Secure and energy efficient optimal routing scheme for wireless sensor networks using IBFA and LDCSN-BSHHO algorithms

Edwin Rajesh.A[1], Dr.Ponmuthuramalingam.P [2]
[1]Research Scholar & Asst Prof., Dept.of Computer Science RJD for Collegiate Educatio Bishop Appasamy College of Arts & Science,Madurai. #129, Race Course Road,Coimbatore-641018.
[2]Research Supervisor & Professor RJD for Collegiate Educatio Bishop Appasamy College of Arts & Science,Madurai. #129, Race Course Road,Coimbatore-641018.
[1]edwinrajesh.a@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: Wireless sensors networks (WSN) are very common because of their advancements in a big quantity of applications. The most vital design-goals aimed at WSN are energy efficiency in addition to secured Data Transmission (DT). This paper addresses the energy as well as security issues of the WSN and proposes a secure and energy-aware optimal routing scheme for WSN using learning of dynamic characteristics of sensor nodes with Bidirectional search based Harris Hawk optimizations (LDCSN-BSHHO). The proposed optimal routing is performed utilizing '4' steps: i) clustering, ii) Cluster Heads (CH) selection, iii) data encryption, and iv) routing. Initially, to expand the Network Life-Time (NLT), the Weigh Utility-based Stratified Sampling (WUSS) method clusters the Sensor Nodes (SN). Next, the Elite Opposition and Ranking Mutation based Butterfly Optimization Algorithm (EORM-BOA) method optimally select the CH for the clusters. After that, an Improved Blowfish Algorithm (IBFA) encrypts the Data Packets (DP) to render data security. Finally, the LDCSN-BSHHO sent the encrypted DP to the Base Stations (BS) via the optimum path. It dynamically studies the node's behavior and selects an optimal path utilizing the BSHHO algorithm for data transfer. This kind of energy and security-centered method for WSN routing is labeled as secure and Energy-Aware Routing (EAR) of WSN. The proposed method's outcomes are examined and weighed against the other prevailing techniques, which shows the proposed methods' efficiency for optimal routing and the data's security.

Key words: Wireless Sensor Network (WSN), Sensor Nodes (SNs), Optimal Routing, Energy aware routing, data security, Clustering, CH selection, Harris Hawks Optimization (HHO).

1. INTRODUCTION

The WSN has become one among the hopeful modalities in present times. The detected alterations occurring in the monitored areas are examined by the WSN's environment. Sound, vibration, pressure, humidity, intensity, temperature, and motion are some of the alternations [1]. The sensors of WSN having finite energy and transmission range, which compels them to perform cooperative transmission with the help of various in-between SN [2]. Therefore, the effective usage of the limited energy is obviously of considerable importance in the maintenance of the overall network's stability [3]. Various methodologies, namely clustering, sleep cycle scheduling, routing, incorporation of mobile sink nodes, etc were used to achieve energy preservation [4]. The most preferential techniques through which energy could be conserved to the maximum are clustering along with routing. A fine selection of the CH supports in the longevity network [5]. The entire network is separated into sub-networks named clusters on the hierarchical architectures [6]. The gathering or fusing of data from nodes that belong to a similar cluster is the responsibility of CH, a special node that leads every cluster [7].

The SN is randomly chosen as a CH without considering available resources at present by various clustering techniques [8]. An optimum CH elected utilizing few predefined parameters in a WSN cluster which can be employed for augmenting the communication range along with the NLT [9]. Some of the optimization algorithms for CH selection effectively, namely Cyclic Rider Optimization Algorithm (C-ROA) [10], Monkey-inspired Optimization (MO) [11], Particle Swarms Optimization (PSO) [12], Krill Herds Optimization (KHO) [13], etc are proposed by several papers. These are effective algorithms that might have an early convergence issue. Energy utilization is reduced by single-hoping for small distances but more energy is used by data transmission causing degradation in performance for longer distances. The mechanism that extends the NLT by reduction of the Energy Consumption (EC) in communication is routing.

The network's structure, data sending techniques, node along with link heterogeneity, EC, node mobility, coverage, data aggregation, connectivity together with the quality of service (QoS) issues must be considered by the routing protocol [14] to be an effective and reliable protocol [15]. The utilization of conventional routing protocols aimed at finding the routes on WSN is not effective and could result in disasters on the sensors [16]. Few routing methods centered on node trust relationships [17] were suggested for evaluating the node's reliability and the network security is improved by isolating the malevolent nodes utilizing the comprehensive trust value attained by direct along with indirect trusts through intercommunication among nodes. However, these are not deemed as strict requirements in energy efficiency on account of the limited capability of computing along with

communication of the WSN [18]. Effectual security mechanisms and an optimal EAR scheme in WSN are proposed by this paper.

This paper is categorized as: Section 2 renders the associated works. Section 3 explained the energy proposed and security-aware optimal routing scheme in WSN. Section 4 exhibits the simulation experiments along with results analysis. Section 5 provides the conclusion and directions for further work.

2. RELATED WORK

Deepak Mehta and Sharad Saxena [19] presented a multiple-objective CH-centered EAR algorithm on WSN. The CH was selected centered on efficient Fitness Function (FF)that was created from many objectives to reduce EC and reduced the total dead SN. Sailfish Optimizer (SFO) was utilized to choose an optimal path to sink node for transmission of data after selecting the CH. The system had performed superior to the existent methods concerning EC, throughput, packet delivery ratios, and NLT as shown by the simulation outcomes. But, the mobility-centered thickly distributed WSN was not supported by the system.

Reeta Bhardwaj and Dinesh Kumar [20] suggested the multiple-objectivesFF centered on energy, delay, distance, traffic rate, along with cluster density. The EAR was performed centered on the Multiple-Objective Fractional Particles Lion (MOFPL). The optimal CH was found by the MOFPL algorithm from several CH nodes on the WSN. The optimum routing path was established centered on the multi-objective function. The size of the population together with the nodes of the WSN was varied for performing the simulation of the system. The system had achieved improved results than the best methods, but it had high computational and communication costs as shown by the results.

Prachi Maheshwari et al. [21] recommended an energy-efficient cluster-centered routing protocol for WSN grounded on a Butterfly Optimization Algorithm (BOA) and Ant Colony Optimizations (ACO). An optimal CH as of a collection of nodes was selected by utilizing the BOA algorithm. The node's residual energy, distances to the neighbors, along with distances to the BS, node degree, together with node centrality were employed for optimizing the CH selection. The route betwixt the CH and the BS was identified concerning the ACO algorithm which selected the optimum route grounded on the distance, residual energy, and node degree. The system had greater network performances when weighted against the prevailing algorithms as signified by the results. Satisfactory results were provided by the system albeit it had less performance.

Vinitha et al. [22] introduced a safe and energy-aware multiple-hop routing protocol in WSN grounded on a Taylor-centered Cat Salps Swarm Algorithm (Taylor C-SSA). The energy-efficient CH was initially chosen grounded on the Lower Energy Adaptives Clustering Hierarchy (LEACH) for efficient data transmission. The data over the CH by the SN transmitted the data to the BS through the selected optimal hop. The optimum hop selection was done centered on the Taylor C-SSA. The trust model which included integrity factor, indirect trust, direct trust, along with data forwarding rate was used to perform the security-aware multiple-hop routing. Satisfactory results were given by the system. However, it was not appropriate for multiple-hop routing and also provided less performance as indicated by the system.

Dipali K. Shende and S. S. Sonavane [23] presented a Crow Whale optimizations algorithm (CWOA) for energy along with trust-aware multicast routing in WSN. Initially, the routes were established for evaluating the trust along with the node's energy that was chosen optimally centered on a CWOA. This optimally selected path was employed for transmitting the data, in which energy along with the individual node's trust was updated at the ending of the individual transmission so the secure nodes could be selected that improved the safe communication on the network. The system had provided better performance results with minimum delay, maximum energy, and maximum throughput as shown by the results. However, the CWOA algorithm didn't offer effective routing and it didn't contrast with too many existing methods, so the system's effectiveness was tough to be analyzed.

Deepak Mehta and Sharad Saxena [24] introduced a Fuzzy Multiple-criteria clustering along with Bio-inspired Energy-efficiency Routing to improve NLT, therefore, enhanced the operating time of WSN applications. An Adaptive Fuzzy Multiple-Criteria Decisions-Making (AF-MCDM) that amalgamated Fuzzy-AHP and 'Technique for Order Preferences by Similarity to an Ideal Solutions' (TOPSIS) was then applied for optimum CH selection. The Emperor Penguins Optimization was utilized for finding the optimum route for transmitting the data from CH to sink after selecting the CH. The system had outperformed the contrasting methods on performance metrics as confirmed by the simulation outcomes. Less efficiency was possessed by the system, and it was not appropriate for other sorts of applications like mobile WSN applications.

S. K. Sathya Lakshmi Preeth et al. [25] designated an adaptive fuzzy rule centered on the energy efficient clustering along with the immune enthused routing protocol aimed at WSN. The AF-MCDM was utilized which was an amalgamation of the fuzzy AHP along with TOPSIS aimed at the optimal CH's selection. The criterion of energy status, node location, and QoS impact were the major factors that could affect the CH's selection whilst each criterion contained a few sub-criteria. The immune-enthused optimization technique was utilized forameliorating the data delivery dependability for routing. The cluster-centered routing was an effective manner for decreasing the EC. However, a less number of BS were deemed by the system. Therefore, it had a high load on the CH and it might provide a minimal NLT in WSN.

3. PROPOSED METHODOLOGY

WSN comprises a larger quantity of spatially distributed SN connected via the wireless medium to monitor as well as record the physical information as of the surroundings. In the WSN environment, energy is a chief challenge as the battery-operated SN on the network consumes a huge quantity of energy amid transmission. This energy restraint affects the network life-time. Presently, to ameliorate the NLT, clustering as well as routing algorithms are extensively utilized in WSN. This paper proposes energy and security-aware optimal routing scheme in WSN called LDCSN-BSHHO. Initially, the WSN's SN is framed as a cluster utilizing WUSS. Secondly, the proposed CH algorithm (EORM-BOA) finds the optimum CH as of disparate CH nodes on the WSN. Next, the DP gathered by means of the CH is encrypted utilizing IBFA and send to a BS by means of an optimal path to render security to the cluster data. The route betwixt the CH and the BS is identified by means of utilizing LDCSN-BSHHO; it chooses the optimal route centered on the distance, residual energy, together with node degree. Thus, the work attains energy in addition to security-aware optimal routing on WSN. The proposed work's architecture is exhibited in figure 1.

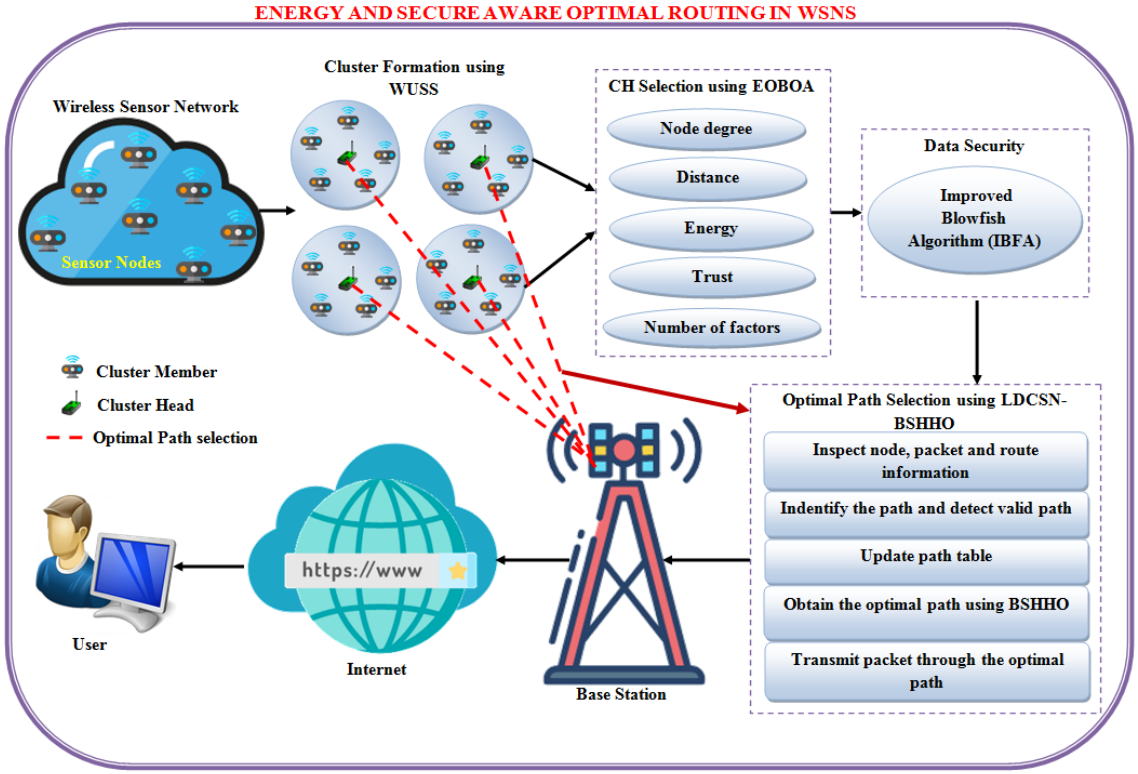


Figure 1: Proposed Architecture

3.1 Cluster Formation

Clustering is basically avitalmethod for expanding the NLT in WSN, in whichit groupsSN into clusters and elects the CH for the entire clusters. This paper utilizes the WUSS method that gauges the weight utility of disparate parameters for clustering. The parameters regarded are transmission radius (node's residual energy) R_N, degree difference (D_{dif}), Sum $(S_{\Delta n})$ of the distances betwixt nodes with all its neighbor's, cumulative time (C_T), Initial

energy (I_E), Signal-to-interferences-plus-noise ratio (S_{INR}), network load (N_{Load}), distance as of SN to base station (D_{SNB}) along with weights $(W_1 - W_8)$.The clustering steps of WUSS is exhibited as,

Step 1: Input the set of SN with $E_{sn}, D_{dif}, S_{\Delta N}, C_T, S_{INR}, N_{Load}, I_E, D_{SNB}, and$ weights

Step 2: Compute the neighbors (node degree) $(N_{\deg})$ of every node N, within R_N utilizing the equation (1)

$$N_{\deg} = \{N | distance(N,N) \le R_N\} \tag{1}$$

Step 3: Compute D_{dif} for every node N and $S_{\Delta n}$ of the distances betwixt nodes N with all its neighbors utilizing equations (2) and (3)

$$D_{dif} = |d_N - Z| \tag{2}$$

$$S_{\Delta n} = \sum_{N \in N_{\deg}} [distance(N,N)] \tag{3}$$

Wherein, d_N signifies the degree of node N and Z implies the maximum node degree

Step 4: Presume the cumulative time C_T wherein node N has acted as a CH. A larger C_T value with node N implies that it has exhausted more resources (such as energy).

Step 5: Presume initial energies I_E of everySN and gauge R_N of every node N subsequent to each communication utilizing the equation (4)

$$R_N = [I_E - E_{tx}(a,d) + E_{rx}(a)] \tag{4}$$

Wherein $E_{tx}(a,d)$ implies the total energy that is spent by means of the transmitter for transmitting a bits of message via distance d and E_{rx} signifies the total energy devoured by the receiver. The E_{tx} and E_{rx} can well be computed as

$$E_{tx}(a,d) = E_{tx \bullet y} + E_{tx \bullet q}(a,d) \tag{5}$$

$$E_{rx}(a) = E_{rx \bullet y} + E_{tx-q}(a,d) \tag{6}$$

Wherein $E_{tx \bullet y}$ signifies the EC of electronic compression, $E_{tx \bullet q}$ implies the amplifier energy, and $E_{rx \bullet y}$ signifies the receiver's EC

Step 6: Compute the SINR utilizing the equation (7)

$$S_{INR}(d) = P_{tx} * G\left(\frac{\beta}{4\pi k}\right)^{\eta} \tag{7}$$

Wherein $S_{INR}(d)$ signifies the received power, P_{tx} implies the transmitted power, G denotes the constant, β signifies the wavelength, k implies the distance betwixt transmitting and receiving node, and η signifies the pre-fined value according to network environment gamut (1–4).

Step 7: Gauge the network load that is influenced by the queue length as well as the load of individual nodes on this queue, which is estimated utilizing the subsequent equation

$$VL_j = H_i + H_{quej} + (\sigma * H_{dropi}) \tag{8}$$

Wherein H_i signifies the total packets in n_i 's queue, H_{quej} implies the total packets in n_j 's queue, σ signifies the retransmitting limit of a single packet, and H_{dropi} signifies the packets dropped by n_i 's because of excessive retransmissions.

Step 8: Compute the distance betwixtBS to everySN by the equation (9)

$$D_{SNB} = \sqrt{(X_{BS} - X_N)^2 + (Y_{BS} - Y_N)^2} \tag{9}$$

Wherein, (X_{BS}, Y_{BS}) and (X_N, Y_N) signify the coordinate positions of BS and everySN,correspondingly.

Step 9: Gauge the combined weight utility values (U_1 & U_2) for every node N as

$$U_1 = u_1(D_{dif}) + u_2(S_{\Delta n}) + u_3(C_T) + u_4(I_E) \tag{10}$$

$$U_2 = \frac{u_5.R_N}{u_6.S_{INR}(d) * u_7.VL_j} \tag{12}$$

Wherein $u_1, u_2, u_3, u_4, u_5, u_6, and\ u_7$ signify the weight values of $D_{dif}, S_{\Delta n}, C_T, I_E, R_N, S_{INR}(d), and\ \mathrm{VL_j}$, whose values lie betwixt 0 and 1.

Step 10: Select the node with a minimum U_1 as well as maximum U_2 as the CH.

Step11: Regard the nodes that are there inside the transmission range as member or follower nodes of that cluster.

Step 13: Create the '1st' cluster of the SN.

Step 14: Eliminate the selectedCHtogether with its neighbors as of the collection of original SN.

Step 15: Re-do the steps 1–14 for the remaining nodes until every node is allotted to a cluster. Subsequent to the execution of these steps consecutively, the disparate clusters are formed and all SN are regrouped into clusters with corresponding CH.

3.2 Cluster Head Selection

Past the clusters' formation, the CH aimed at every cluster is optimally detected by EORM-BOA's aid. Subsequently, the time consumption aimed at choosing the CH is decreased caused by WUSS aimed at carrying out clustering. BOA is the recently established nature stimulated metaheuristics, which imitates the butterflies natural foraging as well as mating behaviour. In the BOA framework, the butterfly's characters are presumed as:

- ✓ Centred on the other butterflies' emanated fragrance, the butterflies have been attracted to each other.
- ✓ Consequently, the butterflies' movement is in a random way or else in the butterfly's direction that emanates higher fragrance.
- ✓ The objective function is utilized to decide the butterfly's stimulus intensity.

EORM-BOA is proposed with the elite opposition (EO) centred learning stratagem and ranking centred mutation (RM) operator. The EO increments the population's diversity and averts the search against stagnating aimed at incrementing the computation accuracy but the RM increments the selection probability. For attaining the optimum solution prevalent in the search space, the EO and RM centred BOA is termed EORM-BOA, which efficiently can balance exploration as well as exploitation. The BOA's fitness or its objective function is enumerated grounded on '4' metrics like remaining energy, node centrality, number of inter-cluster topologies, and trust value.

Step 1: Initialize the butterflies' population utilizing the equation below

$$s_i = \{s_1, s_2, ..s_n\} \tag{13}$$

Step 2: Calculate the individual's fitness utilizing eqn. (14)

$$F = \frac{N_{\deg} + D_{dif} + D_{CHB} + T_v + EC}{N_{fac}} \tag{14}$$

Here, $N_{\deg}$ implies the node degree, D_{dif} signifies the distance betwixt the normal SNs and its CH, D_{CHB} signifies the distance as of the CH to BS, T_v symbolizes the trust value, EC signifies the SNs' consumed energy and N_{fac} implies the number of factors. The T_v and EC are enumerated as:

$$T_v = \frac{P_{cf}}{T_{pf}} \tag{15}$$

$$EC_n = IC_n * EC_{PR} + IC_n * EC_{PA} + EC_{PT}(N_H) \tag{16}$$

Here, IC_n signifies the number of SNs that sue to inter-cluster topology, EC_{PR} implies the EC owing to the received DP, EC_{PA} signifies the EC due to DP aggregation, EC_{PT} represents the EC caused by the transmitted DP, N_H implies the Next-hop, P_{cf} symbolizes the correctly forwarded DPs' value, and T_{pf} represents the totally transmitted DPs' value. The F is calculated by pondering the nodes comprising T_v 's highest values, and the least values of $N_{\deg}$, D_{dif}, D_{SNB} along with EC. The derived FF is utilized aimed at the enumeration of butterfly

fragrance f . The FF is utilized as the butterfly's stimulus intensity; then the butterfly's fragrance is computed for updating its positions.

Step 3: Enumerate the butterfly's fragrance f from the butterfly stimulus intensity function that is equated as:

$$f = (S_m I)^v \tag{17}$$

Here, S_m and v implies the sensory modality as well as the power exponent, which relies on the modality. The values of S_m and v lies betwixt 0 & 1. I signifies the stimulus intensity.

Step 4: Update the algorithm's local search as:

$$s_i^{t+1} = s_i^t + \left(rd^2 \times s_j^t - s_k^t\right) f_i \tag{18}$$

Here, s_j^t and s_k^t signifies the vectors which implies the j^{th} and k^{th} butterflies position at the time t .

Step 5: Update the butterflies' global search position. A step towards the best position $\hat{B}$ centred on the objective function's fitness value is implemented during the global search by the butterfly prior to the eqn. (19) as,

$$s_i^{t+1} = s_i^t + \left(rd^2 \times \widehat{B} - s_i^t\right) f_i \tag{19}$$

Here, s implies a vector which represents the i^{th} butterfly position at the time t , rd signifies the randomly created number that lies betwixt 0 & 1; $\widehat{B}$ implies the best current position. Aimed at enhancing the BOA's global search ability, EO centred learning is engaged which is an effectual search method which increments the population diversity. Past comparing the feasible solution's fitness values, the effective individual is pondered as the elite wave $s_e = \left\{s_{e,1}, s_{e,2}, \ldots\ldots s_{e,D}\right\}$. The wave s_i and elite inverse solution $\left(s_i\right)^*$ are articulated as $s_i = \left\{s_{i,1}, s_{i,2}, \ldots\ldots s_{i,D}\right\}$ and $\left(s_i\right)^* = \left\{\left(s_{i,1}\right)^*, \left(s_{i,2}\right)^*, \ldots\ldots \left(s_{i,D}\right)^*\right\}$, and the formulation is:

$$\left(s_{i,j}\right)^* = x.\left(da_j + db_j\right) - s_{e,j} * \mathrm{f_i} \text{ where } \mathrm{i} = 1,2,\ldots \mathrm{n}, \mathrm{j} = 1,2,\ldots \mathrm{D} \tag{20}$$

Here, n signifies the number of butterflies existent in the population, D implies the search space dimension, $x \in (0,1)$ and da_j and db_j symbolizes the j^{th} decision variable's dynamic boundaries, which is enumerated utilizing the eqns. (21) and (22)

$$da_j = \min\left(s_{i,j}\right) \tag{21}$$

$$db_j = \max\left(s_{i,j}\right) \tag{22}$$

The search space's dynamic boundary replaces the fixed boundary which is helpful for preserving the optimum solution. The inverse solution leaps out $\left(da_j, db_j\right)$and is pondered as the feasible-solution.

$$\left(s_{i,j}\right)^* = rd\left(da_j, db_j\right) * f_i, \text{ if } \left(s_{i,j}\right)^* < da_j or \left(s_{i,j}\right)^* > db_j \tag{23}$$

Step 6: Elect the optimal individual by organizing each butterfly consequent to the relevant fitness values. At first, the population is organized in the ascending order (i.e., as of best to worst) centred on each butterflies' fitness value. An individual butterfly's ranking is articulated as:

$$R_i = P_s - i, \mathrm{i} = 1,2,\ldots . P_s \tag{24}$$

Here, P_s signifies the population's size. The optimum butterfly in the prevalent population acquires the greatest ranking. Past the sorting of each SN's or butterfly's fitness, the i^{th} node's selection probability M_i is:

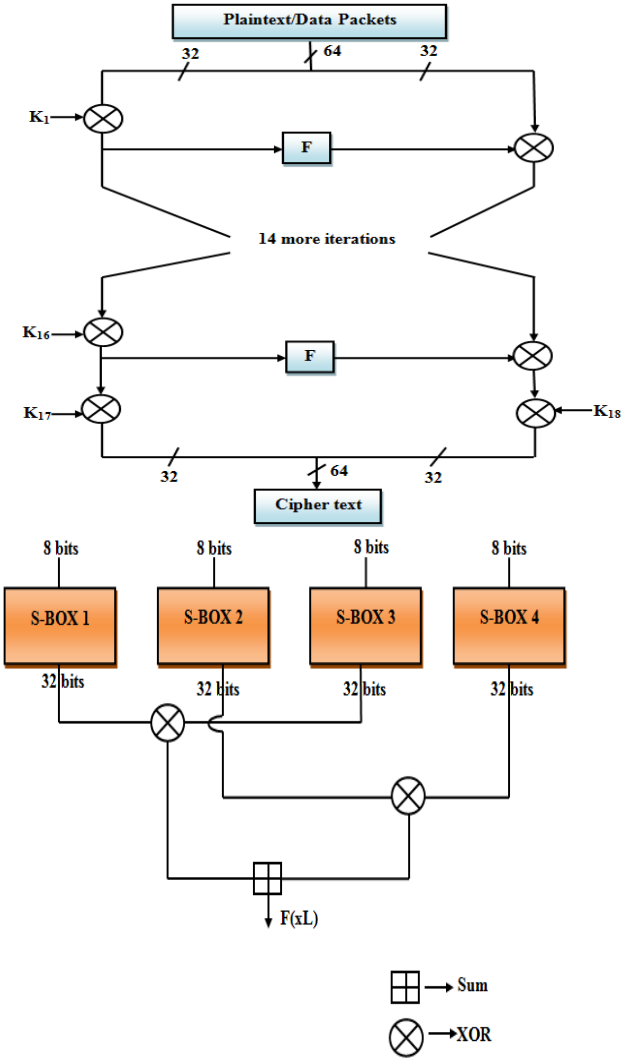
$$M_i = \frac{R_i}{P_s}, \ \mathrm{i} = 1,2,\ldots . P_s \tag{25}$$

The probability that the individual possessing a greater ranking is elected as the base vector or terminal vector present in the mutation operator becomes larger; the objective is to transmit the valuable information as of the present population on to the offspring. The ranking centred mutation operator increments the probability that an excellent individual is elected; this improves the exploitation capability. The elite opposition-centred learning stratagem increments the population's diversity and improves the exploration capability aimed at upgrading the computation accuracy.

3.3 Data Encryption

For the encryptions of SNs' DPs in each cluster, the paper utilized an improved version of the blowfish algorithm (IBFA) for offering security to the SN's data. The alternative technique aimed at the DES Encryption method is Blowfish Algorithm (BFA). It takes the input of '64' bits as well as executes 18 rounds of operations on the inputted data by 18 subkeys (K-array). The Fiestal function is utilized which partitioned a '32'-bit input into '4' bytes and utilizes those as indices into an S-array. For producing the output, the lookup outcomes are summed and XORed. With the constants (i.e.,) the hexadecimal digits of λ, initialization of both arrays are done. Centred upon the user's key, The K-array along with S-array values utilized by BFA is pre-calculated. Effectively, the user's key is transmuted into the K-array and S-array and this procedure is stated as a sub-key generation.

The original function module is ameliorated in IBFA. The S-box 1 along with 2's output is added, and then it is XORed with the S-box 3's output. For obtaining $F(xL)$, XORed output is summed with the S-box 4's output. Here modulo addition is utilized. XOR operations in the original function are accomplished in parallel in the improved function. In parallel, S-box 1 and 3's output and the S-box 2 and 4's outputs are XORed. Then for obtaining $F(xL)$, their outputs are summed. This improves the traditional BFA's complexity and so augmenting the DPs' security effectively. Figure 2 exhibits the BFA round function in addition to the improved Fiestal function's the structure. The IBFA's steps are given as,



(a) BFA (b) Improved function module

Figure 2: Graphical representation of IBFA

✓ With a fixed string, initialization of the K-array along with S-array should be done and this string comprises of hexadecimal digits of k_i.

- ✓ XOR K_1 with the input data's initial 32 bits (DPs), XOR K_2 with the data's second 32-bits, and continues for whole input bits. Carry on the process, Until the whole K -array is XORed with the data bits,
- ✓ Utilizing the subkeys expressed in steps (1) along with (2), the encryption of the whole zero string by the BFA should be done.
- ✓ Replace K_1 and K_2 with the step (3)'s output.
- ✓ Utilizing the BFA, Encrypt the step (3)'s output with the modified subkeys.
- ✓ Replace K_3 and K_4 with step (5)'s the output.
- ✓ By the repeatedly-altering BFA's output, replace every the P-array's entry and after that all '4' S-boxes orderly.

Utilizing LDCSN-BMHHO algorithm, the encrypted DPs (cluster data) are sent to the BS by choosing the optimum path for every CH of the clusters after IBFA encryption.

3.4 Selection of Optimal Routing

The routing mechanisms are vital in WSN since fewer EC, latency, QoS, along with data throughput are offered by them. Utilizing the optimal routing, the DT is carried out and it is initiated by choosing the best paths as of CHs to BS in an optimal manner and it is executed utilizing the proposed BSHHO. A novel approach LDCSN-BSHHO algorithm is proposed for facilitating the effective usage of energy of the nodes, and for improving the NLT. Utilizing Bidirectional Search centred Harris Hawks Optimization (BSHHO) algorithm, LDCSN-BSHHO is proposed that dynamically learns the network environment and optimizes the route. After removing the worst cases, the routing optimization automatically reduces the complexity by choosing the top route. The LDCSN along with BHHO's working is given as below.

3.4.1 LDCSN

The learning of dynamic characteristics of sensor nodes (LDCSN) explores the route betwixt the source (S) and the destination (D) and stores it into path table when the communication is started betwixt the ' S 'and ' D 'node. The individual LDCSN is dynamically built and analyzed for all the route exploration. The LDCSN encompasses 5 major factors that is given as,

$$L_{dstn} = \left\{ f_s, \sum, T_f, z_0, L \right\} \tag{26}$$

Here, the compilation of finite states is signified by f_s, the set of finite input alphabets is represented by $\sum$, T_f implies the transition function, z_0 signifies initial state, L indicates the last state. Each SN in WSN has disparate states that changes as of one state to other state represented as $\{z_0, z_1, z_2, \ldots z_n\}$ and the transitions are given by transition function T_f, z_0 signify the first state and z_n signify the end state (that means the nodes have n -number of states).

$\{p_1, p_2, \ldots p_w\}$ represents the set of paths for the CH routing and the forward path or the reverse path is signified by $F \rightarrow or \, \mathrm{R} \leftarrow$ correspondingly. Utilizing LDCSN function, all this information is automatically learned and the optimum path is identified with the assist of them. The ' T_f ' is activated centred on the node states and the path betwixt ' S ' and ' D '. For updating the information attained by the LDCSN, the LDCSN utilizes the section table (table 1) in the learning process. The updation of the source, intermediate along with destination nodes information is done in the path table for each route discovery. Each time the section table is learned and the path, intermediate nodes and nodes' state values are updated in the table. If the nodes' state in the route is accessible, then the path of that section is recognized and also if it contains the destination node then the transmission is accepted. The section table retrieves the information regarding the node along with path information at a frequent time interval. For checking whether it is valid or not, the section (i.e., the path) is verified.

Table 1: Elements of section table

Elements	***Description***
N_{ID}	Node Id
N_L	Node Location ((x and y co-ordinates)
R_N	Residual Energy
CH_{num}	CH number
D_{ns}	Dead node status
N_{ns}	Neighbor nodes
M_{ns}	Malicious node status
$T_{imestamp}$	Timestamp Information

If it is a valid one then it is denoted as a valid path and it is updated in the path table,. Similarly, the paths (available) for the network is learned initially and utilizing the BSHHO, best (optimal) path is chosen.

3.4.2 BSHHO

An incredible social behaviour in Harris Hawks optimization (HHO) method is pursued by the Harris Hawks aimed at tracking and pouncing on their prey. Looking for the prey, abrupt pounce, and various attacking ways execute the algorithm's explorative and exploitative stages. Harris Hawks are arbitrarily distributed towards the locations waiting for prey utilizing the '2' exploration procedures. In the 1st approach, Harris Hawks' perch on a location pondering other family members' locations, along with the rabbit (prey). In the 2nd approach, the Hawks are waiting upon arbitrary tall trees.

The HHO's fundamental version utilizes the levy random behaviour aimed at electing the finest potential dive. But, levy flight posses demerits like the search area's overflow and the random flights interruption owing to its huge searching steps. Aimed at overcoming these demerits and for improving HHO's local searching ability aimed at optimization issues, a bidirectional search centred HHO termed BSHHO is proposed. This aids to execute the local search in the forward direction and backward direction. Greedy selection is done, whilst choosing the direction. If the solution enhances whilst travelling backwards, the backward traverse is adopted or else forwarded. This modification assists in accelerating HHO's convergence rate. The LDCSN-BSHHO's core target is to decrement the EC of the data transmission as of the source towards the destination and to detect the optimum path as of the source on to the destination. As of the set of potential paths, BSHHO must detect the optimum path centred on each path's total EC. The EC of the path p_1 as of the source i towards the destination j is computed as

$$E(p_1)_{i,j} = \begin{Bmatrix} \infty & \text{j} \notin nx(i) \\ c_{en}(i,j) & \text{OW} \end{Bmatrix} \tag{27}$$

Here, $c_{en}(i,j)$ signifies the energy cost aimed at sending k -bit message at a distance d as of source i towards j, that is articulated utilizing the eqn. (28)

$$c_{en}(i,j) = E_{tx}(t_n,d) + E_{rx}(t_n) \tag{28}$$

Here, $E_{tx}(t_n,d)$ and $E_{rx}(t_n)$ symbolizes the energy dissipated per bit at the transmitter and also at the receiver, that are stated as,

$$E_{tx}(n,d) = R_{\cos t} * t_n + A_f * d^2 * t_n \tag{29}$$

$$E_{rx}(t_n) = R_{\cos t} * t_n \tag{30}$$

Here, $R_{\cos t}$ signifies the circuit energy's cost whilst one bit of data is transmitted or received, t_n implies the number of transmitted data bits, and A_f signifies the amplification factor. HHO's '2' approaches are designed with c 's equivalent chance aimed at each as:

$$p^{t+1} = \begin{cases} p_r^t - r_1 \left| p_r^t - 2r_2 p^t \right| & \text{if } c \geq 0.5 \\ p_{rabbit}(t) - p_m^t - r_3 \left(l_b + r_4 \left(u_b - l_b \right) \right) & \text{if } c < 0.5 \end{cases} \tag{31}$$

Here p^t and p^{t+1} implies the Hawks' position vectors in the present and upcoming iteration. p_r^t signifies a random hawk elected from the population, and $p_{rabbit}(t)$ represents the rabbit's position. c , $r_1, r_2, r_3, and\ r_4$ implies randomly created numbers. l_b and u_b signifies the lower bounds and the upper bounds for producing random locations within the Hawks' home. p_m^t symbolizes the Hawks' mean position in the population that can be equated as:

$$p_m^t = \frac{1}{w} \sum_{i=1}^{w} p_i^t \tag{32}$$

Here, p_i^t signifies each hawk's i^{th} position vector in the population at the iteration t , and w signifies the number of Harris Hawks existent in the population. Centred on the rabbit's escape energy E_E , the algorithm changes as of the exploration to the exploitation segment as:

$$E_E = 2E_0 \left(1 - \frac{t}{M_{it}} \right) \tag{33}$$

Here E_0 implies the initial rabbit's energy that is selected randomly betwixt [−1, 1]. M_{it} signifies the maximal number of iterations. Hawks search for added regions aimed at exploring the rabbit's location whilst $\left| E_E \right| \geq 1$; Or else, the exploitation pace happens. With an equivalent chance c , formulating the success $c \geq 0.5$ or else failure $c < 0.5$ of rabbit escape is performed in the algorithm. Dependant on the rabbit's energy, the Hawks executes a soft $\left| E_E \right| \geq 0.5$ or else hard $\left| E_E \right| < 0.5$ besiege. The soft besiege is formulated as:

$$p^{t+1} = \Delta p^t - E_E \left| R_J * p_{rabbit}(t) - p^t \right| \tag{34}$$

$$\Delta p^t = p_{rabbit}(t) - p^t \tag{35}$$

$$R_J = 2(1 - rd) \tag{36}$$

Here Δp^t signifies the difference amid the hawk's and rabbit's positions, and R_J implies the rabbit's Random jump strength that is drawn utilizing a random number rand. The hard besiege is equated as:

$$p^{t+1} = p^t - E_E \left| \Delta p^t \right| \tag{37}$$

Whilst, $\left| E_E \right| \geq 0.5$ and $c < 0.5$, soft besiege possessing progressive rapid dives is executed as the rabbit can flee successfully. The Hawks can elect the finest potential dive. Bidirectional search is utilized to imitate the prey's leapfrog. This aids to carry out the local search in the forward direction and also in the backward direction. It is speedy that it considerably decrements the amount of essential exploration. For deciding whether the dive is good or bad, the Hawks' upcoming move is estimated utilizing:

$$y = p_{rabbit}(t) - E_E \left| R_J * p_{rabbit}(t) - p^t \right| \tag{38}$$

If the former dive isn't helpful, the Hawks dive employing B pattern as:

$$h = y + s * BS(d) \tag{39}$$

Here, d signifies the problem's dimension and s implies a random vector possessing size d . The Bidirectional pattern (search) is enumerated as

$$BS=\begin{cases} if\left[f\left(p^t+S\right)< f\left(p^t\right)\rightarrow p^t=p^t+S\right] \\ elseif\left[f\left(p^t-S\right)< f\left(p^t\right)\rightarrow p^t=p^t-S\right] \\ otherwise\rightarrow no\,change\,in\,present\,position \end{cases} \tag{40}$$

Here p^t, $f\left(p^t\right), and\ S$ signifies the hawks' current position, objective fitness function value and then the step length. The last soft besiege progressive rapid dives is formulated utilizing:

$$p^{t+1}=\begin{cases} y & \text{if } f(y)< f\left(p^t\right) \\ h & \text{if } f(h)< f\left(p^t\right) \end{cases} \tag{41}$$

Hard besiege with progressive quick dives takes place whilst $\left|E_E\right|\geq 0.5$ and $c<0.5$ as the rabbit do not possess sufficient energy to flee utilizing the Eqn. (40) in which y is articulated utilizing the subsequent equation (41): Figure 3 exhibits the proposed BMHHO's pseudo-code.

$$y=p_{rabbit}(t)-E_E\left|R_J*p_{rabbit}(t)-p_m^t\right| \tag{42}$$

BSHHO algorithm for optimal path selection

Input: Set of available paths
Output: optimal paths of CHs for data transmission

Begin
Initialize the population of w random hawks (available paths) and M_{it}
Compute the fitness of each hawk using equation (27)
Denote the best position of hawk with minimum fitness as p_{rabbit}
$t=1$
While $(t\leq M_{it})$
  Update E_E using equation (29)
  If $\left|E_E\right|\geq 1$
    Update p^{t+1} using equation (27)
  If $\left|E_E\right|<1$
    If $(c\geq 0.5\ \&\&\ \left|E_E\right|\geq 0.5)$
      Update $p^{t+1}=\Delta p^t-E_E\left|R_J*p_{rabbit}(t)-p^t\right.$
    If $(c\geq 0.5\ \&\&\ \left|E_E\right|<0.5)$
      Update $p^{t+1}=p^t-E_E\left|\Delta p^t\right|$
    If $(c<0.5\ \&\&\ \left|E_E\right|\geq 0.5)$
      Update soft besiege with progressive rapid dives $(BS(d))$
    If $(c<0.5\ \&\&\ \left|E_E\right|\geq 0.5)$
      Update hard besiege with progressive rapid dives
    End if
    End if
    End if
    End if
  End if
  If $(\text{fitness}\left(p^{t+1}\right)< fitness(p_{rabbit}))$
    Update $p_{rabbit}=p^{t+1}$
  $t++$
  End if
Return p_{rabbit} position
End while
End

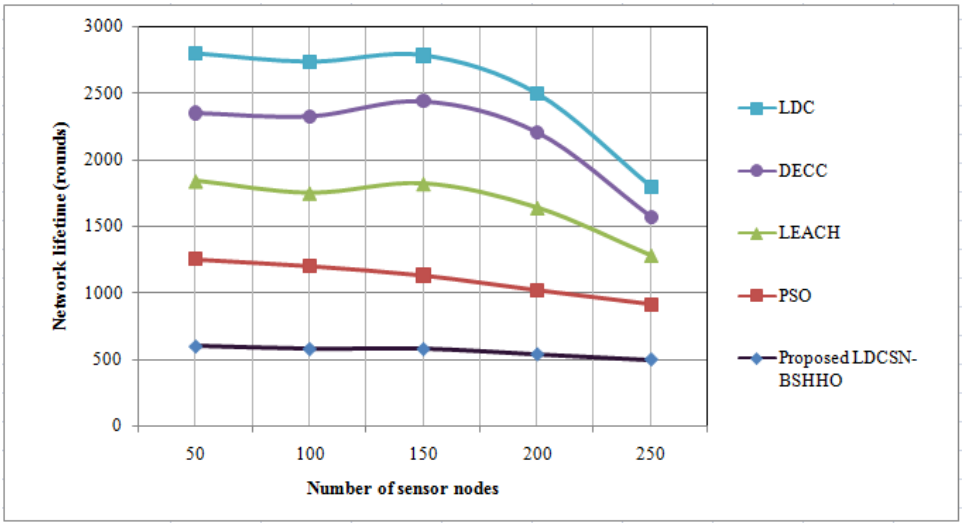
Figure 3: Pseudo-code for the proposed BMHHO

3. RESULT AND DISCUSSION

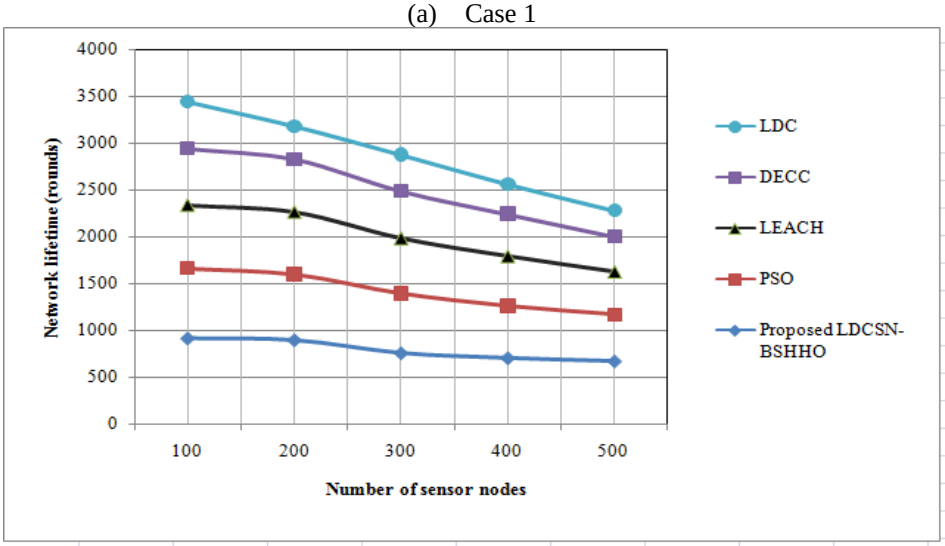
In the NS2 with simulation parameters namely network area: 500 ∗ 500 m^2, Initial energy: 2.0 J, simulation rounds: 200–5000, number of SNs: 50-250 nodes, communication range: 250m, message size: 200bits, packet size: 4000bits, transmitter and receiver electronics: 50nJ/bit, along with transmitter amplifier: 100pJ/bit/m^2, the proposed secure and energy-aware LDCSN-BSHHO is executed. Utilizing several performance metrics, here the

proposed method's outcomes are analyzed. Regarding the NLT (number of rounds), PDR, (%), energy consumption (EC) (Joules), throughput (bps), along with delay (seconds), proposed routing algorithm's outcomes are analogized with the prevailing algorithms namely PSO, LEACH, DEEC, along with LDC. Concerning Encryption Time (ET) along with Decryption Time (DT) (ms), the proposed IBFA is analogized with the prevailing BFA, RSA, along with Advanced Encryption Standard (AES).

By simulating two disparate cases (case 1 and case 2), the experiment is assessed for EC along with NLT. Both the cases take the same network parameters but the BS's position is the only difference. The BS has been located at (500,250) i.e., in a side of the region in case-1 and the BS is located at (250,250) i.e., in the centre of the region in case-2. Figure 4 portrays the techniques' NLT.



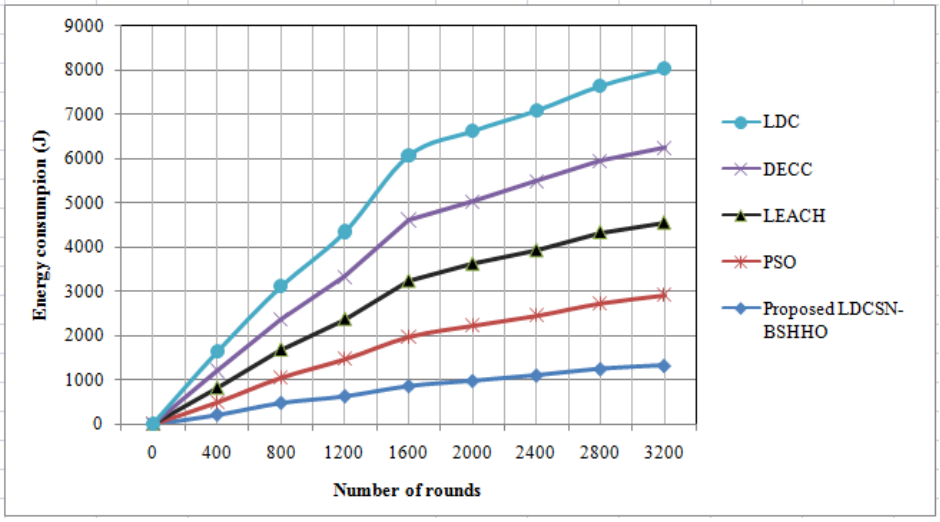
(a) Case 1



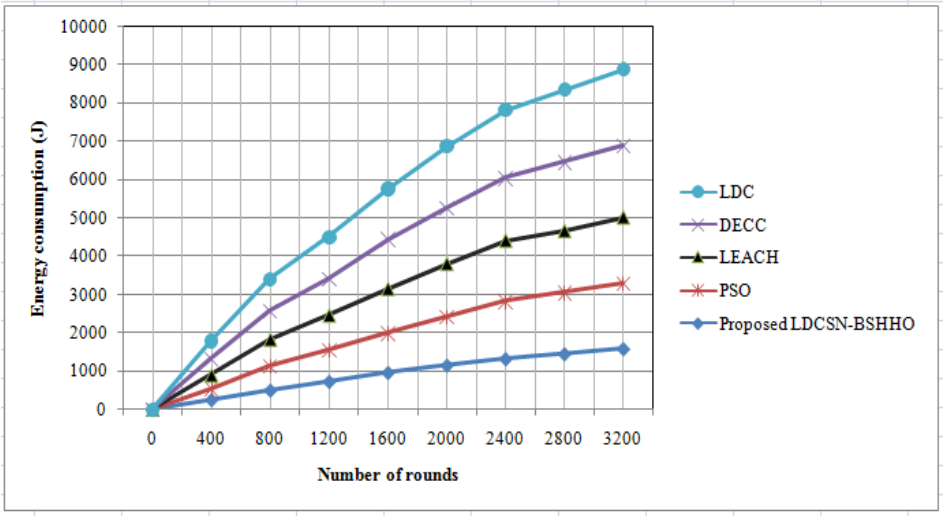
(b) Case 2

Figure 4: Network Lifetime of the techniques

Figure 4 (a) exhibits techniques' NLT (case 1). Regarding NLT, when the proposed network model (LDCSN-BSHHO)'s nodes are 50, then the initial node dies by 600th round and for a network with 100 nodes, the initial node die by 580th round. The initial node's energy exhaustion occurs by 500th round which is superior when analogized with the prevailing algorithm namely, PSO, LEACH, DECC, along with LDC. Figure 4 (b) evinced that the proposed LDCSN-BSHHO offers superior enhancement in NLT when analogized with others. When the node count is 50, it died at the 915th round whereas the node dies in minimum rounds in others. The LDCSN-BSHHO attains better outcomes for both the cases and it achieves longest NLT when analogized with others. Figure 5 exhibits the techniques' EC for both cases (case 1 and case 2).



(a) Case 1



(b) Case 2

Figure 5: Energy Consumption of the techniques

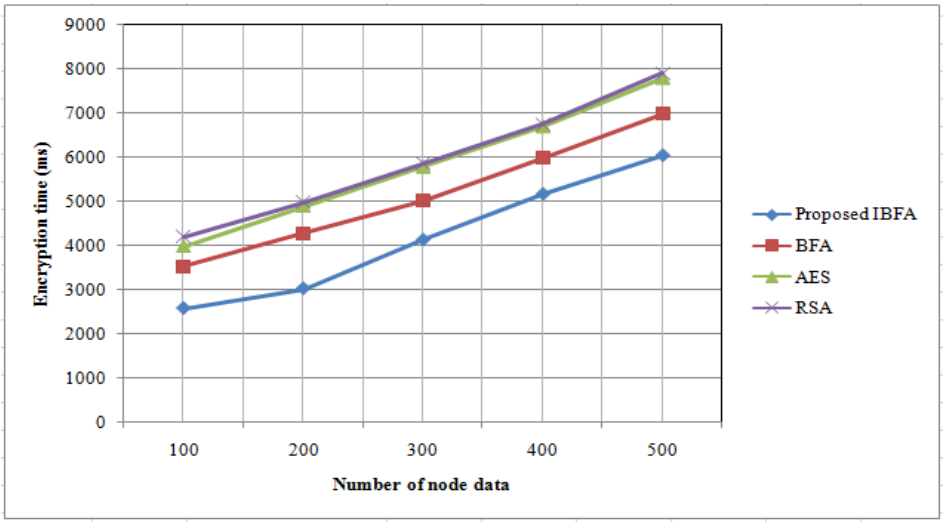
For disparate cases, figure 5 exhibits the techniques' EC. The techniques' EC is plotted for the number of rounds in both scenarios. Initially, for 400 rounds, the energy consumed by the proposed LDCSN-BSHHO is 210J while pondering case 1, whereas 285, 321, 385, along with 425J energy is consumed by the prevailing techniques namely PSO, LEACH, DECC, along with LDC and that is high when analogized with the proposed LDCSN-BSHHO. Similarly, the proposed LDCSN-BSHHO consumes very fewer energy for all rounds when analogized with others. When pondering case 2, the proposed method consumes the energy of 250J for 400 rounds whereas the prevailing PSO, LEACH, DECC, and LDC consumes 295, 350, 421, and 469J for executing the same 400 rounds. The EC augments when the rounds increments, but for executing routing in both cases, proposed method consumes very fewer energy. Thus, the LDCSN-BSHHO's successful energy-aware mechanism which performs clustering, CH selection for achieving an energy-effective routing for WSN is evinced. Centred on other metrics, Table 2 presents the comparison of the techniques.

Table 2: Results of proposed and existing routing algorithms

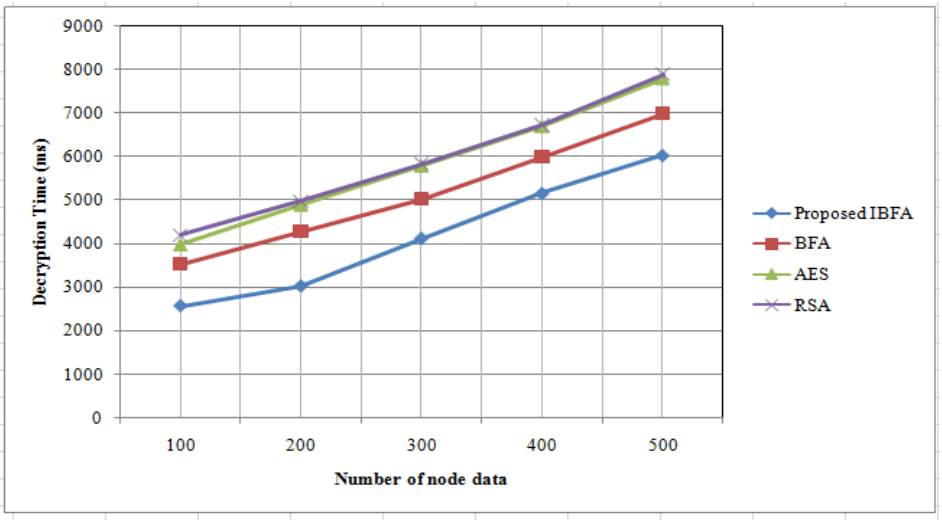
Metrics	Number of nodes	Proposed LDCSN-BSHHO	PSO	LEACH	DECC	LDC
Throughput (Bps)	50	0.8325	0.7685	0.7265	0.6547	0.6023
	100	0.8625	0.8025	0.7523	0.6821	0.6365

	150	0.8987	0.8254	0.7821	0.7021	0.6782
	200	0.9365	0.8589	0.8014	0.7265	0.6987
	250	0.9785	0.8814	0.8236	0.7587	0.7254
Packet Delivery Ratio (%)	50	90	82	68	65.2	58.9
	100	90.2	82.6	68.5	64.3	58.3
	150	90.5	82.2	70.2	66.5	56.3
	200	89.8	81.8	69.2	64.23	59.32
	250	90.6	83.56	70.25	65.38	60.25
Delay (Sec)	50	6.8972	9.3568	12.3456	15.6589	18.6594
	100	9.2563	12.4564	14.5698	17.8963	20.3569
	150	12.3652	15.2365	17.3256	19.8974	23.6478
	200	15.2365	18.2541	19.5683	22.3654	26.5896
	250	18.5689	22.3156	21.3654	25.8931	29.6547

Concerning the PDR, throughput, along with delay, the outcomes are tabulated for the proposed and prevailing algorithms. In general, throughput is stated as the ratio of the number of packets received at the receiver to the packet transmission delay in the routing process. For energy-effective routing, the value of throughput must be high. It is evinced as of table 2, LDCSN-BSHHO attains higher throughput for all number of nodes when analogized with others. The percentage of the addition of DP attained by the receivers to the addition of DPs passed on through the transmitter is termed as PDR and it must be high aimed at better routing protocol. The LDCSN-BSHHO attains 90 % PDR for 50 nodes which are high when analogized with the prevailing methods. The proposed LDCSN-BSHHO achieves 8% higher PDR than PSO, 12% higher PDR than the LEACH, 16% than the DECC, along with 22% higher PDR than the LDC technique. At last, when analogizing the delay outcomes, the very lowest delay is attained by the proposed LDCSN-BSHHO when analogized with others. The average period occupied to route data as of the source to the target node is termed as Delay of the routing protocol. Thus, the proposed LDCSN-BSHHO performs better routing of WSN data in an optimal and energy-effective way which is evinced as of these outcomes. Next, the algorithm's secured awareness is analyzed centred on ET along with DT which is given in figure 6.



(a)



(b)

Figure 6: Encryption and Decryption Time of the techniques

Concerning ET along with DT, figure 6 exhibits the proposed along with prevailing encryption algorithms' performance. The time taken for `converting the plaintext of DPs to the ciphertext is stated as ET, whereas the time taken for retaining the DP's data as of the ciphertext is termed as DT. For encrypting 100 node data, the proposed IBFA takes 2578ms, whereas the prevailing BFA, AES, along with RSA take 3541ms, 3987ms, along with 4200ms, which is high when analogized with the IBFA. The IBFA also takes less time regarding decryption process when analogized with the prevailing algorithms. The ET along with DT increments when the node data augments but, the lowest ET along with DT is attained by the IBFA which evinces the IBFA's less computational complexity over various algorithms. This offers more security to the WSN's DP (node data).

4. CONCLUSION

Here, utilizing the LDCSN-BSHHO, a secure and energy-aware optimal routing scheme is proposed aimed at wireless SN and this algorithm dynamically learns the SN's behaviour each time while executing DTs. Utilizing WUSS along with EORM-BOA, clustering along with CH selection operations are executed for performing DT in an energy effective manner. Then for transmitting the WSN data securely, Utilizing IBFA encryption methodology, the encryption of DPs are done and sent to a BS via the optimal path utilizing LDCSN-BSHHO algorithm. Concerning NLT, throughput, PDR, EC, along with delay, the energy effective along with security aware LDCSN-BSHHO protocol is validated against prevailing methodologies. The LDCSN's outcomes evinced that the technique attains top outcome when analogized with others and it executes the WSN data's secure routing optimally. Regarding both ET along with DT, the IBFA obtains the lowest time and thus reducing the algorithm's complexity and the modification in BFA produces superior security to the WSNs data that prevents the data as of the intruders. For detecting the various forms of attacks in WSN, the attack detection mechanism would be presented utilizing the deep learning algorithm and for protecting the network as of the attack, the advanced prevention mechanism would be given in the upcoming days.

REFERENCES

1. Kale Navnath Dattatraya and K. Raghava Rao, "Hybrid based cluster head selection for maximizing network lifetime and energy efficiency in WSN", Journal of King Saud University-Computer and Information Sciences, 2019, 10.1016/j.jksuci.2019.04.003.
2. Hema Kumar M., V. Mohanraj, Y. Suresh, J. Senthilkumar, and G. Nagalalli, "Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN", Journal Of Ambient Intelligence And Humanized Computing, 2020, 10.1007/s12652-020-02007-w.
3. Feng Li and Li Wang, "Energy-aware routing algorithm for wireless sensor networks with optimal relay detecting", Wireless Personal Communications, vol. 98, no. 2, pp.1701-1717, 2018.
4. Francis Saviour Devaraj A., "Energy aware reliable route selection scheme with clustered RP model for wireless sensor networks to promote interaction between human and sensors",Journal of Ambient Intelligence and Humanized Computing, 2020, 10.1007/s12652-020-02147-z.

5. Kusum Lata Jain and Smarnika Mohapatra, "Energy Efficient Cluster head selection for Wireless Sensor Network: A Simulated Comparison", In IEEE 10th Control and System Graduate Research Colloquium (ICSGRC), pp. 162-166, 2019, 10.1109/ICSGRC.2019.8837086.
6. Damien Wohwe Sambo, Blaise Omer Yenke, Anna Förster, and Paul Dayang, "Optimized clustering algorithms for large wireless sensor networks: A review", Sensors, vol. 19, no. 2, pp. 322, 2019.
7. Amin Shahraki, Amir Taherkordi, Øystein Haugen, and Frank Eliassen, "Clustering objectives in wireless sensor networks: A survey and research direction analysis", Computer Networks, vol. 180, pp. 107376, 2020.
8. Priyank Gour, Neeraj Jain, and Sanjeev Kumar Gupta, "Fuzzy based Adaptive Cluster Head Selection for Wireless Sensor Networks", In IEEE Twelfth International Conference on Contemporary Computing (IC3), pp. 1-5, 2019, 10.1109/IC3.2019.8844907.
9. Syed Kamran Haider, Muhammad Ali Jamshed, Aimin Jiang, Haris Pervaiz, and Qiang Ni, "UAV-assisted Cluster-head Selection Mechanism for Wireless Sensor Network Applications", In IEEE UK/China Emerging Technologies (UCET), pp. 1-2, 2019, 10.1109/UCET.2019.8881889.
10. Ravi Kumar Poluru and Lokesh Kumar Ramasamy, "Optimal cluster head selection using modified rider assisted clustering for IoT", IET Communications, vol. 14, no. 13, pp. 2189-2201, 2020.
11. Tina Gui, Feng Wang, Christopher Ma, and Dawn E. Wilkins, "On cluster head selection in monkey-inspired optimization based routing protocol for WSNs", In IEEE International Conference on Computing, Networking and Communications (ICNC), pp. 126-130. 2019, 10.1109/ICCNC.2019.8685531.
12. Vimalarani C., R. Subramanian, and S. N. Sivanandam, "An enhanced PSO-based clustering energy optimization algorithm for wireless sensor network", The Scientific World Journal, 2016, 10.1155/2016/8658760.
13. Karthick P. T., and Palanisamy C, "Optimized cluster head selection using krill herd algorithm for wireless sensor network", Automatika, vol. 60, no. 3, pp. 340-348, 2019.
14. Geetika Dhand and Kavita Sheoran, "Protocols SMEER (Secure Multitier Energy Efficient Routing Protocol) and SCOR (Secure Elliptic curve based Chaotic key Galois Cryptography on Opportunistic Routing)", Materials Today: Proceedings, 2020, 10.1016/j.matpr.2020.06.503.
15. Nabil Sabor, Shigenobu Sasaki, Mohammed Abo-Zahhad, and Sabah M. Ahmed, "A comprehensive survey on hierarchical-based routing protocols for mobile wireless sensor networks: Review, taxonomy, and future directions", Wireless Communications and Mobile Computing, 2017, 10.1155/2017/2818542.
16. Thaier Hayajneh, Razvi Doomun, Ghada Al-Mashaqbeh, and Bassam J. Mohd, "An energy-efficient and security aware route selection protocol for wireless sensor networks", Security and Communication Networks, vol. 7, no. 11, pp. 2015-2038, 2014.
17. Weidong Fang, Chuanlei Zhang, Zhidong Shi, Qing Zhao, and Lianhai Shan, "BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks", Journal of Network and Computer Applications, vol. 59, pp. 88-94, 2016, 10.1016/j.jnca.2015.06.013.
18. Ziwen Sun, Min Wei, Zhiwei Zhang, and Gang Qu, "Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks", Applied Soft Computing, vol.77, pp. 366-375, 2019.
19. Deepak Mehta and Sharad Saxena, "MCH-EOR: Multi-objective cluster head based energy-aware optimized routing algorithm in wireless sensor networks", Sustainable Computing: Informatics and Systems, vol. 28, pp. 100406, 2020, 10.1016/j.suscom.2020.100406.
20. Reeta Bhardwaj and Dinesh Kumar, "MOFPL: Multi-objective fractional particle lion algorithm for the energy aware routing in the WSN", Pervasive and Mobile Computing, vol. 58, pp. 101029, 2019.
21. Prachi Maheshwari, Ajay K. Sharma, and Karan Verma, "Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization", Ad Hoc Networks, vol. 110, pp. 102317, 2021, 10.1016/j.adhoc.2020.102317.
22. Vinitha A., and M. S. S. Rukmini, "Secure and energy aware multi-hop routing protocol in WSN using taylor-based hybrid optimization algorithm", Journal of King Saud University-Computer and Information Sciences, 2019, 10.1016/j.jksuci.2019.11.009.
23. Dipali K.Shende and S. S. Sonavane, "CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications", Wireless Networks, pp.1-19, 2020, 10.1007/s11276-020-02299-y.
24. Deepak Mehta and Sharad Saxena, "Hierarchical WSN protocol with fuzzy multi-criteria clustering and bio-inspired energy-efficient routing (FMCB-ER)", Multimedia Tools and Applications, pp.1-34, 2020, 10.1007/s11042-020-09633-8.
25. Sathya Lakshmi Preeth SK, R. Dhanalakshmi, R. Kumar, and P. Mohamed Shakeel, "An adaptive fuzzy rule based energy efficient clustering and immune-inspired routing protocol for WSN-assisted IoT

system", Journal of Ambient Intelligence and Humanized Computing, pp. 1-13, 2018, 10.1007/s12652-018-1154-z.

26. Asraf Yasmin, B., Latha, R., & Manikandan, R. (2019). Implementation of Affective Knowledge for any Geo Location Based on Emotional Intelligence using GPS. International Journal of Innovative Technology and Exploring Engineering, 8(11S), 764–769. https://doi.org/10.35940/ijitee.k1134.09811s19