IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155139

A Lightweight Wireless Intrusion Detection System for Real-Time Deauthentication and Rogue Access Point Mitigation.

Nandini Rajesh Kasar

Department of Computer Science Engineering, International Center of Excellence In Engineering and Management (ICEEM), Maharashtra, India

Abstract: The pervasive deployment of IEEE 802.11 wireless networks has revolutionized digital connectivity, but it has simultaneously expanded the attack surface for threat actors. A critical vulnerability within legacy Wi-Fi protocols is the transmission of management frames in an unencrypted and unauthenticated format. This flaw is routinely exploited to execute deauthentication denial-of-service (DoS) attacks and deploy Rogue Access Points (RAPs) or "Evil Twins" to intercept sensitive data. This paper presents a lightweight, low-cost Wireless Intrusion Detection System (WIDS) architecture utilizing a Raspberry Pi and monitor-mode network adapters. By employing a Python-based detection engine leveraging Scapy and tcpdump, the proposed system effectively identifies deauthentication floods, SSID-BSSID duplication, MAC spoofing, and abnormal Received Signal Strength Indicator (RSSI) variations. Experimental results validate the system's ability to provide real-time alerts and forensic packet captures (PCAP) with minimal computational overhead, offering a highly scalable solution for enterprise and edge-network security.

I. INTRODUCTION

Wireless networks rely on open radio frequencies, making them inherently susceptible to interception and spoofing. Unlike wired infrastructure where physical access is restricted, an attacker merely needs to be within radio range to compromise a Wi-Fi network. A fundamental architectural weakness in the IEEE 802.11 standard is that crucial management frames—such as beacons, probes, and deauthentication packets—lack cryptographic protection.

This allows adversaries to easily forge the Media Access Control (MAC) address of a legitimate Access Point (AP) and forcefully disconnect clients (Deauthentication Attack). Furthermore, attackers can configure unauthorized networks broadcasting the same Service Set Identifier (SSID) to trick user devices into connecting, effectively establishing a Man-in-the-Middle (MitM) position (Rogue AP Attack). Because these attacks operate at Layer-2 of the OSI model, conventional IP-based firewalls fail to detect them. This necessitates the deployment of specialized, passive Wireless Intrusion Detection Systems (WIDS) capable of analyzing raw radio frames.

II. RELATED WORK

Securing wireless airspace has been a persistent challenge for network administrators. Early defensive strategies relied heavily on traditional signature-based detection mechanisms. These systems maintain a database of known malicious byte sequences or specific frame patterns and trigger an alert when matching traffic is observed. While this method is highly accurate for well-documented attacks, it is inherently rigid and cannot identify novel, zero-day attack variations. To counter this, researchers shifted toward anomaly-based detection, which learns a baseline of "normal" network behavior and flags statistical deviations. While theoretically more robust against new threats, early anomaly models struggled in dynamic wireless environments, often producing high rates of false positives when legitimate users simply roamed between access points or when environmental interference caused sudden traffic spikes.

III. LITERATURE SURVEY

Current literature reveals a multi-faceted approach to wireless intrusion detection, generally divided into specific analytical techniques:

- **Signature and Threshold Analysis:** Many systems utilize rule engines to count the occurrence of specific frames over a set time period, specifically targeting the repetitive bursts characteristic of deauthentication attacks.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155139

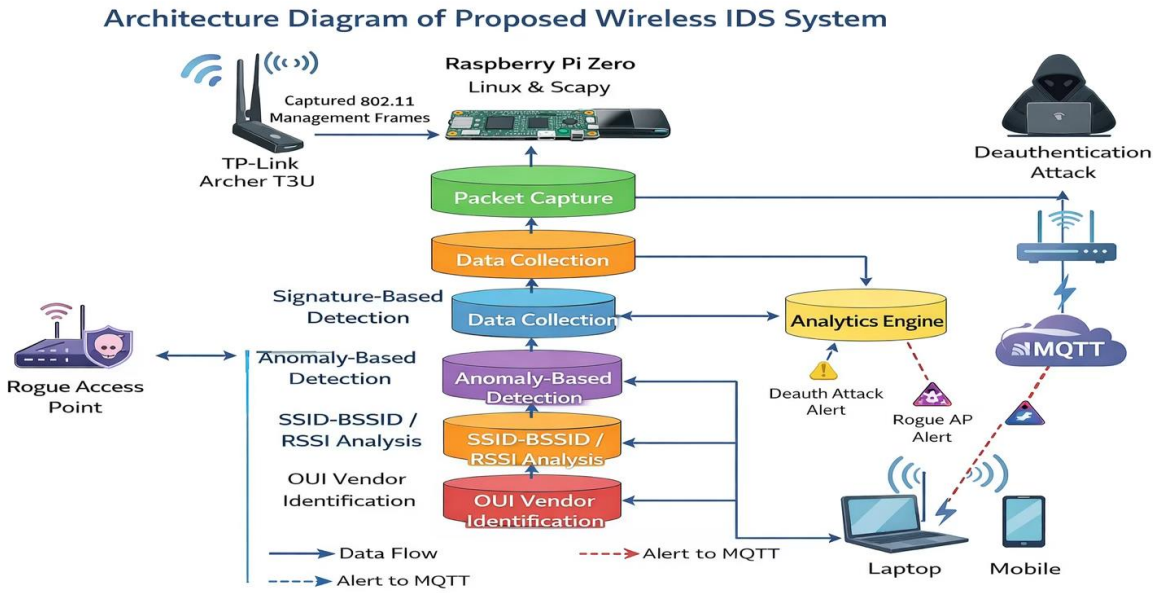
- **SSID-BSSID Mapping:** Attackers frequently clone a target network's name (SSID) to lure victims. Researchers have demonstrated that cross-checking an SSID against its hardware MAC address (BSSID) and tracking these mappings geographically is a highly reliable way to expose Evil Twin access points.
- **Vendor (OUI) Fingerprinting:** Every MAC address contains an Organizationally Unique Identifier (OUI) denoting its manufacturer. Literature suggests that checking the OUI against the expected hardware behavior (e.g., a high-end Cisco router broadcasting a generic ESP8266 manufacturer code) quickly identifies spoofed devices.
- **Machine Learning Integration:** Modern research is heavily focused on deploying supervised learning algorithms (like Support Vector Machines and Random Forests) to automatically classify complex, multi-stage attack traffic, though these models require substantial, high-quality training datasets.

IV. PROPOSED SYSTEM

To address the limitations of rigid legacy systems, we propose a lightweight, highly portable Wireless Intrusion Detection System (WIDS) designed for real-time edge monitoring.

The system's architecture is built on accessible hardware, primarily utilizing a Raspberry Pi 5b alongside a monitor-mode capable external Wi-Fi adapter, such as a TP-Link T3U or an Alfa network card. The software stack runs entirely on a Linux ecosystem, providing a stable foundation for the core operational modules:

1. **Packet Capture Module:** Silently listens to the surrounding radio frequencies, using tools like tcpdump and Scapy to ingest raw 802.11 management frames.
2. **Detection Engine:** The system's logic core, which cross-references incoming packets against threshold rules, SSID duplication checks, and OUI validation databases.
3. **Alert and Logging Module:** Generates immediate, JSON-formatted alert notifications while simultaneously extracting a small PCAP (packet capture) snippet of the exact moment the attack occurred.

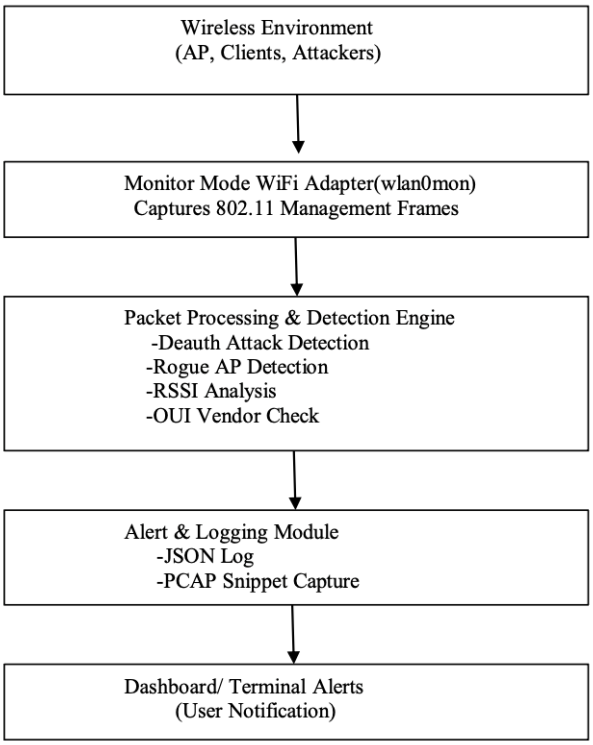


IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155139



V. METHODOLOGY AND VALIDATION

The operational workflow begins by isolating the external Wi-Fi adapter from the operating system's standard networking processes. Using commands like airmon-ng check kill and airmon-ng start wlan0, the interface is successfully transitioned into wlan0mon. In this state, it acts as a passive sniffer, capturing all broadcast traffic without actively associating with any network.

The detection engine continuously evaluates this traffic stream. For instance, it actively charts the Received Signal Strength Indicator (RSSI) of known access points. If the engine detects an abnormal, sudden jump in signal strength from a supposedly stationary AP, it recognizes that an attacker has likely physically moved a spoofing device closer to the target client.

While the lightweight edge sensor successfully operates on a low-power Raspberry Pi, the resulting forensic PCAP files are formatted perfectly so they can be exported to robust local development environments—such as a virtualization-heavy, 16GB memory setup—for deep-dive vulnerability assessment and penetration testing (VAPT) analysis. This architecture not only serves as a practical defensive tool but also provides an excellent, structured framework for teaching foundational cybersecurity and ethical hacking methodologies.

VI. RESULTS

The system was validated through a series of controlled attack simulations, demonstrating high accuracy and low latency.

- **Deauthentication Detection:** When subjected to a simulated deauthentication flood, the system successfully parsed the malicious 802.11 frames. The Python-based Scapy engine immediately triggered an alert, accurately logging the attacker's spoofed MAC address alongside a forensic PCAP file for evidence.
- **Rogue AP Identification:** During an Evil Twin simulation, the detection script successfully caught the SSID-BSSID mismatch in real-time, outputting a duplicate_ssid warning containing the conflicting hardware addresses.
- **Signal Anomaly Tracking:** The RSSI monitoring logic proved highly sensitive. The system successfully recorded a sudden 28 dBm jump in signal strength, accurately flagging the event as a suspected proximity-based impersonation attack

The system was validated through a series of controlled attack simulations, demonstrating high accuracy and low latency.

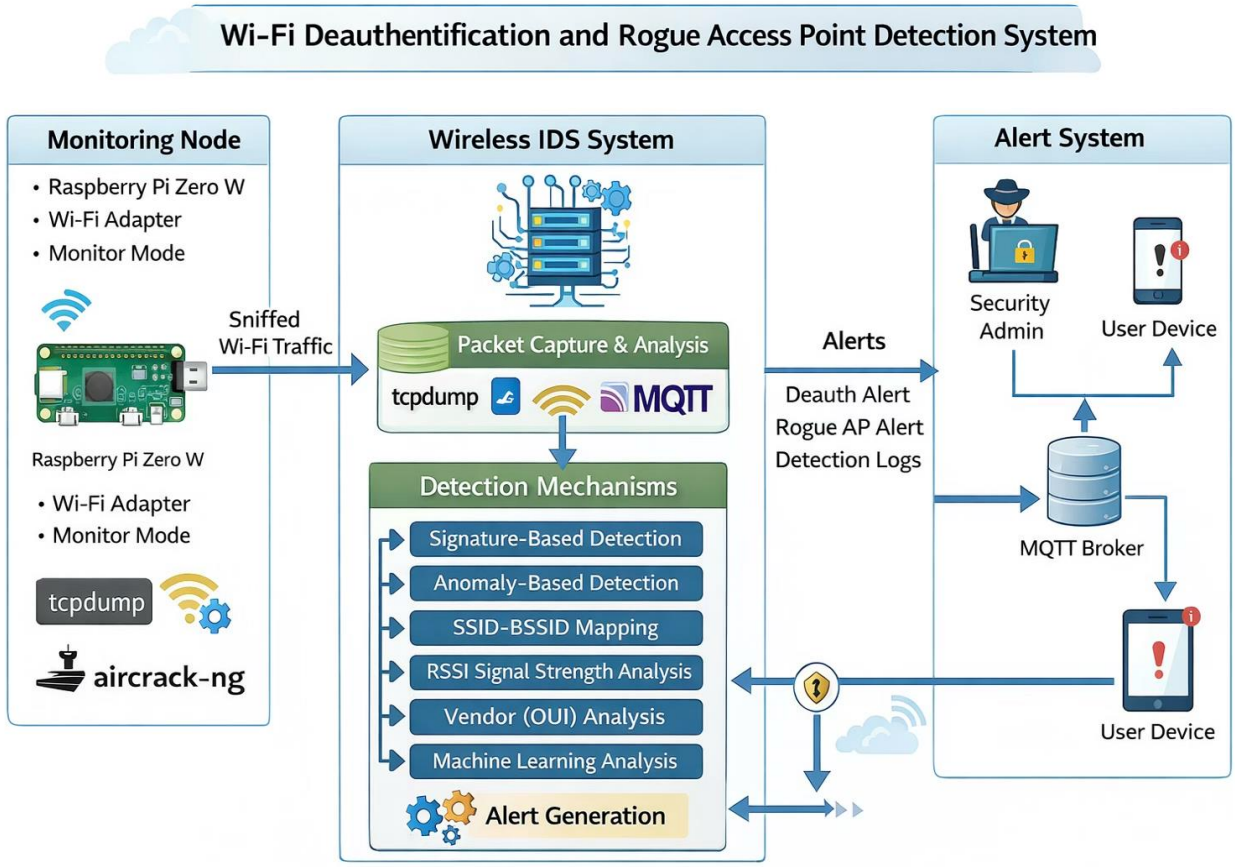
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155139

- **Deauthentication Detection:** When subjected to a simulated deauthentication flood, the system successfully parsed the malicious 802.11 frames. The Python-based Scapy engine immediately triggered an alert, accurately logging the attacker's spoofed MAC address alongside a forensic PCAP file for evidence.
- **Rogue AP Identification:** During an Evil Twin simulation, the detection script successfully caught the SSID-BSSID mismatch in real-time, outputting a duplicate_ssid warning containing the conflicting hardware addresses.
- **Signal Anomaly Tracking:** The RSSI monitoring logic proved highly sensitive. The system successfully recorded a sudden 28 dBm jump in signal strength, accurately flagging the event as a suspected proximity-based impersonation attack.



Software Used:
1. Operating System
Linux OS:Kali Linux,Ubuntu,Raspberry Pi OS

2. Wireless & Monitoring Tools
aircrack-ng:Monitor mode configuration,Channel hopping & testing
airodump-ng:Access point and client scanning
iw / iwconfig:Wireless interface verification

3. Packet Capture & Analysis
Tcpdump:Real-time packet capture,PCAP logging
Wireshark:Offline packet analysis

4. Detection & Automation
Python 3
Scapy:Packet parsing and attack detection
Custom Python Scripts:Deauth detection,Rogue AP detection,RSSI anomaly detection,OUI/vendor mismatch detection

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155139

5. System Management
Systemd:Auto-start detection services on boot
Logrotate:Automatic log rotation

6. Alert & Communication (Optional)
MQTT Broker (Mosquitto):Alert transmission
JSON Logging:Event-based alerts and logs

VII. CONCLUSION AND FUTURE SCOPE

The inherent lack of encryption in IEEE 802.11 management frames continues to leave wireless networks vulnerable to severe disruption and data theft. This research confirms that effective, real-time wireless defense does not require expensive, enterprise-grade hardware. By leveraging open-source Linux tools and affordable microcomputers, organizations can deploy a highly reliable WIDS capable of instantly identifying spoofing, rogue access points, and deauthentication attacks.

Future Scope:
To adapt to increasingly sophisticated adversaries, the system's future iterations will focus on three key areas:

1. **AI-Driven Anomalies:** Integrating advanced Machine Learning classifiers to build real-time behavioral profiles, allowing the system to identify subtle, zero-day threats beyond static threshold rules.
2. **Automated Mitigation:** Evolving the system from passive detection to active prevention (WIPS) by enabling automated responses, such as dynamically blocking malicious MAC addresses or isolating rogue access points.
3. **Cloud Integration:** Developing a comprehensive web-based graphical dashboard for centralized security management, ensuring the architecture is scalable and ready to monitor next-generation IoT and 6G wireless environments.

WiFi deauthentication and rogue access point attacks remain a major concern due to weak management frame protection in IEEE 802.11 networks. This paper reviewed attack mechanisms and summarized detection approaches including signature-based, anomaly-based, signal-based, vendor-based, and machine learning techniques[1],[5]. A lightweight monitoring system using Linux, monitor-mode adapters, tcpdump, and Raspberry Pi Zero offers a practical solution for real-time detection.

REFERENCES

[1]. Beyah, R., Venkataraman, A., "Rogue-access-point detection: Challenges, solutions, and future directions," *IEEE Security & Privacy*, vol. 9, no. 5, pp. 56-61, Sept.-Oct. 2011.
[2]. Dalal, A., Jain, A., Sharma, R., "A Wireless Intrusion Detection System for 802.11 WPA3 Networks," *Proc. Int. Conf. on IoT and Network Security*, pp. 1-6, 2021.
[3]. Chen, H.-H., Lin, H.-T., "A Survey of Wireless Intrusion Detection Systems," *IEEE Commun. Surveys & Tutorials*, vol. 7, no. 3, pp. 38-56, 2005.
[4]. Daryabar, F., Dehghantanha, A., Udzir, N., "Lightweight rogue access point detection algorithm for WiFi-enabled IoT devices," *Journal of Information Security and Applications*, vol. 54, pp. 102-114, 2020.
[5]. Chen, Y., et al., "ETGuard: Detecting Evil Twin attacks in Wi-Fi networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2046-2059, Aug. 2019.
[6]. **Chen, Y., et al.**, "ETGuard: Detecting Evil Twin attacks in Wi-Fi networks," IEEE Transactions on Information Forensics and Security, vol. 14, no. 8, pp. 2046–2059, Aug. 2019.
[7]. **Gurtej, S., Kumar, V.**, "Detection of fake access points using supervised learning algorithms in IEEE 802.11 networks,IEEE Access, vol. 10, pp. 75432–75445, 2022.
[8]. **Sethuraman, S.C., et al.**, "Wireless intrusion detection using hybrid KDE and HMM classification models," IET Networks, vol. 8, no. 2, pp. 112–118, 2019.
[9]. **Kristiyanto, D., Ernastuti**, "Analysis of Deauthentication Attack on IEEE 802.11 IoT devices," Proc. Int. Conf. on Information Technology Systems and Innovation (ICITSI), pp. 177–182, 2018.
[10]. **Ray, B., Chaki, R.**, "A systematic review on intrusion detection in wireless networks: Variants, attacks and applications," Wireless Personal Communications, vol. 130, pp. 1243–1265, 2023.
[11]. **Wu, H., Wu, H., Xu, Q.,** "Detecting Rogue Access Points Using Wireless Intrusion Detection Systems," Proc. IEEE Global Communications Conference (GLOBECOM), pp. 6823917, 2013.
[12]. **Prakash, S., Shukla, S.,** "Wi-Fi Deauthentication Attack and Its Detection in Wireless Networks," *Int. J. of Computer Applications*, vol. 143, no. 6, pp. 1-6, 2016.

