International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Secure and Energy-Efficient Optimal Routing Scheme for WSN Using IBFA And LDCSN-BSHHO Algorithms

Dr. A. Edwin Rajesh[1], Dr. P. Ponmuthuramalingam[2]

[1]Assistant Professor, Dept. of Computer Science, Bishop Appasamy College of Arts & Science, Coimbatore. Tamilnadu, India.
[2]Joint Director of Collegiate Education, Trichy Region, Trichy, Tamilnadu, India.

Abstract
This Paper ultimate aim is to offer a comprehensive solution for securing and efficiently transmitting data in WSNs is provided by the Interlock Triple Authentication and Data RP in a WSN, making it an effective solution for protecting against common vulnerabilities and attacks. Secondly, the WSN's energy along with security problems are addressed and a secure as well as Energy-Aware Optimal Routing (EAOR) scheme for WSN utilizing Learning of Dynamic Characteristics of SNs with Bidirectional Search centered Harris Hawk optimizations (LDCSN- BSHHO) is proposed. By wielding four stages, namely clustering, Cluster Heads (CH) selection, routing, and data encryption, the proposed optimal routing is executed. Primarily, the SN is clustered by the Weigh Utility-centered Stratified Sampling (WUSS) method for expanding the Network Life-Time (NLT). Afterward, the CH is optimally chosen by the Elite Opposition and Ranking mutation-centered Butterfly Optimization Algorithm (EORM-BOA) methodology for the clusters. Later, to render data security, the Data Packets (DPs) are encrypted by the Improved Blowfish Algorithm (IBFA). Consequently, via the optimum path, the encrypted DP is sent by the LDCSN-BSHHO to the Base Stations (BS). It learns the node's behavior dynamically; in addition, an optimal path is elected for data transfer by employing the BSHHO approach. This sort of energy along with security-based methodology for WSN routing is labeled as secure as well as Energy-Aware Routing (EAR) of WSN. The proposed scheme's results are scrutinized as well as evaluated against the other prevailing methods that signify the proposed scheme's efficacy for optimal routing as well as data security.

Keywords: Energy Efficiency(EE),Learning of Dynamic Characteristics of SNs (LDCSN) ,Bidirectional Search centered Harris Hawk optimizations (BSHHO), Network Life-Time (NLT),Base Stations (BS), Energy-Aware Routing (EAR)

1.INTRODUCTION

The WSN has turned out to be one amongst the hopeful modalities in current times. The WSN's environment investigated the detected modifications taking place in the monitored areas. A few alternations are intensity, sound, temperature, vibration, motion, pressure, as well as humidity .Finite energy as well as transmission range is contained in the WSN's sensor that forces them to execute cooperative transmission with the assistance of numerous in-betwixt SN. Thus, the effectual utilization of restricted energy is apparently of substantial significance in the complete network stability's maintenance.

To attain energy preservation, numerous models like the incorporation of mobile sink nodes, sleep cycle scheduling, routing, clustering, and so on were employed. Clustering as well as routing are the utmost preferential methodologies by which energy might be conserved to the maximal. The longevity network was assisted by the fine selection of the CH. On the hierarchical architectures, the whole network is alienated into sub-networks termed clusters. The CH's responsibility is the collection of fusing of data as of nodes belonging to a similar cluster. A special node leading every cluster is named CH.

By numerous clustering techniques, the SN is chosen randomly as a CH devoid of deeming existing resources currently. WSN cluster is an optimum CH chosen for utilizing some predefined parameters. This cluster could be wielded to enhance the communication range as well as NLT. Several papers proposed a few effective optimization algorithms for CHS, namely the Cyclic Rider Optimization Algorithm (C-ROA), Monkey-inspired Optimization (MO), PSO, Krill Herds Optimization (KHO), etc. These effective algorithms have an earlier convergence problem. Single-hoping for small distances diminished energy utilization; however, DT utilized more energy causing degradation in the longer distances performance. Routing is the process, which elongates the NLT by EC diminution in communication.

The RP regarded the network's structure, data-sending methods, node and link heterogeneity, data aggregation, EC, coverage, node mobility, connectivity, as well as QoS problems to be an effectual as well as reliable protocol. The usage of traditional RPs that is aimed at identifying the routes on WSN is ineffective, resulting in disasters on the sensors. For evaluating the node's reliability, a few routing methodologies grounded on node trust relationships were recommended. The security in the network is enhanced by separating the malevolent nodes by employing the extensive TV acquired by direct as well as indirect trusts via intercommunication amongst nodes. Nevertheless, due to the limited capability of computing along with WSN's communication, they aren't pondered as strict needs in energy efficiency. In this chapter, effectual security approaches along with an optimal EAR system in WSN are proposed.

2. PROPOSED SECURE AND ENERGY-EFFICIENT OPTIMAL ROUTING SCHEME FOR WIRELESS SENSOR NETWORKS

A higher number of spatially disseminated SN linked via the wireless medium for monitoring as well as recording the physical information from the surroundings are comprised in WSN. Since a huge quantity of energy amongst transmission is consumed by the battery-operated SN on the network, a chief challenge in the WSN environment is energy. The network's lifetime is affected by this energy restraint. Currently, clustering together with routing algorithms is broadly employed in WSN for ameliorating the NLT.

The optimal routing scheme utilizing the '4' steps mentioned (clustering, CHS, data encryption, and routing) is known as cluster-centered routing. Here's a brief overview of each step:

1. **Clustering:** Here, the sensors in the network are partitioned into clusters centered on their proximity. Every single cluster has a CH that acts as the intermediary betwixt the cluster members and the BS.
2. **Cluster Head Selection:** In cluster-centered routing, the selection of CH is a vital step. The CH should have adequate energy and computational resources for performing the required tasks. Several factors like RE, connectivity, and distance to the BS are considered in selecting the CH.
3. **Data Encryption:** For ensuring the security of the data transmitted in the network, encryption techniques are employed. The data gathered from the sensors are encrypted before transmission, and the CH decrypts it before forwarding it to the BS.
4. **Routing:** After encrypting the data, the CHs forward it to the BS via an MH routing mechanism. The routing mechanism ensures that the data is transmitted via the most EE and secure path.

Cluster-based routing reduces EC and offers secure communication in WSNs by utilizing clustering, CHS, data encryption, and routing. It also assists in extending the NLT by evenly distributing the EC among the sensors.

A security as well as EAOR scheme in WSN named LDCSN-BSHHO is proposed in this chapter. Primarily, utilizing WUSS, the WSN's SN is structured as a cluster. Additionally, the optimum CH as of distinct CH nodes on the WSN is detected by the proposed CH algorithm (EORM-BOA). After that, the DP collected through CH is encrypted employing IBFA as well as sent to the BS via an optimal path for rendering security to the cluster data. By employing LDCSN-BSHHO, the route between the CH and the BS is detected; it elects the optimal route grounded on the distance, node degree, as well as RE. Therefore, energy along with security-aware optimal routing on WSN was attained by this work. Figure 2.1 exhibits the proposed work's architecture.

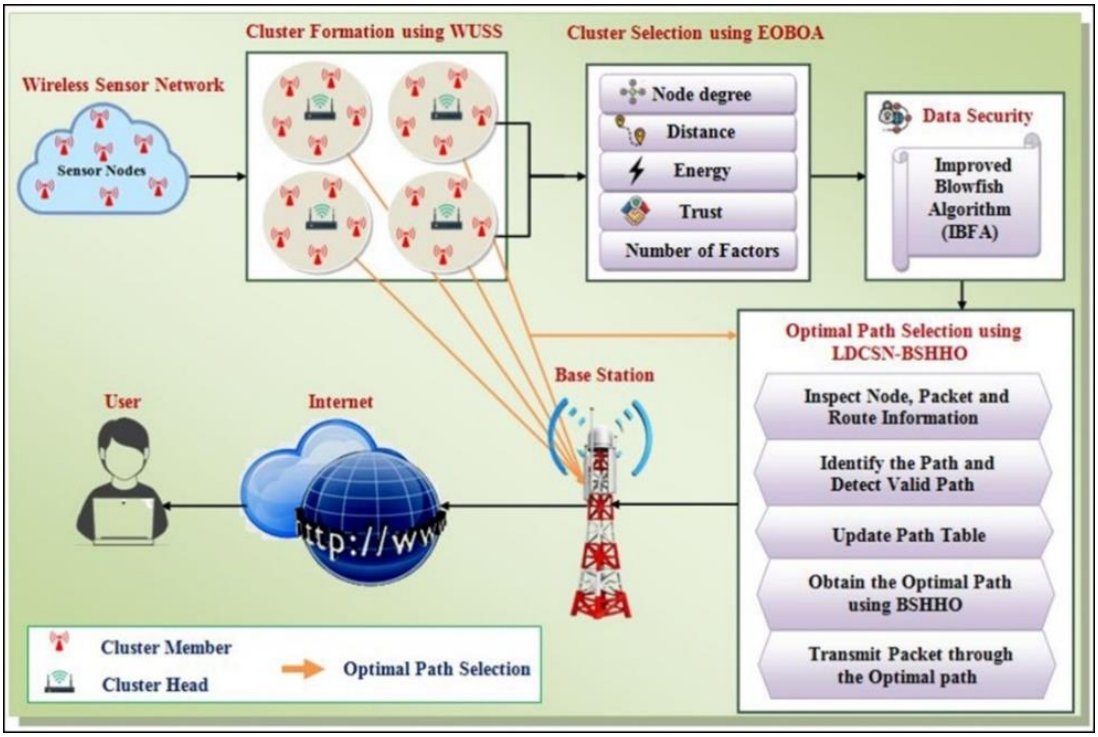

Figure 2.1 Proposed Architecture

2.2 CLUSTER HEAD SELECTION

A crucial step in cluster-centered routing for WSNs is CHS. The selection of CHs affects the network's performance, including energy efficiency, scalability, and DT reliability.

Utilizing various techniques like static and dynamic CHS, the selection of CHs could be executed. In static CHS, CHs are pre-determined grounded on their location, energy level, or other criteria. It is easy to implement static CHS however it mayn't be effective in dynamic network conditions where the network topology changes often.

The EORM-BOA method is an optimization algorithm utilized for selecting the CH for every single cluster in WSNs. This method is grounded on the Butterfly Optimization Algorithm (BOA) and uses elite opposition as well as ranking mutation for improving the optimization process.

The EORM-BOA methodology works by initializing a populace of potential CHs, which are randomly chosen as of the SNs in the network. Every single CH is assessed centered on a fitness function that pon-

ders its energy level, distance to the BS, and the level of data correlation with its cluster members.
The CHs are selected in dynamic CHS centered on real-time conditions like energy level, distance to the BS, as well as connectivity. With the EORM-BOA's aid, the CH aimed at each cluster is detected optimally past the cluster's generation. Then, the time consumption targeted in selecting the CH is diminished by the WUSS that is intended to execute clustering.
The EORM-BOA methodology employs a fitness function that deems the energy level, distance to the BS, and level of data correlation to evaluate potential CHs. The BOA is utilized for optimizing the fitness function, and elite opposition and ranking mutation are wielded to maintain diversity and avert premature convergence. The likelihood that the individual holding a higher ranking is chosen as the terminal vector or else the base vector available in the mutation turns out to be larger; also, transmitting the valuable data as of the current populace to the offspring is the objective. The excellent individual is chosen by the probability that is elevated by the ranking-grounded mutation operator; thereby, enhancing the exploitation ability. The populace's diversity is incremented by the elite opposition-grounded learning scheme, which also augments the exploration ability that is aimed at advancing computation accuracy.

Figure 2.2: Pseudocode for Cluster Head Selection Using EORM-BOA

Input:

- Population sizs (N)
- Maximum Number of iterations (Maxlter)
- Number of dimensions (D)
- Network topology information (E.G neighbour list)
- Sensor nodes information, (Energy level)
- Fitness function (f)

Output

- Cluster head(s) for the current round

Initialization:

Initialize N butterflies randomly in the search space
Main Loop:
For t=110 Max lter do
for i= 1 to N do
Update butterfly i

- Calculate fitness value for butterfly
- Apply Elite Opposition and Ranking Mutation (EORM) operator
- Apply Buttery Movement operator
- Check if the new position within the search space bounds.

If the new positions within he search space bounds then
If the new fitness value is better then the current fitness value then
'update current fitness value and position of butterfly
End for
'Select the best utterly as the cluster head(s) based on the fitness function and network topology information end for Return the selected cluster head (s)
In this pseudo-code (Figure 2.1), a populace of butterflies is used by the EORM-BOA approach for discovering the optimal CH in a WSN. The approach iteratively updates the position and velocity of each

butterfly centered on its fitness value and the positions of the elite and global butterflies. Centered on their fitness values, the butterflies are then ranked, and a new populace is chosen grounded on their selection probabilities. Lastly, the butterfly having the highest fitness is elected as the CH, and the leftover butterflies are assigned to the CH grounded on their distance from it.

2.3 SELECTION OF OPTIMAL ROUTING

Since lesser QoS, EC, data throughput, together with latency are provided by routing mechanisms, they are substantial in WSN. The DT is executed by employing the optimal routing as well as it is commenced by selecting the finest paths as of CHs to BS optimally; in addition, it is performed employing the proposed BSHHO. In the context of WSNs, by electing the best path optimally as of the CH to the BS, the DT is initiated. While ensuring reliable DT with minimal delay, it includes detecting the optimal routing path. For facilitating the effective utilization of nodes' energy and for enhancing the NLT, a novel LDCSN-BSHHO algorithm is proposed. A recent metaheuristic algorithm employed for detecting the optimal routing paths in WSNs is named BSHHO (Bidirectional search-based Harris Hawk optimizations) algorithm, which is grounded on the Harris Hawks' (HH) behavior that are recognized for their hunting skills as well as effective searching schemes.

The LDCSN together with BHHO's functioning is provided as,

2.3.1 LDCSN

The route betwixt the source (S)as well as the destination (D) is explored by the LDCSN and amasses it into the path table 2.1 while the communication is initiated between the 'S'and 'D' node. This algorithm is centered on the principle of learning by doing. As SNs transmit data packets, they analyze the routes taken by the packets and store the information in the path table 2.1. The table 2.1 contains information about the route, including the number of hops, the QoS, as well as the EC of each hop.

The LDCSN algorithm is designed to be adaptive and dynamic. As the network topology modifies owing to node failures, mobility, or other factors, the algorithm adjusts the path table 2.1 accordingly. The approach also ponders the nodes' energy levels and avoids routes that are likely to consume more energy. By employing the LDCSN algorithm, WSNs can achieve more efficient and reliable communication betwixt nodes.

Every single LDCSN is constructed dynamically as well as analyzed for the entire route exploration. 5 major factors incorporated in LDCSN are given as,

$$L_{dstn} = \{f_s, \sum, T_f, z_0, L\}$$

Here, f_s signifies the finite states' compilation, the finite input alphabets' set is notated by $\sum, T_f$ specifies the transition function, the primary state is signified as z_0, and the last state is symbolized as L. Every single SN in WSN contains diverse states, which change as of 1 state to another state specified as $\{z_0, z_1, z_2, ...z_n\}$; in addition, the transitions are offered by the transition function as T_f, z_0 illustrates the 1st state along with the end state is symbolized as z_n (i.e. the nodes contain n-number of states).

For the CH routing, the set of paths is signified as $\{p_1, p_2, ... p_w\}$along with the forward path, or else the reverse path is signified by $F \rightarrow or\ R \leftarrow$, correspondingly. All this information is autonomously learned by wielding the LDCSN function, and the optimum path is detected with their aid. Centered on the node states along with the path between 'S' and 'D', the 'T_f' ' is activated. In the learning process, the LDCSN employs the section table (Table 2.3) to update the information attained by the LDCSN. For every single

route discovery, the source's updation, intermediate, together with DN information are executed in the path table 2.3. The section table is learned at every single time; in addition, in Table 2.1, the path, intermediate nodes, as well as nodes' state values are updated. The path of that section detects whether the nodes' state is accessible in the route; the transmission is accepted if it encompasses the DN. The information concerning the node together with path information is retrieved by this section at a frequent time interval. The section, that is, the path is tested to check if it is valid or else not.

Table 2.3: Elements of Section Table

Elements	Description
N_{ID}	Node Id
N_L	Node Location (x and y coordinates)
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

2.3.2 BSHHO

By employing the BSHHO algorithm, the optimal routing path can be found efficiently, which helps to minimize EC, reduce latency, and enhance the overall network performance. This approach ensures that the WSN operates optimally and that DT is executed in an efficient and reliable manner. The HHs, which aimed at tracking as well as pouncing on their prey, pursued incredible social behavior in the Harris Hawks Optimization (HHO) methodology. The algorithm's explorative as well as exploitative stages are executed by various attacking ways, abrupt pouncing, and looking for prey. Employing the '2' exploration process, HHs are disseminated arbitrarily toward the locations waiting for prey. In the 1st framework, HHs perch on a location deeming other family members' positions, together with the rabbit (prey). The Hawks are waiting upon arbitrary tall trees in the 2nd framework.

The levy random behavior, which is targeted at choosing the finest potential drive, is utilized by the HHO's fundamental version. However, due to its massive search phases, disadvantages like the search area's overflow together with the random flight interruption are possessed by levy flights. A bidirectional search-centered HHO named BSHHO that is intended to tackle those demerits along with enhancing the HHO's local searching ability directed at optimization problems is proposed.

This assists in performing the local search in the forward along with backward direction. Whilst selecting the direction, Greedy selection is performed. The backward traverse is espoused or else forwarded if the solution augments while traveling backward. This alteration helps in speeding up HHO's convergence rate. Decrementing the DT's EC from the source towards the destination as well as detecting the optimum path from the source onto the destination is the LDCSN-BSHHO's core target. Grounded on every single path's entire EC, BSHHO should detect the optimum path from the set of potential paths. The path's $p1$ EC from the source i towards the destination j is calculated as,

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

Here, $c_{en}(i,j)$ notates the energy cost that intended to send k -bit message at a distance d as of source i towards j, that is articulated utilizing the equation

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

Here, $E_{tx}(t_n, d)$ and $E_{rx}(t_n)$ represents the energy dissipated for every bit at the transmitter as well as the receiver, which is stated as, n

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

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

Here, $R_{\cos t}$ notates the circuit energy's cost while 1bit of data is transferred or else received, t_n implies the number of transferred data bits, along with the amplification factor is specified as A_f. HHO's '2' frameworks are designed with c 's equal chance intended at every single stage as:

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

Here, p^t and p^{t+1} implies the Hawks' position vectors in the current as well as forthcoming iterations. p_r^t signifies a random hawk elected from the populace, 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 as well as the upper bounds for generating random positions within the Hawks' home that can be articulated as:

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

Here, p_i^t signifies each hawk's i^{th} position vector in the populace at the iteration t, and w notates the number of HHs present in the populace. Centered on the rabbit's escape energy E_E, the algorithm modifies from the exploration to the exploitation as:

$$E_E = 2E_O \left[1 - \frac{t}{M_{it}} \right]$$

Here, E_0 notates the initial rabbit's energy, which is chosen randomly between [−1, 1]. Mit denotes the maximal number of iterations. Hawks probing for added regions are targeted in discovering the rabbit's position whilst $\left| E_F \right| \geq 1$; If not, the exploitation occurs. In the algorithm, articulating the success $c \geq 0.5$ or else failure $c > 0.5$ of rabbit escape is accomplished with an equal chance c. The Hawks execute a soft $\left| E_g \right| \geq 0.5$ or else hard $\left| E_F \right| < 0.5$ besiege dependent on the rabbit's energy. The soft besiege is articulated as:

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

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

$$R_J = 2(1 - rd)$$

Here, Δp^t notates the difference betwixt the hawk's and rabbit's locations, along with R_J implies the rabbit's Random jump strength derived by using a random number rand. The hard besiege is articulated

as:

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

Whilst, $|E_E| \geq 0.5 and c > 0.5,$ a soft besiege that exhibits gradual quick dives is executed since the rabbit could successfully flee. The finest potential dive could be chosen by the Hawks. For imitating the prey's leapfrog, the Bidirectional search is employed that assists in executing the local search in the forward along with the backward direction. This is rapid in that it significantly diminishes the quantity of necessary exploration. To decide whether the dive is good or else bad, the Hawks' forthcoming move is assessed by employing,

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

If the last dive isn't useful, the Hawks dive utilizing the B pattern as:

$$h = y + s * BS(d)$$

Here, the problem's dimension is specified as d along with a random vector that exhibits a size d is notated as s. The Bidirectional pattern (search) is computed as,

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

Here, p^t, $f\left(p^t\right)$ specify the hawks' present position as well as objective fitness function value, respectively, along with the step length is denoted as S. The final soft besiege progressive speedy dives are articulated by employing:

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

Hard besiege with progressive speedy dives occurs whilst $|E_E| \geq 0.5$ and $c < 0.5$ as the rabbit does not have adequate energy for escaping using the equation in which y is expressed employing the succeeding equation. Figure 4.5 signifies the proposed BSHHO's pseudo-code.

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

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

Begin
Initialize the population of X random hawks (available paths) and M_{it}
Compute the fitness of each hawk using $E(p_1)_{i,j} = \begin{cases} \infty & j \notin nx(i) \\ c_{en}(i,j) & OW \end{cases}$
Denote the best position of hawk with minimum fitness as P_{rabbit}
$t = 1$
while $(t \leq M_{it})$
  Update E_E using $E_{tx}(n,d) = R_{cost} * t_n + A_f * d^2 * t_n$
  if $|E_E| \geq 1$
    Update P^{t+1} using $E(p_1)_{i,j} = \begin{cases} \infty & j \notin nx(i) \\ c_{en}(i,j) & OW \end{cases}$
  if $|E_E| < 1$
    if $(c \geq 0.5 \,\&\&\, |E_E| \geq 0.5)$
      Update $P^{t+1} = \Delta p^t - E_E\left|R_j * p_{rabbit}(t) - p^t\right|$
    if $(c \geq 0.5 \,\&\&\, |E_E| < 0.5)$
      Update $p^{t+1} = p^t - E_E\left|\Delta p^t\right|$

```
        if (c < 0.5 && |E_E| ≥ 0.5)
            Update soft besiege with progressive rapid dives (BS(d))
        if (c < 0.5 && |E_E| ≥ 0.5)
            Update hard besiege with progressive rapid dives (BS(d))
        end if
        end if
        end if
        end if
    end if
    if (fitness(p^{t+1}) < fitness(P_rabbit))
        Update P_rabbit = P^{t+1}
    t++
    end if
Return P_rabbit position
end while
end
```

Figure 2.4 Pseudo-code for the Proposed BSHHO

3. CONCLUSION

Regardless of the widespread utilization of WSNs in numerous applications, ensuring the security and energy efficiency of these networks while maintaining optimal data routing remains a challenge. Adequate security measures or energy optimization strategies may be lacked by the prevailing WSN protocols, causing potential security breaches and energy inefficiency. Thus, there is a need for a WSN protocol that can offer secure as well as EE data routing while maintaining optimal data flow. An interlock triple authentication centered secure and EE optimal data RP in WSN is proposed for tackling this issue. An interlock triple authentication-based secure and EE optimal data RP in WSNs is proposed in this paper.

The proposed algorithm encompasses two methodologies:

- The first methodology proposes an interlock triple authentication method that utilizes ‘3’ layers and ‘1’ DNA station for securing DT.
- The second methodology employs the LDCSN-BSHHO, a secure and EAOR scheme that dynamically learns SNs' behavior and executes DTs in an EE manner.

The Interlock Triple Authentication is to secure DT in WSN. The methodology has three layers and one DNA station. The host discovery layer, TCP port scan layer, and evaluation layer are the ‘3’ layers. The DNA station has a base node, sensor node, and service detection with the aid of an IP trace and IP test book. The base node is accountable for specification analysis and also has event DNA. When compared with prior methods, the Interlock Triple Authentication method becomes a highly secured method for DT owing to the ability and highly secured algorithm.

REFERENCES

1. Jennifer Yick, Biswanath Mukherjee and Dipak Ghosal, “Wireless sensor network survey”, Computer Networks, vol. 52, pp. 2292-2330, 200a8.
2. Guobao Xu, Weiming Shen and Xianbin Wang, “Applications of wireless sensor networks in marine environment monitoring: A survey”, Sensors, vol. 14, pp. 16932-16954, 2014.
3. Mohsen Attaran, “The impact of 5G on the evolution of intelligent automation and industry digitization”, Journal of Ambient Intelligence and Humanized Computing, 2021.https://doi.org/10.1007/s12652-020-02521-x

4. Beom-Su Kim, Ki-Il Kim, Babar Shah, Francis Chow and Kyong Hoon Kim, "Wireless sensor networks for big data systems", Sensors, vol. 19, no. 7, pp. 1-18, 2019.
5. Rathna R, Vaiyshnavi M. P and Maria Anu V, "Reduction of energy consumption using self-organizing tree for wireless sensor networks", Research Journal of Pharmaceutical, Biological and Chemical Sciences, vol. 7, no. 2, pp. 1229-1236, 2016.
6. Taochun Wang, Xiaolin Qin and Liang Liu, "An energy-efficient and scalable secure data aggregation for wireless sensor networks", International Journal of Distributed Sensor Networks, 2013. http://dx.doi.org/10.1155/2013/843485
7. Muhammad Asim, "Self-organization and management of wireless sensor networks", Thesis, School of Computing and Mathematical Sciences Liverpool John Moores University, 2010.
8. John T Ogbiti, Henry C Ukwuoma, Salome Danjuma and Mohammed Ibrahim, "Energy consumption in wireless sensor network", Computer Engineering and Intelligent Systems, vol. 7, no. 8, pp. 63-67, 2016.
9. Alazzawi L and Elkateeb A, "Performance evaluation of the WSN routing protocols scalability", Journal of Computer Systems, Networks, and Communications, 2018. http://dx.doi.org/10.1155/2008/481046
10. Eirini Karapistoli, Ioanna Mampentzidou and Anastasios A Economides, "Environmental monitoring based on the wireless sensor networking technology a survey of real-world applications", International Journal of Agricultural and Environmental Information Systems, vol. 5, no. 4, pp. 1-39, 2014.
11. Milon Islam, Ashikur Rahaman and Rashedul Islam, "Development of smart healthcare monitoring system in IoT environment", SN Computer Science, vol. 1, pp. 1-11, 2020.
12. Oktay Cetinkaya and Ozgur Baris Akan, "Use of wireless sensor networks in smart homes", CRC Press, 1st Edition, ISBN: 9780429075841, 2016.
13. Jaime Lloret, Sandra Sendra, Laura Garcia and Jose M Jimenez, "A wireless sensor network deployment for soil moisture monitoring in precision agriculture", Sensors, vol. 21, no. 21, pp. 1-24, 2021.
14. Pascale A, Nicoli M, Deflorio F, Dalla Chiara B and Spagnolini U, "Wireless sensor networks for traffic management and road safety", IET Intelligent Transport Systems, vol. 6, no. 1, pp. 67-77, 2012.
15. Pooja Krishnath Patil and Patil S. R, "Structural health monitoring system using WSN for bridges", International Conference on Intelligent Computing and Control Systems, 15-16 June 2017, Madurai, India, 2017.
16. Opeyemi Osanaiye, Attahiru S Alfa and Gerhard P Hancke, "A statistical approach to detect jamming attacks in wireless sensor networks", Sensors, vol. 18, no. 6, pp. 1-15, 2018.
17. Keshav Jindal, Surjeet Dalal and Kamal Kumar Sharma, "Analyzing spoofing attacks in wireless networks", 4th International Conference on Advanced Computing & Communication Technologies, 08-09 February 2014, Rohtak, India, 2014.
18. jin-Yong Yu, Euijong Lee , Se-Ra Oh, Young-Duk Seo and Young-Gab Kim, "A survey on security requirements for WSNs: Focusing on the characteristics related to security", IEEE Access, vol. 8, pp. 45304- 45324, 2020.
19. Aseri T. C and Singla N, "Enhanced security protocol in wireless sensor networks", International Journal of Computers Communications & Control, vol. 6, no. 2, pp. 214-221, 2011.
20. Alok Ranjan Prusty, "The network and security analysis for wireless sensor network : A survey", International Journal of Computer Science and Information Technologies, vol. 3, no. 3, pp. 4028-4037, 2012.

21. Shazana Zin, Nor Badrul Anuar, Miss Laiha Mat Kiah and Al-Sakib Khan Pathan, “Routing protocol design for secure WSN: Review and open research issues”, Journal of Network and Computer Applications, vol. 41, pp. 517-530, 2014.