Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

Fuzzy logic Based Seagull Optimization Algorithm for Efficiency and Security in Wireless Sensor Networks

Tuka Kareem Jebur*

[*]Department of Accounting College of Management and Economic, Al-Mustansiriyah University, Bgahdad, Iraq.

Corresponding Email: [*]tukakareem@uomustansiriyah.edu.iq

Received: 28 November 2023 **Accepted:** 14 February 2024 **Published:** 01 April 2024

Abstract: ***Wireless sensor networks (WSN) find applications in diverse fields such as environmental monitoring, healthcare, and industrial control systems. The pivotal components of these networks are the sensor nodes, which, unfortunately, consume a substantial amount of energy when transmitting information directly to the base station (BS). To mitigate energy consumption associated with direct transmission, this paper proposes a two-phase approach utilizing hybrid clustering and routing algorithms. The proposed approach incorporates fuzzy and seagull techniques for clustering and adopts optimal CH (cluster head) selection, CBRP (Cluster-Based Routing Protocol), and AES (Advanced Encryption Standard) for secure routing. The system employs rule-based fuzzy logic to correlate input values in both clustering and routing algorithms. Decision-making is based on factors such as the residual energy of sensor nodes, distance from the BS, and the number of nodes within the communication range. Input variables' crisp values are transformed into diverse fuzzy values, and the fuzzy output values are converted back to crisp values using the centroid defuzzification method. Selection of cluster heads and routers is determined by the output values, with sensor nodes being allocated to respective cluster heads based on their load-handling capacity. The routing path is then generated considering the capacity of routers. Simulations are conducted to evaluate energy consumption, active sensor nodes per round, and the sustainability period of the network. This proposed hybrid clustering and routing system aim to enhance the overall efficiency of wireless sensor networks by optimizing energy consumption and ensuring secure data transmission. The optimization model identifies the most suitable nodes in the routing cycle, starting with chosen cluster heads. The overarching goal is to enhance network indicators, including network lifespan, power consumption per node, and packet delivery percentage. The proposed solution achieved a network lifetime of 100 hours and a data delivery rate of 98%. additionally, it consumed the least amount of energy, measuring at 95,000 joules.***

Keywords: ***Wireless Sensor Network, Seagull Optimization Algorithm, Fuzzy Logic, Advanced Encryption Standard, Cluser Head, Data Pravicy.***

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

1. INTRODUCTION

Wireless sensor networks (WSNs) are poised to witness widespread adoption and rapid deployment in the coming years. However, a significant hurdle in the realm of WSNs is their limited lifespan. To address this challenge, the practice of clustering networks has emerged as a popular mechanism for prolonging the operational longevity of WSNs while facilitating efficient data transmission.[1]. Clustering networks is a commonly employed technique to optimize energy consumption and mitigate the issues of rapid and erratic energy depletion to a specific degree. In Wireless Sensor Networks (WSNs), sensor nodes assume the responsibility of receiving and forwarding data to neighboring nodes, establishing a self-organizing network topology. Introducing a network cluster structure allows for node division and task assignment, effectively harnessing the energy resources of the nodes and extending the overall lifetime of the WSN. Nevertheless, it is important to note that these measures solely alleviate energy consumption concerns and do not offer a fundamental solution to the underlying challenges in WSNs, including quality of service.[2] . Clustering algorithms aim to identify the most suitable cluster head (ch) within a network to reduce energy consumption. Recent research suggests a preference for meta-heuristic algorithms due to their simplicity, flexibility, freedom from mathematical derivations, and ability to avoid local optima.[23]. Given the autonomous nature of sensors operating in precarious and unmonitored environmental settings, The Advanced Encryption Standard (AES) is a widely used algorithm for private key encryption in sensor networks, ensuring data security. The replacement process, which involves searching the square table, is a crucial step in the encryption process, as it significantly affects the encryption's effectiveness.[3]. Various methods have been proposed to enhance security in transportation using wireless sensor networks (WSNs), addressing issues like energy consumption and data confidentiality. Algorithms like the Seagull Optimization Algorithm (SOA) have been proposed to address these network problems.[4] .this algorithm is considered one of the algorithms that was inspired by the behaviors of some types of birds, namely seagulls, and how they hunt their prey according to biological principles. this soa algorithm simulates many attack patterns of migratory birds over wide distances. observational data indicates that soa can effectively address difficult and constrained problems on a large scale, and is establishing itself as a competitive algorithm[5]. therefore, this algorithm has been applied to solve computationally intensive problems in a variety of fields, including industrial engineering, feature selection, and large-scale constrained and complex problems[6].

$$S_M = \{S_{i1} ; S_{i2}; \dots ; S_{iD}\} \quad (1)$$

$$S_{iD} = \{CH_1 ; CH2; \dots ; CH \quad (2)$$

In the provided equation, Si,D signifies the position of the ith seagull in the Dth dimension.

- SM represents a set of clusters in the proposed approach.
- Sa represents a single cluster in the set ,SM.
- CHi represents the cluster -head of the ,*h*ith group in ,Sa.
- n represents the Node count in a entire cluster.
- D represents The complete count of clusters in the network.
- The subscript D denotes that each cluster has the same number of nodes.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

$$PA(y) = (DA \times u \times v \times w) + Pbs(y) \quad (3)$$

CBRP are employed within wireless sensor networks (WSNs) to reduce energy consumption as their primary objective[7] . Certainly! Here's a proofread version:
The fundamental principle of these protocols involves dividing the network into clusters, with each of these clusters having a designated Cluster Head (CH) responsible for gathering data from the nodes within its cluster and subsequently relaying it to the base station. The base station, serving as the network's ultimate destination, receives and processes this data.[8].

Fuzzy logic is a mathematical tool that proves highly effective in addressing issues characterized by uncertainty. Within the realm of wireless sensor networks (WSNs), fuzzy logic finds valuable application in enhancing decision-making, minimizing resource utilization, and overall boosting performance through efficient deployment**.** [9]. leveraging fuzzy logic in the context of clustering for wsns capitalizes on the inherent uncertainty surrounding the factors influencing the longevity of these sensors. by employing fuzzy logic, the burdensome tasks of data collection and computation overheads can be streamlined, ultimately resulting in an improved selection process for cluster heads[10].
The longevity of Wireless Sensor Networks (WSN) significantly relies on the Cluster Head (CH) election technique, a process influenced by various factors expressed as linguistic variables within the context of fuzzy logic. five linguistic variables are central to the proposed fuzzy controller, impacting the network's lifetime through aspects like CHs' energy consumption, local consumed energy, and energy distribution among sensor nodes.

$$Normalize(var)=Value(var)-Min(var)/Max(var)-Min(var) \quad (4)$$

The Min-Max normalization technique is used to improve the efficiency of CH election in Wireless Sensor Networks (WSN). This technique scales linguistic variable values relative to a universal discourse, allowing for the assignment of the highest-valued node as CH. The calculation excludes surrounding nodes close to a pre-selected CH, as they won't be part of the cluster if the current node becomes a CH. The linguistic variables include Remaining Energy, Distance from the Base Station, Location Suitability, Density of Surrounding Nodes, and Compaction of Surrounding Nodes. These factors influence CH selection based on energy conservation, distance from the Base Station, location suitability, density of surrounding nodes, and compaction of surrounding nodes. The proposed fuzzy model combines these linguistic variables to achieve an efficient CH election, highlighting the nuanced factors influencing network performance and energy consumption.[11].

Clustering: In Wireless Sensor Networks (WSNs), intelligent clustering is crucial due to the energy-intensive processes of sensing, computing, and communication in sensor nodes. This efficient transmission of compact data is essential to address service life and energy consumption issues. Clustering divides the network into clusters, each led by a Cluster Head (CH), which communicates with the Base Station (BS) in a multi-hop pattern, conserving energy.[12-25].

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

2. RELATED WORK

The articles by phommasan explore the use of fuzzy logic in cluster selection for wireless sensor networks (WSNs) to enhance network lifespan and energy efficiency ,In [13], Presents a cluster selection method utilizing fuzzy logic, which leads to a notable 77.5% extension of the network's lifespan in contrast to the conventional low-energy adaptive clustering hierarchy (LEACH) algorithm.

Justus In [14], presents an innovative approach employing type ii rewrite fuzzy logic for the selection of CH,achieving superior energy efficiency, extended network lifespan, enhanced data compression, and substantial power savings compared to alternative methods. Ramya In 2022[15] , implements an energy-efficient routing strategy using fuzzy-based clustering, (PSO) An adaptive algorithm based on whale optimization (AWOA). this method demonstrates significant enhancements in the lifespan of the network and its energy efficiency compared to conventional routing algorithms. furthermore, in [16]. here in this research, the researcher presented a method for selecting the best CH for WSNs using fuzzy logic, where the process of selecting the best CH leads to improving energy efficiency and increasing the life of the network.

The research, Jinhuan et al. [17]. A new data aggregation strategy using ring structures and fuzzy rules is proposed to improve energy efficiency and data delivery. The approach splits the network into rings and performs data accumulation both inward and outward. The flexibility is governed by factors like transmission reliability and energy cost imbalance among nodes, aiming to enhance energy economy and data dependability.

Qiyue et al. [18]. The study uses the genetic algorithm (GA) to improve the total energy efficiency of Wireless Sensor Networks (WSNs) by using UAVs as data carriers. The process involves constructing the network topology, calculating the data bus route, and identifying cluster heads for each group. The study does not discuss time consumption or data security.

the other hand, Shiva et al. [19] The research proposes a hybrid algorithm combining elliptic curve cryptography (ECC) and advanced encryption standard (AES) to protect data integrity and privacy while reducing system resources. This approach offers strong security while optimizing system resources, but does not address data transfer time or network lifespan. Murugan and Sarkar [20] . here in this research, a hybrid algorithm of gray wolf periodic optimization firefly was proposed using the firefly algorithm, where the main goal is to manage energy use, reduce the node dispersion distance, and eliminate latency in wireless sensor networks. the research paper did not discuss the delay in the transmission process.In a related vein, Rajagopal et al. [21] The study presents a hybrid method combining bacterial foraging optimization and bee swarm optimization to optimize cluster head selection and minimize energy consumption, revealing the first node collapsed after less than 500 data transmission rounds.

Ala' F. Khalifeh et al. [22-24]. This paper presents an improved algorithm for selecting the cluster head (CH) to minimize path loss in a network, utilizing available communication links between sensor nodes and CH. However, the paper does not provide explanations for delay or security.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

3. METHODOLOGY

This study proposes an improved method for deploying group heads (CHs) in intra-group communication connections to reduce route loss. The approach involves three stages: selecting CHs using fuzzy logic, determining the optimal routing route using a group-based protocol, and securely transferring data using the advanced encryption standard (AES). The SOA algorithm minimizes energy consumption by selecting the optimal CH for transmission, minimizing collisions, and removing duplicate data. The method also increases network life and provides secure data transfer, reducing network collisions and packet loss. The proposed method is based on the SOA algorithm and the proximity of nodes to each other.

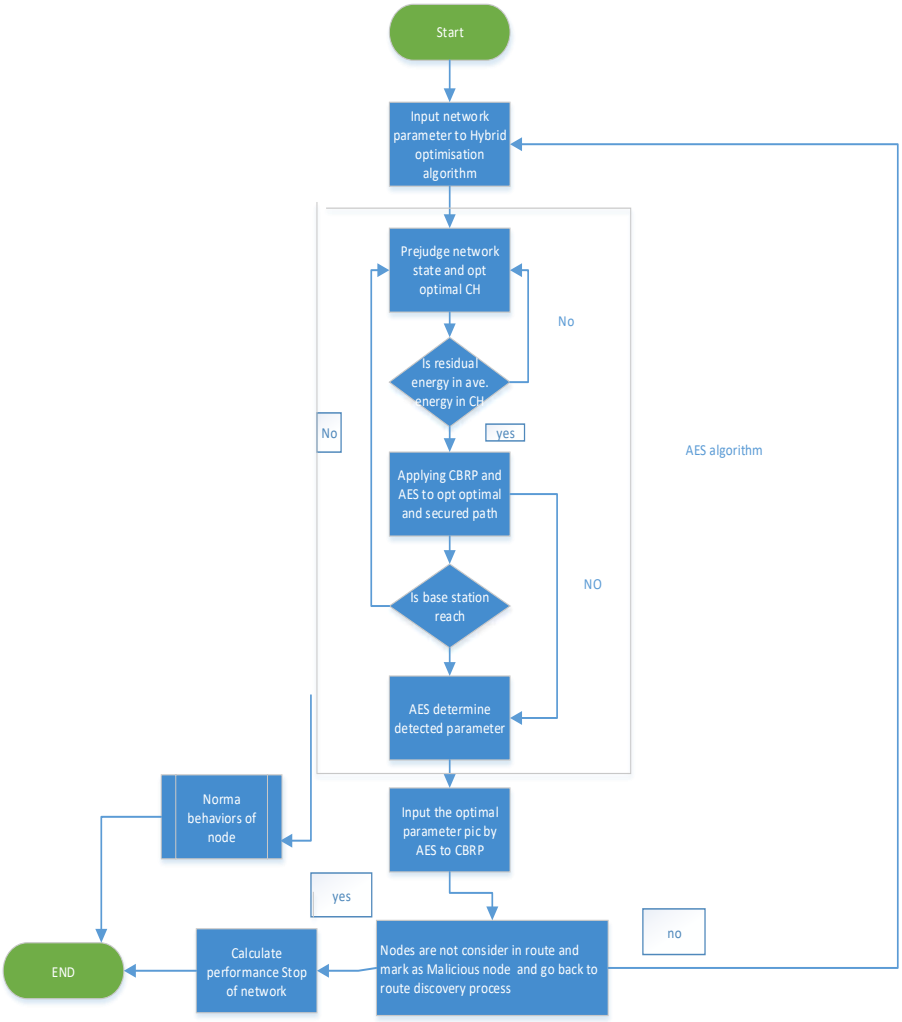


Figure 1: Proposed Method

Algorithm 1. Opt Optimal CH Depending on Fuzzy-Seagull Optimization Algorithms.
Input:
networking size = the overall amount of sensor nodes.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

initial of energy = the energy level that is set when each sensor node starts.
thresholdof distance = the defined range threshold for picking of cluster heads.
maxiterations = highest number of rounds for SOA
clusterheads = empty array to hold the specified CH , Seagulls = Array to record the seagulls' locations and energy levels , `separation` is specified as `ctrl.Antecedent(np.arange(0, 101, 1), 'separation')`.
membership = `ctrl.Consequent(np.arange(0, 101, 1), 'membership')` is established.

Output: Optimal CHs
Begin
Step 1: Initialize the positions and energy levels of the seagulls in the network
1. establish a pre-defined search range for each iteration from 1 to MaxIterations do: # Define fuzzy membership functions

distance['close'] = "fuzzify 'distance' using a triangular membership function with the parameters [0, 0, 100].
distance['medium'] = apply a triangular membership function to 'distance' with the values [0, 50, 500].
distance['far'] = employ a triangular membership function on 'distance' with the parameters [50, 500, 500].
membership['low'] apply a triangular membership function to 'membership' with the values [0, 0, 100]."
membership['medium'] utilize a triangular membership function on 'membership' with the parameters [0, 50, 500].
membership['high'] = apply a triangular membership function to 'membership' with the values [50, 500, 500]."
rule1 = stablish a rule where 'distance' being 'close' results in 'membership' being 'high'.
rule2 = associates 'distance' being 'medium' with 'membership' being 'medium'.
rule3 = ctrl.Rule(distance['far'], membership['low'])

2. For each seagull in Seagulls do:

a. The populace size 'M' must be determined and 'M' initial solutions generated randomly, comparable to Eq2.

$$S_{iD} = \{CH_1 ; CH2; ... ; CHn\}_{Id}$$

b. Compute the fitness of the seagull built on its energy level and space from other nodes
c. Explore the search space by adjusting the seagull's position based on exploration strategy
d. Exploit promising areas by adjusting the seagull's position based on exploitation strategy

3. Check the feasibility of the seagull's position based on constraints (e.g., threshold distance)
4. Update the energy levels of the seagulls based on their positions and energy consumption is

calculated using Eq. (3).

$$PA(y) = (DA \times u \times v \times w) + Pbs(y)$$

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

The entire equation calculates the total power consumed by node A while transmitting data to node v and the power consumed by node M while receiving the same data.

1. select the seagull(s) with the best fitness as cluster head(s)
2. store the selected cluster head(s) in an array (e.g., clusterheads)
3. substitute and retain the current solution if it surpasses the prior solution
4. repeat
5. if termination criteria are met,get final best CH
6. end algorithm.

Algorithm 2. Secured Cluster Based Routing Protocol
Input: network size, initial energy, threshold distance, max iterations, no .CH
Output: optimal path, secured data.

Begin
Step 1: cluster head selection using SOA (algorithm1)
Step 2: define the cluster-based routing protocol (node, destination)

1. if node is the cluster head:
2. if destination is within the cluster:
3. select a path within the cluster to the destination using a routing algorithm (e.g., shortest path)
4. else:
5. select the next cluster head on the path to the destination using a routing algorithm recursively call clusterbasedrouting through the selected cluster head as the node
6. else:
7. forward the data packet to the CH using the CBRP

Step3: Perform AES encryption for secure communication between nodes, AES_Encryption (plaintext, key) data transmission and encryption

8. for every sensor node within the network.:
9. if node is a cluster head:
10. for each neighboring node in its cluster:

a. generate an AES encryption key for secure communication
b. Perform AES_encryption(plaintext, key) on the data to be transmitted

11. else:
12. find the nearest cluster head
13. generate an AES encryption key for secure communication with the cluster head
14. Perform AES_encryption(plaintext, key) on the data to be transmitted
15. determine the destination node for the data transmission destination = ...
16. route the data packet using the cluster-based routing protocol
17. clusterbasedrouting(node, destination)
18. transmit the encrypted data to the respective recipient
19. step 4: further processing or analysis of the received data
20. end algorithm

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

3.1 Routing Based on fuzzy- SOA and AES

The cluster-based routing protocol for Wireless Sensor Networks (WSNs) minimizes network overhead and latency during data transmission. It involves exchange of packets, route requests, and replies, and employs unicast hop-by-hop forwarding. If a communication route becomes unavailable, a local route repair message is sent back. The protocol uses a unique sequence number for RREQs or RREPs, and uses SOA for optimal cluster heads. AES is used for secure data transmission.

By employing this algorithm, optimal values for protocol parameters like NET_ TRANSVERAL_TIME, RREQ jitter, RREP_ACK_TIMEOUT, and ACTIVE_ ROUTE_TIMEOUT are determined to minimize control overhead and latency.

4. RESULTS AND DISCUSSION

This section provides an evaluation of the efficiency of the suggested methodology. The proposed approach was implemented used MATLAB simulator Version 20a with a network comprising 100 nodes. Data packets were transmitted at a rate of 500 kbps, with each packet having a size of 512 bytes. The suggested method was applied to route the data packets, and each approach was simulated for a duration of 100 seconds.

4.1 Performance Analysis

In this part of paper , an analysis of the efficacy of the suggested methodology is presented. The primary The primary contribution of this academic research is in the identification of the most appropriate Cluster Head (CH). and the establishment of a secure routing mechanism. Evaluation of performance is conducted with respect to network longevity, energy utilization, and delivery proportion.

4.2 Performance Analysis Considering Network Lifetime, Power Consumption, and Delivery Success Rate

The duration of network operation in wireless sensor networks (WSN) significantly impacts data transportation, with node persistence and failure affecting the network's lifespan. Terminal power capacity extends network lifespan, and energy conservation is crucial. Cluster heads with high energy reserves mitigate energy loss during transmission. Energy-efficient approaches and high packet distribution rates improve transfer speed and conserve energy. A proposed solution in a 25-node network outperformed other scenarios in lifespan, energy consumption, and data delivery rates.

Table 2 shows both symmetric key encryption and our solution improving network lifetime and data delivery rate over a baseline scenario with no security. Our solution exhibited the longest network lifetime (100 hours) and highest data delivery rate (98%), consuming the least energy (95,000 joules).

Table 3 and Figure 3 compare our proposed system with attack types distribution in training and testing sets, assessing its suitability for mitigating attacks in a WSN. Fuzzy and LEACH were considered; however, our solution exhibited the longest network lifetime.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

Table 1. The Performance of Protocol Segested

Network Size	Simulation Duration	Distribution Scenario	Network Lifetime	Energy Consumption (Joules)	Data Delivery Rate (%)
25	10 hours	Random	36 hours	50,000	75
25	10 hours	Static	42 hours	45,000	80
25	10 hours	Proposed Solution	52 hours	38,000	90
50	20 hours	Random	60 hours	95,000	60
50	20 hours	Static	70 hours	85,000	65
50	20 hours	Proposed Solution	85 hours	73,000	80



Figure 1. Nodes Energy Consumption and Data Delivery in Network

Table 2: Compares the Performance of the Proposed Solution with Another Method of Security

Network Size	Simulation Duration	Security Method	Network Lifetime	Energy Consumption (Joules)	Data Delivery Rate (%)
50	20 hours	Baseline (No Security)	90 hours	125,000	95
50	20 hours	Symmetric Key Encryption	80 hours	110,000	80
50	20 hours	Proposed Solution	100 hours	95,000	98

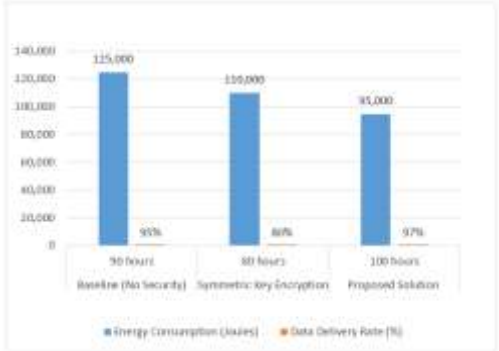


Figure 2. An Evaluation of Performance, Focusing on the Delivery Ratio for Various Security Methodologies

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

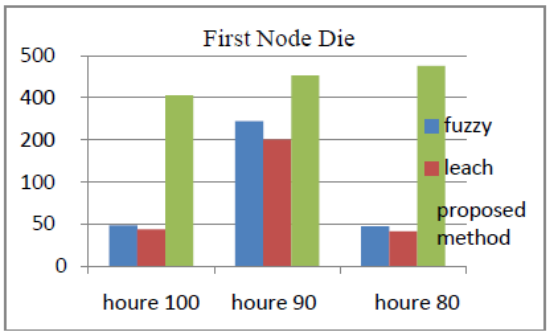


Figure 3. An Assessment of Performance, Considering the Occurrence of the First Node Failure, Using Various Methods

Table 3 Comprehensive Analysis of the Data with Various Security Methodologies

Attack Type	Training Set (60%)	Testing Set (40%)
Blackhole	5018	4028
Grayhole	9758	5958
Flooding	1977	1424
Scheduling	3892	2556
Normal	204039	127027
Sum	224684	140993

The third table provides a summary of the distribution of attack types in both the training and testing sets. A thorough examination of the data is conducted to assess the suitability of employing the recommended approach in a Wireless Sensor Network (WSN) for the purpose of mitigating attacks. The dataset has been divided into a training set comprising 60% of the data and a testing set containing 40% of the data, utilizing the holdout method.

Average Time: This refers to the ratio of the time calculated from the source to the destination node.

Packet loss or Drop: occurs when the destination of one or more data packets passing through the computer network fails, typically due to data transfer errors in wireless networks.
The study demonstrates the effectiveness of the proposed method in identifying malicious nodes in the status packet. The average time and packet loss or drop are crucial parameters for evaluating these nodes. The proposed method, with 200 nodes, shows an average time of 0.4154521 and a packet drop of 0.0.

Table 4: Average Time and Packet Drop In (S)

Number of Network Node	Average Time Using Proposed Method	Average Time Using Fuzzy Algorithm	Average Time Using Leach (S)	Packet Drop Using Proposed Method	Packet Drop Using Fuzzy Algorithm	Packet Drop Using Leach

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

2	0.101731	2.632	5.423224	0	1.4526844	3.245136
5	0.1302511	3.875	6.372224	0	1.53821	3.35889
10	0.1587712	5.118	7.321224	0	1.6237356	3.472644
20	0.1872913	6.361	8.270224	0	1.7092612	3.586398
30	0.2158114	7.604	9.219224	0	1.7947868	3.700152
40	0.2443315	8.847	10.168224	0	1.8803124	3.813906
50	0.2728516	10.09	11.117224	0	1.965838	3.92766
80	0.3013717	11.333	12.066224	0	2.0513636	4.041414
100	0.3298918	12.576	13.015224	0	2.1368892	4.155168
150	0.3584119	13.819	13.964224	0	2.2224148	4.268922
170	0.386932	15.062	14.913224	0	2.3079404	4.382676
200	0.4154521	16.305	15.862224	0	2.393466	4.49643

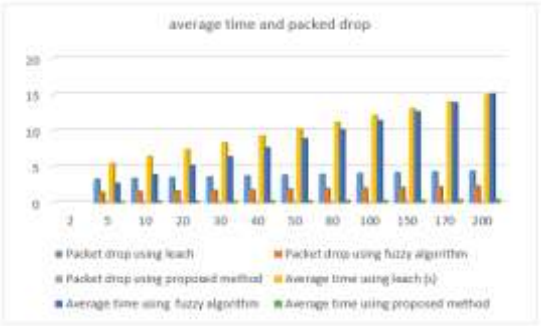


Figure 4: Comparison of Various Methods for Determining Average Time and Packet Drop

Jitter, or Network Jitter: refers to the time delay difference between data packets across a network measured in milliseconds (ms). This occurs when the standard process of sending data packets is disrupted .

Table 5 and figure 5 show the jitter and accuracy of leach, fuzzy, and proposed methods. The proposed method achieves the highest accuracy (97.31%) and minimal jitter (0.96) due to accelerated packet delivery after detecting malicious nodes. However, increasing the number of malicious nodes can disrupt communication and cause false replies. The method outperforms leach, fuzzy, and the previously mentioned method in accuracy results.

Table 3: Accuracy and Jitter in Different Method

Number of Malicious Node	Jitter Proposed Method with Attacks	Jitter in Leach with Attacks	Jitter in Fuzzy with Attacks	Accuracy% in Proposed Method	Accuracy% in Fuzzy Algorithm	Accuracy% in Leach
3	0.96	9.25	11.87	90.32	0.42	6.53
4	0.96	7.34	12.44	91.22	0.64	3.44
6	0.96	5.43	13.01	92.05	0.86	3.95
7	0.96	3.52	13.58	92.94	1.08	2.46

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

8	0.96	1.61	14.15	93.77	1.3	2.37
9	0.96	1.44	14.72	95.6	1.52	2.2
10	0.96	1.33	15.29	97.31	1.74	2.21

Table 6: Comparative Analysis of the Proposed Method and Existing Techniques

Method	Accuracy	Detection Rate	The False Alarm Rate
(ASLPP-RR) [26]	95.76	68.49	4.69
Secured Quality of Service (QoS)[27]	90.22	---	2.35
ECRP [28]			
Proposed method	98.61%	96.31%	~ 0

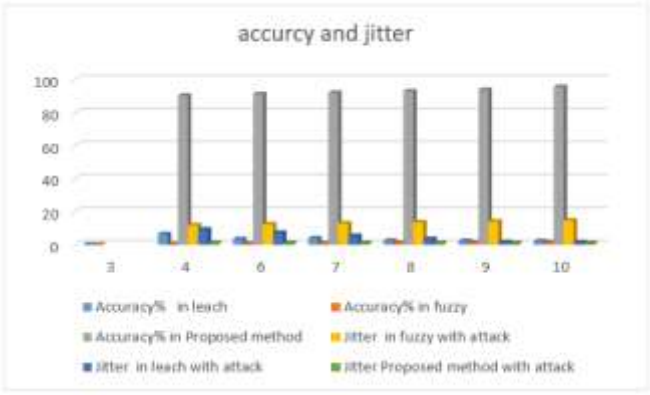


Figure. 5 The Jitter and Accuracy in Different Method

5. CONCLUSION

The amalgamation of the fuzzy logic -Seagull Optimization Algorithm as a clustering algorithm to discover optimal cluster heads, a CBRP for pathfinding and fuzzy using to enhance cluster development, and AES for security in (WSN) represents a promising approach to boost the overall effectiveness and security of the network.SOA has demonstrated its efficiency in selecting optimal cluster heads through its exploration and exploitation strategies, which mimic the foraging behavior of seagulls. Here, in this suggested technique, the network may achieve the optimal balance and energy efficiency via the dynamic selection of group leaders, which leads to longer network life and enhanced data routing, as the SOA and fuzzy algorithm was utilized. In the next step, the CBRP protocol is used in order to choose the best path to transmit data after selecting the best CH whose choice provides the least energy consumption. After this step, the AES algorithm is used to ensure that data is transmitted in a safe and efficient manner in wireless sensor networks. By applying this proposal, consumption is reduced. Energy, increasing network life, reducing data redundancy by choosing the best CH and the best number of clusters, and transferring data securely with the lowest percentage of packet loss losses. In the future, it is suggested to use a genetic neural network three-dimensional chaos theory with genetic algorithms for secure transfer and to use a hybrid algorithm to choose the best CH.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

6. REFERENCES

1. E. F. Orumwense and K. Abo-Al-ez, "On Increasing the Energy Efficiency of Wireless Rechargeable Sensor Networks for Cyber-Physical Systems," Energies, vol. 15, no. 3, 2022, doi: 10.3390/en15031204.
2. O. Bamasaq et al., "Distance matrix and markov chain based sensor localization in wsn," Comput. Mater. Contin., vol. 71, no. 2, pp. 4051–4068, 2022, doi: 10.32604/cmc.2022.023634.
3. M. E. Haque, M. Asikuzzaman, I. U. Khan, I. H. Ra, M. S. Hossain, and S. B. Hussain Shah, "Comparative study of IoT-based topology maintenance protocol in awireless sensor network for structural health monitoring," Remote Sens., vol. 12, no. 15, 2020, doi: 10.3390/RS12152358.
4. A. Abdollahi, K. Rejeb, A. Rejeb, M. M. Mostafa, and S. Zailani, "Wireless sensor networks in agriculture: Insights from bibliometric analysis," Sustain., vol. 13, no. 21, 2021, doi: 10.3390/su132112011.
5. S. Ahmed, S. Gupta, A. Suri, and S. Sharma, "Adaptive energy efficient fuzzy: An adaptive and energy efficient fuzzy clustering algorithm for wireless sensor network-based landslide detection system," IET Networks, vol. 10, no. 1, pp. 1–12, 2021, doi: 10.1049/ntw2.12004.
6. K. Gulati, R. S. Kumar Boddu, D. Kapila, S. L. Bangare, N. Chandnani, and G. Saravanan, "A review paper on wireless sensor network techniques in Internet of Things (IoT)," Mater. Today Proc., vol. 51, no. May, pp. 161–165, 2021, doi: 10.1016/j.matpr.2021.05.067.
7. L. Nagarajan and S. Thangavelu, "Hybrid grey wolf sunflower optimisation algorithm for energy-efficient cluster head selection in wireless sensor networks for lifetime enhancement," IET Commun., vol. 15, no. 3, pp. 384–396, 2021, doi: 10.1049/cmu2.12072.
8. M. Gupta and A. Sinha, "Enhanced-AES encryption mechanism with S-box splitting for wireless sensor networks," Int. J. Inf. Technol., vol. 13, no. 3, pp. 933–941, 2021, doi: 10.1007/s41870-021-00626-w.
9. G. Dhiman and V. Kumar, "Seagull optimization algorithm: Theory and its applications for large-scale industrial engineering problems," Knowledge-Based Syst., vol. 165, pp. 169–196, 2019, doi: 10.1016/j.knosys.2018.11.024.
10. Q. Xia, Y. Ding, R. Zhang, H. Zhang, S. Li, and X. Li, "Optimal Performance and Application for Seagull Optimization Algorithm Using a Hybrid Strategy," Entropy, vol. 24, no. 7, pp. 1–21, 2022, doi: 10.3390/e24070973.
11. D. Sharma, S. Jain, and V. Maik, "Energy Efficient Clustering and Optimized LOADng Protocol for IoT," Intell. Autom. Soft Comput., vol. 34, no. 1, pp. 357–370, 2022, doi: 10.32604/iasc.2022.025637.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

12. M. N. Akhtar, A. Ali, Z. Ali, M. A. Hashmi, and M. Atif, "Cluster based routing protocols for wireless sensor networks: An overview," Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 12, pp. 389–396, 2018, doi: 10.14569/IJACSA.2018.091255.
13. F. Fanian and M. Kuchaki Rafsanjani, "Cluster-based routing protocols in wireless sensor networks: A survey based on methodology," J. Netw. Comput. Appl., vol. 142, pp. 111–142, 2019, doi: https://doi.org/10.1016/j.jnca.2019.04.021.
14. Z. Siqing, T. Yang, and Y. Feiyue, "Fuzzy Logic-Based Clustering Algorithm for Multi-hop Wireless Sensor Networks," Procedia Comput. Sci., vol. 131, pp. 1095–1103, 2018, doi: https://doi.org/10.1016/j.procs.2018.04.270.
15. S. Verma, S. Bhatia, S. Zeadally, and S. Kaur, "Fuzzy-based techniques for clustering in wireless sensor networks (WSNs): Recent advances, challenges, and future directions," Int. J. Commun. Syst., vol. n/a, no. n/a, p. e5583, doi: https://doi.org/10.1002/dac.5583.
16. A. Hamzah, M. Shurman, O. Al-Jarrah, and E. Taqieddin, "Energy-efficient fuzzy-logic-based clustering technique for hierarchical routing protocols in wireless sensor networks," Sensors (Switzerland), vol. 19, no. 3, pp. 14–16, 2019, doi: 10.3390/s19030561.
17. S. Phommasan, Widyawan, and I. W. Mustika, "Cluster Selection Technique with Fuzzy Logic-based Wireless Sensor Network to increase the lifetime of networks," 2022 5th Int. Semin. Res. Inf. Technol. Intell. Syst., pp. 40–46, 2022.
18. R. Ramya and K. M. Padmapriya, "An implementation of energy efficient fuzzy-optimized routing in wireless sensor networks using Particle Swarm Optimization (PSO) and Whale Optimization Algorithm (WOA)," J. Intell. Fuzzy Syst., vol. 44, pp. 595–610, 2022.
19. G. Woraphonbenjakul, A. Masood, and S. Cho, "A Survey on Fuzzy Logic for Cluster Head Selection in Wireless Sensor Networks," 2023 Int. Conf. Inf. Netw., pp. 725–727, 2023.
20. J. Zhang, P. Hu, F. Xie, J. Long, and A. He, "An Energy Efficient and Reliable In-Network Data Aggregation Scheme for WSN," IEEE Access, vol. 6, pp. 71857–71870, 2018, doi: 10.1109/ACCESS.2018.2882210.
21. Q. Wu, P. Sun, and A. Boukerche, "An energy-efficient UAV-based data aggregation protocol in wireless sensor networks," DIVANet 2018 - Proc. 8th ACM Symp. Des. Anal. Intell. Veh. Networks Appl., pp. 34–40, 2018, doi: 10.1145/3272036.3272047.
22. S. Prakash and A. Rajput, "Hybrid cryptography for secure data communication in wireless sensor networks," Adv. Intell. Syst. Comput., vol. 696, pp. 589–599, 2018, doi: 10.1007/978-981-10-7386-1_50.
23. K. N. Dattatraya and K. R. Rao, "Hybrid based cluster head selection for maximizing network lifetime and energy efficiency in WSN," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 3, pp. 716–726, 2022, doi: 10.1016/j.jksuci.2019.04.003.
24. A. Rajagopal, "Performance Analysis for Efficient Cluster Head Selection in Wireless

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.43.34.48

Sensor Network Using RBFO and Hybrid BFO-BSO," Int. J. Wirel. Commun. Mob. Comput., vol. 6, no. 1, p. 1, 2018, doi: 10.11648/j.wcmc.20180601.11.

25. A. Khalifeh, H. Abid, and K. A. Darabkh, "Optimal cluster head positioning algorithm for wireless sensor networks," Sensors (Switzerland), vol. 20, no. 13, pp. 1–26, 2020, doi: 10.3390/s20133719.
26. M. V. Babu, J. A. A. Alzubi, R. Sekaran, R. Patan, M. Ramachandran, and D. Gupta, "An Improved IDAF-FIT Clustering Based ASLPP-RR Routing with Secure Data Aggregation in Wireless Sensor Network," Mob. Networks Appl., vol. 26, pp. 1059–1067, 2020, [Online]. Available: https://api.semanticscholar.org/CorpusID:225171057
27. T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, "QoS Aware Trust Based Routing Algorithm for Wireless Sensor Networks," Wirel. Pers. Commun., vol. 110, pp. 1637–1658, 2020, [Online]. Available: https://api.semanticscholar.org/CorpusID:208118823
28. N. Moussa, Z. Hamidi-Alaoui, and A. E. B. El Alaoui, "ECRP: an energy-aware cluster-based routing protocol for wireless sensor networks," Wirel. Networks, vol. 26, pp. 2915–2928, 2020, [Online]. Available: https://api.semanticscholar.org/CorpusID:210118905

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)