Journal of Advanced Research in Applied Sciences and Engineering Technology 32, Issue 3 (2023) 421-437

SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Fuzzy Enhanced Black Widow Spider with Secure Encryption Random Permutation Pseudo Algorithm for Energy Efficient Cluster Communication in WSN

M. S. S. Sasikumar[1,*], A. E. Narayanan[2]

[1] Periyar Maniammai Institute of Science & Technology, India
[2] Department of Computer Science and Engineering, Periyar Maniammai Institute of Science &Technology, Vallam, Thanjavur, India

ARTICLE INFO

Article history:
Received 23 June 2023
Received in revised form 10 August 2023
Accepted 4 October 2023
Available online 24 October 2023

Keywords:
Cluster; Energy Consumption; Internet of Things (IoT); Network lifetime, Sensor Node;

ABSTRACT

Internet of Things (IoT)-connected devices are being used more and more often. With the aid of these extensions, contemporary mobile apps can be added to low-cost, low-power gadgets. By utilizing inexpensive, low-power sensor nodes, this integration is made achievable. To other receivers or nodes, all sensor nodes either directly broadcast data or do so via a multi-hop path. To enable effective inter-cluster communication through ideal cluster head selection, we build a fuzzy-enhanced black widow spider based on the Secure Encrypted Random Permutation Pseudo Algorithm (FEBWS-SERPPA) in this study. By taking energy, latency, and distance characteristics into account, the suggested FEBWS-SERPPA algorithm enhances the black widow spider optimization method by choosing the optimal cluster head in the cluster. The suggested FEBWS-SERPPA algorithm's performance is evaluated against state-of-the-art methods to ensure its efficacy. In comparison to existing techniques, the proposed FEBWS-SERPPA algorithm provides improved performance speed with exceptionally low energy usage and longer network lifetime. This study utilizes the CRAWDAD dataset for simulating the Wireless Sensor Network (WSN) environment, further enhancing the validity of the proposed approach.

1. Introduction

The creation of wireless sensor networks (WSNs) for environmental monitoring, tracking systems, and disaster management is a result of global technological breakthroughs. Improved sharing protocols can reduce energy usage and increase network longevity. Reduce the amount of energy used when moving data inside a cluster [1]. IoT technology from WSN gathers data from linked networks about the actual world. IoT improves network sharing of WSNs and uses less energy. To protect user information, certain networks are being blocked from receiving data [2]. WSNs have a small number of low-cost nodes and inexpensive sensors, incorporating battery, communication, and detection frameworks. Unique nodes include sensor nodes. The node may send data until the battery

---

[*] *Corresponding author.*
E-mail address: Sasi7273@gmail.com

https://doi.org/10.37934/araset.32.3.421437

it uses from a fully charged node [3] since it cannot be changed. The fundamental equipment and its operations are used to translate the nodes' data into the desired outcome to make a decision. To improve network performance, power consumption must be decreased [4-8].

The base station (BS) and the WSN can be regulated by the sensor nodes, or the BS can receive data directly from the sensor nodes. Control information overflow at the gateway to conserve energy and increase battery life and when trying to maximize performance and reduce current energy leakage, Grey Wolf Optimization (GWO) keeps monitoring on sensor nodes [9-12]. Today, a wide range of IoT applications are commonplace in our environment. The majority of these fall under widespread categories, such as smart homes, smart grids, smart healthcare, and smart transportation. Nevertheless, increasing adoption has brought up several IoT problems, including a lack of hardware, memory resources, computing power, operational traits, large-scale data transfers, diverse data, and various network architectures [13-15].

Data integrity, data security, and individual privacy are further significant IoT issues that need to be addressed, especially with low-resource devices and heterogeneous technologies [16-18]. One of the best techniques to safeguard the privacy of data and conversations is encryption. Moreover, authentication services and message integrity are ensured by encryption. It should be noted that the IoT era makes it extremely difficult or difficult to deploy additional security measures once the manufacturing process is complete because the majority of IoT devices are "closed by design." On the other hand, the available encryption techniques are constrained by the IoT devices' constrained software and hardware resources.

As a result, the desired level of performance and security must be carefully balanced [19]. Users must make their judgments while taking into account both the hardware deployed and the constraints of their IoT applications due to the reason that there is a probability of various quantities of resources and power being used by algorithms that provide the same security level. Decide which option best meets your needs [20]. Because they process data more slowly than symmetric encryption algorithms, public key encryption solutions consume more energy and resources [21]. Asymmetric design should be incorporated into IoT security solutions.

WSN's energy efficiency may be used in the agriculture industry as well. Laws governing precision agriculture (PA) are implemented on fields to manage and direct crops to certain environmental conditions [22]. WSNs collected in sizable agricultural regions may clog the network with traffic. With programmable system-on-chip (PSoC) technology, it may be reduced [23]. Consumer devices also employ wireless sensor networks. The lifespan of the network is shortened by high node workloads. As a result, cluster heads (CH) assign each network's nodes on an individual basis [24-26]. Sensor nodes can send out notifications and keep track of events when significant events happen so that users can make decisions.

In this paper, a clustering method was presented that enhances packet transfer from source to destination. The following is an explanation of this text's major goal:

- For energy-efficient cluster communication, a Fuzzy Enhanced Black Widow Spider (FEBWS-SERPPA) technique with a safe cryptographic random permutation pseudo-algorithm is presented.
- The optimal cluster head is chosen among clusters using the suggested FEBWS-SERPPA method, which takes energy, delay, and distance characteristics into account.
- For energy-effective communication, a “Secure Encrypted Random Permutation Pseudo Algorithm” (FEBWS-SERPPA) has been employed.
- For evaluating the proposed FEBWS-SERPPA algorithm’s performance, several modern algorithms have been utilized.

The organization of this paper is as follows: Section 2 entails a detailed description of plentiful investigations based on power-efficient WSN is presented. Chapter 3 discusses the system model, while Chapter 4 discusses the recommended approach. Section 5 presents the findings as well as the analysis. Sections 6 and 7 conclude the work.

2. Literature Survey

The energy effectiveness of WSN was investigated by Ajimi and others [27] using a population-based genetic algorithm. The primary issue with WSNs is their short battery life. A genetic method based on battery level is improved by Multi Weight Chicken Swarm (MWCSGA). The created technique was evaluated against several variables, including CSOGA and LEACH. As a consequence, precision was attained.

A secure key management strategy for WSN was also suggested by Ahankari *et al.*, [27]. In the described method, authentication and secure key management are provided by elliptic curve cryptography. Furthermore, the suggested approach uses a novel technique based on discrete algebra problems to strengthen security by repelling multiple security assaults. Karpagalakshmi *et al.*, [28] used methods for coordinating the use of group session keys across server and sensor node communications. This strategy is founded on the well-liked AES symmetric key encryption. A close examination of the output of the program revealed that the designs were pricey and extremely safe.

The main problem with these systems is that the base station (BS) does the AES decryption. It is difficult to authenticate sensor nodes effectively in a specific WSN environment. When it comes to energy conservation, resistive cryptography makes use of the least amount to assure rigidity between sensor nodes and ECC-based encryption is a reliable key management technique [29]. In this paper, we evaluate the performance of algorithms based on RSA and ECC. Depending on the output, ECC-based algorithms outperform RSA-based algorithms. However, using RSA for the same technology in the IoT environment requires different network resources [30].

A set of fundamental agreements was presented by Suvitha *et al.*, [31]. The suggested working session key is set between the sensor node and the gateway (GW) for a preset period. The session key will be regenerated for that particular session if network alterations or failures occur. The suggested method also offers implicit WSN node authentication [32]. The suggested approach minimizes network failures and is scalable. The high cost of connection and computing is the project's biggest obstacle, though. Multipasskeying is a method for encrypted communications.

Information transfer that is secure and trustworthy is a fundamental benefit of the suggested study activity. Secure session key agreement is performed using Reed-Solomon codes and the PSMT (Perfectly Secure Message Transmission) protocol throughout each round. The initial consensus steps were not adequately discussed in this study effort. Using the ant colony optimization-based routing algorithm (ACO-RA), an energy-efficient routing system for WSNs was developed [33]. One of the primary issues that WSNs solve is the fact that network lifetime can only be extended with the help of energy efficiency. The ACO-RA system is suggested investigation as a remedy for this problem. ACO-RC uses pseudorandom pathfinding to balance WSN's energy consumption [34]. As a result, our assessment variables outperform those from earlier methodologies.

The cluster is also unusable and unable to handle any network protocols at the same time. Using the RNN-LSTM (Long Term Memory Recurrent Neural Network) method, Venkataramanan *et al.*, [35] took advantage of the energy efficiency of WSNs. The major goals of this research are to decrease the quantity of sent data and limit the overhang of the fusion center in a wireless sensor network (WSN). To verify the signal spacing and the quantity of unstable secret nodes, this research develops an RNN-LSTM model [36]. As a result, the created RNN-LSTM model eliminates dangling signals and achieves an optimal minimum latency of 190 ms. On the other hand, training this model is challenging.

There is a delay in accurate solution identification. Sampathkumar *et al.*, [37], Ramanan *et al.*, [38] and Arumugam *et al.*, [39] used the PSO (Particle Swarm Optimization) technique to build a wireless sensor network (WSN) routing protocol. The key difficulty is addressing wireless sensor networks' low power consumption issue. We offer PSO to deliver energy usage and computation weights for each sensor node to address this issue. The PSO method outperforms the Weighted Rendezvous Planning algorithm, according to experimental findings. In similar study, Sarbini *et al.,* [40] used a well-known modulus attack to assess LUC, LUC3, and LUC4,6 cryptosystems security factors.

A common modulus attack demands that the message be sent to two different receivers with the same modulus. When confronted with a common modulus attack, the LUC, LUC3, and LUC4,6 cryptosystems' advantages and disadvantages were also explored. From the results, it was seen that the LUC4,6 cryptosystem outperforms in terms of security than LUC and LUC3. A cyber security scanning tool namely Nessus was developed by Ali *et al*., [41] to resolve analysis report management issues. The system's objective was to track and assess the maintenance of cyber security while concentrating on vulnerability reporting. Web-based technologies were used in its creation. During the development phase, the prototype-rapid application development process was used to make sure that the prototyping system could be used right away.

3. System Model

As illustrated in Figure 1, the proposed model takes into account a sensor network made up of "Y" sensor nodes, "m" cluster heads (AN), and base stations. The GPS (Global Positioning System) system determines the location of each node. GPS gathers the nodes' latitude and longitude and determines the distance between them. To determine the distance from the base station (BS) to each node, we use the Habergin distance method described in [59]. Every node has a distinct ID (ID), and BS's ID is 0.

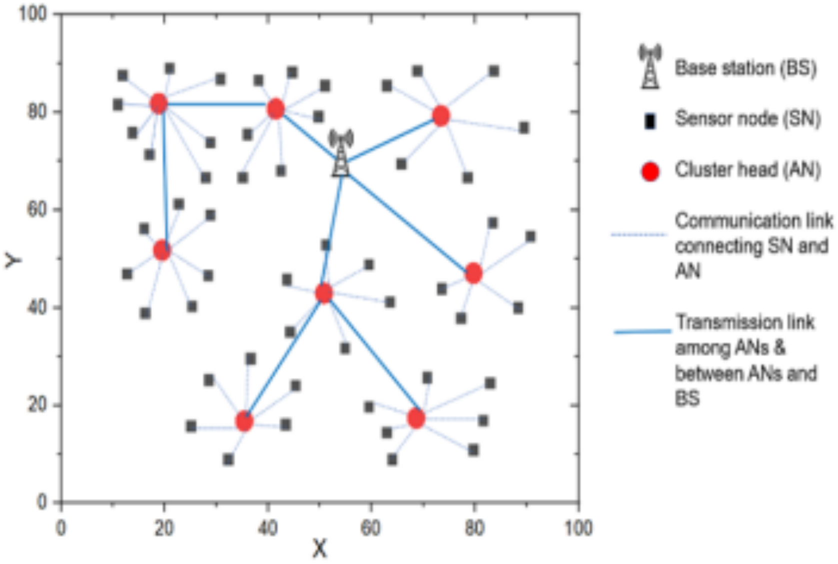

Fig. 1. A Clustered WSN with Cluster Heads and a Base Station

- The suggested algorithm takes into account the following presumptions.
- The number of BSs is set to 1 because there is only one BS on the network.
- The cluster head's forwarding range includes all cluster members.
- The range of each cluster head's communication with the cluster heads adjacent to it.
- Each cluster member transmits information to the cluster leader each iteration.
- Only the cluster head may connect to the base station directly; nodes are unable to send data there.
- Nodes are seen as being in motion, and each iteration updates the location of the cluster head.

As shown in Equation (1) Energy dissipation at the transmitter and receiver follows a multipath fading paradigm. If the distance between the source (sender) and the receiver (receiver) "d" is less than a threshold "th," the energy cost for sending "b" bits in a packet is supplied by.

$$E_s = b * (E_{el} + E_{free} * d^2) \tag{1}$$

As shown in Equation (2) The energy of the starting node "E_s " is provided by: if "d" signifies a value larger than or equal to the threshold " th "

$$E_s = b * (E_{el} + E_{mfad} * d^4) \tag{2}$$

where "E_{free}" denotes energy used in space, "E_{el}" denotes energy used to mimic electricity in electronic circuits, and "E_{mfad}" denotes energy used in multipath fading as shown in Equation (3). The definition of threshold " th " is

$$th = \sqrt{\frac{E_{free}}{E_{mfad}}} \tag{3}$$

As shown in Equation (4), The following energy is expended to get packet bit "b":

$$E_r = b * E_{el} \tag{4}$$

where "n" denotes the number of messages and "EANagg" is the amount of energy required to gather a few packets.

4. The Proposed Methodology

This section uses the Secure Encrypted Random Order Pseudo Algorithm (FEBWS-SERPPA) technique to show how a clustering fuzzy-enhanced black widow spider may transport packets from source to destination efficiently. A wireless network of "n" nodes first forms a cluster of neighboring sensor nodes. Data transmission through ideal nodes and power-saving pathways must be made possible by a longer network lifespan. The best cluster head is picked by the proposed FBWS-SERPPA algorithm among the cluster nodes, and this cluster head sends data to BS over the selected channel.

To enhance cluster communication, one might choose an energy-efficient path to the base station. The clustering strategy's energy efficiency is shown in Figure 2.

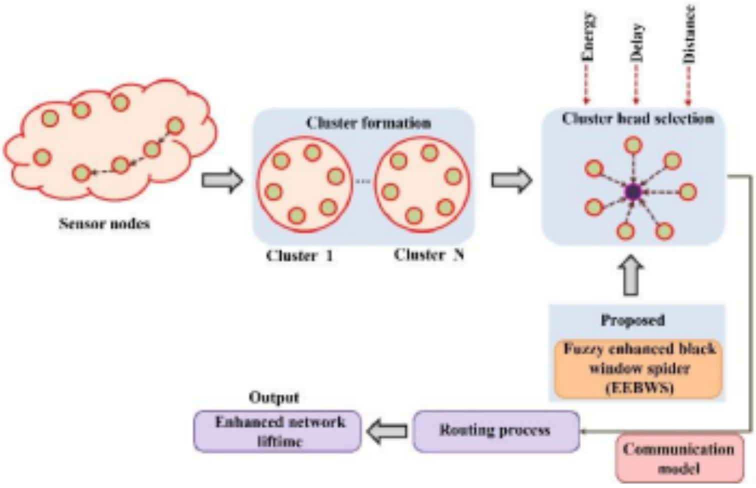

Fig. 2. Structure of proposed energy efficient clustering approach

Cluster Formation

The cluster head is often located by the base station (BS) sending hello packets by group to the node that was chosen as the cluster head. The nodes select the ideal location for the cluster head and incur the least amount of communication costs. Next, choose CH, greet the node with a hello packet, and pick a child node (CN).

Selecting Cluster Head

To facilitate efficient communication between clusters, this work creates a novel FEBWS-SERPPA approach that improves cluster head selection. Below is a thorough explanation of each approach.

Fuzzy Logic System

Instead of describing discriminating functions, fuzzy logic sets describe membership functions. A fuzzy set has a value of either 1 or 0. The membership function represents the probability of each element in the collection of elements. The [0,1] range of the membership function is where it lies. If the membership function is zero, then objects do not match the collection of elements. The object must match the collection of elements if the membership function has an interval of 1. Control strategies for fuzzy logic are described by conditional statements that are not equations. The viability of any plan may be assessed using interference rules. Purge, condition evaluation, and non-purge are the three steps of fuzzy logic control [26].

Phase 1: Fuzzification

All fuzzy logic control systems are implemented through the development of fuzzy rules. The following is a description of the fuzzy rules.

The Condition 1:
If E is $g1$ and F is $h1$, then I will be $j1$;

The Condition 2:
If E is $g2$ and F is $h2$, then I will be $j2$;

According to their classification, the aforementioned conditions include condition parameters, response parameters, and fuzzy variables. These variables are recorded as g_m, h_m *and* $j_m$respectively. The fuzzy interface program, on the other hand, has two conditions as well as a membership function. Determine the condition parameters of the membership function by $\lambda_{g1}(e)$ and $\_\lambda_{h1}(f)$ of condition 1; condition 2. Assume that $R1$and $R2$ are intervals. As a result, the associated purge parameters and the measured values are in agreement.

Phase 2: Evaluating Condition:
Subsequent conditions $E = e$ and $E = f$ can be appended if the fuzzy control criteria are satisfied during conditional execution.
Condition1: $\lambda_{g1}(e) \wedge \lambda_{h1}(f)$;
Condition 2: $\lambda_{g2}(e) \wedge \lambda_{h2}(f)$;

The operator represents the bare minimal function for conditional execution, and the aforementioned criteria reflect the formation of conditions 1 and 2. As the spacing for the output parameter was R3, which. The result of the $\lambda_{gm}(I)$) membership function is the sum of all membership functions. Here is the equation for this circumstance.

$$\lambda_g(I) = \lambda_{a1}(I) * \lambda_{a2}(I) \tag{5}$$

As shown in Equation (5), the * operator denotes the extent to which conditional execution can go.

Phase 3: Defuzzification
Rational conditions produce actual values which can be given as input to a fuzzy logic control system. Still, it is possible to reach the end value of the fuzzy logic control system (I) even though the desired outcome is not fuzzy.
This is an explanation of how to employ the gravity area (COA) approach during the purge phase.

$$Y_{coa} = \frac{\int_y \lambda s(Y)Yey}{\int_y \lambda s(Y)Ye} \tag{6}$$

As shown in Equation (6), the logarithmic integral of all elements of the fuzzy output piecewise membership function of domain A is recorded as $\int_y$. The area of Y_{coa} on both sides is the same.
Enhanced Black Widow (EBW) Spider Optimisation
To initialize the population, use EBW optimization in the rand function. To begin the population and increase the algorithm's diversity, a Gaussian chaotic map is inserted [19]. You may use algorithms to locate places that offer high-quality solutions. enhancing and accelerating the algorithm's rate of convergence as shown in Equation (7) and (8). The Gaussian map, often known as a traditional one-dimensional map, is denoted by

$$a_{y+1} = \{0, a_y = 0 \ \frac{1}{a_y MO(1)}, a_y \neq 0 \tag{7}$$

$$\frac{1}{a_y MO(1)} = \frac{1}{a_y} - \left[\frac{1}{a_y}\right] \tag{8}$$

The residual function is denoted by MO in the formula above. Round the tokens and use a Gaussian $a1$, $a2$, ... , ay to create a chaotic sequence.

The Secure Encryption Random Permutation Pseudo (SERPPA) Algorithm

The SERPPA Algorithm is an innovative encryption technique that builds upon the principles of the Advanced Encryption Standard (AES). SERPPA is designed to provide robust and energy-efficient encryption for data, while also ensuring data security. This algorithm is capable of handling messages of varying lengths, including 128, 192, 256, and 512 bits, offering enhanced protection for sensitive information [31].

In the architecture of SERPPA, several key operations derived from AES contribute to the encryption and decryption processes. These include byte permutation, column shuffle, row shift, and round key operations. The process begins by segmenting sensor node data into manageable 512-bit units, eliminating redundant characters. Byte replacement techniques are employed during the encryption and decryption of these segments. A designated key value is assigned, and to address character gaps, special characters are introduced.

Algorithm 1 governs the decryption process, ensuring the integrity of the data throughout. Additionally, the SERPPA architecture incorporates a crucial key management mechanism that enables the encryption and decryption processes for sensor nodes. This mechanism involves key assignments and basic character processing, ensuring secure communication. The overall architecture of SERPPA is visually depicted in Figure 3, which illustrates the data flow within sensor nodes and outlines the encryption process. Moreover, the architecture underscores the importance of a secure gateway, as depicted in Figure 3. This gateway acts as a shield, protecting user devices from potential threats and malware. By filtering traffic and encrypting data, it enhances security during interactions between user devices and the internet.

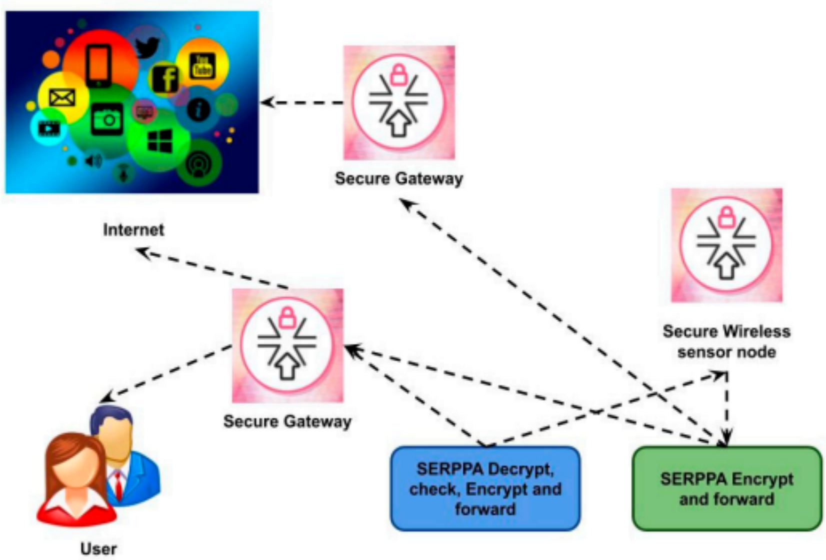

Fig. 3. Architecture of SERPPA

A pivotal aspect of SERPPA's design is its integration with Time Division Multiple Access (TDMA) technology, which facilitates efficient data transmission. The architecture also incorporates Cluster Heads (CH) responsible for organizing clusters of sensor nodes. The selection of the CH is influenced by the Low Energy Adaptive Hierarchy of Clustering (LEACH) method. LEACH employs both the

Medium Access Control (MAC) protocol and TDMA technology to optimize energy consumption within the network. This approach is vital in extending the lifespan of sensor cluster nodes and reducing energy consumption levels.

Algorithm 1 of SERPPA is designed to ensure the confidentiality of messages during the encryption process. It involves the assignment of encryption vectors and key values to different segments of the input message. This iterative process guarantees the security of the transmitted data.

Algorithm 1: of SERPPA

```
    Begin
        start the process of getting 512-bitlength inputs
          remove the presence of same character at multiple times
    do
        assign the encryption vector values [5,15,22,8,9,11] for the 512 bits
    where “x” is first character
    ex: x = 5 of key length is assigned
    then
          taken key [15,22,8,9,11]
    assign to remaining characters of 512 bits
    if
          presence of space between a letter
          assign a special character (\, #, $, &, *)
    end
    do
    encryption
          apply k = [5,15,22,8,9,11] values to first set of 512 input message
    next
          apply k = [11,9,8,22,15,5] to next set of same 512 input message
          Continue . . .
          Stop once the character get over
          end
          end
end
```

Intra-Cluster Communication

To reduce network lifespan and maximize energy consumption, long-distance communications are employed. The member nodes are used to immediately choose the optimal relay node by calculating the energy consumption cost of data transmission on various routing patterns. The routing path computation's energy usage is stated by Gopalan *et al.*, [20].

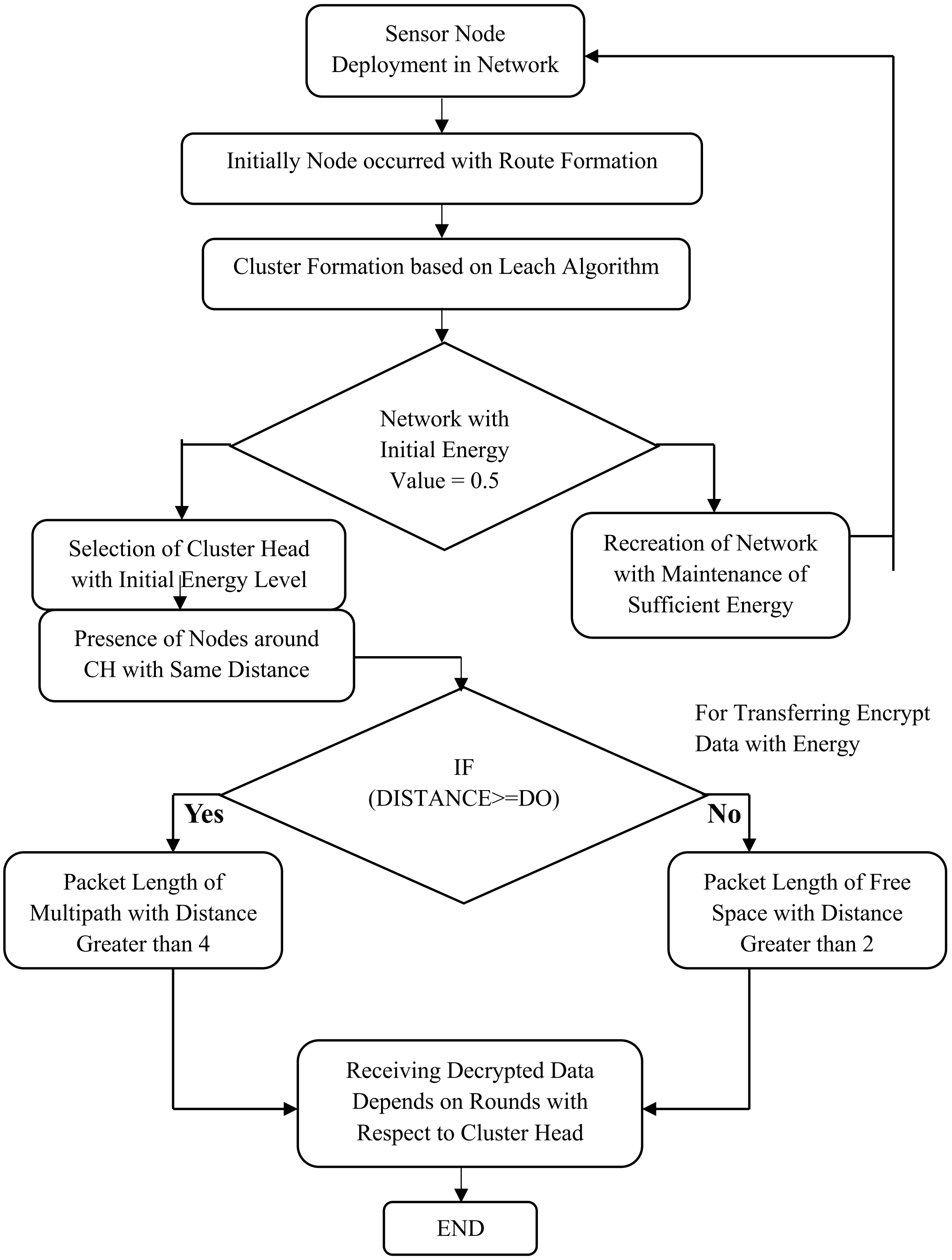

Fig. 4. Illustrates the amount of energy used when sending and receiving encrypted and decrypted data

$$E_1(\delta_j, CH_{\delta j}) = \begin{cases} \tau . E_e + \tau . \epsilon_{gt} . e(\delta_j, CH_{\delta j})^2 if e(\delta_j, CH_{\delta j}) < e_0 \\ \tau . E_e + \tau . \epsilon_{nq} . e(\delta_j, CH_{\delta j})^4 \ if e(\delta_j, CH_{\delta j}) \geq e_0 \end{cases} \quad (9)$$

(δj , $CH\delta j$) The calculation above that is shown in equation (9) stands for the distance between CH and node k. Calculating and expressing the total energy usage is as follows, as shown in Equation (10):

$$E_2(\delta_j, \delta_k, CH_{\delta j}) = E_{rx}(\tau, e(\delta_j, \delta_k)) + E_s(\tau)$$
$$+S_{rx}(\tau, e(\delta_k, CH_{\delta j}))$$
$$=3\tau . E + \epsilon . e^2(\delta_j, \delta_k) + \epsilon . e^2(\delta_k, CH_{\delta j}) \quad (10)$$

The Equation (11) formulas are used to compute and produce intra-cluster communication:

$$E(\delta_j) = MIN(E_1(\delta_j, CH_{\delta j}), E_2(\delta_j, \delta_k, CH_{\delta j})) \quad (11)$$

Inter-Cluster Communication

To avoid long-distance communication, design chains, and the Gridi algorithm are utilized for inter-cluster communication. There are two phases in the chain creation process:
Step 1: The sink transmits a chain creation message in step one to identify all cluster heads and report their locations.
Step 2: The nearest CH is chosen as the leader when the washbasin gets the data from the cluster head. The leader CH assists in sending packets straight to the washbasin.
Step 3: The relay cluster heads, which are extremely near to the sink, receive data packets from all the cluster heads collected via the Griddy method.

5. Feature Extraction

To properly assess the performance of the newly suggested FEBWS-SERPPA algorithm, a collection of attributes was derived from the simulated data. These attributes offer understanding into different facets of network functionality and energy effectiveness. The features that were obtained, along with their comprehensive explanations, are presented in Table 1.

Table 1
Extracted Features and Detailed Descriptions

Sl. no	Feature	Description
1	Energy Efficiency	Calculated efficiency of energy consumption
2	Network Lifetime	Duration for which the network remains operational
3	Throughput	Rate of successful data transmission
4	End-to-end Delay	Time taken for data to travel from source to destination
5	Packet Drop	Number of packets dropped during transmission
6	Packet Delivery Ratio	Percentage of successfully delivered packets
7	Energy Consumption	Total energy used by the network
8	Dataset [42]	The CRAWDAD dataset used for simulating the WSN environment

These extracted features provide a comprehensive understanding of the performance and efficiency of the proposed algorithm in the context of the WSN environment.

6. Experimental Results and Discussions

In this section, an algorithm called (FEBWS-SERPPA) Fuzzy Enhanced Black Widow Spider with Secure Cryptographic Random Permutation Pseudo Algorithm was suggested for increasing the WSNs energy efficiency. A variety of performance metrics was used by the NS-2 simulator to gauge how well the proposed FEBWS-SERPPA algorithm performs, including the features listed above. The full description of the simulation settings can be found in Table 2, and the subsections that follow provide a concise summary of the simulation's outcomes.

Table 2
The Parameters of Simulation

Sl. No	The Parameters of Simulation	Ranges
1	Initial energy	0.5 J
2	Number of nodes	100
3	Simulator	NS-2.34
4	Coverage area	1000×1000
5	Simulation Period	100ms
6	Packet size	4000bits
7	Cluster head percentage	0.05
8	Dataset	CRAWDAD Dataset [42]

Performance Analysis

Other metrics are used to assess how well the suggested FEBWS-SERPPA algorithm performs. Table 3 provides references for the suggested FEBWS-SERPPA algorithm's overall performance.

Table 3
Analyzing Overall Achievements

Sl. No	Performance Indicators	Rate of Performance
1	Energy efficiency	93%
2	Lifetime of the Network	1395 seconds
3	Throughput	684kbps
4	End-to-end delay	85ms
5	Packet drop	110 packets
6	Packet delivery ratio	99%
7	Energy consumption	52%

Comparative Analysis

Table 4 displays the results of an investigation of the nodes' energy efficiency using several approaches, including the ACI-GSO technique, the MWCSGA algorithm, the RNN-LSTM model, the PSO technique, and the FEBWS-SERPPA algorithm. It was discovered that a 93% efficiency was possible in studies using 100 nodes. The suggested FEBWS-SERPPA algorithm outperforms other established techniques. We discovered energy efficiencies of 79%, 85%, 71%, and 62% for the ACI-GSO approach, the MWCSGA algorithm, the RNN-LSTM model, and the PSO technique, respectively.

Table 4
Comparative evaluation based on energy efficiency

No. of nodes	ACI-GSO	MWCSGA	RNN-LSTM	PSO	Proposed
20	16	20	14	10	24
40	31	38	20	18	44
60	49	55	41	36	65
80	60	74	48	44	80
100	79	85	71	62	93

The proposed FEBWS-SERPPA technique, the ACI-GSO technique, the MWCSGA approach, the RNN-LSTM method, and the PSO technique are used in Table 5 to present the end-to-end latency analysis. Almost no end-to-end latency is present in the FEBWS-SERPPA algorithm. While improving the energy efficiency of WSN, the suggested FEBWS-SERPPA algorithm provides a low end-to-end latency of 85 ms.

Table 5
Evaluation of end-to-end latency comparison

No. of nodes	ACI-GSO	MWCSGA	RNN-LSTM	PSO	Proposed
20	46	35	55	75	25
40	65	47	64	125	37
60	98	75	78	120	62
80	104	82	160	200	78
100	160	105	240	270	85

Several techniques, including the MWCSGA technique, the RNN-LSTM approach, the PSO algorithm, and the FEBWS strategy, are shown in Table 6 along with their respective packet loss statistics. With only 110 packets lost, the suggested FEBWS-SERPPA technique surpasses the standard FEBWS-SERPPA technique. The ACI-GSO strategy, the MWCSGA technique, the RNN-LSTM approach, and the PSO technique all experience packet losses of 345, 158, 468, and 627, respectively, in comparison to the other strategies.

Table 6
Comparative evaluation of packet drops

No. of nodes	ACI-GSO	MWCSGA	RNN-LSTM	PSO	Proposed
20	81	42	116	158	32
40	120	85	226	278	45
60	232	125	274	382	86
80	277	148	379	475	103
100	345	158	468	627	110

ACI-GSO, MWCSGA, RNN-LSTM, PSO, and the recently developed FEBWS-SERPPA strategies are just a few of the techniques used to present the node throughput analysis in Table 7. In this side-by-side comparison, a high throughput of 684 kbps is achieved using the proposed FEBWS-SERPPA algorithm. Throughputs of 425 kbps, 625 kbps, 256 kbps, and 198 kbps were achieved, respectively, using the ACI-GSO strategy, MWCSGA method, RNN-LSTM model, and PSO algorithm.

Table 7
Comparative evaluation of throughput

No. of nodes	ACI-GSO	MWCSGA	RNN-LSTM	PSO	Proposed
20	125	194	178	102	205
40	214	268	195	137	353
60	356	592	185	168	589
80	386	624	214	173	642
100	425	625	256	198	684

Table 8 displays the packet rate analysis of several approaches, including the proposed FEBWS-SERPPA algorithm, the ACI-GSO methodology, the MWCSGA technique, the RNN-LSTM method, and the PSO technique. About 99%. The PSO algorithm's packet forwarding rate is roughly 62% lower than that of other cutting-edge techniques. Compared to other approaches, this high packet forwarding rate shows improved performance.

Table 8
Comparative evaluation of packet delivery ratio

No. of nodes	ACI-GSO	MWCSGA	RNN-LSTM	PSO	Proposed
20	15	22	08	05	34
40	25	38	16	15	53
60	54	56	34	36	68
80	63	68	52	54	76
100	82	93	65	62	99

The suggested FEBWS-SERPPA method's network lifetime is contrasted in Table 9 with that of a few of the more well-known algorithms, such as the ACI-GSO algorithm, MWCSGA algorithm, RNN-LSTM model, and PSO algorithm. By extending the network lifetime to 1395 seconds, the proposed FEBWS-SERPPA approach improves WSN energy efficiency. The network lifetime was shown to be 1147 seconds for the ACI-GSO method, 1173 seconds for the MWCSGA methodology, 902 seconds for the RNN-LSTM model, and 810 seconds for the PSO technique.

Table 9
Comparative evaluation of network lifetime

No. of nodes	ACI-GSO	MWCSGA	RNN-LSTM	PSO	Proposed
20	1147	1173	902	810	1395
40	956	1112	876	786	1200
60	913	987	856	764	1186
80	887	945	779	778	1078
100	796	825	795	745	996

The energy consumption of various techniques, including the ACI-GSO algorithm, the MWCSGA algorithm, the RNN-LSTM model, the PSO algorithm, and the suggested FEBWS-SERPPA algorithm, is shown in Table 10. The suggested FEBWS-SERPPA algorithm performs better than its rivals while using 52% less energy. The energy was used by the ACI-GSO algorithm, MWCSGA, RNN-LSTM model, and PSO technique in those orders: 84, 83, 93, and 99%.

Table 10
Comparative analysis of energy consumption

No. of nodes	ACI-GSO	MWCSGA	RNN-LSTM	PSO	Proposed
20	22	19	26	38	14
40	34	24	45	52	8
60	56	38	59	74	23
80	72	64	76	85	41
100	84	83	93	99	52

7. Conclusion

A FEBWS-SERPPA algorithm is suggested in this research to increase the energy effectiveness of WSNs. A cluster-based, energy-efficient communication method is the Secure Cryptographic Random Permutation Pseudo-Algorithm (SERPA). The performance of the suggested strategy is predicted using the NS-2 simulator. Throughput, packet transfer rate, network robustness, energy efficiency, packet loss, and energy consumption are a few examples of performance indicators. The proposed FEBWS-SERPPA method was compared with the ACI-GSO methodology, RNN-LSTM model, MWCSGA algorithm, and PSO algorithm. Following are the specifications of the proposed FEBWS-SERPPA algorithm: 1395s network lifetime, 99% packet forwarding rate, 684kbps throughput, 110 packet drops, and 93% energy efficiency. It's worth noting that the utilization of the CRAWDAD dataset in our simulations has added a layer of realism and relevance to our findings. The suggested FEBWS-SERPPA algorithm outperforms other conventional techniques, according to experimental results. We intend to examine using a wider range of techniques in subsequent studies.

Acknowledgment

The authors want to convey their gratitude to all those who supported them in this undertaking. The researchers did not obtain any particular funding for their venture. The authors state that they hold no monetary or other "conflicting concerns" related to the present investigation that they are obligated to reveal.

References

[1] Burhan, Muhammad, Rana Asif Rehman, Bilal Khan, and Byung-Seo Kim. "IoT elements, layered architectures and security issues: A comprehensive survey." *sensors* 18, no. 9 (2018): 2796. https://doi.org/10.3390/s18092796

[2] Mohamed, Khaled Salah, and Khaled Salah Mohamed. *The era of internet of things: Towards a smart world*. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-18133-8

[3] Rayes, Ammar, and Samer Salam. "Internet of things from hype to reality." *Springer* (2017). https://doi.org/10.1007/978-3-319-99516-8

[4] Atlam, Hany Fathy, Robert Walters, and Gary Wills. "Internet of things: state-of-the-art, challenges, applications, and open issues." *International Journal of Intelligent Computing Research (IJICR)* 9, no. 3 (2018): 928-938. https://doi.org/10.20533/ijicr.2042.4655.2018.0112

[5] Costa, Daniel G., Solenir Figuerêdo, and Gledson Oliveira. "Cryptography in wireless multimedia sensor networks: A survey and research directions." *Cryptography* 1, no. 1 (2017): 4. https://doi.org/10.3390/cryptography1010004.

[6] Kambourakis, Georgios, Felix Gomez Marmol, and Guojun Wang. "Security and Privacy in Wireless and Mobile Networks." *Future internet* 10, no. 2 (2018): 18. https://doi.org/10.3390/books978-3-03842-780-3

[7] Ziegler, Sébastien, ed. *Internet of Things Security and Data Protection*. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-04984-3

[8] Cheruvu, Sunil, Anil Kumar, Ned Smith, David M. Wheeler, Sunil Cheruvu, Anil Kumar, Ned Smith, and David M. Wheeler. "IoT Software Security Building Blocks." *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment* (2020): 213-346. https://doi.org/10.1007/978-1-4842-2896-8_4

[9] Mahmood, Zaigham, ed. *Security, privacy and trust in the IoT environment*. Springer, 2019. https://doi.org/10.1007/978-3-030-18075-1

[10] Banday, Mohammad Tariq, ed. *Cryptographic Security Solutions for the Internet of Things*. IGI Global, 2019. https://doi.org/10.4018/978-1-5225-5742-5

[11] Biryukov, Alex, and Leo Perrin. "State of the art in lightweight symmetric cryptography." *Cryptology ePrint Archive* (2017).

[12] Frustaci, Mario, Pasquale Pace, Gianluca Aloi, and Giancarlo Fortino. "Evaluating critical security issues of the IoT world: Present and future challenges." *IEEE Internet of things journal* 5, no. 4 (2017): 2483-2495. https://doi.org/10.1109/jiot.2017.2767291

[13] Bilal, Muhammad, and Shin-Gak Kang. "An authentication protocol for future sensor networks." *Sensors* 17, no. 5 (2017): 979. https://doi.org/10.3390/s17050979

[14] Saraiva, Daniel AF, Valderi Reis Quietinho Leithardt, Diandre de Paula, Andre Sales Mendes, Gabriel Villarrubia González, and Paul Crocker. "Prisec: Comparison of symmetric key algorithms for iot devices." *Sensors* 19, no. 19 (2019): 4312. https://doi.org/10.3390/s19194312

[15] Ashokkumar, N., P. Nagarajan, and P. Venkatramana. "3D (dimensional)—Wired and wireless network-on-chip (NoC)." In *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2019*, pp. 113-119. Springer Singapore, 2020. https://doi.org/10.1007/978-981-15-0146-3_12

[16] Ashokkumar, N., and A. Kavitha. "A novel 3D NoC scheme for high throughput unicast and multicast routing protocols." *Technical Gazette* 23, no. 1 (2016): 215-219. https://doi.org/10.17559/tv-20141230061413

[17] Ashokkumar, N., and A. Kavitha. "Network on Chip: A Framework for Routing in System on Chip." *Journal of Computational and Theoretical Nanoscience* 12, no. 12 (2015): 6077-6083. https://doi.org/10.1166/jctn.2015.4544

[18] Kumar, N. Ashok, A. Kavitha, P. Venkatramana, and Durgesh Nandan. "Architecture Design: Network-on-Chip." In *VLSI Architecture for Signal, Speech, and Image Processing*, pp. 147-165. Apple Academic Press, 2022. https://doi.org/10.1201/9781003277538-8

[19] G Gopalan, S. Harihara. "ZHRP-DCSEI, a novel hybrid routing protocol for mobile ad-hoc networks to optimize energy using dynamic cuckoo search algorithm." *Wireless Personal Communications* 118, no. 4 (2021): 3289-3301. https://doi.org/10.1007/s11277-021-08180-1

[20] Gopalan, S., and R. Radhakrishnan. "Improved Cuckoo Search Optimisation Based Energy-Delay Aware Routing Algorithm in Manet for Rescue and Emergency Applications." *International Journal of Computer Technology and Applications* 9 (2016): 20.

[21] Gopalan, S. Harihara, and R. Radha Krishnan. "Trust based fuzzy aided ACO for optimal routing with security in MANET." *Asian Journal of Research in Social Sciences and Humanities* 6, no. cs1 (2016): 529-544. https://doi.org/10.5958/2249-7315.2016.00981.3

[22] Gopalan, S. Harihara, and R. Radhakrishnan. "Probability Based Optimized Energy Efficient Routing Algorithm for Mobile AD-HOC Network." *Middle-East Journal of Scientific Research* 22, no. 4 (2014): 591-595.

[23] Kavitha, T., N. Pandeeswari, R. Shobana, V. R. Vinothini, K. Sakthisudhan, A. Jeyam, and A. Jasmine Gnana Malar. "Data congestion control framework in Wireless Sensor Network in IoT enabled intelligent transportation system." *Measurement: Sensors* 24 (2022): 100563. https://doi.org/10.1016/j.measen.2022.100563

[24] Natarajan, Vignesh Prasanna, and Kavitha Thandapani. "Reliable Efficient Cluster Routing Protocol Based HTDE Scheme for UWSN." *Indonesian Journal of Electrical Engineering and Computer Science* 28, no. 1 (2022): 498. https://doi.org/10.11591/ijeecs.v28.i1.pp498-507.

[25] Natarajan, Vignesh Prasanna, and Kavitha Thandapani. "Adaptive Time Difference of Time of Arrival in Wireless Sensor Network Routing for Enhancing Quality of Service." *Instrumentation, Mesures, Métrologies* 20, no. 6 (2021). https://doi.org/10.18280/i2m.200602.

[26] Natarajan, Vignesh Prasanna, and Kavitha Thandapani. "An improvement of communication stability on underwater sensor network using balanced energy efficient joining distance matrix." *International Journal of System Assurance Engineering and Management* 13, no. Suppl 1 (2022): 690-698. https://doi.org/10.1007/s13198-021-01593-y

[27] Ahankari, Sachin, M. Rajmohan, A. PruthaRani, Dichipalli Yeshasree, and T. Kavitha. "Wireless Underwater Communication: A Networking Approach for Estimating First Order Lag in Routing Data." In *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, pp. 743-749. IEEE, 2022. https://doi.org/10.1109/ICEARS53579.2022.9751824

[28] Karpagalakshmi, R. C., P. Vijayalakshmi, K. Gowsic, and R. Rathi. "An effective traffic management system using connected dominating set forwarding (CDSF) framework for reducing traffic congestion in high density vanets." *Wireless Personal Communications* 119, no. 3 (2021): 2725-2754. https://doi.org/10.1007/s11277-021-08361-y

[29] Karpagalakshmi, R. C., and D. Tensing. "Vehicle object observation using position based local gradient model." In *2012 International Conference on Radar, Communication and Computing (ICRCC)*, pp. 293-298. IEEE, 2012. https://doi.org/10.1109/ICRCC.2012.6450598

[30] Boopalan. "Heterogeneous Distort-Prevention Manifold Resource Distribution Mechanism for Cloud Management." *Journal of Advanced Research in Dynamical and Control Systems* 12, no. 3 (2020): 287–94. https://doi.org/10.5373/jardcs/v12i3/20201193

[31] Suvitha, S., R. C. Karpagalakshmi, R. Umamaheswari, K. Chandramohan, and M. S. Sabari. "An Estimation and Evaluation of Network Availability in Link State Routing Networks." *Journal of Network Security Computer Networks (e-ISSN: 2581-639X)* 7, no. 3 (2021): 19-26. https://doi.org/10.46610/jonscn.2021.v07i03.003

[32] Suganyadevi, K., V. Nandhalal, Satheeshkumar Palanisamy, and S. Dhanasekaran. "Data security and safety services using modified timed efficient stream loss-tolerant authentication in diverse models of VANET." In *2022 International Conference on Edge Computing and Applications (ICECAA)*, pp. 417-422. IEEE, 2022. https://doi.org/10.1109/ICECAA55415.2022.9936128

[33] Manikandan, A., and S. Pradeep. "Quantitative analysis of network arrangement in randomized appropriation in WSN." *Journal of Chemical and Pharmaceutical Sciences* 1 (2017): 181-184.

[34] Xia, Feng, Li Liu, Jie Li, Ahmedin Mohammed Ahmed, Laurence Tianruo Yang, and Jianhua Ma. "BEEINFO: Interest-based forwarding using artificial bee colony for socially aware networking." *IEEE Transactions on Vehicular Technology* 64, no. 3 (2014): 1188-1200. https://doi.org/10.1109/tvt.2014.2305192

[35] Venkataramanan, C., S. Ramalingam, and A. Manikandan. "LWBA: Lévy-walk bat algorithm based data prediction for precision agriculture in wireless sensor networks." *Journal of Intelligent & Fuzzy Systems* 41, no. 2 (2021): 2891-2904. https://doi.org/10.3233/jifs-202953

[36] Yousefpoor, Mohammad Sadegh, and Hamid Barati. "DSKMS: A dynamic smart key management system based on fuzzy logic in wireless sensor networks." *Wireless Networks* 26, no. 4 (2020): 2515-2535. https://doi.org/10.1007/s11276-019-01980-1

[37] Sampathkumar, A., Miretab Tesfayohani, Shishir Kumar Shandilya, S. B. Goyal, Sajjad Shaukat Jamal, Piyush Kumar Shukla, Pradeep Bedi, and Meshal Albeedan. "Internet of Medical Things (IoMT) and reflective belief design-based big data analytics with Convolution Neural Network-Metaheuristic Optimization Procedure (CNN-MOP)." *Computational Intelligence and Neuroscience* 2022 (2022). https://doi.org/10.1155/2022/2898061.

[38] Ramanan, M., Laxman Singh, A. Suresh Kumar, A. Suresh, A. Sampathkumar, Vishal Jain, and Nebojsa Bacanin. "Secure blockchain enabled Cyber-Physical health systems using ensemble convolution neural network classification." *Computers and Electrical Engineering* 101 (2022): 108058. https://doi.org/10.1016/j.compeleceng.2022.108058

[39] Arumugam, Sampathkumar, Shishir Kumar Shandilya, and Nebojsa Bacanin. "Federated learning-based privacy preservation with blockchain assistance in IoT 5G heterogeneous networks." *Journal of Web Engineering* (2022): 1323-1346. https://doi.org/10.13052/jwe1540-9589.21414

[40] Sarbini, Izzatul Nabila, Tze Jin Wong, Lee Feng Koo, Ahmad Fadly Nurullah Rasedee, Fatin Hana Naning, and Mohammad Hasan Abdul Sathar. "Security Analysis on LUC-type Cryptosystems Using Common Modulus Attack." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 29, no. 3 (2023): 206-213. https://doi.org/10.37934/araset.29.3.206213

[41] Ali, Firkhan Ali Hamid, Mohd Khairul Amin Mohd Sukri, Mohd Zalisham Jali, Muhammad Al-Fatih, and Mohd Azhari Mohd Yusof. "Web-Based Reporting Vulnerabilities System for Cyber Security Maintenance." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 29, no. 3 (2023): 198-205. https://doi.org/10.37934/araset.29.3.198205

[42] Claro Noda, Shashi Prabh, Mário Alves, Thiemo Voigt and Carlo Alberto Boano, CRAWDAD dataset cister/rssi (v. 20120517), downloaded from https://crawdad.org/cister/rssi/20120517, https://doi.org/10.15783/C7WC75, May 2012.