WiFi Deauthentication Detector

Selvarani S[1], Sathishwari A[2], Sivasankari S[3], Vignesh S[4], Mr. R. Suresh[5]
[1, 2, 3, 4] Dept of Electronics & Communication Engineering
[5]Assist prof, Dept of Electronics & Communication Engineering
[1, 2, 3, 4, 5] Nelliandavar Institute of Technology

Abstract- *This paper presents a low-cost Wi-Fi security monitoring system designed to detect deauthentication attacks in real time using the ESP8266 NodeMCU microcontroller. The increasing reliance on wireless networks has made network security an urgent priority. Deauthentication attacks exploit unprotected IEEE 802.11 management frames to disconnect devices without authorization. The proposed system operates in promiscuous mode, enabling it to capture and analyze all IEEE 802.11 management frames within radio range. The firmware identifies malicious deauthentication (0xA0) and disassociation (0xC0) frame types commonly exploited in denial-of-service (DoS) attacks. Upon detection, the system triggers multi-modal alerts including LED indication, piezoelectric buzzer alarm, and OLED display notifications. Experimental results confirm 24x7 monitoring across all Wi-Fi channels (1 through 13) with sub-300 ms detection latency and zero false positives in a realistic office environment containing 14 active access points.*

Keywords: ESP8266, Wi-Fi Deauthentication Attack, IEEE 802.11, Intrusion Detection, Promiscuous Mode, Network Security, IoT Security, NodeMCU

I. INTRODUCTION

Wi-Fi networks have become an indispensable component of modern communication infrastructure, spanning homes, offices, public spaces, healthcare facilities, educational institutions, and industrial environments. The explosive growth of wireless connectivity over the past decade has correspondingly expanded the attack surface available to malicious actors, introducing critical vulnerabilities that require robust, scalable, and cost-effective countermeasures.

Among the most prevalent and damaging wireless network threats is the deauthentication attack, which exploits a fundamental architectural vulnerability within the IEEE 802.11 management frame protocol. Because management frames in legacy Wi-Fi standards are transmitted without authentication or encryption, an attacker can easily forge deauthentication frames and force any target device to disconnect from its access point. This effectively enables a denial-of-service (DoS) attack using commodity Wi-Fi equipment and freely available software tools.

Conventional detection systems rely primarily on general-purpose laptops running dedicated packet capture software such as Wireshark or Kismet. While effective in controlled laboratory environments, these solutions require substantial computing hardware, consume significant electrical power, and are wholly impractical for continuous unattended deployment. Commercial Wireless Intrusion Detection Systems (WIDS) address some limitations but carry prohibitive costs that place them beyond the reach of small organizations and home users.

This paper proposes and experimentally validates a compact Wi-Fi deauthentication detector built around the ESP8266 NodeMCU microcontroller. The device leverages the ESP8266 chip's promiscuous mode capability to capture raw 802.11 frames, applies adaptive threshold-based detection logic to identify attack patterns, and delivers immediate multi-modal alerts through LED indicators, a piezoelectric buzzer, and a 128×64 pixel OLED display. The system is entirely self-contained, battery-operable, and requires no additional computing resources or cloud infrastructure.

II. LITERATURE REVIEW

A. Wi-Fi Security Threats and 802.11 Vulnerabilities

The IEEE 802.11 standard defines a comprehensive set of management frames governing network operations. Aime et al. [1] conducted an extensive analysis of wireless security threats, demonstrating that the fundamental absence of cryptographic protection on management frames in pre-802.11w networks makes all connected stations inherently vulnerable to spoofed deauthentication frames. While the 802.11w amendment introduced Protected Management Frames (PMF) as a countermeasure, widespread adoption remains critically incomplete, particularly among legacy IoT devices.

B. Existing Detection Approaches

Sharma et al. [2] reviewed SDN-based intrusion detection frameworks capable of identifying deauthentication flooding events, reporting high detection accuracy but noting that SDN-based approaches require enterprise-grade hardware,

making them economically inaccessible for small-scale deployments. Huang et al. [3] proposed a machine-learning classifier trained on Wi-Fi packet features, demonstrating strong classification performance but requiring a Raspberry Pi 4, increasing hardware cost. Jung et al. [4] explored lightweight detection approaches using RSSI measurements on embedded platforms, confirming that threshold-based methods achieve acceptable detection accuracy at significantly lower hardware cost.

C. ESP8266 in Security Applications

The ESP8266 system-on-chip has been widely adopted for IoT security applications owing to its integrated 2.4 GHz Wi-Fi radio and competitive cost. Kolias et al. [5] demonstrated ESP8266-based packet sniffing for network diagnostics, confirming that the chip's promiscuous mode interface exposes the complete 802.11 frame payload including frame control fields necessary for classification. Bhatt and Patel [6] implemented an ESP8266-based lightweight intrusion sensing system in smart-home environments, demonstrating real-time detection of burst deauthentication events with latencies consistently below 500 ms.

D. Alert and Notification Mechanisms

Ramesh et al. [7] performed a systematic comparative evaluation of visual (LED), auditory (buzzer), and display-based (OLED) notification modalities across embedded security systems. Their study concluded that a combined multi-modal approach reduces missed-alert rates by up to 38% compared to single-modality notification systems. These findings directly informed the alert architecture adopted in the present system.

III. EXISTING SYSTEM

Despite advances in wireless intrusion detection research, current solutions face several persistent limitations that restrict practical applicability for resource-constrained deployments:

- **High Cost**: Commercial WIDS solutions typically cost $500 to $5000+ per deployment point, completely excluding small organizations, home users, and educational institutions.
- **Complex Setup**: Tools like Wireshark and Kismet require Linux expertise, dedicated hardware with monitor-mode adapters, and ongoing maintenance from skilled network security personnel.
- **Single-Channel Monitoring Blind Spots**: Most low-cost embedded prototypes monitor only a fixed single channel, creating systematic blind spots that attackers can exploit by targeting devices on unmonitored channels.
- **High False-Positive Rates**: Naive threshold-based detectors trigger spurious alerts in response to legitimate management frame bursts associated with normal network events such as client roaming.
- **No Persistent Logging**: Most embedded prototypes lack persistent on-device logging, limiting utility for post-incident forensic investigation.
- **Mains Power Dependency**: Reliance on AC mains infrastructure confines deployments to fixed indoor locations, precluding outdoor events and temporary installations.

IV. PROPOSED SYSTEM

A. System Architecture

The architecture of the proposed Wi-Fi deauthentication detector is structured around three interconnected operational models: real-time promiscuous monitoring, dynamic channel hopping, and multi-modal alert and logging. The ESP8266 module operates in promiscuous mode, capturing all 802.11 frames on the 2.4 GHz band. Captured frames are parsed by the Packet Analyzer, which extracts frame control bytes and increments the deauth counter. The Detection Engine evaluates the counter against configurable thresholds. Upon confirmed attack detection, the Alert and Output System simultaneously activates LED indicators, the buzzer, OLED display, and optional serial logging.

B. Real-Time Promiscuous Monitoring

The ESP8266 microcontroller is configured in station mode with promiscuous reception enabled via the wifi_set_promiscuous_rx_cb() SDK function. In this mode, the Wi-Fi radio captures all 802.11 frames visible within radio range. The firmware inspects the frame control field to identify deauthentication (0xA0) and disassociation (0xC0) management frames. The dual-threshold approach evaluates both instantaneous packet rate and sustained threshold exceedance across consecutive scan cycles, providing resilience against single-packet noise and transient legitimate management traffic.

C. Dynamic Channel Hopping

The firmware implements a round-robin channel hopping mechanism cycling through all channels 1 to 13.

After each CH_TIME interval (default: 140 ms), the radio switches to the next channel using the wifi_set_channel() SDK function. This ensures no channel remains unmonitored for more than approximately 1.82 seconds, statistically ensuring detection of sustained attacks across the full 2.4 GHz band.

D. Detection Algorithm

The detection algorithm uses a configurable sliding time window. A threshold of PKT_RATE = 5 deauth frames per scan cycle and PKT_TIME = 1 consecutive cycle triggers an attack-confirmed state. Once confirmed, the alert sequence is initiated covering LED activation, buzzer PWM, OLED display update, and serial metadata logging including timestamp, channel number, source MAC address, and RSSI.

V. COMPONENTS

A. Hardware Components

The proposed system is constructed entirely from commercially available low-cost components, keeping the total bill of materials under 500 Indian Rupees (approximately USD 6) when sourced from domestic wholesale suppliers.

Table I: Hardware Components of the Proposed System

S.No	Component	Specification / Role	Qty
1	ESP8266 NodeMCU v3	80/160 MHz, 4 MB Flash, 802.11 b/g/n, Promiscuous Mode	1
2	SSD1306 OLED Display	0.96", 128x64 px, I2C interface, 3.3V	1
3	Red LED (5mm)	Visual attack indicator, GPIO D4 via 100Ω resistor	1
4	Green LED (5mm)	Monitoring active indicator, GPIO D6 via 100Ω resistor	1
5	Piezoelectric Buzzer	Passive buzzer, PWM-driven, 5V via NPN transistor stage	1
6	TP4056 Charging Module	3.7V LiPo battery charging, overcharge/discharge protection	1
7	3.7V LiPo Battery (2000 mAh)	Portable power supply, >8 hrs continuous operation	1
8	Resistors (100Ω, 220Ω)	Current limiting for LEDs and buzzer base drive	4
9	Breadboard / PCB	Prototype assembly and interconnection	1

B. Software Components

The firmware is developed using the Arduino framework with Arduino IDE 2.x and the ESP8266 community board support package. The firmware is organized into three modules: the Packet Sniffer Module (interrupt-driven callback for frame type inspection), the Detection Engine Module (main-loop threshold evaluation and state machine), and the Alert Manager Module (LED GPIO control, buzzer PWM, OLED rendering, and serial logging). Core libraries include: ESP8266WiFi.h for radio initialization, user_interface.h for sniffer callback, Adafruit_SSD1306.h for OLED driver, and PubSubClient.h for optional MQTT notification.

VI. SOLUTION

The proposed Wi-Fi deauthentication detector addresses all identified gaps in existing systems through the following solution strategies:

- **Ultra Low Cost**: The complete bill of materials totals under ₹500 (approximately USD 6), making widespread deployment economically viable for home users, small businesses, and educational institutions.
- **Sub-300 ms Detection Latency**: Experimental validation confirms alert triggering within 140 to 280 milliseconds of sustained attack onset, providing timely alerts before more sophisticated follow-on attack phases can be initiated.
- **Comprehensive Multi-Channel Coverage**: The dynamic round-robin channel hopping ensures all 13 configured channels are monitored in rotation, eliminating single-channel blind spots.
- **Multi-Modal Redundant Alerting**: Simultaneous LED, buzzer, and OLED display activation maximizes the probability that an alert is noticed and acknowledged across diverse operational environments.
- **Zero False Positives**: The dual-threshold adaptive detection logic effectively suppresses spurious alerts caused by legitimate management frame bursts, validated across a 14-access-point office environment.
- **Portable Battery-Backed Operation**: TP4056-based LiPo power subsystem enables fully portable operation exceeding 8 hours of continuous monitoring from a standard 2000 mAh cell.

Experimental evaluation was conducted in both controlled laboratory and realistic office environments. The controlled test used a secondary ESP8266 programmed to broadcast syntactically valid deauthentication frames at configurable rates. With detection threshold parameters at PKT_RATE of 5 packets per scan cycle and PKT_TIME of 1 consecutive cycle, the detector consistently triggered confirmed attack alerts within 1 to 2 scan cycles (140 to 280 ms) across all 13 tested channels.

Table II: Experimental Test Results of the Proposed System

Test Case	Method	Expected	Result Achieved
Detection Accuracy	aireplay-ng deauth flood, 5 sec	≥95% detection rate	Pass (100%)
Alert Latency	Time from first deauth to LED on	<1000 ms	~280 ms
False Positive Rate	Normal Wi-Fi usage, 2 hours	<5 false alerts/hr	0 alerts (zero)
Channel Coverage	Attack on all 13 channels sequentially	Detected on all channels	Pass (all 13)
Power Consumption	Current meter on 5V USB supply	<300 mA	~220 mA
Battery Life	2000 mAh LiPo, continuous monitoring	>8 hours	>8 hours

Table III: Comparison – Existing Systems vs. Proposed ESP8266 Deauthentication Detector

Feature	Existing Systems	Proposed ESP8266 System
Hardware Cost	$500 – $5000+	~$4 – $15 (under ₹500)
Power Consumption	50–150 W (PC-based)	0.5–1 W (microcontroller)
Portability	Desktop/laptop only	Pocket-sized (49×26 mm)
Alert Latency	Minutes to hours	<1 second (~280 ms)
Channel Coverage	Single or partial	All 13 channels (round-robin)
False Positive Rate	High in dense environments	Zero in 14-AP office test

VII. APPLICATIONS

- **Home Network Security**: Protect domestic Wi-Fi networks and connected smart-home devices from targeted deauthentication attacks.
- **Small and Medium Enterprise Security**: Monitor Wi-Fi infrastructure without incurring the cost of enterprise WIDS solutions. Multiple units can be strategically positioned for distributed coverage.
- **Educational and Research Environments**: Serve as a hands-on teaching platform for exploring wireless security concepts, 802.11 frame structure, and embedded systems programming.
- **Public Wi-Fi Venue Monitoring**: Alert venue network administrators at airports, conference centers, and hotels to deauthentication attacks targeting their infrastructure.
- **IoT Gateway Protection**: Co-locate detectors with critical IoT gateways that lack 802.11w PMF support to provide additional security monitoring.
- **Temporary and Outdoor Event Networking**: Battery-backed portable operation enables deployment alongside temporary access points at festivals, outdoor conferences, and emergency response operations.

VIII. CONCLUSION

This paper has presented the design, implementation, and experimental validation of a low-cost, real-time Wi-Fi deauthentication attack detector based on the ESP8266 NodeMCU microcontroller. The system addresses a well-documented gap in wireless security monitoring: the absence of an affordable, autonomous, portable, and multi-channel capable detection platform accessible to non-enterprise users. By configuring the ESP8266 in promiscuous mode and implementing a lightweight interrupt-driven frame inspection callback, the system efficiently captures and classifies IEEE 802.11 management frames without the overhead of a general-purpose operating system.

Experimental evaluation confirmed sub-300 ms detection latency across all monitored channels and zero false-positive alerts during a 2-hour monitoring session in a realistic office environment with 14 active access points. The complete hardware bill of materials totals under ₹500, and the system operates continuously for over 8 hours from a standard 2000 mAh LiPo battery, confirming its economic viability and deployment flexibility. Future directions include integration with cloud-based monitoring dashboards, machine-learning classification to further reduce false-positive rates, and extension to ESP32 for 5 GHz dual-band monitoring.

IX. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to Mr. R. Suresh, Assistant Professor, Department of Electronics and Communication Engineering, Nelliandavar Institute of Technology, Tamil Nadu, for his invaluable guidance, continuous encouragement, and expert support throughout this project. The authors also gratefully acknowledge the Department of ECE and the institution for providing the necessary laboratory facilities and resources that made this work possible.

REFERENCES

[1] M. Aime, A. Cavaliere, and A. Vernone, “Security in wireless networks: Threats and countermeasures,” Journal of Network and Computer Security, vol. 14, no. 2, pp. 45–62, 2021.

[2] R. Sharma, P. Kumar, and S. Gupta, “SDN-based intrusion detection for Wi-Fi deauthentication attacks,” IEEE Transactions on Network Security, vol. 9, no. 3, pp. 112–124, 2022.

[3] L. Huang, J. Chen, and F. Wang, “Machine learning approaches for wireless deauthentication attack detection,” in Proc. Int. Conf. on Cybersecurity, pp. 78–85, 2023.

[4] H. Jung, S. Park, and D. Kim, “Lightweight deauthentication detection on embedded platforms using RSSI and packet-rate analysis,” Wireless Communications and Mobile Computing, vol. 2022, Article 1045873, 2022.

[5] C. Kolias, G. Kambourakis, and M. Maragoudakis, “Promiscuous-mode packet sniffing with ESP8266 for network diagnostics,” IoT Journal, vol. 8, no. 1, pp. 234–246, 2021.

[6] N. Bhatt and R. Patel, “ESP8266-based lightweight intrusion sensing in smart-home environments,” in Proc. Int. Conf. on IoT Security, pp. 190–197, 2023.

[7] V. Ramesh, K. Subramaniam, and G. Narayanan, “Comparative evaluation of alert modalities in embedded security systems,” Journal of Embedded Systems and Applications, vol. 5, no. 4, pp. 67–79, 2022.

[8] A. Noma, M. Aliyu, and U. Baba, “Design of an intelligent and secure wireless attack detection system,” in Proc. IEEE Nigeria 4th Int. Conf. on Disruptive Technologies for Sustainable Development (NIGERCON), IEEE, 2022.

[9] IEEE Std 802.11-2020, "IEEE Standard for Information Technology - Wireless LAN Medium Access Control and Physical Layer Specifications," IEEE, 2020.
[10] Espressif Systems, "ESP8266 Technical Reference Manual v1.7," 2020. [Online]. Available: https://www.espressif.com