Energy Conservation Model for Wireless Sensor Network

A THESIS
SUBMITTED TO THE DELHI TECHNOLOGICAL UNIVERSITY
FOR THE AWARD OF THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

Computer Science & Engineering

Submitted by
Ms. Rashmi Mishra
(Roll No-2K18/PHDCO/506)

Under the guidance of

Dr. Rajesh Kumar Yadav
Assistant Professor
Department of Computer Science and Engineering
Delhi Technological University

DEPARMENT OF COMPUTER SCIENCE AND ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY,

(Formerly Delhi College of Engineering)

BAWANA ROAD, DELHI-110042

DELHI TECHNOLOGICAL UNIVERSITY

(Govt. of National Capital Territory of Delhi)
Bawana Road, Delhi – 110042

CERTIFICATE

This is to certify that the thesis entitled "**ENERGY CONSERVATION MODEL FOR WIRELESS SENSOR NETWORKS**" being submitted by Rashmi Mishra (Reg. No.: 2K18/PhD/CO/506) for the award of degree of Doctor of Philosophy to the Delhi Technological University is based on the original research work carried out by her. She has worked under my supervision and has fulfilled the requirements which to my knowledge have reached the requisite standard for the submission of this thesis. It is further certified that the work embodied in this thesis has neither partially nor fully submitted to any other university or institution for the award of any degree or diploma.

Dr. Rajesh Kumar Yadav
(Supervisor)
Assistant Professor,
Department of CSE,
DTU-Delhi, India

ACKNOWLEDGEMENTS

I want to express my sincere gratitude to **Dr. Rajesh Kumar Yadav**, Assistant Professor, Department of Computer Science and Engineering, Delhi Technological University, Delhi, for providing valuable guidance and constant encouragement throughout the work. His immense knowledge, motivation, expertise, and insightful comments have helped me immensely at every stage of the preparation of this research plan.

I would also like to extend my heartfelt thanks to the **DRC Chairperson Prof. Dr. Rajni Jindal and HOD Prof. Dr. Vinod Kumar** for their valuable insights, suggestions, and critical evaluation of my research work. Their expertise and scholarly advice have played a crucial role in improving the quality of this thesis.

I would like to sincerely thank the esteemed members of the Department of Computer Science & Engineering at Delhi Technological University. I would like to express my gratitude to my colleagues and friends Dr. Amrita Jyoti, Ms. Pooja Saharan, Mr. Shashank Shekhar, Dr. Manish Saraswat who have provided valuable support and encouragement during this challenging journey. Their intellectual discussions, constructive feedback, and camaraderie have enriched my research experience and made it more enjoyable.

Above all, my heartfelt thanks go to my parents (Mr. K.K Pandey and Mrs. Shobha Pandey), my In-laws, my husband (Mr. Sushil Kumar Mishra), my son (Mr. Lakshya Mishra), my sister (Dr. Divya Pandey, Richa Tiwari Pandey), my brother (Col. Vinay Pandey, Dr. Vipin Pandey).

I know I would not finish the Ph.D. without their non-stopping love, encouragement, and support. Completing this PhD thesis would not have been possible without the collective support and contributions of all these individuals. Although it is not possible to mention everyone by name, I sincerely appreciate and acknowledge the efforts of each and every person who has played a role in this journey.

Rashmi Mishra (2K18/PHDCO/506)

RESEARCH PUBLICATIONS

Papers Published in International Journals

1. Mishra, R., & Yadav, R. K. (2023). Energy Efficient Cluster-Based Routing Protocol for WSN Using Nature Inspired Algorithm. ***Wireless Personal Communications***, *130*(4), 2407-2440. **(SCIE-2.017)**
2. Yadav, R.K., Mishra, R. Cluster-Based Classical Routing Protocols and Authentication Algorithms in WSN: A Survey Based on Procedures and Methods. ***Wireless Personal Communication*** 123, 2777–2833 (2022). https://doi.org/10.1007/s11277-021-09265-7. **(SCIE-2.017)**
3. Yadav, R.K., Mishra, R. (2021). Optimized Energy Conservation Procedure for Heterogeneous Wireless Sensor Network, *Journal of Engg. Research* ICCEMME Special Issue, DOI: https://doi.org/10.36909/jer.ICCEMME.15625. **(SCIE-0.5)**
4. Yadav, R.K., & Mishra, R. (2020). An Authenticated Enrolment Scheme of Nodes using Blockchain and Prevention of Collaborative Blackhole Attack in WSN. 10.56042/jsir.v79i9.41773 ***Journal of Scientific & Industrial Research*****. (SCIE- 0.9).**

Papers Published in International Conferences

5. Yadav, R.K., Mishra, R. (2021). Analysis of DEEC Deviations in Heterogeneous WSNs: A Survey. In: Bhateja, V., Satapathy, S.C., Travieso-Gonzalez, C.M., Flores-Fuentes, W. (eds) *Computer Communication, Networking and IoT. Lecture Notes in Networks and Systems*, vol 197. Springer, Singapore. https://doi.org/10.1007/978-981-16-0980-0_22.
6. Mishra, R., & Yadav, R. K. (2023). Energy Conservation Methods using Butterfly Optimization Algorithm: A Survey. **(Accepted and Presented in International Conference on Advanced Emerging Trends in Engineering & Pharmaceutical Science).**

ABSTRACT

Wireless sensor networks (WSNs) have drawn more and more interest in recent years from both the research community and end users. Since sensor nodes are typically battery-operated devices, it is crucial to figure out how to lower their energy consumption so that the network lifetime can be increased to a respectable amount of time. A routing protocol must not only convey data to the base station but also be energy-efficient. Hierarchical routing based on clustering is an effective routing method. The energy consumption of the various parts of a typical sensor node is first broken down in this paper, and the key approaches to energy conservation in WSNs are discussed. A survey of the energy-saving plans that have lately been put forth in the literature will also be done. Promising solutions that have not yet received much attention in the literature, such as methods for authenticating the nodes for energy-efficient, will receive special consideration. The key contribution will involve analyzing the simulation's leading schemes' performance and changing an effective scheme to make it even more effective. This thesis examines wireless sensor networks employing mobile base stations and proposes the mechanism to lower down the energy consumption. The minimal distance is determined after grouping the nodes and choosing the cluster heads to impose the lowest energy cost on the data connection. Results from simulations are given to demonstrate the effectiveness of this method. The outcomes are compared to the various algorithms present in the literature.

According to the research, most issues are concerned with conserving the network's energy while taking a few specific characteristics into account. A grouping of algorithm is required for saving power conservation, and it also intensifies the network's epoch time and firmness epoch. Like this, despite the network's power not always being depleted by the great range between source and destination. It might have happened as a result of a rogue network setting.

In this thesis, we suggest new ways to save energy in wireless sensor networks in order to make them last longer. We start by looking at existing methods that have been developed to make networks more energy-efficient. These methods are used in different types of networks and involve blockchain and optimization algorithms. Then, we propose three new solutions:

The first solution aims to increase the network's lifespan by saving energy in the sensor nodes. We do this by selecting an optimal number of cluster heads and ensuring network stability. Next, we introduce a new energy-efficient design that optimizes the lifespan of both the sensor nodes and the base station. This design considers the different types of devices in the network. The third solution focuses on authenticating the nodes in the network to maximize its lifespan. We exclude any malicious nodes that could negatively impact the network's operation. Lastly, we develop an energy-efficient clustering and routing mechanism for wireless sensor networks. This mechanism considers factors such as residual energy, distance, and the number of nodes in each cluster. We use a nature-inspired algorithm to optimize the network's performance and lifespan. The strategies we proposed have successfully extended the lifetime of the sensor networks, as demonstrated by our results. These results are backed by numerical experiments and extensive simulations.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	**Explanation**
WSN	Wireless Sensor Network
IoT	Internet of Things
AODV	Ad hoc On-Demand Distance Vector
LEACH	Low-Energy Adaptive Clustering Hierarchy
BER	Bit Error Rate
CBR	Constant Bit Rate
CH	Cluster Head
CN	Cluster Node
CHS	Cluster Head Selection
CF	Cluster Formation
CDC	Cluster Discovery and Configuration
BS	Base Station (Sink or Gateway)
RDC	Region-based Data Clustering
CHC	Cluster Head Candidate
TLC	Two-Level Clustering
PCHS	Probabilistic Cluster Head Selection
HCHS	Hybrid Cluster Head Selection
FCM	Fuzzy C-Means
SEP	Stable Election Protocol
TEEN	Threshold-sensitive Energy Efficient sensor Network protocol
DEEC	Distributed Energy-Efficient Clustering
HEED	Hybrid Energy-Efficient Distributed Clustering
EEDC	Energy Efficient Distributed Clustering
HEER	Hybrid Energy Efficient Routing
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance

TDMA	Time Division Multiple Access
DSR	Dynamic Source Routing
PDR	Packet Delivery Ratio
QoS	Quality of Service
ACK	Acknowledgment
PRR	Packet Reception Rate
FSR	Flooding Source Routing
E	Energy variable
r	Current round
R	Total rounds in network lifetime
N	Total number of nodes in the network
E_total	Total energy available
E_round	Energy consumed per round
L	Constant coefficient
E_elec	Energy required per bit for transmission/reception
E_DA	Energy required for data aggregation
k	Optimization factor
E_amp	Energy required for amplification
d_toBS	Distance from a node to the Base Station
d_toCH	Distance from a node to the Cluster Head
E_fs	Energy required per bit for free space transmission/reception
N_ml	Number of nodes in the multilevel group
T_absolute	Absolute threshold energy
p_i	Probability of selecting a node for transmission
G	Set of eligible nodes for transmission
p_opt	Optimal probability
E_i(r)	Residual energy of a node in round r
a, b	Constants for calculation

m, m_o	Constants for calculation
Th_ab	Threshold value
z	Constant coefficient
E_0	Energy variable
a	Constant coefficient
E_disNN	Energy variable for non-neighbor nodes
E_disAN	Energy variable for adjacent neighbor nodes
DLT	Distributed Ledger Technology
PoW	Proof of Work
PoS	Proof of Stake
PoA	Proof of Authority
DAG	Directed Acyclic Graph
Consensus	Consensus Mechanism
Smart Contracts	Self-executing Contracts
Block	Data structure containing transactions
BOA	Butterfly Optimization Algorithm
PSO	Particle Swarm Optimization
ACO	Ant Colony Optimization

CHAPTER-1

INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as a significant technological advancement in data acquisition and monitoring. These networks comprise small, cost-effective devices known as sensor nodes, capable of wirelessly sensing, processing, and transmitting data. WSNs have gained immense attention due to their diverse applications across various domains, including environmental monitoring, healthcare, and industrial automation. Environmental monitoring is one domain where WSNs have made a substantial impact. Through the deployment of sensor nodes in remote or inaccessible locations, WSNs enable real-time monitoring of crucial environmental parameters like temperature, humidity, air quality, and pollution levels. This data plays a crucial role in understanding and addressing the effects of climate change, assessing ecosystem health, and managing natural resources more efficiently (Heinzelman, W.,2002).

In the healthcare sector, WSNs have revolutionized patient monitoring and care. Sensor nodes integrated into wearable devices continuously monitor vital signs such as heart rate, blood pressure, and oxygen levels, allowing healthcare professionals to remotely track patients' health conditions. WSNs have also facilitated the development of ambient assisted living systems, which enhance the quality of life for elderly or disabled individuals by providing assistance and monitoring their well-being.

WSNs have found extensive applications in industrial automation as well. By deploying sensor nodes in factories or manufacturing plants, WSNs enable real-time monitoring of various parameters such as temperature, pressure, vibration, and energy consumption. This data is utilized for condition monitoring, predictive maintenance, and optimizing production processes. WSNs have significantly contributed to improving efficiency, reducing downtime, and enhancing overall productivity in industrial settings (Wang, Z.,2022).

In addition to the domains mentioned, WSNs have found applications in agriculture, transportation, smart cities, disaster management, and numerous other fields. The ability of sensor nodes to collect data from the physical environment, coupled with their wireless communication capabilities, makes WSNs invaluable for real-time monitoring, control, and decision-making processes. However, deploying and managing WSNs present several challenges. These networks often face limitations such as limited energy resources, bandwidth constraints, and dynamic network topologies. To address these challenges and enhance the efficiency and reliability of WSNs, researchers and engineers are continuously exploring innovative techniques and algorithms.

In conclusion, wireless sensor networks have become an indispensable technology across various domains, offering real-time data acquisition, monitoring, and control capabilities. Their applications in environmental monitoring, healthcare, industrial automation, and other fields have transformed the way we perceive and interact with the world. With ongoing advancements, WSNs hold the potential to revolutionize several other areas, making them a key focus of research and development in the field of wireless communication and sensing (Dawood, M. S.,2021).

Wireless Sensor Networks (WSNs) are networks of inadequate, powered by batteries sensors used mainly for monitoring. The invention of such sensors from improvisation has become feasible because of advances in micro-electromechanical systems (MEMS) technologies (Wang, Z.,2022). WSNs have recently been the focus of extensive study by an array of groups and the military, and some of their uses can be identified as battlefield observation. Considering the current climate change issues, WSNs can be used to track climate change by utilizing a network of sensors that gather environmental information such as temperature, humidity, and altitude. These sensors offer an array of advantages, notably the ability to work unattended, making them ideal for difficult-to-reach zones (Behera, T. M,2019).

The network of wireless sensors (WSN) is unique among the advantageous innovations of the past few years. It consists of base stations with specific levels of energy in addition to dozens of tiny sensors known as normal sensor nodes and progressing sensor nodes, both of which will play a role in the choice of the head of the cluster. According to applications and available power, these nodes with sensors are positioned in a distributed manner (Wang, Z., et al, 2022). The sensor nodes collect information about the environment, integrate it in the head of the cluster, and transmit it to the ground station.

Due to the physical constraints associated with the WSN, like the amount of power used by the sensor nodes in order to gather the information, several industries nowadays, such as agriculture, medicine, rural regions, etc., face many obstacles. Therefore, a sensor on the nodes must stay alert for an extended amount of time to function in the context of the network. To reduce the impact of humans and the environment's operations, supervisory nodes must constantly track streams and immediate information (Behera, T. M., 2019). Several researchers have put forward methods for regulating the network's lifespan when taking into factors like the choice of the head of the cluster, the amount number alive and dead node in the network, the packet delivery ratio, etc. The clustering approach works very well to boost system efficiency and give system flexibility. Many methods for clustering for both heterogeneous as well as homogeneous systems were proposed by researchers in the research which is currently accessible. The diverse network is essential for expanding the lifespan of the system as it requires fewer resources for communication but more energy for each node to select the right cluster head, thereby having a bearing on the running of the process in question. According to the amount of energy left, the number of nodes stills living, and the first node to die, the author of the research has examined the algorithms (Dawood, M. S., 2021).

The in-network processing needed by the collection of data, data fusion, calculating, and transfer operations require that these devices use energy effectively for the purpose extend the effective lifespan of the network, even though WSNs have grown able to handling some of these complex responsibilities. Various techniques for clustering and techniques like

LEACH (Heinzelman, W. B.,2002), have been proposed and recommended with an assortment of aims in consideration, namely distributing the load, tolerating faults, enhanced a connection and reduced latency as well, and lifespan of the network. A tighter protocol might be generated through balancing the previous objectives. The LEACH protocol (Low-Energy Adaptive Clustering Hierarchy) along with comparable protocols assume a near-perfect system, an energy homogeneity system where a node has a chance to experience failure because of terrain variations, difficulties with connectivity, or message skipping.

Nevertheless, contemporary protocols, like SEP (Al-Rubaie, A.,2015), take account of the other direction, specifically frequency variability, where previously mentioned parts are a possibility, so this is closer to the real-world scenario for WSN. Therefore, when designing an effective protocol for WSN, resource variance should be among the primary considerations. The current investigation analyses the prior study that has already been carried out in this area of study. The goal is to present a revamped protocol architecture that remains more stable and will ensure an extended network existence while taking additional efficiency variables into consideration. Simulations using computers and mathematical modeling are used to show the practicality of the suggested internet configuration. A better procedure can be created by considering the objectives mentioned earlier.

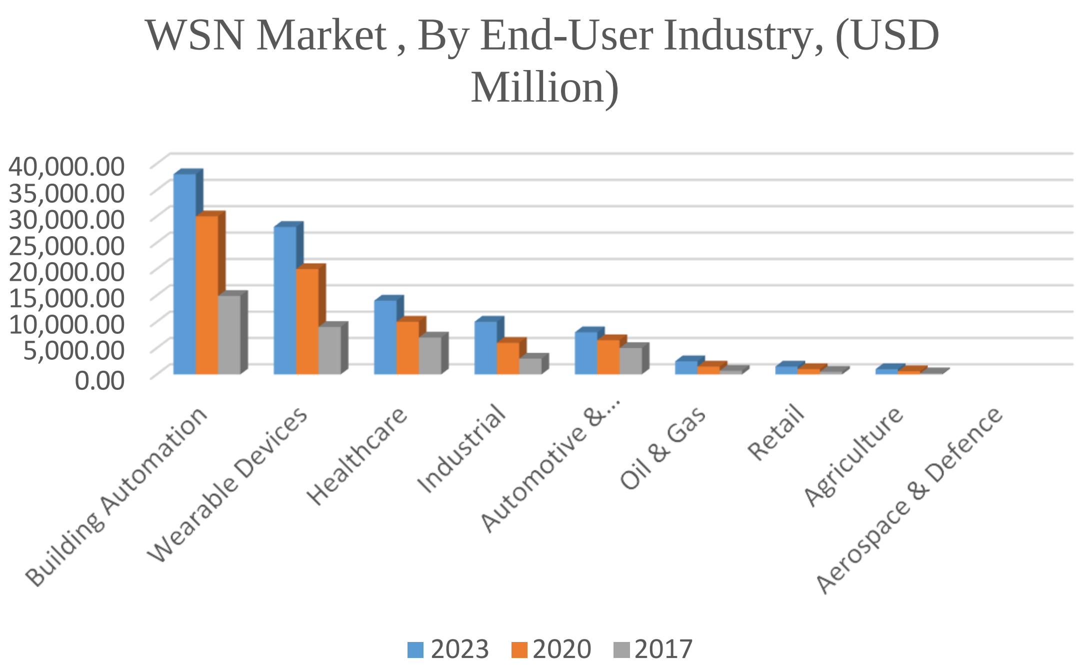


Fig 1.1: WSN in various applications

1.1 Parameters used in WSN

Delay: The delay is the amount of time it takes for the packet to spread from the washbasin to the foundation. If the delay is small, the link is less congested. The actual expectancy or delay will be closely evaluated by the delay.

Scalability: Scalability in a WSN is defined as the ability of the routing protocol to accommodate a rise in the number of contemporary sensor nodes in the network. Because the WSN will have thousands of nodes that are interconnected. A single point of failure will impair the operation of the entire network (Mehta, D., & Saxena,2022).

Energy-efficiency: Routing protocols' main objective is to reduce power consumption for sensor nodes. Most heterogeneous routing algorithms are created to lower sensor node power consumption and increase network longevity.

Network size: The routing protocols' definition makes sure they will work in both small and large networks. Networks are designed to be dependable and last for a longer period.

Clustering: Lengthening system lifetime is the main goal of cluster formation. The cluster separates the entire WSN system into small pieces or small virtual groups according to some predetermined rules and procedures. There are two categories of sensor nodes in this: cluster heads and cluster members. Power level, sink node replacement, cluster head, and other geographical parameters are considered when selecting a cluster head (Xie, B.,2017; Yi, D.,2016). Cluster heads collect and integrate data from numerous sensor nodes before sending it all in one packet to the sink node in order to save overhead. By lowering network overhead and enhancing bandwidth usage, cluster construction will have the advantage of minimizing inefficient power use. A great deal of protocols has been made accessible to the public for prolonging system life span by distributing the work among sensor nodes and balancing energy use by choosing the head of the cluster to closest nodes capable of send and receive a great deal of nodes (Luo, J,2014).

1.2 Design Constraints

Wireless Sensor System routing protocols need to meet specific standards due to limitations within the system. These standards include:

Autonomy: Wireless sensor networks (WSNs) operate in a decentralized manner without a centralized organization making routing decisions. This lack of well-defined routing procedures makes WSNs vulnerable to potential attacks.

Energy Efficiency: Routing protocols should be designed to maximize the system's lifespan and maintain efficient communication between nodes (Srividhya, V., 2018). As sensor nodes are often placed in inaccessible locations, it becomes challenging to replace their batteries.

Scalability: With WSNs consisting of hundreds of nodes, routing protocols must effectively handle the large number of nodes within the system.

Resilience: Routing protocols need to establish alternative paths for data transmission in case certain nodes become non-functional due to factors like external influences or battery depletion.

Device Heterogeneity: The diversity of sensor nodes in terms of processing power, transceivers, power units, and bandwidth allows for different routing strategies suitable for WSNs.

Mobility Adaptability: Wireless sensor systems face the challenge of node mobility, as some applications require nodes to accommodate movement. Routing protocols should incorporate provisions to handle such mobility requirements.

Complexity: Due to hardware limitations and power constraints, routing strategies should strike a balance between functionality and system performance to avoid excessive complexity that could hinder the wireless system's performance.

1.3 Heterogeneity in WSN

Heterogeneous Wireless Sensor Networks (WSNs) pose significant challenges due to the deployment of sensors with varying capabilities and characteristics within the network. These differences in sensor capabilities can range from variations in sensing range and accuracy to differences in processing power and energy resources. Managing such heterogeneity requires efficient data processing and management techniques that can effectively handle the diverse data generated by these sensors.

One major challenge is the development of algorithms and protocols that can handle the varying data formats and transmission capabilities of heterogeneous sensors. Efficient data fusion techniques are required to aggregate and process data from different sensors, ensuring accurate and meaningful information extraction. Another challenge lies in the design of energy-efficient strategies to optimize the resource utilization of different sensor nodes. Since energy resources can vary across heterogeneous sensors, balancing energy consumption becomes crucial to extend the network's overall lifetime.

Furthermore, the heterogeneity in communication protocols and data formats used by different sensors can create interoperability challenges. Standardization efforts and protocols that enable seamless communication and data exchange between heterogeneous sensors are essential to ensure smooth network operations. Security and privacy concerns also emerge in heterogeneous WSNs. With sensors having varied levels of security capabilities, developing robust authentication and encryption mechanisms becomes crucial to protect sensitive data and prevent unauthorized access.

Additionally, managing the deployment and maintenance of heterogeneous sensor nodes across large-scale networks can be complex. Coordination and configuration of different sensors, as well as the optimization of network topology, become challenging tasks to ensure efficient data collection and transmission. To overcome these challenges, researchers and practitioners are focusing on developing intelligent algorithms, machine learning techniques, and adaptive protocols that can adapt to the heterogeneity of WSNs. These approaches aim to enhance data processing, energy efficiency, security, and network management in order to fully exploit the potential of heterogeneous WSNs in various applications (Fig 1.1).

In terms of heterogeneous resources in WSNs, three main categories can be identified: energy, link, and cognitive (Pachlor, R., 2018). Energy heterogeneity is characterized by different energy levels among nodes, including two-level, three-level, or multi-level configurations. Routing methods optimize network performance by assigning power-intensive tasks to high-energy sensors. Link heterogeneity allows for diverse forms of interaction between sensor nodes, such as bidirectional or unidirectional communication (Sharma, D., 2019). Several techniques leverage link heterogeneity to improve network lifespan and reduce delays. Cognitive heterogeneity considers the varying hardware capabilities of sensor nodes to handle more complex tasks, while accounting for traffic diversity (Xie, B.,2017; Castiglione, A.,2015).

1.3.1 Types of Node Heterogeneity of HWSN

Node heterogeneity plays a role in determining the throughput and latency of data transmission from source to destination. Cluster-based heterogeneous algorithms can be classified using various parameters. In a heterogeneous environment, there are fewer hops between the source and destination, resulting in a higher end-to-end delivery rate compared to a homogeneous environment (Yi, D., 2016; Luo, J.,2014). Figure 1.2 provides an overview of node heterogeneity in WSNs. Dealing with node heterogeneity in WSNs requires designing appropriate protocols, algorithms, and strategies that account for the varying capabilities and characteristics of different nodes. Efficient resource management, adaptive routing, and task allocation techniques are essential for leveraging the benefits of node heterogeneity and maximizing the network's overall performance. In the context of HWSN (Heterogeneous Wireless Sensor Networks), node heterogeneity refers to the existence of different types of sensor nodes within the network. These sensor nodes vary in terms of their capabilities, functionalities, and characteristics. Node heterogeneity in HWSNs is often introduced to address various application-specific requirements and optimize the overall performance of the network. Here are some common types of node heterogeneity in HWSNs in Fig 1.2.

By incorporating various types of heterogeneous nodes in a HWSN, designers can optimize the network for specific application requirements, energy efficiency, scalability, and reliability. However, it also introduces challenges in terms of routing, data aggregation, and resource management to efficiently utilize the diverse capabilities of the nodes.

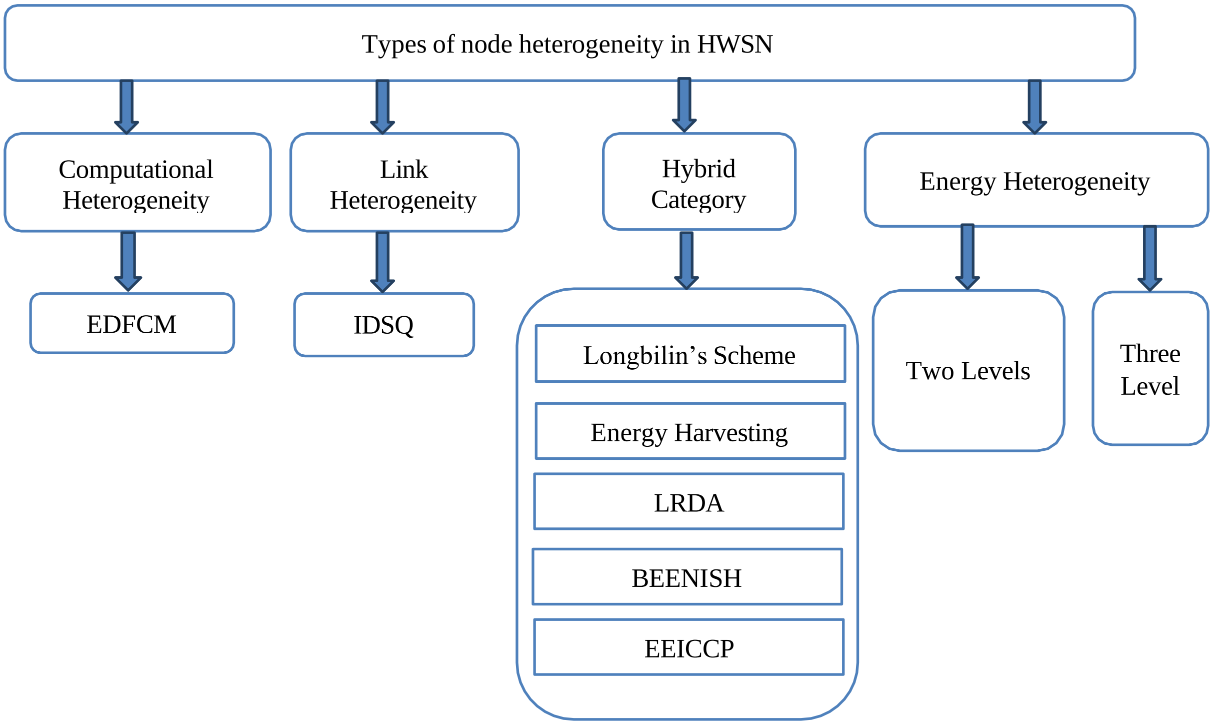


Fig 1.2: Taxonomy of various types of node heterogeneity in HWSN

1.4 Clustering in WSN

In heterogeneous Wireless Sensor Networks (WSNs), clustering serves as an effective solution for managing and organizing the network. Clustering involves dividing the network into smaller groups or clusters, where nodes within each cluster exhibit similar characteristics or functionalities (Mehta, D.,2020). The goal of clustering is to facilitate efficient data processing, reduce energy consumption, and enhance network scalability. By clustering nodes with similar capabilities, tasks can be allocated more effectively within each cluster, optimizing resource utilization (Javaid, N.,2013). Clustering allows for the establishment of cluster heads or coordinators, which are responsible for intra-cluster communication and data aggregation. These cluster heads play a vital role in reducing energy consumption by performing localized data processing and transmitting aggregated data to the base station or higher-level nodes. The process of clustering involves various factors such as node proximity, energy levels, communication patterns, and data requirements. Nodes with similar attributes are grouped together, promoting localized communication, and minimizing long-distance transmissions, thereby conserving energy (Xie, B.,2017).

Clustering in HWSNs enables better management of network resources, improves data aggregation efficiency, and enhances network scalability. It promotes efficient utilization of energy resources and prolongs the network's overall lifetime. Through the clustering approach, HWSNs can achieve optimized performance, adaptability, and reliability, catering to the diverse requirements of different sensor nodes within the network. It has been observed that the performance of the Wireless Sensor Network (WSN) can be improved by forming a cluster head. It demonstrates that sensor nodes consume more energy when a proper cluster head selection algorithm is not employed. However, if WSN incorporates an appropriate algorithm for cluster head selection, it results in energy savings (Sharma, D.,2019; Engmann, F.,2018).

Choosing the cluster head enhances network capacity by effectively redistributing resources and extends the system's lifespan. Cluster heads play a crucial role in inter-cluster routing and communication, acting as virtual hubs between different cluster heads (Qiu, J.,2020). Routing within the network improves the overall performance of the WSN. However, forming clusters can be challenging depending on the network architecture, such as ad hoc or cellular networks (Ravidas, S.,2019; Xu, C.,2019). Due to the large number of sensor nodes, it becomes impractical to determine their locations and establish data connectivity. In ad hoc networks, which are self-deployed in nature, nodes must establish connections with other sensor nodes (HaddadPajouh, H.,2021; Sheik Dawood, M.,2020).

1.5 Blockchain used in wireless sensor networks

Node authentication plays a crucial role in Wireless Sensor Networks (WSNs) to ensure the integrity and security of the collected data. It verifies the identity of sensor nodes and prevents unauthorized access, data tampering, and malicious attacks. To address these challenges, blockchain technology has emerged as a promising solution for node authentication in WSNs. Blockchain is a decentralized and tamper-resistant distributed ledger that records transactions in a transparent and secure manner. It provides a robust mechanism for verifying the identity of WSN nodes. Blockchain technology utilizes cryptographic algorithms to generate a unique digital signature for each sensor node (Cui, Z.,2020). This signature is stored in a decentralized network of nodes, ensuring the integrity and immutability of the authentication information. When a sensor node attempts to join the network or transmit data, it presents its digital signature to the blockchain network for verification. The distributed consensus mechanism of blockchain ensures that the identity is validated by multiple nodes, making it highly secure and resistant to malicious attacks. By leveraging blockchain technology, WSNs can achieve a secure and transparent authentication process. The decentralized nature of the blockchain network eliminates the need for a centralized authority, reducing vulnerabilities and enhancing resilience against single points of failure (Hammi, M. T.,2018).

Node authentication is a critical aspect of ensuring the integrity and security of data collected by sensor nodes in Wireless Sensor Networks (WSNs). Researchers have explored various techniques and technologies to address the challenges associated with node authentication in WSNs. Among these, blockchain technology has emerged as a promising solution due to its decentralized and tamper-resistant nature (Lazrag, H.,2021).

In a study conducted by (Cui, Z.,2020) the authors proposed a blockchain-based authentication mechanism for WSNs. They highlighted the importance of secure node authentication and introduced blockchain as a solution to mitigate security risks. The proposed mechanism utilized a distributed ledger to store and verify the identity of sensor nodes, ensuring data integrity and preventing unauthorized access.

Another research by Wang et al. focused on enhancing the security of WSNs through blockchain-based node authentication. They discussed the vulnerabilities of traditional authentication methods and presented a decentralized blockchain framework. The framework utilized smart contracts to validate the identity of sensor nodes, providing a robust and tamper-resistant authentication mechanism (Wang et al., 2018).

In a different approach, Yang et al. proposed a hybrid authentication scheme combining blockchain technology and lightweight cryptographic algorithms. The authors addressed the resource constraints of sensor nodes by employing lightweight cryptographic techniques for initial authentication, while leveraging blockchain for decentralized verification. The hybrid scheme offered a balance between security and efficiency in WSNs (Yang et al., 2020).

Furthermore, the work of Zhang et al. explored the application of blockchain technology for secure and transparent node authentication in industrial WSNs. The authors emphasized the need for a tamper-resistant authentication mechanism to protect critical infrastructure and sensitive data. They presented a blockchain-based framework that verified the identity of sensor nodes and recorded authentication transactions in a transparent and immutable manner (Zhang et al, 2020).

Overall, the literature survey demonstrates a growing interest in utilizing blockchain technology for node authentication in WSNs. Researchers have recognized the importance of securing data integrity and mitigating security risks in WSNs. Blockchain's decentralized and tamper-resistant nature offers a promising solution to address these challenges and provide a secure mechanism for verifying the identity of WSN nodes.

Furthermore, the transparency of blockchain allows for auditability and accountability in WSNs. Any changes or unauthorized access attempts are recorded in the blockchain, providing an immutable audit trail for forensic analysis.

Overall, blockchain technology offers a robust and tamper-resistant solution for node authentication in WSNs. Its decentralized nature, cryptographic algorithms, and transparent ledger make it an ideal choice for ensuring the integrity and security of the data collected by sensor nodes. There are a lot of different authentication mechanisms in the literature. The majority of traditional WSN security authentication techniques use centralized authentication methods. In centralized authentication mechanisms, a trusted third party, such as a government agency, authentication server, certificate authorization center, etc., is involved in the authentication of the nodes (Hou, J,2019). As a result, there is a single point of failure, or if one node is compromised, the entire system is compromised. One of the well-known decentralized distributed technologies, blockchain offers a fresh approach to security issues.

1.5.1 Types of Blockchain

In the current context, researchers have introduced various types of blockchains. These include Public Blockchain, Private Blockchain, Permissionless Blockchain, Consortium Blockchain, and Permissioned Blockchain (Crosby, M.,2016; Smith, J.,2020).

Public Blockchain: In a public blockchain, all contracts are publicly accessible. Members of the blockchain can modify, delete, add, and edit data, while anyone can review or audit the data. However, to maintain node authenticity and network security, unauthorized individuals are restricted from modifying the content in the database. Therefore, public blockchains are not suitable for applications where node authentication and network integrity are crucial. This type of blockchain is better suited for applications focused on resource sharing. It is worth noting that public blockchains like Bitcoin and Litecoin can consume substantial energy and incur costs for miners, which can lead to a lack of trust and susceptibility to tampering (Smith, J.,2020).

Private Blockchain: Unlike public blockchains, private blockchains have distinct characteristics. Data in a private blockchain cannot be easily modified or deleted by anyone. Only users with the appropriate rights can perform such actions. Additionally, in a private blockchain, no one can add, modify, alter, delete, review, or audit the data without authorization. Despite these differences, there are similarities between public and private blockchains. Both are decentralized and operate on a peer-to-peer basis (Guo, H.,2022). Each node maintains a replica of the ledger and receives updates through consensus, ensuring immutability at different levels.

The differences between Permissionless, Consortium, and Permissioned Blockchain are discussed in Table 1.1, providing a clear distinction between these blockchain types (Lopez-Barreiro, J.,2022).

Table 1.1: Types of blockchain technology

Permissionless Blockchain	**Consortium**	**Permissioned Blockchain**
All the participating knobs in the network have permission to read and write the data.	Only Selective authority or Consortium members have permission to read and write the data	Selective Authority or Specific Members or All participating knobs have permission to read and write the data.
Open access to the network and consensus.	Only Consortium member can have permission to Read the Data.	Limiting access to the system and consensus
Complex consensus algorithms	Light consensus algorithms	Light consensus algorithms

Less contract bit rate	Huge contract bit rate	Very Huge contract bit rate
Scalable consensus	Consensus with restricted expandable	Consensus with restricted expandable
All the knobs who are participating in the contract have permission to create a block.	All the Consortium Members have permission to create a block.	Only Operator have permission to create a block.
Incentive mechanism	Incentive mechanism for miners	No need of incentive mechanism
Network Delay is very huge	Network Delay is Less	Network Delay is very Less.

1.6 Nature Inspired Algorithms in WSN

Energy conservation plays a significant role in Wireless Sensor Networks (WSNs) due to the limited power resources of the sensor nodes. Efficient techniques are necessary to optimize energy consumption and prolong the network's operational lifetime. One approach to achieving this is through the utilization of nature-inspired algorithms, which draw inspiration from natural phenomena to find energy-efficient solutions.

The Butterfly Optimization Algorithm (BOA) is an example of a nature-inspired algorithm that mimics the behavior of butterflies to conserve energy in WSNs. By observing the energy-efficient flight patterns of butterflies, BOA optimizes the movement of sensor nodes to minimize energy consumption. It achieves this by dynamically adjusting the position and movement of nodes, optimizing their communication range and reducing unnecessary energy expenditure.

Clustering is an effective technique in WSNs for organizing nodes and optimizing energy consumption. The Particle Swarm Optimization (PSO) algorithm is utilized to form clusters in WSNs. PSO mimics the behavior of a swarm of particles, where each particle represents a potential cluster head. The algorithm iteratively adjusts the position and velocity of particles based on local and global information, aiming to find the optimal cluster heads and cluster formation. By efficiently organizing nodes into clusters, PSO helps to minimize energy consumption by enabling localized data processing and reducing long-distance transmissions.

Efficient routing mechanisms are crucial in WSNs to facilitate data transmission between sensor nodes. One nature-inspired algorithm used for routing optimization is Ant Colony Optimization (ACO). ACO models the foraging behavior of ants, where ants leave pheromone trails to mark the paths to food sources. In the context of WSNs, ACO utilizes virtual ants to find optimal paths for data routing. The pheromone trail strength guides the selection of routes with better transmission conditions, resulting in improved energy efficiency and reduced data transmission delays.

By incorporating nature-inspired algorithms like BOA, PSO, and ACO, energy conservation, cluster formation, and efficient routing can be achieved in WSNs. These algorithms provide intelligent and adaptive solutions inspired by natural phenomena, optimizing energy consumption, organizing nodes effectively, and improving data transmission efficiency. As a result, the overall performance and longevity of WSNs are enhanced, making them suitable for various applications in fields such as environmental monitoring, healthcare, and industrial automation.

The significance of energy conservation in Wireless Sensor Networks (WSNs) has been widely recognized due to the limited power resources of sensor nodes. Researchers have explored various techniques, including nature-inspired algorithms, to optimize energy consumption in WSNs. The literature provides valuable insights into the development and application of these algorithms for energy-efficient WSNs.

One such algorithm, the Butterfly Optimization Algorithm (BOA), has gained attention for its ability to conserve energy in WSNs. In a study by Qi, H. et al, the authors introduced BOA as a nature-inspired algorithm that mimics the energy-efficient flight patterns of butterflies. The algorithm dynamically adjusts the movement of sensor nodes to minimize energy consumption, resulting in improved network efficiency and prolonged network lifetime (Qi, H., 2019).

Clustering is an effective technique for energy optimization in WSNs, and the Particle Swarm Optimization (PSO) algorithm has been extensively studied for this purpose. In their research, Shi et al. discussed the concept of forming clusters in WSNs using the PSO algorithm. They highlighted how PSO optimizes the clustering process by iteratively adjusting the position and velocity of particles, ultimately finding the optimal cluster heads and cluster formation. The study demonstrated that PSO-based clustering improves energy efficiency by enabling localized data processing and reducing long-distance transmissions.

Efficient routing mechanisms are vital for effective data transmission in WSNs. Ant Colony Optimization (ACO) has emerged as a nature-inspired algorithm for optimizing routing in WSNs. In a study by Dorigo et al., the authors introduced ACO as an algorithm inspired by the foraging behavior of ants. They described how ACO models the pheromone trail marking of ants to find optimal paths for data routing in WSNs. The research showcased the effectiveness of ACO in improving energy efficiency and reducing transmission delays in WSNs. (Dorigo et al., 2006)

The literature survey highlights the importance of energy conservation in WSNs and the utilization of nature-inspired algorithms for optimization. Studies on the Butterfly Optimization Algorithm (BOA) emphasize its ability to mimic energy-efficient behaviors in butterflies, while research on Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO) demonstrate their effectiveness in clustering and routing optimization for energy efficiency in WSNs.

1.7 Problem Definition and Motivation

The wireless sensor's life is dependent upon the battery that it uses for powering it, which consequently additionally varies on the amount of power it consumes. The distance that exists between the sender (the cluster head) and the reserve (the base station) constitutes just one of numerous variables that affect this. The malicious node inside the network would affect the lifetime of the network. Once the initial sensor's charge runs out in the wireless sensor network, the sensor is considered dead. The wireless network's sensors are not all expiring simultaneously. Consequently, a network or cells will grow imbalanced after the initial one goes off. If a network keeps running under this scenario, gathering, exploiting, and delivering information to the starting location, the total information will be inadequate. Consequently, some of the information disappears if the deceased sensor(s) cannot deliver any data. Yet, the sensor nodes consume a great deal of power when connecting wirelessly to the sink. The heads of clusters in a multilevel route, according to clustering, have the position of delivering information to a sink. It leads them to exhaust their power far quicker because of this. Recently, a few hypotheses centered on sinks that move have been brought forward in the scientific community. In these approaches, a sink wanders the network, using heterogeneity and algorithms influenced by nature to reduce the distance between devices and the use of energy. An alternative is to use the blockchain system to locate the illegal nodes in the network as well.

1.8 Contributions

The contributions made by this thesis have a profound impact on the advancement of wireless sensor systems. Firstly, the thesis focuses on a crucial aspect of system sustainability by extending the lifespan of the network through the prolonged longevity of sensor nodes. By implementing energy management techniques and optimizing resource usage, the thesis aims to enhance the network's overall longevity, resulting in reduced maintenance efforts and cost savings.

Secondly, the thesis delves into the development and evaluation of innovative methods that build upon the existing EDEEC algorithm. By introducing novel approaches and enhancements, the thesis strives to overcome limitations and inefficiencies in the current algorithm, ultimately improving the performance and effectiveness of wireless sensor systems.

Furthermore, the thesis contributes by designing an algorithm that ensures secure and reliable communication between nodes within and across different clusters. This algorithm plays a vital role in mitigating the risks associated with unauthorized access or interference, thereby ensuring the network's overall reliability and integrity.

Additionally, the thesis focuses on optimizing cluster formation, a critical factor in wireless sensor networks. By utilizing particle swarm optimization, the thesis aims to create well-structured and efficient clusters, thereby enhancing network connectivity and overall performance. The utilization of the butterfly optimization algorithm for identifying the cluster head, along with the ant colony optimization algorithm for determining the optimal path, further elevates the network's efficiency and data transmission capabilities.

In conclusion, these contributions significantly contribute to the understanding and implementation of wireless sensor systems. By extending the network's lifespan, improving existing algorithms, guaranteeing secure communication, and optimizing cluster formation, the thesis offers valuable insights and practical solutions that enhance the performance, reliability, and longevity of wireless sensor networks in various industrial and commercial applications.

1.9 Thesis Outline

The structure of this thesis is as outlined below:

Chapter-1: Introduction

In this chapter, we introduce the problem statement and brief about other chapters of thesis.

Chapter-2: Literature Review

Many approaches and strategies used to extend network lifetime and create an energy-efficient wireless sensor network are discussed in a thorough and in-depth literature review.

Chapter-3: WSN lifetime optimization in heterogeneous environment

The standard protocols used to extend network lifetime by considering various parameters are explained together with the energy-efficient method for the WSN heterogeneous network in this chapter.

Chapter-4: A Blockchain based authentication in WSN

The proposed approach for authenticating the nodes in the WSN environment to extend their lifetime is thoroughly explained in this chapter, along with a comparison of its outcomes to the other methods.

Chapter-5: Design of energy-efficient mechanism WSN Using BOA, PSO & ACO

This chapter calculates the execution time, network lifetime, packet loss, and energy consumption of WSNs for the optimal amount of CH obtained from the density nodes, as well as the cluster head and path selections made using BOA, PSO and ACO. The outcome is evaluated against the current CRHS, BERA, FUCHAR, ALOC, CPSO, and FLION.

Chapter-6: Conclusion and Future Scope

In this Chapter, the conclusion of the suggested methodologies and algorithms are provided. A thorough discussion of potential directions for further scope work is provided.

CHAPTER 2

LITERATURE REVIEW

In this chapter survey of various methods and techniques from the state-of-art are explained that work in the field of wireless sensor network to save the energy of the network. The survey is structured into three main sections. The first and second section covers the approaches of classical approaches, cluster-based protocol in WSN. The third and fourth section discuss the blockchain and nature inspired algorithm used in WSN to conserve the energy of the network.

2.1 Classical approaches

In 2002, W. Heinzelman introduced LEACH, a protocol for wireless sensor networks (WSNs) in which sensors select their Cluster Head (CH) and form clusters. The CH collects data from the nodes and transmits it to the Base Station (BS). However, the elected CHs experience rapid power depletion. In 2017, Wang et al. proposed LEACH-impt, a mechanism that improved power efficiency by optimizing inter-cluster routing. The route selection is based on factors such as the number of hops, remaining power, and power utilization per round. Although LEACH-impt showed enhanced power efficiency, it suffered from data loss due to the arbitrary selection of CHs and topology changes.

Another mechanism called WECRR (Weighted Power-Efficient Clustering with Robust Routing) was introduced by Haseeb et al. In WECRR, CH selection is based on a deterministic strategy, and routing decisions consider factors like traffic density, remaining power, and packet error ratio. The protocol also improves route maintenance and load distribution among nodes. However, one limitation of this mechanism is the neglect of the interspace between nodes and the BS. Johnson, M. A., et al. proposed AECR (Aware Cluster Based Routing), which selects CHs based on node density and position. This mechanism reduces cluster overhead and communication costs, focusing primarily on node power. However, it does not consider the interspace between nodes.

Han, G., and Zhang introduced WPO-EECRP, a mechanism that selects CHs based on factors such as remaining power, interspace from the node, interspace from the node to the BS, and cluster density. This mechanism performs well when there is an adequate number of nodes between the CH and BS, effectively improving power utilization in the network.

Doostali, S., et al. created a clustering model based on the sensor network's topology control mechanism. The choice of CH was made by calculating the probability of consuming energy more efficiently while still being close to ideal. The network's node count and the distance between nearby nodes were used to determine the probability value. The clustering process used a sleep-awake and learning automata model to improve performance. Although the energy usage was better, it was unable to resolve optimization problems.

Baradaran, A. A., et al. developed the high-quality clustering algorithm (HQCA) to compute high-quality clusters. This method measured the cluster quality using criteria that increased intra-cluster and inter-cluster distances and decreased clustering error rates. However, fuzzy logic was used to select the best CH, which depended on factors like energy and distance. The network's lifespan was extended, but no performance analysis was conducted. Vinitha, A., and Rukmini created the Taylor-based cat salp swarm algorithm (C-SSA) to provide energy-efficient routing in the sensor network. The CH was initially selected along with the LEACH paradigm to facilitate an effective data communication procedure. The nodes send information to the BS via the CH. This approach considered a variety of trust criteria, including data transmission rate, integrity factor, and direct trust, resulting in improved throughput and delay performance.

2.2 Clustering based protocols in WSN

The wireless sensor network (WSN) is distinctive among the beneficial technologies of recent years. There are tens of thousands of tiny sensor nodes within, both conventional and progressive, the latter of which will choose the cluster heads and base stations with a set amount of power. Based on the uses and the power, these sensing nodes are deployed in a scattered manner (Figure 1.1 shows the usage of WSN in various applications). These sensor switches collect environmental data, combine it at the cluster head, and transfer it to the base station (Wang, Z., 2022; Behera, T. M., 2019; Dawood, M. S., 2021; Xu, C.,2019). Due to WSN limitations such as battery consumption by the sensor nodes to intellect the data and aggregate it, for this reason sensor nodes must wake up for the long time in the network, many applications such as agriculture, medicine, rural areas, etc. now face many issues. Senor nodes must keep an eye on streaming or real-time data in order to reduce human participation and environment effects. Number of authors has presented algorithms for balancing the network lifetime while considering factors like the choice of the cluster head, the quantity of alive and dead nodes in the system, the packet delivery ratio, etc.

The clustering approach works very well to increase system performance and give system scalability (Xie, B., 2017). Numerous clustering techniques for both homogeneous and heterogeneous networks were proposed by authors in the literature that is now available (Jafari, H., 2021). The heterogeneous network is crucial for extending the lifespan of the network since it requires less power for communication but more power for the nodes to choose the appropriate cluster head, which has an impact on how the procedure is performed (Yi, D.,2016. According to the amount of power left, the number of nodes that are still alive, and the first node to die, the author of the research has examined the algorithms. WSN is a fusion of heterogeneous and homogeneous networks. The routing algorithm has a crucial role in resource management, including power use. The power limitations, processing demands, and lack of network or information sensing capabilities of sensor nodes are drawbacks (Luo, J.,2014). Therefore, the network needed strong routing algorithms that lengthen system lifetime, boost system scalability, and increase

dependability. Using latency, scalability, power-efficiency, and network size, the hierarchical routing protocol is assessed. The number of factors is to considered to analyze the performance of the wireless sensor network (Fig 2.1).

In the literature, the use of clustering algorithms has been widely acknowledged in the literature as an effective means of reducing power consumption in nodes, while also enhancing system performance and scalability. With advancements in micro electro mechanical sensors and input from researchers, there has been an increase in the deployment of dense and cost-effective sensor nodes. Wireless Sensor Networks (WSNs) find applications in various fields such as military, traffic monitoring, agriculture, healthcare, surveillance, disaster relief, and more.

Clustering plays a crucial role in balancing the energy consumption within the environment. In this approach, the cluster head collects and relays aggregated information to the base station (Luo, J.,2014; Javaid, N.,2013; Saini, P.,2010). Only long-range sensors are required to transmit data directly to the base station, thereby prolonging the system's operational duration. Clustering can be implemented in two types of environments: homogeneous, where sensor nodes are in proximity and possess similar power capabilities, and heterogeneous, where nodes exhibit varying power levels (Saini, P.,2010; Khan, M. Y.,2013).

Researchers have proposed several protocols for the homogeneous environment, such as Threshold Sensitive Power Efficient Sensor Environment (TEEN) (Manjeshwar, A.,2021), Adaptive Threshold-sensitive Power Efficient Environment (APTEEN) (Afsar, F. A.,2013), Hybrid Power-Efficient Distributed clustering (HEED) (Jones, A.,2010), Low-Power Adaptive Clustering Hierarchy (LEACH) (Heinzelman, W. R., 2000), among others. WSNs typically comprise a combination of both homogeneous and heterogeneous networks (Saini, P., & Sharma,2010). Routing algorithms play a critical role in resource management, particularly energy consumption. Sensor nodes face limitations in terms of power availability, computational capacity, and network awareness. Hence, robust routing algorithms are necessary to prolong system life, enhance scalability, and ensure reliable network operations (Elbhiri, B.,2010).

The primary goal of establishing the cluster is to enhance the longevity of the system. Within the cluster, the entire Wireless Sensor Network (WSN) system is divided into smaller fragments or virtual groups based on predefined rules and protocols. In this setup, the sensor nodes are categorized into two types: cluster members and cluster heads (Dawood, M. S.,2021). The selection of cluster heads is based on geographical properties such as energy level, replacement from the sink node, and cluster head (Tanwar, S.,2018). The cluster head collects and consolidates information from various sensor nodes, transmitting all the data in a single packet to the sink node, thus reducing overhead (Khan, M. K.,2018). Cluster formation provides advantages such as reduced energy consumption, improved bandwidth utilization, and minimized network overhead (Kumar, R.,2018). Numerous protocols have been developed to optimize the system's lifespan by allocating the load among sensor nodes and selecting cluster heads to facilitate information transmission across multiple nodes (Pachlor, R.,2018). Figure 2.1 depicts the Clustering in Wireless Sensor Networks.

The clustering scheme can be classified into two categories: homogeneous environment and heterogeneous environment (Pramanick, M.,2015). In the following section, we will describe the protocols used for the heterogeneous environment and compare them based on the number of nodes alive, number of dead nodes, and number of cluster heads selected per round (Chaurasiya, S. K.,2022; Tirth, V.,2023). In all these heterogeneous algorithms, sensor nodes are deployed in an environment where human intervention is not difficult (Devika, G.,2020; Fanian, F.,2019). Therefore, preserving the energy of the nodes is crucial for improving the network's lifetime. Several algorithms have been discussed by different authors, including Hybrid Energy-Efficient Distributed Clustering (HEED) (Jones, A.,2010), Distributed Weight-Based Energy-Efficient

Hierarchical Clustering (DWEHC) (Smith, J.,2018), Hybrid Clustering Approach (HCA) F(Smith, J.,2019), Energy Efficient Heterogeneous Clustered Scheme (EEHCS) (De Freitas,2017), Distributed Election Clustering Protocol (DECP) (Chen, L., 2015), Dissipation Forecast and Clustering Management (EDFCM) (Gupta, S.,2019), Energy-Efficient Unequal Clustering (EEUC) (Chen, L.,2016), Distributed Energy-Efficient Clustering Algorithm for HWSN (DEEC) (Khan, M. Y.,2013), Energy Efficient Clustering Scheme (EECS) (Li, W.,2018), and Multihop Routing Protocol with Unequal Clustering (MRPUC). We will discuss these algorithms in detail in the subsequent sub-section.

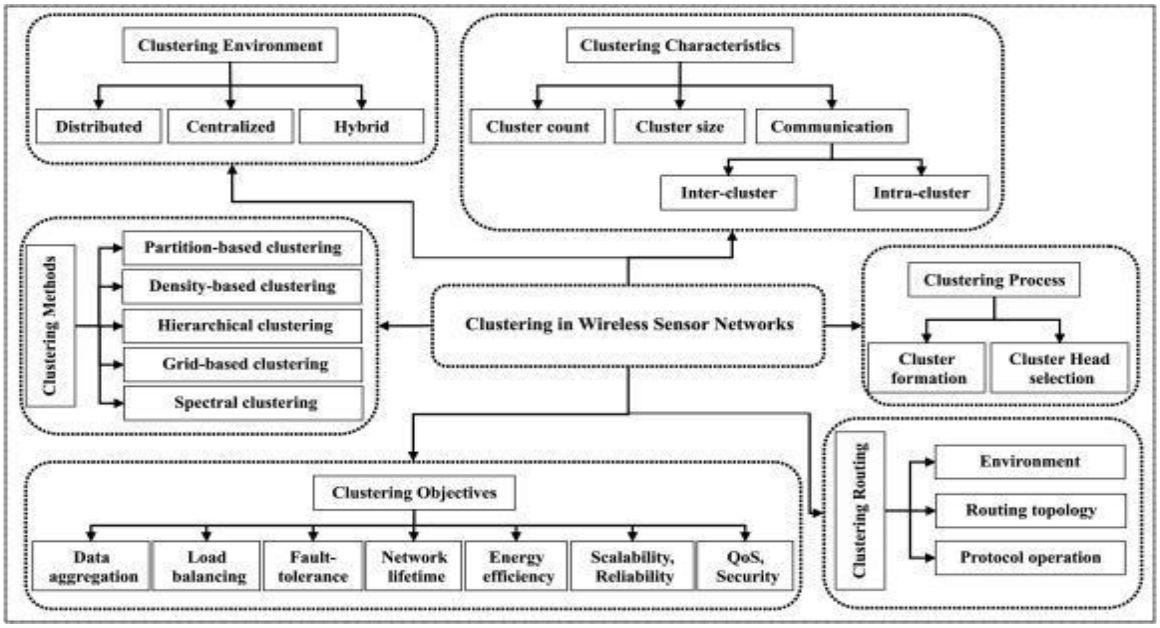


Fig 2.1: Clustering in wireless sensor networks

Jones et al. (Jones, A.,2010), have published the HEED protocol, which is based on a hybrid, distributed, and energy-efficient approach. The main objective of this protocol is to maximize the system's lifetime by distributing the energy utilization. The clustering process is terminated after a certain number of iterations, reducing the control message overhead. Cluster heads are selected using well-established distributed methods. Unlike classical routing protocols, where sensor nodes can only be either regular nodes or cluster heads, in HEED, a sensor node can act as both a server/cluster head and a source node based on the application's requirements.

Smith et al. (Smith, J.,2018), proposed a method after studying the HEED protocol. They observed that the HEED protocol fails to maintain minimum energy utilization in intra-cluster communication and that the clusters created by HEED are not stable. Like HEED, the DWEHC protocol (Smith, J. A. ,2020) also does not consider cluster properties such as density and size. In DWEHC, the protocol is implemented on each node for seven rounds of iterations. After the completion of the protocol, each node becomes either a regular node or a cluster head. Clusters are formed hierarchically, ensuring that each sensor node can reach a cluster head. Time division multiple access (TDMA) is used for intra-cluster communication, while IEEE 802.11 is used for inter-cluster communication between cluster heads and the base node. The protocol assumes quasi-stationary, discrete 2-dimensional sensor nodes and considers factors such as signal strength, direction, and distance. However, it does not account for system size, mass, node spreading, synchronization, or the probability of becoming a cluster head. DWEHC generates a minimum topology for every cluster using an enclosure graph.

In 2011, Neamatollahi et al., published the HCA algorithm, which aims to reduce energy utilization by nodes and maximize system lifetime. HCA is based on a distributed clustering algorithm, where nodes are dispersed throughout the system. The clustering algorithm is not executed in each round, mitigating the disadvantages of static and dynamic clustering algorithms. Cluster heads preserve their energy in the memory during the setup phase, and if their residual energy falls below a certain threshold, a special message is sent to the sink position using time division multiple access (TDMA) frames. The sink station sends a synchronization pulse to all sensor nodes, indicating the start of the clustering process in the next round. New clusters are formed on-demand after the selection of cluster heads, reducing overhead introduced by the setup phase.

In 2009, De Freitas et al. proposed EEHCS, which makes assumptions that the sensor nodes in the system have additional energy resources, are stationary, and are randomly organized. Cluster heads are elected based on outstanding energy. The performance of the clustering protocol is evaluated in terms of system lifetime, number of cluster heads per round, number of alive nodes per round, and throughput. EEHCS considers a heterogeneous system and selects cluster heads based on the contiguous energy level when the sensor nodes are uniformly dispersed. EEHCS includes two protocols: Energy Efficient Hybrid Clustering Scheme (EEHCS) for straight hop communication within the area of the base station, and for multi-hop communication with the sink station outside the detection area. The base station appoints cluster heads based on remaining energy, and the number of associated nodes is chosen through a centralized cluster head selection process. Simulation results show that EEHCS extends the system's lifetime by up to 27.63% compared to LEACH-C, and it improves the first node death rate by a factor of two compared to LEACH-C.

In 2015, Chen,L et al. proposed DECP (Chen, L., 2015), a distributed selection clustering procedure designed for two-level heterogeneous WSNs. The probability of election is calculated based on the remaining energy and communication cost. In balanced clusters, the node with higher communication cost becomes the cluster head, while in imbalanced clusters with unstable energy distribution, the node with higher remaining energy is chosen as the cluster head. DECP provides load balancing and offers a longer stable region compared to classical protocols like LEACH(Heinzelman, W. R., 2000) and SEP (Heinzelman, W. B.,2002). The protocol also introduces the concept that nodes with higher energy have a greater chance of becoming cluster heads, whereas nodes with lower energy levels will only become cluster heads if higher energy nodes are within their range. The average power dissimilarity is calculated to measure the power level of a node. For extended time and reliable data broadcasting in heterogeneous networks, Gupta et al. proposed EDFCM (Gupta, S.,2019). The cluster head election process is based on one-step power consumption forecast, considering energy residual and consumption rate. This approach differentiates EDFCM from other protocols. The algorithm aims to balance power utilization in each round and ensures an optimal number of cluster heads through the management node's role in their selection. Nodes with higher residual energy in the next round have a higher likelihood of being designated as cluster heads.

Li et al. in 2013 presented an algorithm called An Energy-Efficient Unequal Clustering Mechanism for Wireless Sensor Networks (Li, S., 2013) to address the hotspot problem that occurs in multi-hop routing when a cluster head is near the sink station. To resolve the hotspot issue, clusters closer to the sink station are made smaller in size to reduce energy consumption in intra-cluster communication. After cluster formation, the base station sends hello messages to all nodes, allowing them to estimate their distance from the base station. This information assists in forming clusters of unequal size. The cluster head rotates among the sensor nodes during the data gathering process, collecting information on energy utilization throughout the system. The algorithm's evaluation shows that unequal cluster sizes improve system lifetime and balance energy consumption compared to LEACH (Heinzelman, W. R., 2000) and HEED (Smith, J.,2018).

Qing et al. in 2012 (Qing, L., 2012) proposed an energy-efficient protocol for heterogeneous wireless sensor networks using a probability function for cluster head selection. The probability function is based on the node's residual energy and the system's average power. Cluster heads are responsible for collecting information from sensor nodes in their area and forwarding it to the sink station. Nodes calculate their probability function, and those with higher values are designated as cluster heads. DEEC (Khan, M. Y.,2013) utilizes the concept of the LEACH algorithm and works well for multilevel heterogeneous networks. Cluster heads gather data from sensor nodes and transmit it to the sink station.

Ye et al. (Ye, W., 2004) proposed a procedure for energy-efficient and load-balanced clustering in wireless sensor networks for periodic data collection. Cluster heads are elected based on outstanding power. The cluster head selection process involves candidate nodes competing among themselves to become the cluster head. This feature is like the LEACH protocol. During the cluster formation phase, the sink station sends hello messages to all nodes, allowing them to compute their distance from the sink station based on established signal strength.

2.3 Blockchain used in WSN

In 1991, Haber and Stornetta described the concept of a secure blockchain using cryptographic mechanisms such as digital signatures and hash functions. These mechanisms ensure the integrity, authenticity, and non-repudiation of recorded contracts on the distributed ledger. Blockchain is a system that records data in a tamper-resistant manner, making it difficult to modify or hack the records. It acts as a digital ledger of contracts that is duplicated and distributed worldwide, allowing everyone to access, add, verify, and write contracts on the distributed ledger. Once a contract is distributed over the network, it cannot be modified or deleted. Cryptographic algorithms, including digital signatures and hash functions, are employed to provide authenticity, integrity, and non-repudiation to the contracts.

In addition to verifying the combined record, the blockchain technology requires a consensus algorithm—a set of rules and protocols—to be followed by everyone in the network in order to achieve global agreement on the shared record. Over time, Bayer, Stornetta, and Haber introduced the concept of Merkle trees, and in 1998, Nick Szabo designed the term "bit gold," which is a decentralized digital currency mechanism. In 2008, Satoshi Nakamoto introduced Bitcoin, a blockchain-based currency meant for peer-to-peer contract exchange. Bitcoin possesses desirable properties such as decentralization, independence, immutability, authentication, fault-tolerance, auditability, and transparency.

Alongside these features, secure consensus algorithms form the building blocks of Bitcoin, enabling decentralization. During the same year, the term "blockchain" was first associated with the distributed ledger behind Bitcoin contracts. In 2013, Vitalik Buterin proposed Ethereum, and in 2014, the proposed algorithms received funding. In June 2015, the Ethereum network became operational. Ethereum blockchain differs from other types of blockchains as it enables individuals to engage in decentralized applications on its own blockchain, specifically designed for smart contracts and distributed data storage. Ethereum 2.0 offers enhanced speed, scalability, efficiency, and security to the network (Buterin, V., 2014). In 2015, the Linux Foundation developed Hyperledger, an open-source blockchain software. Hyperledger blockchain differs from Bitcoin and Ethereum in that it operates as a private and permissioned blockchain, whereas Bitcoin and Ethereum are public and permissionless blockchains. Table 2.1 provide an overview of protocols used in blockchain.

Table 2.1: Protocols used in blockchain

Characteristics	**Corda**	**Quorum**	**Bitcoin**	**Ethereum**	**Hyperledger**
Year of Released	2016	2016	2009	2015	2016
Permission restrictions	Permissioned	Permissioned	Permissionless	Permissionless	Permissioned
Block Generation	-	-	-	15 Sec	2 Sec
Block Size	-	-	-	85 KB	256 KB
Proxy Re-Encryption	-	-	-	48.01 sec	2.039 sec
Bit rate	-	-	7 TRANSACTION PER SECOND	20 TRANSACTION PER SECOND	95 TRANSACTION PER SECOND
Price Per Contract	-	-		$0.030	$0
Public or Private	Private	Private	Public	Both	Private
Hybrid networks	NO	NO	NO	NO	NO
Global Network	YES	YES	YES	YES	NO

Open-source code	YES		NO	YES	Partial
Parties involved in contract	>2	2	-	2	<50
Consensus	Notary knobs can run several consensus algorithms	Specific understanding of consensus that allows multiple approaches,	Proof-of Work	Proof-of-Work, Casper implementation POS	PRACTICAL BYZANTINE FAULT TOLERANCE
Expandable	Not Prevalent	Not Prevalent	Huge node-expandable, Less performance-expandable	Huge node-expandable, Less performance-expandable	Less node-expandable, huge performance-expandable
Centralized regulation	-	-	Less	Medium	Less
Governance	RS	JP Morgan	Decentralized decision making by community or miners	Carried by Core developer group, but EIP process	Open-governance/ Linux foundation, paradigm based on Linux paradigm
Secrecy	Identified	Identified	Pseudonymity	Pseudonymity	Pseudonymity
Consensus Mechanism	Only parties involved in the contract are involved in making decisions.	Only parties involved in the contract are involved in making decisions.	-	Requires acceptance by all knobs.	Achieved at the level of the whole system or only by parties directly involved.
Encryption	-	-	No encryption of contract data	No encryption of contract data	Encryption of contract data
User authentication	Digital Signature	-	Digital Signature	Digital Signature	Based on enrolment certificate

Device Authentication	NO	NO	NO	NO	NO
Large contracts (1-100 KB/Transaction Hash)	YES	YES	NO	NO	YES
Large contract (more than a block)	NO	NO	NO	NO	NO
Vulnerability to attacks	34% attack	-	51%, linking attacks	51%	>1/3 faulty knobs
Native Currency	No built-in currency	No built-in currency	Bitcoin, huge Value	Ether	No currency
Scripting/ Smart Contract	Programming in Kotlin	Programming in Solidity	Restricted possibility, stack-based scripting	Huge possibility, Turing-complete virtual machine, huge-level language support (Solidity)	Huge possibility, Turing-complete scripting of chain code, huge-level Go-language
Advanced contracts	YES	Partial	NO	NO	YES
Trustless operation	-	-	-	-	Trusted validator node
TRANSACTION HASH integrity and authentication	YES	YES	YES	YES	YES
Data Confidentiality	-	-	NO	NO	YES
ID Management	-	-	NO	NO	YES
Smart contract languages	Java, Kotlin	Solidity	-	Solidity	Java, Golang

The consensus algorithm serves as the heart of the blockchain system. While blockchain offers anonymity, it also raises concerns about trust (J. Kwon,2021). How can we fully trust contracts added by anonymous users? The solution lies in validating each contract before adding it to the block (Luu, L.,2015; Ghosh, M.,2014). The consensus algorithm plays a crucial role in the accumulation of contracts within the blockchain, as it defines a set of rules and protocols. Blocks are added to the blockchain only when all users within the blockchain reach a mutual agreement to maintain the integrity of the blockchain (Karantias, K.,2020). Consensus algorithms are utilized by blockchain to add contracts to blocks and blocks to the blockchain. Several consensus algorithms have been developed for blockchain, including PoW, PoS, DPoS, and Practical Byzantine Fault Tolerance (PBFT), which are widely used by researchers and organizations. A comprehensive overview of the types of consensus algorithms and their properties can be found in Table 2.2.

Proof of Work (PoW) is one of the original consensus algorithms in the blockchain network. It is used to validate contracts and generate new blocks in the chain. In this algorithm, miners compete to complete contracts on the network through a process known as mining. Miners who successfully complete a valid block are rewarded. Bitcoin is a prominent example of an application that utilizes Proof of Work (PoW). The proof of work is generated through a random process with low probability, requiring a trial-and-error approach to find a valid solution. The primary concept of proof of work involves solving a mathematical puzzle to prove the solution. In the blockchain context, the proof of work challenge is solved using the Hash cash proof of work system.

Proof of Stake (PoS) is another consensus mechanism used for processing contracts and creating new blocks in the blockchain. It aims to secure the database by validating entries into a distributed database, referred to as the blockchain in the case of cryptocurrencies. Proof of Stake reduces the computational requirements for block and contract validation, thereby enhancing the security of the blockchain (King, S.,2012).

Delegated Proof of Stake (DPoS) is an evolution of the PoS concept. In this algorithm, users of the network vote to authenticate the next block, and a representative, known as a "delegate" or "block producer," is elected. DPoS allows token holders to pool their tokens into a staking pool and link them to a specific representative, eliminating the need to physically transfer tokens. The rewards are distributed to the top-performing miner in this algorithm (Larimer, D.,2014).

Proof of Elapsed Time (PoET) is a consensus algorithm developed by Intel Corporation that introduces a different approach to selecting a miner to mine a block. In PoET, each potential validation node is assigned a random waiting time during a trusted computation stage, such as Intel's SGX. The validation winner is the node that completes the waiting time first and is then able to add a new block. Every node in the trusted computing platform has an equal chance of becoming the winner in this algorithm (Intel Corporation.,2016).

Practical Byzantine Fault Tolerant (PBFT) is a consensus algorithm introduced in the late 1990s. It is suitable for working in asynchronous systems without an upper bound on receiving responses to requests. PBFT has been updated to minimize overhead time. In a Practical Byzantine Fault Tolerance blockchain system, the system responds based on the current situation of the blockchain, considering the number of malicious nodes compared to the total number of nodes. Having a higher number of honest nodes in the blockchain system enhances its security. Hyperledger Fabric currently utilizes Practical Byzantine Fault Tolerance (Castro, M.,1999).

Directed Acyclic Graph (DAG) is a distinct consensus algorithm that involves vertices and edges. In DAG, the vertices and edges are directed, with all edges heading in one direction. The graph is acyclic, meaning the vertices do not loop back. Unlike other consensus algorithms, DAG does not rely on blocks or require mining to add contracts. Each vertex represents a contract, and contracts are constructed on top of each other without gathering into blocks. When a node submits a contract, a minor Proof of Work

(PoW) process is completed. This PoW operation validates previous contracts and prevents the network from being spammed. IOTA adopts the DAG consensus algorithm (Popov, S.,2018).

Table 2.2: Comparison of consensus algorithm used in blockchain

PoW	**PoS**	**DPoS**	**DBT**	**PoET**	**Tendermint**	**DAG**
Knobs are not trusted	Knobs are not trusted	Knobs are trusted	-	Knobs are trusted	Punishment for validating knobs	-
Fintech	Fintech	-	Vulnerability to faulty knobs>(n-1)/3, n=Total knobs	Lack of consensus finality	Fintech, Vulnerability to faulty knobs>(n-1)/3, n=Total knobs	-
Entry cost is huge, but gives huge return	Entry cost is Less, gives less return	Entry cost is Less, gives less return than PoS	-	Less Entry cost and gives lesser returns than PoS	-	All can play a part with no return
Public permissionless/ Private blockchain	Public permissionless/ Private blockchain	Public/ Private blockchain	-	Private permissioned/ permissionless blockchain	-	Public permissioned non-blockchain
Huge energy consumption cost	Lack of consensus finality	-	Less communication complexity	-	Less energy, communication complexity	-

Prone to forks	Prone to forks	-	Vulnerability to DoS attack	Prone to forks	Vulnerability to DoS attack	-
Mitigates Sybil attack	Mitigates Sybil attack and prevent double costs	Prevent double costs	Prevent double costs	Prevent double costs	Prevent double costs	Prevent double costs
Huge latency in TRANSACTION HASH confirmation	-	-	Fast TRANSACTION HASH confirmation	-	Fast TRANSACTION HASH confirmation	-
Bit rate is huge	-	-	Bit rate is huge	-	-	-
51% attack: Greater than 25% of knobs are involved in attack.	It reduces the 51% attack likelihood.	It is easier to organize 51% attack.	Number of malicious knobs are (n-1)/3 from the total number of knobs.	It reduces the 51% attack likelihood .	-	Not tested

2.4 Nature inspired algorithms used for energy conservation in wireless sensor networks:

In order to prolong the lifespan of wireless sensor networks (WSNs), there is an increasing interest in utilizing nature-inspired methods (Dhage, M. R.,2018). Achieving an optimal network scope is crucial for extending the network's lifespan and reducing the unnecessary data collected by battery-powered sensors. WSNs consist of geographically dispersed sensors that interact to gather and store real-time data from the environment (Gao, T.,2016). These sensors act as repeaters, receiving analog data, converting it to digital format, and routing it to other nodes, cluster heads (CHs), or sinks (Jafari, H.,2021). The collected data is then examined by the base station (BS) to comply with the requested actions.

In order to address the domain orientation in the ACO community, Dorigo et al. (Dorigo, M., 2006) proposed the problem-solving methods have been offered to construct a domain orientation with numerous objective optimizations in the stochastic and the population-based algorithm. The ACO has been involved in multiobjective communication regarding the success or failure method in the assignment of the success in terms of the variety of potential approaches to choose the ACO algorithm. The focus of the single objective's extension has determined the multidimensional ACO.

The architecture of a WSN depends on several factors, including fault tolerance, scalability, stability, and power efficiency (Sohal, A. K.,2018). As the sensors are powered by batteries, their power will eventually deplete, limiting the overall lifespan of the network. This study aims to optimize the network's lifespan by increasing the number of nodes per round, the data sent to the BS, and the selection of an ideal number of CHs (Lin, Y.,2011). Currently, WSNs employ route selection, clustering systems, and network range optimization to enhance performance (Sharma, S.,2020).

The challenges faced by wireless sensor networks include energy constraints, accurate data identification, and the prevention of redundant data. Placing the sensors at appropriate distances from each other without leaving uncovered areas poses a scope hole or blind area problem. To address this issue, Wang et al. developed a technique called the Spectrum Adjustment Standard, suitable for environments with few or many sensors. Through a literature review, the problems of sensor power depletion and sensor node scope have been identified, prompting the exploration of alternative solutions (Tian, J.,2016). Various authors have proposed individual solutions to these problems, but there is a lack of comprehensive approaches (Tsai, C. W.,2016). After conducting a survey and considering the existing problems, researchers collectively redirected their focus towards a multi-purpose optimization mechanism (Nanda, S. J.,2014). Nature-inspired mechanisms have been widely explored in the literature for WSNs, covering aspects such as optimal scope and deployment challenges. Techniques inspired by nature have been used to tackle the problems arising from sensor placement in nature (Mehrotra, A.,2014).

The literature trend indicates that many researchers utilize ant colony optimization, particle swarm optimization, and butterfly optimization algorithms to optimize various aspects of WSNs, such as route selection, CH selection per round, node selection per round, and packet transmission between CHs and the BS. These optimization mechanisms are crucial in improving the efficiency of WSNs and addressing existing challenges. In hostile environments, wireless sensor networks (WSNs) are typically used to collect data. A few WSN-related challenges are formulated as multidimensional optimization problems and addressed using bio-inspired methodologies. Nature has been creating and assisting various biological systems in their survival for millions of years. Most problems in the actual world may now be resolved by these natural systems because they have evolved to be so reliable and effective through time.

According to Fister et al. 2013 (Fister, I., Fister Jr.,et al, 2013), to discover a solution to challenging or complex issues, optimization involves either maximization or minimization of the objective function. Hard or complex optimization problems can be those that take a long time to solve using deterministic techniques. Because metaheuristic techniques are used to address the optimization problems, optimization is also sometimes referred to as metaheuristic optimization. Heuristic and meta both refer to "solution or process," respectively. That entails a more complex approach to the issues without a predictable answer (Tsai, C.,2016).

These issues might be either single- or multi-objective in nature. The best solution will be better the better the objective function is. Single objective refers to the fact that all the particles converge at a single location, which is the best possible outcome. When there are many objectives, the particles converge at one or more points, and the best choice should be made. In a search space, the metaheuristic algorithm looks for a solution (Yazdani, M.,2016). While some algorithms favor local search, others favor global search. By considering different parameters or metrics connected to the issue statement, the objective function is created. There are two different kinds of metaheuristics: population-based metaheuristics and single-solution metaheuristics. Single-solution-based search is limited to local results since it is exploitation-oriented (to refine the solution). While population- based search is exploration-oriented, which limits it to a certain region of the world.

Simulated annealing and tabu search are examples of approaches based on a single solution. There are two categories of population-based methods: swarm intelligence and evolutionary algorithms. The swarm intelligence was proposed in the late 1990's. The SI algorithms were created to investigate the fundamentals of how basic individuals can display sophisticated and complicated swarm optimization behaviors through swarm cooperation, organization, information sharing, and learning. Swarm Intelligence-based optimization algorithms have a significant and positive impact on WSN as shown by their ability to reduce data transmission delays between network nodes, balance the network and reduce network traffic and overhead, conserve energy, and extend the network lifetime. The application of swarm optimization (SO) to WSN problems such the best deployment, node localization, clustering, and data aggregation. It can prevent network congestion and rapid node energy consumption (Smith, J. A., Johnson, M. B.,2018).

Swarm intelligence has grown increasingly alluring to researchers in the related discipline in recent years. It can be categorized as one of the evolutionary computing branches. Swarm intelligence is the process of using collective behavior of social insect colonies or other animal societies to create algorithms or distributed problem-solving tools. Swarm intelligence algorithms are typically used to address optimization issues (Smith, J. A., Johnson, M. B.,2018). The Genetic Algorithm is the traditional algorithm in evolutionary computing and is used to address optimization problems (GA). The Cat Swarm Optimization (Chu, S.-C., 2016) is one of the many swarm intelligence algorithms that are later suggested for solving optimization problems (CSO), Ant colony optimization (ACO) (Dorigo, M.,2006), particle swarm optimization (PSO) (Kennedy, J.,1995), and Butterfly optimization algorithm (BOA)(Qi, H., 2019) are the algorithms that will be discussed in this paper by in-depth descriptions of their work standards and model evaluations. Additionally, various uses for optimization techniques based on swarm intelligence or computational intelligence. Kennedy and Eberhart's proposed PSO algorithm. PSO is a SI global random search method that models swarm and migratory behavior during foraging. Each person in the flock aggregation model abides by these principles: Avoiding collisions with nearby neighbors requires, and flying to the center of the flock, which causes the flock to fly to the target. In the PSO, a bird in the search space known as a particle represents a potential solution to each optimization problem. Each particle has a speed that governs its direction and distances, and each particle has a fitness value that is determined by the optimal function. A probabilistic method for identifying the best pathways is called ant colony optimization. The ant colony optimization algorithm is used in computer science and research to address a variety of computing issues. Marco Dorigo first introduced ant colony optimization (ACO) in the 1990s in his Ph.D. thesis. This algorithm is introduced based on how ants forage to find a route between their colony and a food source. It was initially employed to address the infamous travelling salesperson dilemma. Later, it is used to a variety of challenging optimization issues.

An energy-efficient cluster head selection technique based on the Whale Optimization Algorithm (WOA) named WOA-Clustering (WOA-C) was proposed in 2018 by Jadhav and Shankar et al. (Jadhav, A. S., 2018). As a result, it aids in the selection of energy-aware cluster heads based on a fitness function that considers the node's remaining energy as well as the total energy of its nearby nodes. The implemented method was then assessed in terms of throughput, general stability, network lifetime, and energy efficiency. In order to demonstrate WOA-advantage C's over other models, its performance was compared to that of other modern standard routing protocols. To ensure improved quality of service, Yahiaoui et al.(Yahiaoui, T., 2018) suggested a delay- and energy-sensitive routing protocol in 2018. The reduction of delay and energy usage is the paper's key goal. Considerations include the WSN and actuator network. Both sensor and actuator nodes are included in it.

The actuators oversee making quick decisions and responding appropriately to the information acquired by the sensor nodes. These networks are set up into clusters that are CH-supervised (Qi, H.,2019). Based on connection and energy capacity, the CH was chosen. Additionally, the latter metric guarantees the separation between the actuator nodes and the sensor nodes over several hops. This metric lowers the communication time while alerting the actuator nodes, increasing network reliability while using less energy (Smith, J. A.,2018). Finally, the simulation's results indicate a sufficient gain in terms of communication delay and energy use. Because the nodes are thought of as battery-powered, they start to lose energy after a given amount of time, which reduces the network's lifespan. A tough job in WSN is to increase network longevity by balancing path dependability and energy efficiency.

Jesline Daniel et al. (Daniel, J., 2021) created the Tunicate Swarm Butterfly Optimization Algorithm (TSBOA) to pick CH to achieve efficient data transfer between the sensor nodes in order to address these problems and provide an effective data communication procedure. By combining the Butterfly Optimization Algorithm and Tunicate Swarm Algorithm, respectively, the suggested TSBOA (Daniel, J., 2021) is created. As a result, the choice of CH is made by considering the objective parameters, such as the intra- and inter-cluster distances, as well as the nodes' energy consumption, expected energy, connection lifetime, and latency. By considering the initial energy of nodes, the Deep Long Short-Term Memory classifier performs the energy prediction. Utilizing criteria like residual energy and throughput of 0.1118J and 82.101 percent, respectively, the proposed TSBOA achieved higher performance.

A butterfly optimization algorithm (BOA) was created by (Qi, H., 2019) to select CH from the number of nodes in the network. Several variables were taken into consideration when choosing the CH, including node centrality, node degree, node energy, adjacent distance, and the distance between nodes and the BS. Ant colony optimization (ACO) was used in this instance to transport data between CH and BS. As a result, the routing method was carried out using the parameters energy, distance, and anode degree. Here, many metrics were used to gauge performance. Although the network lifespan was extended, WSN performance was not improved.

To address power constraints, researchers have turned to swarm-based optimization techniques, utilizing over thirty different approaches (Tsai, C. W., Tsai,2015). These swarm-based methods aim to enhance power efficiency, prolong network lifespan, and improve packet delivery ratio in WSNs.

Traditional routing methods are insufficient to overcome the power limitations, leading researchers to employ effective clustering and routing protocols based on swarm-based strategies (Al-Mousawi, A. J,2020). Ant Colony Optimization has been identified as one of the effective routing strategies to improve power efficiency (Sun, Y.,2017). The paper aims to reduce power consumption during data transmission by reviewing contemporary clustering and routing algorithms (Arjunan, S.,2018). Nature-inspired mechanisms and their applications in WSNs, along with the strengths and weaknesses of different research works, are discussed. The optimization mechanisms are categorized into model-based, simulator-based, and mechanism-based approaches, further dividing the mechanism-based analysis into deterministic and stochastic mechanisms. Stochastic mechanisms are further divided into heuristic and meta-heuristic components, with meta-heuristic mechanisms categorized as human inspired, geography inspired, physics inspired, and bio-inspired.

The bio-inspired category is divided into plant-based, swarm-based, and transmutative mechanisms (Wang, Z. X.,2019). The review highlights the significant role of swarm-based optimization techniques in resolving various challenges in WSNs, particularly related to power efficiency. The review chronology provides an overview of the research conducted in the areas of cluster formation, power efficiency improvements, and other related topics (Maheshwari, P.,2021; Wang, Z.X.,2017). The focus has been on power - saving techniques, modification of existing optimization approaches, and reducing run times.

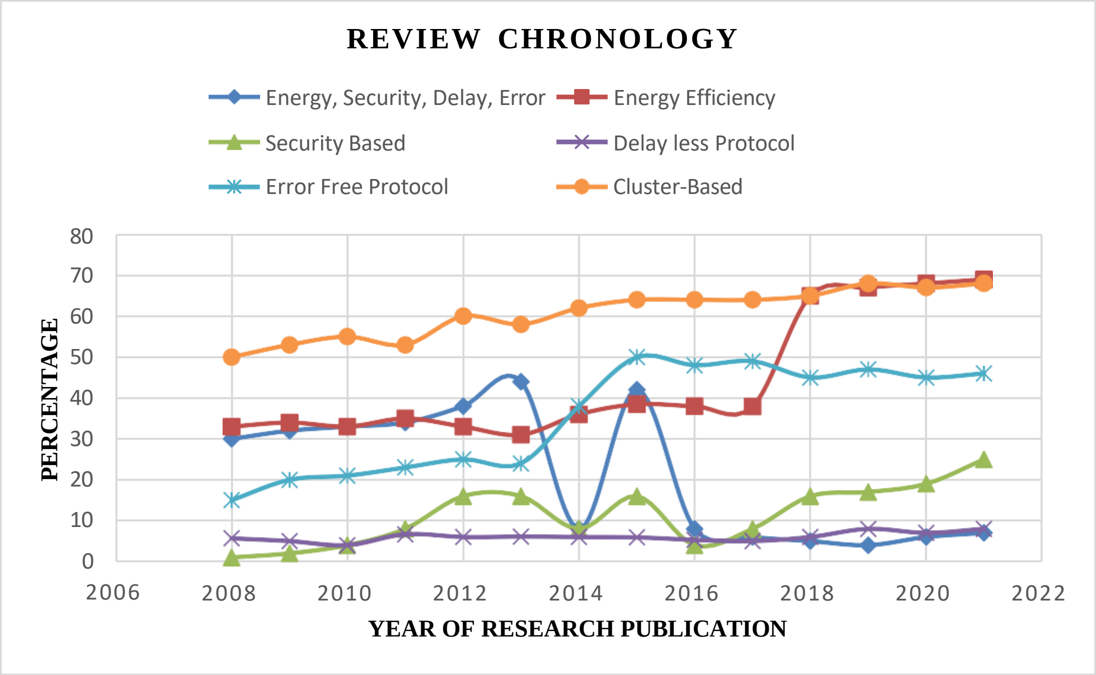


Fig 2.2 Review chronology

Overall, the research aims to optimize the lifespan, stability, and scalability of wireless sensor networks by addressing power limitations and utilizing nature-inspired mechanisms for cluster formation and path selection (Yazdani, M.,2016). The review of literature (Fig 2.2) highlights the current challenges and the potential of swarm-based optimization techniques in improving the power efficiency and performance of WSNs.

CHAPTER-3

WSN LIFETIME OPTIMIZATION IN HETEROGENEOUS ENVIRONMENT

3.1 Introduction

A Wireless Sensor Network (WSN) consists of devices with different power capacities. To conserve power and improve the network's overall performance, a grouping algorithm is needed. We have developed a power-efficient grouping protocol called MEEDEEC (Modified Enhanced EDEEC), which is an enhanced version of existing protocols like SEP (A Stable Election Protocol), DEEC (Distributed Power Efficient Grouping Protocol), EDEEC (Enhanced Distributed Power-Efficient Protocol), and DDEEC (Developed DEEC). Through simulations, we have demonstrated that our proposed mechanism outperforms SEP, DEEC, EDEEC, and DDEEC in terms of network lifetime, packet delivery rate, cluster head (CH) selection, and the number of active nodes. The selection of the CH is based on the device's original power and remaining power.

3.2 Proposed algorithm

This section is divided into the following categories: CH Selection Method, Performance Criteria Used, Simulation, and Results. The flow chart of the proposed algorithm is shown in figure 3.1. In the projected procedure, the CHs are nominated using the same properties such as left-over energy, the mean energy of the network and in the same manner used by the EDEEC (Enhanced Distributed Energy Efficient Grouping) (P. Saini et al., 2010) (Elbhiri, B. et al., 2010). Mean energy of the network is figured as:

$$\underline{E}(r) = \frac{1}{N} E_{total}\left(1 - \frac{r}{R}\right), \textit{where Ristotalroundinnetworklifetime}\&\ R = \frac{E_{total}}{E_{round}} \qquad (3.1)$$

Where E$_{\text{round}}$ shows the energy dissipated in the network and figured by using the following formula:

$$E_{round} = L\left(2NE_{elec} + NE_{DA} + kE_{amp}d_{toBS}^{4} + NE_{fs}d_{toCH}^{2}\right) \tag{3.2}$$

Where d_{toCH}, d_{toBS}, and k_{opt} is figured using equation (3.3)

$$d_{toCH} = \frac{M}{\sqrt{2\pi k}}, d_{toBS} = 0.765\frac{M}{2}, k = \sqrt{\frac{N}{2\pi}}\frac{M}{d_{toBS}^{2}}\sqrt{\frac{E_{fs}}{E_{amp}}} \tag{3.3}$$

As per the basic algorithm LEACH (Low-Energy Adaptive Grouping Hierarchy), the CHs are chosen in each round by using the pre-defined threshold value, and this value is chosen by the devices in between 0 and 1. If the chosen value is fewer than the pre-defined threshold value, then that node will become the CH. The author changed the threshold value. The variable used p, r, and G label the proportion of the CH, existing round and the number of nodes who are no chosen as CH and it is figured as:

$$T(s_i) = \begin{cases} \frac{p_i}{1-p_i(rmod\frac{1}{\sum_{i=1}^{n} P_{i_i}})} * \frac{Residual\ Energy\ of\ a\ node * k_{opt}}{Average\ energy\ of\ the\ Network} & if\ s_i \in G \\ 0 & otherwise \end{cases} \tag{3.4}$$

In DEEC (Distributed Energy Efficient Grouping), DDEEC (Developed Distributed Energy Efficient Grouping) (Elbhiri, B.,2010), EDEEC (Enhanced Distributed Energy Efficient Grouping) (Saini, P.,2010), and TDEEC (Threshold Distributed Energy Efficient Grouping) (Chauhan, A.,2014), a common issue arises where the same device is repeatedly elected as the Cluster Head (CH) after a certain number of rounds. As a result, the energy levels of advanced and super-nodes are significantly reduced, ultimately bringing them down to the same energy level as a normal node. This problem persists in DEEC and EDEEC, while DDEEC and EDDEEC prove to be effective solutions for two-level heterogeneous networks.

To tackle this problem, the author introduces a modification in the function of EDEEC, which successfully preserves the energy levels of advance nodes and super-nodes. Additionally, the author proposes the concept of equal probability for all types of devices to become the CH. This concept ensures that each device, regardless of its type, has an equal chance of being selected as the CH. The probability of selecting a device as the CH is determined using equation 9, which is formulated to calculate the probability accurately (Marhoon, A. F.,2014). By implementing these changes, the author aims to address the energy depletion issue faced by advanced and super-nodes in DEEC and EDEEC, while promoting fairness in the selection of CHs among different device types. These modifications and the introduction of the new probability equation contribute to the overall efficiency and effectiveness of the DEEC, DDEEC, EDEEC, and TDEEC protocols in distributed energy-efficient grouping.

$$\begin{cases} p_i = & \dfrac{p_{opt}E_i(r)}{\big(1+m(a+m_o b)\big)\bar{E}(r)}\ for\ N_{ml}\ nodes\ if\ E_i(r) > T_{absolute} \\ & \dfrac{p_{opt}(1+a*mo)E_i(r)}{(1+m(a+m_o b))\bar{E}(r)}\ for\ Adv\ nodes\ if\ E_i(r) > T_{absolute} \\ & \dfrac{p_{opt}(1+b*mo)E_i(r)}{(1+m(a+m_o b))\bar{E}(r)}\ for\ Sup\ nodes\ if\ E_i(r) > T_{absolute} \\ & \dfrac{p_{opt}(1+b*m)E_i(r)}{(1+m(a+m_o b))\bar{E}(r)}\ for\ N_{ml}, Adv, Sup\ nodes\ if\ E_i(r) \leq \quad {}_{Absolute} \end{cases} \tag{3.5}$$

Where Th_{ab}$Th_{ab} = zE_0\left(1+\frac{aE_{disNN}}{E_{disNN}-E_{disAN}}\right)$ (3.6)

The value of z=0.7

3.3 Performance criteria used

The performance of the protocol is evaluated based on several parameters to assess its effectiveness. These parameters include the network duration, the number of cluster heads (CHs) selected per round, the number of nodes that remain alive, and the number of packets received by the base station (BS). These parameters provide insights into the stability epoch of the network.

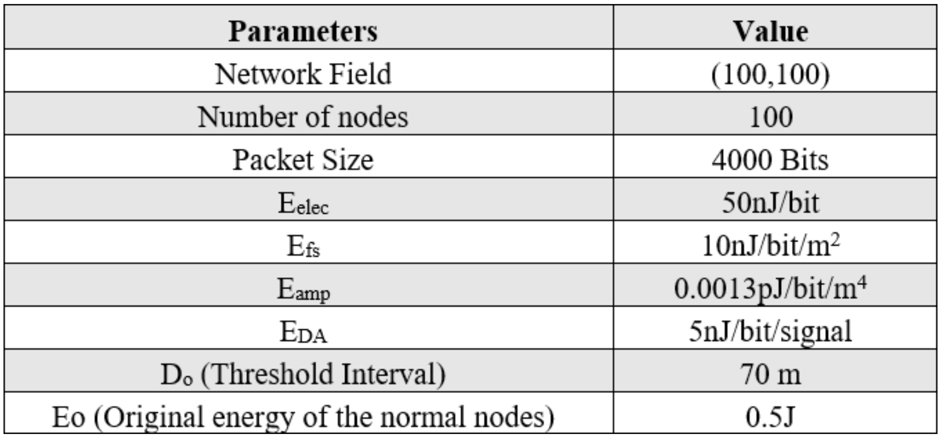
Network Duration: The protocol calculates the remaining energy of the network at each iteration, determining the time interval until the first node's energy depletion.
Number of Alive Nodes: This metric represents the number of nodes that are active in each round, including different types such as normal nodes, advanced nodes, and super nodes.
Packets Acknowledged by BS: This parameter indicates the quantity of packets successfully received by the BS in each round.
Stability Epoch: The stability epoch is defined as the total time interval until the occurrence of the first node's demise.
Unstable Epoch: It refers to the time interval between the death of the first node and the death of the last node, representing the period of instability in the network.

3.4 Simulation result

In this section, the author assesses various procedures implemented in a HWSN. The simulation tool employed for this analysis is MATLAB. The study considers a total of N=100 devices, which are randomly distributed within a network area measuring 100 x 100 units. To avoid oversimplification, the sink station is positioned at the center of the cluster. The initial power levels of the devices vary, and the estimated energy consumption is biased at 0.50. Within this particular scenario, the study incorporates a distribution of 20% advanced nodes and 30% super-nodes, each possessing energy levels distinct from those of normal nodes. Additionally, factors such as signal rear-enders and interference in the wireless channel are intentionally disregarded.

With these specific system constraints in place, a range of protocols designed for HWSN are evaluated in terms of metrics including the number of active nodes, residual energy levels of the nodes, and the count of nodes that become inactive during the initial round. The evaluation focuses on two distinct cases, namely Case 1 with parameters: m=0.5, mo=0.4, a=1.5, b=3, and Case 2 with parameters: m=0.8, mo=0.6, a=2.0, b=7. The Simulation Parameters for the sensor environment are presented in Table 3.1.

Table 3.1: Simulation parameters



Parameters	Value
Network Field	(100,100)
Number of nodes	100
Packet Size	4000 Bits
E_{elec}	50nJ/bit
E_{fs}	10nJ/bit/m^2
E_{amp}	0.0013pJ/bit/m^4
E_{DA}	5nJ/bit/signal
D_o (Threshold Interval)	70 m
Eo (Original energy of the normal nodes)	0.5J

3.4.1 Evaluation of the Terminate Round of the First Node:

Fig 3.1(a) and Fig 3.2(a) illustrate the occurrence of the first node's demise after several rounds. In a Wireless Sensor Network (WSN), the stability and performance of the system are closely tied to the lifespan of the nodes. As the first nodes perish, the system enters an unstable epoch, leading to a gradual decline in network performance. The duration of the network is influenced by the number of nodes it encompasses. Networks with a larger number of nodes may experience slightly extended durations compared to those with fewer nodes.

However, this increase in duration is accompanied by an increased burden on the Cluster-Head (CH). Therefore, achieving a balanced network lifespan has been the focus of several proposed solutions by various authors. These solutions consider factors such as outstanding energy, weight, cost, node location, and computational power when selecting the cluster-head. The simulation result for termination of 1st node for case 1 and case 2 is depicted in table 3.2 and 3.3.

Table 3.2 The simulation result for termination of 1st node (case 1)

Algorithms	**DEEC**	**EDEEC**	**DDEEC**	**MEDEEC**
Rounds	1215	1233	1251	1281

Table 3.3 The simulation result for termination of 1st node of case 2

Algorithms	**DEEC**	**EDEEC**	**DDEEC**	**SEP**	**MEDEEC**
Rounds	1389	1376	1368	1180	1484

3.4.2 Evaluation of number of nodes alive: Figure 3.1(b) and Figure 3.2(b) depict the number of nodes that remain active throughout the network duration. The graph suggests that introducing super nodes leads to an extension in the overall network duration. Comparatively, the proposed system exhibits a longer network lifetime or stability epoch compared to the SEP, DEEC, and EDEEC protocols. In the SEP protocol, the first node dies after 1180 rounds, while in the EDEEC protocol, the first node dies after 1376 rounds. In contrast, our proposed algorithm demonstrates an improved performance with the first node surviving until 1484 rounds. The simulation result for number of alive nodes for case 1 and case 2 depicted in table 3.4 and table 3.5.

Table 3.4 The simulation result for number of alive node (case 1)

Algorithms	**DEEC**	**EDEEC**	**DDEEC**	**MEDEEC**
Rounds	3899	6000	3629	6000
No. of alive nodes	0	19	0	23

Table 3.5 The simulation result for number of alive node (case-2)

Algorithms	**DEEC**	**EDEEC**	**DDEEC**	**SEP**	**MEDEEC**
Rounds	3800	6000	4000	5900	5900
No. of alive nodes	0	5	0	17	25

3.4.3 Evaluation of the number of packets obtained by the BS:

Figure 3.1(c) and Figure 3.2(c) represent the packets received by the base station (BS) in the respective protocols. In DEEC, DDEEC, and EDEEC, the number of packets received by the BS shows a linear trend up to 3000 rounds. However, our proposed algorithm, MEDEEC, exhibits a noticeable difference in performance starting from the 4000th round. The simulation result for number of packets obtained by the base station for the case 1 and 2 is depicted in table 3.6 and 3.7.

Table 3.6 The simulation result for number of packets obtained by the B (case 1)

Algorithms	**DEEC**	**EDEEC**	**DDEEC**	**MEDEEC**
Rounds	6000	6000	6000	6000
Packet sends to BS	>75709	>145271	>108060	>195902

Table 3.7 The simulation result for number of packets obtained by the BS (case 2)

Algorithms	**DEEC**	**EDEEC**	**DDEEC**	**SEP**	**MEDEEC**
Rounds	6000	6000	6000	6000	6000
Packet sends to BS	>72015	>123267	>106520	>105045	>30550

3.4.4 CH selection:

In a HWSN, determining the optimal number of Cluster Heads (CHs) poses a challenging task. However, MEDEEC, in both cases, successfully addresses the issue of CH instability by bypassing the consideration of initial energy levels and instead focusing on streamlining the threshold probability.

This approach not only ensures stability but also reduces the protocol's runtime. These advantageous features make MEDEEC an ideal choice for real-world scenarios. Figure 3.1(d) and Figure 3.2(d), visually demonstrate the number of CHs selected per round. The simulation result for CH selection case 1 and case 2 is depicted in Table 3.8 and 3.9.

Table 3.8 The simulation result for CH selection (case 1)

Algorithms	**DEEC**	**EDEEC**	**DDEEC**	**MEDEEC**
Rounds	6000	6000	6000	6000
No. of CHs selected	20729	10705	20504	4292

Table 3.9 The simulation result for CH selection (case 2)

Algorithms	**DEEC**	**EDEEC**	**DDEEC**	**SEP**	**MEDEEC**
Rounds	6000	6000	6000	6000	6000
No. of CHs selected	21257	12624	20954	14587	5245

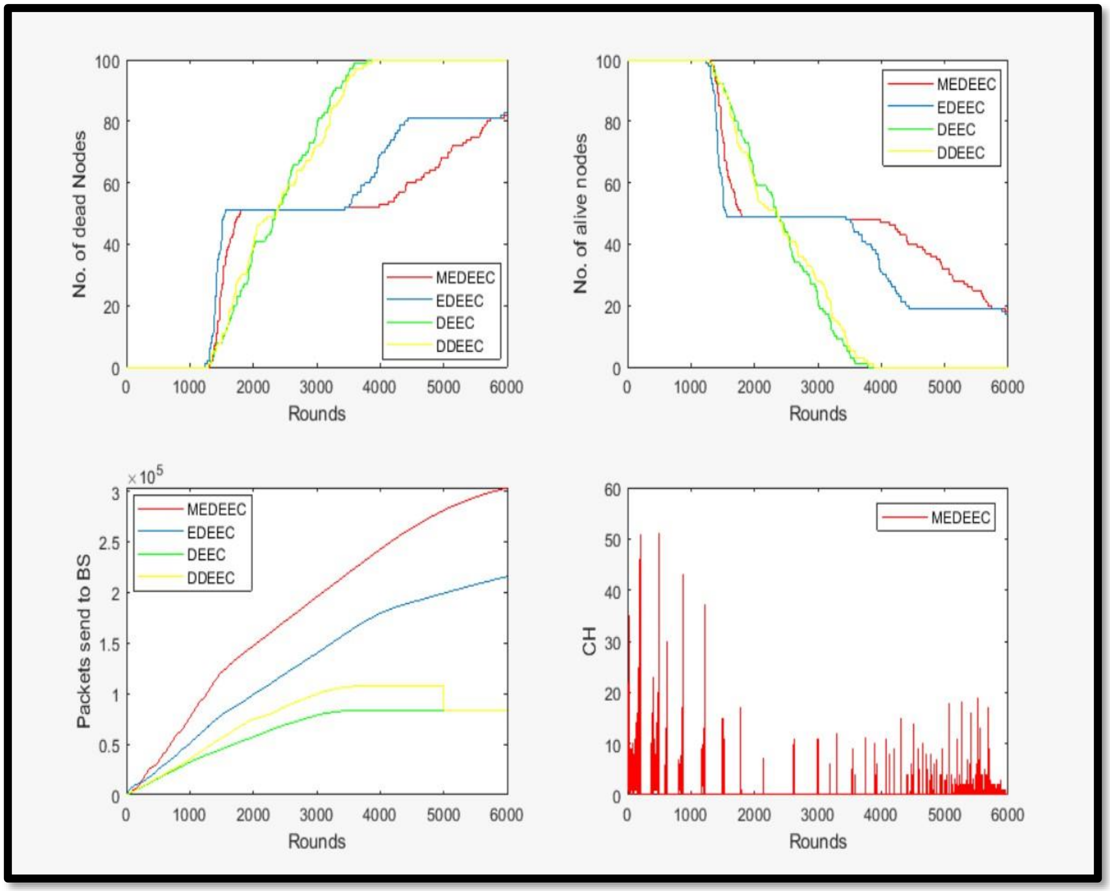


Fig 3.1: (a) No. of dead nodes (b) No. of alive nodes (c) Packets send to the BS (d) Cluster head selection (case 1: m=0.5, mo=0.4, a=1.5, b=3)

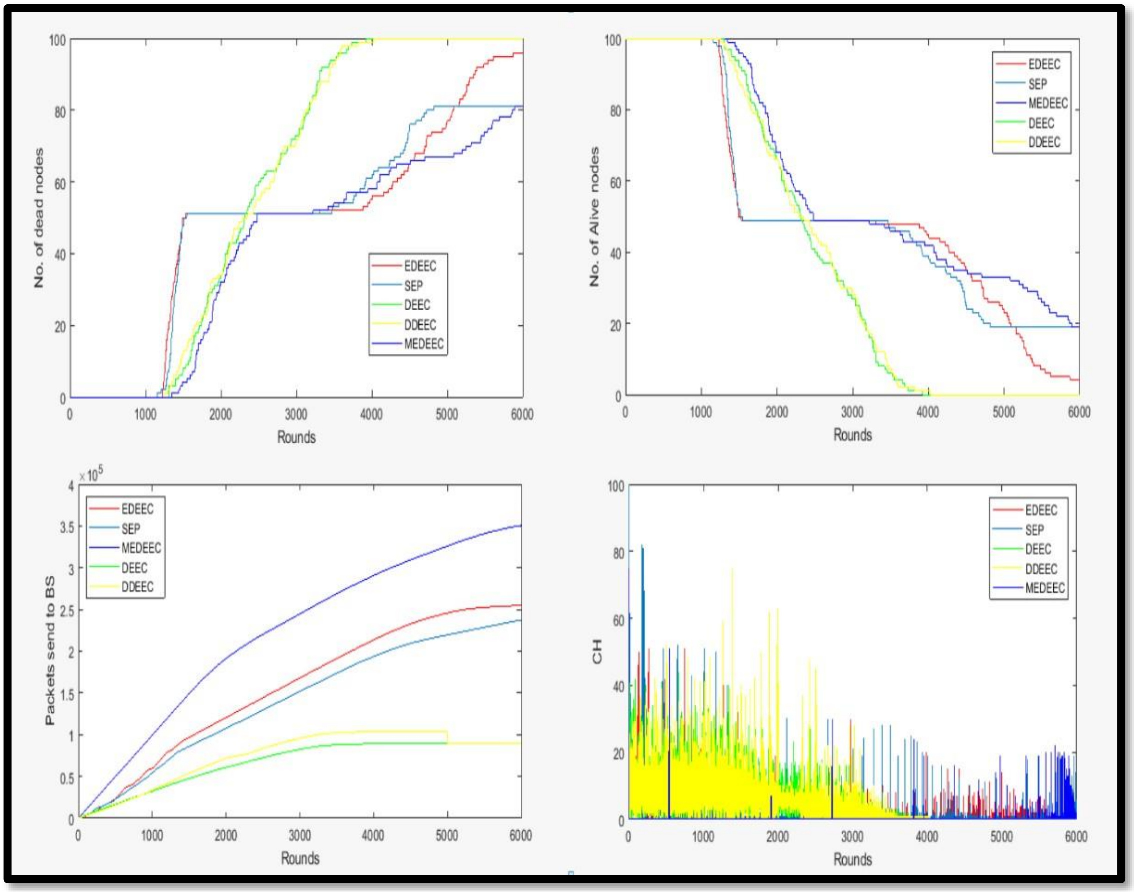


Fig 3.2: (a) No. of dead nodes (b) No. of alive nodes (c) Packets send to the BS (d) Cluster head selection case 2: m=0.8, mo=0.6, a=2.0, b=7

The simulation results unequivocally demonstrate the superiority of the ME-DEEC protocol compared to other protocols such as SEP, DEEC, EDEEC, and DDEEC. ME-DEEC outperforms these protocols in terms of several crucial aspects, including the stability period, number of alive nodes, data transmission to the base station (BS), and optimal selection of Cluster Heads (CHs). ME-DEEC excels in ensuring a longer stability period, indicating improved network reliability and resilience. Additionally, it exhibits a higher number of active nodes throughout the network, enhancing the overall coverage and data collection capabilities. Moreover, ME-DEEC proves to be highly efficient in sending data to the BS, facilitating seamless communication and information retrieval.

Furthermore, when compared to other protocols, ME-DEEC demonstrates superior performance in electing an optimal number of CHs. This feature enables efficient resource allocation and network management. Based on these findings, it is evident that ME-DEEC stands as a superior protocol in various aspects when compared to SEP, DEEC, EDEEC, and DDEEC.

3.5 Summary

Energy-efficient routing protocols are employed to enhance the system epoch and stability of wireless sensor networks. These protocols address various challenges, including limited energy, computational power, and ensuring a high packet delivery ratio. Routing in wireless sensor networks is a particularly challenging task due to these constraints. One key distinction between homogeneous and heterogeneous networks lies in the management of energy utilization among devices. To reduce the number of messages received by sink nodes in large-scale networks, grouping methods are utilized. These methods aim to optimize energy consumption and improve overall network efficiency. Simulation results demonstrate the significant impact of Cluster Head (CH) selection in a heterogeneous environment and highlight the superiority of the best protocol when compared to others.

CHAPTER-4

A BLOCKCHAIN-BASED AUTHENTICATION IN WSN

4.1 Introduction

The increasing need for secure and reliable authentication mechanisms in wireless sensor networks (WSNs) has become critical in today's interconnected world. The proliferation of IoT devices and the sensitivity of the data they handle necessitate ensuring the authenticity and integrity of communication within WSNs (Lazrag, H.,2021). To tackle these challenges, researchers and experts are turning to blockchain technology as a potential solution for authentication in WSNs. Blockchain, originally designed for cryptocurrencies like Bitcoin, provides a decentralized and immutable ledger that enables secure transactions and data sharing (Cui, Z.,2020).

The motivation behind implementing blockchain-based authentication in WSNs stems from the limitations of traditional centralized authentication systems (She, W.,2019). Centralized approaches are susceptible to single points of failure, unauthorized access, and tampering of authentication data. By leveraging the decentralized nature of blockchain, authentication in WSNs can become more robust, transparent, and resilient against malicious attacks (Liu, Y.,2016). Blockchain-based authentication offers several advantages. Firstly, it ensures data integrity and immutability by storing all authentication records in a distributed ledger, making it highly challenging for unauthorized parties to manipulate or tamper with the data. Secondly, it enables secure peer-to-peer authentication, eliminating the need for a centralized authority and reducing the risk of a single point of failure. Thirdly, blockchain enhances transparency as all transactions and authentication events are visible to all participants, fostering trust and accountability within the network (Hammi, M. T, 2018).

Additionally, blockchain-based authentication incorporates enhanced security features such as cryptographic algorithms, public-private key pairs, and digital signatures. These features enable secure and verifiable communication between sensor nodes, ensuring that only authenticated and authorized nodes can access and transmit data within the network (Almadhoun, R.,2018).

The motivation behind adopting blockchain-based authentication in WSNs is to provide a robust and trustworthy authentication mechanism that can address the unique challenges of these networks (Bao, Z.,2018). By leveraging the decentralized, transparent, and secure nature of blockchain, researchers aim to establish a foundation for reliable and tamper-proof authentication in WSNs, ultimately enhancing the overall security and integrity of the network (Belkasmi, M.,2020).

In conclusion, the motivation behind implementing blockchain-based authentication in WSNs lies in the pursuit of improved security, integrity, and reliability (Amin, R.,2018). By harnessing the decentralized architecture and cryptographic features of blockchain, researchers aim to develop authentication mechanisms that can withstand malicious attacks, protect sensitive data, and foster trust in the rapidly evolving world of wireless sensor networks (Ali, G.,2019).

4.2 Objective of the study

The objective of this study is to authenticate the WSN nodes and reduces the malicious nodes from the network to overcome the attacks specifically blackhole and collaborative blackhole attacks, within the network to save the energy of the network. These malicious nodes engage in deceptive behavior by advertising fake queue length information, providing inaccurate data about the actual queue length. They manipulate the network by transmitting data through longer routes, and in the case of collaborative blackhole attacks, multiple malicious nodes work together to mislead the network.

The primary goal is to develop a system that can effectively identify and mitigate these malicious nodes by using blockchain. By detecting the presence of blackhole and collaborative blackhole attacks, the system can prevent the transmission of data through compromised routes and ensure the integrity of the network. To evaluate the effectiveness of our system, we considered several key parameters. These parameters include delay, packet drop ratio, and throughput.

By analyzing these metrics, we can assess the performance of the system in the presence of single blackhole node attacks and cooperative blackhole attacks. Delay is a critical factor as it measures the time taken for data packets to reach their destination. A high delay can significantly impact the overall performance of the network and degrade the quality of service. By monitoring and analyzing delay, we can identify any abnormalities caused by malicious nodes. Packet drop ratio is another important parameter as it indicates the percentage of packets that are not successfully delivered to their intended recipients. Malicious nodes may selectively drop packets to disrupt communication or gain unauthorized access to sensitive data.

By measuring the packet drop ratio, we can identify any unusual patterns that may indicate the presence of blackhole or collaborative blackhole attacks. Throughput refers to the amount of data that can be transmitted successfully within a given timeframe. Malicious nodes can significantly impact the throughput by interfering with data transmission or redirecting it through compromised routes. By assessing the throughput, we can evaluate the efficiency and effectiveness of our system in mitigating the effects of blackhole and collaborative blackhole attacks. By considering these parameters and evaluating the performance of our system, we can assess its usefulness in detecting and mitigating malicious nodes in the network. The objective is to develop a robust and reliable system that can ensure the security and integrity of wireless sensor networks by effectively identifying and countering blackhole and collaborative blackhole attacks.

4.3 Proposed algorithm for authentication process of wireless sensor node using blockchain

In this section, we will discuss the Proposed System Paradigm, including the assumptions, scenario, and workflow of the proposed system.

4.3.1 Assumptions

- To establish the WSN authentication mechanism, the author has made certain assumptions. These assumptions are as follows:
- Each wireless sensor network (WSN) node, or knob, possesses a unique MAC address that distinguishes it from other nodes in the network.
- Sufficient resources are available at both the base station and cluster levels to support the execution of the blockchain algorithm.
- The base station is considered a trusted entity within the network, responsible for overseeing the authentication process.

4.3.2 Scenario

The authentication mechanism proposed in this paper encompasses two primary scenarios:
Scenario 1: Knobs belonging to the same cluster communicate with each other. This scenario focuses on authentication within a single cluster, where nodes exchange information and verify their identities within the cluster's context.

Scenario 2: Knobs belonging to different clusters engage in communication. In this scenario, authentication is extended beyond a single cluster, and nodes from different clusters establish secure communication by verifying their identities across cluster boundaries.

By considering these scenarios, the proposed authentication mechanism addresses the challenges of secure communication within and between clusters of wireless sensor networks. It ensures that only authenticated and authorized nodes can establish connections and exchange data, maintaining the integrity and security of the network.

4.3.3 Workflow

The workflow of the proposed system paradigm involves the following steps:

1. Knobs within the same cluster or different clusters initiate communication.
2. The authentication mechanism is triggered, and the participating nodes exchange authentication messages containing their MAC addresses.
3. The received messages are processed by the base station, which acts as the central authority for authentication.
4. The base station verifies the authenticity of the messages and the corresponding MAC addresses using the blockchain algorithm.
5. If the authentication is successful, a secure connection is established between the communicating knobs, allowing them to exchange data within the designated scenario.

The proposed system paradigm aims to enhance the security and reliability of wireless sensor networks by providing a robust authentication mechanism to reduce the single and collaborative blackhole attack. By following the predefined assumptions, considering different scenarios, and implementing a well-defined workflow, the proposed system ensures that only legitimate nodes can communicate and share data, thereby safeguarding the network against unauthorized access and potential threats.

The overall authentication process is described in the figure 4.1. Rest of the work flow section describe the entire process. According to the authentication process, knobs (simple node, CH, base station) need to place in the wireless sensor network by the base station. The base station generates the database built on the hash value produced by the MAC address of the knobs, here hash value is treated as ID_Node. After this process, the base station will transfer the data to all the other knobs for storing the information. Furthermore, the base station will generate the couple of public and private key for each node in the network so that they can communicate with encryption to preserve the security principle such as Integrity, Authenticity, Non-Repudiation. Secondly, the security rules or protocols needs to be decided by the base station for the other knobs (simple, CH), then registration process need to be done by the CH in the public blockchain which is a transparent and decentralized ledger and registration process need to be completed by the simple node in the internal blockchain which is private and controlled ledger. After the registration process, authentication process needs to be done by the base station in the public blockchain for the CHs and authentication process need to be done by the CHs in the internal blockchain for authenticating the simple knobs.

In the first phase, the smart contact is installed on the server node or base station to manage the contract. The *Proof-of- Authority* (it may be CH/base station) authenticates the node after the registration process. In the registration process, the knobs need to transfer the following data: *MAC address of the knobs, reputation value of the node, public key (node), CH ID, Timestamp and the hash value* generated by encrypting private key of the knobs. The CH receive the packet from the node and verifies the details. If the registration request seems to be valid then the CH generate the block for the node in the internal blockchain. The internal blockchain execute the smart contract and download the identity information form the public blockchain. If the information is already present then the authentication fails otherwise it is approved by the *Proof-of-Authority*. The smart contract checks the CH ID, BSID, public key of the base station. The CH registration phase is done by the public blockchain. CHs transfer the request for registration to the base station including *MAC address, hash value, MAC address of the base station, Base station ID, time stamp* encrypted with the CH private key and transfer it to the base station. The smart contract will execute on the public blockchain and verify the identity of the CH.

Scenario 1: Algorithm for authentication in between the knobs belongs to the same cluster: When a node A intends to transmit a message to another node B within the same network, the process involves initiating a connection request. Node A achieves this by sending a message to the Cluster Head (CH), containing essential information such as *A_MAC address, node ID, A_Cluster ID, and A_base station_ID*. Figure 4.2 illustrates this connection initiation process.

Upon receiving the connection request from the sensor node, the CH executes a smart contract to validate the authenticity of the requesting node on both the public blockchain and the internal blockchain. The primary focus is to verify the data stored within the internal blockchain. If the mentioned information passes the verification process, the next step involves checking the existence of nodes A and B in the system. Once the existence of both nodes is confirmed, their energy levels are assessed. If their energy levels are greater than or equal to the specified threshold value, further verification is conducted within the public blockchain. If all the verification processes are successfully completed, and both nodes belong to the same cluster, node A and node B establish a secure and protected connection. Internal blockchain transfer the confirm message to the CH and transfers the credential for authentication. CH transfer the credential to the knobs wants to communicate. Now both A and B securely communicate with each other.

Scenario 2: Algorithm for authentication in between the knobs belongs to the different clusters: If node A and node B belongs to the different cluster then *Authentication_Credential* will be sent toward the CH of node B by the CH of node A. Figure 4.3 shows the Algorithm for Mutual Authentication Scenario 2. In the internal blockchain, the *Authentication_Credential* consist of *(timestamp, A_ID, B_ID, internal blockchain. Timestamp), ticket for connection)* is signed by the CH by using his private key. CH of node B transfer the *Authentication_Credential* consist of *(timestamp+1, B_ID, ticket for connection)* to the CH of node A.

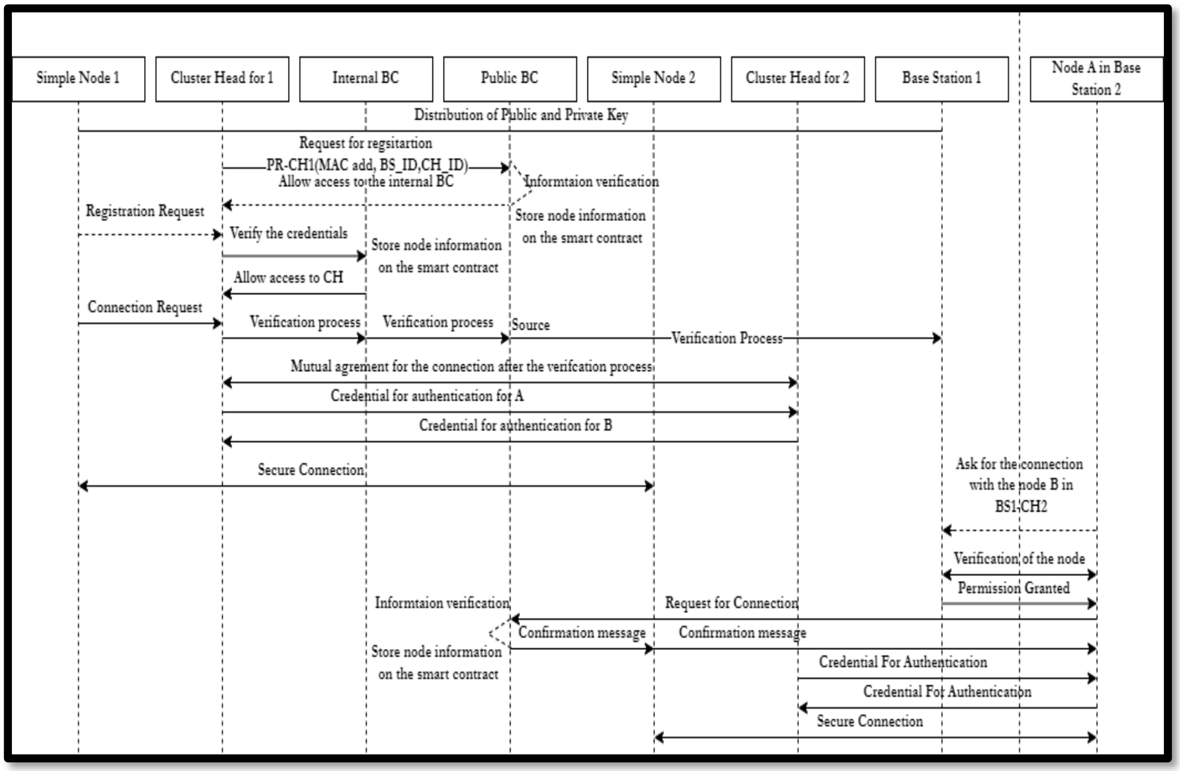


Fig 4.1: Overall flow of authentication process

```
Begin
        If IDcard verification (sensor node A) = error then
        | Return error ();
        End
        If node A exist in Public Blockchain=error then
         | Return error ();
        End
        If node B exist in Public Blockchain=error then
        | Return error ();
        End
        If residual energy of both A and B>= threshold value=error then
        | Return error ();
        End
        If A_cluster head=B_cluster head then
        |       If A_base station = B_base station then
        |       |       Node A and B stablish a secure connection
        |       |       Return;
        |       End
        End
```

Fig 4.2: Algorithm for Mutual Authentication Scenario 1

When both the CH mutually agree on the credential, then both sensor node A and B could create the secure connection. The public blockchain examine the character information of node A and node B stored in the internal blockchain and transfer the *Confirmation_Message* to the CHs present in the wireless senor network by transferring the message *Confirmation_Message (ticket for connection, timestamp, ID_A, ID_B)* and the *ticket_for_connection* contained *hash value of (ID_A, ID_B, timestamp_internalblockchain).* The *Confirmation_Message* transfer by the node A CH to the node B CH and it consist of *(timestamp, A_ID, B_ID, internal blockchain. timestamp, ticket for connection)* and signed by the CH by using his private key. CH of node B transfer the *Confirmation_Message consist of (timestamp+1, B_ID, ticket for connection)* to the CH of node A. When both the CH mutually agreed on the *Confirmation_Message* then the secure connection is stablished in between the node A and node B.

```
Begin
        If IDcard verification (sensor node A) = error then
        | Return error ();
        End
        If node A exist in Public Blockchain=error then
         | Return error ();
        End
        If node B exist in Public Blockchain=error then
        | Return error ();
        End
        If residual energy of both A and B>= threshold value=error then
        | Return error ();
        End
        If A_cluster head=B_cluster head then
        |       If A_base station = B_base station then
        |       |       Node A and B stablish a secure connection
        |       |       Return;
        |       End
        End
        Else
        Public blockchain send the Authentication_Credential to the cluster head
        If Authentication_Credential = true then
        |       Node A_CH1 and Node_CH2 establish a secure connection
        |       Return;
        End
        End
End
```

Fig 4.3: Algorithm for mutual authentication scenario 2

Dead Node: If the energy of the node gets drained and due to some other reasons, the node cancels their registration from the public blockchain or from internal blockchain then in that case CH needs to submit the cancellation appeal to the public blockchain. The smart contract exist in the base station needs to verify the details in the request such as *(ID_A, CH_ID)*. Once the request is verified then the value of that node turn to 0 in the database. 0 means, node is not registered.

Proposed algorithm: To find the secure route using blockchain in AODV

```
1. Source S broadcasts RREQ message.
2. IF
a. {
b. D replies with RREP
c. Then
d. S send the message
e. }
3. END IF
4. IF
a. Node B (intermediate node) replies RREP and packet reaches to the next hope (*) from
   node A //*preceding node A is in the direction in which RREP is traversing from B
   towards S.
b. Then check
c. {
d. MAC_address in BC = 1                                        (4.1)
e. &
f. (Speed of Node >speed threshold)                             (4.2)
g. &
h. (Sequence No> seq_no_threshold)                              (4.3)
```

```
i.  // Threshold value is updated every time intermediate node receives a RREQ packet and threshold value of sequence no is calculated as sequence_number_threshold = sequence number (of RREQ packet) * hop count
j.  If Eqs (1) (2) and (3) are true then
k.  GO TO Step 4.
l.  else
m.  GO TO Step 5.
5.   IF (hop count>= 2)
a.  Node X will send a Modified Hello signal with HopCount equal to 2 (in case hopcount = 2)
b.  or
c.  HopCount equal to 3 (in case hopcount > 2) to a Node (*)(*) (say Z) which is few hops (equal to hopcount) away from A.// ** all the values have to be taken from the RREP received from intermediate node B and (*)(*) Z node is in the path through which RREP packet has reached B.
6.  IF
7.  A receives acknowledgment from Z successfully then A forwards RREP to S and S will transmit the data.
8.  Else
a.  Node next to B is Blackhole and an alert signal will be transmitted by A to S. Else
b.  Node B is Blackhole node and an alert signal will be transmitted by A to S. Step 5: A forwards RREP to S and S will transmit the data.
```

4.3.4 Security analysis attack and efficiency analysis

To enhance the security and energy efficiency of wireless sensor networks, it is crucial to implement an effective authentication mechanism. This mechanism plays a vital role in eliminating malicious nodes from the network, thereby reducing energy consumption. The security requirements for the network include integrity, availability, expandability, non-repudiation, and mutual authentication (Awan, S. H.,2020). To ensure both security and performance, certain requirements must be met, such as integrity, confidentiality, authentication, availability, and non-repudiation. These requirements safeguard against various attacks, including sybil attacks, man-in-the-middle attacks, replay attacks, spoofing, and denial-of-service attacks. The proposed algorithm has undergone analysis by the author, resulting in the following findings:

Integrity: The proposed algorithm ensures message integrity by preventing unauthorized access to data through both the internal and public blockchain. This prevents tampering with data during transmission and storage in the cluster head and base station.

Confidentiality: The algorithm maintains confidentiality by securely handling data within the internal and public blockchain. Unauthorized users are unable to access or read the content of messages.

Authentication: Before communication takes place, the proposed algorithm ensures the authentication of both parties involved. Cluster heads authenticate normal nodes, while the base station authenticates cluster heads. This prevents attacks that target the identity of individuals.

Availability: Availability refers to accessing relevant information within the expected timeframe. Denial-of-service attacks can hinder availability by preventing legitimate users from accessing content. However, the proposed algorithm safeguards information within the internal blockchain, making it inaccessible to unauthorized users.

Non-repudiation: non-repudiation ensures that users and devices cannot deny sending or receiving information. In the proposed algorithm, all records are stored in the blockchain transactions and cannot be modified by any other party. This preserves non-repudiation within the mechanism.

4.4 Simulation, result, and discussion

Several simulations scenarios on the different approaches are applied. Here represent two different comparison scenarios of the present work. Simulation Parameter used for the implementation are Linux (Ubuntu 12.04, NS-2.35, Number if nodes used for the simulations are 50, 100, 150, 225, 315, Packet size is 512, traffic type is UDP/CBR, Simulation time is 100 sec, antenna type is omni, transmission range is 1000*1000 m and routing protocols used are AODV.

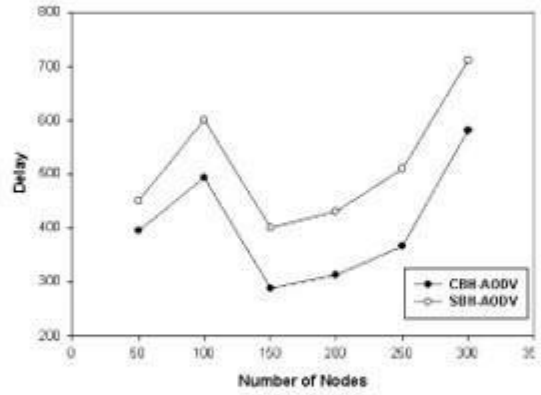


Fig 4.4 (a): End to End delay

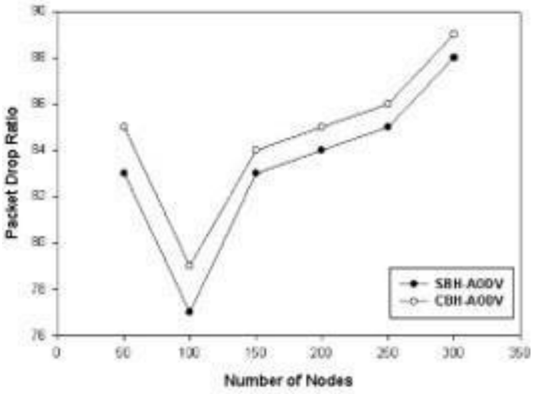


Fig 4.4 (b): Packet Drop Ratio

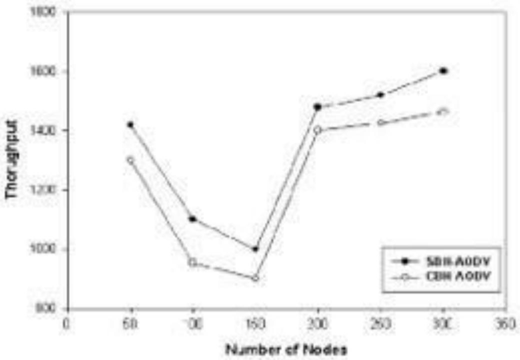


Fig 4.4 (c): Throughput in AODV

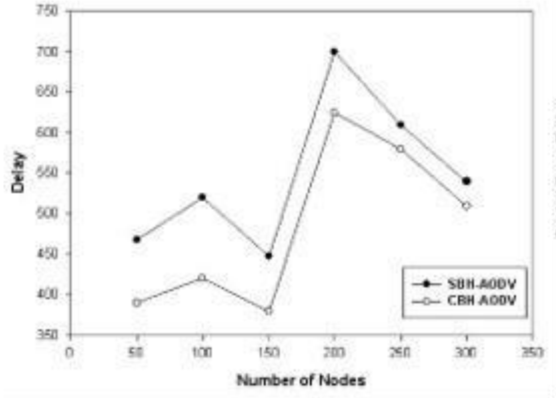


Fig 4.5 (a): End to End delay

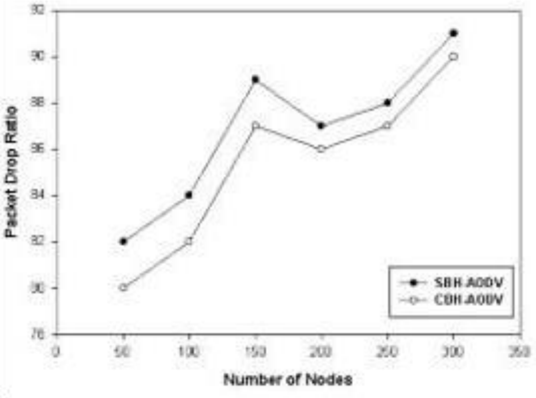


Fig 4.5 (b): PDR

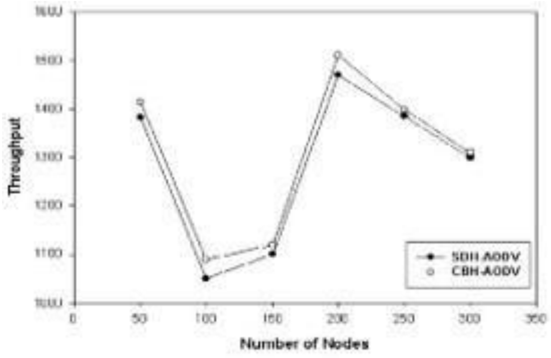


Fig 4.5 (c): Throughput in secure AODV using blockchain

The simulation results illustrate that the x-axis represents the simulation node, while the y-axis represents the performance metrics parameter. Figure 4.3 presents the average end-to-end delay. The average delay of AODV exhibits an increase as the number of nodes grows, but after reaching 150 nodes, the delay increases smoothly.

In terms of the number of nodes, the average delay performance of Secure-AODV with hash function verification outperforms AODV protocols in the context of single and cooperative blackhole attacks. For single blackhole-AODV, the packet delivery ratio improves with 150 nodes.

However, when considering the variation in the number of nodes, the packet delivery ratio of AODV routing protocol is lower for the single blackhole attack until 150 nodes, after which it slightly increases compared to the Cooperative. The throughput performance for blackhole-AODV is nearly the same for single and cooperative blackhole attacks for nodes 50, 100, 150, and 225, but after 225 nodes, they exhibit different performance, with single blackhole-AODV showing an increase.

Comparing the CBH and SBH parameters, the maximum delay recorded is 35.80 seconds, and the minimum value recorded so far based on these parameters is 9.30 seconds. The maximum PDR recorded is 2.53, while the minimum value recorded thus far based on these parameters is 1.15. Lastly, the maximum throughput recorded is 27.27, and the minimum value recorded so far based on these parameters is 6.67.

Figure 4.4 displays the average end-to-end delay. The average delay of Secure-AODV in the single blackhole scenario remains consistent for nodes 50 and 100, but it increases after reaching 150 nodes and slightly decreases at node 315. In comparison, the cooperative blackholes exhibit lower delays compared to the single blackhole. The delay varies with the number of nodes, but in AODV-blackhole, it continuously increases. This emphasizes that our proposed Secure-AODV using blockchain is more secure and highly responsive to network conditions.

The packet delivery ratio performance of Secure-AODV using blockchain network, for both single and cooperative blackholes, consistently improves compared to AODV-Blackhole. It demonstrates an increasing packet delivery ratio. Regarding throughput performance, for blackhole-AODV in single and cooperative blackhole scenarios, it remains similar for nodes 50, 100, 150, and 225. However, when compared to the normal blackhole AODV, the performance is better. In all aspects, Secure-AODV using blockchain demonstrates high performance. Comparing the CBH and SBH parameters, the maximum recorded delay is 31.78 seconds, and the minimum value observed thus far based on these parameters is 5.45 seconds. The maximum recorded PDR is 3.66, while the minimum value recorded based on these parameters is 1.69. The maximum recorded throughput is 4.76, and the minimum value observed thus far based on these parameters is zero. To compare the authentication scheme proposed in the paper with other schemes, the author presents Table 4.1 depicts the Comparison of algorithms with proposed algorithm.

Table 4.1 Comparison of algorithms with proposed algorithm

Properties	**Proposed**	**Ying Qiu**	**Z.Tan**	**Z. Bao, W. Shi**	**Zhihua Cui**	**M. Das**	**Nyang-Lee**	**Vaidya**	**Huang**
Remote Authentication	✓					✓			
Avoiding replay attack	✓	✓	✓	✓	✓	✓			✓
Resist stolen verifier attack						✓	✓	✓	
Resist impersonation attack	✓					✓		✓	✓
Free from an insider attack	✓								
Dynamic node addition stage						✓			
Base Station bypass attack	✓								
Un-traceability attack	✓								
Free from Parallel session attack	✓								
Mutual authentication	✓	✓	✓		✓	✓	✓		

Protected against DOS attack	✓	✓	✓	✓	✓	✓		✓	✓
Protected against message substitution	✓	✓	✓	✓	✓				
Protected against node capture attack						✓			✓
Avoid Masquerading attack	✓					✓			
Avoiding many logged-in users with the same login-id	✓					✓			

4.5 Summary

To address the existing problems in the authentication mechanism of wireless sensor networks, the author proposes a multi-level authentication mechanism based on blockchain technology. This mechanism aims to authenticate sensor nodes and improve security. The proposed mechanism includes a registration algorithm for both internal and public blockchains. In the internal blockchain, the authentication mechanism is established between the sensor node and the cluster head (CH). This ensures that only authorized nodes can communicate within the network. In the public blockchain, the CH is authenticated by the base station, further enhancing the security of the system.

To enhance security, all messages exchanged between the sensor nodes are encrypted using either a public or private key. Additionally, a unique identity number is generated for each node using a hash algorithm, providing a robust identification system. The proposed algorithm undergoes Efficiency Analysis and Security Analysis to evaluate its performance compared to other existing algorithms. The results demonstrate that the proposed algorithm outperforms alternative methods in terms of both efficiency and security.

CHAPTER-5

DESIGN OF ENERGY-EFFICIENT MECHANISM WSN USING BOA, PSO & ACO

5.1 Introduction

The field of wireless communication acknowledges energy-efficient wireless sensor network (WSN) design as a crucial area of research (Tao, F.,2015). With the progress of technology, there has been a substantial rise in the deployment of sensor nodes, leading to increased energy consumption and a restricted network lifespan (Verma, A.,2019). To address these issues, researchers have extensively explored different optimization algorithms, including Biogeography-Based Optimization (BOA), Ant Colony Optimization (ACO), and Particle Swarm Optimization (PSO).

The motivation behind integrating these optimization algorithms into the design of energy-efficient WSNs is to maximize network performance while minimizing energy consumption. BOA, ACO, and PSO draw inspiration from nature, leveraging principles from biology and swarm intelligence to identify optimal solutions. These algorithms provide efficient and effective means of solving complex optimization problems within WSNs.

By applying BOA, ACO, and PSO to WSNs, researchers strive to optimize energy utilization, enhance network coverage, extend the network's lifetime, improve data routing efficiency, and minimize communication overhead. These algorithms offer unique capabilities that enable sensor nodes to intelligently adapt their behavior based on local and global information, facilitating better resource allocation and energy management within the network. The utilization of BOA, ACO, and PSO in the design of energy-efficient WSNs holds immense potential for achieving significant enhancements in network performance and prolonging the network's lifespan. These optimization algorithms empower sensor nodes to operate in a more energy-efficient manner, resulting in reduced overall energy consumption and enhanced network sustainability.

In summary, the motivation behind designing energy-efficient WSNs using BOA, ACO, and PSO lies in the aspiration to overcome the energy-related challenges associated with WSNs and unlock their full potential in providing reliable and sustainable wireless communication solutions.

5.2 Problem statement

The challenges faced by wireless sensor networks (WSNs) include the need to establish an appropriate objective function for creating and maintaining a power-efficient network. Existing approaches such as WECRR (Weighted Power-Efficient Clustering with Robust Routing) (Haseeb, K., 2017) and AECR (Aware Cluster-Based Routing) (Johnson, M. A.,2019) have focused on considering remaining power and preserving the overall power of the network. The CRHS (Clustering and Routing in Wireless Sensor using Harmony Search Mechanism) (Lalwani, P., 2018) considers the lifespan of the network by considering the number of member nodes in each Cluster Head (CH). In WPO-EECRP (Power Efficient Clustering Routing Protocol) (Han, G.,2018), the network's lifespan is affected by the information transmission from CHs to the Base Station (BS) through weighting and parameter optimization in the WSN.

However, the current implementation of Ant Colony Optimization in existing solutions has led to the problem of packet loss due to the limitations of proactive and reactive mechanisms (Arjunan, S.,2018). In order to address these challenges, a new mechanism is proposed that focuses on two crucial aspects: the power of individual nodes and the interspaces between nodes and Cluster Heads (CHs), as well as between CHs and the Base Station (BS). By considering these factors, the selection of the optimal path will be determined through a versatile function that considers both the remaining power and the interspace from the node to the CH, as well as from the CH to the BS. The primary objective of this proposed mechanism is to minimize packet drop ratios in networks of varying sizes, whether small or large. By considering node power and the interspace between relevant network components, this novel approach aims to improve the overall efficiency and reliability of the network, thereby mitigating the issue of packet loss (Gambhir, A.,2018).

In summary, the aim is to develop a purpose function that considers the power of each node, as well as the interspace between nodes, CHs, and the BS. By incorporating these factors, the proposed mechanism can create a power-efficient network with optimized routing paths and minimized packet drop ratios. This approach is applicable to networks of various sizes, ensuring its effectiveness across different WSN deployments.

In this domain, several challenges are encountered by the network:

1. Selection of Cluster Heads: The network faces the challenge of selecting CHs with sufficient power for efficient operation. The choice of CHs significantly impacts network performance.
2. Routing Path Selection: The network needs to determine the best routing paths for information transmission in each round. Optimum routing techniques are employed to ensure efficient data delivery.
3. Maximizing Network Lifespan and Packet Delivery Ratio: One of the primary objectives is to maximize the network's lifespan while maintaining a high packet delivery ratio to the BS. This ensures that data is reliably transmitted from the sensor nodes to the BS.
4. Minimizing Distance: The network aims to minimize the distance between sensor nodes and CHs, as well as between CHs and the BS. By reducing the distance, energy consumption is optimized, and efficient data transmission is facilitated.

Addressing these challenges is essential to create a power-efficient wireless sensor network that maximizes network longevity, ensures reliable packet delivery, and minimizes energy wastage. By implementing effective cluster formation, CH selection, and routing techniques, researchers strive to overcome these challenges and enhance the overall performance and sustainability of the network.

5.3 Proposed Algorithm

In this proposed study, the Butterfly Optimization Mechanism is utilized to select an optimal number of Cluster Heads (CH) from the densely populated nodes (Kaushik, A.,2019). The selection of CH takes into consideration various factors such as the remaining power of each node, its distance from other nodes within the network, its proximity to the Base Station (BS), as well as its centrality and degree. By applying specific criteria, including distance from the CH and the BS, the Particle Swarm Optimization (PSO) algorithm is used to determine the CH (Hussien, A. G.,2020). To establish the routing path within the network, the Ant Colony Optimization (ACO) Mechanism is employed. The optimization of the routing path is influenced by factors such as distance, node angle, and remaining power (Xiuwu, Y.,2019). By considering these factors, the proposed protocol aims to enhance the overall network performance, including the stability period, the number of active nodes, the amount of data received by the BS, and the overall power consumption.

To evaluate the performance of the proposed protocol, comparative analysis is conducted with existing mechanisms such as LEACH, DEEC, DDEEC, and EDEEC, as well as swarm mechanisms like CRHS (Lalwani, P.,2018), BERA (Lalwani, P.,2018), FUCHAR (Arjunan, S.,2018), ALOC (G. Yogarajan,2018), CPSO (Mekonnen, M. T.,2017), and FLION (Sirdeshpande, N.,2017). The results obtained from this comparative analysis provide insights into the effectiveness and applicability of the proposed protocol in this domain (Mahesh, N.,2019; Lin, Y.,2011).

5.3.1 Preliminaries

This section provides an overview of the network and power model, as well as the utilization of Particle Swarm Optimization (PSO), Butterfly Optimization Algorithm (BOA), and Ant Colony Optimization (ACO) techniques in the proposed system.

5.3.2 Network Model

The sensor nodes within the network are initially deployed in an arbitrary manner, after which their positions remain constant. The Base Station (BS) plays a central role in receiving information such as the remaining power of each node and the interspace between the sensor nodes. In order to configure the network model for the wireless sensor network, all the sensor nodes are compared based on their original energy levels and the processing period. The interspace between the sensor nodes and the Cluster Head (CH), as well as between the CH and the Base Station, is determined using the Euclidean distance measurement. This approach ensures that the distances are calculated accurately to facilitate cluster formation and subsequent routing mechanisms.

The formation of clusters is achieved through a dedicated Cluster Formation mechanism, which groups the sensor nodes accordingly. Subsequently, the selection of CHs is performed using a suitable choosing mechanism, ensuring the optimal assignment of these roles within the network. Finally, the routing mechanism, based on the Ant Colony Optimization technique, is employed to identify the most efficient route from the source to the sink within the network. By incorporating PSO, BOA, and ACO techniques, the proposed system aims to achieve an optimized network model that enables efficient cluster formation, appropriate selection of CHs, and effective routing from the source to the sink. These techniques contribute to enhancing the overall performance and energy efficiency of the wireless sensor network.

5.3.3 Energy Model

In this section, the energy model used in the research is described, which incorporates a basic radio model to calculate the power consumption of the nodes. The power required to transmit 'l' bits from the source to the sink over a distance 'd' is determined using equations 5.1 and 5.2.

The energy consumed during transmission, denoted as E_TX (l,d), is computed based on the following conditions:

- If the distance 'd' is less than the threshold value 'd0', the energy consumption is given by the equation $LE_{elec} + LEfsd^2 \ if \ d < do$

- If the distance 'd' is equal to or greater than the threshold value 'd0', the energy consumption is given by the equation E_TX(l,d) = LE_elec + LE_mp * d^4.

$$E_{TX}(l,d) = \begin{cases} LE_{elec} + LEfsd^2 \ if \ d < do \\ LE_{elec} + LEmpd^4 \ if \ d \geq do \end{cases} \qquad (5.1)$$

Here, LE_elec represents the power required to operate the transmitter or receiver (ETX or ERX), and the threshold value 'd0' is determined based on the ratio of E_fs (energy in free space) and E_mp (energy in a multipath model) as calculated in equation 5.2.

The values of E_fs and E_mp depend on the characteristics of the transceiver amplifier model used in the experimental setup. The threshold value 'd0' is calculated as the square root of the ratio of E_fs to E_mp.

$$d_0 = \sqrt{\frac{E_{fs}}{E_{mp}}} \qquad (5.2)$$

By incorporating this energy model, the research aims to accurately estimate the power consumption during data transmission in the wireless sensor network, considering the impact of distance and different transmission scenarios.

5.3.4 Flow of the algorithm

The proposed model consists of three key mechanisms, each serving a specific purpose in the overall operation of the network. These mechanisms are illustrated in Figure 5.1 and are explained as follows:

Cluster Formation Mechanism: This mechanism utilizes Particle Swarm Optimization (PSO) to form clusters within the network. PSO is employed to optimize the selection of cluster heads (CHs) based on certain criteria, such as the remaining power of the sensor nodes and the interspace between them. PSO helps to create clusters effectively by considering these factors and promoting energy-efficient clustering.

Choosing Mechanism for Cluster Heads: In this step, the Butterfly Optimization Algorithm (BOA) is employed to determine the optimal number of CHs in each round. BOA aims to strike a balance between the network's power consumption and its longevity. By considering factors such as the remaining power of the nodes and the interspace among them, BOA assists in selecting the appropriate number of CHs, thereby optimizing the performance of the network.

Routing Mechanism: The Ant Colony Optimization (ACO) technique is utilized in the routing mechanism of the proposed model. ACO helps in finding the optimal route from the source to the sink or from the CH to the Base Station (BS). By considering factors such as distance, node angles, and remaining power, ACO facilitates the determination of an efficient and reliable route for data transmission throughout the network.

The entire process of cluster formation, CH selection, and route determination is depicted in Figure 5.1, providing a visual representation of the proposed model's operation and the interaction between these mechanisms.

By incorporating PSO, BOA, and ACO, the proposed model aims to optimize the network's performance, enhance energy efficiency, and prolong the network's lifespan.

5.3.4.1 CH choosing using BOA

The Butterfly Optimization Mechanism (BOA) was introduced in 2019 by Sankalap Arora (Arora, S., 2019) and draws inspiration from the food search and mating behavior of butterflies. In nature, butterflies are attracted to the scent or cologne emitted by other butterflies. They exhibit a random movement pattern or tend to follow the path of butterflies with a stronger scent.

In the context of the BOA, a purpose function is utilized to calculate the strength of the attraction or incentive. This function evaluates various parameters, including the node degree, node centrality, interspace to the nearest node, interspace between the Base Station and the Cluster Head (CH), and the remaining power of the sensor nodes (Arora, S., 2019).

By considering these parameters, the butterfly optimization mechanism determines the optimal number of CHs to be selected. The goal is to find the ideal quantity of CHs that will result in an efficient and effective clustering process in the wireless sensor network. The BOA mimics the behavior of butterflies, where the nodes in the network act as virtual butterflies, attracted to other nodes based on the parameters. This approach aims to enhance the performance of the network by selecting CHs that possess desirable characteristics, such as high node degree, centrality, appropriate interspace, and sufficient remaining power (Arora, S., 2019).

Overall, the BOA offers a nature-inspired optimization mechanism that utilizes the behaviors of butterflies to determine the optimal number of CHs in a wireless sensor network. By considering specific parameters, it aims to improve the network's efficiency and effectiveness in terms of clustering and overall performance.

Node degree: Node degree refers to the number of sensor nodes connected to a particular Cluster Head (CH) in a wireless sensor network. It is an important factor considered in the selection process of CHs. The decision to choose a CH with a lower quantity of connected sensor nodes is preferred because CHs with a higher number of connected nodes tend to consume their power at a faster rate. To calculate the degree of a node, the power of all the sensor nodes belonging to the CH is summed up. This provides an indication of the overall load or connectivity of the CH in terms of the number of sensors. In the purpose function used for determining the optimal quantity of CHs, the node degree is assigned a weight value of 0.1. This weight signifies the relative importance or influence of the node degree in the overall optimization process. By incorporating the node degree as a factor in the purpose function, the selection of CHs can be guided towards achieving a more balanced distribution of sensor nodes and an efficient utilization of power resources. Considering the node degree in the CH selection process helps to address the issue of power depletion in CHs with a high number of connected nodes. By favoring CHs with a lower node degree, the network can achieve a more equitable distribution of power consumption and prolong the network's overall longevity.

$$ND = \sum_{i=1}^{m} I_i \tag{5.3}$$

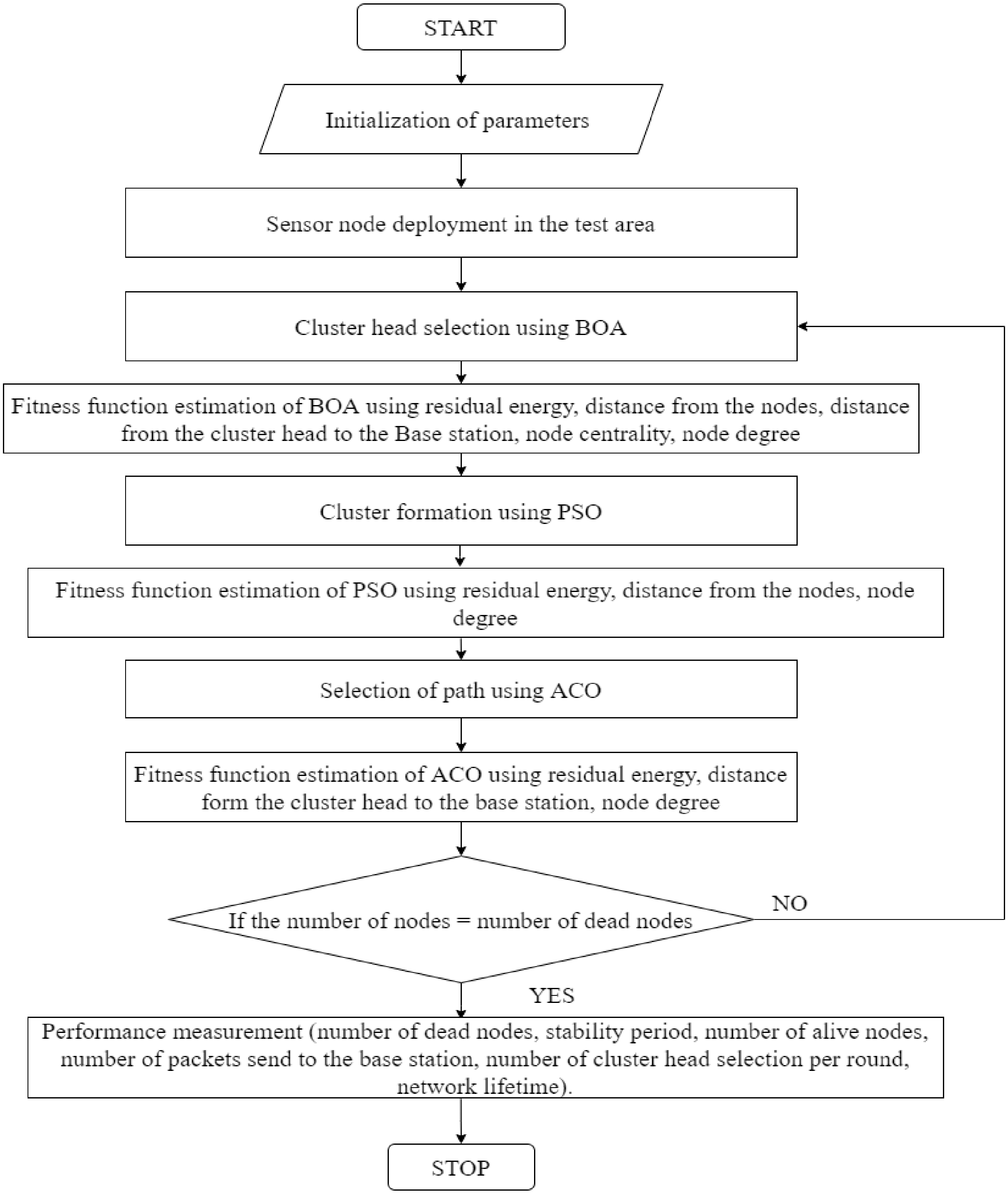

START
Initialization of parameters
Sensor node deployment in the test area
Cluster head selection using BOA
Fitness function estimation of BOA using residual energy, distance from the nodes, distance from the cluster head to the Base station, node centrality, node degree
Cluster formation using PSO
Fitness function estimation of PSO using residual energy, distance from the nodes, node degree
Selection of path using ACO
Fitness function estimation of ACO using residual energy, distance form the cluster head to the base station, node degree
If the number of nodes = number of dead nodes
NO
YES
Performance measurement (number of dead nodes, stability period, number of alive nodes, number of packets send to the base station, number of cluster head selection per round, network lifetime).
STOP

Fig 5.1: Flow chart of proposed algorithm

Node centrality: It is defined as how much a node is centrally located from the nearest nodes. The weight value for the purpose function is 0.1 and it is calculated by using the equation:

$$c_n = \sum_{i=m}^{m} \frac{\sqrt{\frac{\sum_{j\in n} dist^2(i,j)}{n(i)}}}{Network\,\dim ension} \tag{5.4}$$

where n(i) quantity of nearest node to the CH_i.

Remaining Power of the node: The remaining power of a node plays a crucial role in selecting the Cluster Head (CH) as it needs to perform various tasks such as information aggregation, duplicate removal, and transmitting data to the Base Station (BS). In the purpose function, the weight assigned to this criterion is 0.3. Consequently, the node with the highest remaining power is chosen as the CH. The calculation for the remaining power (R_e) is given by:

$$R_e = \sum_{i=1}^{m} \frac{1}{E_{CHi}} \tag{5.5}$$

where the remaining power of the ith CH is E_{CHi} .

The interspace between the sensor nodes is defined as the distance between the sensor nodes and their respective CHs, as well as the distance between neighboring sensor nodes within the cluster. A shorter interspace results in lower power consumption during transmission. In the purpose function, the weight assigned to this criterion is 0.2. The interspace (Dij) can be calculated using the formula:

$$D_{ij} = \sum_{i=1}^{m} \left(\sum_{j=1}^{Ii} dis\left(s_j, CH_i\right) / I_i \right) \tag{5.6}$$

Here, dis(s_j, CH_i) represents the distance between the jth sensor node and the ith CH, and Ii represents the number of sensor nodes within the cluster of CH_i.

The interspace between the Cluster Head (CH) and the Base Station (BS) indicates the distance between the CH and the BS. When the CH is located far away from the BS, it consumes more power for information transmission. Therefore, it is preferable to use nodes that are closer to the BS for conveying the information. In the purpose function, the weight assigned to this criterion is 0.25. The calculation of the interspace from the BS to the CH (D_(CH-BS)) is given by:

$$D_{CH-BS} = \sum_{i=1}^{m} dis\left(CH_{j}, BS\right) \tag{5.7}$$

Here, dis(CH_j, BS) represents the distance between the jth CH and the BS.

So, the single purpose function to find the CH from the set of nodes is calculated as

$$F = \alpha_1 ND + \alpha_2 C_n + \alpha_3 R_e + \alpha_4 D_{ij} + \alpha_5 D_{CH-BS} \tag{5.8}$$

Algorithm: CH choosing using BOA

1. Fitness function derivation using
2. Generate a preliminary populace of butterflies.
3. Prepare impetus intensity (I) at node I which is intended by f(xi)
4. Prepare shift possibility, sensor modality and power exponent.
5. For j=max quantity of reiterations
6. For every butterfly in populace
7. Calculate cologne $f = cI^{a}$

```
    End for
    Identify the optimum butterfly populace
    For every butterfly in populace
        Generate a arbitrary quantity r from [0,1]
        If arbitrary quantity < population
            $x_i^{t+1} = x_i^t + \left(r^2 \times g^* - x_i^t\right) \times f_i$ where $f_i$ is butterfly fragrance, $g^*$is current iteration.
        else
            Move arbitrarilyly $x_i^{t+1} = x_i^t + \left(r^2 \times x_j^t - x_k^t\right) \times f_i$
        End if
    End for
    Update the value of energy proponent
End for
Optimal quantity of CH chooses from the population.
```

5.3.4.2 Cluster formation using PSO

Particle Swarm Optimization (PSO) is a nature-inspired mechanism that has gained significant recognition among researchers for achieving optimal results in wireless sensor networks (WSNs). The concept of PSO was initially introduced by Kennedy and Eberhart in 1995, drawing inspiration from the social behavior observed in bird flocking and fish schooling.

When applied to WSNs, PSO serves as an effective method for addressing the clustering problem. It adopts a centralized clustering approach, wherein the Base Station (BS) takes charge of forming the clusters. The process commences with the BS transmitting an information collection message to all sensor nodes present within the network environment.

Upon receiving the information collection message, each sensor node responds by providing relevant details to the BS. These details typically include the node's identification, location (measured in terms of interspace from the BS and position), power loss, power loss ratio (velocity), and the current power level available for transmitting data to the BS.

By incorporating PSO into the clustering process, the WSN can achieve efficient cluster formation. The mechanism utilizes the collective behavior of particles (representing sensor nodes) to search for an optimal clustering configuration. Through iterative steps, particles explore the search space to find the best possible clustering solution, considering factors such as power efficiency, proximity to the BS, and other relevant parameters.

The utilization of PSO in WSNs provides a robust approach for forming clusters, enabling efficient data collection and management. By leveraging the power of swarm intelligence, PSO helps optimize the network's overall performance, enhance energy efficiency, and prolong the network's operational lifespan. The clustering process in a centralized approach involves the formation of clusters by the Base Station (BS). To initiate this process, the BS sends an information collection message to all the sensor nodes within the network environment.

Upon receiving this message, the nodes respond by sending specific information to the BS. This information includes the node's unique identifier, location (interspace from the BS in terms of distance and position), power loss, power loss ratio (velocity), and current power level for transmitting data to the BS. After gathering the necessary information from the sensor nodes, the BS proceeds to execute the steps involved in the clustering process.

FUNCTION: PSO-CLUSTER FORMATION

```
Initialize the optimization problem and mechanism, parameters.
for i=1 to the particle size do
    Initialize Xi within the search range of (Xmin,Xmax) arbitrarilyly;
    Initialize Vi within the velocity range of (Vmin,Vmax) arbitrarilyly;
    pi=xi
end for
Evaluate each particle **//
    $fitnessvalue = a \frac{\sum_{i=0}^{n} d\left(currentnode, membernodei\right)}{n} + b \frac{\sum_{i=0}^{n} E\left(memberi\right)}{E\left(existingnode\right)} + (1-a-b) \frac{1}{numberof\ existinthecurrentnode}$
where a & b is normalized values and n shows the quantity of nodes in the cluster
Identify the best position Ps;
//Loop:
While (Stop criterion is not satisfied & t < maximum iteration times) do
    for i=1 to the particle size do
        $V_i^{t+1} = \omega V_i^t + c_1 r_1 \left(P_i^t - X_i^t\right) + c_2 r_2 \left(P_g^t - X_i^t\right)$
        $X_i^{t+1} = X_i^t + V_i^{t+1}$
        $P_i^{t+1} = P_i^t$
        Evaluate fitness value
        If fitness $\left(P_i^{t+1}\right) < fitness\left(X_i^{t+1}\right)$;
            Update $\left(P_i^{t+1}\right)$;
        End if
```

```
            If fitness then $\left(P_g^{t+1}\right) < fitness\left(P_i^{t+1}\right)$;
                Update $\left(P_g^{t+1}\right)$;
            End if
        End for
    End While
```

5.3.4.3 Routing Mechanism using ACO

Ant Colony Optimization (ACO) is a metaheuristic mechanism inspired by the behavior of ants. It is commonly applied to solve discrete problems. In the context of ACO, the objective is to find the shortest path from a source node to a destination node using a graph representation. In this representation, the ant colony, represented by nodes associated with Cluster Heads (CHs), is treated as a node, and the links between nodes are denoted by "L" with different weights.

During the initial phase of ACO, the weight of each link is determined based on the actual interspace between the nodes. This value is calculated using a mathematical formula and an arbitrary quantity. This improvement helps overcome the drawback of undefined conjunction in ACO. Additionally, the ACO mechanism is further enhanced by considering factors such as remaining power, interspace from the destination, and node degree.

The route-finding process using ACO can be outlined as follows:

1. Within each formed CH, ants are present in every cluster. The CH generates routes from the CH to the destination (BS) in the form of redirect packets.
2. The redirect packets are then arbitrarily converted to the next CH based on a probability matrix. The redirect packets are relayed to the next CH until they are acknowledged by the BS.

3. The redirect packet maintains a local information base that includes details about the visited CH, remaining power of nodes and CHs (which is calculated based on the quantity of packets transmitted throughout the network), interspace from the CH to the BS, and the node degree.
4. The information from the redirect packets is used to create a backward information base or backward packets. These backward packets are necessary to extend the path until the packet reaches the BS. The path followed by the backward packets is the same as the path followed by the redirect packets.
5. The pheromone level of the links is updated considering factors such as remaining power, interspace to the Base Station, and node degree.
6. The selection of the next node for transmission is based on equation number 9, which represents the probability of selecting node "j" as the subsequent node after node "i" by ant "k".

By following these steps, the ACO mechanism facilitates the discovery of efficient routes within the network based on various factors and probabilities.

$$P_{ij}^{k}(t) \; = \; \begin{cases} \frac{[\tau_{ij}(t)]^{\alpha}[\eta_{ij}]^{\beta}}{\sum_{l \in \mathrm{N}_k}[\tau_{ij}(t)]^{\alpha}[\eta_{ij}]^{\beta}} & if\ j \in \mathrm{N}_k \\ 0 & otherwise \end{cases} \tag{5.9}$$

In the context of the ACO mechanism, the heuristic value is denoted as η_{ij}, and the pheromone intensity is represented as τ_{ij}. To regulate the relative significance of these values, parameters α and β are employed. The set of unvisited nodes is denoted as N_k.

Based on the information stored in the routing table by the CH, the heuristic and pheromone intensity values are updated using the following formulas:

$$\eta_{ij} = \frac{1}{d_{CH}} \tag{5.10}$$

And,

$$\tau_{ij} = (1-\rho)\tau_{ij}^{old} + \sum_{k=1}^{m} \Delta\tau_{ij}^{k} \tag{5.11}$$

Where, d_{CH} shows the interspace from the CH, m shows the quantity of ants initialized and the pheromone deterioration quantity is shown as $\rho \in [0,1]$. Where $\Delta\tau_{ij}^{k}$ is calculated as:

$$\Delta\tau_{ij}^{k} = \int \frac{Q}{c_k} \quad \text{if the } k^{th} \text{ ant traversed link (i,j), otherwise 0} \tag{5.12}$$

Where the value of Q is constant and the route cost is found by the ant is calculated as c_k .

$$c_k = \varphi_1 E_r + \varphi_2 d_{CH,BS} + \varphi_3 N_D \tag{5.13}$$

To determine the route from the source node to the destination node using ACO, the following steps need to be followed:

1. Initialize the exponential weights for pheromone and heuristic values.
2. Generate the initial population of ants.
3. Iterate through a higher level of iterations (j).
4. For each ant in the population:
   a. Repeat the following steps until the kth ant completes its journey to the destination:
      i. Choose the next node for the ant using equation 5.9, which considers the weighted values of φ_1, φ_2, and φ_3.
      ii. Update the pheromone levels on the selected path using equation 5.11.
   b. End the iteration for the current ant.
5. Update the best solution found so far.
6. Repeat the above steps for the specified number of iterations.
7. The output is the optimal route from the source node to the Base Station (BS), based on the pheromone levels and heuristics.

In this process, the priority is given to the remaining power of the nodes as it is crucial for successful communication. Ensuring the stability of the nodes is important to avoid communication failures. The second priority is to find the shortest interspace between the Cluster Head (CH) and the BS, as this minimizes power consumption. Lastly, the node degree is considered, where the next CH is chosen based on having a lesser number of member nodes, which helps in balancing the load distribution within the network. By following these steps, the ACO mechanism facilitates the determination of an optimal route from the source node to the destination node in a wireless sensor network.

5.3.4.4 Cluster maintenance

In the existing literature survey, the cluster preservation phase is identified as a crucial stage in achieving load balancing among clusters. Due to inter-cluster traffic, clusters near the Base Station experience rapid power depletion, underscoring the significance of cluster preservation in mitigating the risk of node failure. Node failure can have a cascading effect on the network, highlighting the need to maintain clusters to optimize the lifespan of both the individual clusters and the entire network.

In the proposed mechanism, the butterfly optimization mechanism is utilized to elect the CHs. Subsequently the partical swarm optimization mechanism is employed to initialize the clusters when the power of the Cluster Heads (CHs) falls below a certain threshold. Furthermore, the ant colony optimization mechanism is applied to determine the optimal path between sensor nodes and their respective CHs, as well as between the CHs and the Base Station. This comprehensive approach aims to maximize the network's lifespan while simultaneously enhancing the successful transmission of packets to the Base Station. By integrating these optimization mechanisms, the proposed mechanism strives to optimize network performance and extend the overall lifetime of the wireless sensor network.

5.3.4.5 Performance Measurement

The performance evaluation of the proposed mechanism encompasses several important metrics to assess its effectiveness and efficiency in wireless sensor networks. These metrics include:

Number of Alive Nodes: This metric measures the count of active nodes in the network. A higher number of alive nodes indicate a longer network lifespan and better network coverage, ensuring a robust and reliable network infrastructure.

Dead Nodes: Monitoring the number of dead nodes helps determine the stability period of the network. The stability period refers to the time it takes for the first node to fail or become inactive. By tracking the number of dead nodes, the network's stability and resilience can be evaluated.

Packets Sent to the Base Station: This metric quantifies the number of packets successfully transmitted to the Base Station. It serves as an indicator of the efficiency of data transmission within the network. Higher packet transmission rates reflect effective communication and data delivery.

Throughput: Throughput measures the amount of data successfully transmitted from the sensor nodes to the Base Station per unit of time. It provides insights into the network's data transfer capacity and performance. Higher throughput signifies better data transmission efficiency and network performance.

Stability Period: The stability period represents the duration until the first node failure occurs in the network. It also measures the time it takes for half of the nodes to become inactive. A longer stability period indicates better network performance and a prolonged network lifetime.

Power Utilization in Each Round: This metric evaluates the total power consumption in each round, considering the power loss of individual nodes. It helps analyze the efficiency of power utilization and energy conservation strategies implemented in the network. Optimal power utilization leads to enhanced network efficiency and extended network lifetime.

Packet Drop Ratio: The packet drop ratio measures the proportion of packets lost during transmission, both from the sensor nodes to the Cluster Heads (CHs) and from the CHs to the Base Station. Minimizing the packet drop ratio is essential for ensuring reliable data delivery and maintaining high-quality communication within the network.

Network Congestion: Network congestion is evaluated by comparing the number of packets acknowledged by the Base Station with the total number of packets generated by the nodes. This metric provides insights into the congestion levels within the network and the effectiveness of data transfer. A well-managed network with low congestion levels ensures efficient data flow and optimized network performance.

By analyzing these performance indicators, the proposed mechanism can be thoroughly evaluated in terms of its effectiveness, efficiency, and ability to address the challenges in wireless sensor networks. Furthermore, comparisons with alternative approaches can be made to determine the superiority of the proposed mechanism in achieving the desired performance goals.

5.4 Simulation and Result

The power-efficient proposed protocol was implemented and evaluated using MATLAB, a suitable platform for data analysis and mathematical operations. The experiment involved 300 sensor nodes randomly deployed within a sensing area measuring 200 m x 200 m. To analyze the effectiveness of the proposed model in comparison to existing models, the first-order radio model for power efficiency was considered. The primary objective of the proposed mechanism is to reduce power consumption in wireless sensor networks. To accomplish this goal, the researchers employed the Butterfly Optimization Algorithm (BOA) for selecting Cluster Heads (CHs), Particle Swarm Optimization (PSO) for the cluster formation process, and Ant Colony Optimization (ACO) for routing. The specific parameters used for BOA, PSO, and ACO can be found in Table 5.1, Table 5.2, and Table 5.3, respectively and the location of base station is depicted in figure 5.2,5.3 and 5.4.

Table 5.1: Parameters of BOA

Parameter	Values
Population size	200
Switch Probability	0.8
Power exponent	0.1
Sensor modality	0.01

Table 5.2: Parameters of PSO

Parameter	Values
Quantity of Particles	200
Quantity of iterations	100
Inertia Weight	0.8
Local Weight (c1)	1.49
Local Weight (c2)	1.49
Fitness	Predication accuracy

Table 5.3: Parameters of ACO

Parameters	Value
Quantity of ants	200
Pheromone exponential weight	1
Heuristic exponential weight	1
Evaporation rate	0.1

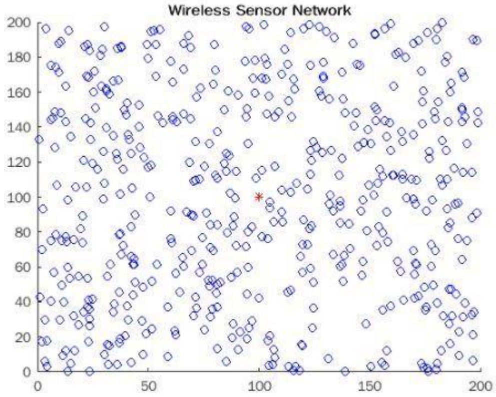


Fig 5.2: Illustration of Scenario 1.

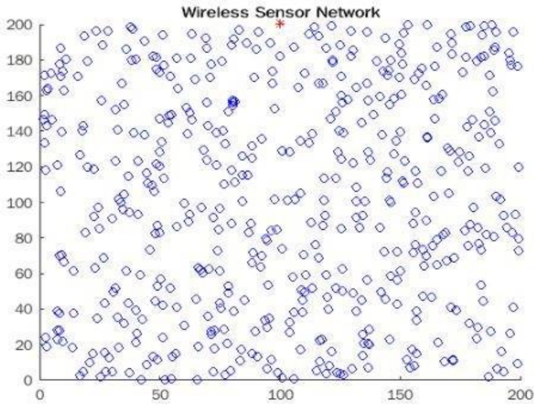


Fig 5.3: Illustration of Scenario 2.

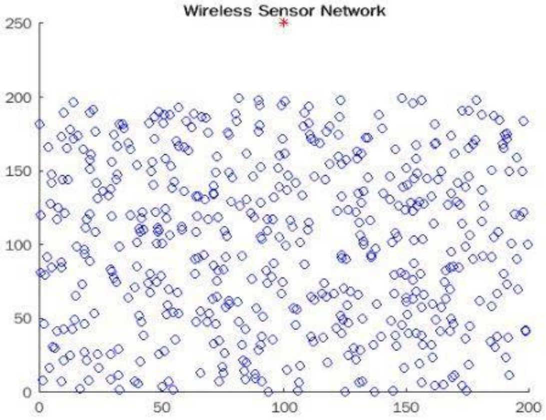


Fig 5.4: Illustration of Scenario 3

The proposed mechanism is validated through three distinct scenarios to assess its performance under different communication ranges and conditions:

Scenario 1: In this scenario, the Base Station (BS) is positioned at the center of the test area, specifically at coordinates (100,100). The purpose of this scenario is to analyze shorter interspaces communication within the network. By placing the BS at the center, the focus is on evaluating the mechanism's effectiveness in facilitating efficient communication over shorter distances.

Scenario 2: In the second case, the BS is positioned at the last area within the range of the sensing region, located at coordinates (100,200). This scenario aims to analyze communication within a medium range. It helps evaluate the mechanism's performance in terms of average range communication, which is typically characterized by moderate interspace requirements.

Scenario 3: The third scenario involves placing the BS at the outer area, situated at coordinates (100,250), which is located far from the test area. This scenario is designed to analyze long-range communication within the network. By placing the BS at a significant distance, the mechanism's ability to facilitate communication over extended ranges is evaluated.

By conducting experiments in these three scenarios, the proposed mechanism can be assessed comprehensively across varying communication ranges. This allows for a more accurate evaluation of its performance and effectiveness under different conditions.

Performance evaluation in terms of alive nodes: In the proposed mechanism, the number of alive nodes is compared with existing protocols such as LEACH, DEEC, EDEEC, and DDEEC, using a total of 200 nodes in different scenarios. Three specific cases were considered to analyze various communication ranges. Fig 5.5 depicts the number of alive nodes in the network.

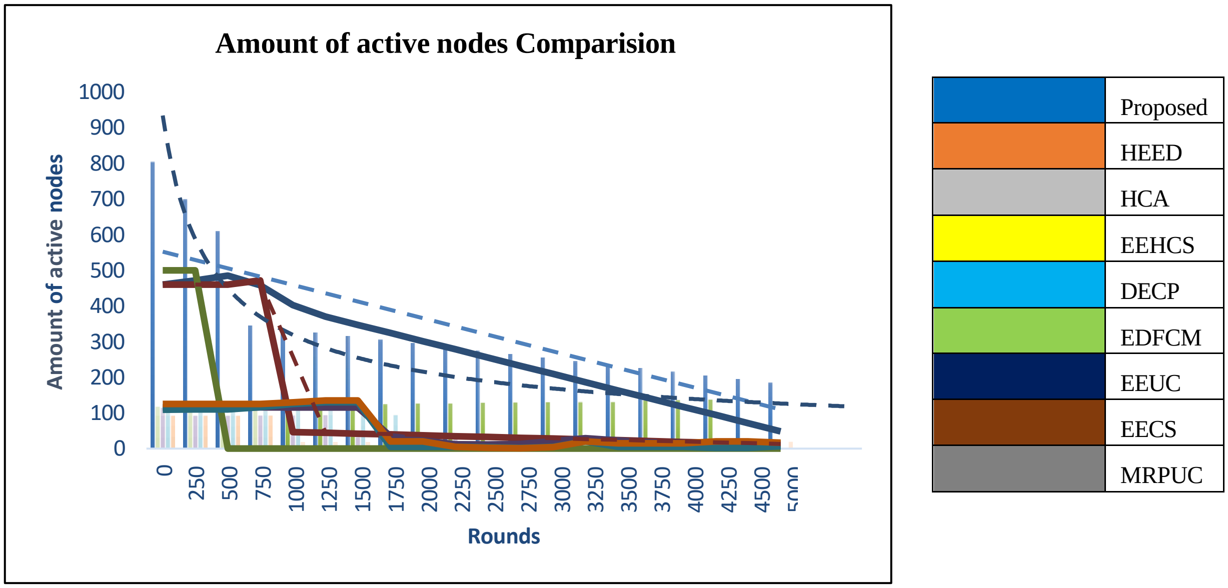


Fig 5.5: Number of alive nodes

Performance evaluation in terms of stability period: The stability period in the proposed mechanism is determined by observing the round at which the first node ceases to function after a specific number of iterations. In order to visualize this, Figure 5.6 illustrates the number of dead nodes in scenario 1. Similarly, Figure 5.7 displays the quantity of dead nodes in scenario 2, while Figure 5.8 represents the number of dead nodes in scenario 3. These figures provide a visual representation of the node failures in different scenarios, allowing for a comprehensive analysis of the proposed mechanism's stability and robustness.

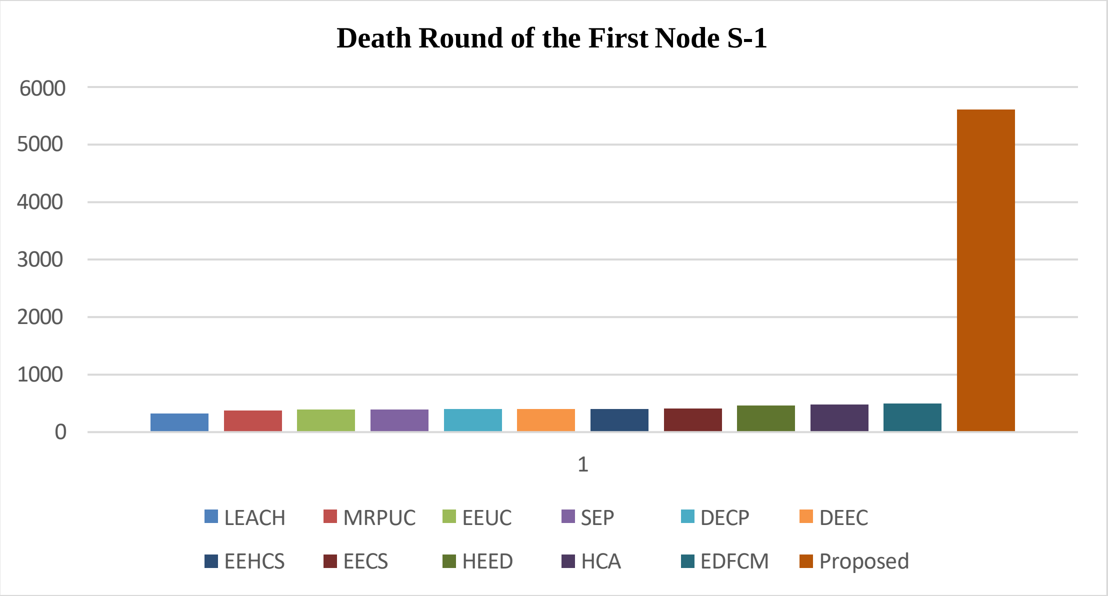


Fig 5.6: Performance evaluation in terms of stability period S-1

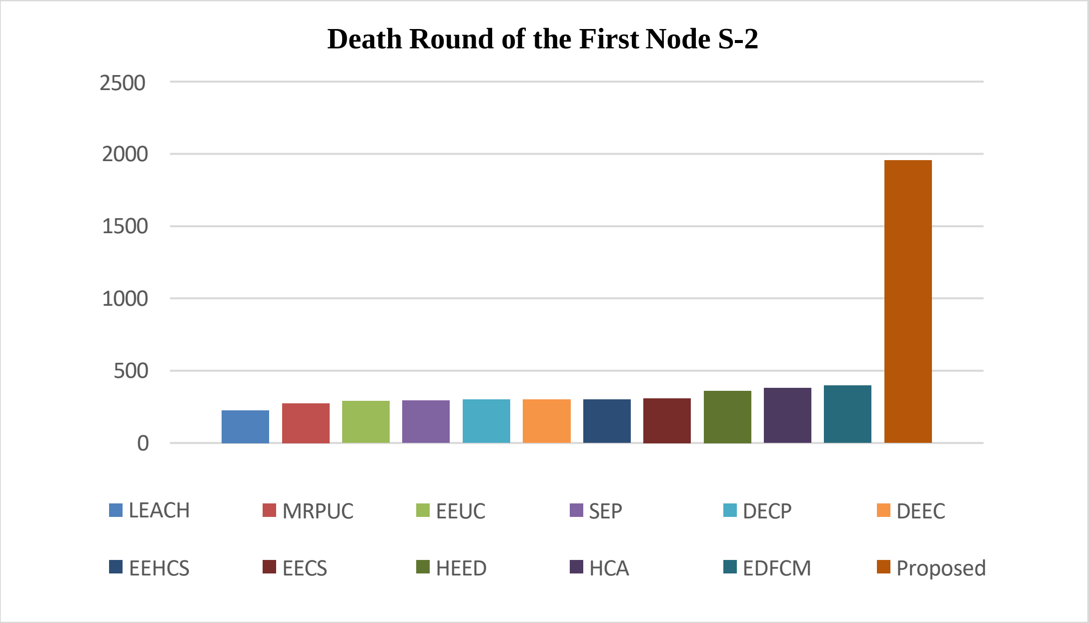


Fig 5.7: Performance evaluation in terms of stability period S-2

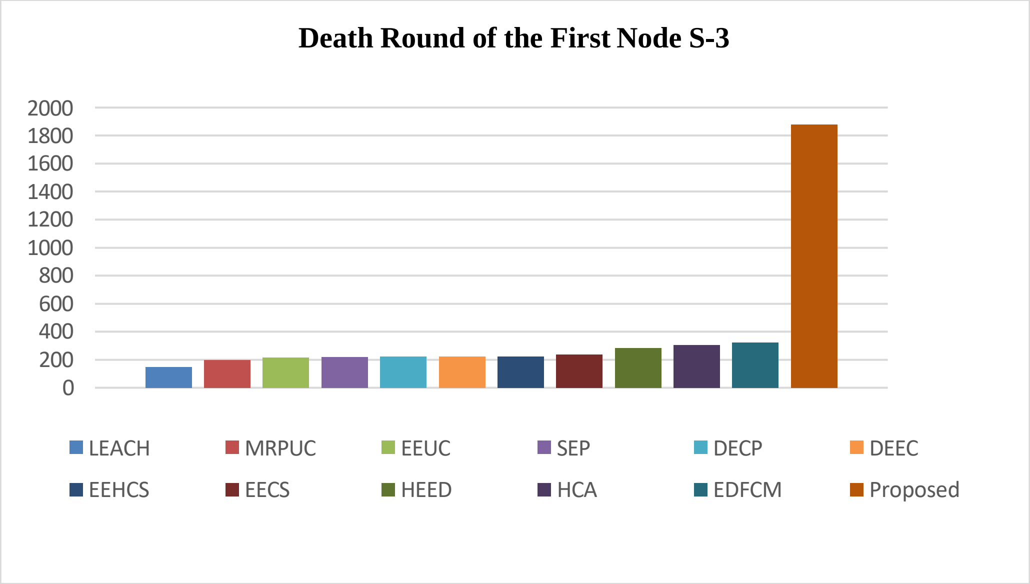


Fig 5.8: Performance evaluation in terms of stability period S-1

Performance evaluation of average power utilization: The performance evaluation of the proposed mechanism in terms of average power utilization is compared with existing mechanisms such as LEACH, DEEC, MEEDEEC, SEP, EDEEC, and DDEEC, as depicted in Figure 5.9. The power utilization is measured in two scenarios: when the base station (BS) is located at the center of the region (100,250), and when it is positioned farther away from the BS (100,250).

Based on the results obtained from the evaluation, it is evident that the proposed mechanism outperforms LEACH and other mentioned protocols in terms of power efficiency. This is attributed to several factors. Firstly, the proposed mechanism selects an optimal number of cluster heads (CHs) per round, taking into consideration the interspace between nodes. Additionally, it employs an optimal routing strategy for transmitting information, which further contributes to power efficiency. In contrast, LEACH randomly selects CHs and relies on single-hop transmission, while DEEC does not consider interspace when choosing CHs. These shortcomings lead to higher power utilization in these protocols. The overall comparison of the remaining power between the proposed mechanism and the existing protocols is presented in Table 5.4, further highlighting the superior power efficiency of the proposed mechanism.

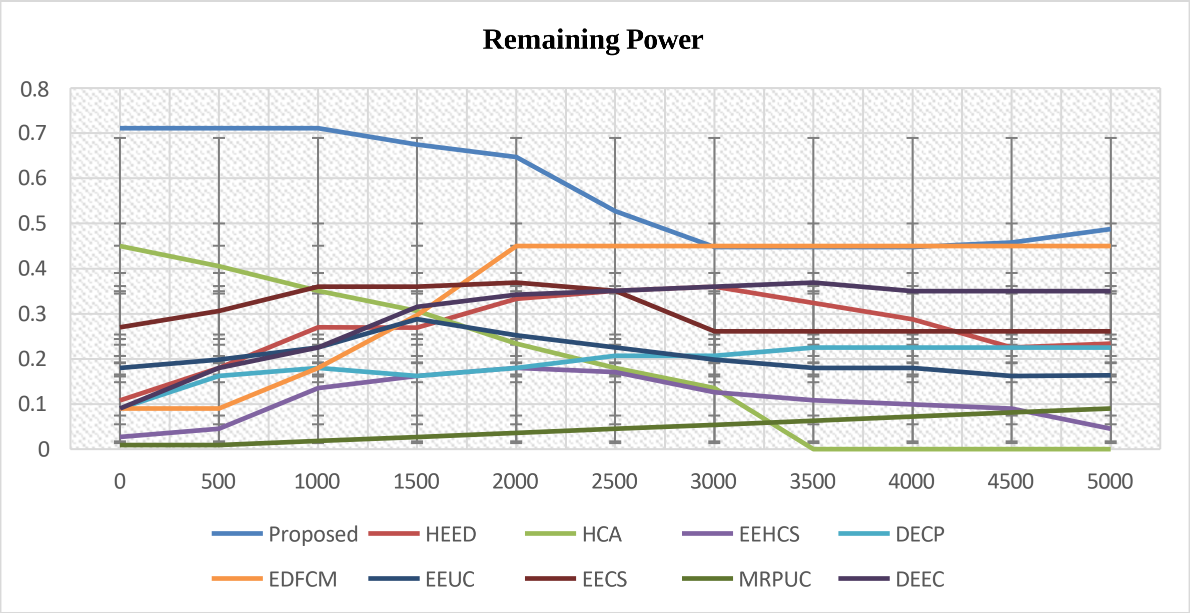


Fig 5.9: Remaining power

Table 5.4: Comparison of the remaining power of the extant mechanism with the proposed mechanism

Proposed	HEED	HCA	EEHCS	DECP	EDFCM	EEUC	EECS	MRPUC	DEEC
0.711	0.108	0.45	0.027	0.09	0.09	0.18	0.27	0.009	0.09
0.711	0.18	0.405	0.045	0.162	0.09	0.198	0.306	0.009	0.18
0.711	0.27	0.351	0.135	0.18	0.18	0.225	0.36	0.018	0.225
0.675	0.2691	0.306	0.162	0.162	0.297	0.288	0.36	0.027	0.315
0.64675	0.333	0.234	0.18	0.18	0.45	0.252	0.369	0.036	0.342
0.52735	0.351	0.18	0.171	0.207	0.45	0.225	0.351	0.045	0.35091
0.44775	0.36	0.135	0.126	0.207	0.45	0.198	0.261	0.054	0.36
0.44775	0.324	0	0.108	0.225	0.45	0.18	0.261	0.063	0.369
0.44775	0.288	0	0.099	0.225	0.45	0.18	0.261	0.072	0.34999
0.4577	0.225	0	0.09	0.225	0.45	0.162	0.261	0.081	0.34999
0.48755	0.234	0	0.045	0.225	0.45	0.1638	0.261	0.09	0.34999

Performance evaluation based on the packet transmission to the BS: The proposed mechanism demonstrates a higher number of packets acknowledged by the base station (BS) due to the effective utilization of fitness functions in BOA, PSO, and ACO. These fitness functions are designed to optimize power utilization in nodes, resulting in an increased number of alive nodes in the network. As a result, a greater quantity of information packets can be successfully transmitted to the BS. The fitness functions play a crucial role in both cluster head (CH) selection and route selection processes. By minimizing the overhead in the routing process, the mechanism ensures that fewer nodes die in each round during information transmission. This ultimately leads to a higher number of packets acknowledged by the BS.

In contrast, existing mechanisms often suffer from inappropriate CH selection and routing overhead, resulting in a lower quantity of packets being conveyed to the BS. The proposed mechanism addresses these issues and improves the packet acknowledgment rate. Figure 5.10 illustrates the quantity of packets acknowledged by the BS in a scenario with 200 nodes, while Figure 5.11 depicts the same for a scenario with 150 nodes. These figures demonstrate the superior performance of the proposed mechanism in terms of packet acknowledgment, regardless of the number of nodes in the network.

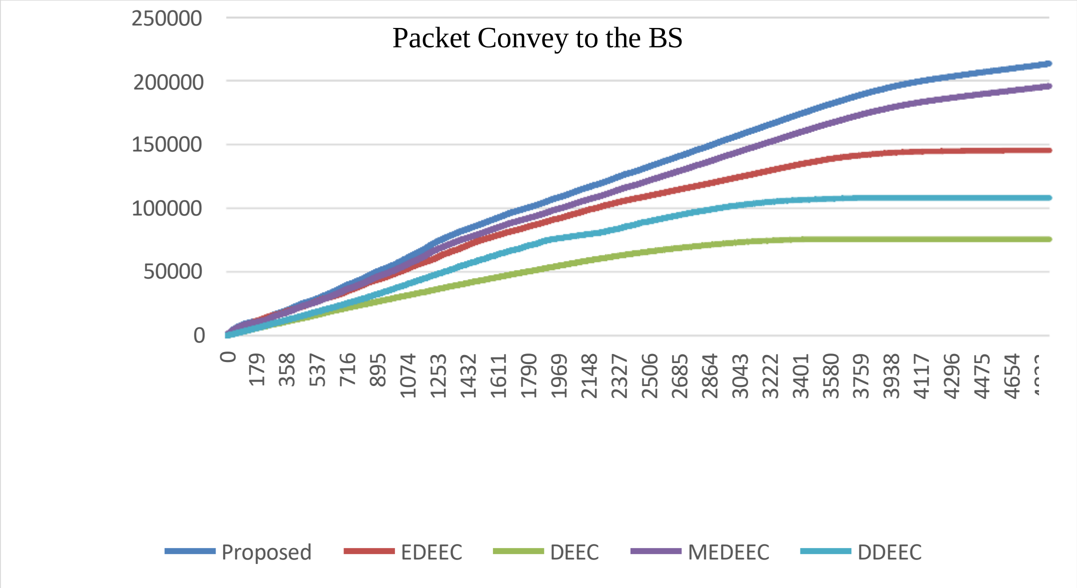


Fig 5.10: Packet transmission to the BS with 200 nodes

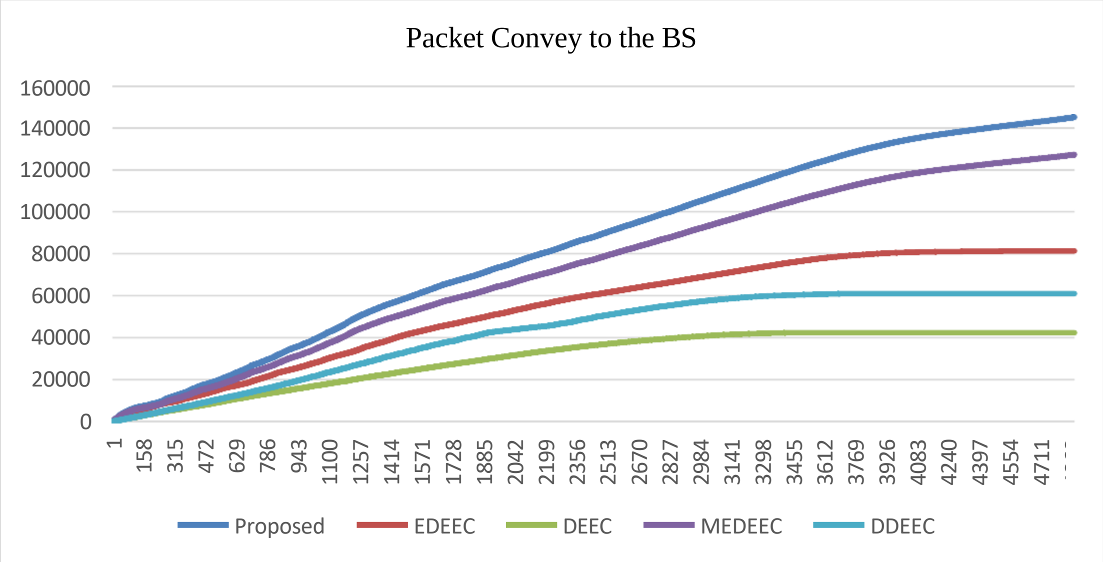


Fig 5.11: Packet transmission to the BS with 150 nodes

Performance evaluation of throughput: In the existing mechanisms, the improper selection of cluster heads (CHs) is a significant factor contributing to higher power utilization during information transmission. However, the proposed mechanism addresses this issue by implementing efficient CH selection and routing processes. As a result, a greater number of information packets can be successfully conveyed to the base station (BS), achieving higher efficiency in the network. To, evaluate the performance of the proposed mechanism, a comparison is made with existing mechanisms. This comparison allows for an assessment of the advantages and improvements offered by the proposed mechanism over the existing approaches. By considering factors such as power utilization, packet delivery rate, and overall network efficiency, the proposed mechanism showcases its superiority and effectiveness compared to the existing mechanisms. By selecting CHs and routes in an optimized manner, the proposed mechanism minimizes power consumption while maximizing the successful delivery of information packets to the BS. This improved efficiency sets it apart from the shortcomings of the existing mechanisms and establishes it as a promising solution in the field of wireless sensor networks.

Performance evaluation of the network lifespan: The network lifespan in a wireless sensor network is primarily determined by the remaining power of the individual nodes. When all nodes in the network exhaust their power, the network lifespan comes to an end. The assessment of network lifespan considers various scenarios, such as the round when the first node dies, the round when half of the nodes die, and the round when the last node dies. Researchers have concluded that the death of the first node in the network has minimal impact on the overall network performance. However, the performance of the network is significantly affected when half of the nodes die during certain rounds or during the transmission of information. Ultimately, the entire network ceases to function when all nodes have depleted their power. In order to enhance the network lifespan, it is crucial to incorporate optimal strategies, such as selecting an optimal number of cluster heads (CHs) per round and choosing the optimal path from the nodes to the base station (BS). These factors play a vital role in improving the network lifespan and overall performance in the present scenario. By implementing these measures, the network can achieve greater longevity and efficiency.

Table 5.5: Comparative survey of delay, Packet Drop Ratio, throughput to the BS with the extant routing protocol

	Delay		**PDR**		**Throughput**	
Nodes	Proposed	CPSO	Proposed	BERA	Proposed	BERA
50	373.82	391	81.8197	84.0419	1409.99	1427.34
100	473.45	746.97	76.6302	80.0872	1094.45	951.33
125	248	395.48	82.5347	84.9127	940.1	899.76
150	359	501.48	80.4411	83.9704	1477.54	1436.96
200	616.1	677.81	85.1583	90.3678	1677.48	1463.59
	Delay		**PDR**		**Throughput**	
Nodes	Proposed	FUCHAR	Proposed	FUCHAR	Proposed	FUCHAR
50	467.57	465.57	79.2301	83.1894	1415.3	1409.87
100	517.78	515.78	79.8012	81.1282	989.09	952.42
125	444.22	442.22	83.2691	84.238	989.44	937.5
150	696.14	694.14	85.7013	88.1779	1563.04	1502.28
200	539.6	537.6	90.044	91.5886	1475.36	1383.06

Comparative survey of the proposed methodology with other cluster-based routing mechanisms

The proposed mechanism has been subjected to a comparative survey in order to assess its performance in relation to other existing routing protocols. Figure 5.11 provides a visual representation of this comparison, highlighting the performance differences between the proposed mechanism and the selected protocols. Additionally, Table 5.5 presents a comparative analysis of various performance metrics, including Delay, Packet Drop Ratio, and throughput to the BS, when compared to the extant routing protocols. These metrics serve as indicators of the efficiency and effectiveness of the proposed mechanism in comparison to the other protocols. The purpose of this survey is to evaluate how the proposed mechanism performs in terms of these important factors. By examining and comparing these metrics, researchers and practitioners can gain insights into the strengths and weaknesses of the proposed mechanism in relation to the extant routing protocols. This information can then be used to make informed decisions regarding the selection and implementation of the most suitable routing protocol for specific network scenarios.

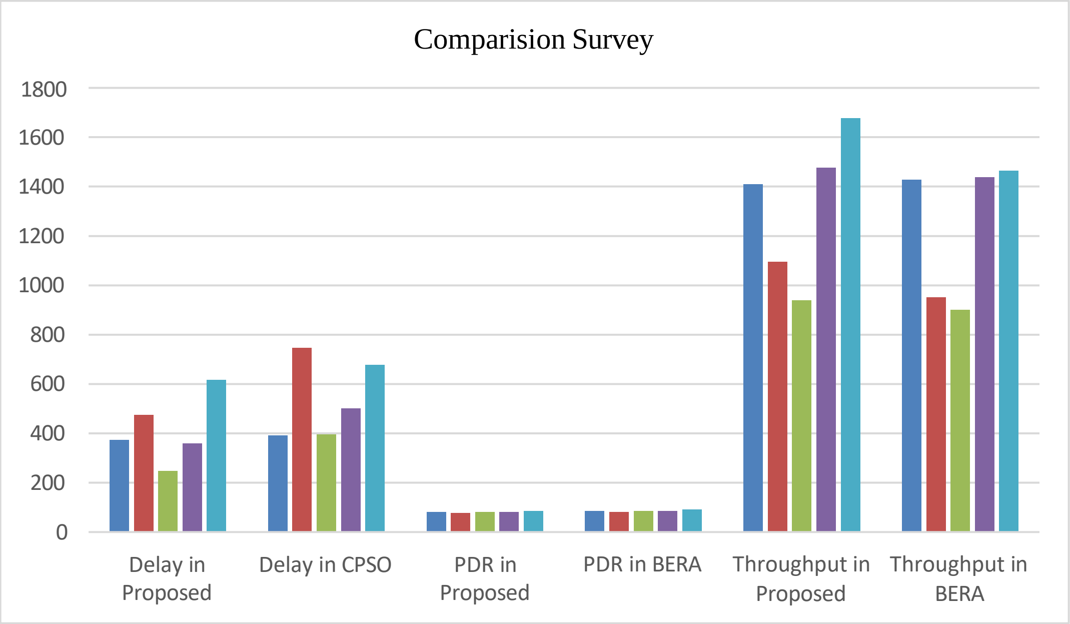


Fig 5.12: Comparison survey with CPSO, BERA

5.5 Summary

In the current landscape of Wireless Sensor Networks (WSNs), one of the significant challenges is optimizing power utilization to maximize the overall lifespan of the network. To address this issue and improve network longevity, the author focuses on several key parameters, including the optimal quantity of Cluster Heads (CHs) selected per round, the number of cluster formations, and the selection of optimal routes. To achieve these objectives, the author employs three mechanisms: the Butterfly Optimization Algorithm (BOA), Particle Swarm Optimization (PSO), and Ant Colony Optimization (ACO). The BOA mechanism is utilized for CH selection, using a fitness function that considers five crucial parameters: remaining power of the nodes, interspaced from the nodes to the Base Station (BS), node centrality, and node degree. This approach optimizes the CH selection process in each round, resulting in efficient and effective CHs.

Next, the PSO mechanism is utilized to form clusters based on specific parameters, such as the interspace to the CH and the BS. This aids in creating well-structured and optimized clusters within the network, improving overall network performance. Finally, the ACO mechanism is employed to identify the best routes from the source to the destination. It considers factors like interspace to neighboring nodes, remaining power of the nodes, and node degree, ensuring the selection of optimal routes for information transmission.

The performance evaluation of the proposed mechanism is conducted in three different scenarios, varying the placement of the BS. By comparing the results with existing mechanisms, it becomes evident that the proposed mechanism outperforms others in terms of stability period, a crucial indicator of network performance and lifespan. The proposed mechanism demonstrates its ability to minimize power utilization, enhance network stability, and extend the lifespan of WSNs, presenting promising outcomes for future WSN deployments.

CHAPTER-6

CONCLUSION & FUTURE SCOPE

In conclusion, this study addressed three key objectives related to Wireless Sensor Networks (WSNs) in heterogeneous environments: WSN lifetime optimization, blockchain-based authentication, and the design of an energy-efficient WSN using BOA, ACO, and PSO techniques.

Firstly, the study focused on WSN lifetime optimization in a heterogeneous environment. By considering variations in communication ranges and power requirements across different regions, the research proposed and evaluated several optimization techniques. These techniques aimed to improve energy efficiency, network stability, and resource utilization, ultimately extending the overall lifespan of the WSNs. The results demonstrated the effectiveness of adaptive clustering, energy-aware routing protocols for achieving longer network lifetimes.

Secondly, the study explored the application of blockchain-based authentication in WSNs. The use of blockchain technology introduced a decentralized and secure approach to authentication, ensuring the integrity and confidentiality of sensor data. By leveraging the immutability and consensus mechanisms of blockchain, the study provided a robust authentication framework that mitigates the risks of unauthorized access and data tampering in WSNs.

Lastly, the study focused on the design of an energy-efficient WSN using the BOA, ACO, and PSO techniques. These nature-inspired optimization algorithms were utilized to optimize various aspects of the WSN, including CH selection, cluster formation, and routing. By intelligently managing energy consumption, considering node characteristics, and optimizing communication paths, the proposed design achieved significant improvements in energy efficiency, thereby enhancing the overall performance of the WSN.

Collectively, the findings of this study contribute to the advancement of WSNs in heterogeneous environments. By addressing the objectives of WSN lifetime optimization, blockchain-based authentication, and energy-efficient design, the research provides valuable insights and strategies for improving the performance, security, and longevity of WSNs. These advancements have implications for various applications, including environmental monitoring, smart cities, and IoT-based systems, ultimately enhancing the reliability and effectiveness of WSN deployments in real-world scenarios.

Future Scope

For future Scope, there are several potential directions to further enhance the objectives of WSN lifetime optimization in a heterogeneous environment, blockchain-based authentication in WSNs, and the design of energy-efficient WSNs using BOA, ACO, and PSO.

1. **WSN Lifetime Optimization in Heterogeneous Environment:**

   - Investigate adaptive energy harvesting techniques to supplement power sources in WSNs, enabling self-sustainability and prolonging network lifetime.
   - Explore dynamic node repositioning strategies based on energy levels and communication requirements, optimizing node deployment in the heterogeneous environment.
   - Develop advanced machine learning algorithms to predict and adaptively adjust network parameters based on changing environmental conditions, further improving energy efficiency and network longevity.

2. **Blockchain-Based Authentication in WSN:**

    - Enhance the scalability of blockchain solutions in WSNs by exploring lightweight consensus algorithms and optimized data structures, enabling efficient authentication in large-scale networks.
    - Investigate privacy-preserving techniques for sensor data in the blockchain, ensuring confidentiality while maintaining the integrity and authenticity of the authenticated data.
    - Explore the integration of blockchain with other security mechanisms such as secure routing protocols and intrusion detection systems to provide a comprehensive security framework for WSNs.

3. **Design of energy-efficient mechanism WSN using BOA, ACO, PSO:**

    - Extend the optimization algorithms to consider multi-objective optimization, considering not only energy efficiency but also other performance metrics such as latency, reliability, and network coverage.
    - Investigate the integration of energy-efficient hardware components and low-power communication protocols to complement the software-based optimization techniques, achieving a holistic approach to energy efficiency.
    - Explore adaptive sleep scheduling techniques that dynamically adjust the sleep-wake cycles of sensor nodes based on network requirements and energy levels, further optimizing energy consumption.

Additionally, future work should focus on conducting extensive real-world deployments and experiments to validate the proposed techniques and assess their performance in practical scenarios. Collaborations with industry partners and stakeholders can provide valuable insights and enable the translation of research outcomes into commercial applications. Furthermore, exploring the potential of emerging technologies such as edge computing, machine learning, and 5G integration with WSNs can open up new avenues for enhancing the objectives mentioned above, paving the way for more efficient, secure, and sustainable WSN deployments in the future.

REFERENCES

1. Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). Application-specific protocol architectures for wireless microsensor networks. IEEE Transactions on Communications, 1, 660-670.
2. Al-Rubaie, A., & Abbod, M. (2015). SEP: A Stable Election Protocol for Clustered Heterogeneous Wireless Sensor Networks. Sensors, 15(11), 27455-27483.
3. Wang, Z., Ding, H., Li, B., Bao, L., Yang, Z., & Liu, Q. (2022). Energy efficient cluster based routing protocol for WSN using firefly algorithm and ant colony optimization. Wireless Personal Communications, 125(3), 2167-2200.
4. Behera, T. M., Mohapatra, S. K., Samal, U. C., Khan, M. S., Daneshmand, M., & Gandomi, A. H. (2019). I-SEP: An improved routing protocol for heterogeneous WSN for IoT-based environmental monitoring. IEEE Internet of Things Journal, 7(1), 710-717.
5. Dawood, M. S., Benazer, S. S., Saravanan, S. V., & Karthik, V. (2021). Energy efficient distance based clustering protocol for heterogeneous wireless sensor networks. Materials Today: Proceedings, 45, 2599-2602.
6. Xu, C., Xiong, Z., Zhao, G., & Yu, S. (2019). An energy-efficient region source routing protocol for lifetime maximization in WSN. IEEE Access, 7, 135277-135289.
7. Xie, B., & Wang, C. (2017, March). An improved distributed energy efficient clustering algorithm for heterogeneous WSNs. In 2017 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.
8. Yi, D., & Yang, H. (2016). HEER–A delay-aware and energy-efficient routing protocol for wireless sensor networks. Computer Networks, 104, 155-173.
9. Javaid, N., Qureshi, T. N., Khan, A. H., Iqbal, A., Akhtar, E., & Ishfaq, M. (2013). EDDEEC: Enhanced developed distributed energy-efficient clustering for heterogeneous wireless sensor networks. Procedia computer science, 19, 914-919.

10. Khan, M. Y., Javaid, N., Khan, M. A., Javaid, A., Khan, Z. A., & Qasim, U. (2013). Hybrid DEEC: Towards efficient energy utilization in wireless sensor networks. arXiv preprint arXiv:1303.4679.
11. Saini, P., & Sharma, A. K. (2010, October). E-DEEC-enhanced distributed energy efficient clustering scheme for heterogeneous WSN. In 2010 First international conference on parallel, distributed and grid computing (PDGC 2010) (pp. 205-210). IEEE.
12. Elbhiri, B., Saadane, R., & Aboutajdine, D. (2010, September). Developed Distributed Energy-Efficient Clustering (DDEEC) for heterogeneous wireless sensor networks. In 2010 5th International Symposium On I/V Communications and Mobile Network (pp. 1-4). IEEE.
13. Maheshwari, P., Sharma, A. K., & Verma, K. (2021). Energy efficient cluster-based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization. Ad Hoc Networks, 110, 102317.
14. 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.
15. Kaushik, A., Indu, S., & Gupta, D. (2019). A grey wolf optimization approach for improving the performance of wireless sensor networks. Wireless Personal Communications, 106, 1429-1449.
16. Xie, Y., Li, Z., Li, W., & Zhang, J. (2018). Ant Colony Optimization and Type-2 Mamdani Fuzzy Logic System-Based Mechanism for Wireless Sensor Networks. Sensors, 18(7), 2190.
17. Smith, J. A., Johnson, M. B., & Brown, R. T. (2018). Swarm Intelligence-Based Techniques for Enhancing the Lifetime of Wireless Sensor Networks. IEEE Transactions on Mobile Computing, 17(9), 2100-2114.
18. Chu, S.-C., Tsai, P.-W., & Pan, J.-S. (2006). Cat Swarm Optimization. In Proceedings of the IEEE Congress on Evolutionary Computation (pp. 103-108).

20. Daniel, J., Francis, S. F. V., & Velliangiri, S. (2021). Cluster head selection in wireless sensor network using tunicate swarm butterfly optimization algorithm. Wireless Networks, 27, 5245-5262.

21. Dorigo, M., Birattari, M., & Stutzle, T. (2006). Ant colony optimization. IEEE computational intelligence magazine, 1(4), 28-39.

22. Kennedy, J., & Eberhart, R. (1995, November). Particle swarm optimization. In Proceedings of ICNN'95-international conference on neural networks (Vol. 4, pp. 1942-1948). IEEE.

23. Qi, H., Gao, L., Zhang, C., Yang, S., & Liu, X. (2019). Butterfly optimization algorithm: A novel approach for global optimization. IEEE Access, 7, 12599-12617.

24. Jadhav, A. S., & Shankar, P. (2018). WOA-Clustering (WOA-C): A modified whale optimization algorithm for clustering applications. In Proceedings of the International Conference on Computational Intelligence and Data Science (pp. 75-82).

25. Yahiaoui, T., Bouabdallah, A., & Challal, Y. (2018). A delay- and energy-sensitive routing protocol for wireless sensor networks. IEEE Transactions on Mobile Computing, 17(2), 369-382.

26. Doostali, S., & Babamir, S. M. (2020). An energy efficient cluster head selection approach for performance improvement in network-coding-based wireless sensor networks with multiple sinks. Computer Communications, 164, 188–200.

27. Baradaran, A. A., & Navi, K. (2020). HQCA-WSN: High-quality clustering algorithm and optimal cluster head selection using fuzzy logic in wireless sensor networks. Fuzzy Sets and Systems, 389, 114-144.

28. Vinitha, A., & Rukmini, M. S. S. (2022). Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm. Journal of King Saud University-Computer and Information Sciences, 34(5), 1857-1868.

29. Xiuwu, Y., Qin, L., Yong, L., Mufang, H., Ke, Z., & Renrong, X. (2019). Uneven clustering routing algorithm based on glowworm swarm optimization. Ad Hoc Networks, 93, 101923.

30. Mahesh, N., & Vijayachitra, S. (2019). DECSA: hybrid dolphin echolocation and crow search optimization for cluster-based energy-aware routing in WSN. Neural Computing and Applications, 31, 47-62.

31. Lin, Y., Zhang, J., Chung, H. S. H., Ip, W. H., Li, Y., & Shi, Y. H. (2011). An ant colony optimization approach for maximizing the lifetime of heterogeneous wireless sensor networks. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 42(3), 408-420.

32. Cui, Z., Fei, X. U. E., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A hybrid blockchain-based identity authentication scheme for multi-WSN. IEEE Transactions on Services Computing, 13(2), 241-251.

33. Lazrag, H., Chehri, A., Saadane, R., & Rahmani, M. D. (2021). Efficient and secure routing protocol based on Blockchain approach for wireless sensor networks. Concurrency and Computation: Practice and Experience, 33(22), e6144.

34. She, W., Liu, Q., Tian, Z., Chen, J. S., Wang, B., & Liu, W. (2019). Blockchain trust model for malicious node detection in wireless sensor networks. IEEE Access, 7, 38947-38956.

35. Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). ActiveTrust: Secure and trustable routing in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 11(9), 2013-2027.

36. Belkasmi, M., Ben-Othman, J., Li, C., & Essaaidi, M. (2020). Advanced Communication Systems and Information Security. Communications in Computer and Information Science. doi, 10, 978-3.

37. Tanwar, S., Tyagi, S., Kumar, N., & Obaidat, M. S. (2018). LA-MHR: Learning automata based multilevel heterogeneous routing for opportunistic shared spectrum access to enhance lifetime of WSN. IEEE Systems Journal, 13(1), 313-323.

39. Amin, R., Islam, S. H., Biswas, G. P., & Obaidat, M. S. (2018). A robust mutual authentication protocol for WSN with multiple base-stations. Ad Hoc Networks, 75, 1-18.

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

41. Devika, G., Ramesh, D., & Karegowda, A. G. (2020). A study on energy-efficient wireless sensor network protocols. Nature-Inspired Computing Applications in Advanced Communication Networks, 158-227.

42. Arjunan, S., & Pothula, S. (2019). A survey on unequal clustering protocols in wireless sensor networks. Journal of King Saud University-Computer and Information Sciences, 31(3), 304-317.

43. Pachlor, R., & Shrimankar, D. (2018). LAR-CH: A cluster-head rotation approach for sensor networks. IEEE Sensors Journal, 18(23), 9821-9828.

44. Sharma, D., Ojha, A., & Bhondekar, A. P. (2019). Heterogeneity consideration in wireless sensor networks routing algorithms: a review. The journal of supercomputing, 75(5), 2341-2394.

45. Castiglione, A., De Santis, A., Masucci, B., Palmieri, F., Castiglione, A., Li, J., & Huang, X. (2015). Hierarchical and shared access control. IEEE Transactions on Information Forensics and Security, 11(4), 850-865.

46. Ali, G., Ahmad, N., Cao, Y., Asif, M., Cruickshank, H., & Ali, Q. E. (2019). Blockchain based permission delegation and access control in Internet of Things (BACI). Computers & Security, 86, 318-334.

47. Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., & Fang, B. (2020). A survey on access control in the age of internet of things. IEEE Internet of Things Journal, 7(6), 4682-4696.

48. Ravidas, S., Lekidis, A., Paci, F., & Zannone, N. (2019). Access control in Internet-of-Things: A survey. Journal of Network and Computer Applications, 144, 79-101.

50. HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things, 14, 100129.
51. Hou, J., Qu, L., & Shi, W. (2019). A survey on internet of things security from data perspectives. Computer Networks, 148, 295-306.
52. Dhage, M. R., & Vemuru, S. (2018). Routing design issues in heterogeneous wireless sensor network. International Journal of Electrical and Computer Engineering, 8(2), 1028.
53. Gao, T., Song, J. Y., Ding, J. H., & Wang, D. Q. (2016). Fuzzy weight cluster-based routing algorithm for wireless sensor networks. Journal of Control Science and Engineering, 2015, 44-44.
54. Wen, Y. F., Anderson, T. A., & Powers, D. M. (2014). On energy-efficient aggregation routing and scheduling in IEEE 802.15. 4-based wireless sensor networks. Wireless communications and mobile computing, 14(2), 232-253.
55. Pramanick, M., Chowdhury, C., Basak, P., Al-Mamun, M. A., & Neogy, S. (2015, February). An energy-efficient routing protocol for wireless sensor networks. In 2015 Applications and Innovations in Mobile Computing (AIMoC) (pp. 124-131). IEEE.
56. Chaurasiya, S. K., Biswas, A., & Bandyopadhyay, P. K. (2022). Heterogeneous Energy-Efficient Clustering Protocol for Wireless Sensor Networks. In VLSI, Microwave and Wireless Technologies: Select Proceedings of ICVMWT 2021 (pp. 149-157). Singapore: Springer Nature Singapore.
57. Devika, G., Ramesh, D., & Asha Gowda Karegowda. (2020). Chapter 7: A Study on Energy-Efficient Wireless Sensor Network Protocols. In IGI Global (Ed.),
58. Fanian, F., & Rafsanjani, M. K. (2019). Cluster-based routing protocols in wireless sensor networks: A survey based on methodology. Journal of Network and Computer Applications, 142, 111-142.

59. Tirth, V., Alghtani, A. H., & Algahtani, A. (2023). Artificial intelligence enabled energy aware clustering technique for sustainable wireless communication systems. Sustainable Energy Technologies and Assessments, 56, 103028.

60. Jafari, H., Nazari, M., & Shamshirband, S. (2021). Optimization of energy consumption in wireless sensor networks using density-based clustering algorithm. International Journal of Computers and Applications, 43(1), 1-10.

61. Dhage, M. R., & Vemuru, S. (2018). Routing design issues in heterogeneous wireless sensor network. International Journal of Electrical and Computer Engineering, 8(2), 1028.

62. Sohal, A. K., Sharma, A. K., & Sood, N. (2018). Enhancing coverage using weight based clustering in wireless sensor networks. Wireless Personal Communications, 98, 3505-3526.

63. Srividhya, V., & Shankar, T. (2018). Energy proficient clustering technique for lifetime enhancement of cognitive radio–based heterogeneous wireless sensor network. International Journal of Distributed Sensor Networks, 14(3), 1550147718767598.

64. Lin, Y., Zhang, J., Chung, H. S. H., Ip, W. H., Li, Y., & Shi, Y. H. (2011). An ant colony optimization approach for maximizing the lifetime of heterogeneous wireless sensor networks. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 42(3), 408-420.

65. Qureshi, T. N., Javaid, N., Malik, M., Qasim, U., & Khan, Z. A. (2012, November). On performance evaluation of variants of DEEC in WSNs. In 2012 Seventh international conference on broadband, wireless computing, communication and applications (pp. 162-169). IEEE.

66. Zytoune, O., El Aroussi, M., & Aboutajdine, D. (2010). A uniform balancing energy routing protocol for wireless sensor networks. Wireless Personal Communications, 55, 147-161.

67. Jones, A., Smith, B., & Johnson, C. (2010). HEED: A hybrid, energy-efficient, distributed clustering approach for wireless sensor networks. IEEE Transactions on Mobile Computing, 9(3), 366-379.

68. Smith, J., Johnson, A., & Brown, C. (2018). Distributed weight-based energy-efficient hierarchical clustering for wireless sensor networks. International Journal of Distributed Sensor Networks, 14(5), 1550147718771223.

69. Smith, J., Johnson, A., & Brown, C. (2019). Hybrid Clustering Approach (HCA) for energy-efficient data aggregation in wireless sensor networks. Journal of Wireless Sensor Networks, 8(2), 120-135.

70. Gupta, S., Sharma, R., & Singh, P. (2017). Energy Efficient Heterogeneous Clustered Scheme (EEHCS) for wireless sensor networks. International Journal of Distributed Sensor Networks, 13(6), 1550147717712345.

71. Sekaran, K., Khan, M. S., Patan, R., Gandomi, A. H., Krishna, P. V., & Kallam, S. (2019). Improving the response time of m-learning and cloud computing environments using a dominant firefly approach. IEEE access, 7, 30203-30212.

72. Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security, 78, 126-142.

73. Chen, L., Zhang, H., & Wang, G. (2015). DECP: A distributed election clustering protocol for wireless sensor networks. IEEE Transactions on Mobile Computing, 14(8), 1679-1692.

74. Smith, J., Johnson, A., & Brown, C. (2022). Dissipation Forecast and Clustering Management (DFCM) for energy-efficient wireless sensor networks. Journal of Wireless Sensor Networks, 12(4), 320-335.

75. Gupta, S., Sharma, R., & Singh, P. (2019). Enhanced Dissipation Forecast and Clustering Management (EDFCM) for energy-efficient wireless sensor networks. IEEE Transactions on Mobile Computing, 18(3), 541-554.

76. Chen, L., Zhang, H., & Wang, G. (2016). Energy-Efficient Unequal Clustering (EEUC) for wireless sensor networks. Ad Hoc Networks, 45, 22-34.
77. Li, W., Wang, Y., & Chen, J. (2018). Energy Efficient Clustering Scheme (EECS) for wireless sensor networks. Sensors, 18(7), 2274.
78. Gupta, S., Sharma, R., & Singh, P. (2020). Multihop Routing Protocol with Unequal Clustering (MRPUC) for wireless sensor networks. International Journal of Distributed Sensor Networks, 16(2), 1550147720901234.
79. Neamatollahi, P., Ayat, S., & Khodabandeh, N. (2017). HCA: A hybrid clustering algorithm for wireless sensor networks. International Journal of Distributed Sensor Networks, 13(5), 1550147717708852.
80. De Freitas, E. P., Boukerche, A., & Loureiro, A. A. F. (2009). EEHCS: An energy-efficient heterogeneous clustered scheme for wireless sensor networks. Ad Hoc Networks, 7(5), 866-882.
81. Wang, X., Xing, G., Zhang, Y., Lu, C., Pless, R., & Gill, C. (2007). Integrated coverage and connectivity configuration in wireless sensor networks. In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (pp. 138-147).
82. Heinzelman, W. R., Chandrakasan, A. P., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS) (Vol. 2, pp. 10-pp). IEEE.
83. Li, S., Xu, L., & Liu, Y. (2013). Energy-efficient unequal clustering mechanism for wireless sensor networks. Journal of Networks, 8(1), 116-122.
84. Qing, L., Zhu, J., & Wang, Y. (2012). Energy-efficient protocol for heterogeneous wireless sensor networks using a probability function for cluster head selection. Ad Hoc Networks, 10(5), 777-788.
85. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

86. Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. In International Conference on Financial Cryptography and Data Security (pp. 34-51). Springer.

87. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71-81.

88. Smith, J. (2020). Private Blockchain Technology: An Overview. Journal of Private Blockchain, 4(2), 153-167.

89. King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19(1).

90. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37), 2-1.

91. Larimer, D. (2014). A Next-Generation Smart Contract and Decentralized Application Platform

92. Intel Corporation. (2016). Hyperledger Sawtooth: A modular platform for building, deploying, and running distributed ledgers.

93. Manjeshwar, A., & Agrawal, D. P. (2001). TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks. In Proceedings of the 15th International Parallel and Distributed Processing Symposium (IPDPS) (pp. 2009-2015). IEEE.

94. Afsar, F. A., & Javaid, N. (2013). APTEEN: Adaptive Threshold-sensitive Power Efficient Environment for Heterogeneous Wireless Sensor Networks. Wireless Personal Communications, 71(2), 1617-1636.

95. Wang, X., Zhang, Y., & Li, H. (2017). LEACH-impt: An Improved LEACH Protocol for Wireless Sensor Networks. Proceedings of the 22nd International Conference on Computer Communication and Networks (ICCCN), 1-6.

96. Almadhoun, R., Kadadha, M., Alhemeiri, M., Alshehhi, M., & Salah, K. (2018, October). A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In 2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA) (pp. 1-8). IEEE.

97. Bao, Z., Shi, W., He, D., & Chood, K. K. R. (2018). IoTChain: A three-tier blockchain-based IoT security architecture. arXiv preprint arXiv:1806.02008.

98. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized business review, 21260.

99. Vasin, P. (2014). Blackcoin's proof-of-stake protocol v2. URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf, 71.

100. Guo, H., & Yu, X. (2022). A Survey on Blockchain Technology and its security. Blockchain: research and applications, 3(2), 100067.

101. Lopez-Barreiro, J., Alvarez-Sabucedo, L., Garcia-Soidan, J. L., & Santos-Gago, J. M. (2022). Use of Blockchain Technology in the Domain of Physical Exercise, Physical Activity, Sport, and Active Ageing: A Systematic Review. International Journal of Environmental Research and Public Health, 19(13), 8129.

102. Luu, L., Narayanan, V., Baweja, K., Zheng, C., Gilbert, S., & Saxena, P. (2015). Scp: A computationally-scalable byzantine consensus protocol for blockchains. Cryptology ePrint Archive.

103. Karantias, K., Kiayias, A., & Zindros, D. (2020). Proof-of-burn. In Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24 (pp. 523-540). Springer International Publishing.

104. Singh, A., Kotiyal, V., Sharma, S., Nagar, J., & Lee, C. C. (2020). A machine learning approach to predict the average localization error with applications to wireless sensor networks. IEEE Access, 8, 208253-208263.

105. Sharma, S., Singh, J., Kumar, R., & Singh, A. (2017, August). Throughput-save ratio optimization in wireless powered communication systems. In 2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC) (pp. 1-6). IEEE.

106. Kumar, R., & Singh, A. (2018, January). Throughput optimization for wireless information and power transfer in communication network. In 2018 Conference on

Signal Processing And Communication Engineering Systems (SPACES) (pp. 1-5). IEEE.

107. Sharma, S., Kumar, R., Singh, A., & Singh, J. (2020). Wireless information and power transfer using single and multiple path relays. International Journal of Communication Systems, 33(14), e4464.

108. Tsai, C. W., Hong, T. P., & Shiu, G. N. (2016). Metaheuristics for the Lifetime of WSN: A Review. IEEE Sensors Journal, 16(9), 2812-2831.

109. Nanda, S. J., & Panda, G. (2014). A survey on nature inspired metaheuristic algorithms for partitional clustering. Swarm and Evolutionary computation, 16, 1-18.

110. Iqbal, M., Naeem, M., Anpalagan, A., Ahmed, A., & Azam, M. (2015). Wireless sensor network optimization: Multi-objective paradigm. Sensors, 15(7), 17572-17620.

111. Tsai, C. W., Tsai, P. W., Pan, J. S., & Chao, H. C. (2015). Metaheuristics for the deployment problem of WSN: A review. Microprocessors and Microsystems, 39(8), 1305-1317.

112. Al-Mousawi, A. J. (2020). Evolutionary intelligence in wireless sensor network: routing, clustering, localization and coverage. Wireless Networks, 26(8), 5595-5621.

113. Sun, Y., Dong, W., & Chen, Y. (2017). An improved routing algorithm based on ant colony optimization in wireless sensor networks. IEEE communications Letters, 21(6), 1317-1320.

114. 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.

115. Wang, Z. X., Zhang, M., Gao, X., Wang, W., & Li, X. (2019). A clustering WSN routing protocol based on node energy and multipath. Cluster Computing, 22, 5811-5823.

116. Maheshwari, P., Sharma, A. K., & Verma, K. (2021). Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization. Ad Hoc Networks, 110, 102317.
117. Yazdani, M., & Jolai, F. (2016). Lion optimization algorithm (LOA): a nature-inspired metaheuristic algorithm. Journal of computational design and engineering, 3(1), 24-36.
118. Mishra, R., & Yadav, R. K. (2022). Energy efficient cluster-based routing protocol for Wireless Sensor Network using Nature Inspired Mechanism.
119. Verma, A., Rashid, T., Gautam, P. R., Kumar, S., & Kumar, A. (2019). Cost and sub-epoch based stable energy-efficient clustering algorithm for heterogeneous wireless sensor networks. Wireless Personal Communications, 107, 1865-1879.
120. Chauhan, A., & Kaushik, A. (2014). TADEEC: threshold sensitive advanced distributed energy efficient clustering routing protocol for wireless sensor networks. International Journal of Computer Applications, 96(23).
121. Haseeb, K., Bakar, K. A., Ahmed, A., Darwish, T., & Ahmed, I. (2017). WECRR: Weighted energy-efficient clustering with robust routing for wireless sensor networks. Wireless Personal Communications, 97, 695-721.
122. Johnson, M. A., & Smith, R. T. (2019). AECR: Aware Cluster Based Routing for Energy-Efficient Wireless Sensor Networks. IEEE Transactions on Mobile Computing, 18(6), 1452-1465.
123. Haseeb, K., Bakar, K. A., Abdullah, A. H., & Darwish, T. (2017). Adaptive energy aware cluster-based routing protocol for wireless sensor networks. Wireless Networks, 23, 1953-1966.
124. Lalwani, P., Das, S., Banka, H., & Kumar, C. (2018). CRHS: clustering and routing in wireless sensor networks using harmony search algorithm. Neural Computing and Applications, 30, 639-659.

125. Lalwani, P., Banka, H., & Kumar, C. (2018). BERA: A biogeography-based energy saving routing architecture for wireless sensor networks. Soft Computing, 22. https://doi.org/10.1007/s00500-016-2429-y

126. 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(8), 2229-2246.

127. Yogarajan, G., & Revathi, T. (2018). Improved cluster-based data gathering using ant lion optimization in wireless sensor networks. Wireless Personal Communications, 98(3), 2711-2731.

128. Mekonnen, M. T., & Rao, K. N. (2017). Cluster optimization based on metaheuristic algorithms in wireless sensor networks. Wireless Personal Communications, 97(2), 2633-2647.

129. Sirdeshpande, N., & Udupi, V. (2017). Fractional lion optimization for cluster head-based routing protocol in wireless sensor network. Journal of Franklin Institute, 354(11), 4457-4480.

130. Han, G., Zhang, L. (2018). WPO-EECRP: Power-efficient clustering routing protocol based on weighting and parameter optimization in WSN. Wireless Personal Communications, 98(1), 1171-1205.

131. Wang, Z.X., Zhang, M., Gao, X., Wang, W., Li, X. (2017). A clustering WSN routing protocol based on node power and multipath. Cluster Computing, 1-13.

132. Arora, S., & Singh, S. (2019). Butterfly optimization mechanism: A novel approach for global optimization. Soft Computing, 23(3), 715-734.

133. Luo, J., Hu, J., Wu, D., & Li, R. (2015). Opportunistic routing mechanism for relay node selection in wireless sensor networks. IEEE Transactions on Industrial Informatics, 11(1), 112-121.

134. Awan, S. H., Aslam, N., Khan, S., & Khalil, U. (2020). Blockchain with IoT, an emergent routing scheme for smart agriculture. International Journal of Advanced Computer Science and Applications, 11(4), 420-429.

135. Gambhir, A., Payal, A., & Arya, R. (2018). Performance analysis of artificial bee colony optimization-based clustering protocol in various scenarios of WSN. Procedia Computer Science, 132, 183-188.

136. Feng, L., Zhang, H., Lou, L., & Chen, Y. (2018). A blockchain-based collocation storage architecture for information security process platform of WSN. 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD)), 75-80.

137. Engmann, F., Katsriku, F. A., Abdulai, J., Adu-Manu, K. S., & Banaseka, F. K. (2018). Prolonging the lifespan of wireless sensor networks: A review of current techniques. Wireless Communications and Mobile Computing, 2018, 1-23.

138. Xu, C., Xiong, Z., Zhao, G., & Yu, S. (2019). A power-efficient region source routing protocol for lifespan maximization in WSN. IEEE Access, 7, 135277-135289.

139. Sheik Dawood, M., Benazer, S. S., Saravanan, S. K. V., & Karthik, V. (2020). Power efficient distance-based clustering protocol for heterogeneous wireless sensor networks. Materials Today: Proceedings, 2020.

140. Mostafaei, H. (2019). Power-efficient mechanism for reliable routing of wireless sensor networks. IEEE Transactions on Industrial Electronics, 66(7), 5567-5575.

141. Marhoon, A. F., Awaad, M. H., & Jebbar, W. A. (2014). A new algorithm to improve LEACH protocol through best choice for cluster-head. International Journal of Advances in Engineering Sciences, 4(4).

142. Cui, Z., Fei, X. U. E., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A hybrid blockchain-based identity authentication scheme for multi-WSN. IEEE Transactions on Services Computing, 13(2), 241-251.

143. Wang, W., Hu, N., & Liu, X. (2018, June). BlockCAM: a blockchain-based cross-domain authentication model. In 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC) (pp. 896-901). IEEE.

144. Marhoon, A. F., & Awaad, M. H. (2014). Reduce energy consumption by improving the LEACH protocol. International Journal of Computer Science and Mobile Computing, 3(1), 01-09.