

An energy-efficient and secure framework for wireless sensor networks

Maruthi Hanumanthappa Chandrappa^{1,2}, Poornima Govindaswamy¹

¹Department of Electronics and Communication Engineering, B.M.S. College of Engineering, Visvesvaraya Technological University, Belagavi, India

²Department of Electronics and Communication Engineering, Government Engineering College, Visvesvaraya Technological University, Belagavi, India

Article Info

Article history:

Received Oct 7, 2024

Revised Jul 24, 2025

Accepted Aug 6, 2025

Keywords:

Digital signature

Energy efficiency

Harmful node detection

Secure routing

Wireless sensor networks

ABSTRACT

In wireless sensor networks (WSNs), achieving energy efficiency, security, and minimizing route change propagation time is essential for maintaining optimal performance. This paper introduces a new approach that combines Bray Jaccard Curtis-based Calinski Harabasz k-means (BJC-CHKMeans) for clustering and Karl Pearson correlation-based egret swarm optimization algorithm (KPC-ESOA) for selecting the best cluster head (CH) and path, along with classifying long short-term memory with gated recurrent units (CLE-GRU) for detecting harmful nodes. The methodology aims to enhance energy usage, improve routing efficiency, and strengthen security by identifying malicious nodes. Additionally, it integrates a secure routing table using elbow de-swinging k-anonymity (EDS-KA) and employs digital signature algorithm-based Zeta Bernoulli Merkle tree (DSA-ZBMT) to ensure secure communication with sink nodes. The WSN-DS dataset was used for training and testing, with rigorous preprocessing, feature extraction, and selection to maintain data integrity. Experimental results revealed that the proposed BJC-CHKMeans and CLE-GRU models outperform traditional methods in power consumption, latency, and accuracy. The system achieved a power consumption of 2.1 mW for clustering and 1.9 mW for classification, while also providing near-perfect accuracy in detecting harmful nodes. These findings demonstrate that the framework significantly enhances the energy efficiency and security of WSNs, making it a highly effective solution for large, dynamic sensor networks.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Maruthi Hanumanthappa Chandrappa

Department of Electronics and Communication Engineering, B.M.S. College of Engineering

Visvesvaraya Technological University

Bengaluru-560019, Karnataka, India

Email: maruthibelagere@gmail.com

1. INTRODUCTION

Wireless sensor networks (WSNs) are widely used in applications such as environmental monitoring, healthcare, industrial automation, and surveillance due to their scalability, cost-effectiveness, and flexibility [1]. These networks consist of numerous sensor nodes that gather and transmit data to a centralized base station. Despite their advantages, WSNs face significant challenges, particularly in the areas of energy efficiency [2], security [3], and timely propagation of route changes [4], especially in time-sensitive and critical environments. Energy efficiency remains a primary concern as sensor nodes typically operate on limited battery power. Communication tasks and frequent routing updates can quickly drain energy, leading to early node failures and reduced network lifespan [5]. In addition, WSNs are often deployed in unsecured

locations, making them vulnerable to security threats such as eavesdropping, data tampering, or physical capture of nodes [6], [7]. Such threats can compromise data integrity and disrupt communication, especially if malicious nodes are not promptly identified and isolated. Another critical issue is the efficient propagation of route changes. Networks must dynamically adapt to node failures or environmental obstacles to maintain communication. However, if route updates are delayed or poorly coordinated, they can result in increased energy consumption, data loss, and latency, ultimately degrading network performance [8].

To address these interconnected challenges, this paper introduces a comprehensive framework that ensures secure, energy-efficient, and responsive routing in WSNs. It integrates Bray Jaccard Curtis-based Calinski Harabasz k-means (BJC-CHKMeans) for effective clustering, Karl Pearson correlation - based egret swarm optimization algorithm (KPC-ESOA) for optimized cluster head (CH) selection and routing, and Zeta Bernoulli Merkle tree (ZBMT) for secure and adaptable communication paths. Unlike conventional approaches that often prioritize one aspect over others, this integrated method balances energy management, security, and route adaptability. It enables real-time malicious node detection [9], minimizes latency, and extends the operational lifespan of the network under dynamic conditions [10], [11].

This paper proposes a unified framework to enhance WSN performance by improving energy efficiency, secure communication, and route adaptability. It integrates multiple techniques to address key challenges such as harmful node detection and dynamic routing. BJC-CHKMeans clusters nodes based on location and energy to minimize intra-cluster communication and reduce power usage. KPC-ESOA optimizes CH selection and aids in identifying malicious nodes through feature selection. ZBMT ensures secure and reliable data transmission between nodes and the base station. Additionally, classifying long short-term memory with gated recurrent units (CLE-GRU), a machine learning model, detects malicious nodes by analyzing their behavior. Together, these methods improve security, conserve energy, and extend network lifetime.

2. BACKGROUND

WSNs are self-organizing systems used to monitor physical or environmental conditions. Initially developed for military applications, they are now widely applied in healthcare, automation, and environmental monitoring [12]. These networks use wireless communication to transmit sensed data to a central base station [13]. Key challenges in WSNs include energy efficiency, security, and reliable data transmission, particularly in critical applications like smart transport and defense [14]. Routing remains complex due to limited energy, dynamic topologies, and decentralized architecture, prompting the need for efficient protocols tailored to specific applications [15], [16]. Several researchers have proposed solutions to address these issues. Gopalan *et al.* [17] integrated bacterial foraging optimization with harmony search algorithm (BFO-HSA) for clustering and cross-layer-based opportunistic routing protocol (CORP) for routing, achieving improved packet delivery, reduced delay, and longer network life. Adaptive energy-efficient balanced uneven clustering (AEBUC) protocol adjusts clustering dynamically based on node density to enhance energy balance and CH selection [18]. Tabbassum and Pathak [19] combined low energy adaptive clustering hierarchy (LEACH) with fuzzy logic and artificial neural network (ANN) to build an intrusion detection system with 97% accuracy. Kaviarasan and Srinivasan [20] used adaptive remora optimization algorithm (AROA) for energy-aware CH selection, significantly extending network lifetime. Kapoor and Sharma [21] applied glowworm swarm optimization (GSO) to improve energy use, connectivity, and coverage with faster convergence.

Srividya and Devi [22] proposed a hybrid method combining bio-inspired hierarchical order chicken swarm optimization (BIHO-CSO), energy competent particle swarm optimization (ECPSO), and recursive binary partitioning decision tree (RBP-DT) for improved CH selection and routing in WSNs, achieving higher throughput but lacking intrusion detection. Another study used safe weighted clustering with a decision tree (DT) classifier, attaining 78% accuracy and longer network life, though with limited feature use [23]. Xue *et al.* [24] adapted cross-layer-based Harris-hawks-optimization (CL-HHO) achieved low energy consumption (0.1 mJ) but faced link failure issues. Cherappa *et al.* [25] adapted adaptive sailfish optimization (ASFO)-based protocol with k-medoids offered low power use and high throughput but struggled with node identification. Suresh and Prasad [26] adapted LEACH for IoT, improving packet-delivery ratio (PDR) but facing routing table instability. These studies highlight the role of optimization and machine learning in enhancing WSNs, though challenges remain unresolved.

3. PROPOSED METHODOLOGY

The approach entails developing a safe, energy-efficient WSN system that seeks to minimize the propagation of route change and optimize detecting malicious nodes. It combines BJC-CHKMeans to cluster, KPC-ESOA to select features and CH optimization, ZBMT to offer a secure communication to sink, CLE-GRU to detect malicious nodes. The process encompasses data preprocessing, and transmission with discrete data security, as well as efficient energy consumption, safe routing and enforced security.

3.1. Dataset used

The experiment makes use of the WSN-DS dataset, a simulated WSN detection system created by Almomani *et al.* [27]. This dataset is specifically designed to assess how well machine learning algorithms can detect and counteract malicious activities in WSNs. It includes both normal traffic and attack traffic, covering common WSN threats like blackhole, grayhole, and flooding attacks. Key features of the dataset, such as packet size, signal strength, energy consumption, and node mobility, are critical for evaluating WSN performance in terms of security, energy efficiency, and routing effectiveness.

3.2. Proposed methodology

This paper proposes a comprehensive methodology aimed at improving energy efficiency, security, and route optimization in WSNs. The system architecture employs a multi-phase approach, including data pre-processing, clustering, CH selection, harmful node detection, and secure data transmission. This ensures that the network operates efficiently while maintaining a high level of security. The block diagram of proposed methodology is represented in Figure 1.

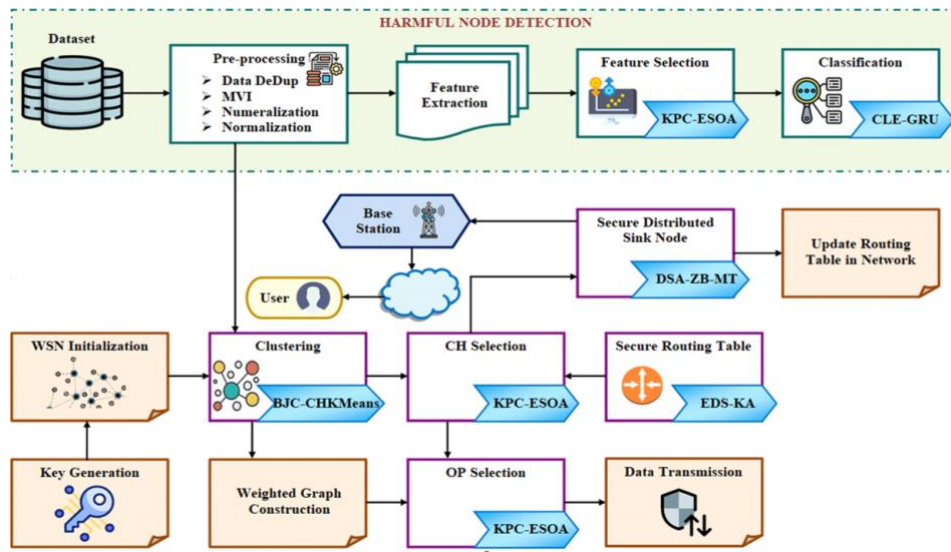


Figure 1. Proposed methodology framework

At the first stage, the WSN-DS dataset [27] is preprocessed, the duplicates are eliminated, missing values addressed, and the data normalized and converted to numerical representation. The data set contains such parameters as energy consumption, node mobility, and packet behavior. It is divided into 292,629 training samples to learn the model and 73,158 testing samples to evaluate the model. This makes the model generalize well on the new data. Preprocessing improves the quality of data, which then facilitates proper extraction and selection of features. After the pre-processing stage, the system transitions to feature extraction, where the essential characteristics for classifying and clustering nodes are identified. To enhance feature selection, the KPC-ESOA is utilized. This step aims to reduce the data's dimensionality, keeping only the most important features to boost classification accuracy and lower computational costs. The KPC-ESOA algorithm addresses this by tackling an optimization problem designed for this purpose. The KPC-ESOA algorithm operates by solving the optimization problem given in (1). Where (x_i, c_k) represents the distance between node x_i and the cluster centre c_k , and w_i represents the weight assigned to the feature.

$$\text{Minimize } (f(x)) = \sum_{i=1}^n (d(x_i, c_k) \cdot w_i) \quad (1)$$

During the next step, sensor nodes are clustered with BJC-CHKMeans algorithm in order to minimize intra-cluster energy expenditure and provide a balance in loads. It is done through clustering based on distance and energy metrics to enhance communication performance. KPC-ESOA next chooses optimum CHs using parameters such as remaining energy, distance, and message frequency. This is addressed as a constrained optimization problem with the objective of minimizing energy consumption and ensuring a good connectivity. After selecting the CH, the KPC-ESOA algorithm is used to identify the optimal path (OP) for data transmission within the WSN. The chosen path aims to minimize energy consumption across the

network while maintaining reliable data delivery. This is done by solving a multi-objective optimization problem. Where E_{Total} is the total energy consumption of the network, E_{tx} is the energy consumed during transmission, and E_{tr} is the energy consumed during reception.

$$\text{Minimize } (E_{Total}) = \sum_{i=1}^n (E_{tx} + E_{tr}) \quad (2)$$

The proposed method employs CLE-GRU to detect malicious nodes by analyzing packet flow patterns, power usage, and anomalies, effectively identifying grayhole and blackhole attacks. This supervised model classifies nodes as normal or malicious, enhancing network security. Digital signature algorithm (DSA)-ZBMT generates authentication keys for secure sink node communication, while elbow de-swinging k-anonymity (EDS-KA) ensures secure routing table creation and safe data delivery to the base station. A weighted graph is then formed based on node connectivity and energy use to identify energy-efficient paths, extending network lifetime. The secure key generation mechanism protects inter-node communication from threats. Together, BJC-CHKMeans, KPC-ESOA, and CLE-GRU ensure efficient routing, strong security, and real-time malicious node detection.

3.3. Performance evaluation

The proposed secure and energy-efficient WSN framework's performance is assessed through various key metrics. These metrics offer valuable insights into the network's efficiency, particularly regarding energy usage, security, and routing capabilities. Energy consumption is a key factor in assessing the efficiency of WSNs, especially considering the limited power availability of sensor nodes. It represents the total energy expended by the nodes for data transmission, reception, and processing. The overall energy consumption (E_{Total}) is determined by summing the energy required for transmitting (E_{tx}) and receiving (E_{tr}) data packets over a specific time frame. This metric helps determine the overall energy efficiency of the network and whether the proposed system conserves energy compared to traditional routing protocols.

$$E_{Total} = \sum_{i=1}^n (E_{tx,i} + E_{tr,i}) \quad (3)$$

The PDR reflects how many packets successfully reach their destination compared to the total sent by the source nodes. It gauges the effectiveness of the routing protocol in transmitting data. A higher PDR suggests that the network is effectively delivering packets with minimal loss, which is crucial for ensuring data integrity and reliability within the WSN.

$$PDR = \frac{P_{received}}{P_{sent}} \times 100 \quad (4)$$

Route change propagation time refers to how fast the network adjusts to changes in its structure, like node failures or mobility, and updates its routing paths. This measurement is vital in dynamic networks where node availability fluctuates. Keeping this time to a minimum is essential for maintaining network stability and ensuring smooth, uninterrupted data transmission.

$$T_{rcp} = T_{update} - T_{failure} \quad (5)$$

Detection accuracy gauges the accuracy of a system to notice malicious nodes within the WSN. It is estimated on the basis of true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN). High accuracy implies that the system is secure and has a correct rate of identifying security-related and regular nodes.

$$DA = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (6)$$

By analyzing these metrics, it is possible to have a clear picture of how the proposed approach can be effective in enhancing energy efficiency, security and communication in WSNs. The findings affirm its effectiveness in minimized energy consumption, ensured reliability in transmission, adjustment to path changes and detection of malicious nodes.

3.4. Verification of encrypted messages

The encrypt-then-sign methods employed in our research endeavor to guarantee the confidentiality, integrity, and non-repudiation of communicated messages among entities. The suggested methodology guarantees privacy by implementing a series of preliminary measures. The data being transferred includes an encrypted coordinate, the current time (t_o), and a signature integer created at random. By using the public key of the sender, the recipient can verify the genuineness of a signed communication.

4. PERFORMANCE EVALUATION

The results and analysis section evaluates the proposed method's performance based on energy consumption, PDR, latency, network lifetime, and detection accuracy. Simulation results show that the integration of BJC-CHKMeans, KPC-ESOA, and CLE-GRU enhances WSN efficiency and security. Compared to existing methods, the approach achieves better energy savings, reliable transmission, and accurate malicious node detection, demonstrating strong scalability and robustness under diverse conditions.

4.1. Quantitative analysis

Figure 2 highlights the latency performance of the proposed KPC-ESO algorithm in comparison to other algorithms, such as egret swarm optimization (ESO), bacterial foraging optimization (BFO), spotted hyena optimizer (SHO), and artificial bee colony optimization (ABCO), as the number of nodes increases. Latency, measured in milliseconds (ms), increases for all algorithms as the number of nodes grows, which is expected due to the additional communication and data handling needed in larger networks. However, KPC-ESO consistently shows lower latency across all node counts compared to the others. While ESO and BFO perform relatively well, they still lag behind KPC-ESO, particularly as the number of nodes increases. The consistently lower latency of KPC-ESO suggests its route optimization is more efficient, minimizing the time for data packets to travel across the network, even as the network grows. This makes KPC-ESO particularly well-suited for large-scale WSNs, where reducing latency is crucial for real-time applications.

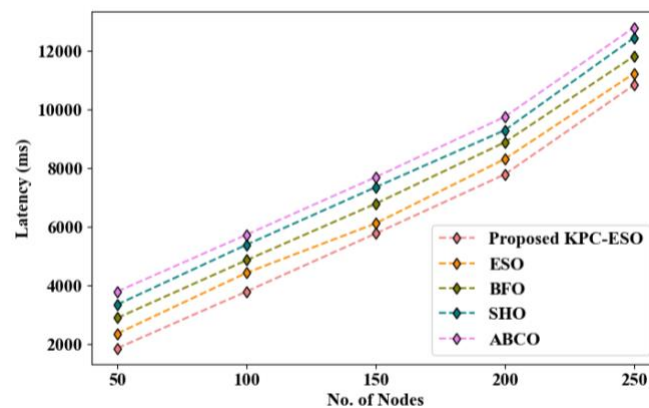


Figure 2. Comparison of latency of proposed model with the peer methods

Figure 3 illustrates the response time of the proposed KPC-ESO algorithm versus ESO, BFO, SHO, and ABCO as node count increases. While all methods show rising response times with network size, KPC-ESO consistently achieves the lowest values. This efficiency stems from its optimized CH selection and routing, minimizing delays. The results confirm KPC-ESO's scalability and suitability for large WSNs requiring fast, real-time communication.

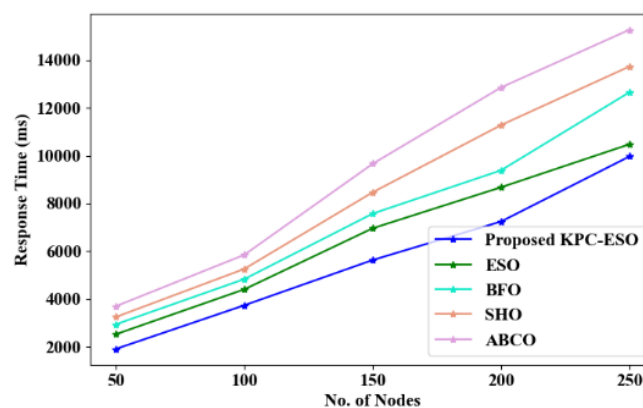


Figure 3. Comparison of response time of proposed model with the peer methods

Figure 4 shows the fitness values over iterations for CH selection using KPC-ESOA, compared to ESOA, BFO, SHO, and ABCO. While all methods improve with more iterations, KPC-ESOA consistently achieves the highest fitness, reflecting better energy efficiency, connectivity, and distance optimization. Its advanced CH selection allows quicker convergence to optimal solutions, enhancing energy balance and extending network life. This demonstrates KPC-ESOA's superior efficiency and performance over traditional approaches.

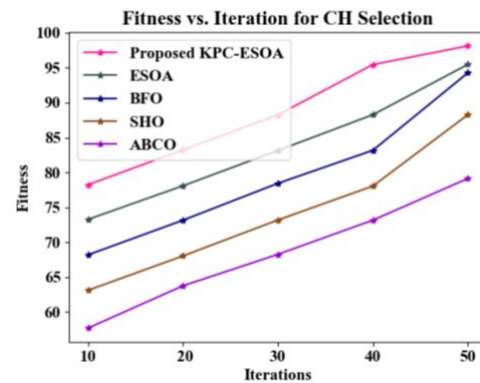


Figure 4. Comparison of fitness vs. iterations of proposed model with the peer methods

Figure 5 shows the execution time of various clustering methods, where BJC-CHKMeans outperforms KMeans, KMedoid, forward capacity market (FCM), and Birch with the lowest execution time. This efficiency makes it ideal for real-time WSN applications, enabling faster processing and better energy management. In contrast, higher execution times in methods like Birch make them less suitable for time-critical or large-scale networks.



Figure 5. Clustering technique execution time comparison

Figure 6 presents a comparison of the accuracy rates for various harmful node classification methods, including the proposed CLE-GRU model and the existing GRU, bidirectional long short-term memory (Bi-LSTM), long short-term memory (LSTM), and recurrent neural network (RNN) models. Accuracy, shown as a percentage, reflects each model's ability to correctly detect harmful nodes within a WSN. The proposed CLE-GRU model stands out, achieving close to 98.6% accuracy, which is significantly higher than the other models. This comparison emphasizes that the CLE-GRU model's advanced feature extraction and classification techniques enable it to more effectively differentiate between normal and harmful nodes. The nearly perfect accuracy of CLE-GRU positions it as a leading option for improving WSN security, particularly in environments where precise identification of harmful nodes is essential for maintaining network performance and data integrity.

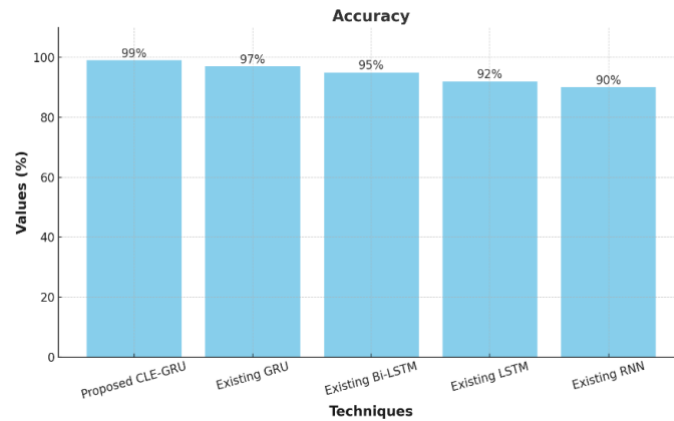
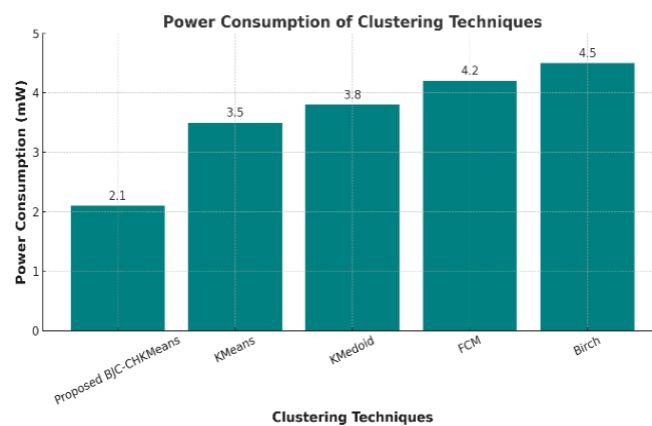
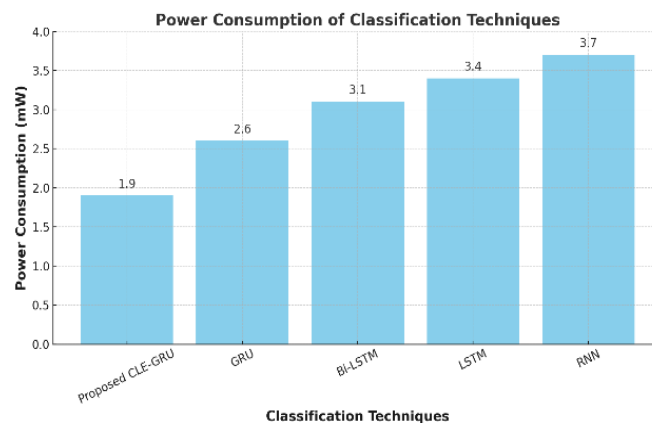


Figure 6. Harmful node classification accuracy

Figure 7 presents a power consumption analysis for both clustering and classification techniques. Figure 7(a) compares power consumption across clustering methods, showing BJC-CHKMeans as the most energy-efficient at 2.1 mW. Its optimized clustering reduces intra-cluster communication, making it ideal for energy-constrained WSNs. Other methods, while effective, consume more power, limiting their suitability for such environments. Figure 7(b) shows harmful node detection methods, where CLE-GRU has the lowest power usage at 1.9 mW. Its efficient design balances computation and memory while maintaining high accuracy. This makes CLE-GRU well-suited for WSNs, where low power consumption is crucial for prolonged network operation.



(a)



(b)

Figure 7. Power consumption analysis of (a) clustering and (b) classification techniques

4.2. Qualitative analysis

The user interface (UI) developed for this project is designed to provide smooth and efficient interaction with the WSN system as shown in Figure 8. It is organized into multiple functional components, making it user-friendly for both the testing and training phases. Essential functions like harmful node detection, clustering, weighted graph creation, and OP selection are presented as buttons, allowing users to activate each process step by step. Figure 9 depicts a weighted network graph for the WSN in this work. Each node represents a sensor within the network, and the connecting edges show the communication links between them. The numbers on these edges reflect the weights of the connections, which could relate to factors like energy consumption, node distance, or signal strength. These weights are essential in determining the most efficient paths for data transmission. Nodes are connected based on proximity and communication capability, creating a web through which data flows across multiple routes. Lower weights indicate more energy-efficient or faster links, while higher weights suggest greater energy use or less efficient paths. This graph likely supports node clustering, CH selection, and routing table formation, aimed at optimizing energy efficiency and security in the WSN.

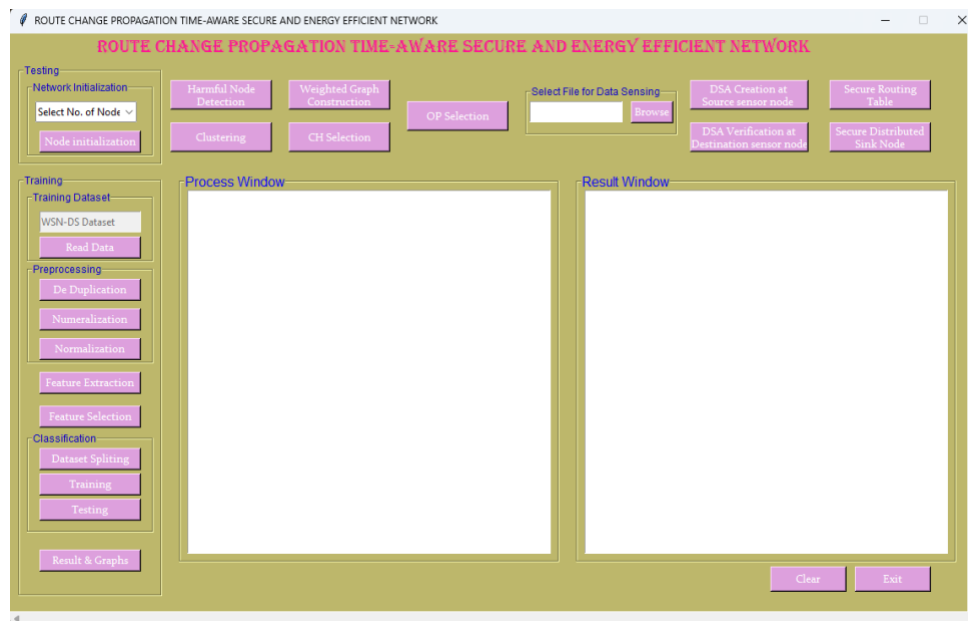


Figure 8. Front-end for the proposed method

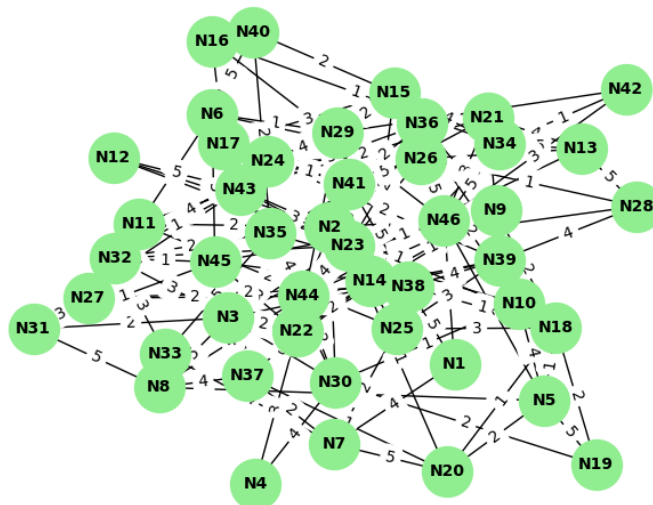


Figure 9. Weighted graph construction

Figure 10 demonstrates interface successfully completes key tasks in WSN operations, such as node initialization, harmful node detection, weighted graph construction, and clustering. It sets up 50 nodes, positioning them and assigning energy values. Harmful node detection and weighted graph construction ensure efficient communication and routing. The clustering process compares algorithms like BJC-CHKMeans, KMeans, and KMedoid, focusing on classification results. The proposed CLE-GRU model stands out with more accurate and reliable classification, making it a better solution for securing and optimizing WSN operations. The interface simplifies testing and performance evaluation, offering real-time feedback and system monitoring.

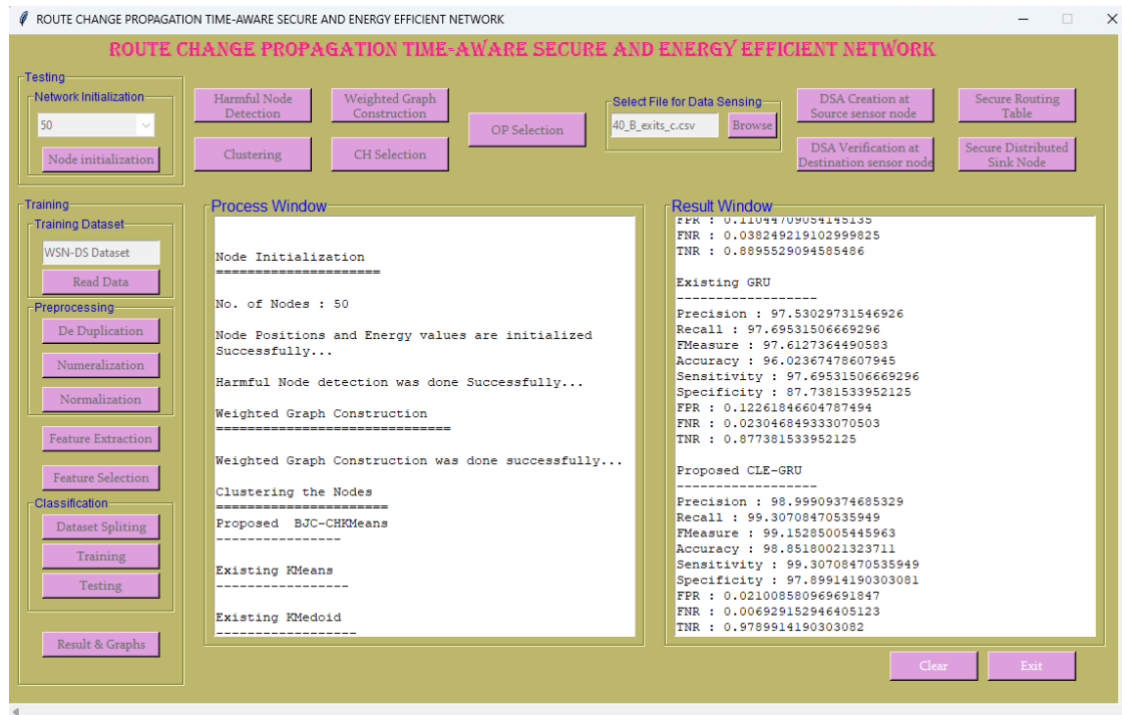


Figure 10. Interface demonstrates successful completion of key tasks

5. CONCLUSION

This paper outlines a thorough framework designed to improve energy efficiency, secure routing, and accurate detection of harmful nodes in WSNs. The approach combines BJC-CHKMeans for clustering, KPC-ESOA for optimizing CH selection and routing, and CLE-GRU for identifying harmful nodes. It tackles major challenges in WSNs, such as high energy usage, security vulnerabilities, and the time taken to propagate route changes. Experimental tests using the WSN-DS dataset show that the proposed methods excel in reducing power consumption, boosting accuracy, and lowering latency. The CLE-GRU model surpassed other classifiers like GRU, Bi-LSTM, and LSTM, achieving a detection accuracy of 98.85% with minimal false positives and negatives. BJC-CHKMeans also proved to be more energy-efficient, significantly reducing power consumption compared to traditional clustering methods. These results affirm the framework's ability to enhance both security and energy efficiency in WSNs, making it well-suited for real-world applications in dynamic, resource-limited settings. Future research may focus on further optimizing the framework for large-scale networks and incorporating real-time adaptive mechanisms to address new threats and evolving network conditions.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

An energy-efficient and secure framework for wireless sensor ... (Maruthi Hanumanthappa Chandrappa)

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Maruthi Hanumanthappa	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓
Chandrappa														
Poornima Govindaswamy		✓		✓		✓	✓			✓		✓	✓	

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.




REFERENCES

- [1] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: an up-to-date survey," *Applied System Innovation*, vol. 3, no. 1, pp. 1–24, 2020, doi: 10.3390/asi3010014.
- [2] J. Amutha, S. Sharma, and J. Nagar, "WSN strategies based on sensors, deployment, sensing models, coverage and energy efficiency: review, approaches and open issues," *Wireless Personal Communications*, vol. 111, no. 2, pp. 1089–1115, 2020, doi: 10.1007/s11277-019-06903-z.
- [3] D. E. Boubiche, S. Athmani, S. Boubiche, and H. T.-Cruz, "Cybersecurity issues in wireless sensor networks: current challenges and solutions," *Wireless Personal Communications*, vol. 117, no. 1, pp. 177–213, 2021, doi: 10.1007/s11277-020-07213-5.
- [4] R. Zagrouba and A. Kardi, "Comparative study of energy efficient routing techniques in wireless sensor networks," *Information*, vol. 12, no. 1, pp. 1–28, 2021, doi: 10.3390/info12010042.
- [5] M. S. Bensaleh, R. Saida, Y. H. Kacem, and M. Abid, "Wireless sensor network design methodologies: a survey," *Journal of Sensors*, vol. 2020, 2020, doi: 10.1155/2020/9592836.
- [6] M. Abedini and I. A.-Anbagi, "Active eavesdropper's detection system in multi-hop wireless sensor networks," in *IEEE Symposium on Computers and Communications*, 2022, vol. 2022-June, doi: 10.1109/ISCC55528.2022.9912466.
- [7] M. Faris, M. N. Mahmud, M. F. M. Salleh, and A. Alnoor, "Wireless sensor network security: a recent review based on state-of-the-art works," *International Journal of Engineering Business Management*, vol. 15, pp. 1–29, Feb. 2023, doi: 10.1177/18479790231157220.
- [8] Z. Liu, Y. Liu, and X. Wang, "Intelligent routing algorithm for wireless sensor networks dynamically guided by distributed neural networks," *Computer Communications*, vol. 207, pp. 100–112, 2023, doi: 10.1016/j.comcom.2023.05.018.
- [9] W. B. Nedham and A. K. M. A.-Qurabat, "A comprehensive review of clustering approaches for energy efficiency in wireless sensor networks," *International Journal of Computer Applications in Technology*, vol. 72, no. 2, pp. 139–160, 2023, doi: 10.1504/IJCAT.2023.133035.
- [10] R. Ahmad, R. Wazirali, and T. A.-Ain, "Machine learning for wireless sensor networks security: an overview of challenges and issues," *Sensors*, vol. 22, no. 13, 2022, doi: 10.3390/s22134730.
- [11] Z. Al Aghbari, A. M. Khedr, W. Osamy, I. Arif, and D. P. Agrawal, "Routing in wireless sensor networks using optimization techniques: a survey," *Wireless Personal Communications*, vol. 111, no. 4, pp. 2407–2434, 2020, doi: 10.1007/s11277-019-06993-9.
- [12] M. A. Matin and M. M. Islam, "Overview of wireless sensor network," in *Wireless Sensor Networks - Technology and Protocols*, vol. 17, InTech, 2012, p. 302.
- [13] M. Islam, A. Kumar, and A. Hossain, "Study of wireless sensor network," *International Journal of Sensors and Sensor Networks*, vol. 7, no. 1, 2019, doi: 10.11648/j.ijssn.20190701.12.
- [14] D. Kandris and E. Anastasiadis, "Advanced wireless sensor networks: applications, challenges and research trends," *Electronics*, vol. 13, no. 12, 2024, doi: 10.3390/electronics13122268.
- [15] A. S. R. Sulthana, R. Mishra, R. Singh, B. Pant, S. S. Bhojne, and C. R. Prasad, "Wireless sensor networks face challenges and issues related to security," in *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2023*, 2023, pp. 943–949, doi: 10.1109/ICACITE57410.2023.10183029.
- [16] B. Kaur and D. Prashar, "Localization in wireless sensor network: techniques, algorithms analysis and challenges," *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2021*, 2021, doi: 10.1109/ICRITO51393.2021.9596135.
- [17] S. H. Gopalan, D. G. Takale, B. Jayaprakash, and V. P. Raj, "An energy efficient routing protocol with fuzzy neural networks in wireless sensor network," *Ain Shams Engineering Journal*, vol. 15, no. 10, 2024, doi: 10.1016/j.asej.2024.102979.
- [18] M. Li, J. Yin, Y. Xu, G. Hua, and N. Xu, "An adaptive energy-efficient uneven clustering routing protocol for WSNs," *IEICE Transactions on Communications*, vol. E107.B, no. 2, pp. 296–308, 2024, doi: 10.23919/transcom.2023EBP3097.
- [19] S. Tabbassum and R. K. Pathak, "Effective data transmission through energy-efficient clustering and fuzzy-based IDS routing approach in WSNs," *Virtual Reality and Intelligent Hardware*, vol. 6, no. 1, pp. 1–16, 2024, doi: 10.1016/j.vrih.2022.10.002.
- [20] S. Kaviarasan and R. Srinivasan, "Developing a novel energy efficient routing protocol in WSN using adaptive remora optimization algorithm," *Expert Systems with Applications*, vol. 244, 2024, doi: 10.1016/j.eswa.2023.122873.




- [21] R. Kapoor and S. Sharma, "Glowworm swarm optimization (GSO) based energy efficient clustered target coverage routing in wireless sensor networks (WSNs)," *International Journal of System Assurance Engineering and Management*, vol. 14, pp. 622–634, 2023, doi: 10.1007/s13198-021-01398-z.
- [22] P. Srividya and L. N. Devi, "An optimal cluster & trusted path for routing formation and classification of intrusion using the machine learning classification approach in WSN," *Global Transitions Proceedings*, vol. 3, no. 1, pp. 317–325, 2022, doi: 10.1016/j.gltp.2022.03.018.
- [23] P. Gite, K. Chouhan, K. M. Krishna, C. K. Nayak, M. Soni, and A. Shrivastava, "ML based intrusion detection scheme for various types of attacks in a WSN using C4.5 and CART classifiers," *Materials Today: Proceedings*, vol. 80, pp. 3769–3776, 2023, doi: 10.1016/j.matpr.2021.07.378.
- [24] X. Xue, R. Shanmugam, S. K. Palanisamy, O. I. Khalaf, D. Selvaraj, and G. M. Abdulsahib, "A hybrid cross layer with Harris-Hawk-optimization-based efficient routing for wireless sensor networks," *Symmetry*, vol. 15, no. 2, 2023, doi: 10.3390/sym15020438.
- [25] V. Cherappa, T. Thangarajan, S. S. M. Sundaram, F. Hajje, A. K. Munusamy, and R. Shanmugam, "Energy-efficient clustering and routing using ASFO and a cross-layer-based expedient routing protocol for wireless sensor networks," *Sensors*, vol. 23, no. 5, 2023, doi: 10.3390/s23052788.
- [26] B. Suresh and G. S. C. Prasad, "An energy efficient secure routing scheme using LEACH protocol in WSN for IoT networks," *Measurement: Sensors*, vol. 30, 2023, doi: 10.1016/j.measen.2023.100883.
- [27] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks," *Journal of Sensors*, vol. 2016, 2016, doi: 10.1155/2016/4731953.

BIOGRAPHIES OF AUTHORS



Maruthi Hanumanthappa Chandrappa    is an Assistant Professor currently working at Government Engineering College, Kushalnagar with an excellent academic track record having 13 years of teaching experience in the Department of Electronics and Communication Engineering. He is pursuing a full-time Ph.D. from Visvesvaraya Technological University, Belagavi under the QIP programme in wireless sensor networks at B.M.S. College of Engineering, Bengaluru. He carries his academic credentials with a Bachelor of Engineering in Electronics and Communication Engineering (2006) and a Master of Technology in Digital Electronics and Communication Systems (2008) from Visvesvaraya Technological University, Belagavi. He rendered his service at various levels in teaching, initially as lecturer, then assistant professor, and has been into research for the last few years. He has attended several seminars, national and international conferences, symposiums, and workshops. His fields of interest are wireless communication and sensor networks. He can be contacted at email: maruthibelagere@gmail.com.



Dr. Poornima Govindaswamy    is a committed academician with over 24 years of experience in the Department of Electronics and Communication, B.M.S. College of Engineering. She obtained her Bachelor of Engineering in Electronics and Communication Engineering from Bangalore Institute of Technology and received her master's degree in digital communication engineering from B.M.S. College of Engineering. She holds a Ph.D. in energy efficient and fault tolerant wireless sensor networks from University Visvesvaraya College of Engineering, Bangalore University, Bengaluru, Karnataka, India. Her research interest includes energy efficient computer networks, fault tolerant signal processing, and energy harvesting in wireless sensor networks. She has extensive experience in designing curriculum and developing education pedagogy. She has published over 30 research papers and edited course materials. She has developed courses for VTU EDUSAT and e-Shikshana Programmes. She has fetched grants from MHRD, DRDO, Bengaluru. She was the organizing chair of the IEEE First International Conference on Networking Embedded and Wireless Systems-2018. She is on the editorial board of the Glacier Journal of Scientific Research. She has served as an evaluator/advisor in several evaluation committees constituted by UPSC, AICTE, KPSC, and VTU. She is an IEEE Senior Grade Member, a Fellow IETE, and a Life Member of ISTE. She was awarded Adarsh Vidya Saraswati Rashtriya Puraska in 2018 and Excellence in Higher Education in the year 2019 from the Centre of Leadership Development, Venus International Foundation. She can be contacted at email: gpoornima.ece@bmsce.ac.in.