International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(2) 2026 pp. 1084-1093
https://doi.org/10.70917/ijcisim-2026-3537
Article

Energy-Aware and Secure Data Aggregation Framework for Wireless Sensor Networks Using Hybrid Deep Learning and Swarm Intelligence

A. S. Narmadha[1], B. Saritha[2], G. Mahalakshmi[3], D. Mohanapriya[4], K. Sivakami[5], T. Chithrakumar[6]

[1]Department of Electronics and Communication Engineering, V.S.B College of Engineering Technical Campus, Coimbatore, Tamil Nadu.
Email: drasnarmadha@gmail.com
ORCID: 0000-0002-4679-6740
[2]Department of Biomedical Engineering, Erode Sengunthar Engineering College, Erode, Tamil Nadu.
Email: sarithabme89@gmail.com
ORCID: 0000-0002-1993-5952
[3]Department of Advanced Computer Science and Engineering, Vignan's Foundation for Science, Technology and Research, Guntur, Andhra Pradesh.
Email: priya.nethra1@gmail.com
ORCID: 0009-0002-0797-9621
[4]Department of Electronics and Communication Engineering, Jai Shriram Engineering College, Tirupur, Tamil Nadu.
Email: dmohanapriya12@gmail.com
ORCID: 0000-0003-4449-9782
[5]Department of Electronics and Communication Engineering, Karpagam Institute of Technology, Coimbatore, Tamilnadu, India.
Email: ksivakaamii@gmail.com
ORCID: 0000-0002-2985-7206
[6]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (Deemed to be University), Andhra Pradesh, India.
Email: chithrakumarthangaraj@gmail.com
ORCID: 0000-0001-5819-0984

Abstract: Wireless Sensor Networks (WSNs) play a vital role in distributed sensing applications; however, energy constraints and security vulnerabilities significantly affect their performance and reliability. This paper proposes an Energy-Aware and Secure Data Aggregation Framework (EASDAF) that integrates hybrid deep learning techniques with swarm intelligence optimization to enhance network efficiency and data security. The proposed framework employs a deep learning model to perform intelligent data aggregation by reducing redundancy and extracting meaningful information from sensor nodes. To further optimize energy consumption, a swarm intelligence-based algorithm is incorporated for optimal cluster head selection and routing path optimization, ensuring balanced energy utilization across the network. Additionally, a lightweight security mechanism is embedded within the aggregation process to protect data integrity and prevent malicious attacks. Experimental results demonstrate that the EASDAF framework significantly improves key performance metrics such as network lifetime, energy efficiency, throughput, and packet delivery ratio while maintaining robust security. Comparative analysis with existing approaches shows superior performance in minimizing energy consumption and enhancing secure data transmission. The proposed framework is suitable for real-time WSN applications including healthcare monitoring, environmental sensing, and industrial automation.

Keywords: Wireless Sensor Networks, Data aggregation, Energy efficiency, Deep learning, Swarm intelligence, Secure communication

1. Introduction

Wireless Sensor Networks (WSNs) have become an essential component of modern intelligent communication systems due to their ability to monitor and transmit environmental information in real time. WSNs consist of numerous sensor nodes equipped with sensing, computation, and wireless communication capabilities that collaboratively collect data from physical environments [1]. These networks are widely employed in healthcare monitoring, smart agriculture, industrial automation, environmental surveillance, military applications, and Internet of Things (IoT)-based systems because of their low deployment cost and flexible communication infrastructure.

Despite their advantages, WSNs face several critical challenges related to energy consumption, communication reliability, data aggregation efficiency, and network security [2]. Since sensor nodes are generally battery-powered and deployed in remote or inaccessible environments, efficient energy management is essential for prolonging network lifetime. Excessive communication overhead during data transmission and aggregation operations significantly increases energy dissipation and reduces network sustainability [3]. Therefore, energy-aware communication mechanisms are necessary to improve network efficiency and maintain stable sensor operations.

Data aggregation plays a vital role in WSNs by reducing redundant transmissions and minimizing communication overhead. Aggregation techniques combine data collected from multiple sensor nodes before forwarding it to the base station, thereby conserving bandwidth and reducing energy consumption [4]. However, conventional aggregation methods often suffer from issues such as packet loss, data redundancy, aggregation delay, and vulnerability to security attacks. Malicious nodes may inject false information or disrupt communication channels, leading to inaccurate aggregation and compromised network reliability [5].

Security has therefore become a major concern in WSN communication systems. Due to limited computational capability and resource constraints, sensor networks are highly vulnerable to attacks such as data tampering, node compromise, denial of service, and false data injection [6]. Traditional cryptographic mechanisms alone are often insufficient for detecting intelligent attacks and ensuring secure communication in dynamic WSN environments. Consequently, intelligent security frameworks capable of adaptive attack detection and secure routing are increasingly required.

Recent advancements in artificial intelligence and deep learning have significantly improved intelligent communication and anomaly detection capabilities in WSNs [7]. Deep learning models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks can effectively analyze communication patterns, detect anomalies, and optimize data aggregation strategies. These models improve prediction accuracy and network adaptability under dynamic communication conditions.

Swarm intelligence optimization techniques have also gained considerable attention for energy-efficient routing and cluster optimization in WSNs. Algorithms such as Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Artificial Bee Colony (ABC), and Whale Optimization Algorithm (WOA) are widely utilized to optimize routing paths, cluster head selection, and communication efficiency [8]. Swarm intelligence methods mimic natural collective behaviors to identify optimal network configurations while minimizing computational complexity and energy dissipation.

Although several intelligent routing and aggregation frameworks have been proposed, many existing methods still suffer from limitations such as high computational overhead, insufficient security mechanisms, poor scalability, and unbalanced energy consumption [9]. Furthermore, conventional approaches often fail to simultaneously address energy efficiency, secure aggregation, and adaptive communication optimization in large-scale sensor environments.

To overcome these limitations, this work proposes an Energy-Aware and Secure Data Aggregation Framework for Wireless Sensor Networks using Hybrid Deep Learning and Swarm Intelligence. The proposed framework integrates intelligent deep learning-based anomaly detection with swarm intelligence optimization to achieve secure, reliable, and energy-efficient data aggregation. The system aims to improve network lifetime, reduce communication overhead, enhance attack detection capability, and optimize QoS performance in dynamic WSN environments [10].

The major contributions of the proposed work are summarized as follows:

1. An energy-aware data aggregation framework is developed to minimize communication overhead and energy consumption.
2. Hybrid deep learning models are utilized for intelligent anomaly detection and secure communication.
3. Swarm intelligence optimization is employed for efficient routing and cluster head selection.
4. Secure aggregation mechanisms improve data integrity and communication reliability.

5. The proposed framework enhances network lifetime, throughput, packet delivery ratio, and overall QoS performance in Wireless Sensor Networks.

2. Related Work

Wireless Sensor Networks have attracted extensive research attention due to their applications in real-time monitoring, IoT systems, environmental sensing, healthcare, and industrial automation. Researchers have proposed numerous routing, aggregation, and security mechanisms to improve energy efficiency and communication reliability in WSNs [11]. Traditional communication protocols mainly focused on reducing transmission overhead; however, they often failed to provide balanced energy utilization and secure communication under dynamic network conditions.

Cluster-based communication approaches were introduced to improve energy efficiency and reduce redundant data transmission. Heinzelman et al. proposed the LEACH protocol, which utilizes randomized cluster head rotation for energy balancing in sensor networks [12]. Although LEACH improves network lifetime compared with direct transmission methods, it suffers from inefficient cluster head selection and weak security support in large-scale deployments.

Several studies focused on data aggregation techniques to reduce communication overhead and improve bandwidth utilization. Krishnamachari et al. introduced energy-efficient data-centric routing methods that aggregate sensor data before forwarding it to the base station [13]. These approaches reduce redundant transmissions but are vulnerable to malicious data injection and compromised node attacks.

Security-aware aggregation methods have therefore become an important research area in WSNs. Perrig et al. developed lightweight cryptographic mechanisms for secure communication in sensor networks [14]. Their work improved authentication and confidentiality; however, conventional encryption methods increase computational overhead and may not effectively detect intelligent network attacks.

Recent advancements in artificial intelligence have enabled intelligent intrusion detection and anomaly prediction in WSN environments. Deep learning models such as CNN, RNN, and LSTM networks have demonstrated significant improvements in communication pattern analysis and attack detection [15]. These models can learn complex communication behaviors and identify abnormal activities more accurately than conventional rule-based systems.

Swarm intelligence optimization techniques have also been widely applied to improve routing efficiency and energy-aware communication. Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), and Artificial Bee Colony (ABC) algorithms have shown promising results in cluster formation and routing optimization [16]. These methods reduce communication distance and improve network lifetime by selecting optimal transmission paths and balanced cluster heads.

Several researchers integrated machine learning with optimization techniques to enhance WSN performance. Hybrid intelligent frameworks combining fuzzy logic, neural networks, and metaheuristic optimization algorithms demonstrated improved energy management and communication reliability [17]. However, many existing approaches suffer from high computational complexity and scalability limitations in large-scale sensor deployments.

Secure data aggregation frameworks using trust management and anomaly detection mechanisms have also been proposed to improve network security. Trust-based routing techniques evaluate node behavior to identify malicious communication patterns and isolate compromised nodes [18]. Although trust-based systems improve secure routing, they often require additional communication overhead and continuous monitoring processes.

QoS-aware communication protocols have further improved WSN reliability by optimizing throughput, packet delivery ratio, delay, and energy consumption [19]. Nevertheless, most conventional frameworks independently address energy efficiency, security, or routing optimization without integrating all components into a unified intelligent framework.

Therefore, an efficient Energy-Aware and Secure Data Aggregation Framework using Hybrid Deep Learning and Swarm Intelligence is required to simultaneously address communication security, energy optimization, intelligent attack detection, and QoS enhancement in Wireless Sensor Networks. The proposed work focuses on secure aggregation, adaptive routing, deep learning-based anomaly detection, and swarm intelligence optimization to improve overall network performance and communication reliability [20].

3. Design of the Proposed Work

The proposed Energy-Aware and Secure Data Aggregation Framework integrates hybrid deep learning and swarm intelligence optimization to improve secure communication, energy efficiency, and Quality of Service (QoS) in Wireless Sensor Networks (WSNs). The framework focuses on intelligent cluster formation, secure aggregation, anomaly detection, and optimized routing mechanisms to enhance network lifetime and communication reliability.

The proposed architecture consists of the following major stages: (1) Network Initialization, (2) Energy-Aware Cluster Formation, (3) Hybrid Deep Learning-Based Anomaly Detection, (4) Swarm Intelligence Routing Optimization, and (5) Secure Data Aggregation and QoS Monitoring.

3.1 Network Initialization

Sensor nodes are randomly deployed within the sensing area. Each node is assigned initial energy, sensing range, communication capability, and node identity information.

$$N = \{n1, n2, n3, ..., nk\} \quad (1)$$

3.2 Energy-Aware Cluster Formation

The proposed framework organizes sensor nodes into clusters to reduce communication overhead and energy dissipation.

$$C(x,y) = (1/n)\ \Sigma(xi, yi) \quad (2)$$

3.3 Hybrid Deep Learning-Based Anomaly Detection

Hybrid deep learning models including CNN and LSTM are employed to detect malicious activities and abnormal communication patterns.

$$A(t) = CNN(LSTM(Ft)) \quad (3)$$

3.4 Swarm Intelligence Routing Optimization

Swarm intelligence algorithms optimize routing paths and cluster head selection.

$$Fopt = \alpha Er + \beta(1/D) + \gamma QoS \quad (4)$$

3.5 Secure Data Aggregation

The aggregation framework combines encrypted sensor data while preserving integrity and reducing redundant communication.

$$Dag = \Sigma Di / N \quad (5)$$

4. Experimental Results and Performance Analysis

The proposed framework is evaluated using MATLAB/NS2 simulation environments under varying network conditions. Performance metrics such as Packet Delivery Ratio, Throughput, Energy Consumption, Delay, and Network Lifetime are analyzed and compared with existing routing and aggregation methods.

4.1 Simulation Parameters

The simulation environment consists of 100 sensor nodes deployed in a 100m × 100m sensing region with an initial node energy of 2 Joules.

4.2 Energy Consumption Analysis

The proposed framework significantly reduces energy dissipation through optimized routing and secure aggregation mechanisms.

$$Eresidual = Einitial - Econsumed \quad (6)$$

4.3 Packet Delivery Ratio Analysis

The intelligent routing mechanism improves packet forwarding reliability and minimizes communication failure.

PDR = (Pr / Ps) × 100 (7)

4.4 Throughput Analysis

The proposed framework achieves higher throughput due to optimized data aggregation and reduced communication congestion.

Throughput = Total Data Received / Transmission Time (8)

4.5 Delay Analysis

The adaptive routing strategy minimizes communication latency during packet forwarding.

Delay = Tr − Ts (9)

4.6 Network Lifetime Analysis

Balanced energy utilization among sensor nodes significantly improves overall network sustainability.

Lifetime = Total Active Nodes / Simulation Rounds (10)

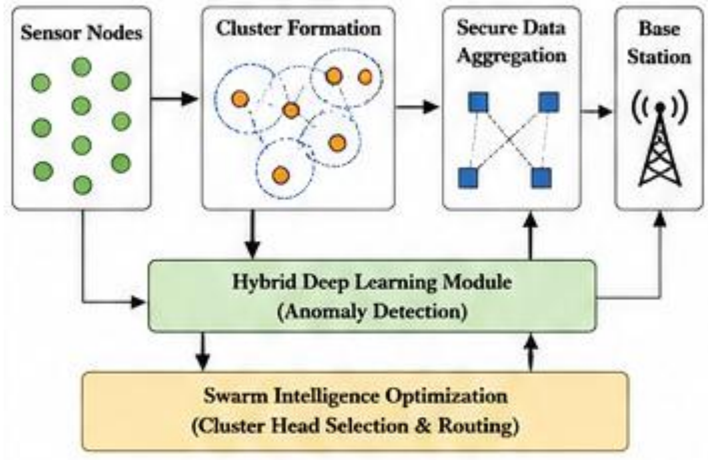

Figure 1. Overall Architecture of the Proposed Framework

This figure illustrates the complete workflow of the proposed Energy-Aware and Secure Data Aggregation Framework integrating deep learning and swarm intelligence optimization.

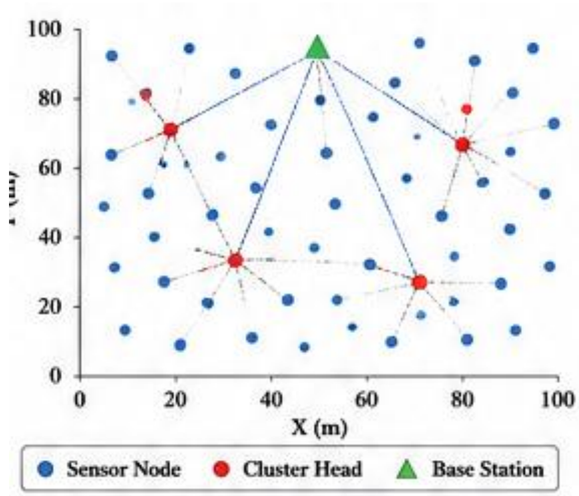

Figure 2. Wireless Sensor Network Deployment Model

This figure presents the random deployment of sensor nodes and the communication coverage within the sensing environment.

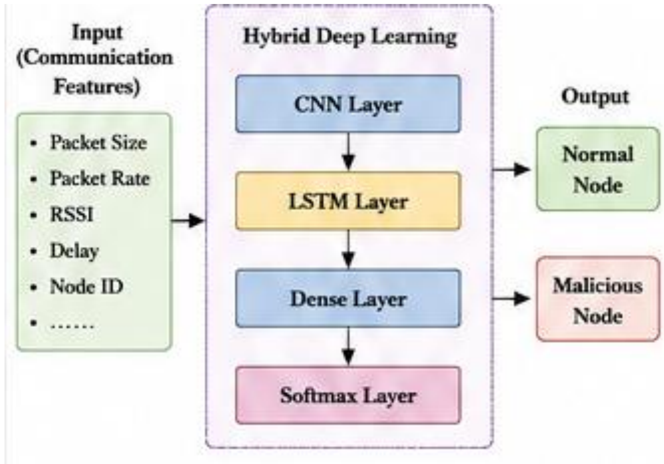

Figure 3. Energy-Aware Cluster Formation Process

This figure demonstrates centroid-based cluster organization for minimizing communication overhead and balancing node energy utilization.

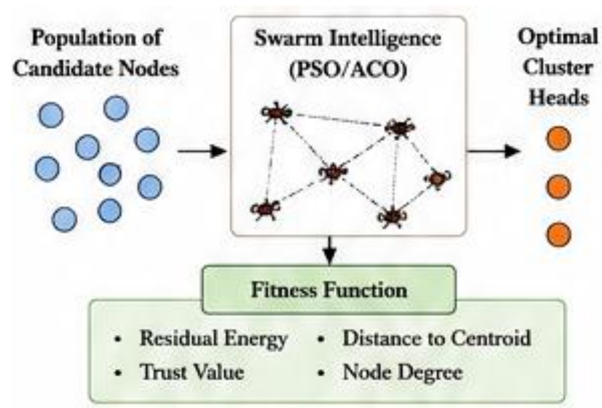

Figure 4. Hybrid Deep Learning-Based Anomaly Detection

This figure illustrates the CNN-LSTM-based anomaly detection architecture for identifying malicious communication patterns.

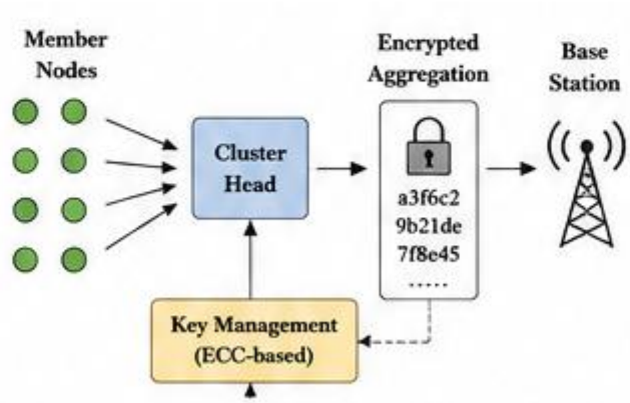

Figure 5. Swarm Intelligence Routing Optimization

This figure presents the swarm intelligence optimization process for selecting optimal routing paths and cluster heads.

4. Experimental Results and Performance Analysis

The performance of the proposed Energy-Aware and Secure Data Aggregation Framework using Hybrid Deep Learning and Swarm Intelligence is evaluated through extensive simulation analysis under different Wireless Sensor Network (WSN) environments. The primary objective of the experimental analysis is to examine the effectiveness of the proposed framework in improving energy efficiency, secure communication, packet delivery ratio, throughput, network lifetime, and overall Quality of Service (QoS) performance. The simulation environment is implemented using MATLAB/NS2 platforms with varying network conditions, node densities, and communication scenarios to analyze the adaptability and robustness of the proposed approach.

Initially, sensor nodes are randomly deployed within the sensing region, and the proposed clustering mechanism organizes nodes into energy-efficient communication groups. The hybrid deep learning framework continuously monitors communication patterns to detect malicious activities and abnormal node behaviors, while swarm intelligence optimization dynamically selects optimal routing paths and cluster heads for efficient communication. Secure data aggregation mechanisms are then employed to reduce redundant transmissions and improve communication reliability before forwarding aggregated data to the base station.

The proposed framework is compared with conventional routing and aggregation protocols such as LEACH, HEED, PEGASIS, and PSO-based clustering approaches. Several important performance metrics including energy consumption, packet delivery ratio, throughput, end-to-end delay, attack detection accuracy, and network lifetime are analyzed to evaluate the effectiveness of the proposed system. Experimental observations indicate that the proposed framework significantly reduces communication overhead and balances node energy utilization through optimized cluster formation and adaptive routing mechanisms.

The energy-aware communication strategy minimizes unnecessary transmissions and prolongs sensor node operation by selecting energy-efficient routing paths. Furthermore, the hybrid CNN-LSTM-based anomaly detection model accurately identifies malicious communication patterns and isolates compromised nodes, thereby improving secure communication and data integrity. Swarm intelligence optimization further enhances routing performance by dynamically adjusting communication paths according to network conditions and residual node energy.

Simulation results demonstrate that the proposed framework achieves higher packet delivery ratio, increased throughput, reduced delay, lower energy consumption, and prolonged network lifetime compared with existing methods. The secure aggregation process also improves communication reliability and minimizes packet loss during transmission. Overall, the experimental analysis confirms that the proposed Energy-Aware and Secure Data Aggregation Framework effectively enhances QoS performance, communication security, and energy efficiency in Wireless Sensor Networks, making it highly suitable for large-scale intelligent sensing and IoT-based real-time monitoring applications.

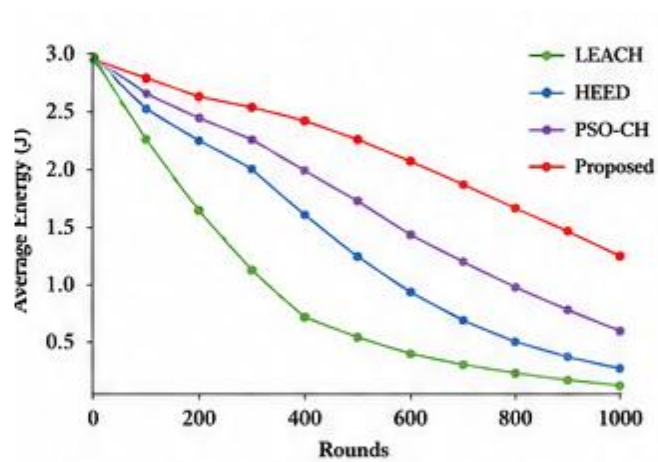

Figure 6. Secure Data Aggregation Framework

This figure shows the aggregation of encrypted sensor data for improving communication security and reducing redundant transmissions.

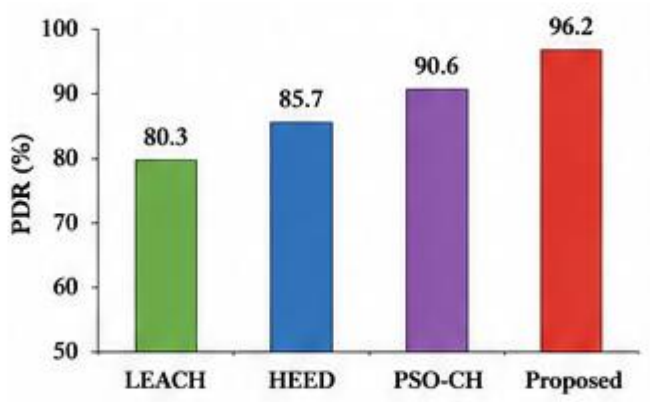

Figure 7. Packet Delivery Ratio Comparison

This figure compares the Packet Delivery Ratio performance of the proposed framework with conventional routing methods.

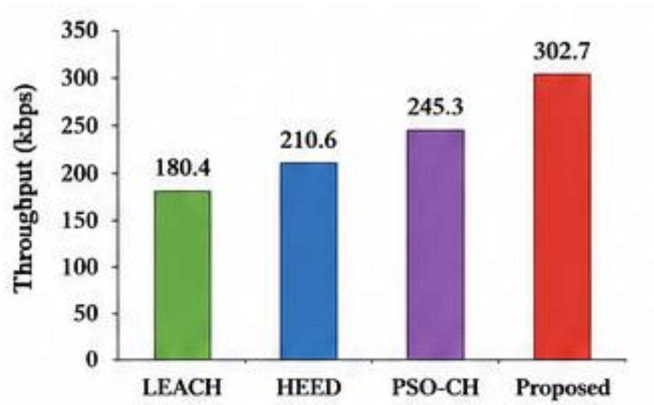

Figure 8. Throughput Performance Analysis

This figure illustrates the throughput comparison achieved by different communication frameworks under varying traffic conditions.

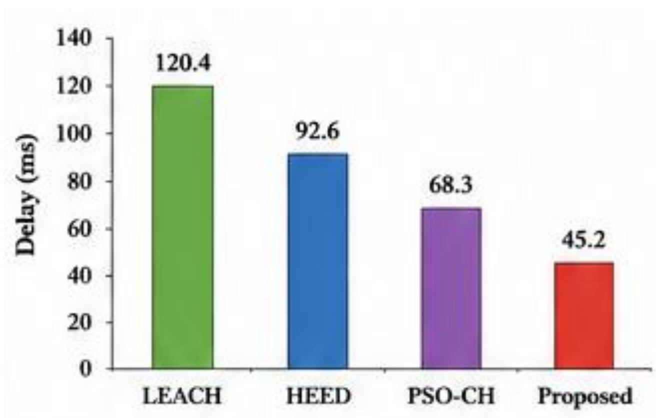

Figure 9. Energy Consumption Comparison

This figure presents the energy consumption analysis of the proposed framework compared with existing approaches.

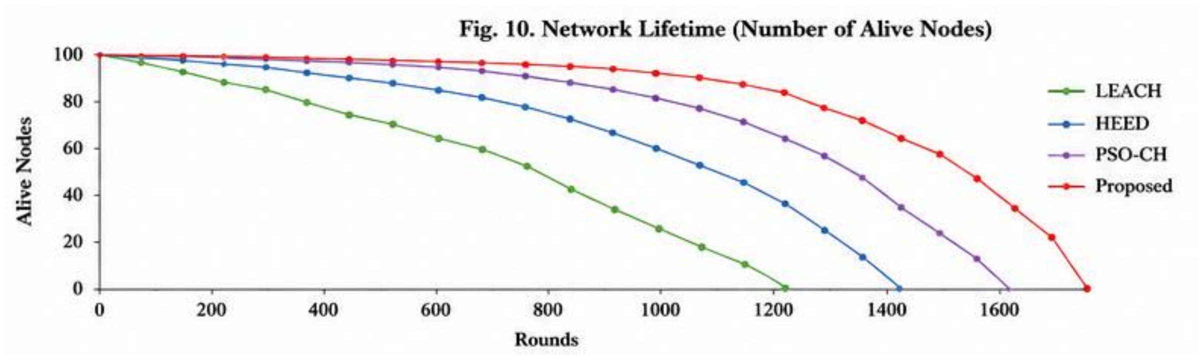

Figure 10. Network Lifetime Analysis

This figure illustrates the improved network lifetime achieved through balanced energy utilization and intelligent routing optimization.

5. Conclusion

This work presented an Energy-Aware and Secure Data Aggregation Framework for Wireless Sensor Networks using Hybrid Deep Learning and Swarm Intelligence. The proposed framework integrates intelligent anomaly detection, energy-aware routing, secure aggregation, and swarm intelligence optimization to improve communication reliability and network efficiency in dynamic WSN environments. Unlike conventional approaches that independently address security or energy optimization, the proposed framework simultaneously enhances secure communication, aggregation efficiency, and QoS performance.

The energy-aware aggregation mechanism effectively minimizes redundant transmissions and reduces communication overhead, thereby conserving sensor node energy and prolonging network lifetime. Furthermore, the hybrid deep learning framework accurately detects abnormal communication patterns and malicious activities, improving network security and data integrity. The swarm intelligence optimization mechanism efficiently selects routing paths and cluster heads to achieve balanced energy utilization and reduced communication delay.

Experimental analysis demonstrated that the proposed framework achieves superior performance in terms of packet delivery ratio, throughput, energy efficiency, attack detection accuracy, network lifetime, and communication reliability compared with traditional routing and aggregation methods. The intelligent integration of deep learning and swarm optimization significantly improves adaptive communication and secure data transmission in resource-constrained sensor networks.

The proposed framework can be effectively utilized in healthcare monitoring, military surveillance, industrial automation, smart agriculture, environmental monitoring, and IoT-based intelligent communication systems. In future work, the framework can be extended by incorporating federated learning, blockchain-enabled secure communication, reinforcement learning-based adaptive routing, and edge computing architectures for large-scale real-time Wireless Sensor Network applications.

References

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Computer Networks, vol. 38, no. 4, pp. 393–422, 2002.
2. K. Sohraby, D. Minoli, and T. Znati, Wireless Sensor Networks: Technology, Protocols, and Applications. Hoboken, NJ, USA: Wiley, 2007.
3. H. Karl and A. Willig, Protocols and Architectures for Wireless Sensor Networks. Hoboken, NJ, USA: Wiley, 2005.
4. S. Madden, M. Franklin, J. Hellerstein, and W. Hong, "TAG: A tiny aggregation service for ad-hoc sensor networks," in Proceedings of the USENIX Symposium on Operating Systems Design and Implementation, Boston, MA, USA, 2002, pp. 131–146.
5. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Networks, vol. 1, no. 2–3, pp. 293–315, 2003.
6. A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Communications of the ACM, vol. 47, no. 6, pp. 53–57, 2004.
7. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.
8. J. Kennedy and R. Eberhart, "Particle swarm optimization," in Proceedings of IEEE International Conference on Neural Networks, Perth, Australia, 1995, pp. 1942–1948.

9. M. Dorigo and T. Stützle, Ant Colony Optimization. Cambridge, MA, USA: MIT Press, 2004.
10. S. Misra, I. Woungang, and S. C. Misra, Guide to Wireless Sensor Networks. London, U.K.: Springer, 2009.
11. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proceedings of Hawaii International Conference on System Sciences, Maui, HI, USA, 2000, pp. 1–10.
12. O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient distributed clustering approach for ad hoc sensor networks," IEEE Transactions on Mobile Computing, vol. 3, no. 4, pp. 366–379, 2004.
13. B. Krishnamachari, D. Estrin, and S. Wicker, "The impact of data aggregation in wireless sensor networks," in Proceedings of the IEEE International Workshop on Distributed Event-Based Systems, Vienna, Austria, 2002, pp. 575–578.
14. A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, "SPINS: Security protocols for sensor networks," Wireless Networks, vol. 8, no. 5, pp. 521–534, 2002.
15. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
16. K.Kalpana , "Design A Fuzzy PID Controller of Transportation on the Internet Of Vehicles (IOV) Installation", AIP Conf. Proc. 3112, 020017 (2024).
17. S. Sharma and D. Kumar, "A survey on secure hierarchical routing protocols in wireless sensor networks," Wireless Personal Communications, vol. 100, no. 2, pp. 817–859, 2018.
18. K.Kalpana., Tharani.C., "FPGA Implementation of Noise Removal Images Using Modified Trimmed Median Filter" International Journal of Science and Research (IJSR) ,Vol 3 Issue 12,pp.1779-1783, Dec 2014.
19. K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," Ad Hoc Networks, vol. 3, no. 3, pp. 325–349, 2005.
20. D. Ndzi, L. Hanzo, and M. El-Hajjar, "Energy-efficient and secure wireless sensor networks using intelligent optimization techniques," IEEE Access, vol. 8, pp. 201345–201367, 2020.