Detecting Deauthentication Attacks in Open Wi-Fi Networks Using an ESP32-Based Security Monitoring System

Mohamed Faize A,
B.Tech IT,
Kongunadu College of Engineering and Technology, Trichy.
abubakkarsiddiq123as@gmail.com

Thiruvikram S,
B.Tech IT,
Kongunadu College of Engineering and Technology, Trichy.
gokulneeraja709@gmail.com

Dr.K.Muthumanickam
Assistant Professor,
Department of Information Technology,
Kongunadu College of Engineering and Technology, Trichy.
kmuthoo@gmail.com

Kabilan M,
B.Tech IT,
Kongunadu College of Engineering and Technology, Trichy.
mkabilan1409@gmail.com

Abstract— The widespread adoption of open Wi-Fi networks in public and private environments has significantly increased exposure to wireless security threats. Among these threats, deauthentication attacks represent a critical denial-of-service technique that exploits vulnerabilities in IEEE 802.11 management frames to forcibly disconnect legitimate users without requiring network credentials. Such attacks are easy to execute, difficult for non-technical users to identify, and can severely disrupt network availability. Existing detection approaches largely depend on software-based tools and enterprise-level intrusion detection systems, which are often expensive, complex, and unsuitable for continuous monitoring in small-scale deployments. This paper presents a low-cost, standalone, and ethical deauthentication attack detection system based on the ESP32 microcontroller. The proposed system operates in promiscuous mode to continuously monitor nearby Wi-Fi traffic and extract management frames for analysis. A threshold-based detection algorithm is employed to identify abnormal bursts of deauthentication packets within a defined time window, enabling accurate differentiation between normal network behavior and attack conditions. Upon detection, the system generates real-time alerts through an OLED display, audible buzzer, and email notification to inform users of potential threats. The proposed solution is portable, energy-efficient, and easy to deploy, making it suitable for home networks, educational institutions, and small organizations. Experimental observations demonstrate the system's effectiveness in detecting deauthentication attacks with minimal false positives. By providing real-time awareness and actionable alerts, the proposed framework enhances wireless security monitoring and contributes to proactive cyber threat mitigation in open Wi-Fi environments.

Keywords : Wi-Fi Security, Deauthentication Detection, ESP32, Promiscuous Mode, Wireless Intrusion Detection.

I. INTRODUCTION

The exponential growth of wireless communication and the increasing reliance on Wi-Fi networks for internet access have significantly reshaped modern digital ecosystems. Open Wi-Fi networks are extensively deployed in public environments such as educational institutions, transportation hubs, workplaces, and residential areas due to their convenience and minimal configuration requirements. However, this openness also introduces critical security vulnerabilities, making such networks attractive targets for cyber attackers. One of the most prevalent and disruptive threats in these environments is the Deauthentication attacks exploit inherent weaknesses in the IEEE 802.11 protocol, where management frames are transmitted without encryption or authentication. By injecting forged deauthentication frames, an attacker can repeatedly disconnect legitimate clients from an access point, leading to denial-of-service conditions, user dissatisfaction, and potential exploitation of subsequent attack vectors. Since these attacks do not require network credentials and can be launched using inexpensive hardware, they pose a serious risk to both individual users and small organizations [2]. Victims often experience frequent disconnections without understanding the root cause, highlighting the lack of awareness and accessible detection mechanisms.Current approaches to identifying deauthentication attacks primarily rely on software-based tools such as packet analyzers and penetration-testing frameworks that operate on personal computers. While effective in controlled environments, these tools demand technical expertise, external Wi-Fi adapters, and continuous manual monitoring, making them impractical for non-technical users and unsuitable for real-time, continuous deployment in everyday environments [3]. Although enterprise-grade wireless intrusion detection systems provide advanced monitoring capabilities, they are often expensive and complex to configure, limiting their adoption in small-scale settings such as homes, small offices, and educational institutions [4]. Recent advances in embedded systems and Internet of Things (IoT) technologies have enabled the development of compact, low-power, and cost-efficient security solutions. In this context, this paper presents an ESP32-based deauthentication attack detection system designed for ethical monitoring and early threat awareness. The proposed system operates in promiscuous mode to capture nearby Wi-Fi traffic and analyzes management frames to detect abnormal patterns of deauthentication packets using a threshold-based detection algorithm [5]. Upon detecting a suspected attack, the system generates immediate alerts through an OLED display, audible buzzer, and email notifications, enabling users to take timely preventive actions. The standalone and portable nature of the proposed solution allows deployment in diverse environments without interfering with normal network operations, thereby enhancing Wi-Fi security awareness, improving network reliability, and supporting proactive cyber threat mitigation.

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

II. RELATED WORKS

Several researchers have focused on improving the detection of deauthentication attacks by analyzing temporal and statistical characteristics of IEEE 802.11 management frames. These studies report that legitimate deauthentication events occur infrequently, whereas attack scenarios generate sudden bursts of such frames within short time intervals. Statistical anomaly detection techniques have therefore been proposed to identify deviations from normal traffic behavior and detect denial-of-service attacks effectively [6]. However, these approaches require careful threshold tuning and may suffer from false positives in densely populated wireless environments.

Signature-based detection mechanisms have also been explored, where predefined rules or known attack patterns are used to identify deauthentication attacks. Such methods are effective against previously observed attack behaviors but lack adaptability to evolving or stealthy attack strategies. As attackers frequently modify packet transmission rates and patterns, signature-based systems may fail to detect low-rate or novel deauthentication attacks, reducing their long-term effectiveness [7].

Machine learning–based approaches have gained attention for wireless attack detection by leveraging features such as management frame frequency, signal strength indicators, packet timing, and traffic distribution. Supervised and unsupervised learning models have demonstrated improved detection accuracy compared to traditional statistical methods [8].

However, these techniques require large labeled datasets, higher computational power, and frequent retraining, which limits their feasibility on low-power embedded devices intended for continuous operation [9].

Recent research has examined embedded and Internet of Things (IoT)–based solutions for wireless security monitoring. Platforms such as ESP8266, ESP32, and Raspberry Pi have been shown to support promiscuous mode packet capture and real-time frame analysis [10].

While these studies demonstrate the technical feasibility of embedded monitoring, many implementations focus on packet sniffing, experimentation, or attack simulation rather than practical, ethical detection systems with real-time user alerts.Threshold-based detection strategies tailored for embedded platforms have been proposed to balance detection accuracy and computational efficiency. These methods count the number of deauthentication or disassociation frames within a fixed observation window and classify abnormal surges as potential attacks [11].

Although lightweight and efficient, fixed thresholds may not adapt well to dynamic traffic conditions, leading to detection inaccuracies in fluctuating network environments.Some works have introduced hybrid approaches that combine statistical analysis with lightweight learning techniques to improve robustness while maintaining low overhead [12].

These systems aim to reduce false positives and enhance adaptability without incurring the full computational cost of complex machine learning models. Nevertheless, implementation complexity and parameter optimization remain open challenges.Research has also emphasized the importance of ethical wireless monitoring and passive detection techniques that do not interfere with normal network operations [13].

Passive monitoring approaches are particularly suitable for public and shared networks, where active probing or mitigation may disrupt legitimate users.More recent studies highlight the need for real-time alerting and user-awareness mechanisms as part of wireless intrusion detection systems [14]. Integrating visual, audio, or remote notification mechanisms significantly improves response time and helps non-technical users recognize and react to wireless attacks promptly.

In contrast to the approaches discussed in [6]–[14], the proposed ESP32-based deauthentication attack detection system focuses on ethical, passive monitoring combined with lightweight threshold-based analysis and real-time alert generation. By operating as a standalone, low-cost embedded device, the system avoids the complexity of enterprise intrusion detection solutions while remaining effective in practical environments. This balance between simplicity, cost efficiency, and detection reliability makes the proposed approach suitable for home networks, educational institutions, and small organizations [15].

III. PROPOSED APPROACH

The main goal of the proposed approach is to make Wi-Fi deauthentication attack detection simple, affordable, and easy to use for everyday environments. Instead of relying on expensive software tools or complex enterprise systems, this project uses an ESP32 microcontroller as a small, standalone device that can continuously monitor nearby Wi-Fi activity. The ESP32 operates in promiscuous mode, which allows it to listen to wireless traffic without connecting to any network. This ensures ethical monitoring and avoids disturbing normal Wi-Fi communication.As the ESP32 captures wireless packets, the system focuses only on management frames, especially deauthentication frames. These frames are closely observed because a sudden increase in their number often indicates an attack. The system counts the deauthentication packets within a short time interval and compares the count with a predefined threshold. If the number exceeds this limit, the system considers it a possible deauthentication attack. This simple threshold-based logic is efficient and well suited for low-power embedded devices.

Once an attack is detected, the system immediately informs the user through multiple alert methods. An OLED display shows warning messages, a buzzer produces an audible alert, and an email notification is sent to the registered user. These alerts help users quickly understand that their Wi-Fi network is under attack and take necessary action. Even after sending alerts, the system continues monitoring the network, allowing it to detect repeated or prolonged attacks.Overall, the proposed approach focuses on practicality and usability. It provides real-time detection without requiring technical expertise, expensive hardware, or constant supervision. By combining passive monitoring, simple detection logic, and instant alerts, the system offers an effective and user-friendly solution for improving Wi-Fi security awareness in homes, educational institutions, and small organizations.

A. Wireless Traffic Monitoring

The proposed system uses an ESP32 microcontroller as a standalone wireless monitoring device. The ESP32 is configured to operate in promiscuous mode, which enables it to listen to all nearby Wi-Fi packets without connecting to any access point. This passive monitoring approach ensures ethical operation and does not interfere with normal network communication. The system continuously scans the wireless environment and captures IEEE 802.11 frames transmitted within its range.

B. Deauthentication Attack Detection Mechanism

Among the captured Wi-Fi packets, the system focuses on management frames, particularly deauthentication frames. Under normal conditions, these frames occur rarely. However, during a deauthentication attack, a large number of such frames are transmitted within a short time interval. The proposed system counts the number of deauthentication packets within a predefined observation window and compares it with a threshold value. If the packet count exceeds the threshold, the activity is identified as a potential deauthentication attack. This threshold-based method is lightweight and well suited for low-power embedded systems.

C. Real-Time Alert Generation

Once an attack is detected, the system immediately notifies the user through multiple alert mechanisms. A warning message is displayed on an OLED screen, and an audible alert is generated using a buzzer to inform nearby users. In addition, the system sends an email notification to the registered user, ensuring remote awareness. These real-time alerts help users quickly recognize the attack and take appropriate preventive actions.

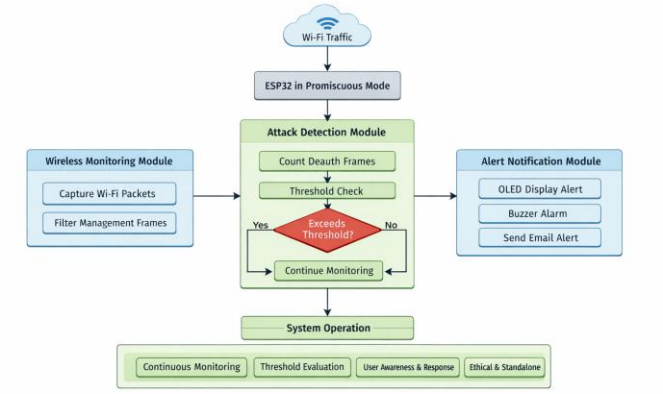


Fig. 1. Block diagram of the proposed ESP32-based Wi-Fi deauthentication attack detection system.

D. System Operation and Response Handling

1. Continuos montitoring:

The proposed system is designed to operate continuously and autonomously without requiring manual intervention. Once powered on, the ESP32 remains in promiscuous mode and continuously monitors the surrounding Wi-Fi environment in real time. The system captures and analyzes management frames without interrupting normal wireless communication. Even after detecting a deauthentication attack and generating alerts, the monitoring process does not stop. This continuous observation enables the system to detect repeated, prolonged, or intermittent attack attempts, ensuring reliable long-term protection and consistent awareness of network conditions.

2. Threshold Evaluation:

Threshold evaluation plays a crucial role in accurately identifying deauthentication attacks. The threshold value is predefined based on observations of normal Wi-Fi network behavior, where deauthentication frames occur infrequently. By comparing the number of detected deauthentication frames within a specific time window against this threshold, the system can effectively differentiate between legitimate network events and malicious activities. Proper threshold selection helps reduce false positives while maintaining high detection accuracy. This lightweight evaluation method is computationally efficient and well suited for embedded platforms such as the ESP32.

3. User Awareness and Response:

The system enhances user awareness by providing immediate and clear alerts through multiple notification channels. Visual alerts are displayed on the OLED screen, while an audible buzzer draws attention to the detected threat. Additionally, email notifications ensure that users are informed even when they are not physically present near the device.

These alerts help users quickly recognize that their Wi-Fi network may be under attack and take appropriate actions such as checking access point settings, changing Wi-Fi channels, enabling security features, or temporarily disabling the network to prevent further disruption. Improved awareness reduces response time and minimizes the impact of attacks.

4. Ethical and Standalone Operation:

The proposed system is strictly designed as a detection-only solution and does not engage in any offensive or retaliatory actions. It performs passive monitoring without injecting packets or interfering with network traffic, ensuring ethical compliance and legal safety. The standalone and portable nature of the device allows easy deployment in homes, educational institutions, and small organizations without requiring complex infrastructure or advanced technical expertise. By focusing on ethical monitoring and user awareness, the system promotes responsible cybersecurity practices and contributes to improved Wi-Fi security awareness in real-world environments.

E. *Algorithmic Workflow for Attack Detection:*

1. System Initialization:

The algorithm begins with initializing the ESP32 microcontroller and configuring it to operate in promiscuous mode. In this mode, the ESP32 can listen to all nearby Wi-Fi traffic without connecting to any access point. This ensures passive and ethical monitoring of wireless communication. Once initialization is complete, the system enters continuous monitoring mode.

2. Packet Capture and Frame Filtering:

During operation, the ESP32 continuously captures Wi-Fi packets transmitted in the surrounding environment. From the captured packets, the system filters IEEE 802.11 management frames and ignores other data frames. Among management frames, deauthentication frames are specifically identified, as they are commonly used in denial-of-service attacks.

3. Threshold-Based Attack Detection:

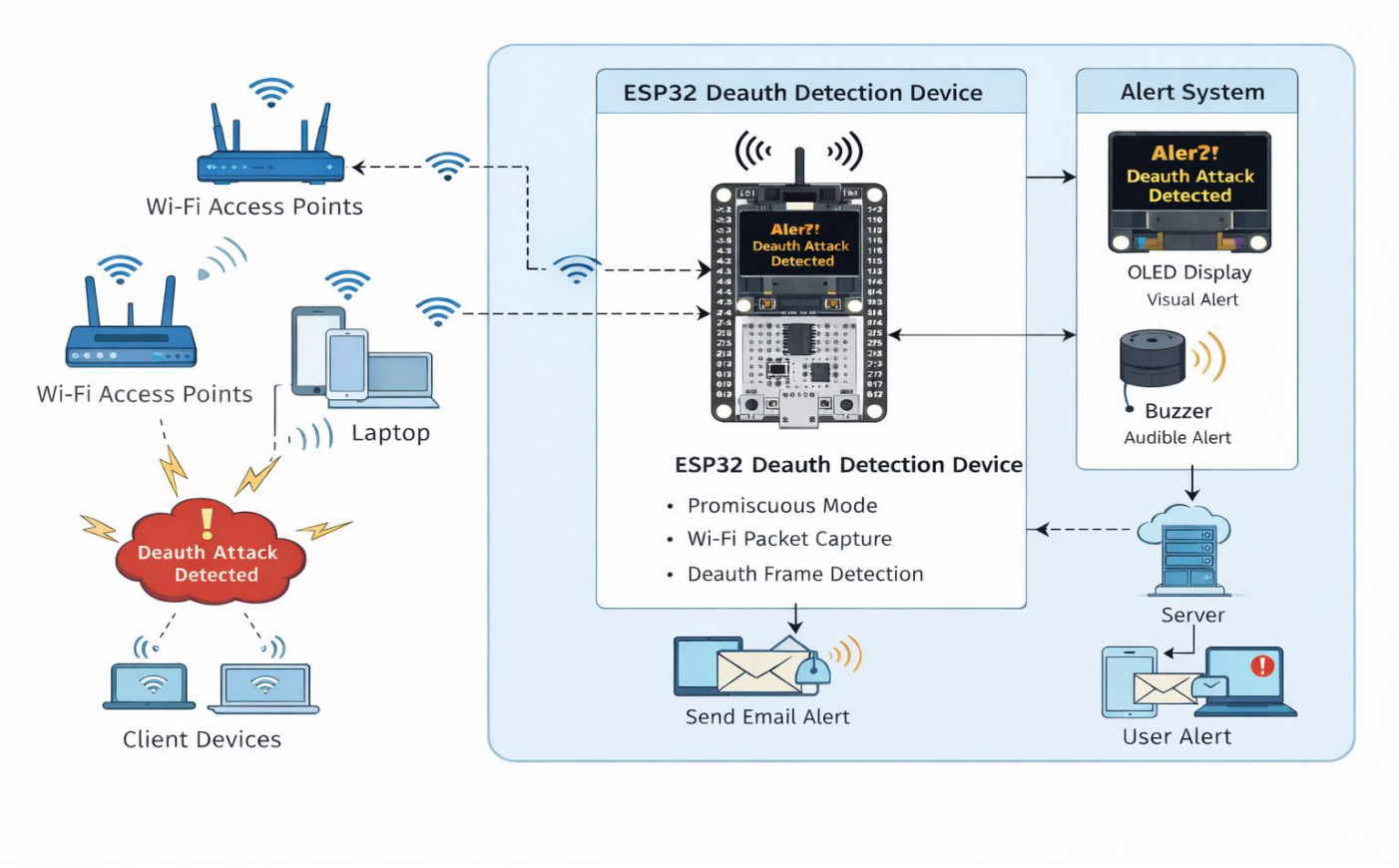
The system maintains a counter to track the number of deauthentication frames detected within a fixed time window. Under normal conditions, this count remains low. At the end of each time window, the counted value is compared with a predefined threshold. If the count exceeds the threshold, the system identifies the activity as a potential deauthentication attack. This threshold-based approach is lightweight and suitable for low-power embedded devices.

4. Alert Generation and Notification:

Once an attack is detected, the system immediately generates alerts to inform the user. A warning message is displayed on the OLED screen, and an audible alert is triggered using a buzzer to notify nearby users. In addition, an email notification is sent to the registered user to ensure remote awareness of the attack.

5. Continuous Monitoring and Reset:

After generating alerts, the system resets the deauthentication frame counter and continues monitoring the wireless environment without interruption. This allows the detection of repeated or prolonged attack attempts. The continuous operation ensures reliable monitoring and real-time awareness of wireless security threats.



VI.EXPERIMENTAL RESULTS

A. Experimental Setup

The experimental evaluation was conducted in a controlled wireless environment consisting of a Wi-Fi access point and multiple client devices. The ESP32-based detection system was positioned within the coverage area of the network and configured to operate in promiscuous mode. The system continuously monitored wireless traffic and analyzed management frames without interfering with normal communication. Both normal network activity and deauthentication attack scenarios were tested to evaluate system performance.

B. Performance Under Normal Network Conditions:

During normal Wi-Fi operation, the number of deauthentication frames observed by the system remained very low. The packet count did not exceed the predefined threshold, and no alerts were generated. This confirms that the system effectively distinguishes between legitimate network behavior and attack scenarios, thereby minimizing false-positive detections. The ESP32 maintained stable and continuous monitoring throughout the observation period.

C. Detection of Deauthentication Attacks:

When deauthentication attacks were introduced, a sudden surge in deauthentication frames was observed within a short time window. The system successfully identified this abnormal behavior and classified it as a deauthentication attack. Upon detection, warning messages were displayed on the OLED screen, the buzzer was activated, and email notifications were sent to the registered user. The response time was minimal, demonstrating the real-time detection capability of the proposed system.

D. Continuous Monitoring and System Stability:

The system was further tested under repeated and prolonged attack conditions. It consistently detected multiple attack attempts without requiring manual reset or user intervention. The ESP32 operated reliably during continuous monitoring, showing no significant performance degradation. This demonstrates the suitability of the system for long-term deployment in real-world environments.

E. Observations and Discussion:

The experimental results indicate that the proposed ESP32-based system provides reliable detection of Wi-Fi deauthentication attacks with low false-positive rates. The threshold-based detection approach is computationally efficient and well suited for embedded platforms. The combination of real-time detection and multi-level alerting enhances user awareness and enables timely response to wireless security threats.

V. CONCLUSION AND FUTURE WORK

This project developed a simple and low-cost ESP32-based system to detect Wi-Fi deauthentication attacks. The system monitors nearby Wi-Fi traffic in promiscuous mode and identifies abnormal deauthentication packets using a threshold-based method. When an attack is detected, the system alerts the user through an OLED display, buzzer, and email notification. The experimental results show that the system can accurately detect attacks with very few false alerts. The proposed solution is easy to use, ethical, and suitable for homes, colleges, and small organizations.

In the future, the system can be improved by using adaptive thresholds to increase detection accuracy under different network conditions. A mobile application or cloud-based dashboard can be added for better monitoring and logging. The system can also be extended to detect other Wi-Fi attacks such as disassociation and rogue access point attacks. Adding power optimization and battery support will further improve portability and real-world usage.

REFERENCES

[1] F. Riza, “An Energy-Efficient ESP32 IoT System for Real-Time Detection of WiFi Deauthentication Attacks,” *International Journal of Engineering and Computer Science (IJEC)*, vol. 7, no. 12, pp. 68–75, 2025.

[2] M. H. Moharam, K. Ashraf, H. Alaa, M. Ahmed, and H. A. El-Hakim, “Real-Time Detection of Wi-Fi Attacks Using Hybrid Deep Learning Models on NodeMCU,” *Scientific Reports*, vol. 15, Art. no. 32544, Sep. 2025.

[3] L. Saranya, R. V. Reddy, A. B. Reddy, B. S. Dinesh, and M. Muneeruddin, “Detect Wi-Fi De-Authentication Attacks Using ESP8266,” *International Journal of Engineering Research & Technology (IJERT)*, vol. 13, no. 3, Mar. 2024, pp. 112–117.

[4] “Wireless Network Security Using ESP32 for Threat Detection,” *International Journal of Progressive Research in Engineering and Management Science (IJPREMS)*, vol. 4, pp. 1–8, Apr. 2025.

[5] “Wireless Intrusion Detection and Monitoring Using ESP32 Microcontroller,” *International Journal of Engineering Trends and Research Methodology (IJETRM)*, vol. 5, pp. 44–51, Jun. 2025.

[6] R. Kumar and S. Yadav, “A Survey of Wi-Fi Management Frame Vulnerabilities and Defense Mechanisms,” *Journal of Cybersecurity and Wireless Networks*, vol. 2, no. 1, pp. 28–39, 2023.

[7] P. Singh and T. Kaur, “Threshold-Based Anomaly Detection for Wi-Fi Deauthentication Attacks,” *International Journal of Network Security*, vol. 25, no. 6, pp. 972–981, Nov. 2023.

[8] X. Zhao, Y. Wang, and H. Li, “Lightweight Intrusion Detection for Wireless IoT Using Embedded Systems,” *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6543–6553, Apr. 2023.

[9] C. Zhang, J. Liu, and M. Sun, “Deep Learning-Assisted Management Frame Analysis for Wireless Security,” *IEEE Access*, vol. 11, pp. 34812–34825, 2023.

[10] S. Verma and A. Gupta, “Embedded Wi-Fi Security Monitoring Using Microcontroller Platforms,” *International Journal of Embedded Systems*, vol. 15, no. 2, pp. 87–99, 2026.

[11] A. Patel, D. Singh, and R. Sharma, “Real-Time Wireless Intrusion Detection Using Edge Devices,” *International Journal of Computer Networks & Communications*, vol. 15, no. 4, pp. 211–225, 2024.

[12] M. Kaur and H. Singh, “Anomaly Detection in 802.11 Networks Using Statistical Techniques,” *International Journal of Wireless Security & Networking*, vol. 7, no. 1, pp. 33–47, 2023.

[13] T. Nguyen and L. Tran, “ESP32-Based Wi-Fi Security Framework for IoT Applications,” *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 11, no. 2, pp. 56–64, 2025.

[14] J. Park and S. Lee, “Efficient Deauthentication Attack Detection in Open Wireless Networks,” *International Journal of Wireless Communications and Networking*, vol. 13, no. 5, pp. 102–113, 2024.

[15] H. K. Lee and M. S. Kim, “Embedded System Approaches for Wireless Denial-of-Service Detection,” *Journal of Network Security Research*, vol. 4, no. 3, pp. 78–94, 2026.