The Scientific Temper (2024) Vol. 15 (4): 3247-3260
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2024.15.4.34
https://scientifictemper.com/
RESEARCH ARTICLE

Integrated energy-efficient routing and secure data management for location-aware wireless sensor networks with PFO leveraged improved fuzzy unequal clustering algorithm (IFUC)

L. Amudavalli*, K. Muthuramalingam

Abstract

Combining energy-efficient routing with secure data management for LAWSNs represents a challenging research domain and an emerging scientific paradigm. This approach includes various elements, for example, data collection, asymmetrical clustering and hybrid optimization as well as a model of the combined encryption Wireless Sensor Networks (WSNs). In the process of data collection, sensor nodes will sense environmental information (temperature, humidity, etc.), sample regularly and fuse to detect redundancy information for power saving. Geospatial clustering with IFUC is important in location-aware routing. This approach overcomes the hot spot problem and provides energy-efficient management of traffic within and between clusters by optimizing cluster sizes based on their access to the base station. Here, a hybrid encryption model is presented to combine asymmetric RSA with symmetric data encryption standard (3DES) encryption in order to carry out absolute encrypted data transmission, minimizing the probability of unauthorized accessible information. All the keys are systematically managed, periodically renewed, and handpicked through the phoenix fusion optimiser (PFO). The data transfer process is about the encryption of data by hardcoded keys and how this encrypted information is sent on the best route possible. The cluster heads (CHs) fuse data in clusters to minimize the redundant transmission of data. This data is then shared along the inter-cluster pathways to become a base station. A holistic energy-efficient, secure and optimized data handling solution tailored for location-aware wireless sensor networks (WSN) is thus proposed, extending the lifespan and enhancing the efficiency of the network using an integrated strategy.

Keywords: Wireless sensor network, Phoenix fusion optimizer, improved fuzzy unequal clustering, Cluster head, RSA, Date encryption standard.

Introduction

With advancements in the ability to embed sensors into our environment, the use of wireless sensor networks (WSN) has become more prevalent with applications such as environmental monitoring, industrial automation, healthcare and smart cities. It consists of multiple tiny, resource-constrained sensors that collect data and transmit it to a base station or sinks in the form of packets (Bhanu, D., & Santhosh, R. (2023); Soundari, A.G.,& Jyothi, V.L. (2020)). Large-scale deployment of Wireless Sensor Networks (WSN) can influence on potential of its applications, but it faces many challenges for efficient operation and protect data. TweetEnergy efficiency and the management of secure data can be daunting prospects to face. This research provides a solution to these problems by focusing on the design and development of an energy-efficient location-based routing protocol for Wireless Sensor Networks (WSN). Clustering, deep learning, optimal path detection, optimization algorithms and encryption are included in the protocol (Sridhar, M., & Pankajavalli, P.B., (2020); Kumar, R., Shekhar, S., Garg, H., Kumar, M., Sharma, B. & Kumar, S., (2022)). A collection of challenges in LPWSNs exists, such as mobility, location dissemination, traffic mapping and information surveying, which leads to a leading multifaceted problem involving many combination techniques and methods for the efficient operation of location-aware wireless sensor networks (WSN). A WSN is a wireless network typically made up of many dispersed sensors that cooperatively monitor physical or environmental conditions, such as temperature,

Department of Computer Science, Bharathidasan University, Tiruchirappalli, Tamil Nadu, India.

***Corresponding Author:** L. Amudavalli, E-Mail: amudalog@gmail.com

How to cite this article: Author. (2024). Article Title. The Scientific Temper, **15**(4):3247-3260.

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.4.34

Source of support: Nil

Conflict of interest: None.

Received: 10/10/2024 **Accepted:** 16/11/2024 **Published** : 20/12/2024

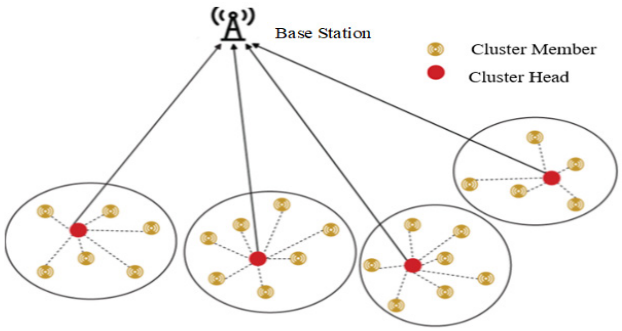


Figure 1: General architecture of WSN

sound, vibration, pressure, motion, or pollutants (Gupta, S.K., Kumar, S., Tyagi, S. &Tanwar, S., (2020)). The data collected by the sensors is sent to a central sink or a gateway for further processing and analysis Anandh, S.J. &Baburaj, E., (2020). This architecture of a WSN is shown in Figure 1, and it consists of sensor nodes, a data sink and a communication backbone.

Wireless Sensor Network (WSN) is a structure where varied kinds of technologies for many applications, such as Precision Agriculture, Habitat Monitoring, Industrial Automation, healthcare systems, etc., are in wide usage Kang, B., Park, C. and Choo, H., (2019). The constrained energy and processing capabilities of Wireless Sensor Networks (WSNs) are a primary obstacle to functional deployment. According to Vashisht, S. & Jain, S. (2019), Mohanadevi, C. &Selvakumar, S. (2022), sensor nodes are generally low-power devices and deployed in a distributed or remote environment powered by a battery. So, it is critical to save energy to maximize the network's operational lifetime and minimize its maintenance. Routing plays a vital role in enhancing energy efficiency to combat the power constraints in Sensor nodes for Wireless Sensor Networks (WSN) Hu H., Han, Y., Yao, M. & Song, X., (2021). The traditional routing strategies, especially advert-hoc and mesh networks, are inefficient for WSNs because of their vitality unconsciousness. In contrast, energy-efficient routing protocols attempt to increase the network lifetime by decreasing the individual node energy consumption. Sensor data collected over WSNs is typically private and must be secured from unauthorized access and tampering Prithi, S. & Sumathi, S, (2020). Besides, securing data confidentiality and integrity and ensuring the authenticity of transmission in resource-constrained scenarios is a very challenging issue Suresh Kumar, K. & Vimala, P, (2021).

Clustering in WSNs involves arranging sensor nodes in clusters to improve network efficiency. These heads, usually nodes with a higher capacity than the rest of the members, collect and pool data before transmitting it to the central processing unit Haseeb, K., Islam, N., Javed, Y. & Tariq, U., (2020). Optimized Clustering: Data transfer, which would be useless will be minimized and energy preserved. Deep learning or remote sensor network also applies to a subset of machine learning and make future predictions. In simple terms, it does the Forecast of NETWORK metrics. Importantly, deep learning algorithms can use historical data and trends combined to make smart decisions on routing that consequently reduce energy consumption Binu, G.S. &Shajimohan, B., (2020). The main part of energy-efficient routing is to search for the best way to transmit data. This involves selecting routes that minimize the spatial scale of information propagation, avoid areas with high population density and optimize the use of energy resources. Optimization algorithms are employed to finely tune routing decisions. The particular features of these algorithms focus on fine-tuning parameters such as transmission power and routing routes to save energy. To ensure data management security, encryption technology is employed to protect data in transmission and storage Bhandari, S., Wang, X. & Lee, R., (2020). The security measures include encrypting data packets and setting up authentication mechanisms to prevent a breach. Integrating these techniques into all in one place location-based routing system may significantly improve the energy efficiency and data confidentiality index of WSN. It is a complex area of study with a lot of potential since it needs innovative solutions to make the best out of Wireless Sensor Networks (WSN) capability while keeping data optimum and the network lasting long.

The following exhibits the research's main contribution:

- It is to improve the process by making sure that sensor nodes are efficiently collecting environmental data like temperature, humidity, and other vital parameters for WSN Data acquisition. In addition, the system uses periodic sampling and data aggregation at sensor nodes.
- An algorithm for adjusting the system to handle different inter-sensor node distances from the BS in a way that enables heterogeneously clustered and hybrid optimization in WSNs. The infrastructure of this system uses location-aware routing by employing non-equal clustering to increase the distribution of load by fading out the size of a cluster with the faded approach toward the base station. This paper proposes a distributed method named IFUC, where fuzzy logic is used for cluster head selection and cluster radius calculation, considering it as an approach that aims to save energy and extend the network lifetime. It introduces PFO as a hybrid inter-cluster routing optimization structure, integrating BRO and FHO architecture for improved network efficiency and routing performance.
- An innovative hybrid encryption scheme is proposed to improve data transmission security. This technology combines asymmetric encryption for secure key exchange with symmetric encryption

for efficient data transfer. Public key authentication (PFO) is included in the key selection procedure for encryption and decryption, therefore guaranteeing a strong security regime.

- If the distance between two troops is less than a threshold of 3, the soldiers in BRO increase their damage level by 1 to decide the optimization method utilized. After the damage level is more than zero, BRO is utilized for additional optimization. FHO is employed if the threshold is higher. This strategy combines FHO exploration with competitive BRO behavior according to particular scenario requirements.

The remaining sections of this article are organized as follows: In Section II, the literature studies that were done on energy-efficient routing and secure data management are covered. The proposed methodology is described in Section III. Section IV summarises the conclusions drawn from the projected model, and the research is concluded in Section V.

Literature Review

The authors have developed a Low Energy Adaptive Clustering Hierarchy (LEACH) single-hop inter-cluster routing, yet falls short for extensive networks. Enter the optimized Orphan-LEACH (O-LEACH) protocol, a novel clustering process. It minimizes energy consumption and extends network longevity by efficiently deploying orphan nodes. It is a very cutting-edge protocol and shines when it comes to keeping the network connected. By using hybrid optimization, CH election is well controlled and balances the routing paths in order to reduce the power consumption, which lengthens the WSN lifetime too many foldsSenthil, G.A., Raaza, A. & Kumar, N., (2022).

The authors have used the cluster routing protocols (Mehta, D. &Saxena, S., (2020)), stand out as key methodologies. The protocols form the clusters with cluster heads (CH), which help in transmitting data packets from one CH to another till they reach the base station. Data packets hop from node to node using Type 1 fuzzy logic-based multi-hop transmission (considering trust value and distance). This strategic service will provide a longer network life for WSN deployment and reduce the overhead, which is essential to operate WSN with the small scale of energy harvesting (Balaji, S., Golden Julie, E. & Harold Robinson, Y., (2019)).

The authors have proposed a MultiObjective Based Clustering and Sailfish Optimizer (SFO) guided routing approach in 2020. It is the most adaptive approach to CH selection and path to sink which will save energy and the lifetime of sensor nodes. The macroscopic comparison of the proposed technique from some existing works, such as grey wolf optimization (GWO), genetic algorithm (GA), ant lion optimization (ALO) and particle swarm optimization (PSO), shows an achievable improvement in energy efficiency (Khabiri, M. & Ghaffari, A., (2018)).

The authors have suggested a clustering-based routing protocol known as energy-aware and cuckoo optimization algorithm for wireless sensor networks, which prevents using the CRP to choose a group head by proposing a new criterion to select an optimal cluster head while simultaneously considering four criteria. MATLAB simulation results are compared with other algorithms like LEACH and LACH-EP algorithm to show better performance in the reaction of Node life a packet delivery ratio, Bhardwaj, R. & Kumar, D., (2019).

The authors have suggested that fitness function which factored in energy, delay, traffic rate, distance and cluster density. The multi-objective fractional particle lion (MOFPL) algorithm is the method of choosing the best cluster heads and deploying routing paths. The results indicate that MOFPL can enhance the network energy conservation and node endurance properties (Khan, M.K., Shiraz, M., ZrarGhafoor, K., Khan, S., SafaaSadiq, A. & Ahmed, G., (2018)).

The authors have presented a novel, energy efficient routing protocol for WSNs. It consists of a data transmission algorithm, cluster head selection, and cluster formation. Compared with existing protocols, EE-MRP reduces the reclustering to a minimum effectively and adopts static clustering, illustrated by simulation results that it has a longer lifetime of the network, higher throughput as well as energy efficiency (Arjunan, S. & Sujatha, P., (2018)).

The authors have introduced a Novel clustering compound technique that has been employed using fuzzy logic-based unequal clustering and ant colony optimization (ACO)- based routing to overcome the above problem constraints and to maximize hot spots issue-free along with network lifetime extension. The protocol is categorized into cluster head (CH) selection, inter-cluster routing, and maintenance. To choose the CH nodes properly, fuzzy logic is the best option, and clusters are unequal in shape and size dependent on factors of energy, distance to BS (Base Station) and node centrality. Data transmission from CHs to the BS is guaranteed through routing using ACO (Mittal, N., (2019)).

The authors have used a threshold dependent energy-efficient clustering protocol (TECP) optimized by moth flame optimization (MFO). Cartwheel node: An MFO improves network stability by load balancing and energy optimization through multi-hop communication between CHs and the BS. The analytical and simulation results indicate that the proposed TECP significantly outperforms existing protocols in terms of energy efficiency, network lifetime and stability (Shahbaz, A.N., Barati, H. &Barati, A., (2021)).

The authors have developed a three-phase homogenous WSN multipath routing strategy. The former uses the firefly algorithm (FFA) for network clustering, while fuzzy logic is adopted as a routing strategy between CH and primary/backup path selection. This method is a better performer

Q 3

in end-to-end delay, energy efficiency, packet loss ratio, and network lifetime than other routing methods throughout the simulation results (Edla, D.R., Kongara, M.C. &Cheruku, R., (2019)).

The authors have engineered for numerical optimization in Swarm Routing. It utilizes a new fitness function that takes account of relay nodes, gateway to base station distance and relay load factor. The experiments confirm the superiority of the PSO-based routing in significantly prolonging WSN lifetime in contrast to alternative bio-inspired methods that were used (Shishehgarkhaneh, M.B., Azizi, M., Basiri, M. &Moehler, R.C., 2022).

Problem Statement

An important issue for WSNs is minimizing computational time and ensuring trusted data. These networks are used in a wide range of applications, including environmental monitoring, health care and military operations. Power-constrained sensor networks consist of small sensor nodes having limited power resources, necessitating long operational lifetimes (Bhanu D & Santhosh R, (2023)). In order to face this problem, we propose in this research an energy-efficient routing protocol based on location for the wireless sensor network WSN (Kumar, R., Shekhar, S., Garg, H., Kumar, M., Sharma, B. & Kumar, S., (2022); Vashisht, S. & Jain, S., (2019)). For an efficient node grouping with minimal data redundancy and energy, it uses clustering algorithms. These integrate deep learning methods to improve the adaptive optimization of data routing through the network itself. This paper investigates strategies for determining the most energy-efficient path, taking into account load balancing between sensor nodes. The research studies encryption programs as data gets confidence and congruence. We propose an energy-efficient and secure data management in location-aware wireless sensor networks (WSNs) with clustering to realize a complete solution by considering key components such as clustering, deep learning (DL), optimal routing (OR), optimization algorithm (OA) and encryption.

Proposed Methodology

Designing energy-efficient routing protocols for WSN is a challenging but largely demanded area. We contribute a novel and comprehensive study that utilizes clustering, deep learning, and path optimization as well as encryption for the reduction of security breaches to increase the efficiency and reliability of WSN. The proposed approach couples the pathfinder and obstacle factor-using clustering (PFO) with the cordial face using centroid algorithm to minimize data transmission, energy consumption, and security in location aware WSNs which is cost-effective for a range of applications.

Data Collection

In a network, these sensor nodes measure environmental characteristics such as temperature, humidity or other parameters of interest. In order to save power and reduce duplicate information sending, thereby achieving a cyclic sampling and data aggregation in these nodes. Rather than transmitting raw data all the time, nodes periodically sum up the information they accumulated and send it in a batch, which enables efficient communication, leading to reduced energy consumption of the sensor nodes — one of the most important metrics defining the lifetime of a network. Figure 2 illustrates the proposed architecture as a whole, showcasing the complete system design and its components.

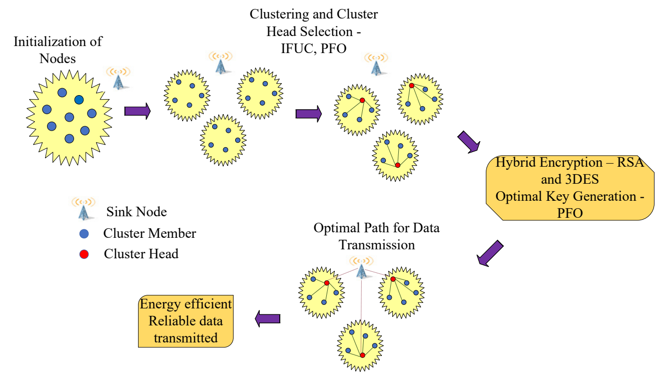


Figure 2: Overall proposed architecture

Enhancing WSN efficiency through Hybrid Optimization Leveraged IFUC

Unequal clustering plays a crucial role in location-aware routing in WSN. It addresses the challenge of varying distances of sensor nodes from the base station (BS) by forming clusters based on proximity. This approach acknowledges that nodes near the BS have different routing roles than those farther away, particularly in location-based routing. There are two types of traffic in clustered WSNs: intra-cluster traffic (within the cluster) and inter-cluster traffic (between clusters). Cluster members sense real-world parameters and send data to their CH, which aggregates and transmits data to the BS directly or via intermediate CHs.CHs near the BS consume energy quickly due to heavy intra-cluster and inter-cluster traffic, causing network connectivity issues and creating hotspots. Unequal clustering techniques mitigate this problem by balancing the load between CHs. Clusters close to the BS are smaller, resulting in fewer cluster members and lower intra-cluster traffic.

IFUC

Conversely, the bigger clusters further from the BS carry out more intra-cluster traffic and less inter-cluster traffic. It keeps energy used at the maximum efficient level.

Distributed IFUC saves battery life, prevents hotspots and increases network lifetime. Fuzzy logic is employed for selecting CHs and setting cluster radii by taking energy, distance to the BS and node density into account. Tentative CHs contend for the position of final CH status, given their probability and broadcasting radius. Finals only choose the CHs with possible greatest probabilities to ensure the process of forming clusters is more efficient. IFUC is able to solve the energy and load balancing in WSN, which is helpful in improving the network performance and lifetime.

Membership Function Definition: For the primary values such as energy, distance to BS and maybe some other related parameters like node density, IFUC starts by defining fuzzy membership functions. They divide into three linguistic approximations of membership functions to produce the low, medium, or high values of the parameters.

Node Evaluation: Every sensor node in the network performs its own evaluation on parameters, which include available energy and distance of each node to the BS. These parameters are being evaluated using the fuzzy membership functions to check if this node is ready to act like a CH.

Calculation of CH Probability: Using the fuzzy evaluation, calculate the probability for each node to become a CH. This probability is between 0 to 1, which shows the effectiveness of the node to work as a CH.

Competition of CH role: The nodes are contending for the role of CH. Nodes with a higher probability are more likely to be selected as CHs. However, not all nodes become cluster heads (CHs); it is probabilistic in nature.

Cluster Formation: The nodes identified as CHs establish clusters in the network. For instance, they would collect the data with other clusters based on trees if the clusters are organized in a hierarchical manner and forward them to the BS. The obtained competitions will provide differences in cluster sizes and shapes.

Dynamic: Clusters can be formed periodically (or in response to changes in network conditions), so the process is dynamic. This adaptability allows the network to adjust its cluster structure as nodes deplete their energy or as the network's topology changes.

IFUC leverages fuzzy logic to provide a degree of flexibility in cluster formation. It helps address the problem of nodes with varying energy levels and varying distances to the BS. By considering these factors in a fuzzy manner, it optimizes the energy consumption in the network, prolonging the network's lifetime while ensuring efficient data routing to the BS.

IUCF Clustering Algorithm

1. Initialize Parameters
    - Set T as the probability of becoming a tentative cluster head.
    - Set nodeState to CLUSTERMEMBER.
    - Create an empty list for clusterMembers.
    - Identify the current node as myClusterHead.
    - Initialize the flag beTentativeHead as TRUE.
2. Generate Random Number
    - Generate a random number μ in the range [0, 1].
3. Tentative Cluster Head Selection
    - If μ is less than T proceed to calculate the Rcomp (competition radius) using fuzzy if-then mapping rules.
4. Candidate Cluster Head Message
    - Send a CandidateCHMessage to other nodes in the network, including the node's ID, the calculated Rcomp, and the energy level (Energy).
5. Evaluate Candidate Messages
    - Upon receiving CandidateCHMessages from other nodes (e.g., node N), compare the energy of the current node (this. energy) with that of node N (N. Energy).
    - If the current node's energy is lower than node N, set the beTentativeHead flag to FALSE and advertise a QuitElectionMessage with the node's ID to withdraw from the cluster head competition.
6. Tentative Cluster Head Confirmation
    - If the beTentativeHead flag remains TRUE, indicating that the current node is selected as a tentative cluster head, advertise a CHMessage with the node's ID.
7. Cluster Head Status
    - Change the nodeState to CLUSTERHEAD, signifying that the node has become a cluster head.
8. JoinCHMessage Reception
    - If node N receives a JoinCHMessage from the current node, add node N to the clusterMembers list, indicating its membership in the cluster.
9. Exit or Closest Cluster Head Selection
    - If the beTentativeHead flag is FALSE, the node exits the cluster head competition.
    - If multiple CHMessages are received, select the closest cluster head as myClusterHead and send a JoinCHMessage to that cluster head to signify membership.

This algorithm guides the autonomous decision-making process for nodes in a WSN, allowing them to determine whether they should take on the role of a cluster head or remain a regular cluster member. It accounts for factors such as energy, fuzzy logic, and probability, leading to efficient and adaptive cluster formation within the network.PFO combines BRO and FHO for inter-cluster clustering in WSN.

Phoenix Fusion Optimizer (PFO)

BRO Dehghani, M., Hubálovský, Š. &Trojovský, P., (2020) is inspired by the battle royale video game concept. In this optimization approach, multiple agents or solutions compete against each other. Over time, weaker solutions are eliminated, and only the strongest ones survive. This mimics the competitive and survival aspects of battle royale games.

FHO Rahkar Farshi, T., (2021) is inspired by the behavior of certain birds, known as Fire Hawks, that intentionally spread fires to aid in their hunting. FHO optimizes by simulating this behavior, with agents dropping and spreading information to find optimal solutions.PFO integrates these two algorithms, drawing on their strengths. Like in a battle royale game, solutions compete and are ranked in terms of their performance. The elimination process, inspired by BRO, helps identify promising solutions. FHO aspect introduces the idea of spreading information, possibly from stronger solutions to weaker ones, enhancing the overall optimization process. The fusion of these two optimization approaches aims to create a more robust and efficient method for solving complex problems. PFO leverages competitive selection and information sharing, drawing inspiration from both the competitive world of battle royale and the intelligent behavior of Fire Hawks.

Initial Random Population: BRO's inspiration is drawn from battle royale games where players parachute onto a map. Similarly, BRO begins with a random population uniformly distributed across the problem space. Each individual in this population represents a soldier or player in the optimization process.

Competitive Behavior: In BRO, these soldiers engage in competitive behavior. They attempt to damage the nearest soldier by shooting a virtual weapon. When one soldier successfully damages another, the damaged soldier's damage level increases by one as shown in Eq. (1).

$$y_i.damage = y_i.damage + 1 \tag{1}$$

where $y_i.damage$ is the damage level of the ith soldier among the population.

In BRO, if the distance between soldiers is less than a threshold of 3, their damage level increases by 1. If the damage level exceeds 0, BRO is used for further optimization Eq. (2). However, when the threshold is greater, FHO is employed Eq. (3). This approach combines competitive behavior BRO with exploration inspired by FHO based on the situation's requirements.

$$y_{damag,\dim} = y_{damag,\dim} + rand\left(y_{best,\dim} - y_{damag,\dim}\right) \tag{2}$$

$$fh_a^{new} = fh_a + \left(rand_1 \times gb - rand_2 \times fh_{near}\right), a = 1,2,...,n \tag{3}$$

In Eq. (2), $rand$ and $y_{damag,\dim}$ suggests that $rand$ is a randomly generated number uniformly distributed between 0 and 1, and $y_{damag,dim}$ represents the position of the damaged soldier in dimension dim. In Eq. (3), fh_a^{new} is the new position vector of the a*th* Fire Hawk $\left(fh_a\right)$, the new position of a Fire Hawk is determined based on its proximity to the global best solution (*gb*) and another Fire Hawk $\left(fh_{near}\right)$. The random numbers $rand_1$ and $rand_2$ play a role in determining the movements of the Fire Hawks either toward the main fire or toward the territories of other Fire Hawks.FHO, which utilizes the behavior of birds known as Fire Hawks to update positions in the optimization process. These birds collect burning sticks from the main fire to spread fire in selected areas and force prey to flee. FHO incorporates these behaviors into its position updating procedures, adding an element of intelligent exploration to the optimization process.

Position Changing: After being damaged, a soldier seeks to change its position immediately. It moves toward a point located between its previous position and the best position found so far (elite player). This movement reflects an exploitation strategy to improve its chances. This competitive and dynamic process mimics the interactions and strategies seen in battle royale games. Soldiers compete, and those who are damaged seek to adapt and find a better position to continue the competition.

Exploration and exploitation: In PFO, allowing soldiers (individuals) to re-enter the problem space after they have been removed or killed due to certain conditions helps prevent the algorithm from converging prematurely. This reintroduction of individuals provides a better exploration of the problem space, enabling the algorithm to continue searching for optimal solutions rather than prematurely settling on a suboptimal one.

$$y_{damag,dim} = rand\left(upbo_{dim} - lo\,bo_{dim}\right) \tag{4}$$

In Eq. (4), $lo\,bo_{dim}$ represents the lower bound and $upbo_{dim}$ represents the upper bound of dimension *dim* within the problem space. These bounds define the allowable range for variables in that dimension. In every Δ iteration, the feasible search space of the problem starts to decrease or shrink towards the best solution. The initial value for Δ is calculated as $\Delta = \Delta + log_{10}\, max\, circle$ but is then updated to $\Delta = \Delta + round\left(\frac{\Delta}{2}\right)$, $max\, circle$ refers to the maximum number of generations or cycles in the algorithm. The purpose of this mechanism appears to be gradually reducing the search space as the optimization process progresses, ultimately focusing the search on the most promising areas of the problem space. Exploration and exploitation both benefit from this interplay. Thus, the following updates are being made to the lower and upper bound.

$$lo\,bo_{dim} = y_{best,dim} - sd\left(\overline{y_{dim}}\right)$$

$$upbo_{dim} = y_{best,dim} + sd\left(\overline{y_{dim}}\right) \tag{5}$$

In Eq. (5), $sd\left(\overline{y_{dim}}\right)$ refers to the standard deviation, which measures the amount of variation or dispersion in a set of values, $\overline{y_{dim}}$ represents a specific dimension in the problem space, $y_{best,dim}$ is the position of the best solution found so far for that dimension, $lo\,bo_{dim} / upbo_{dim}$ suggests that if a variable exceeds its original lower or upper bound, it is set back to the original lower or upper bound. This ensures that variables do not go beyond the defined boundaries. The best player or soldier (the one with the best solution) is preserved and treated as an elite individual. Elitism is often used to maintain the best solutions throughout the optimization process, preventing them from being lost in subsequent iterations.

Termination: The termination condition for the PFO algorithm is defined by two components. Firstly, the algorithm terminates if the number of iterations reaches the maximum number of iterations. This ensures that the algorithm does not continue indefinitely and provides a limit to the search process.

Hybrid Encryption Model for Security

The suggested hybrid encryption framework utilizes provides security and improves_rate_adjusted efficiency. It starts with secure key exchange using RSA asymmetric encryption to agree upon a shared secret/key. This is followed by 3DES symmetric encryption, which allows fast data transmission and security. A hybrid optimization model for choosing keys during the encryption/decryption process that are managed securely and rotated regularly. One advantage is this combination contributes to robust security and high speed data processing. Symmetric encryption (3DES) is quicker and less computationally intensive than asymmetric encryption, and it is used to encrypt data while we are sending data in real-time. The secure key management and regular rotation limit the risk of a key compromise over the long term.

Secure Key Exchange (RSA)

- The communicating nodes should first establish a secure connection as well as exchange encryption keys.
- Asymmetric encryption (for example RSA) – for key exchange. In ACA-Py, each node creates an RSA keypair, a public/private pair.
- Public keys are known to everyone, but private keys are secret. Nodes encrypt the shared symmetric key (3DES key) using each other's public keys.
- Encrypted 3DES key is sent to the target node, which decrypts using a private key and obtains the shared 3DES key ·
- This operation allows only the recipient to decrypt the shared key, thus ensuring a secure key exchange.

Data Transmission (3DES)

- Translate the servers to 3DES for data transport with the symmetrical key called by both Virtual nodes using 3DES protection.
- It is a type of symmetric encryption algorithm which uses a single key that both encryptions and decryptions respectively.
- Every node uses the encrypted key to secure and release the exchanged data by this 3DES encryption key.
- Symmetric encryption is faster than asymmetric encryption so if there's a lot of data to encrypt (and decrypt) it would be faster and more efficient.

Secure Key Management and Rotation

- Secure and regularly rotate encryption keys to ensure security.
- Key management, including protection of the RSA private keys and the shared 3DES key
- Rekey periodically creates new RSA key pairs for key exchange and fresh 3DES keys for symmetric encryption.
- Key rotation – When an attacker gets access to a key that is replaced very often so the impact that injecting the key has can only manifest itself for a limited time.

In section 3.2.2, a hybrid model PFO is presented that integrates BRO and FHO to improve the key selection in encryption. However, the PFO allows for a new hybrid optimization model to generate encryption and decryption keys. It uses sophisticated algorithms to automatically select the most secure and fastest keys that can be used for encryption and decryption, and this will actually improve the security of your data protection processes, as well as their performance.

Data Transmission and Aggregation

During this operation process, encryption using keys in use is a known encryption that does not compromise data security. Then, the data is encrypted and sent through the best possible route from a measured, efficient networking perspective. Node dynamics of CH in data aggregation. This ensures that the data transmission is not repeated in the cluster thereby reducing resource wastage with minimal consumption energy. The aggregated data is then passed on inter-cluster toward the base station. It stores energy in clusters and collects data efficiently at the BS for information collection & processing from geographically distant parts of WSN.

Result and Discussion

Experimental Setup

Python is used to implement the suggested model. The performance of the proposed technique was analyzed, as well as its performance was compared to that of other algorithms, such as BRO, FHO, Coati Optimization

Algorithm (COA)Dehghani, M., Montazeri, Z., Trojovska, E. &Trojovsky, P,(2023). Tasmanian Devil Optimization (TDO)Dehghani, M., Hubalovsky, S. &Trojovsky, P., (2020). Evaluation of the suggested model's effectiveness in terms of energy consumption, energy efficiency, latency, network lifetime (NLT), and data delivery ratio (DDR). Fig. 3 displays communication between node 50 and node 250 within the network. In Fig. 4, the illustration portrays the clustering of sensor nodes connecting node 50 to node 250 within the network. Fig. 5 demonstrates data aggregation taking place at cluster heads spanning from node 50 to node 250 in the network.

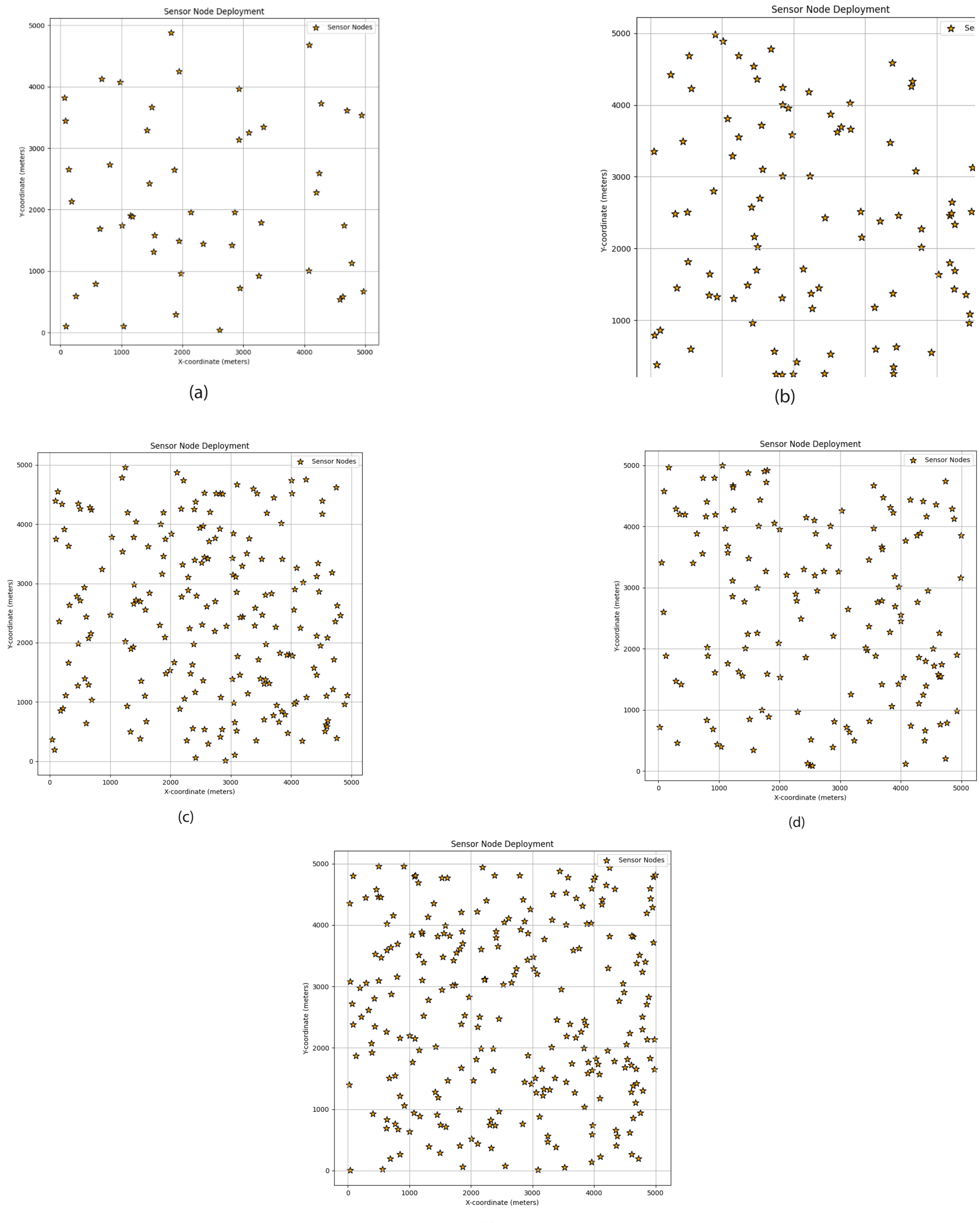


Figure 3: Interconnection between Node 50 and Node 250

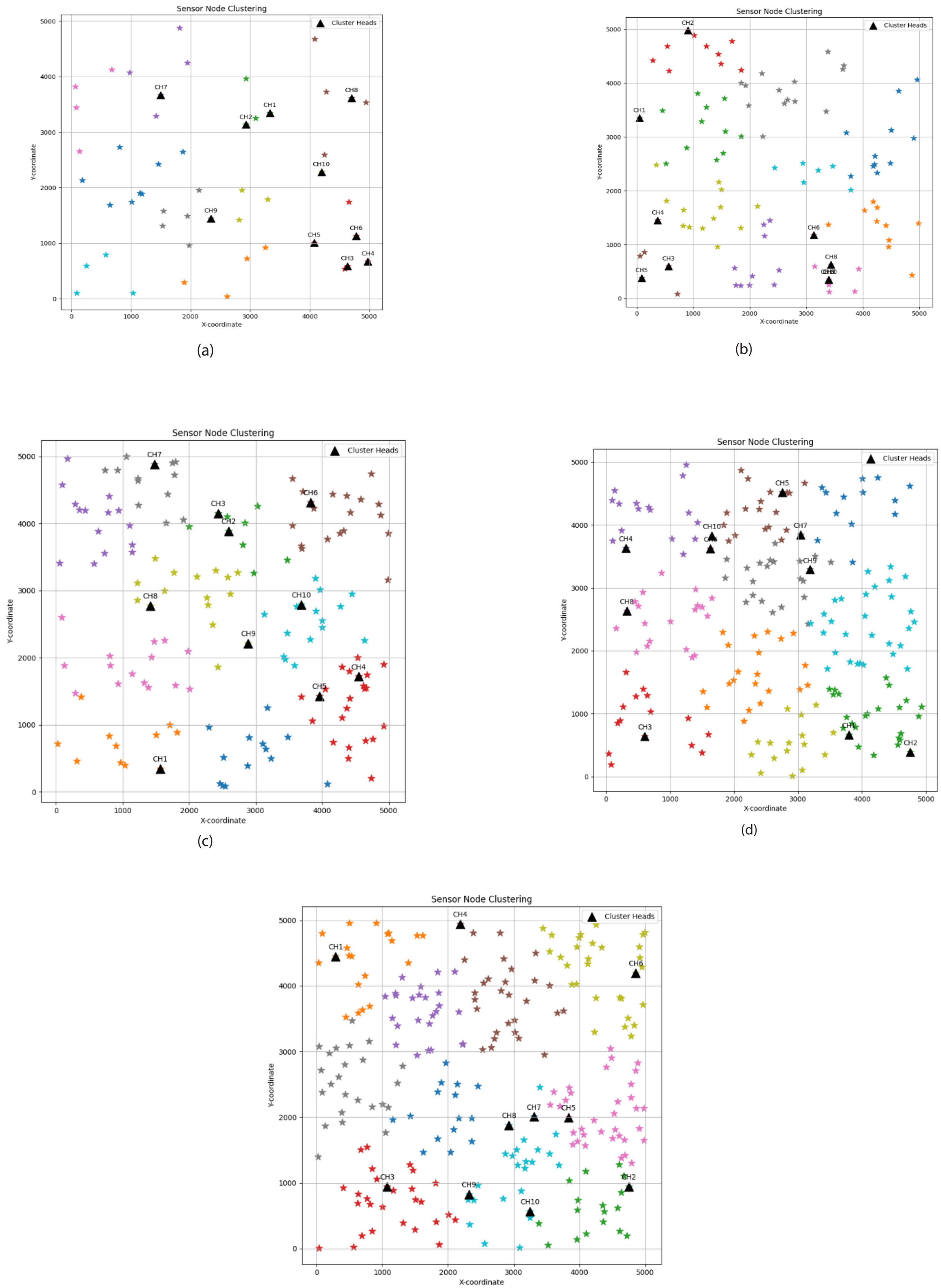


Figure 4: Sensor node clustering between node 50 to node 250

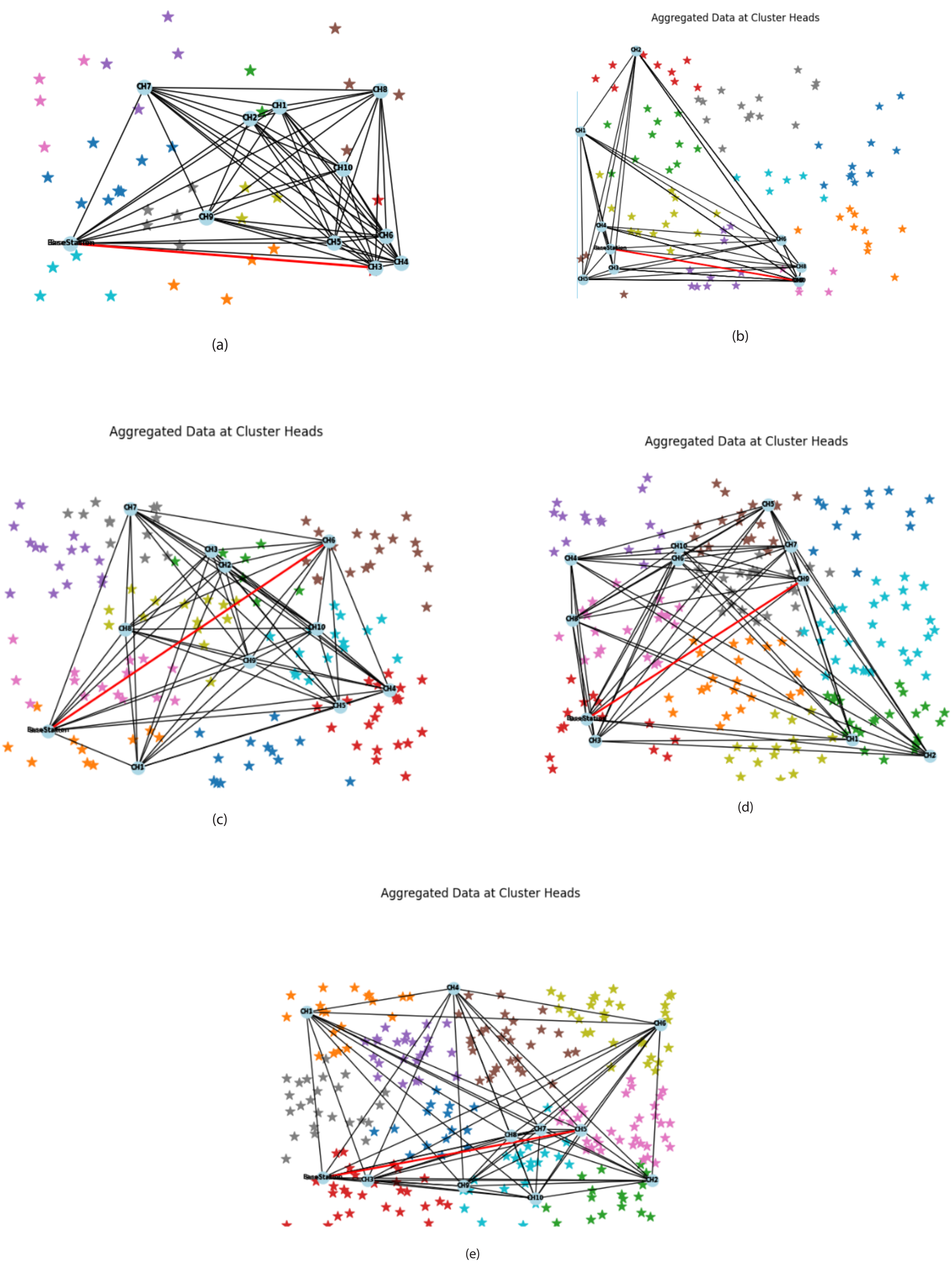


Figure 5: Data aggregation at cluster heads from node 50 to 250

Performance Metrics Overall Analysis

Table 1 presents a comprehensive analysis of performance metrics for node 50, utilizing various methods, including BRO, FHO, COA, TDO, and the proposed method. Energy consumption measures the amount of energy used by each method, with lower values indicating more efficient energy utilization. Among the methods, the proposed method is the most energy-efficient, consuming 35.036 units, while TDO consumes the highest energy at 43.930 units. Energy efficiency is quantified in arbitrary units, and higher values signify better efficiency. The proposed method exhibits the highest energy efficiency at 2,036,187 units, surpassing other methods, with TDO being the least efficient. Latency is the time it takes for data to travel from the source to the destination. Lower latency values are preferable. The proposed method achieves the lowest latency at 2.009 units, indicating faster data transmission. In contrast, FHO exhibits the highest latency at 3.865 units.NLT is a measure of how long the network can operate effectively. The proposed method has the longest NLT at 3,718,181 units, suggesting a prolonged network lifespan. TDO, on the other hand, has the shortest NLT among the methods.DDR quantifies the ratio of successfully delivered data. The proposed method has the highest DDR at 0.994, indicating a high rate of successful data delivery. Also, TDO has the lowest DDR at 0.921.

Table 1: Overall analysis - performance metrics for node 50

Methods	*BRO*	*FHO*	*COA*	*TDO*	*Proposed*
Energy Consumption	36.965	37.028	39.952	43.930	35.036
Energy Efficiency	1555256	1508816	1491590	1207152	2036187
Latency	3.247	3.865	2.989	2.435	2.009
NLT	3084760	3572949	3331413	3572948	3718181
DDR	0.983	0.971	0.959	0.921	0.994

Table 2 provides a comprehensive analysis of performance metrics for Node 100, evaluating the performance of different methods, including BRO, FHO, COA, TDO, and the proposed method. Among the methods, the proposed approach exhibits the lowest energy consumption at 35.185 units, while COA consumes the most energy at 40.549 units. The Proposed method demonstrates the highest energy efficiency at 1,519,568 units, surpassing other methods. COA exhibits the lowest energy efficiency among the methods. Latency represents the time it takes for data to traverse from source to destination. Lower latency values are preferred. The proposed method boasts the lowest latency at 3.234 units, indicating faster data transmission. In contrast, TDO has the highest latency at 5.315 units. The proposed method boasts the longest NLT at 3,541,541 units, suggesting an extended network lifespan. COA, on the other hand, has the shortest NLT among the methods.

Performance metrics from the node 150 were analyzed in detail (Table 3). It is clear that the proposed method has the best energy utilization at 35.212 units, which, on the other hand, BRO needs to consume more energy than aloof components, i.e., 37.297 units for the incremental deployment phase. This method achieves maximal energy efficiency at 1,595,926 units, while COA is the least efficient among those properties. This method had the lowest latency of 3.166 units, hence faster data communication and TDO had having highest latency. Figure 3 shows that this

Table 2: Overall analysis - performance metrics for node 100

Methods	*BRO*	*FHO*	*COA*	*TDO*	*Proposed*
Energy Consumption	36.084	37.168	40.549	39.656	35.185
Energy Efficiency	1504825	1503556	1449321	1496664	1519568
Latency	5.096	3.658	4.165	5.315	3.234
NLT	3084760	3241321	3425413	3524768	3541541
DDR	0.962	0.972	0.954	0.965	0.973

Table 3: Overall analysis - performance metrics for node 150

Methods	*BRO*	*FHO*	*COA*	*TDO*	*Proposed*
Energy Consumption	37.297	36.617	39.985	39.649	35.212
Energy Efficiency	1569666	1503556	1400265	1496664	1595926
Latency	5.850	3.622	4.455	5.322	3.166
NLT	3015441	3536544	3425569	3161946	3616464
DDR	0.960	0.944	0.951	0.930	0.964

Table 4: Overall analysis - performance metrics for node 200

Methods	*BRO*	*FHO*	*COA*	*TDO*	*Proposed*
Energy Consumption	37.915	36.617	39.985	39.649	35.212
Energy Efficiency	1569958	1503556	1400265	1496664	1595926
Latency	5.945	4.415	4.895	5.313	3.247
NLT	3049871	3514674	3491162	3185946	3694964
DDR	0.960	0.945	0.933	0.922	0.969

Table 5: Overall analysis - performance metrics for node 250

Methods	*BRO*	*FHO*	*COA*	*TDO*	*Proposed*
Energy Consumption	37.969	36.536	39.355	39.456	35.035
Energy Efficiency	1565163	1553156	1423856	1496435	1594564
Latency	4.656	4.575	4.347	5.457	3.465
NLT	3098986	3065549	3497461	3188749	3521164
DDR	0.941	0.931	0.927	0.927	0.955

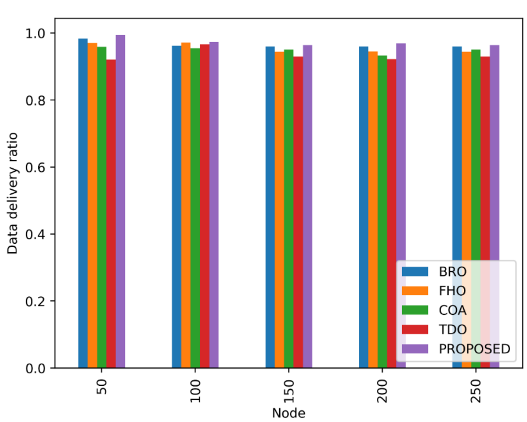
method has the longest did and NLT at 3616464 of enhanced network life span, while FHO got the shortest NLT. Finally, the proposed method provides the highest DDR with 0.964 (best DD performance); however, TDO has the lowest and worst capacity among them all.

Table 4 shows in-depth performance metrics for node 200. This method has efficient energy usage, which is 35.212 units, and on the other hand, BRO shows the worst energy consumption, going up to 37.915 units, way too higher than our proposed method. COA yields the least energy-efficient result of all methods, and the proposed method achieves an energy efficiency of 1,595,926 units. The proposed method exhibits the lowest latency at 3.247 units, signifying faster data transmission. FHO displays the highest latency among the methods. The proposed method boasts the longest NLT at 3,694,964 units, indicating an extended network lifespan. COA has the shortest NLT in comparison. The proposed method achieves the highest DDR at 0.969, indicating a high rate of successful data delivery. TDO displays the lowest DDR among the methods.

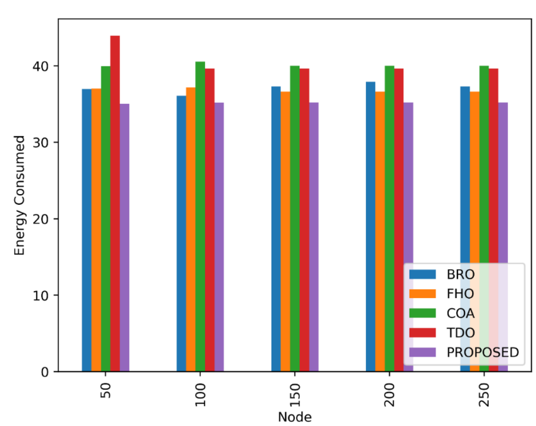
Table 5 presents a comprehensive analysis of performance metrics for node 250. The proposed method exhibits the most efficient energy consumption at 35.035 units, while BRO consumes the most at 37.969 units. The proposed method demonstrates the highest energy efficiency at 1,594,564 units, while COA displays the lowest efficiency among the methods. The proposed method boasts the lowest latency at 3.465 units, indicating faster data transmission. TDO has the highest latency among the methods. The proposed method has a comparatively long NLT at 3,521,164 units, suggesting an extended network lifespan, while FHO exhibits the shortest NLT. The proposed method achieves the highest DDR at 0.955, indicating a high rate of successful data delivery. FHO displays the lowest DDR among the methods.

Overall graphical representation

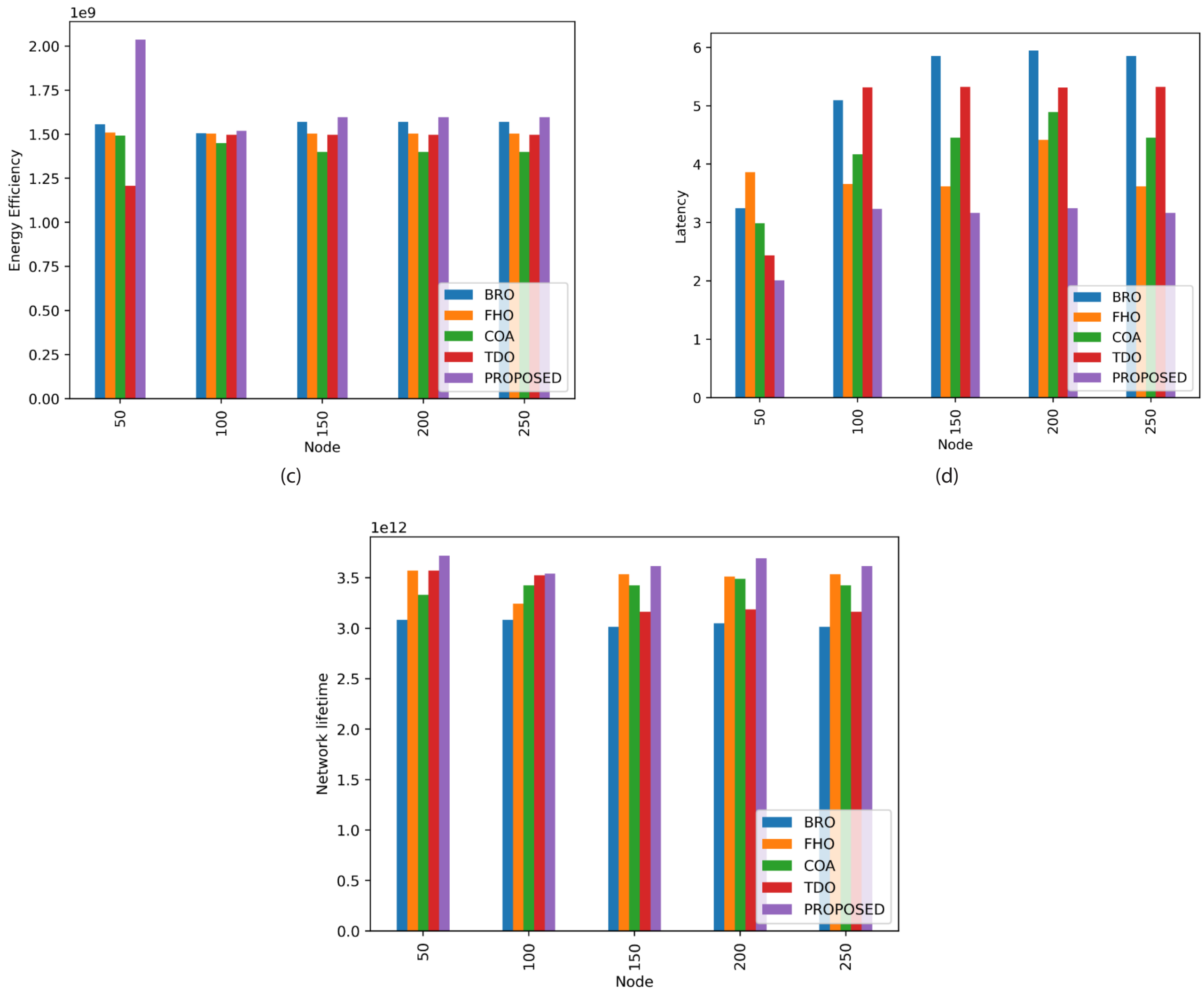
Graphical representation (a) DDR (b) Energy consumption (c) Energy efficiency (d) Latency (e) NLT is shown in Figure 6.



(a)



(b)



(c) (d)

(e)

Figure 6: Graphical representation (a) DDR (b) Energy consumption (c) Energy efficiency (d) Latency (e) NLT

Conclusion

For WSN, this work established an energy-efficient location-based routing protocol with an emphasis on clustering, deep learning, optimal path identification, optimization methods, and encryption. In order to cut down on redundancy and save energy, sensor nodes collected environmental data during the data-collecting phase, including temperature and humidity. This data was then periodically sampled and aggregated. IFUC, which powers unequal clustering, was essential to location-aware routing. The hot spot issue was successfully resolved, and energy-efficient intra- and inter-cluster traffic management was ensured by optimizing cluster sizes depending on base station proximity. To improve security, symmetric 3DES and asymmetric RSA encryption were merged into a hybrid encryption paradigm for safe data transmission.PFO was utilized to securely maintain, rotate, and choose the keys on a regular basis. Data was encrypted using pre-established keys and sent via the best path throughout the data transmission phase. In order to reduce redundant data transfer, CH aggregated data within clusters. After that, data was sent via inter-cluster paths to the base station. In the end, this integrated strategy increased the lifespan and efficiency of the network by providing a complete solution for data management in location-aware WSNs that is safe, optimized, and energy-efficient.

Ethical Approval

This article does not contain any studies with human participants performed by any of the authors.

Acknowledgment

We wish to thank the Editor, Associate Editor and reviewers for their invaluable comments and suggestions, which significantly enriched the manuscript.

References

Anandh, S.J. & Baburaj, E. (2020). Energy efficient routing technique for wireless sensor networks using ant-colony optimization. *Wireless Personal Communications*, 114(4), 3419-3433.

Arjunan, S. & Sujatha, P. (2018). Lifetime maximization of wireless sensor network using fuzzy based unequal clustering and ACO based routing hybrid protocol. Applied Intelligence, 48, 2229-2246.

Balaji, S., Golden Julie, E. & Harold Robinson, Y. (2019). Development of fuzzy based energy efficient cluster routing protocol to increase the lifetime of wireless sensor networks. *Mobile Networks and Applications*, 24, 394-406.

Bhandari, S., Wang, X. & Lee, R. (2020). Mobility and location-aware stable clustering scheme for UAV networks. *IEEE Access*, 8, 106364-106372.

Bhanu D & Santhosh R. (2023). Fuzzy enhanced location aware secure multicast routing protocol for balancing energy and security in wireless sensor network. *Wireless Networks*, 1-20.

Bhardwaj, R. & Kumar, D. (2019). MOFPL: Multi-objective fractional particle lion algorithm for the energy aware routing in the WSN. *Pervasive and Mobile Computing*, 58, 101029.

Binu, G.S. &Shajimohan, B. (2020). A novel heuristic-based energy efficient routing strategy in wireless sensor network. *Peer-to-Peer Networking and Applications*, 13, 1853-1871.

Dehghani, M.,Hubálovský, Š. &Trojovský, P. (2020). Tasmanian devil optimization: a new bio-inspired optimization algorithm for solving optimization algorithm. IEEE Access, 10, 19599-19620.

Dehghani, M., Montazeri, Z., Trojovska, E. &Trojovsky, P. (2023). Coati Optimization Algorithm: A new bio-inspired metaheuristic algorithm for solving optimization problems, Knowledge-Based Systems, 259(1). DOI: 10.1016/j.knosys.2022.110011

Edla, D.R., Kongara, M.C. &Cheruku, R. (2019). A PSO based routing with novel fitness function for improving lifetime of WSNs. *Wireless Personal Communications*, 104(1), 73-89.

Gupta, S.K., Kumar, S., Tyagi, S. &Tanwar, S. (2020). Energy efficient routing protocols for wireless sensor network. *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's,* 275-298.

Haseeb, K., Islam, N., Javed, Y. & Tariq, U. (2020). A lightweight secure and energy-efficient fog-based routing protocol for constraint sensors network. *Energies*, 14(1), 89.

Hu, H., Han, Y., Yao, M. & Song, X. (2021). Trust based secure and energy efficient routing protocol for wireless sensor networks. *IEEE Access*, 10, 10585-10596.

Kang, B., Park, C. & Choo, H. (2019). A location aware fast PMIPv6 for low latency wireless sensor networks. *IEEE Sensors Journal*, 19(20), 9456-9467.

Khabiri, M. &Ghaffari, A. (2018). Energy-aware clustering-based routing in wireless sensor networks using cuckoo optimization algorithm. *Wireless Personal Communications*, 98, 2473-2495.

Khan, M.K., Shiraz, M., ZrarGhafoor, K., Khan, S., SafaaSadiq, A. & Ahmed, G. (2018). EE-MRP: energy-efficient multistage routing protocol for wireless sensor networks. *Wireless Communications and Mobile Computing,* 1-13.

Kumar, R., Shekhar, S., Garg, H., Kumar, M., Sharma, B & Kumar, S. (2022). EESR: Energy efficient sector-based routing protocol for reliable data communication in UWSNs. *Computer Communications*, 192, 268-278.

Mittal, N. (2019). Moth flame optimization-based energy efficient stable clustered routing approach for wireless sensor networks. *Wireless Personal Communications*, 104, 677-694.

Mehta, D. &Saxena, S. (2020). MCH-EOR: Multi-objective cluster head-based energy-aware optimized routing algorithm in wireless sensor networks. *Sustainable Computing: Informatics and Systems*, 28, 100406.

Mohanadevi, C. &Selvakumar, S. 2022. A qos-aware, hybrid particle swarm optimization-cuckoo search clustering based multipath routing in wireless sensor networks. *Wireless Personal Communications,* 127(3), 1985-2001.

Prithi, S. &Sumathi, S. (2020). LD2FA-PSO: A novel learning dynamic deterministic finite automata with PSO algorithm for secured energy efficient routing in wireless sensor network. *Ad Hoc Networks*, 97, 102024.

Shahbaz, A.N., Barati, H. &Barati, A. (2021). Multipath routing through the firefly algorithm and fuzzy logic in wireless sensor networks. *Peer-to-Peer Networking and Applications*, 14(2), 541-558.

Shishehgarkhaneh, M.B., Azizi, M., Basiri, M. &Moehler, R.C. 2022. BIM-based resource tradeoff in project scheduling using fire hawk optimizer (FHO). *Buildings*, 12(9), 1472.

Soundari, A.G., &Jyothi, V.L. (2020). Energy efficient machine learning technique for smart data collection in wireless sensor networks. *Circuits, Systems, and Signal Processing*, 39, 1089-1122.

Sridhar, M., &Pankajavalli, P.B. (2020). An optimization of distributed Voronoi-based collaboration for energy-efficient geographic routing in wireless sensor networks. *Cluster Computing*, 23(3), 1741-1754.

Suresh Kumar, K. &Vimala, P. (2021). Energy efficient routing protocol using exponentially-ant lion whale optimization algorithm in wireless sensor networks. *Computer Networks*, 197, 108250.

RahkarFarshi, T. (2021). Battle royale optimization algorithm. *Neural Computing and Applications*, 33(4), 1139-1157.

Vashisht, S. & Jain, S. (2019). An energy-efficient and location-aware medium access control for quality-of-service enhancement in unmanned aerial vehicular networks. *Computers & Electrical Engineering*, 75, 202-217.