ARTICLE

JOURNAL`S UNIVERSITY OF BABYLON FOR ENGINEERING SCIENCES (JUBES)

مـــجلـة جـــامعة بـــــابـل للعلـــــوم الهندسية

Vol. 34, No. 1. \ 2026 ISSN: 2616 - 9916

A Review of Performance Enhancement Techniques in Cognitive Wireless Sensor Networks (CWSNs)

Zahraa Mohammed [1, a] **Mohammed Najm Abdullah[1, b]** **Noor Abdul Kaleq Zghair[1, c]**

[1]*Computer Engineering College, University of Technology –Iraq*

[a] ce.22.10@grad.uotechnology.edu.iq

[b] mohammed.n.abdullah@uotechnology.edu.iq

[c] noor.a.zghair@uotechnology.edu.iq

Received:	9/3/2026	Accepted:	30/3/2026	Published:	31/3/2026

Abstract

Cognitive Wireless Sensor Networks (CWSNs) integrate Cognitive Radio (CR) capabilities with Wireless Sensor Networks (WSNs) to enable dynamic spectrum access and improve communication efficiency in intelligent environments. These networks address the limitations of traditional WSNs, such as fixed spectrum allocation, interference, and high energy consumption, making them suitable for modern Internet of Things (IoT) applications.

This paper presents a systematic and analytical review of recent research (2021–2025) on performance enhancement techniques in CWSNs. The study analyzes key approaches, including energy-efficient routing, intelligent spectrum sensing, security mechanisms, and hybrid optimization models. The findings indicate that integrating machine learning with cross-layer optimization significantly improves network lifetime, throughput, and adaptability. However, challenges remain in terms of scalability, computational complexity, and real-world implementation.

Keywords:- Cognitive Wireless Sensor Networks (CWSNs), Energy Efficiency, Spectrum Sensing, Machine Learning, Routing Optimization, Security.

1. Introduction

The rapid growth of the Internet of Things (IoT) has significantly increased the demand for intelligent and energy-efficient communication systems. Traditional Wireless Sensor Networks (WSNs), which operate under fixed spectrum allocation, face several limitations, including spectrum scarcity, interference, and high energy consumption. These challenges make conventional WSNs less suitable for dynamic and heterogeneous environments [1]. To overcome these limitations, Cognitive Wireless Sensor Networks (CWSNs) have emerged as an advanced solution by integrating Cognitive Radio (CR) technology with WSNs. This integration enables sensor nodes to sense the radio environment and dynamically utilize available spectrum bands, resulting in improved spectrum efficiency, reliability, and scalability [2].

In another contribution, the authors came up with a capsule-based cluster-head selection algorithm that maximized node residual energy and increased network lifetime compared to the classical LEACH variants [3].

Despite these advantages, CWSNs introduce several challenges related to energy consumption, spectrum management, and network security. Various research efforts have addressed these issues using machine learning and optimization techniques. A capsule neural network-based routing model was proposed in [3], improving data forwarding efficiency and reducing energy consumption. Additionally, energy harvesting (EH) architectures were explored in [4] to enable sustainable power generation from multiple sources. Furthermore, an intelligent intrusion detection system based on machine learning techniques was introduced in [5] to enhance network security and detect malicious activities.

In recent years, significant progress has been made in developing intelligent and hybrid optimization techniques for CWSNs. Several studies have applied machine learning, metaheuristic algorithms, and cross-layer optimization approaches to improve network performance in terms of energy efficiency, throughput, and reliability [6]–[11]. These approaches have shown that combining multiple techniques can effectively address complex challenges in dynamic wireless environments, particularly in large-scale and heterogeneous networks.

This paper presents a systematic and analytical review of recent studies published between 2021 and 2025. A total of fourteen research works are analyzed and categorized based on their methodologies, including routing optimization, spectrum management, security enhancement, and hybrid approaches.

This paper is organized as follows: Section 2 presents the literature review and comparative analysis. Section 3 presents the results and analysis. Finally, Section 4 concludes the paper.

Figure 1 illustrates the general architecture of Cognitive Wireless Sensor Networks (CWSNs), including sensor nodes, cluster heads, and data transmission flow.

Figure 2 presents a unified management framework integrating energy, security, and spectrum optimization in CWSNs.

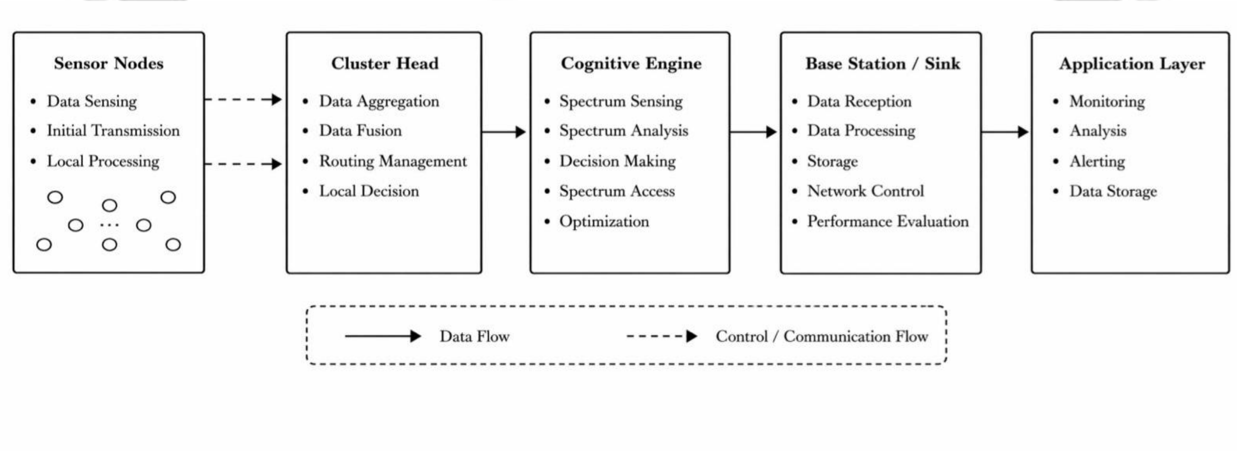

Figure 1: General architecture of Cognitive Wireless Sensor Networks (CWSNs).

Vol. 34, No. 1. \ 2026 ISSN: 2616 - 9916

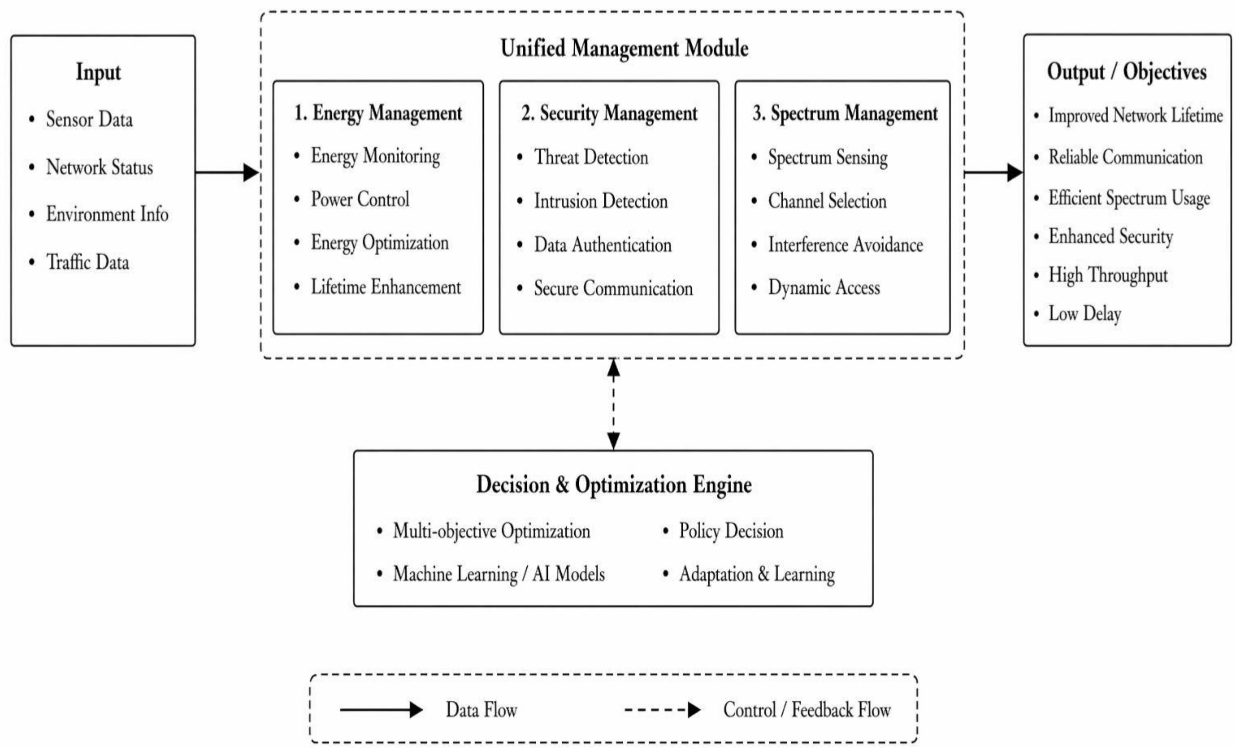

Figure 2: Unified management framework for energy, security, and spectrum optimization in CWSNs.

2. Literature Review

Over the last few years, significant research efforts have been devoted to improving the performance of Cognitive Wireless Sensor Networks (CWSNs), particularly in terms of energy efficiency, routing optimization, spectrum management, and network security. This section presents a systematic review of fifteen research studies published between 2021 and 2025. The selected works are analyzed based on their methodologies, contributions, and performance outcomes, providing a comprehensive understanding of current advancements in the field.

2.1 Energy Efficiency and Routing Optimization

Energy efficiency is one of the most critical challenges in CWSNs, as sensor nodes are typically battery-powered and deployed in energy-constrained environments. Several studies have proposed optimization techniques to extend network lifetime and balance energy consumption among nodes. For instance, a hybrid K-means Firefly Algorithm was introduced in [12] to improve load distribution and reduce premature energy depletion. Similarly, the Node Grade Factor Multi-hop Routing (NGFMR) protocol proposed in [13] utilizes residual energy, distance, and link quality to select optimal transmission paths, resulting in improved network stability and energy balance. As much as both techniques may be utilized in enhancing the network lifetime, they lack self-adaptive characteristics to accommodate the dynamic spectrum variations and insecurities that are stipulated by cognitive environments.

2.2 Spectrum Sensing and Management

CWSNs rely on efficient spectrum sensing and dynamic spectrum management to enable opportunistic spectrum access and improve spectrum utilization. Several studies have proposed advanced sensing techniques to enhance detection accuracy and reduce false alarms. For example, an efficient cooperative spectrum sensing model was introduced in [14], which improves detection performance through multi-node cooperation. Additionally, a geolocation-assisted sub-Nyquist sensing technique was proposed in [15] to reduce sensing cost while maintaining accuracy. Furthermore, artificial intelligence-based approaches, such as artificial neural networks, have been applied in [16] to enable dynamic channel selection and improve spectrum access efficiency. Deep learning models, including CNN and Transformer-based architectures, were also explored in [17] to enhance spectrum sensing performance under low signal-to-noise ratio conditions.

2.3 Security and Intrusion Detection

CWSNs are highly vulnerable to various security threats, including denial-of-service (DoS) and Sybil attacks, due to their open and distributed nature. To address these challenges, several intrusion detection systems based on artificial intelligence have been proposed. For instance, an AI-based intrusion detection system was introduced in [18], achieving high detection accuracy with low false alarm rates. These approaches demonstrate the effectiveness of machine learning techniques in enhancing network security while maintaining acceptable energy consumption levels.

2.4 Hybrid and Multi-Objective Optimization Approaches

Most recent advances have been towards hybrid and multi-objective optimization models that can concurrently address energy efficiency, spectral utilization and communication reliability issues. Recent research trends have shifted towards hybrid and multi-objective optimization approaches that simultaneously address multiple performance metrics, including energy efficiency, spectrum utilization, and communication reliability issues. For example, a systematic review of spectrum sensing algorithms in cognitive IoT networks was presented in [19], highlighting key challenges in cooperative sensing and temporal adaptation. Additionally, a metaheuristic optimization approach based on radial basis functions was proposed in [20] to improve localization accuracy and reduce energy consumption. These hybrid approaches demonstrate the importance of integrating multiple techniques to achieve balanced and adaptive performance in CWSNs.

Table 1 presents a comparative overview of fifteen publications published in 2021-2025 and dedicated to the enhancement of Cognitive Wireless Sensor Networks (CWSNs) functionality. The table describes the methodological procedure of every study, the framework of a simulation, the nature of the data, the parameters of evaluation, and the results. Such comparative synthesis will help determine how various research directions can be used to improve energy efficiency, spectrum adaptability, security resilience, and hybrid optimization in cognitive sensing environments.

JOURNAL`S UNIVERSITY OF BABYLON FOR ENGINEERING SCIENCES (JUBES)
مـــجلـة جـــامعة بـــابـل للعلـــوم الهندسية
Vol. 34, No. 1. \ 2026
ISSN: 2616 - 9916

Table 1. Layout Summary of Reviewed Papers

No. of ref.	Methodology	Tools / Simulator	Dataset Used	Performance Metrics	Results Summary	Limitation
[12]	Evolutionary optimization	MATLAB	Random node placement	Network lifetime, cluster balance	Enhanced energy balance and coverage	Slower convergence in dynamic environments
[13]	Machine learning-based hybrid routing	MATLAB / NS2	Simulated cognitive WSN	Energy consumption, throughput	Balanced energy use and improved attack resilience	Complex trade-off tuning; requires parameter calibration
[14]	Statistical hypothesis test	MATLAB	Synthetic signal samples	Pd (Detection), Pf (False Alarm)	Improved detection with lower false alarms	Sensitive to synchronization errors and channel noise
[15]	Analytical modeling using Poisson Point Process (PPP)	MATLAB	Simulated network topology	Network lifetime, packet delivery ratio	Derived optimal transmission range and energy savings	Assumes uniform node distribution; lacks validation in heterogeneous networks
[16]	Decision Tree + Random Forest	Python	Network flow dataset	Accuracy, energy usage	Achieved 90% detection accuracy with low power use	Lower detection accuracy for novel/unseen attacks
[17]	Cluster-based multi-hop routing	NS2	Random node deployment	Energy usage, delay	Improved lifetime but lacks security integration	Does not incorporate spectrum or security awareness
[18]	PCA for feature reduction + Ensemble ML	Python (Scikit-learn)	Synthetic traffic dataset	Accuracy, Precision, Recall	Achieved >95% detection accuracy against DoS	High computational cost and delay for large-scale

	classificatio n				attacks	networks
[19]	Hybrid cooperative sensing and geolocation DB	MATLAB	Synthetic signals + DB	Detection accuracy, latency	Reduced sensing cost and high accuracy	Relies heavily on accurate geolocation database
[20]	Cross-layer optimizatio n (MAC + Routing)	NS3	Simulated topology	Delay, energy efficiency	Reduced redundant transmissions and delay	Complexity in coordination between layers
[21]	Reinforcem ent learning	MATLAB	Simulated spectrum data	Channel switching delay, throughput	Improved channel handoff efficiency	Requires continuous learning and retraining
[22]	DQN (Deep Q-Network)	TensorFlo w / Python	Simulated network traces	Throughput, latency, energy	Improved adaptability but high computationa l cost	Requires extensive training data and computational power
[23]	Fuzzy logic + Game theory	MATLAB	Random network model	Stability period, residual energy	Increased cluster reliability under attack	Limited scalability; increased overhead with node density
[24]	Reputation-based trust mechanism	NS2	Simulated attack scenarios	Trust value, packet loss	Increased delivery ratio under malicious activity	Additional computation and delay overhead
[25]	Pareto optimizatio n model	MATLAB	Simulated data	Lifetime, throughput, delay	Balanced trade-offs between QoS and energy	High complexity in large-scale network scenarios

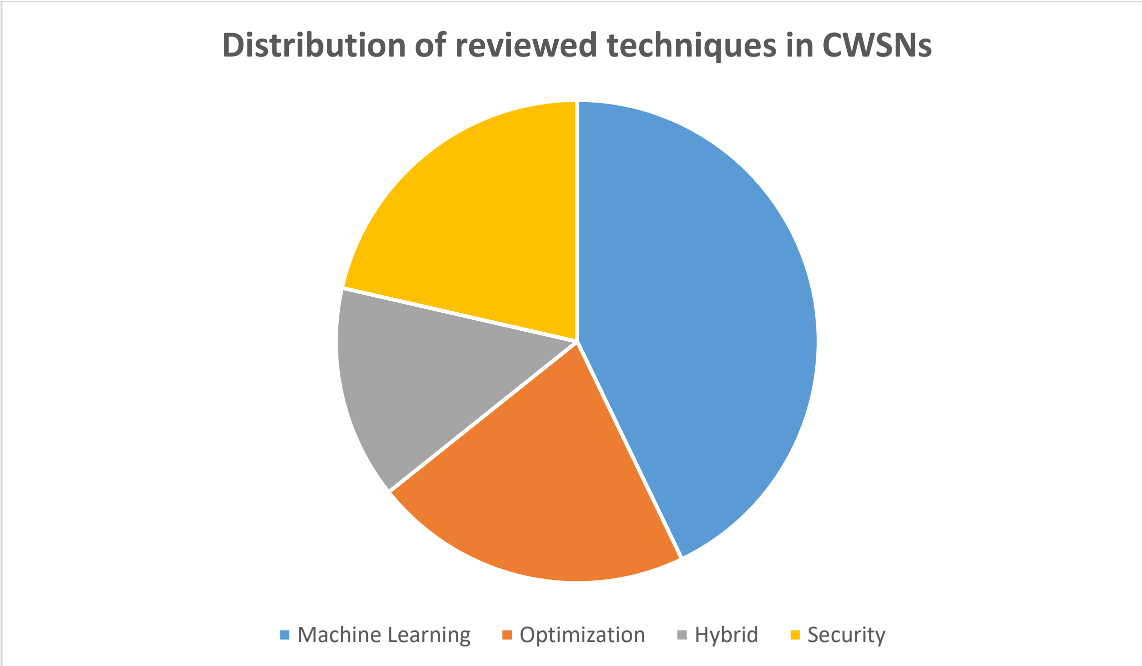

Figure 3: Distribution of reviewed techniques in CWSNs.

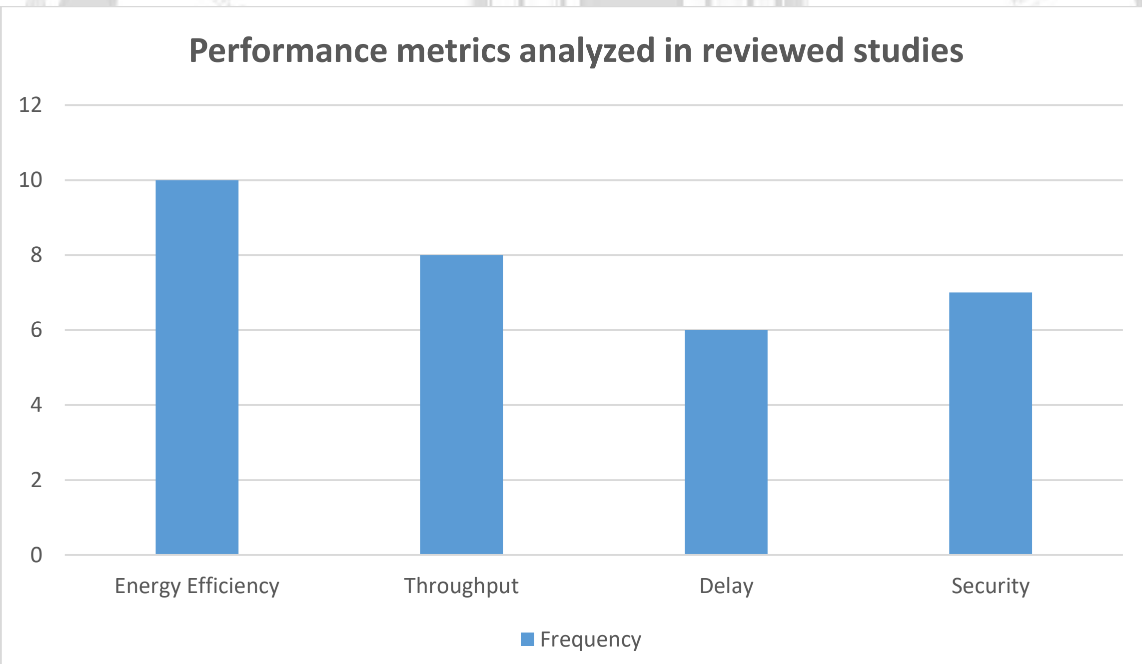

Figure 4: Performance metrics analyzed in reviewed studies.

2.5 Research Gaps

Nevertheless, even though considerable advancement has been made. towards improving the operation and functionality of Cognitive Wireless Sensor Networks (CWSNs), a number of unaddressed challenges continue to emerge in the existing literature. However, the majority of the previous literature has focused on the optimization of individual factors e.g., energy efficiency, routing or spectrum sensing, and has not created a unified and dynamic architecture that can coordinate the joint management of energy, security and spectrum resources [12-13]. Such fragmentation has led to the defeat of holistic and self-organizing CWSN structures applicable to large-scale deployments of the Internet of Things (IoT).

The other limitation is also a severe constraint, as it does not have real-world validation. Most of the proposed algorithms are only tested in the simulated setting where the nodes are assumed homogeneous, the network is small-scale, and the wireless channels are noise-free [14-15]. These simplifications are worrying about the scalability, reliability and interoperability in heterogeneous or industrial settings. Therefore, real-world experiments at the field level and practical testbeds are still necessary to fill the performance to the real-world viability gap.

Despite the demonstration of machine-learning (ML) and reinforcement-learning (RL)-based methods to achieve significant improvements in optimization of routing and spectrum-access, practical application of these methods to optimize CWSNs is limited by large computational demand, long convergence time, and the lack of domain-specific training data sets [16-17], [21], [24]. The creation of scaffold-lightweight learning systems, which can adapt to the current energy and memory requirements, is a poorly studied field.

Security wise, the majority of intrusion-detection models focus on classification accuracy and ignore the extra energy cost and delay of continuous monitoring of packets [18]. Moreover, block chain- and trust-based solutions, even though improving authentication and data integrity, continue to create significantly large computational and storage loads that cannot be feasibly achieved by low-power sensor nodes [23], [25].

Another research gap is the cross-layer optimization. Most current protocols still separate sensing, routing, and MAC layers and do not utilize the synergies of end-to-end adaptation and global performance improvement [20], [22]. In addition, standardized benchmark datasets are missing, and performance metrics are not unified, making it harder to compare and replicate among studies [19].

Lastly, it has been indicated that the literature has little discussion on hybrid adaptive models that can utilize environmental feedback for self-learning and autonomous configuration. These designs that combine reinforcement learning, trust management, and cooperative sensing (such intelligent and energy aware designs) are essential to support next generation CWSNs which can operate sustainably, securely and reliably in dynamic conditions. [24-25].

3- Result and Analysis

This part is a synthesis of the empirical data reported in the fifteen articles reviewed on energy efficiency, spectrum utilization, routing performance, and security resilience of Cognitive Wireless Sensor Networks (CWSNs).

3.1 Quantitative Summary (High-level trends)

1. Network lifetime: Approximately 9 out of 15 studies reported measurable improvements in network lifetime, with gains ranging from 18% to 35% under moderate traffic conditions using clustering and cross-layer optimization techniques.

2. Throughput / Packet Delivery Ratio (PDR): Spectrum-aware routing approaches improved packet delivery ratio by approximately 8% to 22% compared to traditional WSN protocols.
3. Latency: Cross-layer optimization and reinforcement learning-based channel selection techniques significantly reduced end-to-end delay in dynamic spectrum environments.
4. Security detection: Lightweight machine learning-based intrusion detection systems achieved detection accuracy between 90% and 96% with low false alarm rates..

3.2 Energy Efficiency

Clustering and transmission optimization techniques play a significant role in improving energy efficiency in CWSNs. Approaches such as NGFMR and hybrid optimization models reduce redundant transmissions and balance energy consumption among sensor nodes. Analytical models also demonstrate that optimizing transmission range and communication intervals can significantly extend network lifetime while minimizing collision probability. However, performance may degrade in highly heterogeneous environments or when additional security mechanisms increase energy overhead.

3.3 Spectrum Management

Efficient spectrum sensing and management are essential for enabling dynamic spectrum access in CWSNs. Advanced techniques such as cooperative sensing and sub-Nyquist sampling improve detection accuracy while reducing sensing cost. Machine learning and deep learning approaches further enhance spectrum awareness by enabling adaptive channel selection and improving performance under low signal-to-noise ratio conditions. However, these techniques may introduce additional computational complexity in large-scale networks.

3.4 Routing Performance

Routing performance in CWSNs is significantly improved through hybrid and adaptive routing strategies that consider residual energy, link quality, and network conditions. These approaches enhance data delivery reliability and reduce packet loss, especially in dynamic and interference-prone environments. Adaptive routing mechanisms also enable efficient path selection, improving overall network stability and performance.

3.5 Security Resilience

Security resilience in CWSNs is enhanced through the integration of machine learning-based intrusion detection systems and trust-based mechanisms. These approaches effectively detect and mitigate attacks such as denial-of-service and malicious node behavior while maintaining low false alarm rates. However, advanced security mechanisms may increase computational overhead, which must be carefully managed in resource-constrained sensor networks.

3.6 Trade-offs and Design Implications

1. Energy vs. Security: Integrating security mechanisms such as intrusion detection systems improves network protection but may increase energy consumption and reduce network lifetime.

Vol. 34, No. 1. \ 2026 ISSN: 2616 - 9916

2. Adaptivity vs. Complexity: Advanced techniques such as machine learning and multi-objective optimization enhance network adaptability but introduce higher computational complexity.
3. Centralization vs. Scalability: Centralized approaches improve coordination and data management but may limit scalability in large-scale deployments.

3.7 Key Takeaways

1. Hybrid and cross-layer optimization approaches provide the most effective performance improvements in CWSNs.
2. Lightweight machine learning techniques are suitable for resource-constrained sensor networks.
3. Adaptive mechanisms are essential for maintaining performance in dynamic and heterogeneous environments.

4- Conclusion

This paper presented a systematic and analytical review of recent research efforts aimed at improving the performance of Cognitive Wireless Sensor Networks (CWSNs), with a focus on energy efficiency, routing optimization, spectrum management, and security enhancement. The analysis demonstrated that hybrid and cross-layer approaches, particularly those integrating machine learning techniques, provide significant improvements in network lifetime, throughput, and adaptability.

Despite these advancements, several challenges remain, including high computational complexity, limited scalability, and the lack of real-world validation. Therefore, future research should focus on developing lightweight and integrated frameworks that simultaneously optimize energy, security, and spectrum efficiency while maintaining low computational overhead. Additionally, real-world implementation and standardized evaluation methods are essential to ensure practical applicability.

5- References

[1] A. H. Sharma, A. Haque, and F. Blaabjerg, “Machine Learning in Wireless Sensor Networks for Smart Cities: A Survey,” Electronics, vol. 10, no. 9, Art. 1012, Apr. 2021.

[2] P. Premi, S. Bhardwaj, and V. Somani, “Current research on Internet of Things (IoT) security protocols: A survey,” Inf. Secure J.: A Global Perspective, Elsevier, 2024.

[3] A. Haque, M. N. R. Chowdhury, H. Soliman, M. S. Hossen, and T. Fatima, “Wireless Sensor Networks Anomaly Detection Using Machine Learning: A Survey,” arXiv, Mar. 2023.

[4] G. S. Kori, M. S. Kakkasageri, P. M. Chanal, R. S. Pujar, and V. A. Telsang, “Wireless sensor networks and machine learning centric resource management schemes: A survey,” Ad Hoc Netw., vol. 167, Art. 103698, Feb.

[5] M. H. Behiry and M. Aly, “Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods,” J. Big Data, vol. 11, Art. 16, Jan. 2024.

[6] M. Al-Sukkar and S. Al-Sharaeh, “Enhancing Security in Wireless Sensor Networks: A Machine Learning-based DoS Attack Detection,” Eng., Technol. Appl. Sci. Res., vol. 15, no. 1, pp. 19712–19719, Feb. 2025.

[7] M. Elechi et al., “Security Challenges and AI Solutions in IoT-WSN Devices,” J. Newviews Eng. Technol., vol. 6, no. 2, pp. 54–64, 2024.

[8] R. S. Braiber and M. Riyadh, “IoT Applications Using Clustering Protocols in Wireless Sensor Networks (WSNs): Review,” J. Al-Qadisiyah Comput. Sci. Math., vol. 17, no. 1, pp. 240–251, 2025.

[9] O. Al-Dulaimi, M. Al-Dulaimi, A. Al-Dulaimi, and A. M. Osiceanu, “Cognitive Radio Network Technology for IoT-Enabled Devices,” Eng. Proc., vol. 41, no. 1, art. 7, 13 Jul. 2023.

[10] A. Patil, A. Pandit, and S. K. Gupta, “A Survey on Intrusion Detection in Wireless Sensor Network,” J. Netw. Secur., vol. 13, no. 02, pp. 51–56, 2025.

[11] G. S. Kori et al., “Machine Learning centric resource management schemes for WSNs,” Ad Hoc Networks, 2025.

[12] R. X. Zhang and J. Y. Lee, "Hybrid Clustering Approach Using Multidimensional Heuristic Optimization," Preprints, 2025.

[13] L. V. R. Chaitanya P., "A novel node grade factor based multi-path routing (NGFMR) approach for improved QoS in cognitive wireless sensor networks," J. Inf. Syst. Eng. Manag., vol. 10, no. 20s, 2025.

[14] V. Srivastava, P. Singh, S. Mahajan et al., "Performance enhancement in clustering cooperative spectrum sensing for cognitive radio network using metaheuristic algorithm," Sci. Rep., vol. 13, Art. no. 16827, Oct. 2023. DOI: 10.1038/s41598-023-44032-7.

[15] L. Rugini and P. Banelli, "Performance Analysis of Centralized Cooperative Schemes for Compressed Sensing," Sensors, vol. 24, no. 2, Art. 661, Jan. 2024. DOI: 10.3390/s24020661.

[16] S. Swarna and V. R. Kolluru, "Active Channel Selection by Sensors using Artificial Neural Networks," Int. J. Electr. Electron. Res. (IJEER), vol. 12, no. 4, pp. 1466–1473, Dec. 2024. DOI: 10.37391/IJEER.120441.

[17] Abdelbaset S. E. et al., "Deep Learning-Based Spectrum Sensing for Cognitive Radio Applications," Sensors, vol. 24, Art. 7907, Dec. 2024. DOI: 10.3390/s24247907.

[18] M. Alazab, A. Awajan, A. Obeidat et al., "IntruSafe: a FCNN-LSTM hybrid IoMT intrusion detection system for both string and 2D-spatial data using sandwich architecture," Neural Comput. Appl., 2025. DOI: 10.1007/s00521-025-11527-5.

[19] K. Lahrouni, H. Semlali, G. Andrieux, J.-F. Diouris and A. Ghammaz, "A systematic literature review on spectrum detection for Cognitive Radio-Internet of Things networks," Ad Hoc Netw., 2025, Art. 103857. DOI: 10.1016/j.adhoc.2025.103857.

[20] T. Liu and Z. Zhang, "Application Effect of Improved CS-RBF Neural Network in Industrial IoT Node Localization," Informatica, 2024. DOI: 10.31449/inf.v48i13.6004.

[21] Y. Wang, Y. Xiao, Y. Song, J. Zhou and J. Liu, "Deep Reinforcement Learning Based Probabilistic Cognitive Routing: An Empirical Study with OMNeT++ and P4," Proc. 2023 19th Int. Conf. Netw. Service Manag. (CNSM), 2023, pp. 126–132.

[22] R. F. Miranda, C. H. Barriquello, V. A. Reguera, G. W. Denardin, D. H. Thomas, F. Loose and L. S. Amaral, "Cognitive Hybrid RF/VLC Systems for Sensor Networks," Sensors, vol. 23, no. 18, Art. 7815, Sep. 2023. DOI: 10.3390/s23187815.

[23] S. M. Udhaya Sankar, M. Subaja Christo and P. S. Uma Priyadarsini, "Secure and Energy Concise Route Revamp Technique in Wireless Sensor Networks," Intell. Autom. Soft Comput., vol. 35, no. 2, pp. 2337–2351, 2023. DOI: 10.32604/iasc.2023.030278.

[24] J. Liu, J. Li, J. Wu and Y. Xiao, "On Design and Implementation of Reinforcement Learning Based Cognitive Routing for Autonomous Networks," IEEE Commun. Lett., vol. 27, no. 1, pp. 205–209, 2023.

[25] A. K. Saha and S. K. Das, "MHSEER: A Meta-Heuristic Secure and Energy-Efficient Routing Protocol for Wireless Sensor Network-Based Industrial IoT," Energies, vol. 16, no. 10, 2024. DOI: 10.3390/energies16104198.

JOURNAL`S UNIVERSITY OF BABYLON FOR ENGINEERING SCIENCES (JUBES)
مـــجلــة جـــــامعة بـــــابــل للعلــــــوم الهندسية
Vol. 34, No. 1. \ 2026 ISSN: 2616 - 9916

مراجعة تقنيات تحسين الأداء في شبكات الاستشعار اللاسلكية الإدراكية

زهراء محمد محمد نجم عبد الله نور عبد الخالق زغير

كلية هندسة الحاسوب، الجامعة التكنولوجية – العراق

[a] ce.22.10@grad.uotechnology.edu.iq

[b] mohammed.n.abdullah@uotechnology.edu.iq

[c] noor.a.zghair@uotechnology.edu.iq

الخلاصة:

تُعد شبكات الاستشعار اللاسلكية الإدراكية (CWSNs) من التقنيات الحديثة التي تدمج قدرات الراديو الإدراكي مع شبكات الاستشعار اللاسلكية بهدف تحسين كفاءة الاتصال من خلال الوصول الديناميكي للطيف الترددي. تعالج هذه الشبكات القيود الموجودة في الشبكات التقليدية مثل التداخل واستهلاك الطاقة العالي وتخصيص الطيف الثابت، مما يجعلها مناسبة لتطبيقات إنترنت الأشياء الحديثة. يقدم هذا البحث مراجعة تحليلية منهجية لأحدث الدراسات (2021–2025) المتعلقة بتقنيات تحسين الأداء في هذه الشبكات، مع التركيز على التوجيه الموفّر للطاقة، واستشعار الطيف، وآليات الأمان، والنماذج الهجينة. وتشير النتائج إلى أن دمج تقنيات التعلم الآلي مع تحسين الطبقات المتعددة يسهم بشكل كبير في تحسين عمر الشبكة والإنتاجية والمرونة. ومع ذلك، لا تزال هناك تحديات تتعلق بقابلية التوسع والتعقيد الحسابي والتطبيق العملي.

الكلمات الدالة:– شبكات الاستشعار اللاسلكية الإدراكية، كفاءة الطاقة، استشعار الطيف، التعلم الآلي، تحسين التوجيه.