# Beacon Frame Analysis for Rogue AP Detection

Akintoye Oyedola · School of Computing, University of North Florida · CNT 6519 Wireless Network Security

## Motivation & Problem Statement

Rogue access points (APs), including evil-twin devices that mimic legitimate Wi-Fi networks, allow attackers to intercept traffic or steal user credentials in enterprise WLAN environments. Detecting these attacks is difficult because malicious APs can replicate legitimate identifiers such as SSIDs and BSSIDs [3, 2]. Existing detection approaches often rely on **active probing, client monitoring, or infrastructure-based** intrusion prevention systems. These methods introduce additional overhead costs or privacy concerns [1]. I investigate whether passive beacon-frame and probe-response analysis alone, using structural and signal features from 802.11 management frames, can reliably detect rogue APs with low false-positive rates in realistic wireless environments [6].

## System Design

A passive rogue AP detection pipeline analyzes IEEE 802.11 management frames captured from a wireless monitoring interface, enabling continuous background monitoring without active probing:

1. **Beacon Capture Layer**: A monitor-mode Wi-Fi adapter (Qualcomm Atheros AR9271) captures raw 802.11 management frames across 8 labeled sessions using `airodump-ng`, generating PCAP traces totaling 6,607 packets across sessions S1–S8.
2. **Feature Extraction Layer**: Python 3 scripts using **Scapy** parse raw frame control bytes to extract structural and signal features including SSID/BSSID consistency, sequence number deltas, inter-frame timing, and RSSI statistics [2].
3. **Detection Engine**: Rule-based anomaly detection (SSID/BSSID mismatch, RSSI range threshold, hidden SSID flag) and supervised machine learning classifiers implemented in **Scikit-learn** [3].
4. **Analysis and Output Layer**: Classification metrics including detection rate, false alarm rate, precision, recall, and ROC curves assess system performance [6].

The experimental pipeline, from hardware capture to machine learning evaluation, is illustrated in Fig 1

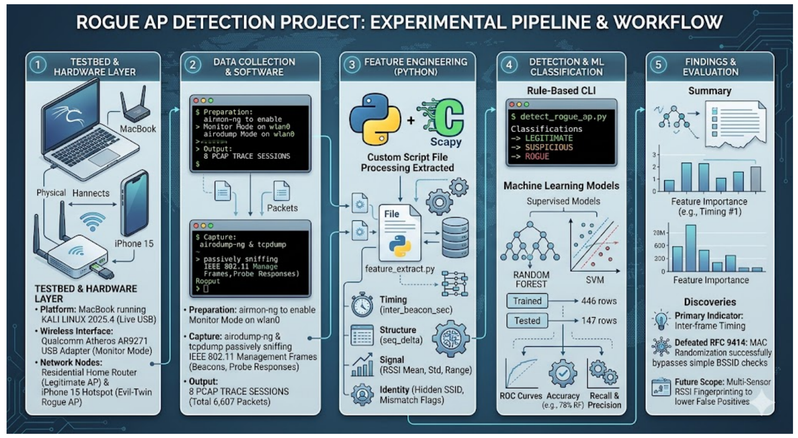



***Fig. 1.*** *This visualization illustrates the workflow from hardware capture (Kali Linux/Atheros AR9271) to machine learning classification (Random Forest/SVM). Image generated by Gemini 3 Flash based on author's experimental data [4]. Graphic generated by Google Gemini, [March 25, 2026], https://gemini.google.com/ .*

## Key Technologies & Components

**Wireless Packet Capture**

- **airodump-ng**: Captures IEEE 802.11 management frames in monitor mode across wireless channels.
- **tcpdump**: Records raw PCAP traces for offline analysis.

**Packet Analysis & Feature Extraction**

- **Scapy**: Parses management frames via raw frame control byte inspection; extracts BSSID, SSID, sequence number, RSSI, and inter-frame timing.
- **Wireshark**: Validates captured packets and verifies frame structure.

**Data Processing**

- **Python 3.13**: Primary language for packet parsing and feature automation.
- **Pandas**: Organizes extracted features into structured labeled datasets.

**Detection Models**

- **Scikit-learn**: Implements Random Forest and SVM classifiers with `class_weight='balanced'`.
- **Rule-Based Detection**: Flags SSID/BSSID mismatches, RSSI anomalies, and hidden SSIDs.

**Evaluation Metrics**

- Accuracy, Precision, Recall, F1-score
- False Positive Rate (FPR)
- ROC Curve and AUC
- Confusion Matrix

## Data Collection & Implementation

| Session | Condition | Frames | Label | Role |
|---|---|---|---|---|
| S1 | Legitimate-only baseline | 207 | 0 | Training |
| S2 | Evil-twin, different channel | 62 | 1 | Training |
| S4 | Legitimate-only, different time | 192 | 0 | Training |
| S5 | Evil-twin, distance variation | 287 | 1 | Training |
| S6 | SSID-cloaked legitimate AP | 182 | −1 | Qualitative |
| S7 | Legitimate-only repeat | 218 | 0 | Test |
| S8 | Evil-twin repeat | 121 | 1 | Test |

*Experimental session matrix: capture conditions, frame counts, labels, and roles for evil-twin AP detection.*

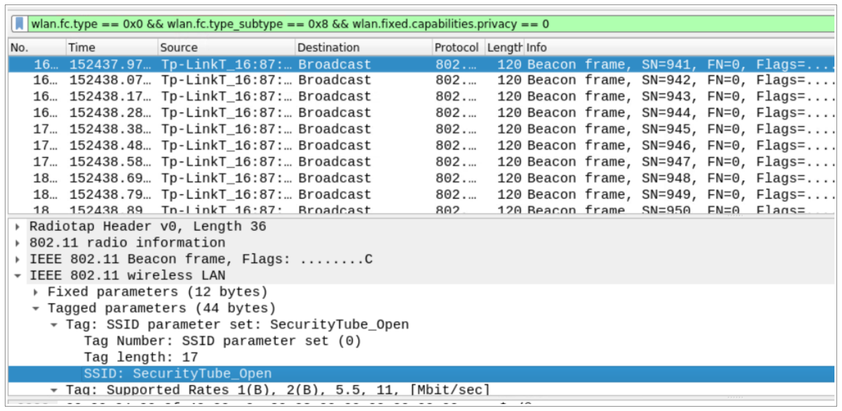



***Fig. 2.*** *Sample IEEE 802.11 beacon frame from Wireshark with management frame fields. [5]*

### Experiment Setup

1. 8 labeled capture sessions conducted across 2 sittings on different days using a Kali Linux live environment with a monitor-mode USB Wi-Fi adapter.
2. Sessions ran 10 minutes each; raw PCAP files totaled 1.4–2.1 MB per session across 6,607 total packets.
3. Dataset included frames from a legitimate home router (BSSID `54:4e:67:34:56:4d`) and an iPhone 15 Personal Hotspot configured as an evil-twin AP with identical SSID (`ATTNg4VMGJ`).
4. 593 labeled management frames extracted after filtering to known BSSIDs: 123 legitimate (label 0), 470 rogue (label 1), 182 cloaked (label −1, qualitative only).
5. Extracted features fed into Scikit-learn Random Forest and SVM classifiers with session-stratified train/test split.

## Key Findings

- **593 labeled frames** extracted across 7 sessions from 2 capture sittings on different days.
- **SSID cloaking** (S6) eliminated SSID-based detection entirely, forcing reliance on RSSI and timing features alone [3].
- **False positive rate** on legitimate frames exceeded the 5% target from Zhang et al. [6], due to class imbalance and single-device legitimate AP dataset.

## Performance Results

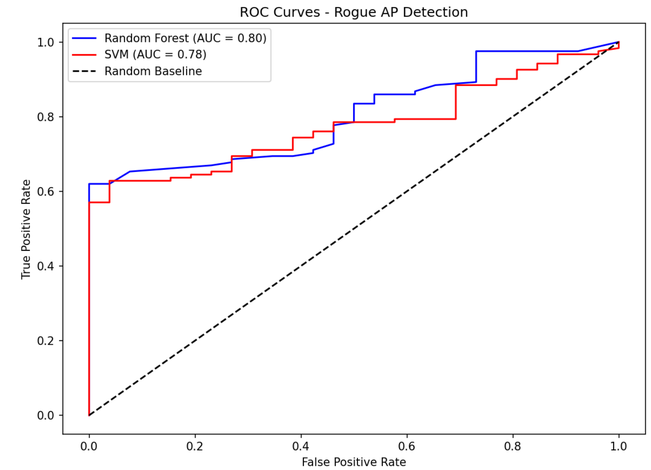
### Classifier Comparison (Held-Out Test Set: S7, S8)

| Classifier | Class | Precision | Recall | F1 |
|---|---|---|---|---|
| Random Forest | Legitimate | 0.39 | 0.50 | 0.44 |
| | Rogue | 0.89 | 0.83 | 0.86 |
| | *Accuracy* | | *0.78* | |
| SVM | Legitimate | 0.26 | 1.00 | 0.42 |
| | Rogue | 1.00 | 0.48 | 0.57 |
| | *Accuracy* | | *0.50* | |

## Performance Results

### Random Forest Feature Importance

| Feature | Importance |
|---|---|
| inter_beacon_sec | 0.8316 |
| seq_num | 0.1649 |
| ssid_bssid_mismatch | 0.0001 |
| rssi_mean, rssi_std, rssi_range | ≈0.0000 |




*ROC curves for Random Forest and SVM on held-out test set (S7, S8). Random Forest achieves higher AUC, reflecting stronger discrimination between legitimate and rogue AP frames.*

## Conclusions

- The **Random Forest classifier** achieved **83% recall** on the rogue class and **78% overall accuracy**, outperforming the SVM on all rogue-detection metrics.
- **Inter-frame timing** (importance: 0.83) was the dominant discriminating feature, reflecting structural differences between periodic router beacons and reactive iPhone probe responses.
- **MAC address randomization** (RFC 9414 [7]) defeated the SSID/BSSID mismatch rule: the iPhone hotspot's randomized BSSID prevented evil-twin flagging in both the rule-based script and the ML feature vector.
- **SSID cloaking** (S6) eliminated SSID-based detection entirely, consistent with Liu et al. [3], forcing reliance on RSSI and timing features alone.
- **False positive rate** on the legitimate class (≈50%) exceeded the 5% target from Zhang et al. [6], driven by class imbalance and single-device legitimate AP diversity.
- Future work should incorporate **multi-sensor RSSI fingerprinting**, beacon-focused (not probe-response-dominated) captures, and larger datasets with diverse rogue AP hardware to improve generalization.

## References

[1] B. Da, Z. Zhang, and X. Wang. "Rogue access point detection: A survey". In: *IEEE Communications Surveys & Tutorials* 23.1 (2021), pp. 245–268. DOI: 10.1109/COMST.2020.3040256. URL: https://doi.org/10.1109/COMST.2020.3040256.

[2] J. Lin, J. Wang, and T. Xu. "Detecting rogue access points via beacon frame analysis and machine learning". In: *IEEE Transactions on Network and Service Management* 19.3 (Sept. 2022), pp. 2105–2118. DOI: 10.1109/TNSM.2022.3164421. URL: https://doi.org/10.1109/TNSM.2022.3164421.

[3] H. Liu, S. Chen, and M. Zhou. "Position-based rogue AP detection using spatial signal properties". In: *Journal of Network and Computer Applications* 221 (Jan. 2024), p. 103784. DOI: 10.1016/j.jnca.2023.103784. URL: https://doi.org/10.1016/j.jnca.2023.103784.

[4] Akintoye Oyedola. *Rogue AP Detection Project: Experimental Pipeline & Workflow.* [Infographic]. Generated by Gemini 3 Flash based on data from *Wireless Network Security: Beacon Frame Analysis for Passive Rogue Access Point Detection.* University of North Florida, School of Computing. Mar. 2026.

[5] Andrew Walding. *Capturing wi-fi beacon frames with WinFi.* Sept. 2025. URL: https://www.cellstream.com/2025/06/30/capturing-wi-fi-beacon-frames-with-winfi/?utm_source=chatgpt.com.

[6] L. Zhang, Y. Yang, and C. Wang. "PRAPD: Passive rogue access point detection using RSSI fingerprinting". In: *Proc. IEEE Global Communications Conference (GLOBECOM).* 2018, pp. 1–7. DOI: 10.1109/GLOCOM.2018.8647145. URL: https://doi.org/10.1109/GLOCOM.2018.8647145.

[7] J. C. Zúñiga, C. J. Bernardos, and A. Andersdotter. *Privacy considerations for IEEE 802.11 operating procedures.* Request for Comments 9414. IETF, Jan. 2023. URL: https://www.rfc-editor.org/rfc/rfc9414.html.