Jamming Echoes: On the Impact of Out-of-Band Interference on Radio Frequency Fingerprinting

Ingrid Huso*†, Salvatore Carbonara*, Savio Sciancalepore‡§, Gabriele Oligeri¶, Giuseppe Piro*†, Gennaro Boggia*†

*Dept. of Electrical and Information Engineering - Politecnico di Bari, Bari, Italy;
†CNIT, Consorzio Nazionale Interuniversitario per le Telecomunicazioni;
‡Eindhoven Artificial Intelligence Systems Institute (EAISI), Eindhoven, Netherlands;
§Eindhoven University of Technology, Eindhoven, Netherlands;
¶College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar;

***Abstract*—Radio Frequency Fingerprinting (RFF) has recently emerged as a lightweight and efficient strategy for classifying wireless devices based on their Radio Frequency (RF) emissions at the physical layer. Such emissions contain device-specific distortions that, although not affecting the quality of the communication link, can be extracted from the received signals through capable hardware (Software-Defined Radios—SDRs) and be used to classify via Deep Learning (DL) techniques the specific transmitters in a pool of RF devices. Recent research has shown that, although promising, RFF is a fragile phenomenon whose performance is significantly affected by various phenomena, e.g., channel fluctuations, device reboot, and firmware reload operations. In this paper, we shed light on yet another phenomenon affecting the reliability and robustness of RFF, i.e., interfering out-of-band signals. Through an extensive real-world experimental campaign involving seven heterogeneous SDRs and state-of-the-art DL image-based RFF systems, we demonstrate that out-of-band interfering signals emitted on neighboring frequencies (less than 5 MHz apart from the main communication channel), independently from being malicious, reduce the accuracy of RFF up to a random guess of the transmitter, while not significantly impacting the Bit-Error Rate of the communication link. These results foster further research in the design of reliable and robust DL-based RFF systems, capable of mitigating real-world deployment factors.**

***Index Terms*—Physical Layer Security, Radio Frequency Fingerprinting (RFF), Internet of Things (IoT).**

I. Introduction

The majority of Internet of Things (IoT) applications heavily rely on wireless networks, which, while allowing the creation of dynamic and scalable environments, exposes the IoT devices to several security issues, including unauthorized access and privacy violations, due to the open nature of the wireless communication channel [1]. Herein, authentication is an essential property for securing wireless communications [2]. The use of crypto-based solutions to guarantee authentication, which has been standard practice in past and current cellular networks, appears to be inadequate to address the anticipated challenges of future networks [2], such as devices with limited resources and key management for massive deployments.

In this context, Physical (PHY)-layer authentication is emerging as a promising technique to prove the identity of a device by leveraging its unique physical layer characteristics derived from its transmitted signal [2]. These inherent attributes, which do not require changes or computational effort at the transmitter side, serve as unique identifiers [2]. Specifically, Radio Frequency Fingerprinting (RFF) is a technique that leverages the inherent hardware characteristics of a transmitter, which are unintentionally reflected in the transmitted signal, thus allowing a passive receiver to identify the transmitter [3]. Electronic components such as oscillators, amplifiers, and modulators generate variations in the phase and frequency of the emitted signal without affecting the signal quality [4]. By extracting these characteristics, RFF can uniquely identify a device similar to the biometric signature of humans.

However, the impact of wireless channel conditions presents a significant challenge for RFF-based identification of wireless devices, particularly in wideband communication systems [5]. Traditional RFF techniques extract features that are a combination of the actual device-specific hardware impairments and wireless channel conditions, with the latter frequently dominating the signal representation [6]. As a result, RFF becomes unreliable when the channel conditions change, leading to high location dependency [6]. In this context, recent research demonstrates that Deep Learning (DL)-inspired image-based RFF models can obtain more reliable performance than classical DL models (involving the use of raw information from the radio spectrum), by mitigating the multipath effect from the wireless channel [7]. This methodology involves pre-processing the information collected from the physical layer of the radio spectrum (I-Q samples) and translating them into images to be considered as input for state-of-the-art image classification algorithms, such as Convolutional Neural Networks (CNNs). Thus, due to their robustness, DL image-based RFF models have been recently employed for RFF in several wireless environments [8] [9] [10].

In this context, the vast majority of the literature on RFF suggests performing RFF when the quality of the link between the transmitter and the receiver is high (low Bit Error Rate (BER)), to minimize the effect of the multipath fading. However, to the best of the authors' knowledge, no research has yet

explored the impact of jamming (i.e., intentional) or interfering (i.e., unintentional) signals acting near the communication bandwidth of the transmitter-receiver link.

Contribution. In this work, we systematically investigate the effect of out-of-band interference on the accuracy and robustness of RFF systems. Through extensive real-world controlled experiments utilizing Software Defined Radios (SDRs) and state-of-the-art DL image-based RFF models, we evaluate the impact of a source of interference against RFF. Our investigation reveals that out-of-band interfering signals, although negligibly affecting the BER of the communication link, can significantly affect the performance of RFF models, reducing the accuracy of state-of-the-art RFF systems down to a random guess of the transmitter. Specifically, our analysis reveals that out-of-band interference introduces yet another challenge for consistent and reliable device identification from PHY-layer data in real-world deployments.

Paper organization. The rest of the paper is organized as follows. Section II provides background concepts, Sec. III presents related work, Section IV introduces the conceived scenario, Section V details the deployed methodology, Section VI discusses the experimental tests and the obtained results, and Section VII concludes the paper and presents future work.

II. Background

In this section, we introduce preliminary concepts on digital modulation techniques and CNNs.

Digital Modulation. Wireless communication systems use digital modulation techniques to convert baseband to high-frequency signals suitable for transmission over the wireless channel [11]. In detail, a digital modulation scheme generates a modulated signal characterized by an in-phase (I) and a quadrature (Q) component, commonly represented as complex In-Phase Quadrature (IQ) values $I+jQ$, where I and Q denote the real and imaginary parts, respectively. The transmitter maps a bit sequence into symbols and then I-Q samples using a specific modulation scheme. The receiver decodes the original bit sequence from the received I-Q samples by associating to the received IQ value the symbol characterized by the minimum error, assuming that the noise affecting the received signal is minimal.

Convolutional Neural Network. CNNs are a widely used DL architecture mostly adopted in computer vision applications [12] and image processing [13]. Specifically, using images or labeled data, CNNs learn to generate hierarchical representations of the data, which can then be used effectively for accurate and reliable target classification [14] reaching high accuracy [15]. CNNs consist of three types of layers, i.e., convolutional, pooling, and fully-connected layers, where neurons perform convolutional operations and enhance the performance of the model through a process of iterative learning [16]. Convolutional layers handle feature extraction by applying convolutional filters to the input data, producing a corresponding feature map. Subsequently, the pooling layers are used to reduce computational overhead by downsampling the spatial dimensions of the feature map. Finally, fully connected layers are responsible for high-level feature processing and for making final predictions [16]. CNNs have gained popularity in the literature mainly for their remarkable performance in classifying images.

III. Related Work

RFF have recently gained popularity in the scientific community as a novel approach for authenticating Radio Frequency (RF) devices by analyzing their unique PHY-layer signal characteristics [2]. Overall, scientific approaches dealing with transmitter identification from PHY-layers signals are divided into two primary categories: i) traditional methods based on statistical analysis, and ii) approaches leveraging DL algorithms [3]. Traditional RF fingerprinting methods, relying on customized features, often face challenges in generalizing to real-world environments [17]. In contrast, DL automatically extracts complex features by directly using the raw I-Q data as input values, enhancing accuracy and adaptability [18]. While effective in many scenarios, this strategy produces sensitive fingerprint models that struggle to adapt to varying channel conditions, mobility, and power cycling of RF devices [7]. In this context, DL image-based RFF systems, converting raw I-Q samples into 2-D or 3-D images, have demonstrated superior identification performance over previous techniques under challenging channel conditions and across power cycles of the devices [19], [7]. DL Image-based RFF systems have been recently used also for the detection of several attacks in wireless scenarios, e.g., and jamming [9]. To mention a few relevant works using DL image-based RFF, Alhazbi et al. [8] propose a solution for early jamming detection and identification in mobile scenarios, leveraging DL to analyze image-transformed I-Q samples at the PHY layer and accurately detect and classify jamming types, including Gaussian noise and tone jamming. Along the same line, Sciancalepore et al. [9] perform jamming detection by focusing on an indoor scenario and extending the work in [8] with different modulation techniques, enhanced adversary models, and sparse autoencoders on image transformed I-Q samples. Moreover, Irfan et al. [10] present an approach for detecting jamming signals in Power Line Communication (PLC) systems by converting PHY-layer I-Q samples into images and applying CNN for classification.

Overall, although DL image-based RFF approaches have gained popularity in the PHY-layer security domain, currently available research concentrates on identifying jamming attacks, leaving unexplored the effect of interferences (intentional or not) on the accuracy of RFF. Moreover, none of these works analyzes the impact of an out-of-band interference on the performance of RFF. Indeed, whereas jamming on nearby channels has little effect on BER, RFF is much more fragile and can be potentially corrupted even when interferences do not occur on the same channel and bandwidth as the primary communication.

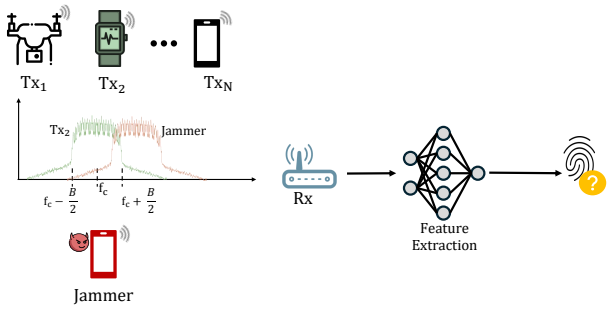

Fig. 1. Reference scenario.

IV. Reference Scenario

Fig. 1 illustrates our reference scenario, which considers N devices transmitting RF signals over the air for communicating with an RF receiver deployed on purpose to collect the signals emitted on the wireless spectrum and a jammer acting as an interference source. By being part of the network, the receiver always knows the frequency where a specific communication may occur, so being able to collect the raw PHY-layer information (IQ samples) corresponds to such transmissions. For ease of discussion, we assume that signals are modulated according to the Binary Phase-Shift Keying (BPSK) modulation scheme, although our considerations apply independently of the specific digital modulation technique and carrier frequency.

In our scenario, the receiver is responsible for identifying the transmitting device using RFF. Thus, the receiver collects IQ samples corresponding to valid received packets and delivers them to a central processing unit responsible for classifying the device emitting such packets by using RFF. In our scenario, we exploit state-of-the-art DL image-based RFF models, in line with the one adopted in [19], due to its enhanced robustness to channel variation and real-world effects characterizing embedded systems, such as radio reboot [7] and firmware reload [20]. Moreover, since the RFF system knows the RF profile of all the devices that can transmit on the wireless channel, it uses multi-class classification via CNNs to classify the device(s) that emit signals.

Herein, in line with standard RFF research, we assume that RF profiles are generated using wireless signals collected before the deployment in a controlled environment with no interference. However, at runtime during testing, wireless interference may occur in-band, i.e., on the same channel(s) of the regular communications, and out-of-band, i.e., on frequencies close but not coincidental with the ones included in the bandwidth of the regular communication channel. Throughout this paper, we refer to such interferences as *jamming*, independently from the nature of such interference, which could be unintentional (benign) or intentional (malicious).

In the following sections, we investigate the impact of such out-of-band interference on the accuracy of DL image-based RFF.

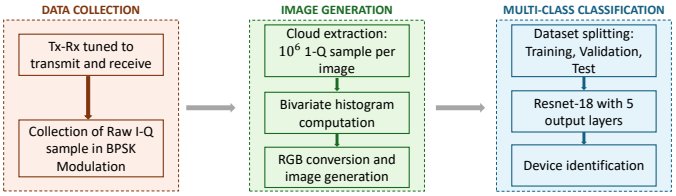

Fig. 2. Main steps of the DL image-based RFF Methodology.

V. RFF Methodology

This section describes the methodology used to assess the impact of the out-of-band interference on the RFF. The considered approach transforms I-Q samples into images, in line with state-of-the-art approaches relying on DL image-based RFF [7], [8], [19], [21], [22]. On the one hand, we note that DL image-based RFF provides considerable resilience against multi-path and other disturbances. On the other hand, our choice of using state-of-the-art tools for RFF aligns with the main objective of our research, i.e., demonstrating the impact that out-of-band interference has on RFF. In line with this methodology, the RFF problem is reformulated as an image recognition problem. Fig 2 depicts the three main steps of the employed methodology: (i) *Data Collection*, (ii) *Image Generation*, and (iii) *Multi-class classification*.

Data Collection. We collect raw PHY-layer data in the form of IQ samples from the wireless channel by aligning both the transmitter and receiver to the same frequency channel. We use the BPSK modulation technique, where the in-phase component takes on values of either -1 or +1, while the quadrature component is zero. The I and Q components are mapped to the real and imaginary parts of a complex number, respectively, as outlined in Eq. 1.

$$s(t) = \begin{cases} -1 \ \cos(2\pi f_c t), & \text{if b = 0,} \\ +1 \ \cos(2\pi f_c t), & \text{if b = 1,} \end{cases} \quad (1)$$

where $s(t)$ represents the transmitted signal, f_c denotes the carrier frequency, and b indicates the bit value. Therefore, for a given carrier frequency f_c, the pairs [-1, 0] and [1, 0] correspond to the theoretical positions of the transmitted I-Q samples on the I-Q plane. However, due to imperfections in radio hardware and fluctuations in the wireless propagation, the actual received I-Q samples are dispersed across the IQ plane, forming a pattern that embeds a unique fingerprint for the device.

Image Generation. This step involves processing the acquired raw I-Q samples and producing Red-Green-Blue (RGB) images, in accordance with the baseline procedure outlined in [7]. Specifically, the process entails slicing the received IQ samples into chunks of $K = 10^5$ IQ samples and then dividing the IQ plane, along with the corresponding point clouds produced by the IQ samples, into $Y \times J$ tiles. The parameters Y and J determine the dimensions of the final image. For each tile $i_{y,j}$, we determine the quantity of IQ samples that are contained within the tile, so generating a bivariate histogram. More in detail, an image is represented

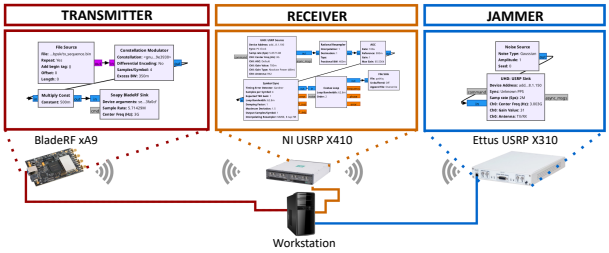

Fig. 3. Experimental Testbed—hardware and software components of our measurement setup.

TABLE I
COMMUNICATION SETTINGS PARAMETERS.

Parameter	Value
Reference Frequencies (Tx-Rx)	1 GHz, 2.4 GHz, 3 GHz
Communication Bandwidth	2 MHz
Roll-off factor (α)	0.35
Samples per symbol (Sps)	4
Sample rate	5.8 Msps
Jammer Carrier Frequencies	0.995-1.005 GHz, 2.395-2.405 GHz, 2.995-3.005 GHz
Jamming Bandwidth	2 MHz

as a matrix of dimensions $[Y \times J \times 3]$, where each color is one layer, and each pixel value in the range of 0 to 255 is assigned based on the tile value, according to the following scheme:

- If $0 \leq n_T < 255$, then $p_R = 0$, $p_G = 0$, and $p_B = n_T$,
- If $256 \leq n_T < 511$, then $p_R = 0$, $p_G = n_T - 255$, and $p_B = 255$,
- If $n_T > 511$, then $p_R = n_T - 510$, $p_G = 255$, and $p_B = 255$,

where n_T represents the tile value derived from the bivariate histogram, and p_R, p_G, and p_B correspond to the red, green, and blue pixel values, respectively. To ensure that the value corresponds to a valid pixel intensity in the generated image, if the count exceeds 255 (the maximum allowable pixel value), we truncate such value to 255. Note that it is crucial to adjust the number of IQ samples per image to minimize information loss, particularly from having too many tiles with a sample count exceeding 255.

Multi-class Classification. This phase allow performing RFF by correctly classifying the images generated in the previous step. In accordance with the scenario illustrated in Section IV, the objective of the proposed multi-class classification problem is to identify the transmitting device in the pool of N transmitters. To this aim, we split the collected dataset of I-Q samples into three subsets: training, validation, and testing. Moreover, we consider a state-of-the-art CNNs pre-trained on the ImageNet database [23], i.e., ResNet-18. We use the implementation of such models provided by MATLAB 2024a, with modifications made to the input and output layers to suit the specific classification task. The input layers are resized to match the dimensions of the images generated from raw IQ samples, while the output layers are restructured to account for the number of classes in the experiments, based on the number of transmitters.

VI. EXPERIMENTAL MEASUREMENTS AND ANALYSIS

Experimental Testbed. Fig. 3 illustrates the implemented experimental testbed used for our real-world tests. The testbed includes seven SDRs, with five of them working alternatively as transmitters, one working as jammer, and one working as the receiver. Specifically, the testbed is composed of the following devices:

i) Five *BladeRF 2.0 micro xA9* devices, used as transmitters, equipped with *LMS6002D* RF transceivers capable of supporting various wireless standards and mobile communication protocols. These devices can transmit wireless signals in the bandwidth $[47 - 6,000]$ MHz, with a gain up to 66 dB.

ii) One *NI Ettus USRP X410*, used as the receiver, providing four independent transmit and receive channels, each supporting up to 400 MHz of instantaneous bandwidth, and covering frequencies from 1 MHz to 7.2 GHz using a two-stage superheterodyne architecture.

iii) One *Ettus Research USRP X310*, employed as a jammer, supporting frequency coverage from DC to 6 GHz, with a maximum baseband bandwidth of 160 MHz.

The receiver is connected to a workstation running Linux Ubuntu 24.04 and equipped with an AMD Ryzen Threadripper PRO 5965WX @3.28 GHz processor and an NVIDIA GeForce RTX 4070 Ti, responsible for running RFF.

We used the software development toolkit GNU Radio, version 3.10, to control the operation of the SDRs and to customize the RF behavior with the required communication settings, as defined in Table I. In this context, the GNU Radio *transmitter chain* used on the Blade RF devices consists of three main blocks: i) a *File Source*, used to generate a (repeating) message made up of a string of 256 bytes with incremental values; ii) a *Constellation Modulator*, featuring a Root Raised Cosine (RRC)-filter, configured for the BPSK modulation scheme; and iii) a *Soapy BladeRF Sink*, which takes complex data as input and streams them to the BladeRF process unit to be then transmitted over the air. The *receiver* chain exploits the following five main blocks: i) a *UHD Source*, which acquires the I-Q samples from the USRP and streams them for further processing in the signal chain; ii) a *Rational Resampler*, which changes the sample rate of the received I-Q samples; iii) an *AGC*, which dynamically adjusts the gain of the signal to maintain a constant output amplitude, despite fluctuations in the channel; and finally, iv) a *Symbol Sync*, which is utilized to perform clock recovery by synchronizing with the symbols in the digital signal, subsequently decoding the digital signals; and v) a *Costas Loop*, which locks onto the center frequency. Finally, as for the *jammer*, we connect a *Gaussian Noise Source* generator directly to *UHD Sink* block, configured with a sample rate of 2 Msps, so to obtain an interference signal characterized by a nominal bandwidth of 2 MHz.

During our real-world tests, to minimize the impact of

TABLE II
ACCURACY OF RFF IN INTERFERENCE-FREE SCENARIOS.

Reference Frequency	1 GHz	2.4 GHz	3 GHz
RFF Accuracy	0.9831	0.9921	0.9692

FPGA reload [20] and power cycling on the RFF [7], we executed data collection without turning off the receiver and the jammer, while alternatively using the five *BladeRF* as transmitters. We selected three bandwidths of interest, i.e., $[990, 1010]$ MHz, $[2395, 2405]$ MHz, and $[2995, 3005]$ MHz, where we let the five signal transmitters emit signals of bandwidth 2 MHz on the carrier frequencies 1000 MHz, 2400 MHz and 3000 MHz, respectively. For each of such carrier frequencies, we conducted two distinct experiments. First, in an interference-free scenario, we performed 10 data acquisition sessions per communication frequency on each transmitter, lasting 25 seconds each. Then, we activated the jammer, injecting interference with bandwidth 2 MHz on all frequencies in the bandwidth of interest with a step of 1 MHz, and executed 5 data collection sessions per communication frequency on each transmitter for each jammer carrier frequency.

After data collection, for RFF, we generated images using $K = 10^5$ IQ samples, with image dimensions set to $225 \times 225 \times 3$, aligning with the image size in the ImageNet database in MATLAB 2024a. Then, for the multi-class classification, we split the dataset into 60% for training, 20% for validation, and 20% for testing, and we used the CNN resnet18 for classification, in line with recent relevant scientific contributions on RFF [24], [19].

Analysis of out-of-band interferences. In the following, we present the results of our investigation by resorting to two metrics, i.e., the average BER of the communication link and the average accuracy of the considered RFF technique. Firstly, we consider the five (5) transmitters in an interference-free environment to assess the (best) performance of the considered RFF technique. Table II shows the average accuracy of the CNN *ResNet-18*, denoting the capability of the RFF system to identify each of the five(5) radios in our pool when such radios transmit on three different reference frequencies, i.e., 1 GHz, 2.4 GHz, and 3 GHz. We observe that the accuracy is always higher than 0.96. Thus, the considered RFF technique can detect and identify each of the transmitters in the radio spectrum from PHY-layer data.

Fig. 4, 5, and 6 show the results of our analysis for the three reference frequencies considered in this work, i.e., 1 GHz, 2.4 GHz, and 3 GHz, respectively. We obtained the results in each figure by setting the communication frequency between the transmitter and the receiver to the reference frequency and then by sweeping the jammer frequency as indicated in the x-axis of the figures. Firstly, we observe that a Gaussian noise jammer featuring a baseband of 2 MHz affects the quality of the communication link (on average) in the range $[-3, +3]$ MHz with respect to the reference frequency. Thus, the modulated noise signal is characterized by a passband of about 6 MHz —this phenomenon being the result of the side

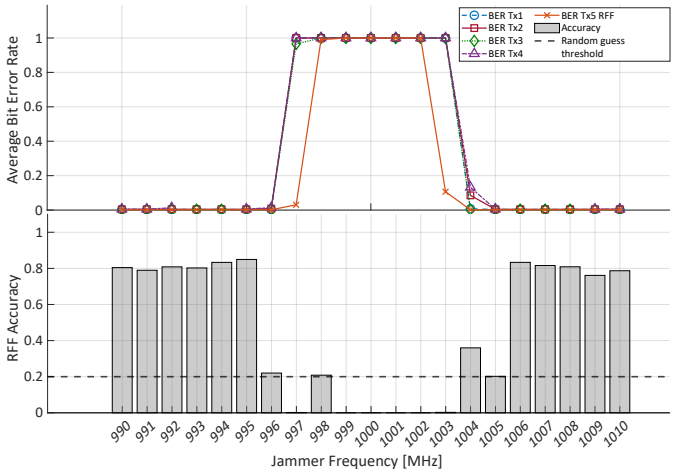

Fig. 4. BER (top) and Accuracy of RFF (bottom) as a function of the jammer frequency, with communication frequency at 1 GHz and jammer sweeping between 990 MHz and 1010 MHz.

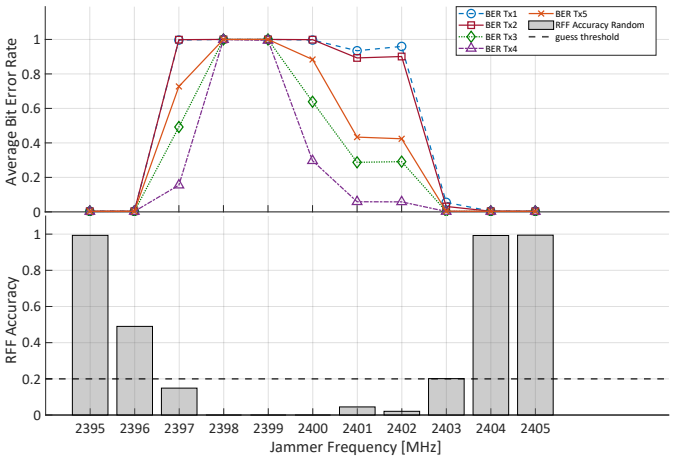

Fig. 5. BER (top) and Accuracy of RFF (bottom) as a function of the jammer frequency, with communication frequency at 2.4 GHz and jammer sweeping between 2395 MHz and 2405 MHz.

lobes of the modulated noise signal.

In such an area, the BER is equal to 1, and communication between the transmitter and the receiver is prevented. Outside that frequency range, when BER is equal to zero, the accuracy of the RFF is always between 0.8 and 1. This latter represents our ground truth and confirms that our RFF system works effectively.

We stress that the actual behavior of the interference in the RF domain (bandwidth amplitude being equal to 6 MHz) is out of the scope of this work while we focus on the analysis of the edges. Indeed, the most interesting phenomenon occurs at the edge of the range previously discussed when the BER changes from 0 to 1 and vice versa. Notably, there are frequencies where both the BER and the RFF accuracy are low. A few examples are 996 MHz and 1004 MHz (1 GHz, Fig. 4), 2396 MHz and 2403 MHz (2.4 GHz, Fig. 5), and finally, 3004 MHz (3 GHz, Fig. 6). At such frequencies, the high quality of the link (low BER) is not a sufficient condition to

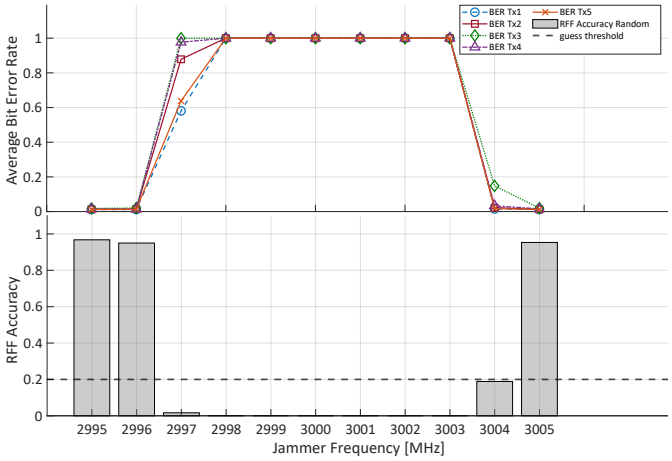

Fig. 6. BER (top) and Accuracy of RFF (bottom) as a function of the jammer frequency, with communication frequency at 3 GHz and jammer sweeping between 2995 MHz and 3005 MHz.

justify the performance of the RFF. Despite certain exceptions influenced by channel conditions and device stability (e.g., frequencies 998 MHz and 1005 MHz), we claim, based on these results, that low BER is a necessary but not sufficient condition to perform successful RFF.

VII. Conclusions

In this work, we have investigated the impact of in-band and out-of-band interferences on the performance of Radio Frequency Fingerprinting. RFF is an ephemeral phenomenon that can be observed under specific conditions and involving the configuration of the radio, the channel, and the classifier parameters. Our analysis, supported by real-world measurements, proves that high-quality link is a necessary but not sufficient condition to perform a successful RFF. Indeed, an out-of-band interference (jammer) might not affect the quality of the link, i.e., BER close to zero, but it could significantly hinder the ability of the receiver to detect and extract radio fingerprints, i.e., RFF accuracy close to a random guess of the transmitter, thus preventing the identification of the transmitter. Our analysis, performed at different frequencies in the radio spectrum (1 GHz, 2.4 GHz and 3 GHz), highlights the presence of a transition region in the radio spectrum where both the BER and the accuracy are almost zero, thus confirming that a high-quality link cannot always be considered for RFF. Future research will further investigate this phenomenon by examining the impact of different types of interfering signals and their transmission power on RFF, as well as conducting an in-depth analysis of the multi-path effect.

Acknowledgment

This work was supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, Mission 4, Component 2, in the context of partnership on “Telecommunications of the Future” (PE00000001 - program “RESTART”, CUP:D93C22000910001), national center on “Sustainable Mobility” (CN00000023-program “MOST”, CUP: D93C22000410001), and partnership on “Cybersecurity” (PE00000007 - program “SERICS”, CUP:D33C22001300002, project ISP5G+). It was also supported by the PRIN 2022 projects INSPIRE (grant no. 2022BEXMXN 01) and HORUS (grant no. 2022P44KA8) funded by the Italian MUR, by the HORIZON MSCA project BRIDGITISE (grant no. 101119554), and by “The house of emerging technologies of Matera (CTEMT)” project funded by the Italian MIMIT.

References

[1] Q. Lu, et al., “MRFE: A deep-learning-based multidimensional radio frequency fingerprinting enhancement approach for iot device identification,” *IEEE Internet of Things Journal*, 2024.
[2] S. Al-Hazbi, et al., “Radio frequency fingerprinting via deep learning: Challenges and opportunities,” in *2024 International Wireless Communications and Mobile Computing (IWCMC)*, 2024.
[3] A. Jagannath, et al., “A comprehensive survey on radio frequency (RF) fingerprinting: Traditional approaches, deep learning, and open challenges,” *Computer Networks (Elsevier)*, 2022.
[4] N. Soltanieh, et al., “A Review of Radio Frequency Fingerprinting Techniques,” *IEEE Journal of Radio Frequency Identification*, 2020.
[5] A. Al-Shawabka, et al., “Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting,” in *IEEE Conference on Computer Communications*, 2020.
[6] H. Fu, et al., “Deep learning-based rf fingerprint identification with channel effects mitigation,” *IEEE Open Journal of the Communications Society*, 2023.
[7] S. Alhazbi, et al., “The Day-After-Tomorrow: On the performance of radio fingerprinting over time,” in *Proc. of ACSAC*, 2023.
[8] ——, “BloodHound: Early Detection and Identification of Jamming at the PHY-layer,” in *IEEE Consum. Commun. & Network. Conf.*, 2023.
[9] S. Sciancalepore, et al., “Jamming detection in low-ber mobile indoor scenarios via deep learning,” *IEEE Internet of Things Journal*, 2024.
[10] M. Irfan, et al., “Jamming Detection in Power Line Communications Leveraging Deep Learning Techniques,” in *Int. Symp. on Networks, Computers and Communications (ISNCC)*, 2023.
[11] T. S. Rappaport, *Wireless communications: principles and practice*. Cambridge University Press, 2024.
[12] H. He, et al., “Deep learning-based channel estimation for beamspace mmwave massive mimo systems,” *IEEE Wirel. Commun. Lett.*, 2018.
[13] J. Xie, et al., “Activity Pattern Aware Spectrum Sensing: A CNN-Based Deep Learning Approach,” *IEEE Commun. Lett.*, 2019.
[14] Y. Dong, et al., “Weighted feature fusion of convolutional neural network and graph attention network for hyperspectral image classification,” *IEEE Transactions on Image Processing*, 2022.
[15] A. Hermawan, et al., “CNN-Based Automatic Modulation Classification for Beyond 5G Communications,” *IEEE Commun. Lett.*, 2020.
[16] A. Younesi, et al., “A Comprehensive Survey of Convolutions in Deep Learning: Applications, Challenges, and Future Trends,” *IEEE Access*, 2024.
[17] A. Al-Shawabka, et al., “Exposing the Fingerprint: Dissecting the Impact of the Wireless Channel on Radio Fingerprinting,” in *IEEE INFOCOM*, 2020.
[18] B. Hamdaoui, et al., “Deep-learning-based device fingerprinting for increased lora-iot security: Sensitivity to network deployment changes,” *IEEE Network*, 2022.
[19] G. Oligeri, et al., “PAST-AI: Physical-layer authentication of satellite transmitters via deep learning,” *IEEE Trans. on Inf. Forens. and Secur.*, 2023.
[20] M. Irfan, S. Sciancalepore, and G. Oligeri, “On the Reliability of Radio Frequency Fingerprinting,” *arXiv preprint arXiv:2408.09179*, 2024.
[21] G. Oligeri, et al., “SatPrint: Satellite Link Fingerprinting,” in *ACM Symp. on Applied Comput.*, 2024.
[22] A. Sadighian, et al., “FadePrint: Satellite Spoofing Detection via Fading Fingerprinting,” in *IEEE Consum. Commun. & Netw. Conf.*, 2024.
[23] O. Russakovsky, et al., “ImageNet Large Scale Visual Recognition Challenge,” *International journal of computer vision*, 2015.
[24] L. Papangelo, et al., “Adversarial Machine Learning for Image-Based Radio Frequency Fingerprinting: Attacks and Defenses,” *IEEE Commun. Magaz.*, 2024.