International Journal of Computer and Engineering Optimization (IJCEO)
Volume 02, Issue 04, July – August (2024)

RESEARCH ARTICLE

EO-SSPR: EURYGASTER OPTIMIZED SECURE SHORTEST PATH ROUTING PROTOCOL IN WIRELESS SENSOR NETWORK

T. Rajesh [1, *] and S. Sony Helen [2]

[1] Professor, Department of Electronics and Communication Engineering, PSN College of Engineering and Technology, Tirunelveli, Tamil Nadu, India

[2] Research Scholar, Department of Computer Science and Engineering, Anna University, Chennai, Tamil Nadu, India

[*]*Corresponding e-mail: tnanjilrajesh@gmail.com*

Abstract – Wireless sensor network (WSN) has numerous sensor nodes connected to sink nodes creating a network that is both dynamic and resource limited. The ever-changing environment and the sensor nodes' limited resources make it difficult to determine the best and most secure network structure. The data relay paths are one of the key issues with data transfers in WSNs strategy. In these situations, meeting the quality-of-service requirements is essential. To overcome these challenges and to find the shortest path Eurygaster optimized secure shortest path routing (EO-SSPR) approach has been proposed. The goal of EO-SSPR is to determine the shortest path while ensuring the secure data transmission. The sensor data collected from the patient is DNA encrypted and further encryption is done with the help of Crystal Kyber encryption. Shortest path is determined with the help of Eurygaster optimization. With the help of key generated, DNA decryption is performed further and the original signal data is finally recovered. The authorized user finally receives the original signal data via the shortest path determined. The encryption and decryption time of the proposed EO-SSPR is 12.03%, 8.57%, 4.01% better than DynCH, SEAMHR, SPSRN respectively.

Keywords *– Wireless sensor network, Eurygaster optimization, Crystal Kyber encryption, encryption time, decryption time.*

1. INTRODUCTION

Wireless sensor Network (WSN) have advanced rapidly in recent years along with the development of wireless communication, because they are so widely used in many other fields, including civic, military, healthcare, environmental monitoring, and many more others [1]. Among their many other skills are perception, measurement, and computation. These wireless nodes feature restricted memory capacity, short battery life, restricted bandwidth, and limited computational capability [2].

Sensors must work dependably with constrained energy, bandwidth, and computing resources in order to serve these challenging and crucial applications [3,4]. Additionally, inorder to guarantee minimal latency and prolonged network lifetime, the resource-constrained sensors must be very efficient. One of the crucial problems data transfers occurs in WSNs. strategy, or the data relay pathways, to fulfill the quality-of-service requirements under these conditions[5].

Routing is the process of determining the path that connects the starting point and the final destination. The features that set routing apart from other communication and ad hoc networks make it a challenging problem[6]. Because there are many sensor nodes, routing is not practical for designing the overall problem-solving scheme. Transferring data to the Base Station (BS)from several sources is required for all sensor network applications. Energy, processing and storage capacity, and transmission power are the only resources available to sensor nodes. Since data collection depends on location, sensor position information is essential. As several sensors in the neighborhood produce comparable data, redundancy present in the data flow[7].

Multi-hop data transfer is employed for packet forwarding because of the high sensor node density and restricted communication range. In WSN, there are many restrictions during the routing process. Route reliability is the first drawback. The second limitation is the lag across the links in WSN and the third constraint is battery power. All of the nodes function as routers. The Route REQUEST (RREQ) message is broadcast by a node using the route discovery method if it is unable to determine the path. Following receipt of the RREQ packet, neighboring nodes obtain the QoS parameters across pathways, including movement and location data[8].

The traditional shortest path serves as the foundation for many path selection techniques. However, taking the same route may lead to hotspots or traffic bottlenecks. Alternatively, we may think of the temporal delay as the ideal dynamic edge length, taking into account the actual distance between two nodes[9]. This point of view states that when congestion arises on a particular path, the random shortest route will select an alternative route. The stochastic shortest path problem's solution is therefore still relevant and very

helpful. Furthermore, the solution to this problem can be used to a number of situations, including emergency response, robot navigation, and road networks[10]. As a result, wireless sensor networks are among the numerous situations in which the shortest path problem solution is helpful. To determine the quickest route between plain and cipher text , the Eurygaster optimized secure shortest path routing (EO-SSPR) approach has been proposed. The following summarizes the main findings of the study.

- A novel EO-SSPR is proposed for secure data transmission and to identify the shortest path between the nodes.
- In first layer the key generation and data encryption is done by crystal kyber encryption for privacy preserving and secure data encryption.
- In the second layer, DNA cryptography is utilized for data encryption and decryption to protect the confidential data from unauthorized user.
- Eurygaster optimization is utilized to identify the shortest path between the sender and the receiver.

2. LITERATURE SURVEY

In 2020, Mehra, P.S., Doja, M.N. and Alam, B., [11] had explained a fuzzy-based balanced cost CH choosing algorithm (FBECS) that considers the distance from the sink, residual energy, and density of the node. By choosing the most eligible applicant for the cluster coordinator post while taking into consideration the probability allocated to each sensor node, this protocol achieves load balancing. Based on improved stability over an extended length of time with load balancing and large amounts of data being delivered to the sink, the testing results justify FBECS's performance in comparison to its competitors BCSA and LEACH.

In 2021, Srinivas, T. and Manivannan, S.S., [12] had established a security technique to recognize and stop medical IoT-black WSN's hole and selective forwarding attacks. This paper's primary contribution is the coordination of objective model parameters, including distance, packet loss ratio, trust, and delay or latency, to determine the optimal shortest route path. In order to detect and stop the two main attacks on the healthcare sector—a black hole and selective forwarding from IoT-WSN—the entire phase will be extremely active.

In 2021, Abu-Ain, T., et al., [13] had introduced the Dynamic Cluster Head (DynCH) method, makes it automatically to choose WSN CH nodes are calculated depending on the energy and separation of the nodes in mobile WSN node, to analyse the power consumption of the nodes. The complexity of DynCH in various contexts is also included in this analysis to demonstrate its superiority over the stable CH mechanism. Additionally, the study shows that FlexenTech used 52%, Speck128 used 26%, AES used 78%, and TEA used 65% of the wireless network lifetime in contrast to insecure wireless network transmission

In 2021, Poluru, R.K. and Kumar R, L., [14] had proposed an Improved Fruit Fly Optimization Algorithm (IFFOA) for choosing cluster head. The objective is to define CH, optimal clusters, and the amount of energy that each CH candidate has left when the CH algorithm is chosen. Additionally, the described methodology permits CHs to be distributed uniformly across a network of sensors, leading to improved clustering. The findings of the suggested scheme show that the current analysis saves electricity, increases network longevity, and makes the right CH choices.

In 2021, Rathore, P.S., et al., [15] had introduced, the shortest path selection for relay node (SPSRN) process, which chooses a CH from a field of randomly dispersed sensors. The objective of the technique is to enhance the effectiveness of cluster selection to choose cluster pathways. Higher energy consumption is the outcome of densely loaded subcluster nodes and the selected In order to attain normal energy depletion, a trajectory cluster is launched. As a result of the proposed method's lower energy use, the sensors' lifespan was improved.

In 2022, Gurram, G.V., et al.,[16] proposed Secure Energy-Aware Meta-Heuristic Routing (SEAMHR) protocol for WSNs to provide better security and improved performances. It seeks to enhance data transport and energy efficiency, but it ignores data security, making it simple for hackers to get in. The proposed SEAMHR protocol outperforms Heuristic-Based Energy-Efficient Routing (HBEER), Sec Trust-RPL, and Secure and Energy-Aware Heuristic-based Routing (SEHR) all use less energy.

In 2022, Zhou, H. and Bi, H., [17] had developed an enhanced identity encryption-based wireless sensor method. A hybrid chaotic mapping method that meets the needs of wireless sensing networks, the fundamental idea of chaotic system mapping must first be carefully examined. The test outcomes demonstrate that, when compared to other encryption methods, the encryption algorithm suggested in this work runs at a speed of just 18.51 ms, which is faster than that of other techniques.

In spite of the fact that plenty of research is available there are still a few issues that need to be resolved. The search for a secure and ideal network design is an ongoing challenge due to the dynamic nature and restricted resources of sensor nodes. To overcome these challenges, Eurygaster optimized secure shortest path routing (EO-SSPR) approach has been proposed.

3. PROPOSED METHODOLOGY

In this section, a novel EO-SSPR technique is proposed for secure data transmission and to establish the shortest path between the sender and the receiver. The overall block diagram for the proposed technique is given in Figure 1.

3.1. Data acquisition

The sensor data from the patient is monitored and collected here inorder to encrypt the data via the shortest path.

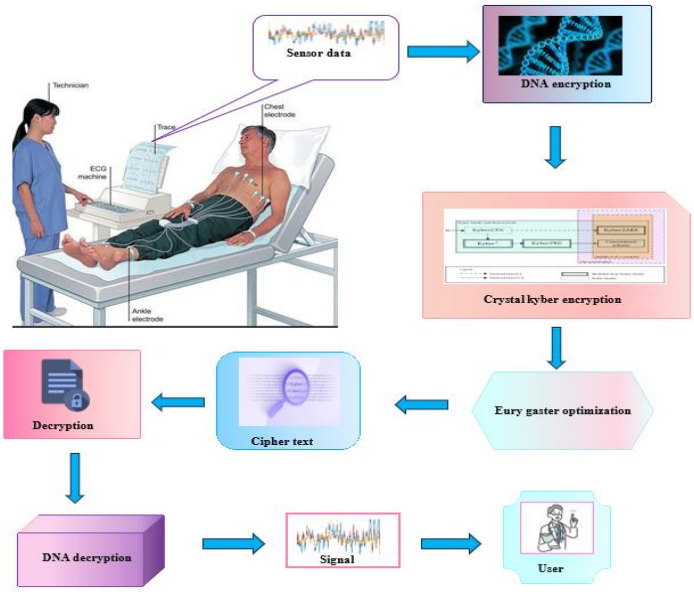

Figure 1. Overall workflow of the proposed EO-SSPR

3.2. DNA encryption

The DNA encryption layer gets information from the sensor and the input for this is the source data, which is in text format. This step involves translating each character in the original data to its corresponding ASCII value before converting it to its binary value. A detailed explanation of the method is provided below.

Consider the message that will be delivered to the recipient, and consider the various procedures for encryption as follows:

Step 1: Each text character is converted to an ASCII code.

Step 2: Convert ASCII code to binary sequence

Step 3: Convert binary sequence to DNA sequence using in the form of nucleotides

Step 4: Extract and separate the sequence using DNA indexing process as represented in table 1.

Table 1. The genetic database's key dictionary

DNA	Key indexing
AAAA	221, 1036, 5002, 32654 ….
AAAT	12, 566, 9354 ….
AAAG	856, 6549, 22354 ….
AAAC	23, 66, 647, 6985, 63745 ….
.....	
CCCC	478, 6324, 26583 ….

The encryption procedure is carried out by substituting a value from the key dictionary for one byte of plain text, as shown in Table 1. The key index as an integer value is the process's final output.

3.3. crystal kyber Encryption

Kyber is based on the module lattice learning-with-errors problem, which is an IND-CCA2-secure KEM. By employing regularization information, IND-CPA cryptography, and a slightly altered Fujisaki-Okamoto (FO) conversion in IND-CCA2 KEM steganography, the entire Kyber protocol can be encrypted or decrypted. Let k, ht, hu, and hv be positive integers and let m=256. Since each message n∈N can be viewed as a polynomial in S with coefficients in {0,1}, let N= 〖{0,1}〗 ^256 represent the message space. The cipher text is (v,u)∈ 〖{0,1}〗 ^(256·kh_v) 〖×{0,1}〗 ^(256·kh_u).

Algorithm :1 Key generation

$\boldsymbol{\delta, \mu} \leftarrow \{\mathbf{0},\mathbf{1}\}^{\mathbf{256}}$

$\boldsymbol{B \sim S_p^{k \times k} := msg(\delta)}$

(r, E) $\sim \boldsymbol{\alpha_n^k \times \alpha_n^k : msg(\mu)}$

$\boldsymbol{t := compress_p\,(B_r + E, h_t)}$

$\boldsymbol{return\ (Pub_k := (t, s), Pr_k := P_k}$

Algorithm:2 Kyber. Enc $(\boldsymbol{Pub_K = (t, \delta)}, \boldsymbol{n} \in \boldsymbol{N})$: $\boldsymbol{encryption}$

$\boldsymbol{s} \leftarrow \{\mathbf{0},\mathbf{1}\}^{\mathbf{256}}$

$\boldsymbol{t := decompress_p(t, h_t)}$

$\boldsymbol{B \sim S_p^{k \times k} := msg(\delta)}$

$\boldsymbol{(s, E_1, E_2) \sim \alpha_n^k \times \alpha_n^k \times \alpha_n := msg(s)}$

$\boldsymbol{v := compress_p(B^T s + E_1, h_v)}$

$\boldsymbol{u := compress_p(t^T s + E_2 + \left[\frac{p}{2}\right] \cdot n, h_u}$

$\boldsymbol{return\ c := (v, u)}$

Algorithm :3 Kyber ($\boldsymbol{Pr_k = P_k}$, c= (v, u)): decryption

$\boldsymbol{v} \coloneqq \boldsymbol{Decompress_p}(\boldsymbol{v}, \boldsymbol{h_v})$

$\boldsymbol{u} \coloneqq \boldsymbol{Decompress_p}(\boldsymbol{u}, \boldsymbol{d_u})$

$\boldsymbol{return\ compress_p}(\boldsymbol{u} - \boldsymbol{r^T u}, \boldsymbol{1})$

3.4. DNA Decryption

Decryption refers to the process of retrieving encrypted data to its original form. This decryption procedure can be carried out remotely or manually. Additionally, a combination of keys or passwords can be used. A specific piece of ciphertext must be decrypted using the same key that was used to encrypt the data. It is the encryption procedure in reverse. The original signal is the output, and the ciphertext is the input.

3.5. Routing encrypted data using Eurygaster optimization

The wireless network sensor is made up of many remotely controllable sensors. There are three nodes in this network: the source, the intermediate, and the destination. A message can be sent from the source node to the destination node in a variety of ways. In order to deliver secure data, but it can be challenging to identify the quickest path. The shortest path determination is crucial for enhancing overall performance, cutting latency, and maximizing network efficiency. To overcome this issue Eurygaster optimization algorithm is utilized.

The place of EG in Q-dimensional space at i is defined as,

$$q^{i+1} = q^i + \mathrm{sf}\,(\mathrm{f}\,(q_{ai}) - \mathrm{f}\,(q_{bi}) * \mathrm{c} * \mathrm{ss}^i \quad (1)$$

$$q_{ai} = q^i + \widehat{dist}^i * \widehat{dir} \quad (2)$$

$$q_{bi} = q^i - \widehat{dist}^i * \widehat{dir} \quad (3)$$

The fitness function (FF) rates f (q_{ai}) and (q_{bi}), which are determined using the suggested model, define the shortest path for data transmission. Presume that the EG swarm properties can be enhanced by using such that D = $d_1,\ldots d_n$.In the D-dimension search space is signified by D_i = $(d_{i1}, d_{i2}, \ldots d_{iD})^T$. The speed of EG (Eury Gaster) is defined by $v_i = (v_i 1, v_i\, 2, \ldots\ldots, v_{iD})^T$. This value of v_i It can be utilized to label the extremes of every EG. Global extreme is defined by $D_i = (dx_{i1}, dx_{i2}, \ldots \ldots dx_{iD})^T$. The EOA places and speeds up the upgrading process as:

$$c_{iD}^{j+1} = c_{iD}^j + \alpha v_{iD}^{j+1} + (1\text{-}\alpha)\mu_{id}^j \quad (4)$$

$$v_{iD}^{j+1} = \theta v_{iD}^j + i_{d1}\mathrm{r}f_1(d_{iD}^i + c_{iD}^j) + i_{d2}\mathrm{r}f_2(dx_{gD}^j + c_{gD}^i) \quad (5)$$

$$\mu_{id}^j = \lambda v_{id}^j \sin(\mathrm{f}(c_{rfd}^j) - \mathrm{f}(c_{id}^j) \quad (6)$$

Where,

$$c_{id}^j = c_{id}^j + v_{id}^j \frac{\hbar}{2} \quad (7)$$

Where $i = 1,2 \ldots n, d = 1,2, \ldots D$ and $j.\mu$ Is the migration value, α and θ Releasing factor and immobility weight. The size of encounters is detailed. $i_{d1}$and i_{d2} , whereas rf_1 and rf_2 Implies the random functions. The approach also allocates Fast. v_i And it's status c_i Arbitrarily. The cost ℏ is designed with $(E)^t$ 0:01 + 0:95()$^{t-1}$. The proposed diagram's outcome semi-code is as follows:

I← the number of clusters

While I ≠ 0 do

Initialization: produce euragasters or particles according to characteristic of one partition Distribution: distribute eurygasters on the regions of the partition

Evaluation: evaluate suitability of each eurygaster or particle depend on the problem

If the suitable result of the partition is not obtained

Change the position of Eurygasters in the partition

goto 3

If the result of the problem is not obtained

I—

goto 1

Else

Stop algorithm or break

End while

Report the solution of the problem.

4. RESULTS AND DISCUSSION

The experimental setup of this study was implemented by using MATLAB. In terms of network throughput, encryption time, end-to-end delay, execution time, decryption time, as well as computational cost, our suggested method is related to the traditional methods SEAMHR [16], SPSRN [15] and DynCH [13].

Table 2. Simulation and Parameter

Simulation	Parameters
Initial Energy	50 J
Base station location	(50,50)
Packet Size	4000 bits
Network size	100m X 100m
Simulation Time	400s
Number of nodes	100
Number of CH	10

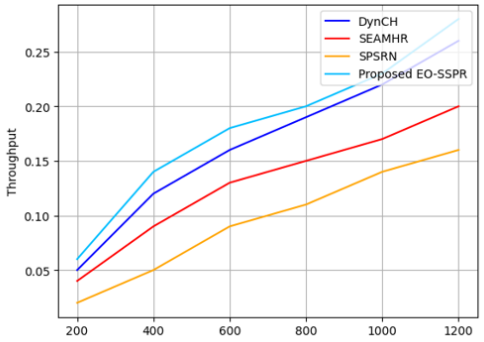

Figure 2. Throughput

Figure 2 displays the comparison between the simulation results and the conventional techniques. Finally, comparing to SEAMHR, SPSRN, DynCH, our proposed technique has received a significant amount of data packets at the BS

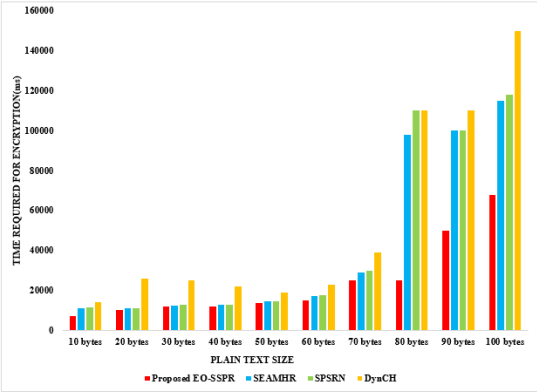

Figure 3. Encryption time analysis

Figure 3 indicates that the encryption time taken by the proposed EO-SSPR for practically all data sizes between 10 KB and 100 KB is lower than all other existing techniques process, The E0-SSPR proposed in this research has the lowest encryption time.

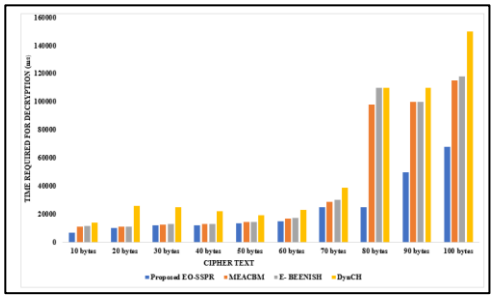

Figure 4. Decryption time analysis

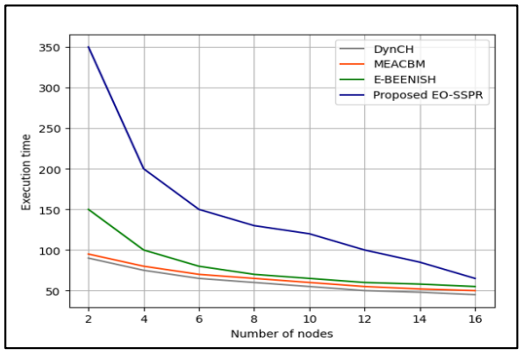

Figure 5. Execution time analysis

Figure 4 shows that the decryption time taken by the proposed EO-SSPR is lower than the other techniques and figure 5 shows a plot of the number of nodes and the training time. The amount of data required for training must be adequate; otherwise, performance might be impacted by the overhead of parallelization.

5. CONCLUSION

In this research, EO-SSPR has been proposed to determine the shortest path and to transmit data securely. The proposed EO-SSPR technique provide Two-layer encryption for secure data transmission. In first layer the key generation and data encryption is done by crystal kyber encryption for privacy preserving and secure data encryption. In the second layer, DNA cryptography is utilized for data encryption and decryption to protect the confidential data from unauthorized user. The Eurygaster optimization is used to identify the shortest path between the nodes. The proposed framework is compared with traditional frameworks such as DynCH, SEAMHR, SPSRN in terms of throughput, encryption and decryption time and execution time. The proposed technique improves the encryption and decryption time by 12.03%, 8.57%, 4.01% better than DynCH, SEAMHR, SPSRN. The experimental results shows that the proposed SSPR approach performs better than the current model.

CONFLICTS OF INTEREST

This paper has no conflict of interest for publishing.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] I. Daanoune, B. Abdennaceur, and A. Ballouk, "A comprehensive survey on LEACH-based clustering routing protocols in Wireless Sensor Networks," *Ad Hoc Networks*, vol. 114, pp. 102409, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] S. Muthukumar, A. Hevin Rajesh, and D. Jenice Prabhu, "Reduancy aware dynamic routing protocol using salp swarm optimization algorithm," *International Journal of System Design and Computing*, vol. 01, no.01, pp. 35-42, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] D.E. Boubiche, S. Athmani, S. Boubiche, and H. Toral-Cruz, "Cybersecurity issues in wireless sensor networks: current challenges and solutions," *Wireless Personal Communications*, 117, pp. 177-213, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] K. Vijayan, S.V. Harish, and R.A. Mabel Rose, "Chicken Swarm Optimization Based Ensembled Learning Classifier For Black Hole Attack In Wireless Sensor Network," *International Journal of Data Science and Artificial Intelligence*, vol. 02, no. 04, pp. 110-120, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] J. Ramasamy, and J.S. Kumaresan, "Image encryption and cluster based framework for secured image transmission in wireless sensor networks," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1355-1368, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Jeyaraman Sathiamoorthy, M. Usha, and P. Senthilraja, "SELECTIVE FORWARDING ATTACKS DETECTION IN WIRELESS SENSOR NETWORKS USING BLUE MONKEY OPTIMIZED GHOST NETWORK," *International Journal of Data Science and Artificial Intelligence*, vol. 02, no. 03, pp. 74-80, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] T. Srinivas, and S.S. Manivannan, "Black Hole and Selective Forwarding Attack Detection and Prevention in IoT in Health Care Sector: Hybrid meta-heuristic-based shortest path routing," *Journal of Ambient Intelligence and Smart Environments*, vol. 13, no. 2, pp. 133-156, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] M. Prabhu, B. Muthu Kumar, A. Ahilan, "Slime Mould Algorithm based Fuzzy Linear CFO Estimation in Wireless Sensor Networks," *IETE Journal of Research*, pp. 1-11, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] W. Xia, C. Di, H. Guo, and S. Li, "Reinforcement learning based stochastic shortest path finding in wireless sensor networks," *IEEE Access*, vol. 7, pp.157807-157817, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] M. Ramya Devi, K.V. Sreelekha, and R. Jayaraj, "JARROT BUTTERFLY OPTIMIZED FLAMINGO SEARCH ALGORITHM FOR OPTIMAL ROUTING IN WSN," *International Journal of Data Science and Artificial Intelligence*, vol. 02, no. 02, pp. 48-54, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] P.S. Mehra, M.N. Doja, and B. Alam, "Fuzzy based enhanced cluster head selection (FBECS) for WSN," *Journal of King Saud University-Science*, vol. 32, no. 1, pp. 390-401, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] T. Srinivas, and S.S. Manivannan, "Black Hole and Selective Forwarding Attack Detection and Prevention in IoT in Health Care Sector: Hybrid meta-heuristic-based shortest path routing," *Journal of Ambient Intelligence and Smart Environments*, vol. 13, no. 2, pp. 133-156, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] T. Abu-Ain, R. AHMAD, and E.A. Sundararajan, Analysis the Effect of Dynamic Clustering and Lightweight Symmetric Encryption Approaches on Network Lifetime in WSNs, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] R.K. Poluru, and R, L. Kumar, "An Improved Fruit Fly Optimization (IFFOA) based Cluster Head Selection Algorithm for Internet of Things," *International Journal of Computers and Applications*, vol. 43, no. 7, pp.623-631, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] P.S. Rathore, J.M. Chatterjee, A. Kumar, and R. Sujatha, "Energy-efficient cluster head selection through relay approach for WSN," *The Journal of Supercomputing*, vol. 77, pp. 7649-7675, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] G.V. Gurram, N.C. Shariff, and R.L. Biradar, "A secure energy aware meta-heuristic routing protocol (SEAMHR) for sustainable IoT-wireless sensor network (WSN)," *Theoretical Computer Science*, vol. 930, pp. 63-76, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] H. Zhou, and H. Bi, "Wireless Sensor Network Security Based on Improved Identity Encryption," *Scientific Programming*, vol. 2022, 2022. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

T. Rajesh has completed B.E in ECE at M.S University in the year 2003 , M.E in Applied Electronics at Anna university in the year 2006 and Ph.d in Information and Communication Engineering at Anna university during the year 2019.He is working as an Professor at PSN College of Engineering and Technology. He is having 19 years of teaching experience. His research interests are medical image Processing and wireless communication. He has published more than 30 papers in national and international journals

S. Sony Helen is a dedicated Full-Time Research Scholar in the Department of Information and Communication Engineering at Anna University, India. With a profound interest in cutting-edge technologies, her research spans diverse areas such as Image Processing, Networking, the Internet of Things, Cloud Computing in Medical, and Cryptography. Having showcased her scholarly achievements on an international stage, Ms. Helen has presented her research at prestigious conferences, contributing valuable insights to the academic community. Her academic journey includes roles as a Lecturer in the Department of Computer Science and Engineering at Bhajarang Engineering College, Chennai, India. Additionally, she has served as a Software Faculty for MCA, BCA, and PGDCA at the Alagappa University Study Center, India. In these capacities, she has imparted knowledge and nurtured the academic growth of her students. As a versatile developer, she specializes in diverse domains, including but not limited to Computer Networks, Medical Systems, Computer and Electrical Engineering, Neural Computing and Applications, Cluster Computing, and Image Processing. Her proficiency in these areas reflects a keen understanding of technological trends and a commitment to pushing the boundaries of innovation. Her dynamic contributions to academia and research position her as a valuable asset in the pursuit of knowledge and technological advancement. Her dedication to excellence and continuous learning underscores her commitment to making meaningful contributions to the ever-evolving landscape of information and communication engineering.

Arrived: 15.07.2024
Accepted: 19.08.2024