IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46ICT/2025/4639025/
Vol. 2025 (35), Article ID 4639025

Comparative Analysis of the Effectiveness of Machine Learning Algorithms Used for WLAN Network Protection*

Piotr Augustyniak, Adrian Gruszecki and Piotr Zwierzykowski

Institute of Computer and Communication Networks,
Faculty of Computing and Telecommunications,
Poznan University of Technology, Poznań, Poland

Correspondence should be addressed to: Piotr Augustyniak, piotr.augustyniak@put.poznan.pl

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

The rapid development of wireless technologies and the growing dependency on WLAN infrastructures have significantly increased the surface of potential cyber threats. Among these, Evil Twin and Rogue Access Point attacks remain some of the most persistent and dangerous due to their ability to mimic legitimate network entities and deceive end users. This paper presents a comparative analysis of machine learning algorithms applied to the detection, prediction, and prevention of WLAN attacks, with a particular focus on the Evil Twin attack family. The study provides an overview of datasets used in research—namely AWID3 and NSL-KDD—and summarizes recent approaches identified through a literature review of IEEE publications from the past three years. The results highlight the consistently high accuracy of various supervised learning algorithms and emphasize the need for lightweight, computationally efficient models suitable for real-time wireless intrusion detection systems. The paper concludes with recommendations for future research directions, focusing on optimizing traditional machine learning algorithms for resource-constrained environments.

Keywords: WLAN security, Evil Twin attack, intrusion detection, machine learning, network protection, wireless cybersecurity.

Introduction

Ensuring the secure use of computer networks remains a major challenge for enterprises and other organizations, regardless of their size. Larger entities, possessing greater financial resources, can more easily provide security to their users by investing in appropriate hardware and software solutions. In contrast, smaller organizations face significantly greater difficulties in this regard. Due to budget constraints, they often resort to outsourcing security services—typically based on cloud solutions—or rely on open-source alternatives.

Security risks are particularly evident in the area of wireless networks, which, by their very nature—specifically the ease of access to the communication channel—are inherently more vulnerable to attacks. The issue of wireless local area network (WLAN) security primarily focuses on two domains. The first domain concerns maintaining security when the WLAN communication layer lies outside the administrator's control. The second domain addresses the security of the end user. Within this latter area, the most prominent threats currently include *Evil Twin* and *Rogue Access Point (Rogue AP)* attacks, against which effective defense is, in practice, nearly impossible. Moreover, these attacks are relatively easy to execute while maintaining a high success rate [1,2].

The research presented in this paper focuses on the second domain—end-user security. In the initial phase of this study, *Evil Twin* and *Rogue AP* attacks were adopted as the representative attack models. Based on an extensive literature review and subsequent analysis, it was determined that the family of attacks collectively known as *Evil Twin* can be treated as a reference category encompassing most of the characteristic features of attacks targeting wireless local area networks.

Cite this Article as: Piotr Augustyniak, Adrian Gruszecki and Piotr Zwierzykowski, Vol. 2025 (35) "Comparative Analysis of the Effectiveness of Machine Learning Algorithms Used for WLAN Network Protection" Communications of International Proceedings, Vol. 2025 (35), Article ID 4639025, https://doi.org/10.5171/2025.4639025

This paper presents a review of selected machine learning techniques applied to the detection of this family of attacks (*Evil Twin*). Furthermore, it outlines specific datasets used in the experiments. The results are summarized in comparative tables presenting the detection accuracy of individual methods along with their specific applications, allowing for the formulation of relevant conclusions.

Terminology

To effectively navigate the topic of attacks targeting networks operating under the IEEE 802.11 family of standards, it is necessary to establish the taxonomy of attacks used throughout this paper. In the literature, the most common classifications are those that categorize attacks according to their objective (e.g., *Denial of Service*—where the goal is to disrupt service availability), method (e.g., *social engineering*), or target (e.g., *network infrastructure elements* or *web applications*).

In this paper, an approach based on the objective of the attack within WLAN networks is adopted. Regardless of other factors, two primary categories of attacks can always (i.e., without exception) be distinguished: Man-in-the-Middle (MitM) attacks and Denial of Service (DoS) attacks.

Man-in-the-Middle (MitM)

In general terms, this type of attack involves a cybercriminal secretly intercepting and relaying communication between two parties. In WLAN environments, the attacker transmits data between any access point and a client, thereby gaining the ability to eavesdrop on the traffic and modify packets before they reach their intended destination.

In the case of an *Evil Twin* attack, a fake access point is created that replicates the characteristics of an authorized one—such as the same MAC address, BSSID, SSID, and IP addressing scheme—effectively mirroring the legitimate network. Once a client connects to the rogue access point, the attacker can intercept and modify transmitted data, capture authentication credentials, display false or misleading information, use network services on behalf of the victim, and perform various other malicious actions.

Denial of Service (DoS)

This relatively straightforward category of attacks aims to compromise the availability of system resources selected by the attacker, making them inaccessible to legitimate users. In the context of Evil Twin attacks, this includes all activities designed to disconnect clients from authorized access points. Examples include flooding the network with Deauthentication or Deassociation frames.

The attacker's goal is to reinforce the effectiveness of the traditional MitM-style attack—by forcibly disconnecting legitimate clients, the likelihood of their reconnection to the rogue access point increases, thereby enhancing the probability of a successful compromise.

Based on the conducted literature review and subsequent analysis, it can be concluded that Evil Twin attacks simultaneously encompass both categories—Man-in-the-Middle and Denial of Service—and will be analyzed within this dual framework in the following sections of this paper.

Datasets

In intrusion detection research—particularly when employing methods and techniques from the broad field of artificial intelligence—datasets play a fundamental role. In this section, two datasets of particular significance to the methods discussed in this paper are briefly described AWID3 [3].

The focus was on data sets related to Evil Twin attacks or their characteristic features. Evil Twin attack detection is based on the analysis of 802.11 frames (e.g., via Wireshark) and traffic characteristics. The key features used for detection (and not related to the signal – or more generally to the physical layer) are:

- MAC Address / BSSID: duplicate BSSIDs (the same address for multiple APs). In AWID: the "BSSID" feature – monitoring duplicates
- SSID: Identical network names, but with anomalies in beacon frames. Features: "SSID" and "Beacon Interval"
- Response time / Latency: Higher delay in a fake AP. In AWID3: features such as "Timestamp" and "Inter-Frame Space" (IFS)

- Frame Patterns: Excessive beacon/probe response frames, no response to probe requests. Features: “Frame Type/Subtype,” “ToDS/FromDS bits” (set to 0 in the attack), “Number of Associations/Disassociations.”
- Channel / Frequency: Same channel, but anomalies in switching. Features: “Channel Number,” “Frequency.”
- Traffic Anomalies: Low throughput, deauth frames before the attack.
- Beacon Frames Anomalies: Irregular beacon intervals (e.g., shorter). Features: “Beacon Interval,” “Supported Rates.”

AWID3 Dataset

A distinctive feature of the AWID3 dataset is that all analyzed attacks were conducted under conditions where the Protected Management Frames (PMF) function was active. To support the development of Wi-Fi intrusion detection systems, the dataset was collected in CSV format and contains a set of 254 manually selected attributes, of which 253 represent general parameters, and one serves as the class label. These features were extracted from the analysis of the Medium Access Control (MAC) and application layers, based on Packet Capture (PCAP) files.

The dataset was generated in a laboratory testbed environment simulating the structure of a typical enterprise network. The experiments involved 16 physical devices and virtual machines, enabling the replication of realistic network infrastructure. The dataset includes 34,715,948 instances of normal operation and 2,234,467 instances of various attack-related events.

Among the threats represented in the dataset are: Re-Assoc, Botnet, Deauth, Disas, Evil_Twin, Kr00k, Krack, Malware, RogueAP, SQL Injection, SSDP, SSH, and website spoofing attacks, along with data illustrating normal system behavior [3].

The vast majority of intrusion detection algorithms in the literature are based on the AWID3 (Aegean Wi-Fi Intrusion Dataset 3) dataset—the latest version of the AWID dataset (2021), containing over 200 million records of 802.11 traffic in an enterprise . It covers normal traffic and attacks on Wi-Fi networks. The previous version of AWID (2016) contained traffic from SOHO (small office/home office) networks. It includes attacks specific to Wi-Fi.

AFSD Dataset

In 2023, Fahd Alhaidari created the AirForce Security Dataset (AFSD) [4] and made it available on the IEEE platform.

As described, this is the first public dataset dedicated specifically to detecting Evil Twin (ET) attacks on Wi-Fi (802.11) networks. It contains data from current protocols (WPA3, 802.11ax) – unlike AWID3. In order to be able to compare work on these sets, AFSD also has the same number of features, equal to 155, and is publicly available. This allows the same model to be trained (both on AWID3 and AFSD) without changing the data structure.

The author's adaptation of the AFSD structure has additional advantages. Of particular note is the fact that it is possible to transfer code – AWID preprocessing scripts work on AFSD without changes – thanks to, among other things, the same column names and the same *.csv format.

According to the author, if a given model achieves greater accuracy on AFSD than on AWID, this is directly due not to the number of features (which is identical) but to a better representation of the Evil Twin attack – it better reflects this attack.

Despite the promising information presented by the author of this dataset, the authors of the article were unable to find any publications where this dataset had been used. If we assume that the process of adopting new datasets (and AFSD should be considered as such – publication date April 2023) takes 1-2 years, we can expect to see works using it in the near future.

Compared to AWID3, it is still a niche solution.

Criteria and Methodology

To conduct a literature review and analysis of available scientific research, specific article selection criteria were applied to ensure that the studies included in the paper were not only thematically related to the issue under discussion, but also provided relevant results regarding the detection, prevention, and prediction of Evil Twin attacks and other threats in WLANs. The article selection process consisted of several key stages:

Database

The articles were mainly searched for in one of the most important scientific databases in the field of information and communication technologies: IEEE Xplore. This database is considered one of the most comprehensive and reputable sources in this field, containing publications related to computer engineering, network security, and the use of artificial intelligence in solving cyber threat problems.

Selection Criteria

The selection of articles was based on several key criteria:

Thematic Relevance

The work had to focus on technologies for detecting attacks on WLAN networks using machine learning algorithms, particularly in the context of Evil Twin attacks. These attacks were considered representative of the broader problem of end-user security in wireless networks.

Publication period:

The selection was limited to works published in recent years (2020-2025) in order to take into account the latest trends and methodologies in the field of detecting and preventing attacks on WLAN networks.

Type of Methodology:

The selection included only works that used machine learning methods, both supervised and unsupervised, to detect attacks, including Man-in-the-Middle (MitM) and Denial of Service (DoS) attacks in the context of 802.11 networks.

Specifics of the Attack:

Particular emphasis was placed on studies that examined the Evil Twin attack in detail as an attack model, including various aspects of its detection, prevention, and prediction, based on available data sets.

Search queries

Keyword-based queries directly related to the subject under study were used to search for articles. Examples of queries include:

"Evil Twin attack detection machine learning", "Wireless LAN intrusion detection", "802.11 security machine learning", "Evil Twin WLAN attack prevention", "Machine learning for Wi-Fi security"

In addition, search filters were used to limit the results to scientific articles (journals and conference papers) and exclude results from other categories, such as books or technical reports, which were not peer-reviewed scientific works.

Scope of Work Compliance Analysis

From among the articles obtained using the above queries, a preliminary selection was made based on titles, abstracts, and keywords. Only those works were selected that:

- They concerned broadly understood WLAN security.
- They focused on the use of machine learning algorithms in the context of attack detection.
- They contained specific experimental data, such as classification accuracy in detecting attacks (e.g., Evil Twin), and indicated the methods used and the data sets employed.

Selection Based on Datasets Used

Additionally, due to the specific nature of the subject under study, great emphasis was placed on articles that used recognizable and applicable data sets.

4.6 Selection Based on Methods and Results

The final selection included only those papers that contained reliable experimental results concerning the detection of Evil Twin attacks and their comparison with other methods. Particular attention was paid to papers that:

- They demonstrated high classification accuracy using machine learning algorithms.
- They discussed the limitations and challenges associated with the use of these algorithms in practical applications.
- They pointed to potential directions for further research, particularly in the context of optimizing algorithms for environments with limited computing resources.

Analysis of Current Research

The selection of articles for review was based on criteria such as thematic relevance, modernity of research, methods used, and available experimental data. This made it possible to present a review of studies that fully corresponded to the topic of the thesis, focusing on the use of machine learning methods to detect Evil Twin attacks in WLAN networks. The selection also focused on works published in recent years in order to take into account the latest achievements in this field.The results presented in Table 1 summarize research studies that, upon detailed review, were classified as works focusing on the application of specific methods for detecting particular types of attacks in WLAN networks, with a primary emphasis on Evil Twin attacks.

It can be observed that not all of the analyzed studies addressed prior research involving the same algorithms or specific datasets. This indicates that the findings from the selected works provide new insights into previously unexplored aspects of this issue.

Furthermore, when examining the column related to classification accuracy of network traffic depending on the applied method and dataset, a consistently high level of effectiveness can be observed across various machine learning techniques.

Table 1: Summary of Research Articles Related to the Detection of Evil Twin Attacks in Wireless Networks

Study No. 1
Title: Feature Selection in Wireless Intrusion Detection Systems for Detecting Evil Twin Attacks [7]
Application: Detection
Machine Learning Techniques Used: Random Forest, REP Tree, J48, Random Tree, Hoeffding Tree, Decision Stump
Type of Attack: Evil Twin
Previously Reported Detection Accuracy: Decision Tree Classifier – 99.92%, Random Forest – 99.93%, J48 – 91.24%
Dataset Used: AWID3
Classification Accuracy for Network Traffic: REP Tree – 99.9834%, J48 – 99.9834%, Random Tree – 99.9474%, Random Forest – 99.9889%, Hoeffding Tree – 99.7826%, Decision Stump – 94.8463%
Study No. 2
Title: Cyberattack Identification System Using Deep Learning [8]

Application: Detection
Machine Learning Techniques Used: Deep Q-Network (DQN); K-Means Clustering with Random Forest (RF); Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM); Principal Component Analysis (PCA) and Mutual Information (MI) with LSTM; Auto Encoder (AE), Stacked Auto Encoder (SAE), Deep Auto Encoder (DAE) with Deep Neural Networks (DNN); Recurrent Neural Networks (RNN); Dual/Constrained Attention Mechanism with Gated Recurrent Units (GRU) and RNN; Conditional Deep Belief Network (CDBN); Stacked Contractive Auto-Encoder (SCAE); Decision Tree; Artificial Neural Network (ANN); Random Forest (RF); Self-Organizing Map (SOM); K-Means and Expectation Maximization (EM); Deep Belief Network (DBN) with Genetic Algorithm (GA), Artificial Fish Swarm Algorithm (AFSA), and Particle Swarm Optimization (PSO); Recursive Feature Elimination (RFE) with Ensemble Classifier (RF, SVM, Swell); Fuzzy C-Means (FCM).
Type of Attack: Flooding-type attacks (Kr00k, Deauthentication, Dissociation, Reassociation); Spoofing attacks (Rogue AP, Krack, Evil Twin); Botnet and DDoS attacks.
Previously Reported Detection Accuracy: (1) Ensemble method using RFE and classifier ensemble (RF, SVM, Swell) – 99.98% (AWID-CLS-Test); (2) Radial Basis Function Classifier (RBFC) – 98% (AWID); (3) Network trained on AWID3 dataset – 99%.
Datasets Used: AWID3, NSL-KDD, CIC-IDS2017.
Classification Accuracy for Network Traffic: (1) Hybrid K-Means + RF + CNN + LSTM (Apache Spark) – 85% (NSL-KDD) and 99.9% (CIC-IDS2017); (2) LSTM-PCA – 99.36%; (3) Conditional Deep Belief Network (CDBN) – 97.4%; (4) DBN with GA, AFSA, PSO – 98% (NSL-KDD); (5) Deep Q-Network (DQN) – 97.90%; (6) Radial Basis Function Classifier (RBFC) – 98% (AWID).

Table 2: Presentation of a Selected Study Related to the Prediction of Specific Attacks in Wireless Networks

Study No. 1
Title: Prediction of Man-in-the-Middle Attacks Using Machine Learning [5]
Application: Prediction
Machine Learning Techniques Used: Logistic Regression, K-Nearest Neighbors (KNN), Decision Tree, Bernoulli Naive Bayes
Type of Attack: Man-in-the-Middle (MitM) attacks, Denial-of-Service (DoS) attacks, and Probe attacks
Previously Reported Detection Accuracy: Not available
Dataset Used: Dataset collected from various wireless network monitoring devices and general communication channels
Classification Accuracy for Network Traffic: K-Nearest Neighbors (KNN) – 98.87%; Logistic Regression – 98.67%; Bernoulli Naive Bayes – 95.40% Decision Tree – 53.46%

Table 2 presents a single research article focusing on the application of specific methods for predicting Evil Twin attacks. The authors do not provide any results derived from earlier studies.

When examining the column related to classification accuracy, it can be observed that nearly all employed methods—except for the Decision Tree (53.46%)—achieved high effectiveness levels exceeding 95%.

Table 3: Presentation of a Selected Study Related to the Prevention of Attacks in Wireless Networks

Study No. 1
Title: Enhancing Eavesdropping Detection in Home Wi-Fi IoT Networks Using an Ensemble Learning Approach Based on a Network Monitoring System (NMS) [6]
Application: Prevention
Machine Learning Techniques Used: Random Forest, XGBoost, and LightGBM (ensemble methods based on bagging and boosting); Decision Tree algorithm
Type of Attack: Sniffing (eavesdropping) attacks
Previously Reported Detection Accuracy: Not available
Dataset Used: Dataset obtained from a supervised learning experiment consisting of 12,000 instances with 31 attributes
Classification Accuracy for Network Traffic: Accuracy of ensemble machine learning methods (Decision Tree, Random Forest, XGBoost, and LightGBM) exceeded 99% in detecting sniffing attacks in home Wi-Fi IoT networks

Table 3 presents a research article that explores the use of machine learning algorithms for preventing attacks on wireless networks. It is important to note that eavesdropping represents a *passive attack*, which makes it particularly challenging to detect.

The article provides evidence that eavesdropping in WLAN environments can, in fact, be detected through the application of machine learning techniques, demonstrating their potential for enhancing the security of wireless communication systems.

Conclusions

Each of the reviewed and analyzed research studies employed various machine learning techniques. However, the limited number of studies focusing specifically on Evil Twin attacks prevents drawing definitive or statistically meaningful conclusions.

With the exception of a single publication, all available studies concentrate on a broader spectrum of attacks on wireless networks, rather than on a specific attack family — such as Evil Twin. Moreover, there is no clear trend toward evaluating less resource-intensive methods, which would require lower computational power and could therefore be more practical in real-world applications.

Future Work

The authors plan to conduct their own experimental research, initially focusing on traditional machine learning algorithms, excluding deep learning and generative artificial intelligence approaches.

The main objectives of the future work include:

- achieving better algorithm-to-problem matching through the use of smaller and more focused datasets (limited to a single, strongly correlated attack family), and
- reducing computational requirements while maintaining high detection accuracy
- experimental comparison on two datasets, AWID3 and AFSD.

Such an approach is expected to facilitate more efficient and scalable intrusion detection in wireless network environments.

Acknowledgments

This research was funded by the Polish Ministry of Science and Higher Education
(No. 0313/SBAD/1311).

References

- P. Augustyniak, O. Rogowicz, P. Zwierzykowski: *Concept and Phases of the Rogue Access Point Attack* [in]: Artificial Intelligence and Machine Learning. 43rd IBIMA Conference, IBIMA-AI 2024, Madrid, Spain, June 26–27, 2024, Revised Selected Papers, Part-I / red. Khalid S. Soliman - Cham, Switzerland : Springer Nature Switzerland AG, 2025 - pp. 290-302
- P. Augustyniak, O. Rogowicz, P. Zwierzykowski: *Theoretical and Practical Aspects of the Evil Twin Attack. The Attacker's Perspective and Defense Methodology* [in]: Artificial intelligence and Machine Learning. 41st IBIMA International Conference, IBIMA-AI 2023, Granada, Spain, June 26–27, 2023, Revised Selected Papers / red. Khalid S. Soliman - Cham, Switzerland : Springer Nature Switzerland AG, 2024 - pp. 224-236
- https://icsdweb.aegean.gr/awid/awid3 (accessed on: 27.10.2025)
- https://ieee-dataport.org/documents/airforce-afsd (accessed on: 03.11.2025)
- A. Kamble and D. Kshirsagar, "Feature Selection in Wireless Intrusion Detection System for Evil Twin Attack Detection," *2023 3rd International Conference on Innovative Sustainable Technologies & Applications (ISTA-23)*, pp. 362-368. doi: 10.1109/ISTA-23/072126 (Proc. 072/072126) ([proceedings.com][1])
- M. M. Hussain, N. Khalid, A. Amjad and M. Shoaib, "Cyber Attack Identification System Using Deep Learning," in *Proceedings of the 2024 IEEE International Conference on Advances in Cyber Security (ICACS 2024)*, pp. 1-13, Feb. 19 2024. doi: 10.1109/ICACS60934.2024.10473266.
- K. Venkateswara Rao, B. Renu Akshaya, G. G. Satvik, *et al.*, "Machine Learning based Man-in-the-Middle Attack Prediction," in *Proceedings of the International Conference on Applied Artificial Intelligence and Computing (ICAAIC) 2024*, IEEE, 2024. doi: 10.1109/ICAAIC60222.2024.1057579
- H. J.Jin, F. R. Ghashghaei, N.Elmrabit: *Enhancing Sniffing Detection in IoT Home Wi-Fi Networks: An Ensemble Learning Approach With Network Monitoring System (NMS)*, IEEE Access, Volume: 12, 2024, s. 86840-86853