BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

Fake Wi-Fi (Evil Twin) Detection Using Machine Learning: A Review and a Random Forest-Based Detection Framework

[1]Aditya Mahendra Salve, [2]Prof. Varsha Babar

[1]Student, Dept. of Artificial Intelligence and Data Science Engineering
[2]Faculty Guide
[1]Ajeenkya DY Patil School of Engineering, Pune, India

Abstract

Public Wi-Fi hotspots, although convenient, compromise the privacy and security of the users since attackers can launch Evil Twin attacks by deploying rogue access points that mimic the legitimate ones and lure devices to connect to them. Checking a single parameter such as the network name or signal strength is insufficient to detect such fake access points since attackers can spoof these values. The paper evaluates the latest machine learning algorithms for rogue access point detection, compares their approaches and shortcomings, and identifies research gaps. Based on the review, the paper proposes a client-side approach that employs the Random Forest algorithm and a set of parameters including SSID, BSSID, RSSI, channel, security, MAC address, and response mask to classify access points as legitimate or malicious and alert the user before connecting. Finally, the paper presents a proposal for evaluation using accuracy, precision, recall, F1-score, and false-positive rate, reports the results from the reviewed articles, but does not perform any experiments.

Keywords: Evil Twin attack, fake hotspot, rogue access point, wireless network security, machine learning, random forest, RSSI, anomaly detection.

I. Introduction

Wireless local area networks (WLAN) are becoming ubiquitous in today's world. They are everywhere from airports and hotels to coffee shops, campuses, railway stations and shopping malls. At the same time, most of us are not aware of the possible security threats when using such networks. WLANs, in particular, are vulnerable to the so-called Evil Twin attacks where an attacker uses an access point (AP) with the same name as the legitimate AP to lure innocent users and read their data [1], [2]. Once a user connects to the attacker's AP, all their traffic passes through it giving the intruder an opportunity to perform eavesdropping, phishing, redirection, or capture the credentials of the user [1], [3].

The threat of unauthorized access is growing every day as more and more smartphones, personal computers and IoT devices are using shared networks. Moreover, the trend to make financial transactions via mobile devices or the cloud is gaining speed. It is therefore of paramount importance to make networks safe. Network security solutions based on conventional firewalls are no longer sufficient, and new approaches such as learning-based intrusion detection systems [1] and zero-trust networks, are now being explored.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

It goes without saying that checking the characteristics of a network manually is not an option. First of all, most of them can be imitated by attackers. For instance, the Service Set Identifier (SSID) which is essentially the network name can be easily spoofed. On the other hand, Received Signal Strength Indicator (RSSI) is greatly affected by the distance between the client and the AP and the surrounding topology and cannot be used for reliable detection [2], [4]. Most researchers agree that using a single characteristic for Evil Twin detection is not advisable [2], [4]. Instead, one should consider a combination of attributes and train a classifier to recognize APs based on the features it extracts. Many researchers have used K-Nearest Neighbor, Decision Tree, Support Vector Machine, Logistic Regression, and Random Forest classifiers to tackle the problem [2], [5], [6].

The current paper focuses on the use of ML algorithms for Evil Twin detection. In particular, it aims to

- provide an overview of recent research,
- identify areas for improvements,
- and propose a client-side detection framework based on the Random Forest algorithm.

This article is structured as follows: Section II describes the target security attack and the features that can be used for detection purposes. Section III reviews the related work done in this area while Section IV highlights the gap in the research. The following section presents the proposed framework, while Section VI describes the evaluation and verification process. Finally, Section VII concludes the paper and identifies areas for future research.

II. Background

A. Evil Twin Attack

In an Evil Twin attack the adversary configures an AP to impersonate a legitimate one. Since most client devices pick networks by name and signal strength, a counterfeit AP that is nearer to the victim, or louder, may attract the connection. Once associated, the victim's traffic can be observed or manipulated. The attack relies on user trust in familiar names, and thus is successful even when the genuine network is itself well configured [1].

B. Observable Access Point Features

An AP can be characterized through several parameters that can be observed by a client summarized in Table I. The SSID is the visible name of the network while the Basic Service Set Identifier (BSSID) identifying the specific AP. The Received Signal Strength Indicator (RSSI), the operating channel, the encryption type and security configuration, the MAC address, the response time and the packet behavior provide additional evidence if an AP matches the expected profile of the real network [2], [4].

Table I: Access Point Features Considered for Classification

Feature	Role in detection
SSID	Visible name; easy to copy, so weak on its own
BSSID / MAC	Identifies the AP hardware; mismatches with known APs are suspicious
RSSI	Signal pattern; affected by the environment

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

Feature	Role in detection
Channel	Operating frequency; shared by many APs
Security settings	Encryption and authentication type
Response behaviour	Timing and packet behaviour of the AP

C. Limits of Individual Parameters

Each parameter has its disadvantages. An attacker can copy the SSID, the strength of the signal depends on the environment, several APs in the same territory can share the same channel. Instead of a reliable detector, a number of different features should be implemented that would function simultaneously, making it impossible to use just one. [2], [4].

III. Related Work

Early analyses revealed that identifiers like SSID, BSSID and IP-related information can be falsified by an attacker, so identifier-based checks can be bypassed. Protocol-level approaches were explored. Selvarathinam et al. used discrete event systems over IEEE 802.11 behaviour to identify rogue APs with low computational cost, although their method is not ML-based [7]. Kolias et al. contributed the AWID public dataset for 802.11 intrusion research, which later work has used to train and test classifiers [8].

Lightweight ML for end users was examined by Harsha et al., who demonstrated that ML can improve Wi-Fi security even with limited resources, albeit their evaluation was small and did not compare against newer models [9]. Asaduzzaman et al. classified Wi-Fi frames with a J48 decision tree and feature selection and achieved approximately 91% accuracy using frame-level features, although they assessed it offline only [10].

Signal-based methods have utilised KNN. Banakh et al. demonstrated that signal characteristics, together with triangulation, can separate legitimate from Evil Twin APs, although signal strength depends on the physical environment [4]. A later data-mining study by the same group applied KNN to collected wireless data; its datasets may not represent every real-world setting [1].

Dataset-driven work has compared several classifiers. Nanayakkara et al. used feature selection on AWID2 with Random Forest, KNN and Naive Bayes and reported 99.9186% accuracy for Random Forest, although results depend on the dataset and chosen features [2]. Akparibo and Bankas evaluated Random Forest, Logistic Regression and Decision Tree on AWID3 and added a real-time monitoring interface, although evaluation was tied to one intrusion dataset [5]. Kamble and Kshirsagar combined Gini index-based feature selection with Random Forest, which demonstrates the value of reducing features, although large wireless datasets raise processing needs [6]. Kumar et al. proposed a real-time framework using Random Forest, SVM and deep learning for detection and mitigation and noted that more validation across environments is needed [11]. Augustyniak et al. compared ML algorithms for WLAN protection and stressed the need for lightweight models for resource-constrained devices [12].

Several works target deployment. EvilSpot detects and mitigates suspicious APs across multiple channels, but at the network level rather than by ML classification [13]. Mwinuka et al. built an Android client-side detector for hotspot spoofing, whose performance depends on information the device exposes [3]. Hsu et

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

al. proposed active user-side detection from packet-forwarding behaviour that requires no additional infrastructure, but depends on observable forwarding behaviour [14]. Table II summarises these studies.

Table II: Summary of Reviewed Studies

Study	Method	Key finding	Limitation
Selvarathinam et al. 2019 [7]	Discrete event systems on 802.11 behaviour	Low-overhead rogue AP detection	Protocol-level, not ML-based
Harsha et al. 2019 [9]	Lightweight ML application	ML can improve security with limited resources	Small evaluation; few model comparisons
Asaduzzaman et al. 2020 [10]	J48 tree on Wi-Fi frames	About 91% accuracy	Offline evaluation only
Banakh et al. 2023 [4]	KNN on signal data with triangulation	Signal patterns separate legitimate and rogue APs	Environment-dependent signal
Kamble and Kshirsagar 2023 [6]	Random Forest with Gini-based feature selection	Feature selection helps intrusion detection	Heavy processing on large data
EvilSpot 2023 [13]	Multi-channel detection and mitigation	Handles several channels	Network-level, not ML
Mwinuka et al. 2022 [3]	Android client-side detector	Detects hotspot spoofing on device	Depends on device information
Hsu et al. 2022 [14]	Packet-forwarding behaviour	Works without extra infrastructure	Needs observable forwarding
Banakh et al. 2024 [1]	Data mining with KNN	Identifies Evil Twin from Wi-Fi traits	Controlled data may not generalise
Nanayakkara et al. 2024 [2]	RF, KNN, Naive Bayes; AWID2	99.9186% accuracy with Random Forest	Dataset- and feature-dependent
Akparibo and Bankas 2025 [5]	RF, LR, DT; AWID3	Real-time monitoring interface	Single dataset
Kumar et al. 2025 [11]	RF, SVM, deep learning framework	Real-time detection and mitigation	Needs wider validation
Augustyniak et al. 2025 [12]	Comparison of ML for WLAN	Compares recent ML approaches	Need for lightweight models

IV. Research Gap

The review presented several open problems.

1) many approaches are built upon a single feature, e.g., the signal strength or response time, which can be easily spoofed by advanced attacks

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

2) many of models were evaluated on curated/controlled sets only and have not been tested on the noisy public Wi-Fi

3) some approaches make use of require a specialized hardware, such as multiple sensors, that are not available to an average user

4) solutions that provide the lightweight real-time eavesdropping of the user's own device are rarely found since most of the study focuses on the administration-side inspection of traffic

5) there is a lack of research that combines multiple features or models for better attack identification with a balanced false positive rate for practical application. use.

V. Proposed Framework

The framework addresses these gaps with a client-side classifier that fuses several features. Fig. 1 shows the workflow.

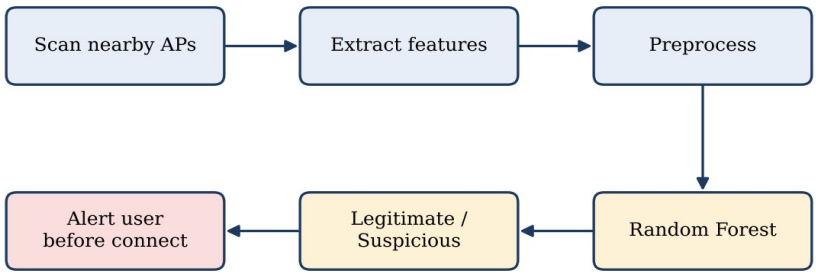


Fig. 1. Workflow of the proposed Evil Twin detection framework.

A. Data and Features

Labelled observations of legitimate and malicious APs are required. Public wireless intrusion datasets such as AWID2 and AWID3 have been used in previous work [2], [5], [8], and locally captured scans can complement them to approximate real public Wi-Fi conditions. Each observation has the features of Table I: SSID, BSSID, RSSI, channel, security settings, MAC address and response behaviour.

B. Pre-processing and Feature Selection

Records with missing values are handled, categorical fields such as security type are encoded and numeric fields are scaled where needed. Selection of useful features, for instance using Gini importance, filters uninformative attributes and reduces computation, which aids on a user's device [6].

C. Random Forest Classifier

The random forest algorithm creates many decision trees. Each tree is trained on a random subset of data and features and then the trees' votes are aggregated into one label [2], [6]. The algorithm was selected for its ability to work with multiple mixed features and the proven accuracy in the previous studies. The final prediction is

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

$$\hat{y} = \text{mode}\{h_1(x), h_2(x), \ldots, h_T(x)\} \quad (1)$$

where $\hat{y} \in \{\text{legitimate, suspicious}\}$.

D. Real-Time Alerting

After being trained, the model can be stored and utilized to score newly discovered APs, as the device scans. If an AP is marked as suspicious, the user is warned before connecting. Because signal and traffic conditions change, the design allows for retraining at periodic intervals and the addition of new features [3], [14].

VI. Evaluation Plan

Performance will be judged with a confusion matrix whose entries are true positives (TP), false positives (FP), true negatives (TN) and false negatives (FN), where a malicious AP is the positive class. The following measures will be computed:

$$\text{Accuracy} = (TP + TN) / (TP + TN + FP + FN) \quad (2)$$

$$\text{Precision} = TP / (TP + FP) \quad (3)$$

$$\text{Recall} = TP / (TP + FN) \quad (4)$$

$$F1 = 2 \cdot \text{Precision} \cdot \text{Recall} / (\text{Precision} + \text{Recall}) \quad (5)$$

$$FPR = FP / (FP + TN) \quad (6)$$

The false positive rate is underlined because several false alarms on the users' side suggest ignoring alerts. The comparison will be made with methods such as KNN, Decision Tree, SVM, Logistic Regression on the same splits. To close the gap with controlled data, the tests will comprise captures from public noisy environments, and the results of a dataset used for training will be checked on data from another environment. As this paper does not report any experiments, no performance indicators are claimed for the proposed solution.

VII. Conclusion and Future Work

Evil Twin attacks remain a threat to public Wi-Fi because of the possibility that an intruder pretends to be an authorized node and the variance of radio conditions. The articles reviewed for this study establish that ML, and specifically Random Forest, can differentiate between legitimate and rogue APs. However, the contributions were limited to using one distinguishing feature, working in controlled settings, requiring specialized hardware, or relying on administrative supervision. The project proposed a client-side Random Forest approach that uses multiple features and warns the user before establishing a connection and described an evaluation plan that focuses on accuracy and false-positive rate.

The next steps in the research would be to gather a data set, engineer features and train a model, monitor results, use more features, refine the selection, implement the solution on a mobile platform, and test it in varied conditions.

References

[1] R. Banakh, E. Nyemkova, C. Justice, A. Piskozub, and Y. Lakh, "Data mining approach for Evil Twin attack identification in Wi-Fi networks," *Data*, vol. 9, no. 10, p. 119, 2024, doi: 10.3390/data9100119.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

[2] J. D. A. S. K. Nanayakkara, M. M. P. R. M. Bandara, M. S. Mawjood, R. A. P. M. Perera, K. Yapa, and D. Siriwardana, "Enhanced detection of Evil Twin attacks in public Wi-Fi networks using machine learning algorithms," in *Proc. 9th Int. Conf. Information Technology Research (ICITR)*, 2024.

[3] L. J. Mwinuka, A. Z. Agghey, S. F. Kaijage, and J. D. Ndibwile, "FakeAP Detector: An Android-based client-side application for detecting Wi-Fi hotspot spoofing," *IEEE Access*, vol. 10, pp. 13611–13623, 2022, doi: 10.1109/ACCESS.2022.3146802.

[4] R. Banakh, A. Piskozub, and I. Opirskyy, "Devising a method for detecting 'Evil Twin' attacks on IEEE 802.11 networks (Wi-Fi) with KNN classification model," *Eastern-European J. Enterprise Technologies*, vol. 3, no. 9(123), pp. 20–32, 2023, doi: 10.15587/1729-4061.2023.282131.

[5] N. A. Akparibo and E. K. Bankas, "Machine learning for Evil Twin attack detection," *STEM Education Review*, vol. 3, no. 1, 2025.

[6] A. Kamble and D. Kshirsagar, "Feature selection in wireless intrusion detection system for Evil Twin attack detection," in *Proc. 3rd Int. Conf. Innovative Sustainable Computational Technologies (CISCT)*, 2023.

[7] N. S. Selvarathinam, A. K. Dhar, and S. Biswas, "Evil Twin attack detection using discrete event systems in IEEE 802.11 Wi-Fi networks," in *Proc. 27th Mediterranean Conf. Control and Automation (MED)*, Akko, Israel, 2019, pp. 316–321, doi: 10.1109/MED.2019.8798568.

[8] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 184–208, 2016, doi: 10.1109/COMST.2015.2402161.

[9] S. Harsha et al., "Improving Wi-Fi security against evil twin attack using light weight machine learning application," *COMPUSOFT*, vol. 8, no. 3, 2019.

[10] M. Asaduzzaman, M. S. Majib, and M. M. Rahman, "Wi-Fi frame classification and feature selection for Evil Twin detection," 2020.

[11] V. Kumar, V. Manaee, and R. Nirala, "A machine learning-based framework for Evil Twin attack detection and mitigation in IEEE 802.11 wireless networks," in *Proc. Int. Conf. Emerging Technologies and Innovation for Sustainability (EmergIN)*, 2025, pp. 642–647.

[12] P. Augustyniak, A. Gruszecki, and P. Zwierzykowski, "Comparative analysis of the effectiveness of machine learning algorithms used for WLAN network protection," in *Smart Networks and Security – IoT, Wireless Systems, and Positioning: 46ICT*, 2025.

[13] S. A. A., T. Arora, V. Abrol, and K. Sharma, "EvilSpot: Detection and mitigation in multi channel," in *Proc. Int. Conf. Advances in Electronics, Communication, Computing and Intelligent Information Systems (ICAECIS)*, 2023.

[14] F.-H. Hsu, M.-H. Wu, Y.-L. Hwang, C.-H. Lee, C.-S. Wang, and T.-C. Chang, "WPFD: Active user-side detection of Evil Twins," *Applied Sciences*, vol. 12, no. 16, p. 8088, 2022, doi: 10.3390/app12168088.