System with the Existing Systems with respect to the (a) Number of Alive Nodes and (b) Number of Dead Nodes

Figure 4 displays the comparative analysis of the proposed research methodology with the existing research methods such as K-Means and LEACH in terms of (a) alive nodes and (b) dead nodes. In Figure 4 (a) the number of alive node is higher for the proposed methodology. In Figure 4(b) the number of dead node is lower for the proposed approach that is, for 40 numbers of nodes only 4 nodes are dead nodes. Similarly, for the remaining number of nodes the proposed methodology achieves better performance. Because, the proposed approach is based on SDM-FCM based clustering and CH selection by the LEVO algorithm.

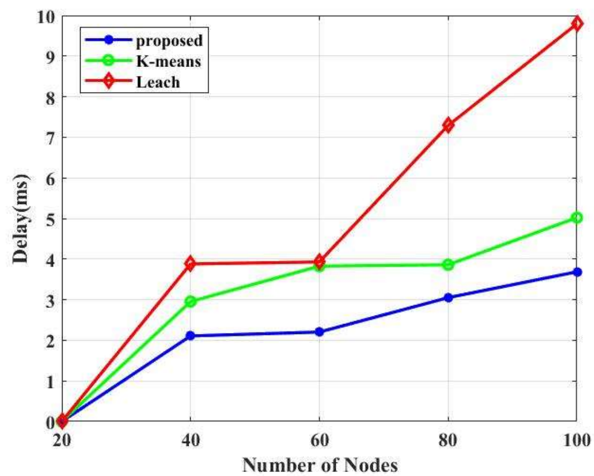


Figure 5 Delay Analysis of the Proposed Approach with the Existing Approaches

Figure 5 shows the delay analysis of the proposed approach with the existing algorithms. The average period occupied to route a data from the source node to target node is deliberated as delay in milliseconds. The delay for the proposed methodology is lesser than the existing work. When the number of node count is 80 then the proposed methodology has 3ms time which is lower than the proposed methodology. Thus, it deduced that the proposed method is highly helpful for the energy aware routing process in WSN system.

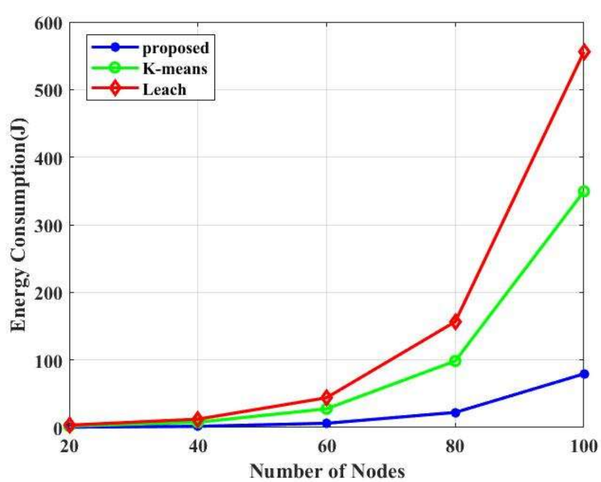


Figure 6 Energy Consumption Analysis

Energy consumption is defined as the sum of receiving energy with the number of nodes and the transmitted energy. Thus, the energy consumption of the proposed and existing research methodology is shown in Figure 6. For the number of nodes, energy consumption has slightly increased, but it is very low while comparing to the existing methodologies. For a better communication, this energy consumption should be low to prevent the node from network failure. The proposed approach attains lower energy consumption than the existing algorithms.

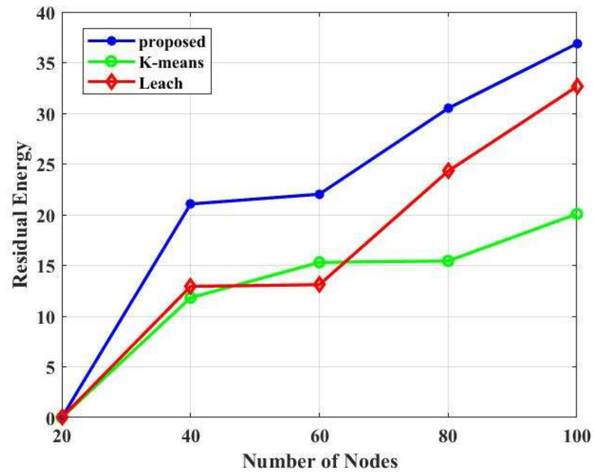


Figure 7 Residual Energy Analysis

Figure 7 displays the residual energy analysis of the proposed approach with the existing approaches. The residual energy for the proposed algorithm is higher at all the node count. For the node count 60 the obtained residual energy is 22 but the existing K-means has 15 and the LEACH has below 15 energy. Thus, it defines that the proposed approach attains better outcome than the existing research methodologies.

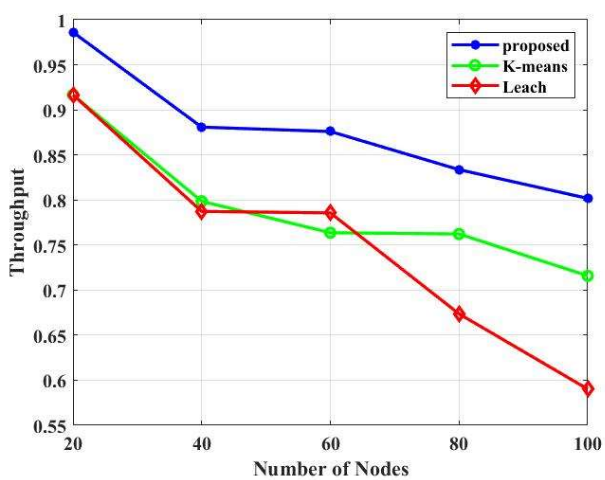


Figure 8 Throughput Analysis

Figure 8 displays the throughput analysis of the proposed and existing research methodologies. Throughput is the number of packets received at the receiver to the packet transmission delay in the process. The above graph represents that the proposed technique attained the highest throughput when compared to other existing techniques. When number of node are 20 the proposed method obtained above 0.95 throughput value. When using K-Means and LEACH, the throughput is obtained above 0.9. The throughput analysis of these two approaches is lesser than the proposed approach. Finally, the proposed technique obtained the highest throughput when compared to other existing methods.

(b) Performance Analysis for the Optimal Path Selection

In this sub-section the performance of the proposed BDSAF-DLNN based path selection is compared with the existing Artificial Neural Network (ANN) and Support Vector Machine (SVM) in terms of accuracy, F-Measure, precision, recall, specificity, and sensitivity.

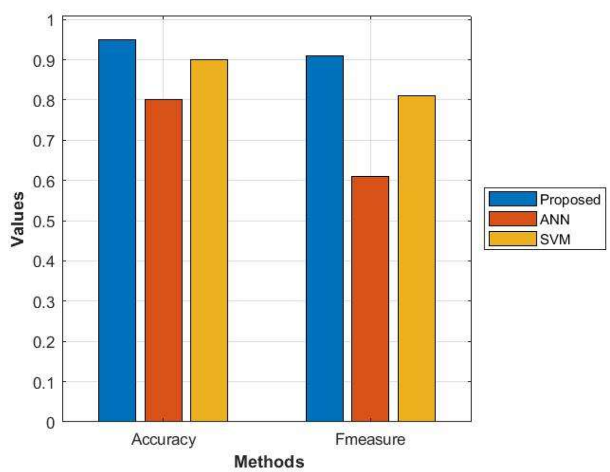


Figure 9 Proposed Path Selection Approach is Compared with the Existing Approaches in Terms of Accuracy and F-Measure Metrics

The accuracy and F-measure analysis of the proposed BDSAF-DLNN based path selection is compared with the existing ANN and SVM approaches with respect to the accuracy and F-Measure metrics. Here, the accuracy of the proposed methodology is above 0.9 but other two methods have 0.8 for ANN and 0.9 for the SVM approach. Thus, it indicates that the proposed method based path selection attains better result than the existing research approaches.

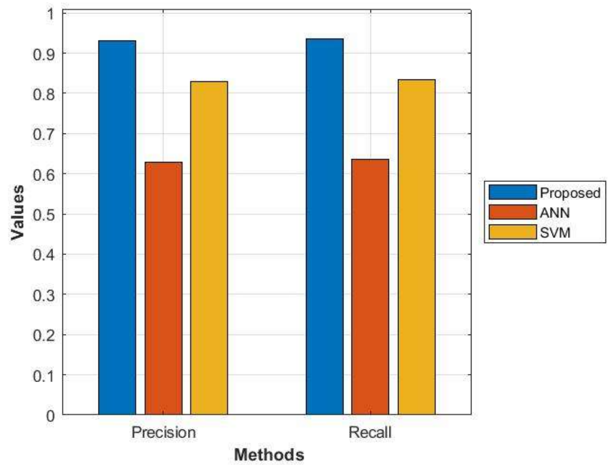


Figure 10 Precision and Recall Analysis

Figure 10 displays the precision and recall analysis of the proposed and existing ANN and SVM approaches. The precision and recall value of the proposed method is above 0.9 but the ANN and SVM attains less precision and recall values when compared to the proposed research approach. Because, the proposed research methodology uses the better activation function with the distribution function based dropout layer.

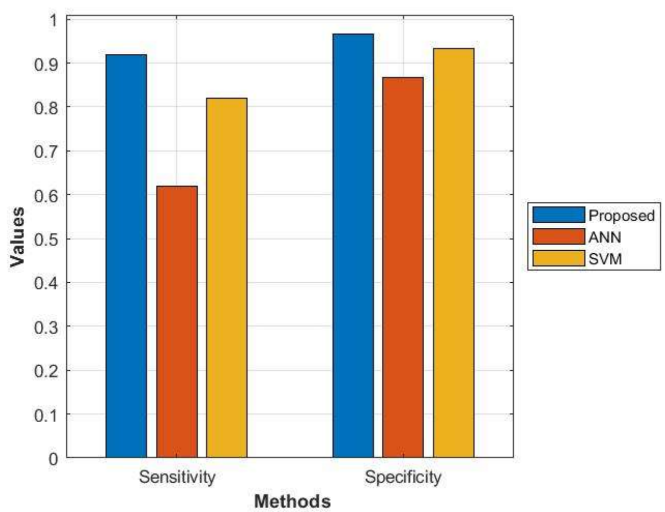
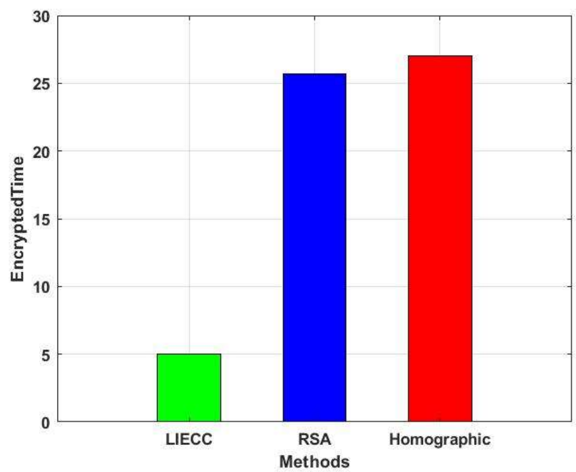


Figure 11 Comparative Analysis of the Proposed Approach with the Existing ANN and SVM based on Sensitivity and Specificity

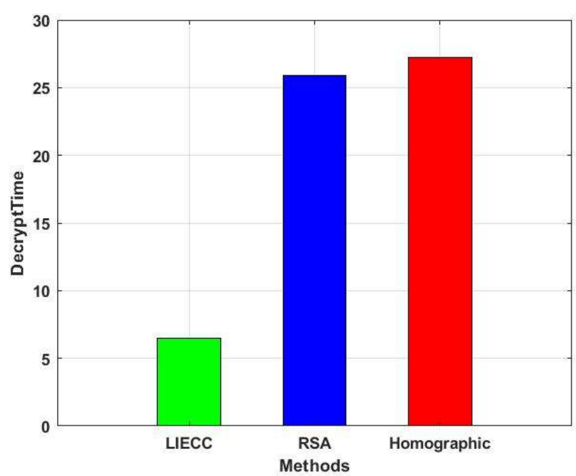
The sensitivity and specificity analysis of the proposed and existing ANN and SVM is showed in Figure 11. Here, the sensitivity and specificity value is worst for the existing ANN when compared with the existing SVM. But the SVM also has lowest sensitivity and specificity value. Thus, the graphical representation shows that the proposed approach achieves better performance than the existing research approaches.

(c) Performance Analysis for the Secure Data

Here, the performance of the proposed LIECC approach based data security is compared with the existing Rivest, Shamir, Adleman (RSA), and Homographic algorithms based on encryption time and decryption time.



(a)



(b)

Figure 12 (a) Encryption Time and (b) Decryption Time Analysis of the Proposed LIECC with the Existing Algorithms

Figure 12 displays the encryption time and decryption time of the proposed and existing algorithms. The encryption time of the proposed method is 5s but the existing algorithm takes more time to encrypt the data. Similarly, with respect to the decryption time the proposed methodology attains better performance than the existing research approaches.

5. CONCLUSION

In this paper the Energy-Aware Optimal Clustering and Secure Routing (EAOCSR) system for WSN is proposed. Here, the cluster formation is done by the SDM-FCM and the cluster head is selected by using the LEVO algorithm. Then, best path for the data transmission is selected by using the BDSAF-DLNN and secure the data by LIECC approach. In experimental analysis the performance of the proposed approach is analyzed with the existing research approaches. The proposed clustering and cluster head selection of the proposed is compared with the existing K-Means and LEACH approaches based on the alive node, dead node, energy consumption, throughput, delay and residual energy. Based on all metrics the proposed research attains higher performance than the existing approaches. Similarly, the proposed path selection approach is compared with the ANN and SVM and the proposed LIECC based secure data process is analyzed with the RSA and homomorphic approach. Overall analysis shows that all the proposed research approaches achieves better performance than the existing research methods. But the research only secure the sensed data not concentrated on the trust level of the node it may also provide security issues. To solve those research problem this paper can be extended by trust level assessment with advanced technique for improve proposed approach.

REFERENCES

1. MallanagoudaBiradar, and Basavaraj Mathapathi, "Secure, reliable and energy efficient routing in WSN: A systematic literature survey", In 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), pp. 1-13, IEEE, 2021.

2. Mohammed Amine Tamtalini, Abdelbaki El Belrhiti El Alaoui, and Abdeslam El Fergougui, "ESLC-WSN: a novel energy efficient security aware localization and clustering in wireless sensor networks", In 2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), pp. 1-6, IEEE, 2020.

3. Maryam Shafiq, Humaira Ashraf, Ata Ullah, and Shireen Tahira, "Systematic literature review on energy efficient routing schemes in WSN–a survey", Mobile Networks and Applications, vol. 25, pp. 882-895, 2020.

4. Christos Nakas, DionisisKandris, and Georgios Visvardis, "Energy efficient routing in wireless sensor networks: A comprehensive survey", Algorithms, vol. 13, no. 3, pp. 72, 2020.

5. A. B. Feroz Khan, and G. Anandharaj, "A cognitive energy efficient and trusted routing model for the security of wireless sensor networks: CEMT", Wireless Personal Communications, vol. 119, no. 4, pp. 3149-3159, 2021.

6. Pooja Gulganwa, and Saurabh Jain, "EES-WCA: energy efficient and secure weighted clustering for WSN using machine learning approach", International Journal of Information Technology, vol. 14, no. 1, pp. 135-144, 2022.

7. Rachid Zagrouba, and Amine Kardi, "Comparative study of energy efficient routing techniques in wireless sensor networks", Information, vol. 12, no. 1, pp. 42, 2021.

8. V. Nivedhitha, A. Gopi Saminathan, and P. Thirumurugan, "DMEERP: A dynamic multi-hop energy efficient routing protocol for WSN", Microprocessors and Microsystems, vol. 79, pp. 103291, 2020.

9. Adam Raja Basha, "Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network", IET Wireless Sensor Systems, vol. 10, no. 4, pp. 166-174, 2020.

10. Huangshui Hu, Youjia Han, Meiqin Yao, and Xue Song, "Trust based secure and energy efficient routing protocol for wireless sensor networks", IEEE Access, vol. 10, pp. 10585-10596, 2021.

11. V. Kavidha, and S. Ananthakumaran, "Novel energy-efficient secure routing protocol for wireless sensor networks with Mobile sink", Peer-to-Peer Networking and Applications, No. 12, pg.no: 881-892 , 2019.

12. Dongwan Kim, Jaekeun Yun, and Daehee Kim, "An Energy-Efficient Secure Forwarding Scheme for QoS Guarantee in Wireless Sensor Networks", Electronics, vol. 9, no. 9, pp. 1418, 2020.

13. Rahman Hajian, and Seyed Hossein Erfani, "CHESDA: continuous hybrid and energy-efficient secure data aggregation for WSN", The Journal of Supercomputing, vol. 77, no. 5, pp. 5045-5075, 2021.

14. Dhanashri Narayan Wategaonkar, S. V. Nagaraj, and T. R. Reshmi, "Multi-hop Energy-Efficient reliable Cluster-based sectoring scheme using Markov chain model to improve QOS parameters in a WSN," Wireless Personal Communications, vol. 119, no. 1, pp. 393-421, 2021.

15. Liangrui Tang, Zhilin Lu, and Bing Fan, "Energy efficient and reliable routing algorithm for wireless sensors networks", Applied Sciences, vol. 10, no. 5, pp. 1885, 2020.

16. Fatma H. El-Fouly, and Rabie A. Ramadan, "E3AF: energy efficient environment-aware fusion based reliable routing in wireless sensor networks", IEEE Access, vol. 8, pp. 112145-112159, 2020.

17. Sheng Hao, Hu-yin Zhang, and Jing Wang, "A learning automata based stable and energy-efficient routing algorithm for discrete energy harvesting mobile wireless sensor network", Wireless Personal Communications, vol. 107, pp. 437-469, 2019.

18. Wei Feng, Feng Wang, Dan Xu, Yingbiao Yao, Xiaorong Xu, Xianyang Jiang, and Mingxiong Zhao, "Joint energy-saving scheduling and secure routing for critical event reporting in wireless sensor networks", IEEE Access, vol. 8, pp. 53281-53292, 2020.

19. Farman Ullah, M. Zahid Khan, Mohammad Faisal, Haseeb Ur Rehman, Sohail Abbas, and Foad S. Mubarek, "An energy efficient and reliable routing scheme to enhance the stability period in wireless body area networks", Computer communications, vol. 165, pp. 20-32, 2021.
20. S. Prithi, and S. Sumathi, "LD2FA-PSO: A novel learning dynamic deterministic finite automata with PSO algorithm for secured energy efficient routing in wireless sensor network", Ad Hoc Networks, vol. 97, pp. 102024, 2020.