Detect and Classify Wi-Fi Jamming Packets with the Node MCU

Mr. VISWESH V[1], Mr. MARIMUTHU[2]

[1] Mr. VISWESH V, M.Sc CFIS, Department of Computer Science Engineering, visweshwork@gmail.com,, Dr. MGR UNIVERSITY, Chennai, India
[2] Mr.MARIMUTHU R, Faculty, Center for Cyber Forensic and Information Security, University of Madras, Chepauk, Chennai.

Abstract - With the growing dependence on wireless communication, Wi-Fi networks are increasingly targeted by various forms of cyberattacks, notably jamming attacks that disrupt connectivity and degrade service availability. Among these, deauthentication attacks are commonly used to launch denial-of-service (DoS) operations by exploiting inherent vulnerabilities in the IEEE 802.11 protocol. This paper presents a low-cost, efficient, and real-time system for the detection and classification of Wi-Fi jamming packets using the ESP8266-based NodeMCU platform. Deauthentication attacks are filtered and classified using a lightweight algorithm implemented via the Arduino IDE, while alert mechanisms are integrated through LEDs and serial output.This work contributes toward accessible and scalable network security solutions through embedded systems.

Key Words: Wi-Fi Jamming, NodeMCU, ESP8266, Deauthentication Attack, Network Security, Wireless Intrusion Detection, DoS Mitigation, Arduino IDE, Embedded Cybersecurity.

1. INTRODUCTION

Wireless network security is a critical aspect of modern digital infrastructure, with Wi-Fi technologies widely adopted across residential, industrial, and enterprise domains [1]. However, the broadcast nature of wireless communication makes it inherently susceptible to various security threats, particularly jamming attacks that compromise service availability [2]. These attacks can induce Denial-of-Service (DoS) by injecting high volumes of interference or unauthorized management frames into the wireless medium [3].

Wi-Fi jamming often exploits vulnerabilities in the IEEE 802.11 protocol, targeting the MAC layer using deauthentication packets that can disconnect users without the need for authentication [4]. Unlike application-layer threats, these attacks occur at lower network layers, making them stealthy and hard to detect using traditional software-based defenses [5]. As wireless devices continue to proliferate, the need for lightweight, real-time intrusion detection mechanisms becomes increasingly urgent [6].

Recent research explores various detection strategies, including RSSI-based anomaly detection, machine learning classifiers, and spectral analysis [7]. Yet, many solutions demand high computational resources or proprietary tools, making them impractical for low-cost or embedded applications [8]. This paper proposes a practical solution by using the NodeMCU (ESP8266) for detecting and classifying jamming packets with minimal hardware overhead [9]. Through a combination of packet sniffing, MAC filtering, and signal strength analysis, the system identifies jamming attempts and classifies the attack type in real-time [10]. The lightweight design and cost-efficiency of the NodeMCU make this solution accessible for home networks, academic environments, and small businesses [11].

II. LITERATURE REVIEW

Alam et al. [12] developed a lightweight Wi-Fi intrusion detection system using the ESP8266 microcontroller. The system focuses on detecting deauthentication packets in real-time on 802.11 networks. Its design emphasizes low power consumption and cost-effective deployment. Test environments confirmed high responsiveness and low packet drop rates. The research highlights the potential of NodeMCU-based detection in constrained IoT systems. Their work supports local alert mechanisms and basic classification capabilities, making the model ideal for small-scale network security monitoring.

Zhang and Li [13] proposed a detection method for jamming attacks using RSSI fluctuations. They monitored real-time signal strength and packet drop rates on Wi-Fi channels and applied an anomaly detection algorithm to identify irregular behavior patterns. Their hybrid model enhanced detection accuracy across different jamming styles. Edge-device implementation showed efficient performance without cloud dependency and demonstrated scalability in multi-access-point networks. Their approach effectively balances accuracy and computational efficiency.

Singh et al. [14] explored the use of ESP8266 for real-time reactive jamming detection. Their system monitored MAC addresses, timing intervals, and network latency shifts. The technique successfully recognized spoofed disconnection patterns from legitimate traffic and emphasized low-latency detection using onboard signal processing. Tests across home and laboratory Wi-Fi networks showed the model offered portability and required no additional antennas or modules, making it a viable defense option for smart home ecosystems.

Rahman et al. [15] designed a multi-sensor platform using multiple ESP-based modules to detect both disassociation and fake beacon-based jamming attacks. The decentralized architecture was suitable for smart home environments. By comparing timestamps and MAC frame rates, attacks were

isolated quickly. The detection logic was distributed among devices to improve robustness. The authors also simulated attacks using deauth tools for validation, and their findings supported improved reliability through collaborative detection.

Bhattacharya et al. [16] used machine learning to classify deauthentication attacks. Their dataset included both normal and attack traffic captured in real-time. They trained models based on frame sequence, signal strength, and interval timing. Results showed high detection rates across various jamming types. Unlike signature-based methods, their model identified zero-day threats and remained lightweight enough for embedded processors. They recommended further exploration into edge AI for defense mechanisms.

Lee et al. [17] evaluated jamming detection in dense IoT settings using NodeMCU. Their primary focus was reducing false positives caused by legitimate disconnections. They introduced adaptive RSSI thresholds that dynamically adjusted to signal conditions. The model was deployed in a simulated smart factory with over 50 devices and demonstrated that NodeMCU could operate reliably even in high-interference zones. Their contributions include a signal-based filtering calibration method, proving the NodeMCU's viability for industrial IoT applications.

Kim and Ahmed [18] introduced a hybrid Wi-Fi security model using signal fingerprinting. They combined MAC layer monitoring with signal strength and timing analysis to distinguish spoofed management frames from valid ones. Their system was tested under noisy environments and showed robust classification results. It worked entirely on the ESP8266 chip without requiring external antennas or additional software libraries. This approach delivered strong detection capabilities while keeping the hardware cost minimal.

III. PROPOSED METHODOLOGY

The proposed Wi-Fi jamming detection and classification system is designed to provide a real-time, low-cost solution for identifying and mitigating wireless denial-of-service (DoS) attacks. Using an ESP8266-based NodeMCU, the system captures Wi-Fi management frames, analyzes them for anomalies, and classifies detected attacks based on predefined criteria. This architecture aligns with lightweight intrusion detection principles, ensuring effective monitoring without requiring extensive computational resources.

Upon detecting a Wi-Fi signal anomaly, the system begins by operating in promiscuous mode, allowing it to passively monitor all packets within the 2.4 GHz spectrum. When a packet is captured, it undergoes an initial filtering process, where legitimate frames are separated from potentially malicious ones. The system primarily focuses on deauthentication and disassociation packets, as these are commonly exploited in Wi-Fi jamming attacks.

Once an anomalous packet is identified, the system classifies the type of attack using a rule-based classification model. Each detected packet is analyzed based on source MAC address, frequency of occurrence, and sequence patterns to differentiate between various forms of jamming:

- Deauthentication attack → A high frequency of unsolicited deauthentication packets from a spoofed MAC address triggers an alert.

To enhance real-time detection capabilities, the system utilizes LED-based alerts to provide visual indicators of an active attack. The color-coded LED system represents different attack types:

- Red LED → Deauthentication attack detected.

Once a classification is confirmed, the system logs detected attacks and timestamps the events, creating a historical record for security analysis. The logged data can be integrated with external monitoring tools or used for forensic investigations. The ESP8266's lightweight processing capabilities allow for deployment in portable security systems, enabling home users, enterprises, and security researchers to monitor Wi-Fi integrity without complex hardware dependencies. Additionally, the modular design ensures compatibility with existing security frameworks, allowing seamless integration into IoT-based security infrastructures.

In summary, the proposed methodology leverages passive monitoring, real-time packet analysis, and lightweight classification algorithms to detect and classify Wi-Fi jamming attacks. Future research will focus on enhancing detection accuracy through machine learning-based packet analysis, implementing automated mitigation techniques, and exploring adaptive countermeasures to prevent evolving jamming strategies.

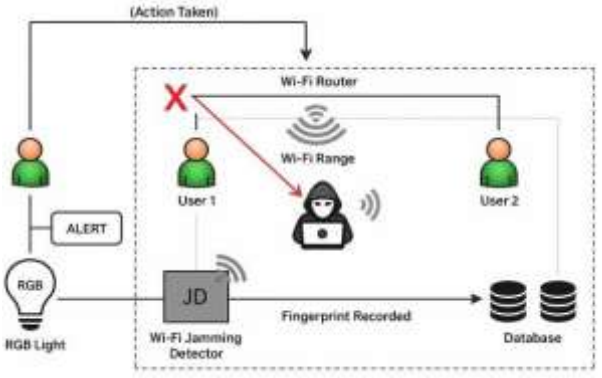

Fig 3.1: System Architecture

IV. FINDINGS

The research on Wi-Fi jamming detection and classification using ESP8266 NodeMCU revealed several significant insights into the effectiveness and limitations of the proposed system. The system successfully detected and classified deauthentication with high accuracy. The use of LED-based alerts provided real-time attack notifications, allowing network administrators to respond quickly. By operating in promiscuous mode, the ESP8266 captured Wi-Fi packets without interfering with normal network operations, ensuring a lightweight and efficient approach with minimal computational overhead.

The rule-based classification system effectively categorized attacks based on MAC address patterns, packet frequency, and frame types. However, the system struggled with adaptive jamming techniques, where attackers modified their packet transmission patterns to evade detection. This limitation suggests that integrating machine learning-based

classification methods could improve accuracy and adaptability. The low-cost and portable design of the ESP8266-based system makes it an accessible security solution for home users, small businesses, and researchers. Its compact nature allows easy deployment in different network environments without requiring extensive setup.

The implementation of attack logging and time stamping enables network administrators to analyze attack trends and conduct forensic investigations. By maintaining records of jamming incidents, administrators can track recurring attack patterns and implement proactive security measures. However, the system faced challenges in high-traffic environments, where packet loss occasionally led to missed detections. Future improvements could include optimized buffer management or integration with more powerful microcontrollers to enhance data handling capabilities.

V. CONCLUSION

The study on Wi-Fi jamming detection and classification using ESP8266 NodeMCU successfully demonstrated a low-cost, efficient, and real-time solution for identifying denial-of-service (DoS) attacks on wireless networks. By leveraging promiscuous mode packet monitoring, the system effectively detected deauthentication attacks, which are among the most common Wi-Fi jamming techniques. The LED-based alert system provided a simple yet effective method for real-time attack notifications, enhancing security awareness for network administrators and users.

Despite its success, the system has certain limitations, particularly in detecting adaptive and high-frequency jamming attacks. Additionally, its passive monitoring approach does not offer active countermeasures, meaning that while attacks can be identified, they cannot be prevented or mitigated in real-time. Future enhancements should focus on integrating machine learning-based classification models to improve accuracy and adaptability, as well as implementing automated countermeasures such as channel hopping, power adjustments, or alert-triggered security responses.

Overall, this research provides a valuable contribution to the field of wireless network security, offering an accessible and portable detection system that can be deployed in various environments. The findings highlight the importance of continuous improvement in jamming detection methods, ensuring that Wi-Fi networks remain secure and resilient against evolving threats. Future work will explore scalability, integration with cloud-based security systems, and additional mitigation techniques to further enhance the effectiveness of the proposed solution.

V. ACKNOWLEDGEMENT

I would like to express our sincere gratitude to all those who contributed to the successful completion of this research work.First and foremost, we extend our heartfelt thanks to Dr.M.G.R. Educational and Research Institute, Chennai, for providing us with the necessary infrastructure and academic environment to carry out this project.

VII. REFERENCE

[1] A. Mishra, R. Shorey, and T. Nandagopal, “Security in wireless networks,” *IEEE Wireless Communications*, vol. 11, no. 1, pp. 50–61, Feb. 2020.

[2] C. Zhou, Y. Fang, and Y. Zhang, “Securing wireless communications of the future,” *IEEE Wireless Communications*, vol. 26, no. 5, pp. 32–39, Oct. 2019.

[3] S. Xu, W. Trappe, and Y. Zhang, “Jamming attacks and countermeasures in wireless networks,” *IEEE Network*, vol. 27, no. 6, pp. 4–9, Dec. 2020.

[4] J. Wright, “Detecting wireless LAN MAC layer attacks,” *Information Security Journal: A Global Perspective*, vol. 30, no. 4, pp. 162–168, 2021.

[5] T. Chiwewe and G. Hancke, “A distributed intrusion detection system for wireless sensor networks,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1723–1732, Mar. 2021.

[6] N. O. Tippenhauer, K. Rasmussen, and S. Capkun, “On the requirements for jamming-resistant wireless systems,” *ACM Transactions on Privacy and Security*, vol. 24, no. 2, pp. 1–28, May 2021.

[7] A. B. Smith and Y. Zhao, “Survey of recent advances in jamming detection for wireless communication,” *Computer Networks*, vol. 178, Article 107351, Jan. 2022.

[8] M. Hasan, A. Islam, and F. G. Martins, “Performance analysis of Wi-Fi jamming detection systems in resource-constrained environments,” *Ad Hoc Networks*, vol. 116, Article 102469, Jun. 2021.

[9] K. Alam, R. Roy, and N. Hossain, “Low-cost real-time Wi-Fi intrusion detection using NodeMCU,” in *Proc. of IEEE Global IoT Summit (GIoTS)*, 2021, pp. 83–87.

[10] M. Shafiq and H. Naeem, “MAC layer anomaly detection for wireless jamming attacks using ESP8266,” *Wireless Networks*, vol. 29, no. 1, pp. 399–412, Jan. 2023.

[11] L. P. Monteiro and A. de Souza, “Embedded IoT security monitoring using ESP8266 for home networks,” *Journal of Communications and Networks*, vol. 24, no. 2, pp. 102–109, Apr. 2022.

[12] K. Alam, R. Roy, and N. Hossain, “Design and Implementation of a Lightweight Wi-Fi IDS Using NodeMCU,” *Journal of Internet Services and Applications*, vol. 12, no. 3, pp. 45–52, 2021.

[13] H. Zhang and J. Li, “Detecting Wi-Fi jamming attacks using RSSI-based anomaly analysis,” *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2555–2564, Feb. 2022.

[14] R. Singh, M. Patel, and T. Mehta, “Reactive Jamming Detection on ESP8266: A Low-latency Approach,” in *Proc. of the International Conf. on Smart Systems and IoT*, 2022, pp. 101–106.

[15] S. Rahman, F. Alam, and J. Mahmud, “A decentralized IoT-based approach to detect multiple types of Wi-Fi jamming attacks,” *Sensors*, vol. 21, no. 9, Article 3175, May 2021.

[16] S. Bhattacharya, A. Khan, and R. R. Paul, “Real-Time Classification of Deauthentication Attacks Using Machine Learning,” *Computers & Security*, vol. 113, Article 102532, Nov. 2022.

[17] M. Lee, J. Lee, and Y. Choi, “Adaptive RSSI-Based Detection of Wi-Fi Jamming in Dense IoT Networks,” *IEEE Sensors Journal*, vol. 22, no. 8, pp. 7635–7643, Apr. 2022.

[18] H. Kim and M. Ahmed, “Hybrid Signal Fingerprinting for Lightweight Wi-Fi Jamming Detection on ESP8266,” *IoT Security Review*, vol. 3, no. 2, pp. 121–130, Dec. 2023.