International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 15 Issue 3, March-2026

# Rogue Access Points Detection

Akash Ankush Chitale[1], Aniket Manikro Barkade[2]

[1,2]Department of Computer Engineering, Navsahyadri Group of Institutions, Pune, Maharashtra, India

**ABSTRACT**

**Wireless networking technologies based on IEEE 802.11 standards have become indispensable in modern communication infrastructure. Enterprises, educational institutions, healthcare systems, government offices, and public environments rely heavily on WiFi connectivity to support operational efficiency and digital transformation. Despite their flexibility and scalability, wireless networks are inherently vulnerable due to the broadcast nature of radio frequency communication. Unlike wired networks, where physical access is required, wireless signals propagate through open air and can be intercepted by any device within range. This exposure significantly increases the attack surface.**

**Among the most critical wireless threats is the Rogue Access Point (RAP). A rogue access point is any unauthorized wireless device operating within or near an organization's legitimate network. Such devices may be maliciously deployed by attackers to intercept sensitive information or unintentionally installed by employees without administrative approval. Rogue access points can facilitate credential harvesting, traffic interception, denial-of-service attacks, lateral movement within the network, and man-in-the-middle exploitation. The increasing adoption of bring-your-own-device (BYOD) policies further complicates the detection of unauthorized wireless infrastructure.**

**This research proposes a real-time Rogue Access Point Detection System (RAPDS) based on passive wireless monitoring and identifier validation. The system operates by capturing IEEE 802.11 beacon frames in monitor mode, extracting essential parameters including SSID, BSSID, channel information, encryption type, and signal strength, and validating them against a predefined database of authorized access points. Suspicious access points are identified using rule-based classification and logged through a centralized monitoring interface. Experimental evaluation in a controlled environment demonstrates high detection accuracy, low false positive rate, and near real-time response capability.**

**The proposed framework offers a cost-effective and scalable wireless intrusion detection mechanism suitable for small and medium enterprises. It enhances wireless visibility, strengthens security posture, and provides a practical foundation for advanced research in wireless threat detection.**

**Keywords: Rogue Access Point, Wireless Intrusion Detection System, IEEE 802.11 Security, BSSID Verification, Evil Twin Detection, Packet Sniffing, Network Monitoring, Cybersecurity, Wireless Threat Analysis**

## INTRODUCTION

Wireless communication has transformed networking by eliminating physical connectivity constraints and enabling mobility across diverse environments. The proliferation of smart devices, cloud-based services, and remote working models has significantly increased dependency on wireless networks. Organizations deploy multiple access points to provide seamless connectivity across offices, campuses, and branch locations.

Despite these advantages, wireless networks face unique security challenges. Radio frequency signals extend beyond physical building boundaries, allowing external entities to intercept or inject traffic without direct network access. Attackers exploit this exposure to perform reconnaissance, impersonation, and interception attacks.

One major threat category is infrastructure-based attacks, particularly rogue access point deployment. A rogue access point is defined as any unauthorized wireless access device operating within the coverage area of an organization’s network. These devices may connect directly to internal switches or operate externally while imitating legitimate networks.

**Rogue access points can be categorized into three types:**

1. Internal rogue AP – connected directly to organizational LAN.

2. External rogue AP – operating nearby without physical LAN connection.
3. Evil twin AP – mimicking legitimate SSID to deceive users.

Attackers deploy rogue access points to capture authentication credentials, redirect traffic to malicious gateways, inject malware, or monitor encrypted sessions. In enterprise environments, a single rogue device can compromise confidential data, intellectual property, and user credentials.

Traditional network security mechanisms such as firewalls and wired intrusion detection systems focus primarily on IP-layer monitoring and fail to detect wireless infrastructure anomalies. Therefore, dedicated wireless intrusion detection mechanisms are necessary.

This research aims to design and evaluate a real-time rogue access point detection framework using passive wireless monitoring and identifier validation techniques. The system is designed to be affordable, efficient, and deployable without specialized enterprise hardware.

## I. METHODOLOGY

This research adopts an experimental and implementation-based methodology to design and evaluate a rogue access point detection framework in a wireless network environment. The methodology integrates wireless spectrum monitoring, access point identification, database verification, and intrusion detection analysis to accurately identify unauthorized wireless devices.

### A. Research Design

The study follows a structured approach consisting of system setup, data acquisition, detection processing, and performance evaluation. A controlled wireless network environment was established to simulate both authorized and rogue access points. The experimental setup allows controlled testing of detection accuracy and response time under realistic operating conditions.

**The methodology is divided into four major phases:**

1. Wireless Environment Configuration
2. Data Collection and Monitoring
3. Rogue Access Point Identification
4. Performance Evaluation

### B. Experimental Setup

The implementation environment consists of:

• Kali Linux operating system
• Wireless network adapter supporting monitor mode
• Aircrack-ng suite
• Kismet wireless detection tool
• Wireshark packet analyzer
• Authorized Access Point Database

The wireless adapter was configured in monitor mode to capture raw 802.11 frames without associating with any specific access point. This allows passive observation of all broadcasting wireless devices within range.

### C. Data Collection Process

During the monitoring phase, the system continuously scans the wireless spectrum and collects access point parameters, including:

• SSID (Service Set Identifier)
• BSSID (MAC address of the access point)
• Channel number
• Encryption type (WEP, WPA, WPA2, WPA3)
• Received Signal Strength Indicator (RSSI)

These parameters are extracted from beacon frames broadcast by wireless access points. Passive packet capturing ensures that no additional traffic is generated during monitoring, reducing detection visibility to potential attackers.

### D. Rogue Access Point Detection Mechanism

The detection process combines signature-based and rule-based verification techniques.

**Step 1: Authorized Database Verification**

The system maintains a predefined list of legitimate access points, including their MAC addresses and configuration parameters.

Captured BSSID values are compared against this authorized database.
If a detected access point is not present in the database, it is marked as suspicious.

**Step 2: SSID Duplication Analysis**
The system identifies duplicate SSIDs operating on unexpected channels or with inconsistent signal characteristics. If two access points broadcast the same SSID but have different MAC addresses or abnormal signal behavior, the system flags a potential Evil Twin attack.

**Step 3: Signal Strength Pattern Evaluation**
Signal strength trends are analyzed to identify irregular transmission patterns.
Significant deviations in RSSI values from known access points may indicate unauthorized device placement.

**Step 4: Alert Generation**
Once a rogue access point is identified, the system generates a real-time alert to the network administrator for further investigation.

**E. Performance Evaluation Metrics**
The effectiveness of the proposed detection system is evaluated using the following parameters:
• Detection Accuracy
• False Positive Rate
• False Negative Rate
• Detection Time
• System Reliability

Detection accuracy is calculated as the ratio of correctly identified rogue access points to the total number of rogue access points present during testing. False positives occur when legitimate access points are incorrectly classified as rogue, while false negatives represent undetected rogue devices.

**F. Ethical and Security Considerations**
All experiments were conducted within a controlled laboratory environment to prevent unauthorized access to external networks. The testing framework was designed solely for research and educational purposes, ensuring compliance with cybersecurity ethics and responsible disclosure principles.

## II. MODELING AND ANALYSIS

This section describes the system model, detection framework, and analytical approach used to identify rogue access points in a wireless network environment. The proposed model is based on continuous wireless monitoring, access point parameter extraction, and comparison with an authorized access point database. The system is designed to detect unauthorized wireless devices efficiently and generate alerts in real time.

**A. System Model**
The wireless network environment consists of multiple access points, client devices, and a monitoring system. Access points broadcast beacon frames containing important network parameters such as SSID, MAC address (BSSID), channel number, and security configuration. The proposed detection system captures these beacon frames using a wireless network adapter configured in monitor mode.

**The system model includes the following components:**

• Wireless Access Points (Authorized and Rogue)
• Wireless Monitoring Interface
• Packet Capture and Analysis Module
• Authorized Access Point Database
• Detection and Alert Generation Module

Authorized access points are registered in a secure database, while rogue access points represent unauthorized devices attempting to operate within the network.

**B. Detection Framework**

The detection framework is based on passive wireless monitoring and parameter analysis. The monitoring system continuously scans the wireless spectrum and collects access point information. The captured data is processed and analyzed to identify unauthorized devices.

**The detection process consists of the following steps:**

1. Wireless Signal Monitoring
2. The wireless adapter captures beacon frames transmitted by access points within the network range.
3. Parameter Extraction
4. The system extracts relevant parameters from captured packets, including:
   - SSID
   - BSSID (MAC address)
   - Channel number
   - Signal strength (RSSI)
   - Encryption type

5. Database Comparison

The extracted BSSID is compared with the authorized access point database.
If the BSSID does not match any authorized entry, the access point is classified as suspicious.

6. Rogue Access Point Identification

Access points with unknown MAC addresses or abnormal network characteristics are identified as rogue devices.

7. Alert Generation

The system generates alerts and logs the detected rogue access point for further investigation.

**C. Mathematical Model**

The rogue access point detection process can be represented using a comparison-based classification model.
Let:
A = Set of authorized access points
D = Set of detected access points
R = Set of rogue access points

Then:
$R = D - A$
This means rogue access points are those detected access points that are not present in the authorized access point database.
Detection condition:
If BSSID_detected $\notin$ BSSID_authorized
Then Access Point = Rogue
Otherwise:
Access Point = Authorized

**D. Signal Strength Analysis Model**

Signal strength analysis is used to detect abnormal access points. Each access point transmits signals with specific strength characteristics.

Let:
RSSI_expected = Expected signal strength of authorized access point
RSSI_detected = Detected signal strength

If:
$|RSSI_{detected} - RSSI_{expected}| > Threshold$
Then the access point may be considered suspicious.
This method helps detect Evil Twin attacks and unauthorized devices placed near the network.

**F. Analysis of Detection Efficiency**

The effectiveness of the detection system depends on several factors:
- Accuracy of MAC address verification
- Efficiency of packet capture process
- Reliability of authorized access point database
- Signal strength monitoring accuracy
- Real-time processing capability

The use of automated wireless monitoring tools improves detection efficiency and reduces the possibility of human error.

### G. Security Analysis

The proposed system enhances wireless network security by identifying unauthorized devices before they can perform malicious activities. It prevents attackers from exploiting rogue access points to intercept network traffic or bypass security controls.

The detection framework provides the following security benefits:
- Early detection of unauthorized access points
- Improved network visibility
- Prevention of unauthorized network access
- Enhanced protection against wireless attacks

## IV. RESULTS AND DISCUSSION

The proposed rogue access point detection system was implemented in a controlled wireless network environment using Kali Linux and wireless monitoring tools. The objective of the experiment was to evaluate the effectiveness of the system in identifying unauthorized access points and analyzing its detection performance under real-time conditions.

### A. Experimental Observations

During the experiment, the wireless monitoring system continuously scanned the surrounding wireless network and collected access point parameters such as SSID, BSSID (MAC address), channel number, encryption type, and signal strength. The system successfully detected both authorized and unauthorized access points operating within the network coverage area.

The captured access point information was compared with the authorized access point database. Any access point whose MAC address was not present in the database was classified as a rogue access point. The system generated alerts immediately after detecting unauthorized devices.

The detection system was able to identify rogue access points created using wireless hotspot devices and unauthorized routers. Additionally, the system successfully detected access points with duplicate SSIDs, indicating potential Evil Twin attack scenarios.

### B. Detection Performance Analysis

The performance of the detection system was evaluated using key performance metrics, including detection accuracy, detection time, and reliability.

#### Detection Accuracy

Detection accuracy is defined as the percentage of rogue access points correctly identified by the system.
Detection Accuracy = (Number of correctly detected rogue access points / Total rogue access points) × 100
During testing, the system detected 19 out of 20 rogue access points.

Detection Accuracy = (19 / 20) × 100 = 95%
This indicates that the system provides high detection accuracy.

#### Detection Time

Detection time refers to the time required by the system to identify a rogue access point after it becomes active.
Observed detection time ranged between:
- Minimum: 2 seconds
- Maximum: 6 seconds
- Average: 4 seconds

This demonstrates that the system provides near real-time detection capability.

#### False Positive and False Negative Analysis

False Positive: Authorized access point detected as rogue
False Negative: Rogue access point not detected

Experimental results showed:
- False Positive Rate: 5%
- False Negative Rate: 5%

These values indicate reliable detection performance.

### C. Experimental Results Table

| Parameter | Result |
|---|---|
| Detection Accuracy | 95% |
| Average Detection Time | 4 seconds |
| False Positive Rate | 5% |
| False Negative Rate | 5% |
| Real-time Detection | Yes |
| System Reliability | High |

### D. DISCUSSION

The experimental results demonstrate that the proposed wireless monitoring-based detection system is effective in identifying rogue access points in real time. The use of wireless packet capture and MAC address verification enables accurate identification of unauthorized devices.

## III. CONCLUSION

Wireless networks play a critical role in modern communication systems by providing flexible, scalable, and efficient connectivity across various organizational and public environments. However, the open and shared nature of wireless communication makes these networks highly susceptible to security threats, particularly rogue access points. Rogue access points introduce unauthorized entry points into the network, allowing attackers to intercept sensitive information, perform man-in-the-middle attacks, and bypass network security controls. Therefore, detecting and mitigating rogue access points is essential to maintain network confidentiality, integrity, and availability.

This research presented the design and implementation of a wireless monitoring-based rogue access point detection system using wireless scanning and intrusion detection techniques. The proposed system continuously monitors wireless network activity, captures access point parameters such as SSID, MAC address, channel information, and signal strength, and compares the detected devices with an authorized access point database. The implementation was carried out using Kali Linux and wireless monitoring tools, which enabled real-time detection of unauthorized access points.

The experimental results demonstrated that the proposed system effectively identified rogue access points with high detection accuracy and minimal detection delay. The system was able to detect unauthorized wireless devices, including malicious access points and duplicate SSIDs, thereby improving network visibility and security. Automated monitoring significantly enhanced detection efficiency compared to manual methods, reducing human effort and improving response time.

Although the proposed system provides reliable detection performance, certain limitations exist, such as potential evasion through MAC address spoofing and challenges in highly dynamic wireless environments. These limitations highlight the need for more advanced detection techniques.

Future enhancements may include the integration of machine learning and artificial intelligence-based detection methods to improve accuracy and adaptability. Intelligent detection systems can analyze network behavior patterns and identify advanced threats more efficiently. Additionally, integrating automated response mechanisms to isolate or block rogue access points can further strengthen wireless network security.

In conclusion, the proposed rogue access point detection system provides an effective and practical solution for identifying unauthorized wireless devices and enhancing the overall security of wireless networks. The implementation of automated detection and continuous monitoring mechanisms is essential for protecting modern wireless infrastructure from evolving cybersecurity threats.

## IV. REFERENCES

[1]. A. Mishra, V. Shrivastava, and S. Banerjee, “Partially overlapping channels not considered harmful,” *Proceedings of the ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*, pp. 63–74, 2006.

[2]. Y. Zhang and W. Lee, “Intrusion detection in wireless ad-hoc networks,” *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom)*, pp. 275–283, 2000.

[3]. N. Cam-Winget, R. Housley, D. Wagner, and J. Walker, "Security flaws in IEEE 802.11 wireless networks," *IEEE Communications Magazine*, vol. 41, no. 10, pp. 35–39, 2003.
[4]. K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," National Institute of Standards and Technology (NIST), Special Publication 800-94, 2007.
[5]. O. Abouabdalla, H. Zedan, and S. Al-Raweshidy, "Wireless intrusion detection systems: A survey and analysis," *Proceedings of the IEEE International Conference on Computer Systems and Applications (AICCSA)*, pp. 1–8, 2015.
[6]. M. S. Gast, *802.11 Wireless Networks: The Definitive Guide*, 2nd ed., O'Reilly Media, 2005.
[7]. J. Wright, "Detecting and locating rogue access points," *SANS Institute Information Security Reading Room*, 2010.
[8]. Aircrack-ng Development Team, "Aircrack-ng suite for wireless security testing," Available:
[9]. Wireshark Foundation, "Wireshark network protocol analyzer documentation," Available:
[10]. M. Raya, J. Hubaux, and I. Aad, "DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots," *IEEE Transactions on Mobile Computing*, vol. 5, no. 12, pp. 1691–1705, 2006.