International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

AI-Driven Intrusion Detection and Energy-Efficient Routing in Internet of Things (IoT) Networks

Mr. Mamoun Yaqoub Mmoun[1], Mr. Abdulghader Jalgum[2]

[1,2]Information Technology, College Of Science And Technology Alzweah, Alzweah, Wadi Alshatti, Libya

Abstract

The Internet of Things (IoT) has become an important part of modern communication systems by connecting sensors, smart devices, wearable technologies, industrial equipment, and other physical objects through the internet. Although IoT networks provide many benefits, they also face serious challenges related to cybersecurity and energy consumption. Most IoT devices have limited processing power, memory, and battery capacity, making them vulnerable to cyberattacks and difficult to protect using traditional security methods. This paper proposes an AI-driven framework for intrusion detection and energy-efficient routing in IoT networks. The framework uses machine-learning techniques to identify malicious network traffic and classify it as normal or abnormal. At the same time, it applies an energy-aware routing strategy to select communication paths based on node energy level, link quality, delay, and security status. The proposed approach aims to improve attack detection while reducing unnecessary energy consumption in IoT devices. The framework can be evaluated using security metrics such as accuracy, precision, recall, F1-score, and false-positive rate, as well as network metrics including packet delivery ratio, delay, throughput, residual energy, and network lifetime. The study is expected to show that combining artificial intelligence with energy-aware routing can improve both the security and efficiency of IoT networks.

Keywords: Internet of Things; IoT Security; Intrusion Detection System; Artificial Intelligence; Machine Learning; Energy-Efficient Routing; Network Security; Wireless Sensor Networks; Cyberattacks.

1. Introduction

The Internet of Things has changed the way devices communicate and exchange information. IoT networks consist of many connected devices such as sensors, cameras, smart home appliances, wearable health devices, vehicles, industrial machines, and environmental monitoring systems [1]. These devices collect data from their surroundings and send it through communication networks to servers, cloud platforms, gateways, or other connected devices. IoT technology is now widely used in healthcare, agriculture, transportation, smart cities, manufacturing, education, and home automation [2].

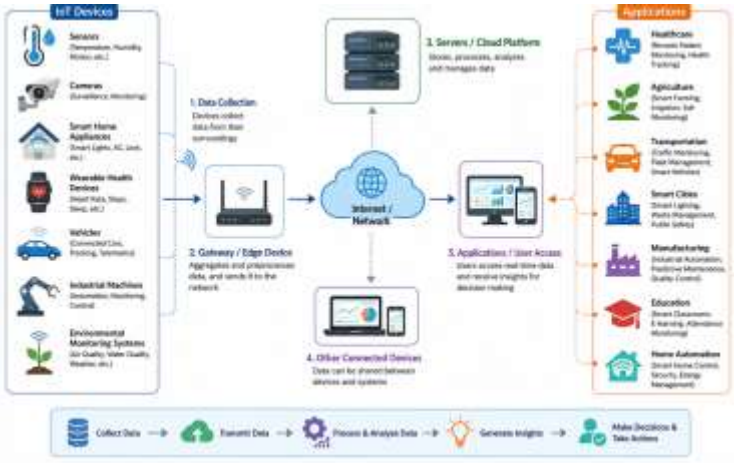

Figure 1. IoT Communication and Applications

Despite its advantages, IoT also introduces several technical challenges [3]. One of the main challenges is cybersecurity [4]. IoT devices are often connected to wireless networks and may have weak security settings because of their limited memory, battery power, and processing capabilities. This makes them vulnerable to attacks such as denial-of-service attacks, distributed denial-of-service attacks, spoofing, botnet attacks, malware, scanning, and unauthorized access [5]. These attacks can interrupt communication, steal sensitive data, reduce network performance, or take control of connected devices.

Another important challenge is energy consumption. Many IoT devices operate using batteries and may be deployed in remote locations where replacing or charging batteries is difficult. Traditional routing protocols may select communication paths without considering the remaining energy of network nodes [6]. As a result, some nodes may lose their energy faster than others, which can cause communication failures and reduce the overall lifetime of the network [7].

Artificial intelligence has become a useful tool for improving network security. Machine-learning algorithms can analyze network traffic and identify patterns that may indicate malicious behavior. Unlike traditional rule-based systems, AI models can learn from historical data and detect different types of attacks more effectively [8]. However, security alone is not enough for IoT networks. The routing process must also be energy efficient to ensure that devices can continue operating for a longer period [9].

This paper proposes an AI-driven intrusion detection and energy-efficient routing framework for IoT networks [10]. The framework combines machine-learning-based attack detection with routing decisions that consider energy consumption, link quality, delay, and node security status [11]. The purpose is to create a more secure, reliable, and energy-efficient IoT communication environment.

2. Problem Statement

The rapid growth of IoT networks has increased the number of connected devices that exchange data through wireless communication. These devices are often limited in battery power, memory, and processing capability. As a result, they are more vulnerable to cyberattacks and may not be able to use complex traditional security mechanisms [12].

IoT networks may face several attacks, including denial-of-service attacks, distributed denial-of-service attacks, spoofing, botnet activity, malware, and unauthorized access. These attacks can reduce network performance, interrupt communication, steal sensitive information, and cause devices to behave

abnormally [13]. Traditional intrusion detection systems are often based on predefined rules and signatures. Such systems may not detect new or unknown attacks effectively [14].

At the same time, routing in IoT networks creates another challenge. Many routing protocols select paths without considering the remaining energy of devices or the security condition of network nodes. As a result, some nodes may consume energy faster than others, causing network disconnection and reducing the overall lifetime of the IoT system. In addition, a routing path may include a compromised or malicious node, which can place transmitted data at risk [15].

Therefore, there is a need for an intelligent framework that combines intrusion detection with energy-efficient routing. The proposed system should identify suspicious network traffic using artificial intelligence and avoid selecting unsafe or low-energy nodes during routing. This can improve security, reduce energy consumption, and increase the reliability and lifetime of IoT networks [16].

3. Research Objectives

The main objective of this research is to develop an intelligent framework that improves security and energy efficiency in IoT networks.

The specific objectives are:

1. To develop an AI-based intrusion detection model for identifying malicious traffic in IoT networks.
2. To classify IoT network traffic into normal and attack categories using machine-learning algorithms.
3. To compare the performance of different machine-learning algorithms, such as Decision Tree, Random Forest, Support Vector Machine, and Long Short-Term Memory networks.
4. To design an energy-efficient routing mechanism that considers the remaining energy of nodes, communication distance, link quality, delay, and security status.
5. To evaluate the proposed framework using security metrics, including accuracy, precision, recall, F1-score, and false-positive rate.
6. To evaluate network performance using packet delivery ratio, end-to-end delay, throughput, average residual energy, and network lifetime.
7. To compare the proposed framework with traditional intrusion detection methods and conventional routing approaches.

4. Literature Review

The Internet of Things has received significant attention because it enables communication between physical devices, sensors, and online services. However, the large number of connected devices has also created new security risks. Many IoT devices are designed with limited computational resources, which makes it difficult to apply traditional cybersecurity solutions. Researchers have therefore explored lightweight security mechanisms and intelligent intrusion detection systems for IoT environments [17].

Machine learning has become one of the most common approaches for intrusion detection in IoT networks. Machine-learning models can analyze network traffic and identify patterns associated with normal and malicious behavior. Algorithms such as Decision Tree, Random Forest, Support Vector Machine, K-Nearest Neighbors, and Neural Networks have been used to classify network traffic. These models can provide better detection performance than rule-based systems because they learn from historical traffic data and can identify complex attack patterns [18].

Random Forest is widely used in intrusion detection because it can process large datasets, select important features, and achieve good classification accuracy. Decision Tree models are also useful because they are

easy to understand and can produce clear decision rules. Support Vector Machine is effective for binary classification problems, especially when the dataset contains well-separated classes. Deep-learning approaches, such as Long Short-Term Memory networks, can be useful when network traffic has sequential behavior or time-dependent features [18].

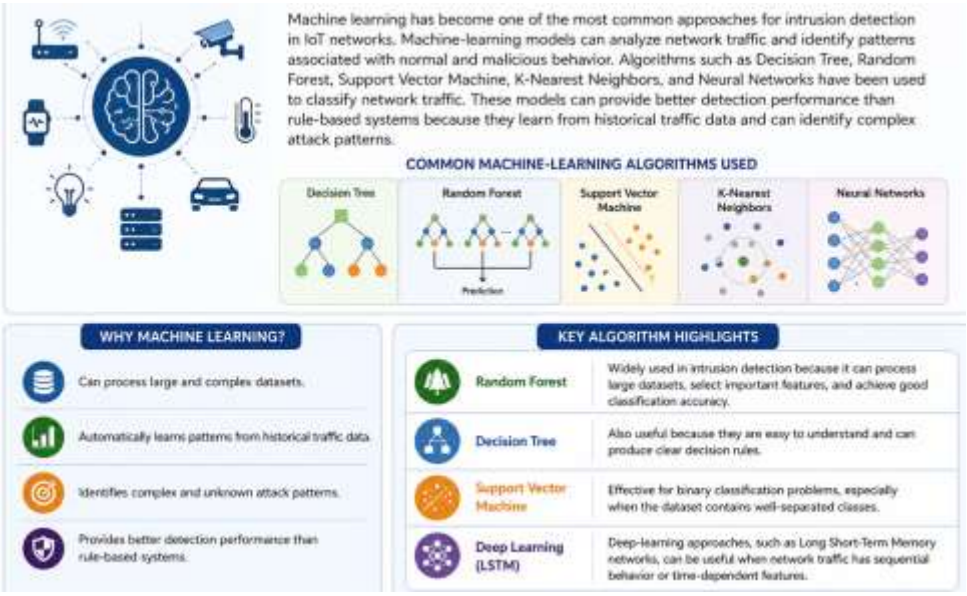

Figure 2. Machine Learning for Instruction Detection in IoT Networks

Several datasets have been developed for evaluating intrusion detection systems in IoT environments. Common examples include Bot-IoT, TON_IoT, N-BaIoT, and CICIoT2023. These datasets contain normal traffic and different types of malicious traffic, such as denial-of-service, distributed denial-of-service, scanning, botnet attacks, and data injection attacks. They are useful for training and testing machine-learning models [20].

Energy efficiency is another important research area in IoT networks. Since many IoT devices operate using batteries, routing protocols must reduce unnecessary communication and balance energy use between nodes. Energy-efficient routing methods often consider factors such as residual energy, communication distance, link quality, congestion, and packet delay. Protocols that ignore these factors may cause certain nodes to consume energy quickly, reducing the lifetime of the network [21].

Previous studies have addressed intrusion detection and energy-efficient routing separately. Some studies focus mainly on detecting attacks, while others focus on reducing energy consumption. However, there is still a need for integrated solutions that consider both security and energy efficiency at the same time. The proposed research contributes to this area by combining an AI-based intrusion detection model with a routing mechanism that avoids suspicious nodes and selects paths with sufficient remaining energy [22].

5. Proposed Framework

The proposed framework consists of four main layers: the IoT device layer, the gateway or edge layer, the intrusion detection layer, and the energy-efficient routing layer.

The IoT device layer includes sensors and smart devices that collect data from the surrounding environment. These devices may include temperature sensors, wearable health devices, smart cameras,

industrial sensors, and home automation devices. The collected data are transmitted through the IoT network to a gateway or edge device.

The gateway or edge layer receives traffic from IoT devices and performs initial processing. This layer can collect traffic information such as source address, destination address, protocol type, packet size, communication frequency, and transmission time. The collected information is then prepared for analysis by the intrusion detection system.

The intrusion detection layer uses machine-learning algorithms to classify network traffic as normal or malicious. The model is trained using an IoT cybersecurity dataset containing different types of attacks. When suspicious traffic is detected, the system assigns a risk level to the related node. Nodes with high-risk behavior can be blocked or excluded from the routing process.

The energy-efficient routing layer selects the most suitable communication path based on several factors. These factors include the remaining energy of nodes, communication distance, link quality, packet delay, congestion level, and security status. The routing mechanism avoids nodes that are identified as malicious or have low remaining energy. This helps reduce energy consumption and improve network reliability.Classification system for various methods of ML.

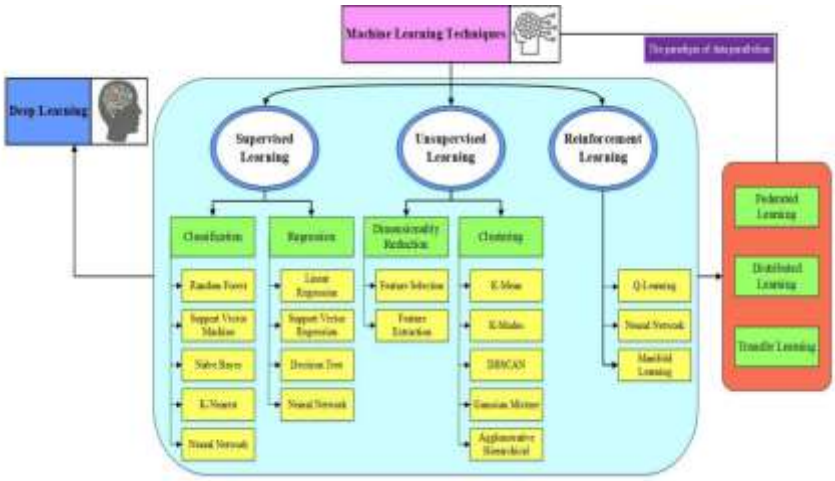

Figure 3. Classification system for various methods of ML.

6. Research Methodology

This research will follow an experimental methodology based on data analysis, machine learning, and network simulation. The methodology will include data collection, data preprocessing, model development, routing design, simulation, and performance evaluation.

First, an IoT cybersecurity dataset will be selected for training and testing the intrusion detection model. Suitable datasets may include Bot-IoT, TON_IoT, N-BaIoT, or CICIoT2023. The selected dataset should contain normal network traffic and different types of attacks, such as denial-of-service, distributed denial-of-service, botnet activity, spoofing, scanning, and unauthorized access.

Before training the machine-learning models, the dataset will be preprocessed. This process will include removing missing values, duplicate records, and irrelevant features. Categorical data will be converted into numerical values using encoding techniques. Numerical features may be normalized to ensure that values are within a similar range. Feature-selection techniques may also be used to identify the most important traffic features for intrusion detection.

Several machine-learning algorithms will be implemented and compared. These algorithms may include Decision Tree, Random Forest, Support Vector Machine, and Long Short-Term Memory networks. The dataset will be divided into training and testing sets. The training set will be used to build the models, while the testing set will be used to measure their performance on unseen data.

The performance of the intrusion detection models will be evaluated using accuracy, precision, recall, F1-score, confusion matrix, and false-positive rate. The best-performing model will be selected for integration with the energy-efficient routing mechanism.

The routing component will be simulated using NS-3. The simulation environment will include IoT nodes with different battery levels, communication ranges, and traffic loads. Each node will have information about its remaining energy, link quality, delay, and security status. The routing algorithm will select paths that avoid suspicious nodes and reduce energy consumption.

7. Evaluation Metrics

The intrusion detection component will be evaluated using the following security metrics:

- Accuracy: Measures the percentage of correctly classified traffic records.
- Precision: Measures how many records classified as attacks are actually attacks.
- Recall: Measures how many actual attacks are correctly detected.
- F1-score: Combines precision and recall into one measurement.
- False-positive rate: Measures how often normal traffic is incorrectly classified as malicious.

The routing component will be evaluated using the following network-performance metrics:

- Packet delivery ratio: Measures the percentage of packets successfully delivered to their destination.
- End-to-end delay: Measures the time required for packets to travel from source to destination.
- Throughput: Measures the amount of data successfully transmitted over the network.
- Average residual energy: Measures the remaining energy of IoT nodes after communication.
- Network lifetime: Measures how long the network continues to operate before a significant number of nodes lose their energy.

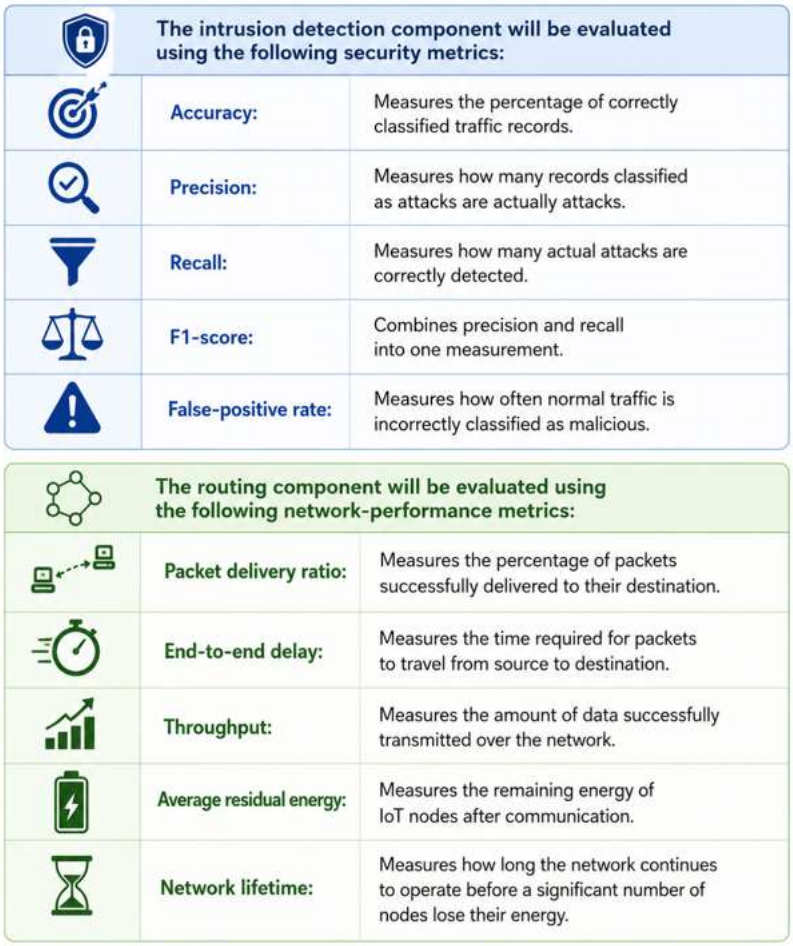

Figure 4. Evaluation Metrics

8. Expected Results

The proposed framework is expected to improve the detection of malicious traffic in IoT networks. Machine-learning models such as Random Forest and Long Short-Term Memory are expected to achieve higher detection accuracy than traditional rule-based intrusion detection systems. The model should also reduce the false-positive rate, which is important because frequent false alarms can reduce the reliability of a security system.

The energy-efficient routing mechanism is expected to reduce energy consumption by selecting nodes with sufficient remaining battery power and avoiding unnecessary communication. It should also improve packet delivery ratio and network lifetime by preventing overloaded or low-energy nodes from being selected repeatedly.

By combining intrusion detection with routing decisions, the proposed framework is expected to provide better protection against attacks while maintaining efficient communication. The system should avoid malicious nodes during packet forwarding, reduce the risk of data loss, and improve the overall reliability of the IoT network.

9. Conclusion

IoT networks are becoming increasingly important in modern applications, but their growth also creates serious challenges related to cybersecurity and energy consumption. Because IoT devices usually have

limited resources, they are vulnerable to attacks and may lose energy quickly when inefficient routing methods are used. Traditional security and routing approaches may not provide enough protection or efficiency for large and dynamic IoT environments.

This paper proposes an AI-driven intrusion detection and energy-efficient routing framework to address these challenges. The framework uses machine-learning techniques to identify malicious traffic and combines this information with routing decisions based on energy level, link quality, delay, and node security status. By avoiding suspicious nodes and selecting energy-efficient communication paths, the proposed system is expected to improve both network security and device lifetime.

The expected outcome of this study is a practical framework that can support safer and more reliable IoT communication. The results may show that combining artificial intelligence with energy-aware routing improves intrusion detection performance, reduces energy consumption, increases packet delivery ratio, and extends the overall lifetime of IoT networks. Future work may include testing the framework with real IoT devices, applying deep-learning models at the network edge, and integrating blockchain or federated learning to provide stronger privacy and security.

References

1. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.
2. M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, “ROP: A Robust and Efficient Framework for Securing the Internet of Things,” *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9894–9908, 2020.
3. N. Moustafa and J. Slay, “The Evaluation of Network Anomaly Detection Systems: Statistical Analysis of the UNSW-NB15 Data Set and the Comparison with the KDD99 Data Set,” *Information Security Journal: A Global Perspective*, vol. 25, no. 1–3, pp. 18–31, 2016.
4. N. Moustafa, “TON_IoT Datasets: A New Generation of Data Sets of IoT and IIoT for Data-Driven Intrusion Detection Systems,” *IEEE Access*, vol. 9, pp. 165130–165150, 2021.
5. Y. Meidan et al., “N-BaIoT: Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders,” *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.
6. L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, “IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?” *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41–49, 2018.
7. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-Efficient Communication Protocol for Wireless Microsensor Networks,” in *Proceedings of the Hawaii International Conference on System Sciences*, 2000.
8. J. N. Al-Karaki and A. E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey,” *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6–28, 2004.
9. C. Pu, “Sybil Attack in RPL-Based Internet of Things: Analysis and Defenses,” *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4937–4949, 2020.
10. M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, “Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis,” *IEEE Access*, vol. 9, pp. 138509–138542, 2021.

11. Koroupi, F., Talebi, S. & Salehinejad, H. Cognitive radio networks spectrum allocation: An ACS perspective. Sci. Iran. 19. https:/ /doi.org/10.1016/j.scient.2011.04.029 (2012).
12. Cao, X., Xiangwei, Z. L., Liu, L. & Yu, C. Energy-efficient spectrum sensing for cognitive radio enabled remote state estimation over wireless channels. IEEE Trans. Wirel. Commun. 14. https://doi.org/10.1109/TWC.2014.2379642 (2015).
13. Letaief, B., Chen, W., Shi, Y., Zhang, J. & Zhang, Y. J. A. The roadmap to 6G: AI empowered wireless networks. IEEE Commun. Mag. 57. https://doi.org/10.1109/MCOM.2019.1900271 (2019).
14. Zeng, Y. & Liang, Y. C. Eigenvalue-based spectrum sensing algorithms for cognitive radio. IEEE Trans. Commun. 57. https://doi. org/10.1109/TCOMM.2009.0901.060118 (2009).
15. Ma, Y., Li, T., Zhou, Y., Yu, L. & Jin, D. Mitigating energy consumption in heterogeneous mobile networks through data-driven optimization. IEEE Trans. Netw. Serv. Manag. 21, 4369–4382. https://doi.org/10.1109/TNSM.2024.3416947 (2024).
16. Zheng, B. et al. Reinforcement learning-based plasma flow control of asymmetric vortices over a slender body at high angles of attack. Phys. Fluids 37 (2025).
17. Dai, M., Sun, G., Yu, H., Wang, S. & Niyato, D. User association and channel allocation in 5G mobile asymmetric multi-band heterogeneous networks. IEEE Trans. Mobile Comput. 24, 3092–3109. https://doi.org/10.1109/TMC.2024.3503632 (2025).
18. Hu, F., Chen, B. & Zhu, K. Full spectrum sharing in cognitive radio networks toward 5G: A survey. IEEE Access 6. https://doi.org /10.1109/ACCESS.2018.2802450 (2018).
19. Song, L., Sun, G., Yu, H. & Niyato, D. ESPD-LP: Edge service pre-deployment based on location prediction in MEC. IEEE Trans. Mobile Comput. 24, 5551–5568. https://doi.org/10.1109/TMC.2025.3533005 (2025).
20. Qadir, J., Baig, A., Ali, A. & Shafi, Q. Multicasting in cognitive radio networks: Algorithms, techniques and protocols. J. Netw. Comput. Appl. 45. https://doi.org/10.1016/j.jnca.2014.07.024 (2014).
21. Luo, H., Sun, G., Chi, C., Yu, H. & Guizani, M. Convergence of symbiotic communications and blockchain for sustainable and trustworthy 6G wireless networks. IEEE Wirel. Commun. 32, 18–25. https://doi.org/10.1109/MWC.001.2400245 (2025).
22. Zeng, Y., Liang, Y. C., Hoang, A. T. & Zhang, R. A review on spectrum sensing for cognitive radio: Challenges and solutions. EURASIP J. Adv. Signal Process. 2010, 1. https://doi.org/10.1155/2010/381465 (2010).