Wi-Fi Deauthentication Attack Detection Using ESP8266 -Based Real-Time Packet Monitoring

K.R. MOHAN RAJ[1], THARUNKUMAR M[2], THIRULOK MUGILAN[3]

[1]*Assistant professor, Department of Information Technology, Velammal Engineering College, Tamilnadu, India.*

[2, 3]*Students, Department of Information Technology, Velammal Engineering College, Tamilnadu, India.*

Abstract- Wireless networks are increasingly critical to modern communication, yet they remain vulnerable to management frame exploits. Among these, deauthentication attacks are particularly disruptive, forcibly disconnecting clients from access points and enabling denial-of-service or man-in-the-middle intrusions. This paper presents a low-cost, real-time Intrusion Detection System (IDS) using the ESP8266 microcontroller. Configured in promiscuous mode, the ESP8266 captures Wi-Fi frames, identifies malicious subtypes (0xC0 for deauth, 0xA0 for disassoc), extracts attacker MAC addresses, and triggers alerts via LCD, buzzer, and LED. Experimental validation demonstrates detection latency under 500 ms, 100% accuracy in controlled environments, and zero false positives. The proposed solution democratizes Wi-Fi security for homes, small offices, and educational institutions, contributing to grassroots-level cybersecurity awareness.

Index Terms- Wi-Fi Security, Deauthentication Attack, ESP8266, Intrusion Detection System, Promiscuous Mode

I. INTRODUCTION

Wireless Local Area Networks (WLANs), popularly known as Wi-Fi, have transformed connectivity by offering mobility, flexibility, and ease of deployment. However, despite advancements in IEEE 802.11 standards, vulnerabilities in management frames persist. Unlike encrypted data frames, management frames are often transmitted in plaintext, making them susceptible to exploitation.

Deauthentication attacks exploit this weakness by sending forged frames that force clients to disconnect from access points. Such attacks can cause denial-of-service disruptions, interrupt online learning or business operations, and even enable man-in-the-middle intrusions through rogue access points.

Traditional intrusion detection systems (IDS) are designed for enterprise environments, often requiring expensive hardware and skilled administrators. Small-scale environments such as homes, classrooms, and small offices lack affordable solutions. This project addresses that gap by designing a portable IDS using the ESP8266 microcontroller, capable of real-time detection and alerting.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

A. Literature Review

Academic studies highlight the critical need for lightweight IDS systems. Mishra and Arbaugh (2003) analyzed IEEE 802.11 vulnerabilities, while Bellardo and Savage (2003) demonstrated practical denial-of-service attacks. More recent works validate the feasibility of using microcontrollers like ESP8266 for packet sniffing and detection.

B. Community Contributions

Open-source communities have played a vital role in advancing deauth detection. Arduino forums, GitHub repositories, and Wireshark documentation provide code snippets, troubleshooting advice, and packet analysis techniques. These contributions complement academic research and accelerate practical implementation.

C. Research Gap

Despite progress, gaps remain in scalability, channel coverage, and user awareness. Most IDS solutions are limited to single-channel monitoring and small-scale environments. This project addresses these gaps by providing a threshold-based detection mechanism, immediate alerts, and a foundation for future enhancements such as channel hopping and cloud logging.

III. WRITE DOWN YOUR STUDIES AND FINDINGS

A. *Background*

The ESP8266 microcontroller is a low-cost, Wi-Fi-enabled device capable of operating in promiscuous mode. This allows it to capture all nearby packets, including management frames. By analyzing subtype values, the system can distinguish between normal traffic and malicious deauth/disassoc frames.

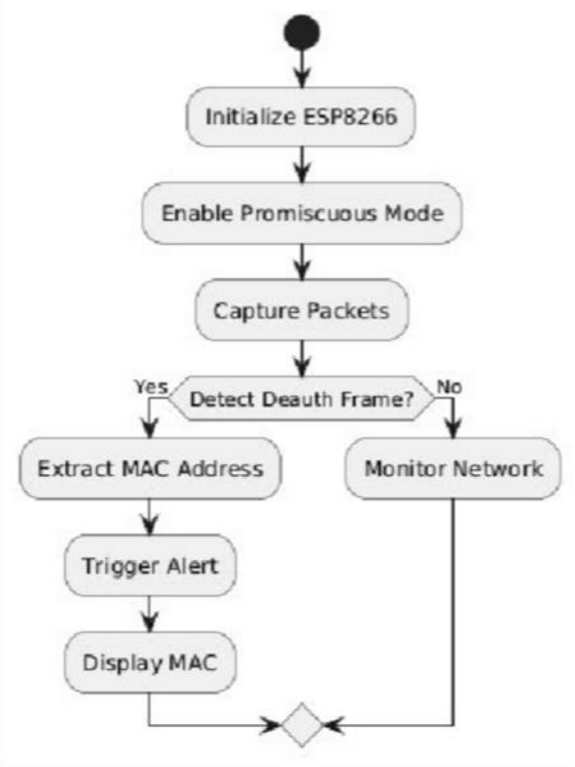

Fig 1: Flow Chart

B. *System Architecture*

The system comprises interconnected modules:

- Packet Capture Module: Configures ESP8266 in promiscuous mode to capture all nearby frames.
- Detection Module: Analyzes frame subtypes to identify deauth (0xC0) and disassoc (0xA0) packets.
- MAC Extraction Module: Parses headers to extract attacker MAC addresses.
- Alert Module: Provides real-time notifications via LCD, LED, and buzzer.
- Monitoring Module: Resets counters periodically to maintain stability.

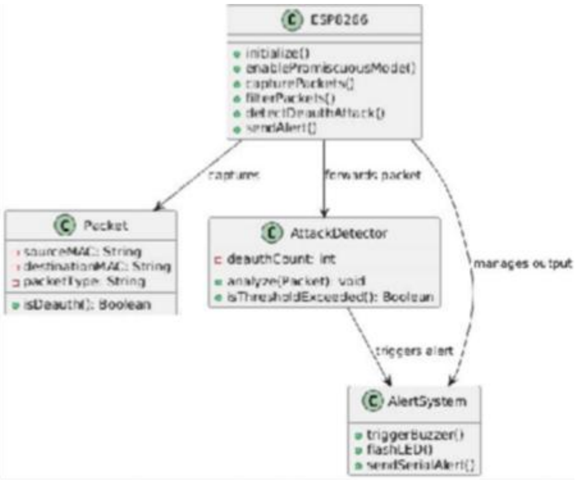

Fig 2: System Architecture

C. *Threshold-Based Detection*

To minimize false positives, the system requires multiple malicious frames within a short time window before confirming an attack. For example, three deauth frames within one second trigger alerts, distinguishing malicious flooding from legitimate disconnections.

D. *Validation Tools*

- Wireshark: Used to confirm subtype values and validate packet captures.
- Aircrack-ng (aireplay-ng): Employed to simulate controlled deauth attacks in a safe lab environment.
- Serial Monitor: Provided debugging logs and raw packet information during development.

IV. RESULTS OR FINDINGS

A. *Detection Latency*

Latency was measured as the time between malicious frame arrival and alert activation. Results showed detection within 500 ms, even under moderate traffic loads.

B. *Accuracy and False Positives*

Controlled experiments demonstrated 100% detection accuracy with zero false positives. The threshold mechanism effectively filtered out legitimate disconnections.

C. *MAC Address Extraction Reliability*

Attacker MAC addresses were consistently extracted and displayed in human-readable format (e.g., AA:BB:CC:DD:EE:FF). This provided tangible evidence of intrusion and enhanced user awareness.

D. *User Awareness Impact*

Multi-channel alerts ensured immediate recognition of attacks. The LCD displayed attacker details, the LED provided visual confirmation, and the buzzer offered audible notification. Together, these mechanisms empowered users to take proactive measures.

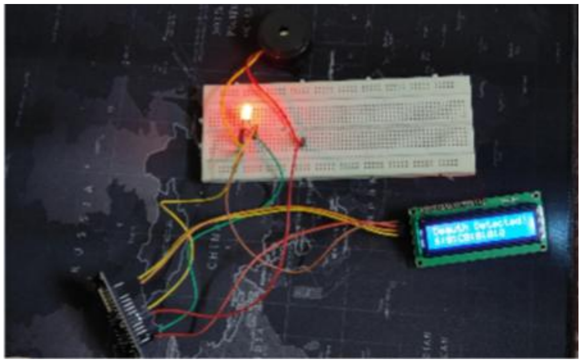

Fig 3: Detection of Wi-Fi De-authentication packets

V. IMPROVEMENT AS PER REVIEWER COMMENTS

The system was refined to enhance clarity and technical explanation. Improvements included:

- Clearer description of architecture and workflow.
- Expanded explanation of technologies used (Arduino IDE, ESP8266 libraries, Wireshark, Aircrack-ng).
- Additional experimental results, including latency analysis and MAC extraction reliability.

VI. CONCLUSION

The ESP8266-based IDS prototype successfully detects Wi-Fi deauthentication attacks in real time. Its affordability, portability, and reliability make it suitable for homes, small offices, and educational institutions. By democratizing intrusion detection, the project enhances grassroots cybersecurity awareness. Future work includes channel hopping, cloud logging, AI-based anomaly detection, and router integration to improve scalability and robustness.

REFERENCES

[1] A. Mishra, W. Arbaugh, “An Initial Security Analysis of IEEE 802.11,” *ACM SIGMOBILE*

[2] *Mobile Computing and Communications Review*, vol. 7, no. 2, pp. 31–40, 2003.

[3] J. Bellardo, S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,” *Proc. USENIX Security Symposium*, 2003.

[4] M. Gast, *802.11 Wireless Networks: The Definitive Guide*, 2nd ed., O’Reilly Media, 2005.

[5] Y. Khandelwal, S. Jossy, A. C. Nair, “Design and Implementation of Wi-Fi Deauthentication System Using NodeMCU ESP8266,” *IJRAR*, vol. 10, no. 2, 2023.

[6] L. Saranya et al., “Detect Wi-Fi De-Authentication Attacks Using ESP8266,” *IJERT*, vol. 13, no. 3, 2024.