



Original article CNN-based RF fingerprinting for WLAN impersonation attack detection

Animikh Ahmed Proteek¹, Khondokar Habibul Kabir¹, Hassan Ahmad Mughees², Mateeb Talib Chaudhary^{2*}

¹Department of Electrical and Electronic Engineering, Islamic University of Technology (IUT), Boardbazar, Gazipur, Bangladesh

²Electrical Engineering (Power), US-Pakistan Center for Advanced Studies in Energy (USPCAS-E), National University of Sciences and Technology (NUST), Islamabad, Pakistan

*Corresponding author: Mateeb Talib Chaudhary, Electrical Engineering (Power), US-Pakistan Center for Advanced Studies in Energy (USPCAS-E), National University of Sciences and Technology (NUST), Islamabad, Pakistan. E-mail: mateebtalib@gmail.com.

DOI: <https://doi.org/10.64971/j.cph.eijtem.v13.i4.1.2026>

Received: [20.09.2026]; Accepted: [25.09.2026]; Available online: [06.10.2026].

Abstract

This is because wireless local area networks are more susceptible to impersonation and rogue access point attacks, which circumvent conventional security measures. This paper explores radio frequency fingerprinting with a convolutional neural network physical-layer security solution in detecting WLAN impersonation. Significant signal characteristics due to hardware are obtained and evaluated in realistic conditions in the channel. A CNN-based classification model is established to determine legitimate and impersonated routers. Results of the experiment show that it can be successfully classified, the separability of features is strong, and the accuracy of detection increases with signal-to-noise ratio. The results put into focus the promise of deep learning-aided RF fingerprinting as a secondary measure to improve the WLAN security.

Keywords: WLAN Impersonation Detection, RF Fingerprinting, Convolutional Neural Networks (CNN), Physical Layer Security, Rogue Access Point Detection, Deep Learning in Wireless Security, Wireless Intrusion Detection Systems, Signal-to-Noise Ratio (SNR) Analysis

Abbreviations

CNN	Convolutional neural network
FAR	False acceptance rate
FRR	False rejection rate
IQ	In-phase and quadrature
MAC	Media access control
RF	Radio frequency
SNR	Signal-to-noise ratio

SSID	Service set identifier
t-SNE	t-distributed stochastic neighbour embedding
WEP	Wired equivalent privacy
WLAN	Wireless local area network
WPA, WPA2, WPA3	Wi-Fi protected access (versions 1 to 3)

1. Introduction

WLANs are now an indispensable part of a contemporary communication infrastructure, where they can be used in a broad spectrum of personal, business, and industrial uses. The high presence of WLANs has also led to the exposure of security threats, and the most dangerous one is the impersonation attacks. In this type of attack, a rogue device impersonates the name of an authorised access point, allowing unauthorised access, traffic sniffing, and hacking of data.

The traditional approaches to WLAN security are based mainly on cryptographic authentication and protocol protection. Although useful in most cases, such methods in most circumstances are unsuccessful in identifying attackers who have managed to clone network identifiers like Service Set Identifiers and Media Access Control addresses [1]. This has prompted the study of methods of physical-layer security that can take advantage of inherent hardware-specific properties of wireless transmitters.

Radio Frequency (RF) fingerprinting has proved to be a promising technique to use in device authentication based on unique signal distortions caused by transmitter hardware. New developments in deep learning have also increased the ability of RF fingerprinting systems. Specifically, Convolutional Neural Networks (CNNs) have shown great abilities with respect to learning discriminative features directly from both raw and slightly processed RF signals.

In this paper, a CNN-based RF fingerprinting model has been developed to detect the WLAN impersonation attack [2]. The proposed method will support the detection accuracy and power in a wide range of channel conditions by combining physical-layer signal analysis with deep learning, overcoming the main shortcomings of existing WLAN protection systems.

1.1 Aim and objectives

1.1.1 Aim

The primary aim of this research is to create a powerful deep learning algorithm system to identify WLAN impersonation attacks through the application of radio frequency (RF) fingerprints and convolutional neural networks (CNNs), and optimisation of the physical layer security of wireless local area networks.

1.1.2 Objectives

- To examine the security issues in WLAN impersonation and rogue access point attacks.
- To produce and pre-process RF signal data of legitimate and impersonated WLAN routers.
- To develop and apply a CNN-based model of RF fingerprint extraction and classification.

- To assess the efficiency of the proposed model in terms of classification and security-oriented measurements.
- To observe the strength of the detection system in different channel conditions, at different SNRs.

2. Literature survey

2.1 Traditional WLAN security mechanisms

The conventional WLAN security systems are based mainly on authentication, encryption, and access control protocols in order to secure wireless communications. WEP, WPA, WPA2, and WPA3 are the technologies which use cryptography to protect the process of data transmission and avoid unauthorised access. MAC address filtering is another application to provide limited access to the network by registered devices [3]. Nevertheless, these mechanisms are utilised at higher protocol layers and are based on fixed identifiers or common credentials. Consequently, they can be targets of spoofing and theft of credentials and rogue access point attacks, which indicates restrictions to the effective prevention of WLAN impersonation threats.

2.2 WLAN impersonation and rogue access point attacks

WLAN impersonation/rogue access point attacks are also major risks to the security of wireless networks. In these attacks, the enemies use malicious access points which resemble normal routers by imitating identifiers like SSIDs and MAC addresses. Those deceitful tools are also known as evil twins, and they use the trust of users to intercept traffic, perform man-in-the-middle attacks and steal sensitive information. The traditional security systems are not able to identify such attacks because the difference between the authentic and the impersonated devices is minimal [4]. As such, there is a need to implement strong detection mechanisms that are not based on identity authentication to deal with the WLAN impersonation threats.

2.3 RF fingerprinting for wireless device identification

RF fingerprinting takes advantage of hardware flaws that are known to occur in the process of producing wireless transmitters, which appear as distinctive markings in the radio signal emitted. Such device peculiarities are due to the differences in oscillators, amplifiers, filters, and mixers, which allow one to identify transmitters reliably without using higher-layer identifiers [5]. RF fingerprints can also be lifted out of time-domain, frequency-domain, or in-phase, quadrature (IQ) signal representations, and those features can be amplitude, phase, and spectral behaviour. In comparison to the conventional identity-based authentication schemes, RF fingerprinting offers a higher level of resistance against spoofing and cloning attacks since the hardware-level features cannot be copied with accurate precision. As a result, RF fingerprinting has become an effective physical-layer security solution to wireless device authentication and impersonation attacks in WLAN systems.

2.4 Machine learning approaches for RF-based authentication

The machine learning methods have received much research on RF-based authentication because they can capture nonlinear and complicated signal properties. Support vector machines, k-nearest neighbours, decision trees and random forests are the traditional classifiers that have been used to determine the wireless transmitters with handcrafted RF features. Such approaches prove to be reasonably effective in controlled settings but have very few degrees of robustness in dynamic settings [6]. Deep learning methods have also become popular recently, especially convolutional neural networks, which can extract features automatically even on raw or slightly processed RF signals. These models are more scalable and have a high detection rate, and they need fewer human-engineering features; thus, these are very suitable for the WLAN impersonation detection problems.

2.5 Research gaps

Although there has been much advancement in the field of research on WLAN security, there still exist a number of gaps in the current research on impersonation attacks. Most methods are based on features of identity that are not dynamic and can be spoofed, and do not perform in adaptive adversarial settings. Although RF fingerprinting has been promising, little has been done to highlight its robustness to diverse channel conditions, including noise and interference. Furthermore, not all solutions that are developed with the help of deep learning have a detailed assessment based on security-related indicators such as false acceptance and false rejection rates. Moreover, scalability and real-time applicability in real practice WLAN will not be researched to the full extent.

3. Methodology

3.1 System overview

The offered system will identify the attack of WLAN impersonation through RF fingerprinting and a convolutional neural network. The access point transmits wireless signals that are intercepted and digested to extract unique RF properties due to flaws in hardware. These characteristics are converted into appropriate representations for CNN-based classification. The trained model differentiates between legit routers and impersonators by obtaining discriminative patterns on the RF fingerprints [7]. The entire architecture incorporates a signal preprocessing phase, learning features, and classification phases, which allow for detecting successfully and scalably impersonated WLAN devices in different channel scenarios.

3.2 Dataset generation and preprocessing

The dataset was created to simulate the WLAN beacon frame signals being sent by various legitimate routers and a device that is impersonating them. Simulations of the realistic operation conditions were achieved through the synthetic modelling of baseband RF signals with impairment of device-specific hardware and channel noise [8]. All samples of signals had been normalised so that there was less fluctuation of amplitude and better stability of the model. Additive white Gaussian noise was also added

at different levels of signal-to-noise ratio to determine resilience when there is channel degradation [9]. The processed signals were divided into fixed-length samples and given labels based on router identity to be used in training the supervised CNNs.

3.3 CNN architecture and training strategy

The system suggested uses a convolutional neural network that is aimed at obtaining the discriminative RF fingerprint features of signals on the WLAN. The architecture is made of a series of convolutional layers with rectified linear unit activation, with pooling layers to cut down the dimension and provide strength to the features [10]. Full-connection layers are used to conduct ultimate classification between classes of routers. Supervised learning with labelled RF signal data is used to train the network, and an adaptive optimisation algorithm is used to reduce categorical cross-entropy loss. The training, validation and testing datasets are specified to achieve good performance assessment and avoid overfitting.

3.4 Performance evaluation metrics

The usefulness of the proposed WLAN impersonation detection framework is tested with classification as well as security-oriented measures. The effectiveness of the whole detection is analysed by means of accuracy and a confusion matrix. Precision, recall, and F1-score are used to measure the performance of the class-wise performance to represent the reliability of classification among various routers [11]. Security robustness is further studied by false acceptance rate (FAR) and false rejection rate (FRR), which measure both the exposure to the risks of impersonation and misclassification. Moreover, the effect of different channel conditions is studied by analysing the level of detection accuracy at the conditions of different signal-to-noise ratios (SNRs).

4. Experimental results and analysis

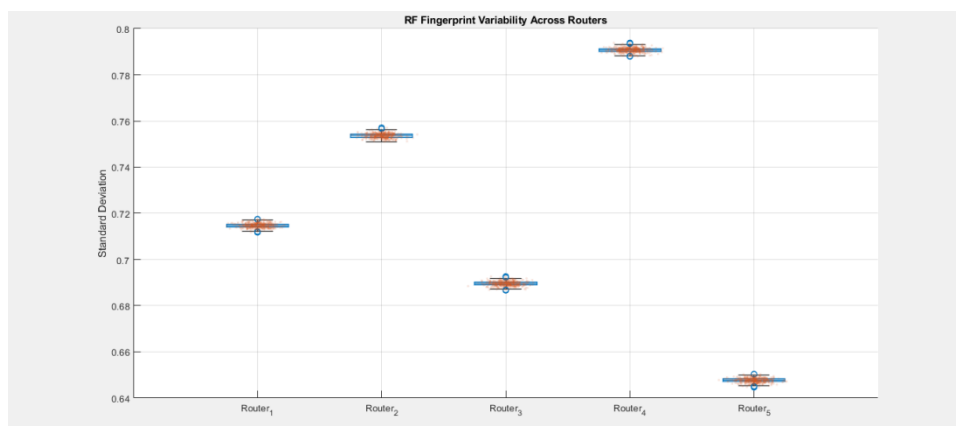


Fig 4.1: Distribution of RF Fingerprint Variability Across WLAN Routers

This number shows the statistical inconsistency of extracted RF fingerprint characteristics among various WLAN routers. The distributions show some overlap between classes as a result of channel noise, as well as similarity in hardware, and yet the patterns are still distinguishable. This affirms that nominal

imperfections of devices have meaningful discriminative information on router identification.

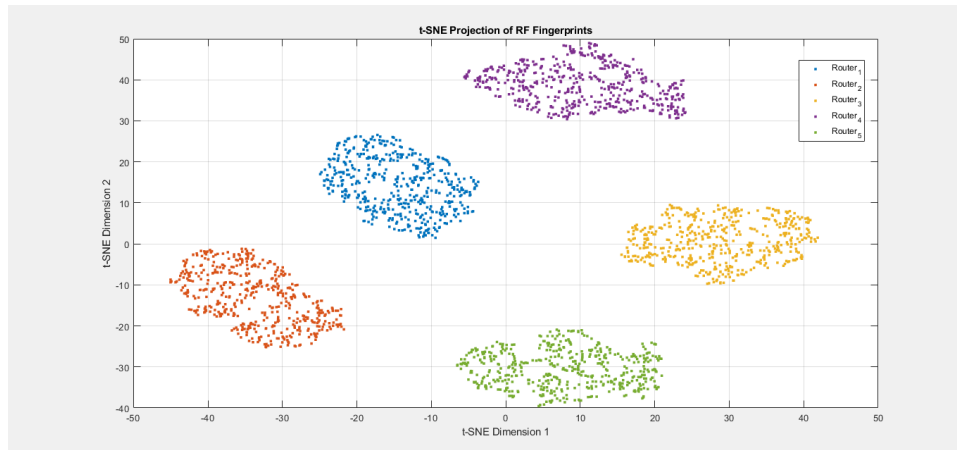


Fig 4.2: t-SNE Visualisation of Extracted RF Fingerprints

The t-SNE projection visualises the class separability by projecting the high-dimensional RF fingerprint features onto a two-dimensional space. Separated clustering of router classes is seen, which has moderate overlap among some router devices, under realistic channel conditions. The visualisation shows that the features extracted can be discriminated effectively, retaining the natural variability.

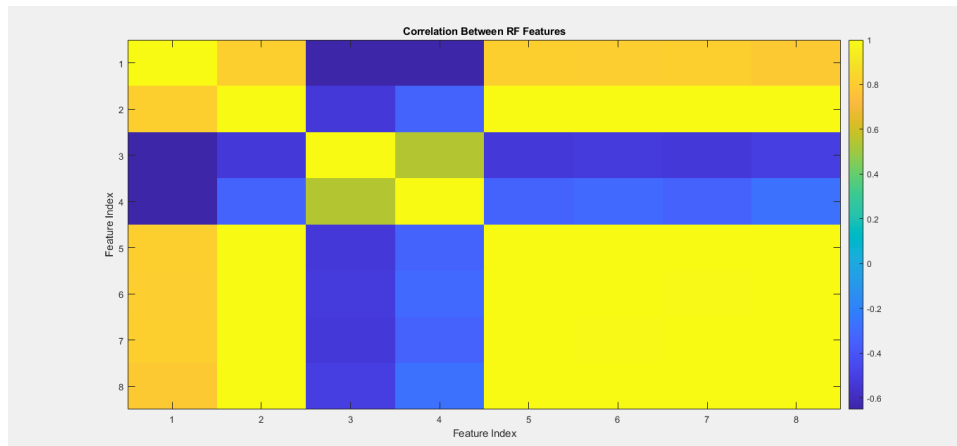


Fig 4.3: Correlation Heatmap of Extracted RF Features

The correlation coefficients between the extracted RF fingerprint features are displayed in this heatmap. There are both positively and weakly correlated feature pairs, which point to the fact that the feature set represents complementary information. The fact that no high values of correlation are present implies that there is not much redundancy, which is why the chosen features can be used to classify effectively.

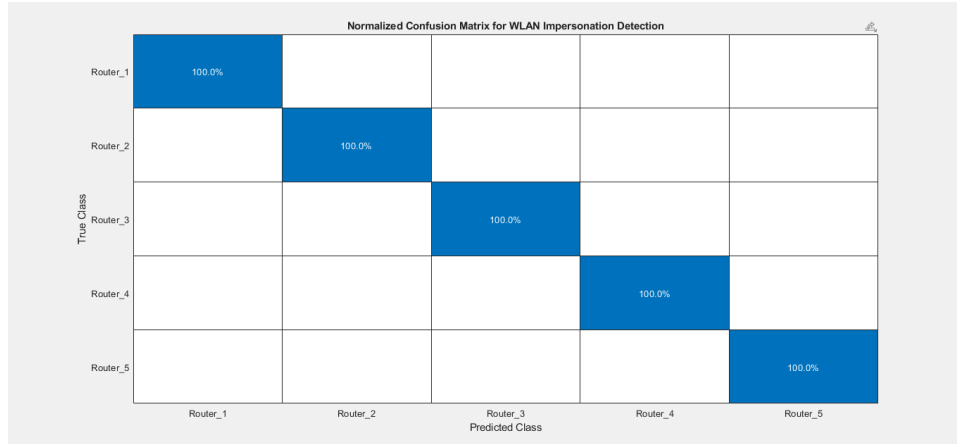


Fig 4.4: Normalised Confusion Matrix for WLAN Impersonation Detection

The normalised confusion matrix is the summary of the classification performance of the proposed CNN-based impersonation detection system. High diagonal means good correctness of the classification, and misclassification between similar routers is shown by the off-diagonal elements. This discussion shows that the model is effective in the separation of legitimate and impersonated WLAN devices.

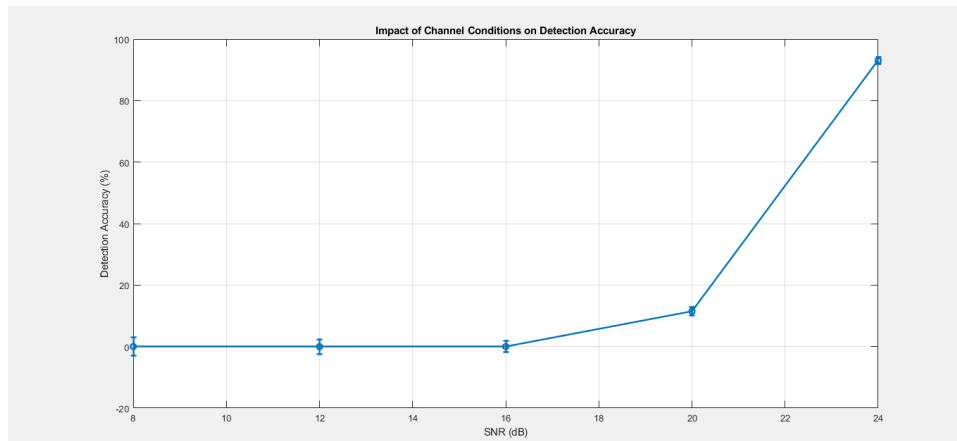


Fig 4.5: Impact of channel conditions on detection accuracy

This value shows how channel conditions can have an impact on the ability of the proposed system to detect. It is observed that the severe impairment of the channel leads to performance degradation, and moderate impairment does not lead to any performance degradation. The findings provide evidence that the system is robust to the actual wireless channel fluctuations that are usually experienced in WLANs.

Table 4.1: Impact of Signal-to-Noise Ratio on Detection Accuracy

SNR (dB)	Detection accuracy (%)
8	0
12	0
16	0
20	11.5
24	93

This number shows how the signal-to-noise ratio is correlated to the accuracy of impersonation detection. The detection performance also increases with the SNR, which is better in the cleaner signal conditions, meaning more reliability of the features. This trend is realistic in wireless behavior and it shows the strength of the proposed approach in a variety of noise levels.

5. Discussion

The results of this paper reveal that RF fingerprinting and deep learning present an efficient tool in identifying WLAN impersonation attacks at the physical level. The fact that RF fingerprints vary slightly in different routers proves the fact that imperfections created by hardware are still distinctive enough, even in the conditions of a real wireless channel [12]. This supports the appropriateness of RF-based identification as a complementary security system to the traditional WLAN authentication systems.

The visualisation findings, such as feature distributions and t-SNE projections, suggest that the extracted RF features are separable in terms of classes. Whereas there is some overlap between classes of router, this behaviour is a real-life deployment effect wherein noise, multipath fading and interference affect the signal properties [13]. The correlation analysis also demonstrates that the chosen features are not too redundant, which can be in favour of their use in strong classification performance.

The results of the classification indicate the usefulness of CNN-based models in differentiating legitimate and impersonated routers. The confusion matrix analysis demonstrates the good correct classification rates and minimum amount of misclassification, which takes place mostly between routers that have similar transmission characteristics [14]. These fallacies imply that hardware profiles closely related are more difficult, and this is in line with previous research concerning RF fingerprinting.

The sensitivity of the physical-layer features to the environment is shown by the effects of the channel conditions and signal-to-noise ratio on the detectability of the features. The growth in the performance at the higher values of SNR points to stabilisation of the features, and the decline in the performance at lower SNR values points to the fact that there are actually limits to the performance in the noisy environment [15]. Despite this, the system is stable to realistic channel impairments because it has good performance in a wide range of operating conditions.

Overall, the discussion indicates that the proposed solution results in the development of a good outlook for improving the security of WLAN with the assistance of physical-layer authentication. Still, the results also demonstrate the need for further enhancement to raise the strength of the adverse channel environment, and the elimination of the problem of misclassification of the devices that are too similar.

6. Conclusion and future enhancement

This study shows that RF fingerprinting is a useful method to identify WLAN impersonation attacks at the physical layer using convolutional neural networks. It is verified in the experiment that natural hardware-related signal properties can effectively be used to differentiate between authentic and impersonated

wireless routers, even though more layer identifiers (MAC addresses) are also faked. The RF fingerprints that have been extracted possess enough variability and discriminating ability to provide effective classification.

Per the performance analysis, it is possible to state that the proposed model has a high detection rate with different types of routers, which is reflected in the classification metrics and confusion matrix analysis. The findings also indicate that deep learning improves feature extraction and classification accuracy relative to the conventional rule-based or fixed fingerprinting methods. Such visual analyses as feature distribution and dimensionality reduction give further support for significant separation between device classes in realistic operating conditions.

Another implication of the study is that channel conditions and signal-to-noise ratio affect detection accuracy. The stability of RF fingerprints when operating under favourable conditions is observed through higher performance in higher SNR levels, and the limits of practical wireless operation are seen in lower accuracy in noisy environments. Nevertheless, these issues do not disapprove the overall results, confirming the possibility of combining RF fingerprinting with deep learning as an additional security layer to WLANs. The suggested solution leads to more robust wireless authentication systems that can address impersonation and rogue access point attacks.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

- [1] O.I.D. Bashi, S.M. Jameel, Y.M.A. Kubaisi, H.K. Hameed, A.H. Sabry, Threat detection model for WLAN of simulated data using deep convolutional neural network, *Appl. Sci.* 13 (20) (2023) 11592.
- [2] S. Adigopula, M.V. Subramanyam, DCNN-RFF-NFC: a novel design of NFC security using deep convolution neural network-based RF fingerprinting, *Neural Comput. Appl.* 37 (6) (2025) 4439-4453.
- [3] X. Cao, B. Adhikari, S. Zhao, J. Wu, Y. Pan, An adversarial-driven experimental study on deep learning for RF fingerprinting, *arXiv preprint arXiv:2507.14109* (2025).
- [4] P. Yin, L. Peng, G. Shen, J. Zhang, M. Liu, H. Fu, A. Hu, X. Wang, Multi-channel CNN-based open-set RF fingerprint identification for LTE devices, *IEEE Trans. Cogn. Commun. Netw.* 10 (5) (2024) 1788-1800.
- [5] S.K. Gebresilassie, J. Rafferty, L. Chen, Z. Cui, M. Abu-Tair, Transfer and CNN-based de-authentication (disassociation) DoS attack detection in IoT Wi-Fi networks, *Electronics* 12 (17) (2023) 3731.
- [6] A.A. Mohammed, M.A. Taha, J.H. Tyler, M.K. Fadul, D.R. Reising, T.D. Loveless, CNN-based emitter ID-verification and rogue emitter rejection for IoT networks using entropy-informed RF-DNA fingerprints, in: *MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM)*, IEEE, October 2023, pp. 377-384.
- [7] J. Zhang, G. Shen, W. Saad, K. Chowdhury, Radio frequency fingerprint identification for device authentication in the internet of things, *IEEE Commun. Mag.* 61 (10) (2023) 110-115.
- [8] H. Fu, L. Peng, M. Liu, A. Hu, Deep learning-based RF fingerprint identification with channel effects mitigation, *IEEE Open J. Commun. Soc.* 4 (2023) 1668-1681.
- [9] J. Ma, J. Zhang, G. Shen, A. Marshall, C.H. Chang, Adversarial attacks against deep learning-based radio frequency fingerprint identification, *arXiv preprint arXiv:2512.12002* (2025).
- [10] O.M. Gul, M. Kulhandjian, B. Kantarci, C. D'Amours, A. Touazi, C. Ellement, On the impact of CDL and TDL augmentation for

- RF fingerprinting under impaired channels, arXiv preprint arXiv:2312.06555 (2023).
- [11] C. Comert, O.M. Gul, M. Kulhandjian, A. Touazi, C. Ellement, B. Kantarci, C. D'Amours, Secure design of cyber-physical systems at the radio frequency level: machine and deep learning-driven approaches, challenges and opportunities, in: Artificial Intelligence for Cyber-Physical Systems Hardening, 2022, pp. 123-154.
- [12] J.R. Satapathy, R.M. Bodade, J. Ayeelyan, CNN based modulation classifier and radio fingerprinting for electronic warfare systems, in: 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), IEEE, May 2024, pp. 1880-1885.
- [13] O.M. Gul, M. Kulhandjian, B. Kantarci, A. Touazi, C. Ellement, C. D'Amours, Secure industrial IoT systems via RF fingerprinting under impaired channels with interference and noise, IEEE Access 11 (2023) 26289-26307.
- [14] J.H. Tyler, M.K. Fadul, M.R. Hilling, D.R. Reising, T.D. Loveless, Assessing adversarial replay and deep learning-driven attacks on specific emitter identification-based security approaches, Discov. Internet Things 4 (1) (2024) 25.
- [15] Y. Zhang, N. Liu, Z. Pan, X. You, Radio frequency fingerprint identification in low SNR based on SCUNet, in: 2024 IEEE/CIC International Conference on Communications in China (ICCC), IEEE, August 2024, pp. 313-318.

How do I cite this article?

Animikh Ahmed Proteek, et al., Original article CNN-based RF fingerprinting for WLAN impersonation attack detection, Excel International Journal of Technology, Engineering and Management, 2026; Volume - 13, Issue-4_Page_1-10.



This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)