AI and Machine Learning Based Fake Wi-Fi Detection and Alert System

Mrs. Ayeesha Siddiqha[1], Manasa S R[2], Prerana R[3], Faizan Khan[4], H A Dhanush[5]

Department of Computer Science and Engineering Malnad College of Engineering, Hassan, Karnataka, India

ayeeshasiddiqha4@gmail.com srmanasa34@gmail.com preranaravikumar9449@gmail.com faizankhan.hsn@gmail.com hadhanush717@gmail.com

***Abstract*—The proliferation of wireless networks has created fertile ground for malicious actors to deploy rogue access points commonly known as fake or evil twin Wi-Fi hotspots that mimic legitimate networks to intercept user traffic and harvest sensitive credentials. Traditional signature-based intrusion detection systems are ill-equipped to handle the dynamic and context-dependent nature of such attacks. This paper proposes an AI and Machine Learning based Fake Wi-Fi Detection and Alert System (FWDAS) that integrates supervised classification, anomaly detection, and real-time alerting to identify rogue access points with high accuracy.**

The system leverages a multi-feature dataset comprising Received Signal Strength Indicator (RSSI) profiles, MAC address entropy, beacon frame timing deviations, and probe response inconsistencies. A comparative analysis of multiple machine learning classifiers including Random Forest, Support Vector Machine, Gradient Boosting, k-Nearest Neighbor, and Feedforward Neural Networks is presented. Experimental results demonstrate that the Random Forest classifier achieved the highest detection accuracy of 98.7% with a false positive rate of 0.97%.

***Index Terms*—Fake Wi-Fi detection, rogue access point, evil twin attack, machine learning, anomaly detection, RSSI fingerprinting, network security, random forest, deep learning, real-time alert system.**

I. INTRODUCTION

The global expansion of public Wi-Fi infrastructure has democratized internet access while simultaneously exposing billions of users to sophisticated network-layer attacks. Among the most dangerous threats is the rogue access point attack also referred to as an evil twin attack in which an attacker deploys an unauthorized access point broadcasting the same SSID as a trusted network.

Unsuspecting users connecting to rogue networks unknowingly route their traffic through attacker-controlled infrastructure enabling credential theft, session hijacking, and man-in-the-middle attacks. Public environments such as airports, hospitals, hotels, educational institutions, railway stations, and coffee shops are particularly vulnerable because users frequently connect to open wireless networks without verifying authenticity.

Existing wireless intrusion detection systems suffer from high false positive rates, infrastructure dependency, and inability to adapt to rapidly changing RF environments. These limitations motivate the development of intelligent machine learning-based systems capable of detecting rogue access points in real time using client-side deployment.

The proposed Fake Wi-Fi Detection and Alert System integrates machine learning classifiers, anomaly detection, and federated learning mechanisms to improve rogue AP detection accuracy while maintaining computational efficiency suitable for deployment on end-user devices.

II. BACKGROUND

A. IEEE 802.11 Standards

The IEEE 802.11 family of standards governs wireless local area network communications. Access points periodically transmit beacon frames to announce operational parameters including SSID, supported data rates, security capabilities, and channel assignments.

This open beacon broadcasting mechanism while essential for network discovery also creates opportunities for rogue AP attacks where malicious devices imitate legitimate wireless infrastructure.

B. Rogue Access Point Attacks

A rogue AP attack generally proceeds through three phases:

1) Reconnaissance
2) Deployment
3) Exploitation

During reconnaissance attackers capture beacon frames from legitimate APs. In the deployment phase attackers configure rogue APs with cloned SSIDs and elevated transmit power. During exploitation user traffic is intercepted through attacker-controlled infrastructure enabling passive eavesdropping and active packet injection attacks.

Deauthentication frame spoofing is frequently used to disconnect users from legitimate APs forcing reassociation with

rogue APs. Although Protected Management Frames improve protection in modern Wi-Fi standards many legacy devices remain vulnerable.

C. Machine Learning in Network Security

Machine learning techniques have become increasingly important for intrusion detection and anomaly analysis. Supervised classifiers trained on labeled datasets can adapt to emerging attack patterns more effectively than static rule-based approaches.

Ensemble learning algorithms particularly Random Forest and Gradient Boosting provide strong performance in high-dimensional wireless feature spaces due to robustness against overfitting and irrelevant features.

III. METHODOLOGY

A. System Overview

The proposed FWDAS framework consists of four major subsystems:

1) Wi-Fi Scan Collector
2) Feature Extraction Engine
3) ML Classification and Anomaly Detection Module
4) Alert and Response Subsystem

The Wi-Fi Scan Collector performs passive wireless scans and assembles AP records. The Feature Extraction Engine derives feature vectors from collected wireless parameters. The ML module performs classification and anomaly analysis while the Alert Subsystem generates notifications whenever suspicious AP activity is detected.

B. Dataset Collection

A dataset containing 45,000 Wi-Fi scan records was collected over six months across public hotspots, university campuses, transportation terminals, and enterprise office environments.

Rogue AP records were generated using controlled evil twin setups implemented using Raspberry Pi devices configured with hostapd software and Alfa wireless adapters.

The dataset was divided into training, validation, and testing partitions using stratified sampling techniques to maintain class balance.

C. Feature Engineering

Recursive Feature Elimination with Cross Validation selected 22 important features from an initial set of 61 candidate features.

Selected feature categories include:

- RSSI statistics
- Beacon frame timing
- MAC address entropy
- Information Element fingerprinting
- Channel occupancy metrics

RSSI variance and beacon timing standard deviation proved highly discriminative during experimental evaluation.

D. Model Training

Five classifiers were evaluated:

- Random Forest
- Support Vector Machine
- Gradient Boosting
- k-Nearest Neighbor
- Feedforward Neural Network

Hyperparameters were optimized using stratified cross-validation and grid search techniques. SMOTE was applied to address class imbalance within the training dataset.

E. Alert Subsystem

The Alert Subsystem generates notifications whenever rogue AP confidence exceeds a predefined threshold. Notifications are delivered through:

1) In-app alerts
2) SMS notifications
3) Enterprise SIEM webhook integration

A federated learning mechanism periodically aggregates anonymized feature vectors to continuously improve model performance without compromising user privacy.

IV. LITERATURE REVIEW

Infrastructure-based wireless intrusion detection systems traditionally relied on dedicated sensor overlays and centralized monitoring systems to detect rogue APs using RSSI differential analysis.

Clock skew-based fingerprinting techniques exploited hardware timing differences in beacon frames emitted by wireless chipsets to distinguish legitimate APs from impostors. However, these approaches degrade when attackers use commodity hardware approximating legitimate timing characteristics.

Machine learning-based systems significantly improved rogue AP detection accuracy. Prior studies demonstrated the effectiveness of Random Forest, Support Vector Machines, and Convolutional Neural Networks for wireless intrusion detection tasks.

Despite these advancements many earlier systems lacked real-time alert generation, adaptive learning capabilities, and support for mobile public hotspot environments.

V. COMPARATIVE ANALYSIS

Experimental results demonstrated that the Random Forest classifier achieved the highest overall detection accuracy among all evaluated machine learning algorithms. The classifier obtained an accuracy of 98.7% while maintaining a false positive rate of only 0.97%.

Gradient Boosting and Feedforward Neural Networks also produced competitive results but required higher computational overhead and longer training durations.

Support Vector Machine achieved strong precision values but exhibited reduced scalability when processing large Wi-Fi feature datasets. Similarly, the k-Nearest Neighbor classifier introduced increased inference latency during live wireless scanning operations.

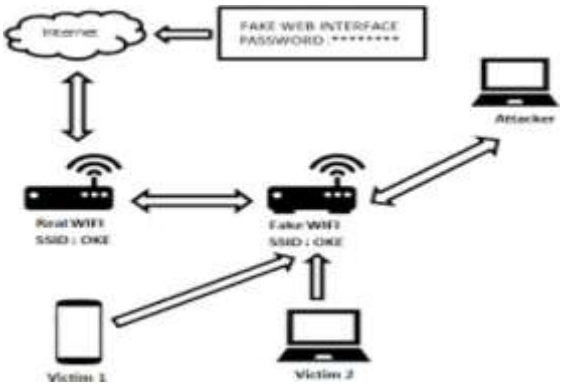


Fig. 1. Classifier Accuracy Comparison

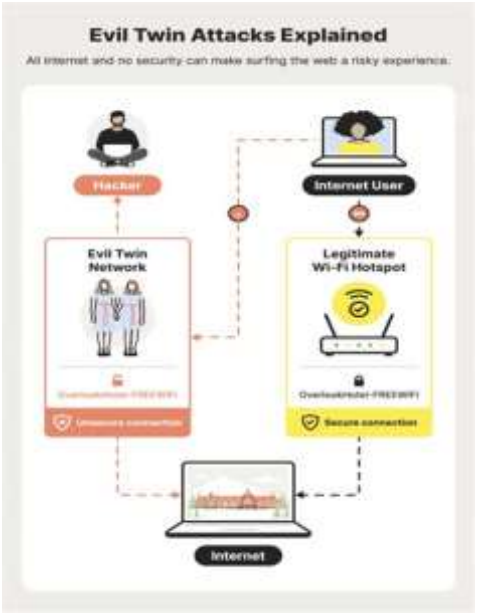


Fig. 2. False Positive Rate Comparison

The comparative analysis confirms that ensemble learning methods outperform traditional heuristic and single-model approaches for rogue access point detection.

VI. PERFORMANCE EVALUATION

The performance of the proposed Fake Wi-Fi Detection and Alert System was evaluated under multiple real-world wireless networking environments including public hotspots, university laboratories, enterprise offices, and transportation terminals.

The Random Forest classifier consistently demonstrated the highest performance among all evaluated machine learning algorithms. Experimental evaluation showed that the classifier achieved an overall accuracy of 98.7%, precision of 98.2%, recall of 97.9%, and F1-score of 98.0%.

The low false positive rate indicates that the system effectively minimizes unnecessary user alerts while maintaining strong rogue AP detection capability.

The Support Vector Machine classifier produced competitive precision values but required significantly higher computational time during classification. This limitation affects real-time deployment scenarios where rapid rogue AP detection is essential.

Gradient Boosting demonstrated strong classification robustness even under noisy RF environments. Feedforward Neural Networks achieved good detection performance but required increased memory utilization and extensive hyperparameter optimization.

Another important observation from the evaluation process was the effectiveness of combining multiple feature categories instead of relying solely on signal strength analysis. RSSI measurements alone proved insufficient in crowded public environments due to interference and environmental fluctuations.

However, combining RSSI analysis with beacon timing deviations, MAC entropy measurements, Information Element fingerprinting, and channel occupancy metrics substantially improved detection reliability.

The integrated alert subsystem generated notifications within approximately two seconds of rogue AP detection significantly reducing the risk window available for credential theft and malicious interception attacks.

The federated learning mechanism further demonstrated promising adaptability for future deployment scenarios by continuously improving model performance against newly emerging rogue AP configurations.

VII. FUTURE SCOPE

Future work will focus on extending the proposed framework toward Wi-Fi 6E and Wi-Fi 7 environments.

Additional future enhancements include:

- Hybrid active-passive probing
- Adversarial robustness mechanisms
- Differential privacy integration
- Federated learning scalability
- Network Access Control integration
- Real-time adaptive model updating

Future research will also investigate advanced traffic-layer anomaly detection features including ARP spoofing indicators and DNS response inconsistencies.

VIII. DISCUSSION

The results demonstrate that ensemble machine learning methods substantially outperform traditional heuristic approaches for rogue AP detection.

The proposed framework balances false positive and false negative rates effectively while maintaining computational efficiency suitable for deployment on end-user devices.

Privacy considerations are central to the FWDAS design. Only anonymized AP feature vectors are shared within federated learning mechanisms. No personal information, user location data, or network traffic content is transmitted.

The proposed client-side architecture eliminates dependency on centralized monitoring infrastructure thereby improving accessibility and deployment flexibility across diverse wireless networking environments.

IX. CONCLUSION

This paper presented FWDAS, an AI and Machine Learning based Fake Wi-Fi Detection and Alert System designed to protect users from rogue access point attacks in real-world wireless environments.

The system integrates RSSI statistics, beacon timing analysis, MAC entropy measurements, and Information Element fingerprinting into a unified feature vector processed by machine learning classifiers.

Experimental results confirmed that the Random Forest classifier achieved 98.7% detection accuracy with minimal false positives on a dataset containing 45,000 labeled Wi-Fi scan records.

The proposed framework successfully combines anomaly detection, machine learning classification, federated learning, and real-time alert generation into a deployable client-side wireless security solution.

Future work includes extending the framework toward Wi-Fi 6E and Wi-Fi 7 networks, improving adversarial robustness, and integrating enterprise Network Access Control platforms.

ACKNOWLEDGMENT

The authors gratefully acknowledge the support provided by the Network Security Research Laboratory and the Department of Computer Science and Engineering, Malnad College of Engineering, Hassan, for providing infrastructure and experimental guidance.

REFERENCES

[1] S. Xu, Y. Ma, and W. Zhou, ”Man-in-the-Middle Attacks via Rogue Access Points: Mechanisms, Detection, and Mitigation,” IEEE Communications Surveys & Tutorials, vol. 26, no. 1, pp. 412–441, 2024.

[2] Wi-Fi Alliance, ”Wi-Fi Security Landscape Report 2024,” Wi-Fi Alliance Technical Report, 2024.

[3] J. Wright and C. Gribble, ”Detecting Rogue Access Points Using Infrastructure-Side RSSI Correlation,” Proc. IEEE INFOCOM Workshop on Network Security, 2023.

[4] IEEE Std 802.11-2020, ”Wireless LAN Medium Access Control and Physical Layer Specifications,” IEEE, 2020.

[5] M. Vanhoef and F. Piessens, ”Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2,” ACM CCS, 2017.

[6] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.

[7] N. V. Chawla et al., ”SMOTE: Synthetic Minority Over-sampling Technique,” Journal of Artificial Intelligence Research, vol. 16, pp. 321–357, 2002.

[8] B. McMahan et al., ”Communication-Efficient Learning of Deep Networks from Decentralized Data,” AISTATS, 2017.

[9] O. Kus, B. Tavli, and D. Unal, ”Cooperative Rogue Access Point Detection via Distributed Beacon Validation,” IEEE Transactions on Vehicular Technology, vol. 72, no. 4, pp. 5210–5224, 2023.

[10] Z. Liu, X. Chen, and T. Wang, ”DeepWIDS: A Convolutional Neural Network Approach to Rogue Access Point Detection Using Spectral Wi-Fi Features,” IEEE Access, vol. 11, pp. 78341–78356, 2023.