Article

Bluetooth Device Identification Using RF Fingerprinting and Jensen-Shannon Divergence

Rene Francisco Santana-Cruz , Martin Moreno-Guzman , César Enrique Rojas-López ,
Ricardo Vázquez-Morán , Rubén Vázquez-Medina *

Posted Date: 29 January 2024

doi: 10.20944/preprints202401.1955.v1

Keywords: Identification systems; Radio Frequency Fingerprints (RFF); IoT device identification; Cybersecurity; Wireless Communication

Article

Bluetooth Device Identification Using RF Fingerprinting and Jensen-Shannon Divergence

Rene Francisco Santana-Cruz [1], **Martin Moreno** [2], **César Enrique Rojas-López** [3], **Ricardo Vázquez-Morán** [3] and **Rubén Vázquez-Medina** [1,*]

[1] Instituto Politécnico Nacional, Centro de Investigación en Ciencia Aplicada y Tecnología Avanzada, Unidad Querétaro, 76090 Querétaro, Mexico
[2] Universidad Tecnológica de San Juan del Río, San Juan del Río, 76800 Querétaro, Mexico
[3] Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánia y Eléctrica, Unidad Culhuacan, 04440 Mexico City, Mexico
* Correspondence: ruvazquez@ipn.mx

Abstract: The proliferation of radio frequency devices in today's society, especially in smart homes, Internet of Things devices, and smartphones, underscores the urgent need for robust identification methods to strengthen cybersecurity. This paper delves into the field of radio frequency fingerprinting to propose a Bluetooth device identification method based on the application of the Jensen-Shannon divergence to the statistical distribution of noise in Bluetooth signals. A detailed case study is performed to investigate the Bluetooth radio frequency noise recorded at 5 Gsps from different devices is investigated to define a statistical radio frequency fingerprint for each Bluetooth device. A noise model is used to extract a unique, universal, persistent, recoverable, and robust statistical radio frequency fingerprint that identifies each Bluetooth device. Then, using the Jensen-Shannon divergence, different noise signals provided by each Bluetooth device are compared with the statistical radio frequency fingerprint of all devices and a membership resolution is declared. The study shows that the proposed method can discriminate between devices of the same brand and model, achieving an identification effectiveness of 99.5 %. By leveraging the statistical radio frequency fingerprint of Bluetooth devices, this research not only contributes to the advancement of the field of implicit device authentication systems based on wireless communication but also provides valuable insights into the practical implementation of radio frequency identification techniques that could be useful in forensic processes.

Keywords: identification systems; radio frequency fingerprints (RFF); IoT device identification; cybersecurity; wireless communication

1. Introduction

In the technology-driven world, radio frequency (RF) Bluetooth devices have become an integral part, enabling seamless communication in smartphones, smartwatches, and Internet of Things (IoT) devices [1,2]. In this context, accurate identification of devices is critical to provide security and effective management of network services [3]. Bluetooth technology, which operates in the 2.4 GHz band reserved for industrial, scientific, and medical purposes (ISM band), uses RF signals for short-range communication [4], making it ubiquitous in personal area networks and IoT applications [5,6]. However, the widespread use of Bluetooth poses challenges in distinguishing individual devices within the crowded RF spectrum, requiring advanced identification techniques based on machine learning, signal spectral analysis, or statistical analysis approaches.

The machine learning approach uses algorithms such as support vector machines (SVMs), random forests, and deep learning to improve the quality of the RF device identification process [7–25]. SVMs excel in classification tasks and provide reliable identification by recognizing unique RF fingerprints [7–13]. Random forests, known for their robustness, enhance classification accuracy [14]. Deep Learning, leveraging artificial neural networks, excels at complicated tasks such as classification and regression [15–25]. Machine learning techniques, while powerful, come with inherent complexities [7]. In this regard, the development and training of machine learning algorithms require specialized knowledge and expertise due to their intricate nature [8]. Moreover, their implementation often requires significant computational resources, making them challenging for applications with limited computing capabilities [19]. In addition, it is essential to collect a large data set of radio frequency signals from Bluetooth devices for effective training [17]. However, obtaining this data can be daunting and costly, posing a significant challenge to the use of machine learning for RF device identification [9]. These factors underscore the need for dedicated expertise, sufficient computational power, and meticulous data collection efforts in the realm of machine learning-based identification methods.

Signal spectral analysis methods, including swept-frequency, vector signal and real-time analysis schemes, are crucial for decoding and exploiting the complex RF signals emitted by Bluetooth devices [26]. Swept-frequency analysis precisely pinpoints the frequency band and power level of a device, providing nuanced insight. Vector signal analysis delves into amplitude, phase, and frequency, decoding modulation schemes and evaluating signal quality. Real-time analysis continuously monitors Bluetooth signals, providing dynamic feedback on signal stability and fluctuations. In addition, real-time analysis captures signal power, enabling continuous monitoring of RF signals from Bluetooth devices. These techniques provide dynamic insights that facilitate tracking of signal stability, fluctuations, and adaptive adjustments. In the field of wireless communications, these analyses are invaluable because they provide in-depth understanding, comprehensive analysis, and optimization of Bluetooth signals, ensuring efficient and reliable data transmission. In addition, these techniques involve a level of complexity that requires specialized training to ensure their effective use. This complexity underscores the need for skilled professionals who can utilize spectrum analysis tools to their full potential. Furthermore, the limitations of these techniques are evident in their dependence on the sensitivity and accuracy of the equipment used. The accuracy of the analysis highly dependent on the quality and capabilities of the equipment, so it is imperative to invest in high quality tools to obtain accurate results.

In statistical analysis, there are some tools based on probability theory that can be used to distinguish between two systems being analyzed in the time or spectral domains. For example, the Jensen-Shannon divergence (JSD) stands as a valuable statistical metric that measures the similarity between two probability distributions [27,28]. When applied to RF noise signals extracted from Bluetooth devices, JSD excels at detecting subtle statistical discrepancies in the signals, and thus its usefulness can be extended to a variety of tasks related to Bluetooth technology. As will be discussed later, JSD applied to noise signals in the Bluetooth frequency band can be used to distinguish devices by statistically comparing their RF fingerprints, enabling the development of secure authentication protocols and facilitating device tracking. In addition, JSD can be used to identify statistical deviations in the RF noise signals from Bluetooth devices when compared to a reference RF noise signal (RF fingerprint), enabling the location of compromised or malfunctioning devices for early intervention. By monitoring RF signal quality, JSD also helps troubleshoot Bluetooth device and network issues to ensure optimal performance.

A notable strength of the JSD when applied to the statistical comparison of noise signals for Bluetooth device identification is its resilience to signal variations, making it ideal for real-world scenarios where environmental conditions can be unpredictable. In addition, its computational efficiency allows for real-time discrimination of many devices, a crucial aspect in dynamic environments. To address the existing research gap on JSD applied to Bluetooth noise signals for device identification, comprehensive studies are needed to evaluate its performance on various datasets and under different environmental conditions.

This paper presents a comprehensive approach to the development of a Bluetooth device discrimination method. This method is based on a statistical criterion, specifically the application of the JSD to analyze the probability density function (PDF) of intrinsic noise and the statistical fingerprints extracted from Bluetooth devices. Considering the mentioned issues, the effectiveness of the proposed system needs to be evaluated and compared with the artificial intelligence based discrimination methods proposed by Uzundurukan *et al.* [9,17].

The rest of this paper is structured into six sections. Section 2 defines the five specifications for device fingerprints: uniqueness, universality, persistence, collectability, and robustness. These criteria ensure that each fingerprint is unique, applicable to a wide range of devices, stable over time, easy to collect and robust under various conditions. Section 3 delves into the specifics of Bluetooth signal processing. It covers the necessary steps such as signal filtering, state detection, and definition of the device RFF based on reference noise signals recorded under controlled conditions when the Bluetooth radio is turned on in each participating device. Section 4 presents a case study using the noise signal database developed by Uzundurukan *et al.* [9,17]. It introduces a criterion based on mean squared error (MSE) for determining the number of reference noise signals that must be evaluated to establish a device RFF. It also proposes a method to compensate for the amplitude difference in noise signals provided by the same device recorded by varying the distance between the receiver and the transmitter. This section concludes with a demonstration of the practical application of the estimated RF fingerprints for device discrimination using the JSD. Section 5 provides a critical analysis of the results, comparing the proposed discrimination method with Uzundurukan's method when applied to the same case study. Finally, section 6 gives the conclusions of this paper.

2. RF Fingerprint Specifications

The study of device identification based on RF fingerprints defined from noise signals in the Bluetooth frequency band has been a central topic in wireless communication research [7–25]. Numerous influential studies have significantly advanced on this topic, using various methods and innovative approaches to improve the precision and dependability of RF fingerprinting techniques [8,9,15,18,20,21,23,24]. A Bluetooth signal can be treated as an investigative object to identify potential threats or attacks. In this context, radio frequency fingerprinting (RFF) is a promising technique for secure device discrimination, identification or authentication. According to Soltanieh *et al.* [29], RFF methods are scrutinized against five fundamental specifications to ensure their efficacy and reliability as follows:

- **Uniqueness**. It ensures distinctiveness by preventing any two devices from sharing identical RFF, thus facilitating individual device identification.
- **Universality**. It guarantees unique RFF features for each device, providing complete coverage of all devices on a given network.
- **Persistence**. It requires the RFF to remain constant over time, unaffected by environmental fluctuations, ensuring stability and reliability in device identification.
- **Collectability**. It requires that the RFF be quantitatively measurable, allowing for accurate data analysis and device identification using rigorous measurement techniques.
- **Robustness**. It preserves the integrity of the RFF against environmental changes and device-related factors, ensuring consistent and reliable authentication regardless of varying conditions.

3. Bluetooth Signals for the Device Discrimination

This section presents a noise model of the Bluetooth signals, which lays the foundation of the analysis. Next, the details of model-based signal filtering are described, which is critical for limiting the broadband of Bluetooth signals. The highlight of this section is the construction of RF fingerprints for Bluetooth devices, which is essential for device discrimination.

3.1. Noise Model

The analysis of the noise model is defined as:

$$\eta = \eta_{Tx} + \eta_{Rx} \, , \tag{1}$$

This equation represents the total noise received, η, from a Bluetooth transmitter. The term η_{Tx} denotes the intrinsic noise from the transmitter under study, while η_{Rx} denotes the additional noise introduced from the receiver. This model is crucial for analyzing and understanding the characteristics of the composite noise in Bluetooth communication. Then, solving Eq. 1 yields Eq. 2, which is basic to isolate the transmitter-specific noise signal from the total noise.

$$\eta_{Tx} = \eta - \eta_{Rx} \, . \tag{2}$$

Figure 1 visually presents the noise model as described in Eq. 2. It is noteworthy that in the initial state, the noise is comes mainly from the receiver Rx. However, during the transient state, the transmitter Tx is activated, and total noise then embodies both the transmitter and receiver noise components. This transient state gradually stabilizes, reflecting the integration of Tx and Rx, and thus transitions to a stable state. This visual representation helps to understand the dynamic interaction between transmitter and receiver noise within the Bluetooth communication system.

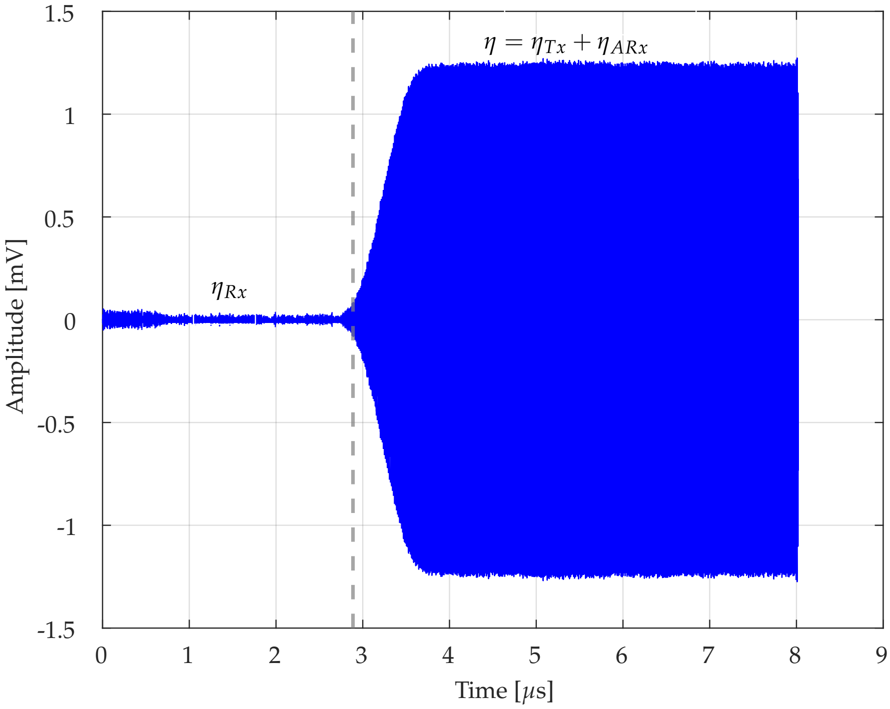

Figure 1. Noise model dynamics in Bluetooth communication systems.

This analysis describes the interaction between the intrinsic noise of the transmitter η_{Tx} and the additive noise from the receiver η_{Rx}, and their impact on the total noise η. It analyzes how noise dominance shifts from the receiver to the transmitter during a transitional phase, culminating in a combined transmitter-receiver noise state. This approach provides insight into the dynamics of noise in Bluetooth systems.

3.2. Signal Filtering

Because the signals received at the Bluetooth receiver span contain a variety of components over a wide frequency spectrum, it is required to apply a bandpass filter is needed. This filter is specifically designed to isolate and extract the Bluetooth ISM band from 2.4 GHz to 2.485 GHz (as depicted in Figure 2). In addition, the choice of sampling frequency for this process must adhere to the Nyquist theorem. This theorem states that the sampling frequency must be at least twice the highest frequency component of the signal in order to accurately reconstruct the signal without aliasing. Therefore, the sampling frequency was chosen to be equal to or greater than 4.97 GHz to ensure the integrity and fidelity of the Bluetooth signal. Note that Figure 2 shows two different signals. The first signal shows the wide range of frequencies in the original, unfiltered signal. The second signal shows the ISM band, illustrating how the bandpass filter narrows the frequencies down to only those present inside Bluetooth band.

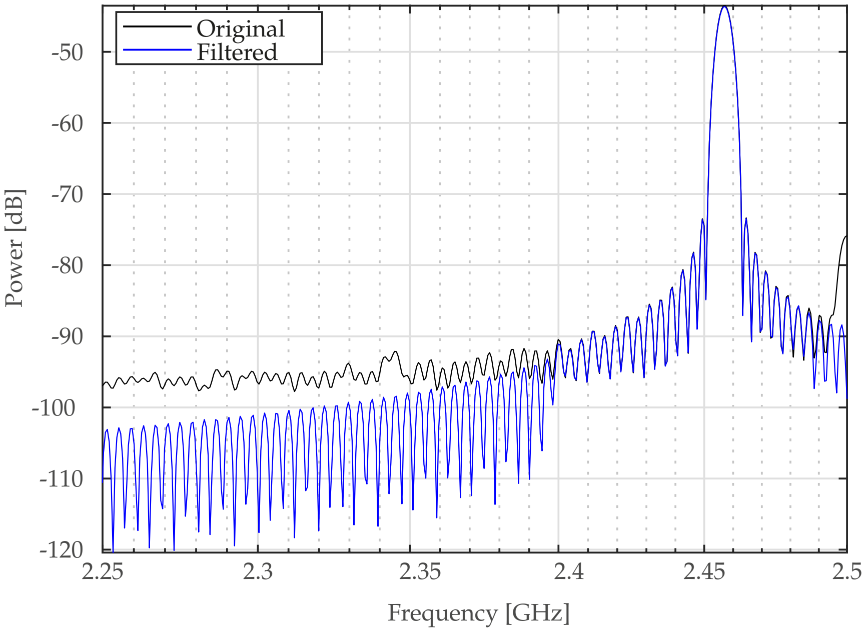

Figure 2. Spectral analysis of bandpass filtered signals in the frequency domain.

3.3. State Detection

Figure 3 provides a clear representation of the different states of a Bluetooth signal as it is received by a Bluetooth receiver. The signal is divided into three distinct parts: the initial state, the transient state, and the steady state. The transient state marks the transition of the signal from its initial state to a steady state. The transient state is identified by specific changes in the signal amplitude. It begins when the signal amplitude is just above its lowest level.

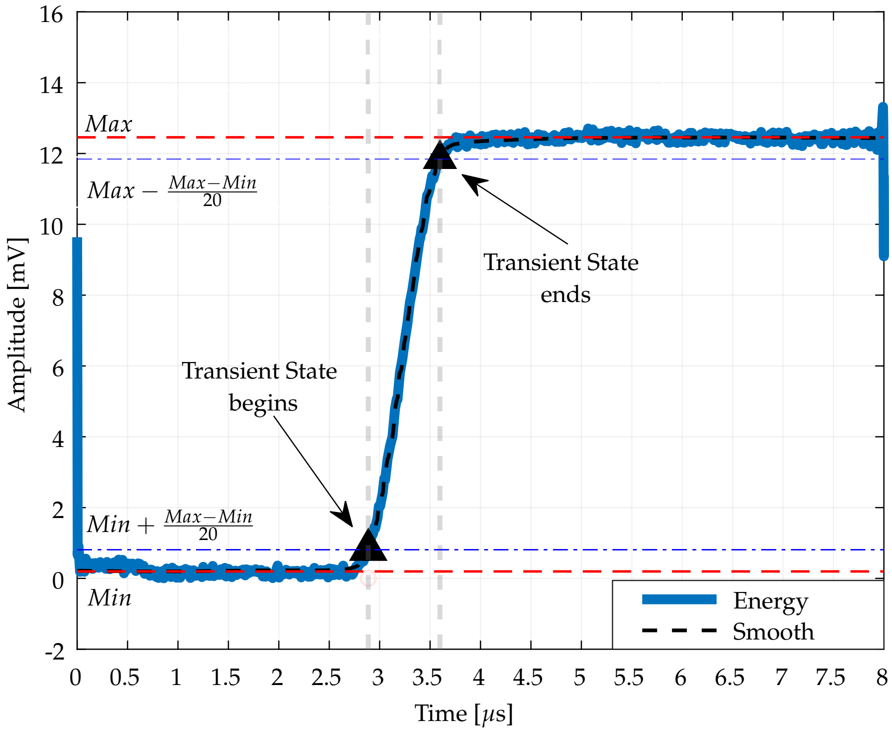

Figure 3. Quantitative assessment of signal state identification and detection from reference transient state.

This starting point is mathematically defined as $Min - \frac{Max-Min}{20}$, where Min and Max are the minimum and maximum values, respectively, of the smoothed envelope of the Bluetooth signal. In contrast, the end of the transient state is marked when the signals amplitude approaches, but does not quite reach, its maximum level. This end point is described by the expression $Max - \frac{Max-Min}{20}$. This expression helps to determine exactly when the signal goes from changing to reaching a steady state. In summary, Figure 3 is a tool for analyzing a Bluetooth signal, providing a guide to follow the progression of the signal through its initial, transient and steady states, with special emphasis on the transient state because of its significant effect in highlighting the change between the initial and steady states of the Bluetooth signal.

3.4. RF Fingerprints for Bluetooth Devices

To create the RF fingerprint, it is necessary to concatenate a set of noise signals extracted from the steady state of the RF signals at the Bluetooth receiver for each Bluetooth transmitter. This set of noise signals forms the noise reference signals, which are extracted from the Bluetooth signal at the receiver under the assumption that these signals are collected in a controlled experimental setup. For each noise signal in this set, its PDF is calculated. The median PDF, derived from the average of all calculated PDFs, constitutes the statistical RF fingerprint to be used in this work. It should be noted that each PDF of the noise signal is calculated using Eq. 2, and this process is visually demonstrated in Figure 4.

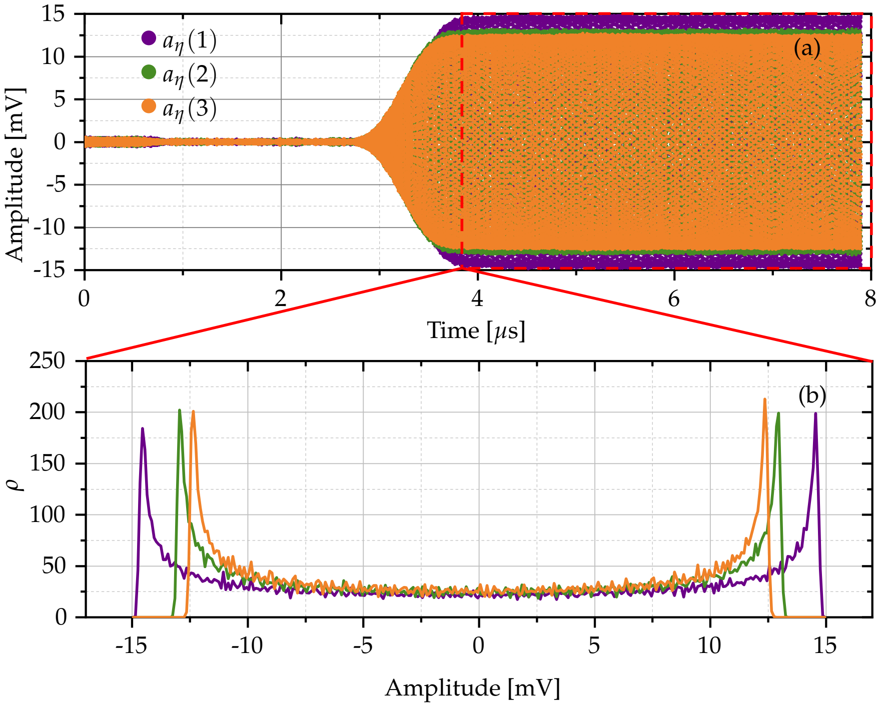

Figure 4. Steady state using three signals on a single device: a) Signal analysis in time domain, and b) PDF projection derived from (a).

In signal analysis, especially when dealing with noise reference signals in Bluetooth communication, a crucial step is to identify the optimal number of these signals needed for accurate analysis. This process is guided by the MSE criterion, a statistical method for evaluating the accuracy of signal representation. The method involves a comparative analysis of the PDF computed using n noise reference signals against the PDF obtained using $n+1$ noise reference signals. The aim here is to find the point at which increasing the number of signals does not significantly improve the accuracy of the PDF representation. However, the number of noise reference signals that are required should be determined. For this purpose, the MSE criterion was applied between PDF with n noise reference signals and PDF with $n+1$ noise reference signals. According to Figure 5, thirty noise reference signals were considered assuming that MSE is less than 3.5. Note in Figure 5a that the MSE has been calculated from n = 2 up to n = 100 and when $n \geq 30$, the MSE is very small compared to the initial values when $n < 30$. As depicted in Figure 5, a critical threshold is identified at 30 noise reference signals. This decision is based on the assumption that an MSE value of less than 3.5 is acceptable for accurate signal representation. When examining the MSE values for n ranging from 2 to 100, as shown in Figure 5a, a notable pattern emerges. It is observed that once the number of noise reference signals reaches 30 or more, the MSE decreases to a level significantly smaller than its values for $n < 30$. This implies that beyond the count of thirty signals, the gain in accuracy, as quantified by the MSE, reaches a plateau, suggesting that additional signals provide minimal improvement.

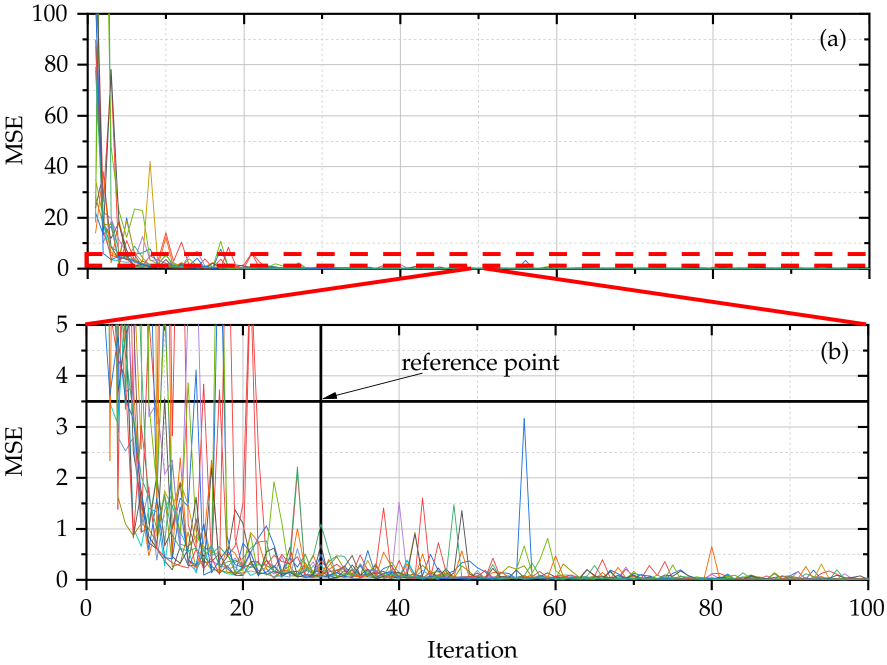

Figure 5. Convergence analysis of the estimated PDF by MSE comparison for n and $n+1$ noise signals. a) Analysis over the full signal range, and b) Detailed zoom in on (a).

4. Discrimination of Bluetooth devices

This section delves into the case study discussed and presents a basic scaling method for data analysis and interpretation. It also defines a statistical fingerprint to uniquely identify each device in the study. Using the Jensen-Shannon divergence, the devices are distinguished by their statistical fingerprints, and a detailed description of the methodological framework and the tools used in the analysis is provided.

4.1. Case Study

The study uses a comprehensive database of Bluetooth devices, prepared and compiled in 2020 by Uzundurukan *et al.* [17]. This database includes eight different models from four different brands of smartphones, as detailed in Table 1. The inclusion of multiple models and brands ensures a wide range of data, which helps to perform a comprehensive analysis.

Table 1. Bluetooth device models and brands used in the case study.

Brand	Model
iPhone	5
	5s
	6
	6s
LG	G4
Samsung	Note3
	S5
Sony	Xperia M5

In the database, each smartphone model is paired with a twin variant, leading to a total of sixteen devices. A significant number of signals, specifically one hundred and fifty unique signals per device, are available for analysis. All signals in the database were sampled at a high frequency (5 Gsps), ensuring the acquisition of high-resolution data. This results in a comprehensive collection of two thousand four hundred signals, providing a rich and varied dataset for the study.

doi:10.20944/preprints202401.1955.v1

4.2. Bluetooth Signal Matching

In this work, a statistical method is proposed for the definition of RFF for Bluetooth devices. Statistical characteristics, such as the mean or standard deviation, although commonly used, are often insufficient to provide insight into the behavior of a device. Therefore, the PDF is selected for further analysis. The PDFs calculated for three noise signals in the steady state from a single device are shown in Figure 4. This representation carefully considers the integration of receiver noise with the noise generated by the Bluetooth transmitter, providing a nuanced view of the signal characteristics unique to the device.

In order to minimize potential errors, a scaling method has been proposed, as detailed in the Eq. 3. It is designed to normalize the amplitude of signals received from different transmitters. In this framework, $a(i)$ is defined as the signal detected at the receiver by monitoring the transmitter i; $a_{MAX}(i)$ represents the maximum amplitude of $a(i)$ and $a_{MAX}(1)$ indicates the highest amplitude of $a(1)$. In particular, the transmitter signal 1, when monitored, is used as the reference point for scaling. Note, however, it should be noted that any other signal can be used as a reference in this scaling process.

$$a_e(i) = \frac{a(i)}{a_{MAX}(i)} \cdot a_{MAX}(1) \tag{3}$$

In graphs of Figure 6 can be noted a general overview of the used scaling method. Figure 6a shows a visual representation of the PDF of the three unique noise signals from a single Bluetooth device before of the scaling method has been applied. Note the inherent amplitude variation found between PDFs of noise signals of that device. However, Figure 6b demonstrates the result of the applying scaling. Note that the PDFs of the three unique noise signals are more uniform and consistent with each other, showing the ability of the method to standardize the signal characteristics.

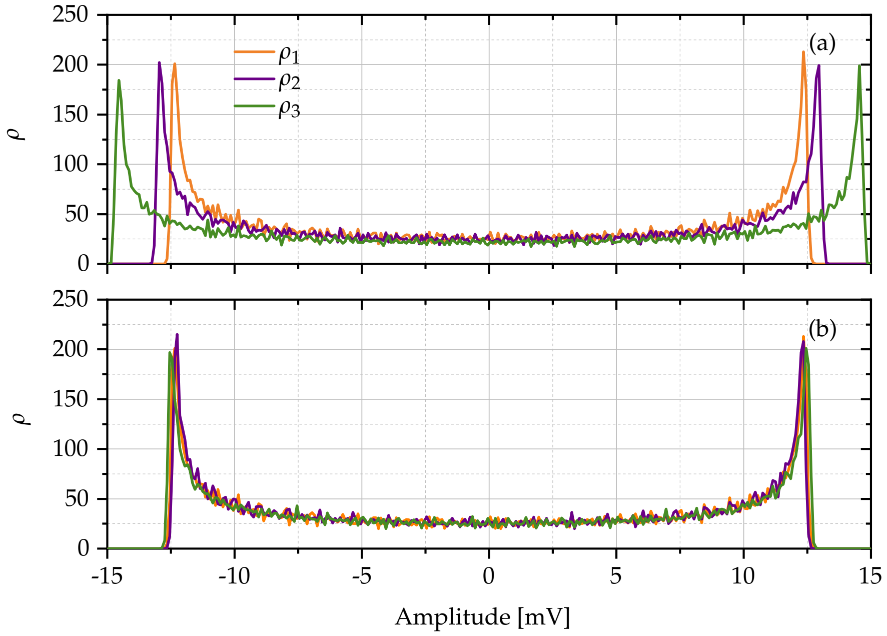

Figure 6. PDF of three noise signals from a single Bluetooth device. a) Before scaling and b) After scaling.

4.3. Statistical RFF for Case Study

Figure 7 illustrates the results obtained from the sixteen devices that were examined in the case study. It is important to note that only the positive part of the PDFs of the noise signals was considered. This decision is based on the bimodal and symmetric properties of these statistical distributions. It should be noted that each RFF associated with the devices is unique. This uniqueness of the RFFs accentuates the individual characteristics of each device signal, highlighting the distinctiveness and specificity that the RFF methodology brings to the analysis of device signals. This distinctiveness is useful for understanding and identifying the unique aspects of each noise signal profile within the broader context of the study.

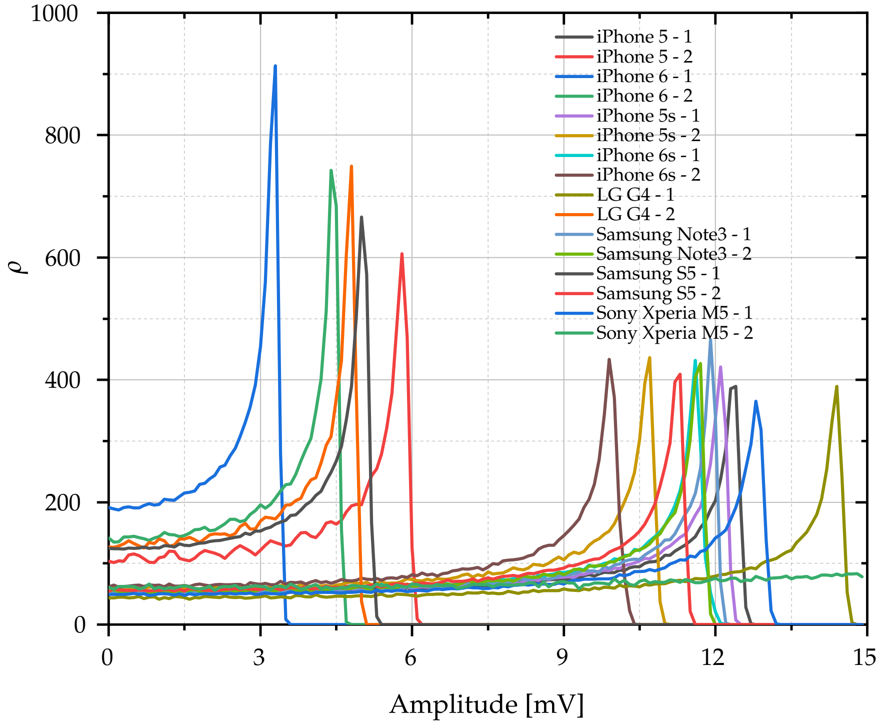

Figure 7. Characterization and analysis of unique RFF patterns from multiple Bluetooth devices.

4.4. Device Identification by Using Statistical RFF and JSD

For this work, the JSD was used to discriminate the Bluetooth devices in the process of defining a RFF for each, according to Section 3.4. An integral part of this methodology is the use of fifty dispute signals for each device in the discrimination process. The signal that provides the lowest Jensen-Shannon divergence, calculated according to equation 4, is then assigned to the respective device. The disputed PDF P is compared to the reference PDF, which is the RFF extracted from the noise component of the RF signal emitted by a device Q. Using the JSD given in Eq. 4 for this comparison ensures that disputed signals are assigned to their respective devices, thereby increasing the accuracy of device identification within the study.

$$JSD(P \parallel Q) = \frac{1}{2}KLD(P \parallel M) + \frac{1}{2}KLD(Q \parallel M)\,, \tag{4}$$

where $M = \frac{1}{2}(P+Q)$.

The findings of this research are presented in Table 2, which shows the confusion matrix derived from the case study. This matrix reveals an accuracy rate of 99.5 %. Within this matrix, a notable discrepancy is observed, with an 8% error rate in distinguishing between devices twelve and seven. This specific issue is further explored in Figure 7, which shows the RFF of both devices, in addition to a signal that was wrong assigned to the incorrect device.

The cause of this misattribution can be attributed to the peculiarities of the disputed signal. In particular, its oscillation pattern appears to be the key factor in the error. This pattern differs significantly from the standard patterns observed in the RFFs of these devices. Normally, RFFs are expected to be consistent and distinctive for each device, allowing accurate identification. However, when a signal exhibits atypical patterns, such as unique oscillations that are not characteristic of the device's standard RFF, it can lead to misidentification.

Table 2. Confusion matrix from the results obtained using the proposed method.

		Predicted device															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Real device	1	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	2	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	3	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	4	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	5	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	6	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	7	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.08	0.00	0.00	0.00	0.00
	8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	9	0.00	0.00	0.00	0.00	0.00	0.000	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
	11	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
	12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.92	0.00	0.00	0.00	0.00
	13	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00
	14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00
	15	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
	16	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00

5. Discussions and Comparisons

In this section, the discussion focuses on the analysis of the results obtained in the previous section of the study. The aim is to delve deeper into the findings and provide a deep understanding of their implications and meaning within the context of the study. The methodological approach and results of Uzundurukan *et al.* will also be examined in detail in the next section.

5.1. Discussion

The results achieved in this study strengthen the concept of developing systems for authenticating individuals using mobile devices identified within an IoT network. In this context, the findings facilitate the creation of algorithms tailored to uniquely identify devices. These algorithms are capable of identifying devices in IoT networks using unique identifiers such as MAC addresses, communication patterns, or unique signatures/fingerprints that are both universal and unique to each device. Such technological advances are crucial to strengthening the security of networked environments, where the accurate authentication and identification are essential to prevent unauthorized access and to maintain network integrity, thereby guaranteeing the security and reliability of interconnected systems.

5.2. Device Identification by Uzundurukan's Method

A comprehensive comparison is made between the results obtained with the proposed method and with Uzundurukan's method applied to the case study defined in Section 4.3. This comparison not only evaluates the effectiveness but also takes into account the implementation time, which includes the resources and time required for both the training process and the identification phase. According to Uzundurukan *et al.* [9,17], the Uzundurukan's method uses a nonlinear support vector machine (SVM) with a quadratic kernel, and it applies a process to scale the amplitude of the noise signals similar to that used in the proposed method and detailed in Section 4.2. Although they reported that their SVM-based method achieved an accuracy rate of 97.9%, it could be determined that this accuracy rate was 80.13% when applied to the case study mentioned in Section 4.1. These results, shown in Table 3, allowed us to establish a baseline for the comparative analysis. The discrepancy found could be attributed to the fact that the original method uses the transient state of the noise signals, while the current application focuses on their steady state. First, it is assumed that the noise signal extracted from the transient state is analyzed against the RFF using a SVM. The discrimination process of the RFF consists of two main stages: a) *training phase*, in which the SVM model is applied to a dataset representative of the noise signal using the transient state of the noise signals, allowing the SVM model to learn and adapt, and b) *discrimination phase*, in which the trained RFF is used to analyze new signals and evaluate their congruence with the trained model. This bifurcated methodology, which integrates both training and practical application, facilitates effective device identification.

Table 3. Confusion matrix from the Uzundurukan's method results.

		Predicted device															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Real device	1	0.57	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.17	0.00	0.00	0.03	0.00
	2	0.00	0.13	0.00	0.00	0.00	0.00	0.00	0.00	0.10	0.00	0.00	0.00	0.03	0.00	0.00	0.00
	3	0.03	0.00	0.97	0.03	0.03	0.00	0.00	0.00	0.00	0.03	0.00	0.03	0.00	0.00	0.00	0.00
	4	0.00	0.03	0.03	0.77	0.00	0.00	0.00	0.00	0.00	0.37	0.00	0.00	0.00	0.00	0.00	0.00
	5	0.00	0.00	0.00	0.00	0.90	0.10	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	6	0.10	0.00	0.00	0.00	0.03	0.77	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.10	0.00
	7	0.00	0.00	0.00	0.00	0.00	0.00	0.93	0.00	0.00	0.00	0.00	0.13	0.00	0.00	0.00	0.00
	8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	9	0.00	0.77	0.00	0.03	0.03	0.00	0.00	0.00	0.87	0.10	0.00	0.00	0.10	0.00	0.00	0.00
	10	0.00	0.00	0.00	0.17	0.00	0.00	0.00	0.00	0.03	0.50	0.00	0.00	0.00	0.00	0.00	0.00
	11	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
	12	0.23	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.67	0.00	0.00	0.00	0.00
	13	0.00	0.07	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.87	0.00	0.00	0.00
	14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00
	15	0.03	0.00	0.00	0.00	0.00	0.07	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.87	0.00
	16	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00

6. Conclusions

This study concludes that the RFF can be accurately defined by using the PDF of RF noise signals, which are carefully collected from each Bluetooth device in a well-controlled laboratory environment. The statistically derived RFFs satisfy the fundamental characteristics of a device fingerprint, including aspects such as uniqueness, universality, persistence, collectability, and robustness. In addition, the application of Jensen-Shannon divergence to the PDFs of noise signals, especially in the steady state of the RF signal received by the Bluetooth receiver, and their subsequent comparison with the RFFs of corresponding Bluetooth devices has proven effective for device classification. The proposed statistical classifier shows promise for broad applicability across different radio frequency technologies, requiring only the computation of statistical distributions of noise signals according to their operating frequency bands. The results of this study clearly highlight the improved efficiency of the proposed statistical method compared to the machine learning approach advocated by Uzundurukan *et al.* [9]. Remarkably, the statistical classifier achieves a processing time of only 0.21 seconds, significantly outperforming the machine learning method based on a nonlinear SVM, which requires about 5.35 seconds. This significant discrepancy in processing time underscores the exceptional speed and computational efficiency of the statistical model, making it particularly advantageous for scenarios requiring rapid data processing. The findings in this work underscore the practical utility of the statistical methodology, especially in situations where time-sensitive data processing is essential for decision making or real-time applications. The efficiency of the statistical classifier, as evidenced by its fast computational capabilities, also makes it a viable option for resource-intensive tasks. This study not only reaffirms the importance of considering processing speed in the selection of analytical methods, but also contributes valuable insights to the field of data analysis, underscoring the importance of using statistical techniques for efficient data-driven solutions in various contexts.

Funding: Authors thank to the Instituto Politécnico Nacional (IPN-México) for the financial support granted through project SIP–20240745 (R. Vázquez–Medina).

Acknowledgments: R. F. Santana-Cruz (CVU 1242157) thanks to CONAHCYT-Mexico and C. E. Rojas-López thanks to COTEBAL-IPN for the financial support granted by the Postgraduate Scholarship.

Conflicts of Interest: The authors declare no conflict of interest. The founders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Math-Semicolon Tutor.* **2015**, *17*, 2347–2376. https://doi.org/10.1109/COMST.2015.2444095.
2. Gomathi, R.M.; Krishna, G.H.S.; Brumancia, E.; Dhas, Y.M. A survey on IoT technologies, evolution and architecture **2018**. https://doi.org/10.1109/ICCCSP.2018.8452820.
3. Schiller, E.; Aidoo, A.; Fuhrer, J.; Stahl, J.; Ziörjen, M.; Stiller, B. Landscape of IoT security. *Computer Science Review* **2022**, *44*, 100467. https://doi.org/10.1016/j.cosrev.2022.100467.
4. Bisdikian, C. An overview of the Bluetooth wireless technology. *IEEE Communications Magazine* **2001**, *39*, 86–94. https://doi.org/10.1109/35.968817.
5. Pau, G.; Arena, F.; Gebremariam, Y.E.; You, I. Bluetooth 5.1: An analysis of direction finding capability for high-precision location services. *Sensors* **2021**, *21*, 3589. https://doi.org/10.3390/s21113589.
6. Callebaut, G.; Leenders, G.; Mulders, J.V.; Ottoy, G.; Strycker, L.D.; der Perre, L.V. The art of designing remote IoT devices—technologies and strategies for a long battery life. *Sensors* **2021**, *21*, 913. https://doi.org/10.3390/s21030913.
7. Zamora, G.O.; Bergin, S.; Kennedy, I.O. Using support vector machines for passive steady state RF fingerprinting **2009**. pp. 183–188. https://doi.org/10.1007/978-90-481-3662-9_31.
8. Zhang, Z.; Guo, X.; Lin, Y. Trust Management Method of D2D Communication Based on RF Fingerprint Identification. *IEEE Access* **2018**, *6*, 66082–66087. https://doi.org/10.1109/ACCESS.2018.2878595.
9. Uzundurukan, E.; Ali, A.M.; Dalveren, Y.; Kara, A. Performance analysis of modular RF front end for RF fingerprinting of Bluetooth devices. *Wireless Personal Communications* **2020**, *112*, 2519–2531. https://doi.org/10.1007/s11277-020-07162-z.
10. Reus-Muns, G.; Jaisinghani, D.; Sankhe, K.; Chowdhury, K.R. Trust in 5G open RANs through machine learning: RF fingerprinting on the Powder Pawr platform **2020**. https://doi.org/10.1109/GLOBECOM42002.2020.9348261.
11. Aghnaiya, A.; Dalveren, Y.; Kara, A. On the performance of variational mode decomposition-based radio frequency fingerprinting of Bluetooth devices. *Sensors* **2020**, *20*, 1704. https://doi.org/10.3390/s20061704.
12. Reising, D.; Cancelleri, J.; Loveless, T.D.; Kandah, F.; Skjellum, A. Radio identity verification-based IoT security using RF-DNA fingerprints and SVM. *IEEE Internet of Things Journal* **2021**, *8*, 8356–8371. https://doi.org/10.1109/JIOT.2020.3045305.
13. Shi, J.; Lu, S.; Zhang, J.; Zhou, P.; Yang, F.; Gao, Y.; Wu, H.; Feng, W. A radio frequency fingerprint identification method for wireless devices based on ShuffleNet-SVM **2022**. https://doi.org/10.1109/ICCC56324.2022.10065708.
14. Ji, W.; Zhao, K.; Zheng, Z.; Yu, C.; Huang, S. Multivariable fingerprints with random forest variable selection for indoor positioning system. *IEEE Sensors Journal* **2022**, *22*, 5398–5406. https://doi.org/10.1109/JSEN.2021.3103863.
15. Yu, J.; Hu, A.; Li, G.; Peng, L. A robust RF fingerprinting approach using multisampling convolutional neural network. *IEEE Internet of Things Journal* **2019**, *6*, 6786–6799. https://doi.org/10.1109/JIOT.2019.2911347.
16. Ali, A.M.; Uzundurukan, E.; Kara, A. Assessment of features and classifiers for Bluetooth RF fingerprinting. *IEEE Access* **2019**, *7*, 50524–50535. https://doi.org/10.1109/ACCESS.2019.2911452.
17. Uzundurukan, E.; Dalveren, Y.; Kara, A. A database for the radio frequency fingerprinting of Bluetooth devices. *Data* **2020**, *5*, 55. https://doi.org/10.3390/data5020055.
18. Jian, T.; Rendon, B.C.; Ojuba, E.; Soltani, N.; Wang, Z.; Sankhe, K.; Gritsenko, A.; Dy, J.; Chowdhury, K.; Ioannidis, S. Deep learning for RF fingerprinting: A massive experimental study. *IEEE Internet of Things Magazine* **2020**, *3*, 50–57. https://doi.org/10.1109/IOTM.0001.1900065.
19. Robinson, J.; Kuzdeba, S.; Stankowicz, J.; Carmack, J.M. Dilated causal convolutional model for RF fingerprinting **2020**. https://doi.org/10.1109/CCWC47524.2020.9031257.
20. Wang, S.; Peng, L.; Fu, H.; Hu, A.; Zhou, X. A convolutional neural network-based RF fingerprinting identification scheme for mobile phones **2020**. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9163058.
21. Lee, W.; Baek, S.Y.; Kim, S.H. Deep-learning-aided RF fingerprinting for NFC security. *IEEE Communications Magazine* **2021**, *59*, 96–101. https://doi.org/10.1109/MCOM.001.2000912.

22. Li, B.; Cetin, E. Waveform domain deep learning approach for RF fingerprinting **2021**. https://doi.org/10.1109/ISCAS51556.2021.9401486.
23. Qing, G.; Wang, H.; Zhang, T. Radio frequency fingerprinting identification for zigbee via lightweight CNN. *Physical Communication* **2021**, *44*, 101250. https://doi.org/10.1016/j.phycom.2020.101250.
24. Zeng, Y.; Gong, Y.; Liu, J.; Lin, S.; Han, Z.; Cao, R.; Huang, K.; Letaief, K.B. Multi-Channel Attentive Feature Fusion for Radio Frequency Fingerprinting. *IEEE Transactions on Wireless Communications* **2023**, pp. 1–1. https://doi.org/10.1109/TWC.2023.3316286.
25. Batres, A.E.; Ouarab, T.; Talbi, L. Passive radio localization system using channel impulse response and deep learning **2023**. https://doi.org/10.1109/iEECON56657.2023.10126633.
26. Grimaldi, S.; Mahmood, A.; Gidlund, M. Real-time interference identification via supervised learning: Embedding coexistence awareness in IoT devices. *IEEE Access* **2019**, *7*, 835–850. https://doi.org/10.1109/ACCESS.2018.2885893.
27. Menéndez, M.L.; Pardo, J.A.; Pardo, L.; Pardo, M.C. The Jensen-Shannon divergence. *Journal of the Franklin Institute* **1997**, *334*, 307–318. https://doi.org/10.1016/S0016-0032(96)00063-4.
28. Tsai, S.C.; Tzeng, W.G.; Wu, H.L. On the Jensen–Shannon divergence and variational distance. *IEEE Transactions on Information Theory* **2005**, *51*, 3333–3336. https://doi.org/10.1109/TIT.2005.853308.
29. Soltanieh, N.; Norouzi, Y.; Yang, Y.; Karmakar, N.C. A review of radio frequency fingerprinting techniques. *IEEE Journal of Radio Frequency Identification* **2020**, *4*, 222–233. https://doi.org/10.1109/JRFID.2020.2968369.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.