electronics

MDPI

Article

Deployment and Implementation Aspects of Radio Frequency Fingerprinting in Cybersecurity of Smart Grids

Maaz Ali Awan [1], Yaser Dalveren [1], Ferhat Ozgur Catak [2,*] and Ali Kara [3,*]

[1] Department of Electrical and Electronics Engineering, Atilim University, Ankara 06830, Turkey; awan.maaz@student.atilim.edu.tr (M.A.A.); yaser.dalveren@atilim.edu.tr (Y.D.)
[2] Electrical Engineering and Computer Science, University of Stavanger, 4021 Rogaland, Norway
[3] Department of Electrical and Electronics Engineering, Gazi University, Ankara 06570, Turkey
* Correspondence: f.ozgur.catak@uis.no (F.O.C.); akara@gazi.edu.tr (A.K.)

Abstract: Smart grids incorporate diverse power equipment used for energy optimization in intelligent cities. This equipment may use Internet of Things (IoT) devices and services in the future. To ensure stable operation of smart grids, cybersecurity of IoT is paramount. To this end, use of cryptographic security methods is prevalent in existing IoT. Non-cryptographic methods such as radio frequency fingerprinting (RFF) have been on the horizon for a few decades but are limited to academic research or military interest. RFF is a physical layer security feature that leverages hardware impairments in radios of IoT devices for classification and rogue device detection. The article discusses the potential of RFF in wireless communication of IoT devices to augment the cybersecurity of smart grids. The characteristics of a deep learning (DL)-aided RFF system are presented. Subsequently, a deployment framework of RFF for smart grids is presented with implementation and regulatory aspects. The article culminates with a discussion of existing challenges and potential research directions for maturation of RFF.

Keywords: radio frequency fingerprinting; machine learning; deep learning; software-defined radio; Internet of Things; cybersecurity; smart city; smart grid

Citation: Awan, M.A.; Dalveren, Y.; Catak, F.O.; Kara, A. Deployment and Implementation Aspects of Radio Frequency Fingerprinting in Cybersecurity of Smart Grids. *Electronics* **2023**, *12*, 4914. https://doi.org/10.3390/electronics12244914

Academic Editors: Dariusz Rzońca and Tomasz Rak

Received: 23 October 2023
Revised: 30 November 2023
Accepted: 4 December 2023
Published: 6 December 2023

1. Introduction

Over the past few years, smart cities have experienced substantial growth and expanded their horizon considerably. Notably, recent breakthroughs in IoT have opened exciting avenues, serving as pivotal technological foundations for smart cities [1]. These advancements facilitate the creation and automation of cutting-edge services and sophisticated applications tailored to the diverse needs of urban communities, thus benefiting a wide range of city stakeholders. Figure 1 illustrates key components of a modern smart city.

Complementary to these advancements, smart grids are transformative for smart cities, optimizing energy usage in real time and pre-empting potential problems [2]. Smart grids are an essential national asset for any country, playing a crucial role in modernizing energy infrastructure. Traditional power grids comprise power generation, transformation, transmission, and distribution. Smart grids incorporate diverse power equipment and may incorporate IoT devices that sense humidity, temperature, immersion, vibration, current leakage, and record video data. Pointed IoT equipment may enable implementation of intelligent power systems [3–5]. These IoT devices establish wireless device-to-device (D2D) communication at the physical layer [6]. Each network has a gateway for data concentration which constitutes the network layer, and the control station serves the application layer of IoT in smart grids. While smart grids offer immense benefits to smart cities, they also present significant security challenges. A substantial review was conducted by Alsuwian et al. [7] concerning cybersecurity threats in IoT of smart grids. These networks in smart grids operate at the intersection of the physical layer, network layer, and application layer, making them susceptible to cyber threats at multiple levels. Therefore, their security at all

levels is paramount. The interconnected nature of smart grids entails that vulnerability at one layer may cascade across the entire system, potentially leading to widespread disruptions.

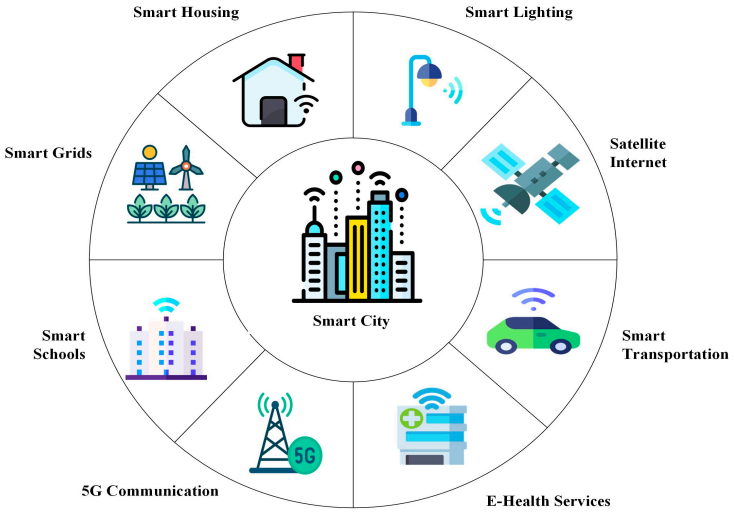

Figure 1. Concept of smart city [1].

Security requirements in a wireless network encompass several critical aspects to safeguard the integrity and privacy of data transmission [8]. Authenticity is paramount because unauthorized access is a major security concern, especially in life-critical IoT applications [9]. In existing IoT devices, coprocessors are employed for symmetric key-based encryption such as AES-128 and AES-256 [10]. However, maintenance of these keys is an administrative overhead and must be mitigated through the use of public/private key pairs [11]. Such pairs are mathematically correlated and allow for enhanced data security compared to symmetric cryptography. Nevertheless, generating mathematically complex key pairs using true random number generators is not a possibility on most low resource IoT devices for the time being. It is envisioned that IoT of the future may benefit from the massive potential of quantum cryptography in the post-quantum computing era. High-efficiency quantum digital signature (QDS) protocols are being developed using asymmetric quantum keys [12]. Another novel concept, Internet of Predictable Things (IoPT), could be employed in mitigation of cyberattacks using energy forecasting in smart grids with machine learning (ML) aids to detect anomalous data patterns [13]. These directions possess substance in the improvement of cybersecurity for future IoT.

The authentication challenge extends to confidentiality and integrity compelling drastic measures to limit access to sensitive data, allowing only intended users to view or modify it. Lastly, availability is mandatory for allowing authorized users to reliably access network resources whenever and wherever needed. Physical layer security measures such as the long-range frequency hopping spread spectrum (LR-FHSS) [14] are gaining popularity due to integration in contemporary long-range (LoRa)-based IoT devices. In the event of jamming or interference, frequency hopping at multiple channels can ensure better link availability. These security requirements collectively form the foundation of a robust and reliable wireless network. Wired networks rely on physical cables for node connections, while wireless networks are more vulnerable due to their broadcast nature making them susceptible to eavesdropping, denial-of-service (DoS), spoofing, man-in-the-middle (MITM) attacks, and message falsification. Cryptographic techniques are commonly used to prevent eavesdropping, ensuring identity verification. In IoT, security gaps exist due to reverse engineering threats and challenges in rapidly installing cryptographic protocols on insecure devices. On the other hand, noncryptographic methods, such as device-specific signal pattern analysis, complement traditional cryptography by identifying known devices and detecting rogue ones, offering essential security without modifying the IoT devices.

Radio frequency fingerprinting (RFF), being a noncryptographic method, has been in use for a few decades now. However, its potential as a physical layer security feature in wireless sensor networks of IoT has been gaining popularity recently [15,16]. RFF uses hardware impairments in the radio section of an IoT device for classification. These impairments are unique to each IoT device due to inherent nonlinearities in the manufacturing process of these inexpensive devices. The components of an IoT device are shown in Figure 2. It is imperative to point out that the aim of most studies on RFF has been device authentication at the physical layer—threat elimination at the first line of defense.

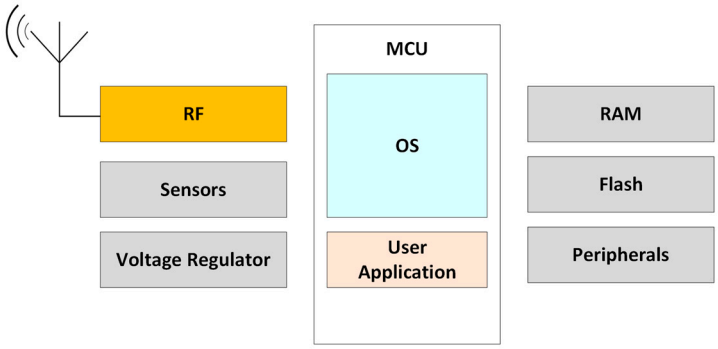

Figure 2. Components of an IoT device.

To this end, a gap exists in studying RFF deployment in a smart grid use case. This article primarily explores the feasibility of integrating RFF into the existing infrastructure of wireless sensor networks in smart grids. The body of this work investigates the potential of RFF as a physical layer security feature for the said application and presents a deployment framework.

The remainder of the article is structured as follows: Section 2 provides an overview of related research. Section 3 illustrates ingredients of a typical DL-aided RFF system. Security challenges and associated discussions are detailed in Section 4. Smart grids as a use case for RFF deployment is covered in Section 5. The ensuing Section 6 argues the potential challenges and directions for future research. Finally, Section 7 concludes the article.

2. Related Work

The core concept behind RFF involves the extraction of distinct patterns or features from devices and utilizing them as signatures for device classification. Previously, a wide range of features including but not limited to physical (PHY) layer and medium access control (MAC) layer have been employed in RFF. However, some straightforward identifiers like Internet Protocol (IP) addresses, MAC addresses, and international mobile station equipment identity (IMEI) numbers are susceptible to spoofing. Similarly, received signal strength indication (RSSI) and channel state information (CSI) could be affected by mobility and environmental changes. A recent research focus has been the investigation of features that are intrinsic to a specific device, possess stability over time, and are challenging for malicious actors to replicate. The authors' prior work has contributed to the advancement of RFF while it was still a topic of academic research. However, the focus of this work is the discussion of practical deployment aspects of RFF in real-world applications. The following subsections cover the related work from all the domains associated with this body of work.

2.1. Previous Work

The primary focus of previous work has been the development of cost-effective techniques for extracting RF fingerprints. In this context, a method for modifying transient signals was presented [17]. Emphasizing cost-effectiveness, a modular RF front end for RFF analysis of Bluetooth signals was offered [18]. Given the passive nature of RFF, modular solutions are particularly relevant, enabling a single RFF system to classify multiple IoT devices without any modification. A common use case of classifying Bluetooth radios of

cellular devices was addressed in [19]. Firstly, the signal was preprocessed through transient signal decomposition using variational mode decomposition (VMD). Subsequently, a linear support vector machine (LSVM) was employed as a classifier. A comparative study on classifiers, considering varying signal-to-noise ratio (SNR) levels and dataset sizes was organized in [20]. The experimental results yielded excellent classification accuracy even at low SNR values, implying tremendous relevance in real-world scenarios. Adhering to open science principles, a rich dataset to aid the research community in advancing RFF technology was submitted in [21]. The goal was to aid prospective researchers with the inclusion of an acquisition method for gathering Bluetooth signals. Another potential avenue for academic exploration is the application of RFF for localization. Addressing this, [22] presented a discussion on recent advances and challenges surrounding RFF localization in outdoor environments.

2.2. Cybersecurity in Smart Grids

As smart grids emerge to play an integral role in the evolution of smart cities, a rising need to overhaul their cybersecurity is imminent. The threat spectrum of cyberattacks being faced by smart girds is tremendous [23]. Various organizations, such as the National Institute of Standards and Technology (NIST) and the Smart Grid Interoperability Panel (SGiP), are shaping security requirements for smart grids. Authentication and authorization are central to the overall security of smart grids. Per the guidelines for smart grid cybersecurity published by NIST [24], the focus of security has been limited to cryptographic techniques only. A detailed framework for key management and associated operational issues was provided in the referred document. Key management can be improved using physically unclonable functions (PUF). Generation of PUF hinges on the intrinsic uniqueness within the integrated circuit of a device. A key generated by a device employing PUF can only be regenerated by the same device. This characteristic is leveraged by the utility to authenticate data generated by smart meters [25]. With developed countries increasingly embracing smart grids, the security concerns and potential remedies have become a focal point for researchers and industry experts [26]. Ongoing endeavors are directed towards securing the network and application layers of IoT in smart grids. Remarkably, the non-cryptographic security techniques in IoT for smart grids have not been extensively studied. This represents a novel area where RFF may emerge as a promising candidate.

2.3. Historical and Contemporary Use of RFF

The classification of signals using passive radio frequency (RF) receivers enhanced by artificial intelligence has a historical precedent dating back three decades. Initial use of RFF involved the classification of signals from multiple radar sources leveraging their distinct attributes [27]. More recently, RFF has gained popularity in IoT with experiments on wireless devices using frequency, magnitude, phase offsets, and in-phase and quadrate (I/Q) imbalance as differentiating features [28]. Utilizing RFF for device authentication finds its most straightforward application in RFID systems [29]. The cited studies exhibit the relevance of RFF in various legacy and contemporary applications.

2.4. Physical Layer Security in Wireless Communication

There have been substantial studies concerning physical layer security in wireless communication of IoT devices. In the era of ML and DL, physical, network, and application layers of IoT are susceptible to security threats [30]. As adversarial attacks grow more and more complex, security measures on all layers of communication networks are emerging on the horizon. In this regard, classification efforts on cellular phones using their integrated physical components have been conducted [31]. Non-cryptographic methods for user authentication and device identification in static and mobile wireless networks have seen academic interest [32]. Nevertheless, there are advantages, limitations, and implementation challenges associated with these novel methods. A literature review of relevant studies

underscore the potential of physical layer security in wireless communication between IoT devices for authentication.

2.5. Machine Learning in RFF

Emitter-specific hardware attributes can be leveraged without the use of machine learning employing expert features in RFF extraction algorithms such as signal phase [33]. However, this approach is over-reliant on the quality of the received signal, which is not practical in actual scenarios as wireless signals undergo drastic changes in amplitude and phase due to channel effects. Conversely, DL-aided RFF has gained popularity due to its ability to detect unique features in datasets. This approach has made the identification and classification problem scalable to cater unseen devices. More precisely, convolutional neural networks (CNN) have exhibited even more accurate results [34]. Automated feature extraction in DL has proven to be a potent solution, surpassing traditional methods employing only the handcrafted features. However, hybrid models have exhibited even better results when a handcrafted feature such as carrier frequency offset (CFO) is used in unison with DL [35]. An examination of reference studies reveals a multitude of prevalent ML, DL, and hybrid methods. The choice of a specific model hinges on the adopted representation of the RF signal, whether it be I/Q, spectrogram, or fast Fourier transform (FFT).

3. Typical DL-Aided RFF System

The two major domains in an RFF system comprise RF and DL. The choice of an SDR architecture for the RF domain is governed by its flexible nature to process raw waveforms and a wide range of operating frequencies. For the DL part, the host processor serves as a platform for training a neural network (NN) on a given dataset followed by classification in the inference stage. The following subsections provide some explanation for the process of RF signal acquisition followed by the rationale for pre-processing before the signal is subject to the training and inference stage.

3.1. RF Signal Acquisition

The first step in RFF comprises the RF signal acquisition. To make the signal fitting for the classification stage, there is a need to pre-process the signal. The collection of signals followed by pre-processing collectively constitutes the signal acquisition process. The requirement for pre-processing stems from the problem statement inherent in the RFF-based device classification. The classical wireless communication model serves a simple mathematical explanation. For the sake of simplicity, the high-frequency carrier component is omitted. Baseband signal at the input of the RFF system, $y(t)$, can then be given:

$$y(t) = G(h(\tau, t)) * F^K(x(t)) + n(t), \tag{1}$$

where $x(t)$ is the theoretical modulated signal. $G(\cdot)$ denotes the hardware effects of the receiver and $h(\tau, t)$ is the impulse response of time dispersive wireless channel with delay τ. $F^K(\cdot)$ signifies the transmitter specific effect of device under test (DUT), K, $n(t)$ is the additive white Gaussian noise (AWGN), and $*$ is the convolution operation. The goal of RFF is to extract $F^K(\cdot)$, unique to each hardware and difficult to clone or tamper. There are, however, some common hurdles in the development of a robust RFF. Firstly, the transmitter specific $F^K(\cdot)$ is miniscule and overly reliant on the signal quality [33]. One approach could be to artificially create artifacts in the transmitter, but this could hamper communication performance. Moreover, in practical wireless channels, the received signal $y(t)$ undergoes amplitude and phase dispersion due to channel impulse response $h(\tau, t)$. Therefore, the NN shown in Figure 3 has the tendency to make inaccurate predictions, since $h(\tau, t)$ is not predictable and may vary significantly between training and inference. As already highlighted, DL-aided RFF systems have shown performance improvement; however, DL relies on the assumption that the data points follow an independent and identical distribution (i.i.d). In other words, statistical parameters, such as mean and variance, must remain consistent across the entire dataset. The varying impulse response

of a time-dispersive channel could therefore be a cause for a DL model to generalize poorly on unseen data. In dynamic scenarios, the variance of $h(\tau, t)$ is an even bigger challenge. In addition to the channel variance, the relative motion between the communicating nodes induces Doppler shift given by the following expression:

$$\Delta f = f_c \frac{c}{v} cos(\theta), \tag{2}$$

where Δf is the Doppler shift in the carrier frequency f_c due to relative motion between the communicating nodes having a relative velocity v at an angle θ, and c is the speed of light. The effect of Doppler shift causes signal degradation, which in turn affects the classification performance. CFO is another challenge that is prevalent in inexpensive radios; by virtue, low-cost crystal oscillators have accuracies in the excess of multiple tens of parts per million (PPM). Amidst these challenges, there is a burgeoning requirement to pre-process the signal before it is stacked in a dataset to train the NN. Pre-processing comprises signal conditioning, as employed in any legacy radio receiver, for accurate symbol detection. The most important aspect of pre-processing is to mitigate the channel effects, since it is the most unpredictable variable in the entire process. Various mitigation methods are prevalent in the literature, such as the channel-independent spectrogram for narrowband communication channels that experience very little change in a short time interval [36]. Another direction is data augmentation where a channel simulator may aid in training the NN on simulated channel conditions. This approach can minimize the channel effects since a NN trained on a dataset containing diverse channel conditions shall generalize much better in the inference stage. Nonetheless, rationale for the requirement of channel equalization is clear and justified. Detailed discussion of the implementation of channel equalizers is beyond the scope of this work. More importantly, it must be realized that synchronization is a mandatory step for channel equalization. Among other issues, the effect of the receiver $G(\cdot)$ must not alter the classification performance. A practically deployable RFF system must be agnostic to the effects of the receiver. A NN trained on one RFF system must be able to perform equally well on the other if there is a need to replace it in the event of failure. Lastly, normalization of the received signal is performed to bar the NN from using signal strength as a feature for training.

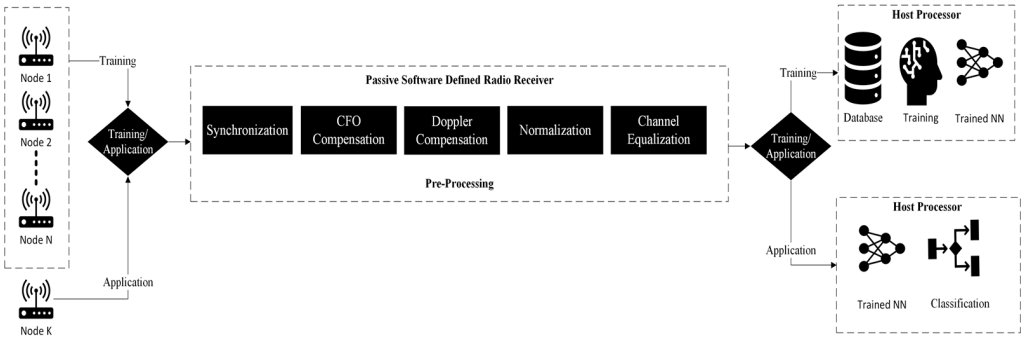

Figure 3. Typical DL-based RFF system.

3.2. Deep Learning

Figure 3 illustrates the working of a modern RFF system as a two-stage process, training and inference. As evident, training comprises receiving samples from N unique devices and an RF signal is received from device K in the inference stage to differentiate between a legitimate and rogue transmitter on a per packet basis. The mathematical model for the classification problem ensues. Let D^{train}, a training dataset from N devices be given by

$$D^{train} = \{(y_m, P_m)\}_{m=1}^{M_{train}}, \tag{3}$$

where y_m is the mth training sample and P_m is the respective output of the one-hot encoding function $O(\cdot)$ for the mth DUT label, given by

$$P_m = O(l_m), \tag{4}$$

where l_m is the ground truth DUT label of the mth training sample. If M_{train} is the total number of training samples in a neural network $f(y;\Theta)$, parameters Θ can be optimized using D^{train} by the following expression:

$$\Theta = \underset{\Theta}{argmin} \frac{1}{M_{train}} \sum_{(y,p)\in D^{train}} L_{ce}\left(f(y;\Theta), p\right), \tag{5}$$

where $L_{ce}(\cdot)$ is the cross-entropy loss. In the inference stage, the receiver captures a signal y′ and feeds it into the well-trained neural network $f(y;\Theta)$ for prediction. A probability vector $\hat{\boldsymbol{p}}$ is obtained in the inference stage as

$$\hat{p} = f(y';\Theta), \tag{6}$$

where $\hat{p} = \{\hat{p}_1, \ldots, \hat{p}_k, \ldots, \hat{p}_N\}$ is a probability vector over all the N DUTs, and $\hat{p}_K$ is the estimated probability for the Kth DUT. The predicted device label $\hat{l}$ is derived by simply selecting the index of the element with the highest probability as defined below.

$$\hat{l} = \underset{k}{\text{argmax}}(\hat{p}). \tag{7}$$

The model outlined above serves as the foundation for device classification, utilizing labels derived from a predefined dataset. To declare an unknown device as rogue, each element from the set $\hat{p}$ must exhibit a probability value below a predetermined threshold. This criterion designates a device as absent from the roster of legitimate devices, thereby classifying it as rogue. This ability of the NN to identify unseen devices adds scalability to the system and makes the classification step an open-set problem.

To summarize, a typical DL-aided RFF system must have a common set of attributes. The scope of this article is to present a practically deployable RFF system. Therefore, based on state-of-the-art and literature reviews of relevant dissertations [37,38] and an elaborate survey [39], essential features of a practical DL-aided RFF system are listed:

1. Synchronization.
2. CFO Compensation.
3. Doppler Compensation.
4. Normalization.
5. Channel Equalization.
6. Receiver Agnostic.
7. Scalability.

4. IoT in Smart Grids

The US Department of Energy defines smart grids as modernized electrical grids that leverage advanced technology to enhance the efficiency, reliability, and sustainability of electricity generation, distribution, and consumption [40]. They incorporate various power generation sources, including customer-generated energy, solar, wind, and more. Understanding the role of IoT in smart grids and the security challenges it presents is crucial before delving into discussions about the necessity to bolster cybersecurity.

4.1. D2D Wireless Communication in Smart Grids

The effectiveness of smart grids is rooted in their ability to anticipate fluctuations in energy supply, optimize grid operations, and promptly respond to changes in demand and power failures. This capability not only strengthens grid stability but also contributes to the reduction in energy wastage, enhancing overall sustainability [41]. Central to the

realization of this concept is D2D wireless communication between IoT devices at the control center, the power station, and consumers. Figure 4 shows the evolution of power grids. The dotted lines mark the communication network, which is crucial in achieving the functionality of smart grids.

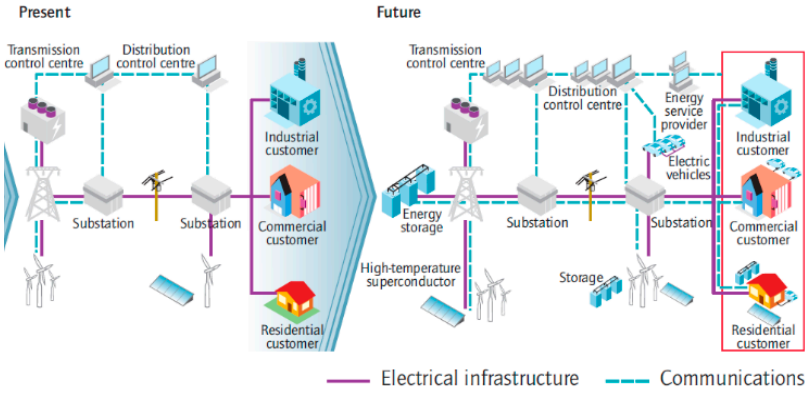

Figure 4. Evolution from conventional to smart grids [41].

4.2. Security Challenges in Wireless Communication

In wired networks, nodes are physically linked by cables. Conversely, wireless networks face heightened vulnerability due to their broadcast nature. They are susceptible to various malicious attacks, such as eavesdropping [42], denial-of-service (DoS) [43], spoofing [44], man-in-the-middle (MITM) [45], message falsification/injection [46], etc. To ensure confidentiality and authentication, existing systems commonly use cryptographic techniques to prevent eavesdropping and unauthorized access to networks [47,48].

Conventional cryptography ensures identity verification using techniques like message authentication codes, digital signatures, and challenge-response sessions [49]. However, in widely distributed IoT, security gaps persist due to reverse engineering threats [50], impracticality of rapid cryptographic protocol installation in insecure devices [51], and inefficacy against hijacked devices.

In a post-quantum computing era, the above cited challenges could be overcome using quantum cryptography. For instance, quantum light could be used to generate inherently unforgeable quantum cryptograms [52]. These cryptograms have exhibited the potential to be used in practical applications with near-term technology. Future IoT may benefit tremendously at the application layer as a solution to vulnerabilities present in symmetric cryptographic schemes. Non-cryptographic methods, such as device-specific signal pattern analysis, supplement traditional cryptography by identifying known devices and detecting rogue ones [53]. These approaches are crucial for enhancement of cybersecurity in IoT, without requiring major system modifications [54].

4.3. Cybersecurity in Smart Grids

The layered architecture in IoT of smart grids is illustrated in Figure 5 [55]. At the physical layer, data from sensors, actuators, and smart meters are collected at the gateways. At the network layer, data from multiple gateways are concentrated and relayed to the application layer operating on servers in the control center using legacy communication methods. The goal of cybersecurity in IoT is to ensure protection at every layer; the same is applicable in smart grids as well. A closer look at the threat spectrum being faced by smart grids underscores the importance of device authentication [56,57], although physical layer intrusion detection systems have the capacity to perform device authentication at the first stage of defense in wireless networks [58]. But, to this end, there has not been a study on the implementation of physical layer security measures in wireless communication between IoT devices of smart grids for authentication. To fill this gap, RFF emerges as a potential solution and this article builds the case for discussion on the associated deployment aspects in smart grids.

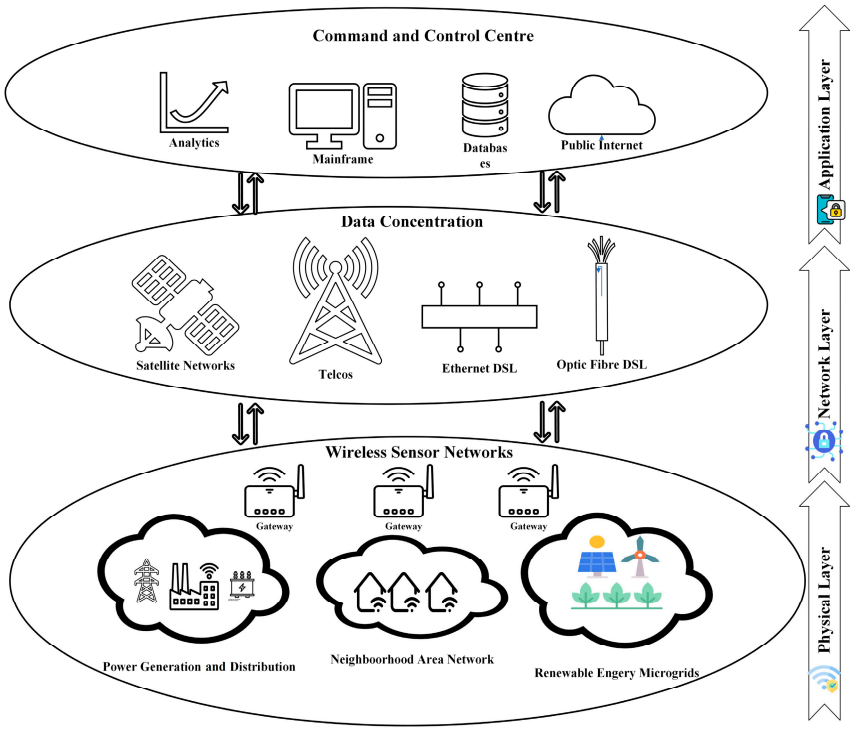

Figure 5. Cyber security in smart grids [55].

5. Deployment of RFF in Smart Grids

The aim of this article is to conduct a feasibility study and discuss practical deployment consideration apropos of the use of RFF in smart grids. Existing IoT frameworks have been considered for seamless integration of RFF with minimal changes. The core idea is to present RFF as an addition to existing IoT infrastructure instead of reinventing the wheel. The following sub-sections provide considerations and requirements for deployment of RFF in smart grids.

5.1. Network Considerations

In line with the aim of this article, performance metrics of existing IoT serve as a good starting point. Coverage and energy efficiency are important metrics for choosing a network topology [59]. Furthermore, data rate, range, application layer security, and localization are important factors for selecting a particular low-power wide-area network (LPWAN) [60]. From a practical standpoint, cost and scalability hold particular significance [61]. In the UK, smart meters communicate via cellular networks, utilizing 2G or 3G waveforms [62]. However, the use of a long-range wide-area network (LoRaWAN), a star-of-star network topology, in advanced metering infrastructure has been reported as well [63,64]. Given the novelty of RFF and the consideration of performance metrics including cost, energy efficiency, network topology, and communication range, LPWAN is a suitable candidate for the deployment of RFF.

5.2. Security Considerations

Cybersecurity experts have expressed concerns, revealing that 70% of IoT devices are vulnerable to cyberattacks [65]. The wireless sensor network of IoT exhibits vulnerabilities across various layers, and cyberattacks can manifest at different stages [66]. Likewise, LPWAN is not exempt from cyber threats [67]. Wireless sensor networks in smart grids comprise IoT devices equipped with temperature, humidity, light, and wind sensors. The threat from rogue IoT devices to generate falsified data is a significant concern. For instance, exaggerated sensor readings from a smart meter could lead to an unwarranted stimulus from the control station. The limitations of existing security schemes have been discussed

in the introduction section of this article. Considering the vulnerability of higher layers to attacks, a novel approach is to secure the physical layer of D2D wireless communication across the network. It is proposed that this extra layer of security should always be in the loop for all end-to-end data transactions between IoT devices in the network.

5.3. Proposed RFF Framework

A key facet of smart grid infrastructure is the real-time estimation of household loads [40,41]. This requirement can be effectively addressed by smart energy meters transmitting data wirelessly at regular intervals. However, this simple task becomes challenging from a cybersecurity perspective in the presence of rogue devices. This scenario is accurately addressed in the physical layer security framework of RFF, as depicted in Figure 6. The proposed configuration ensures that all data transmission from the sensors must pass through the physical security barrier of the RFF system before reaching the control station. The star-of-stars network topology ensures that all the sensors first concentrate their data at their respective gateways. Hosted on the IoT gateways, RFF serves as a filter to allow readings from only legitimate sources while filtering the rogue ones on a per packet basis. Since these gateways can send and receive wireless data, they can filter data from rogue gateways as well.

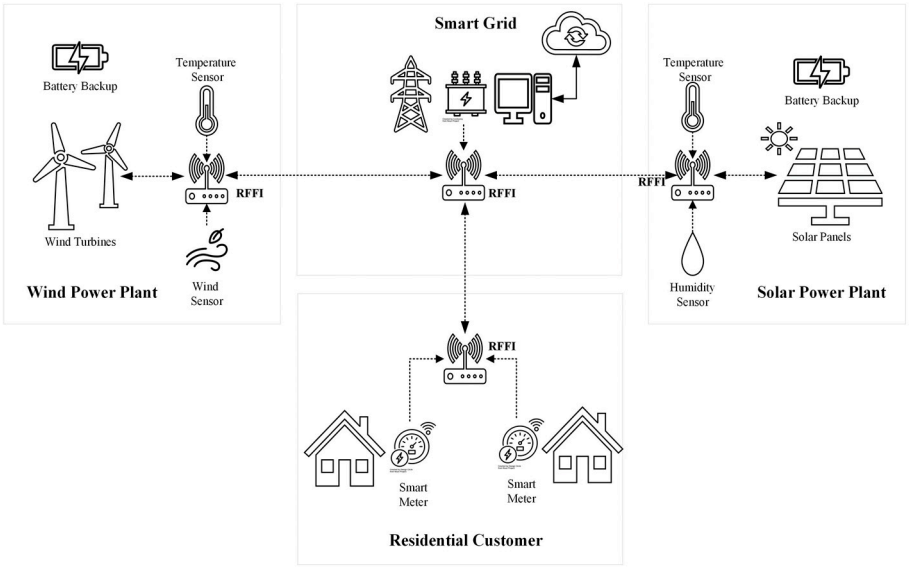

Figure 6. Proposed RFF framework for smart grids.

It is worth mentioning that within a mini star network, multiple gateways could be employed for time-based direction of arrival estimation. This can be extremely helpful in the localization of a rogue device followed by necessary remediation. The IoT devices equipped with sensors communicate unidirectionally with their respective IoT gateways. However, to cater for dynamic load requirements, the control station may issue commands to renewable energy plants, directing them to release stored energy into the system or increase power generation. This requires bidirectional communication in line with the fundamental characteristics of a smart grid [40,41]. This bidirectional communication offers a significant challenge for deployment of RFF in existing low-resource IoT devices, which is discussed in Section 6.

5.4. Performance Considerations

Before a technology is deemed suitable for practical deployment, it is important to estimate its performance considering real-world conditions. The aim of presenting a typical DL-aided RFF system in Section 3 was to highlight the hurdles in achieving the desired outcome. The key performance indicator (KPI) of an RFF system is its classification accuracy.

There has not been a study on the estimation of this KPI in a smart grid use case. However, the authors' previous work in [19] covered the performance comparison of various ML-aided classifiers with different SNR values of the received signal. Table 1 summarizes the experimental results from that study. The results show decent performance even in low SNR conditions. Given that the IoT devices in wireless sensor networks of smart grids are deployed in a static setting, empirical propagation measurements in urban environments may serve as a good reference for RSSI estimation [68]. Figure 7 provides a path loss curve in decibels (dB) against the distance between communicating nodes. Using the locations of smart meters, sensors, and IoT gateways, the expected RSSI could be estimated at the RFF receiver.

Table 1. Comparison of classifiers with various levels of SNR [19].

Classifier	SNR (dB)		
	(8–10)	**(12–15)**	**(18–23)**
L-SVM	79.3%	82.1%	90.5%
Complex Tree	66.8%	68.8%	85.4%
LDA	76.6%	77.8%	83.6%

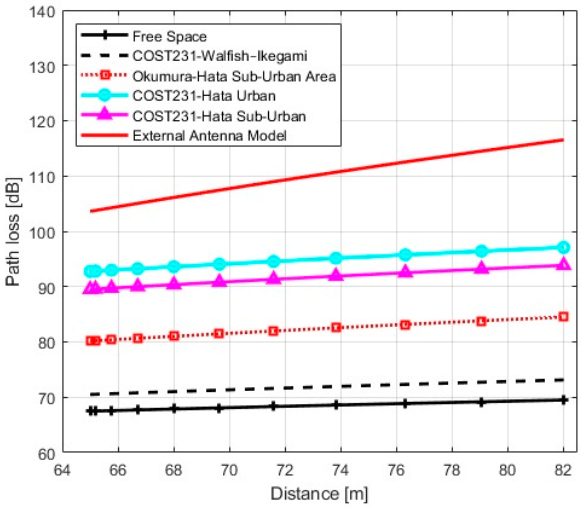

Figure 7. Empirical propagation model in urban environment [69].

Subsequently, the resultant SNR could be used to estimate the classification accuracy using Table 1. It is pointed out that the scope of this study is not limited to a specific smart grid. It is expected that through careful decision making in the selection of appropriate classifier and signal attributes, decent classification accuracy can be achieved, even with low SNR. The classification accuracies of various signal representations for as many as 60 unique LoRa devices are given in Table 2. It may be noted that there is another important aspect in gauging the performance of an RFF system: the time required for training. It is only reasonable to assume that installation, repair, and maintenance of IoT devices in smart grids is likely to be conducted by electric supply companies. Hence, this one-time training activity, even in a practical deployment scenario, may be tolerable given the extraordinary classification performance achieved as a trade-off. Therefore, for a smart grid use case, training time may not be treated as a KPI. Referring to the star network topology outlined in Section 5.3, each wireless sensor network incorporates an IoT gateway. These gateways have been proposed as an optimal site for RFF, ensuring comprehensive access to all IoT devices within the network for accurate classification. Considering the performance metrics across a large set of devices, the findings from referred studies can be reasonably extrapolated as a valuable reference for the smart grid.

Table 2. Classification accuracy of different models with required training time [37].

Signal Representation	DL Model	Accuracy			Number of Parameters	Training Time (minutes)
		w/o CFO Comp.	w/o CFO Comp.	Hybrid		
I/Q samples	MLP	54.08%	55.73%	78.26%	19,018,009	25
	CNN	64.10%	92.26%	98.11%	4,361,545	75
	LSTM	61.16%	89.54%	95.14%	4,267,289	70
FFT results	MLP	55.44%	94.48%	96.17%	19,018,009	25
	CNN	61.14%	82.10%	85.58%	4,361,545	75
	LSTM	49.20%	58.26%	82.81%	4,267,289	69
Spectrogram	MLP	88.60%	91.82%	95.95%	8,821,017	22
	CNN	83.53%	95.35%	96.40%	1,545,193	20
	LSTM	68.16%	89.50%	98.04%	3,427,609	80

5.5. Implementation Aspects

The RFF for smart grids emerges as a highly feasible solution for deployment, primarily owing to its cost-effectiveness and seamless integration capabilities within existing systems. Positioned at the intersection of two prominent domains, RF and ML, RFF may seem intricate from a technical perspective, but from the user's perspective, it can be offered as a plug-and-play solution, hence, simplifying its adoption into existing IoT. Smart grids, being a critical infrastructure from an operation standpoint, can benefit from the passive nature of RFF systems during training as well as inference stages. This can be helpful in ensuring uninterrupted functionality of the smart grids during the deployment process. RFF systems do not necessitate integration into every IoT device. Instead, they can be intelligently deployed only into IoT gateways and leverage the available processing prowess. Moreover, power efficiency poses no significant challenge since RFF systems operate in passive mode, necessitating no significant power requirement. Considering RFF is deployed as a technology, the hardware infrastructure overhead is minimal. In the features of a typical DL-aided RFF system, the ability to be receiver agnostic was discussed as a desirable feature. It would be a highly recommended feature in the event of a device failure, allowing hot replacement but not necessitating training the NN again. Lastly, an RFF system for smart grids was proposed as an open-set solution. This signifies that once the NN is trained on all legitimate IoT devices, any number of rogue devices could be detected [38]. This scalability further adds to the practicality of RFF. Overall, cost effectiveness, power efficiency, low deployment overhead, and scalability make RFF an appropriate practical choice. It is noteworthy that mobility-induced challenges such as antenna cross-polarization loss and Doppler shift may not pose significant hurdles within the context. This assertion is based on the observation that RFF gateways and IoT sensors predominantly exhibit static characteristics in the said application. These elements further simplify the implementation process.

5.6. Regulatory Requirements

The adherence to regulatory standards for RF-based systems stands as a crucial concern. Every country delineates unique requirements governing the utilization of frequency bands. Moreover, there is a limit on maximum permissible power levels for RF transmission. However, RFF, being a passive technology, poses no challenges in this regard. Since the addition of RFF has been proposed for existing LPWAN, the use of industrial, scientific, and medical (ISM) bands for operation is possible. The use of LPWAN in unlicensed bands is a viable direction for smart cities [53]. Having no additional regulatory compliance contributes to the overall feasibility and cost-effectiveness [54] of implementing RFF technology in wireless sensor networks of smart grids. However, the SDR of an RFF system may require EMC certification [69] subject to user needs.

6. Challenges and Future Directions

Being a novel technology and an unprecedented use case in smart grids, RFF entails challenges as well as significant potential for growth in the future. The aim of this section is to underscore the existing challenges and their potential solutions that can significantly advance the deployment of RFF in real-world applications. Additionally, prospective research directions aimed at the maturation of RFF as a technology are deliberated.

6.1. Challenges

RFF for wireless sensor networks of smart grids faces a multifaceted set of challenges. To start, long-term deviation in hardware impairments remains a largely uncharted territory. There has not been a study on long-term operational performance of RFF in IoT. Additionally, bidirectional communication security remains a notable challenge, particularly in scenarios where IoT devices are deployed as receivers. Due to limited resources available on these devices, identification of rogue gateways using RFF is not possible at the present. Addressing these multifarious challenges constitutes a burgeoning area of academic research. The longevity and robustness of RFF technology in the evolving landscape of wireless sensor networks of smart grids needs to be closely monitored in the years to come. Moreover, the emergence of deep generative attackers employing generative adversarial networks is a growing apprehension. These attackers pose a significant threat to device identification even at the physical layer. By leveraging these models, malicious entities can effectively train highly realistic signal or data packet generators capable of mimicking the signal characteristics of legitimate devices. This threat can overcome the ability of RFF systems to identify rogue devices as the success rate of spoofing attacks may increase from less than 10% to approximately 80% [70]. Another significant challenge lies in the availability of abundant datasets for conducting research and experimentation. Addressing these challenges can further add to the potential of RFF as a practical solution for the enhancement of cybersecurity in smart grids.

6.2. Future Research

Research efforts in the realm of RFF are required for channel estimation and equalization. This area holds immense potential for enhancing the reliability and performance of RFF systems in practical scenarios. Specifically, researchers can focus on developing advanced channel estimation techniques that effectively counteract signal distortion caused by time-dispersive channels. However, long training sequences (LTS) can be used to achieve high classification accuracy in 802.11 devices even if the training samples are collected from diverse locations [71]. This research direction has massive potential to benefit LPWAN as well. Simultaneously, the design of a receiver chain that minimizes the combined impact of the channel and receiver components is of paramount importance. Such research efforts can aid in the collection of I/Q datasets that closely resemble the originally transmitted signals, thereby bolstering the overall resilience and classification accuracy of RFF in real-world deployment scenarios. There is another issue in scenarios where IoT devices may be spoofed from a rogue RFF gateway, mimicking its hardware attributes. Such threats may be mitigated using multiple input multiple output (MIMO) receivers. Such localization methods can aid in estimating the difference between the expected and actual position of an IoT device. This additional check can be very useful, especially in smart grids, since the devices in the network are static. But these research directions remain unexplored to this end. Moreover, as already cited in the previous section, there is a pressing need for the collection and publication of open-source datasets. The creation of such datasets will not only facilitate a deeper understanding of RFF as a technology but also empower researchers to develop and validate new algorithms and models effectively. A few datasets have been published in [21,72], but this trend is limited. By fostering an environment of open data sharing and collaboration, the research community can collaborate in improving RFF as a technology for practical deployment in real-word scenarios.

7. Conclusions

The article argues for the potential of RFF as a physical layer security feature for wireless communication between IoT devices of smart grids. It underscores the importance of smart grids and identifies associated cybersecurity threats. It offers RFF as a complementary addition to contemporary cryptographic methods in existing IoT. Characteristics of a typical DL-aided RFF system were presented and the rationale behind design choices was highlighted. Previous work and the reference literature were reviewed as a substantial starting point. Cybersecurity aspects, network architecture, regulatory considerations, and implementation aspects of RFF for smart grids were deliberated. The article culminates with a discussion on the existing limitations and future research directions to improve RFF as a technology and its utilization as a long-term solution for smart grids.

Author Contributions: Investigation, resources, visualization, writing—original draft preparation, M.A.A.; conceptualization, M.A.A., Y.D. and A.K.; validation, supervision, writing—review and editing, Y.D., F.O.C. and A.K.; project administration, A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data is contained within the article.

Acknowledgments: This work was supported in part by Gazi University under grant FGA-2022-8043.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bellini, P.; Nesi, P.; Pantaleo, G. IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies. *Appl. Sci.* **2022**, *12*, 1607. [CrossRef]
2. Mehmood, Y.; Ahmad, F.; Yaqoob, I.; Adnane, A.; Imran, M.; Guizani, S. Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. *IEEE Commun. Mag.* **2017**, *55*, 16–24. [CrossRef]
3. Chen, S.; Wen, H.; Wu, J.; Lei, W.; Hou, W.; Liu, W.; Xu, A.; Jiang, Y. Internet of Things Based Smart Grids Supported by Intelligent Edge Computing. *IEEE Access* **2019**, *7*, 74089–74102. [CrossRef]
4. Rana, M.M.; Xiang, W.; Wang, E. IoT-Based State Estimation for Microgrids. *IEEE Internet Things J.* **2018**, *5*, 1345–1346. [CrossRef]
5. Babar, M.; Tariq, M.U.; Jan, M.A. Secure and Resilient Demand Side Management Engine Using Machine Learning for IoT-Enabled Smart Grid. *Sustain. Cities Soc.* **2020**, *62*, 102370. [CrossRef]
6. Abujubbeh, M.; Al-Turjman, F.; Fahrioglu, M. Software-Defined Wireless Sensor Networks in Smart Grids: An Overview. *Sustain. Cities Soc.* **2019**, *51*, 101754. [CrossRef]
7. Alsuwian, T.; Shahid Butt, A.; Amin, A.A. Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review. *Sustainability* **2022**, *14*, 14226. [CrossRef]
8. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
9. Halperin, D.; Heydt-Benjamin, T.S.; Ransford, B.; Clark, S.S.; Defend, B.; Morgan, W.; Fu, K.; Kohno, T.; Maisel, W.H. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In Proceedings of the 2008 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 18–22 May 2008; pp. 129–142. [CrossRef]
10. Kumar, S.; Deora, S.S. Comparative Analysis of Security Techniques in Internet of Things. In Proceedings of the 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, India, 25 November 2022; pp. 407–412. [CrossRef]
11. Word to the Wise. Cryptography with Alice and Bob. 2014. Available online: https://wordtothewise.com/2014/09/cryptography-alice-bob/ (accessed on 18 September 2023).
12. Yin, H.-L.; Fu, Y.; Li, C.-L.; Weng, C.-X.; Li, B.-H.; Gu, J.; Lu, Y.-S.; Huang, S.; Chen, Z.-B. Experimental Quantum Secure Network with Digital Signatures and Encryption. *Natl. Sci. Rev.* **2023**, *10*, nwac228. [CrossRef]
13. Semtech. Application Note: LR-FHSS System Performance, AN1200.64 Rev 1.2. 2022. Available online: https://semtech.my.salesforce.com/sfc/p/#E0000000JelG/a/3n000000v6Za/sHlDztpPfXWzJd7mr01Yj7CaMR0Uxbqy71YmSVpxxIw (accessed on 19 September 2023).
14. Tian, Q.; Lin, Y.; Guo, X.; Wen, J.; Fang, Y.; Rodriguez, J.; Mumtaz, S. New Security Mechanisms of High-Reliability IoT Communication Based on Radio Frequency Fingerprint. *IEEE Internet Things J.* **2019**, *6*, 7980–7987. [CrossRef]
15. Cali, U.; Kuzlu, M.; Sharma, V.; Pipattanasomporn, M.; Catak, F.O. Internet of Predictable Things (IoPT) Framework to Increase Cyber-Physical System Resiliency. *arXiv* **2021**, arXiv:2101.07816.

16. Nouichi, D.; Abdelsalam, M.; Nasir, Q.; Abbas, S. IoT Devices Security Using RF Fingerprinting. In Proceedings of the 2019 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, United Arab Emirates, 26 March–10 April 2019; pp. 1–7. [CrossRef]
17. Ali, A.M.; Uzundurukan, E.; Kara, A. Improvements on Transient Signal Detection for RF Fingerprinting. In Proceedings of the 2017 25th Signal Processing and Communications Applications Conference (SIU), Antalya, Turkey, 15–18 May 2017; pp. 1–4. [CrossRef]
18. Uzundurukan, E.; Ali, A.M.; Kara, A. Design of Low-Cost Modular RF Front End for RF Fingerprinting of Bluetooth Signals. In Proceedings of the 2017 25th Signal Processing and Communications Applications Conference (SIU), Antalya, Turkey, 15–18 May 2017; pp. 1–4. [CrossRef]
19. Ali, A.M.; Uzundurukan, E.; Kara, A. Assessment of Features and Classifiers for Bluetooth RF Fingerprinting. *IEEE Access* **2019**, *7*, 50524–50535. [CrossRef]
20. Aghnaiya, A.; Ali, A.M.; Kara, A. Variational Mode Decomposition-Based Radio Frequency Fingerprinting of Bluetooth Devices. *IEEE Access* **2019**, *7*, 144054–144058. [CrossRef]
21. Uzundurukan, E.; Dalveren, Y.; Kara, A. A Database for the Radio Frequency Fingerprinting of Bluetooth Devices. *Data* **2020**, *5*, 55. [CrossRef]
22. Dogan, D.; Dalveren, Y.; Kara, A. A Mini-Review on Radio Frequency Fingerprinting Localization in Outdoor Environments: Recent Advances and Challenges. In Proceedings of the 2022 14th International Conference on Communications (COMM), Bucharest, Romania, 16 June 2022; pp. 1–5. [CrossRef]
23. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 5–20. [CrossRef]
24. *Guidelines for Smart Grid Cybersecurity*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf (accessed on 25 September 2023). [CrossRef]
25. Nabeel, M.; Kerr, S.; Ding, X.; Bertino, E. Authentication and Key Management for Advanced Metering Infrastructures Utilizing Physically Unclonable Functions. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; pp. 324–329. [CrossRef]
26. Komninos, N.; Philippou, E.; Pitsillides, A. Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1933–1954. [CrossRef]
27. Willson, G.B. Radar classification using a neural network. In *Applications of Artificial Neural Networks*; SPIE: Bellingham, WA, USA, 1990; Volume 1294, pp. 200–210. [CrossRef]
28. Candore, A.; Kocabas, O.; Koushanfar, F. Robust Stable Radiometric Fingerprinting for Wireless Devices. In Proceedings of the 2009 IEEE International Workshop on Hardware-Oriented Security and Trust, San Francisco, CA, USA, 27 July 2009; pp. 43–49. [CrossRef]
29. Danev, B.; Capkun, S.; Jayaram Masti, R.; Benjamin, T.S. Towards Practical Identification of HF RFID Devices. *ACM Trans. Inf. Syst. Secur.* **2012**, *15*, 1–24. [CrossRef]
30. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685. [CrossRef]
31. Baldini, G.; Steri, G. A Survey of Techniques for the Identification of Mobile Phones Using the Physical Fingerprints of the Built-In Components. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1761–1789. [CrossRef]
32. Zeng, K.; Govindan, K.; Mohapatra, P. Non-Cryptographic Authentication and Identification in Wireless Networks. *IEEE Wirel. Commun.* **2010**, *17*, 56–62. [CrossRef]
33. Hall, J.; Barbeau, M.; Kranakis, E. Detection of Transients in Radio Frequency Fingerprinting Using Signal Phase. *Wirel. Opt. Commun.* **2003**, *9*, 13–18.
34. Riyaz, S.; Sankhe, K.; Ioannidis, S.; Chowdhury, K. Deep Learning Convolutional Neural Networks for Radio Identification. *IEEE Commun. Mag.* **2018**, *56*, 146–152. [CrossRef]
35. Shen, G.; Zhang, J.; Marshall, A.; Peng, L.; Wang, X. Radio Frequency Fingerprint Identification for LoRa Using Deep Learning. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 2604–2616. [CrossRef]
36. Shen, G.; Zhang, J.; Marshall, A.; Cavallaro, J.R. Towards Scalable and Channel-Robust Radio Frequency Fingerprint Identification for LoRa. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 774–787. [CrossRef]
37. Shen, G. Deep Learning Enhanced Radio Frequency Fingerprint Identification for LoRa. Ph.D. Thesis, University of Liverpool, Liverpool, UK, June 2023.
38. Andrews, S.D. Extensions to Radio Frequency Fingerprinting. Ph.D. Thesis, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA, 2019.
39. Youssef, K.; Bouchard, L.; Haigh, K.; Silovsky, J.; Thapa, B.; Valk, C. Vander Machine Learning Approach to RF Transmitter Identification. *IEEE J. Radio Freq. Identif.* **2018**, *2*, 197–205. [CrossRef]
40. U.S. Department of Energy. Smart Grid. Available online: https://www.energy.gov/oe/services/technology-development/smart-grid (accessed on 16 September 2023).
41. Txone Networks. Achieving Energy Transformation: Building a Cyber Resilient Smart Grid. Available online: https://media.txone.com/prod/uploads/2023/04/Achieving-Energy-Transformation-Building-a-Cyber-Resilient-Smart-Grid-TXOne-WP-202303.pdf (accessed on 16 September 2023).

42. Lakshmanan, S.; Tsao, C.-L.; Sivakumar, R.; Sundaresan, K. Securing Wireless Data Networks against Eavesdropping Using Smart Antennas. In Proceedings of the 2008 the 28th International Conference on Distributed Computing Systems, Beijing, China, 17–20 June 2008; pp. 19–27. [CrossRef]
43. Raymond, D.R.; Midkiff, S.F. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervasive Comput.* **2008**, *7*, 74–81. [CrossRef]
44. Kannhavong, B.; Nakayama, H.; Nemoto, Y.; Kato, N.; Jamalipour, A. A Survey of Routing Attacks in Mobile Ad Hoc Networks. *IEEE Wirel. Commun.* **2007**, *14*, 85–91. [CrossRef]
45. Meyer, U.; Wetzel, S. A Man-in-the-Middle Attack on UMTS. In Proceedings of the 3rd ACM Workshop on Wireless Security, Philadelphia, PA, USA, 1 October 2004; ACM: New York, NY, USA, 2004; pp. 90–97. [CrossRef]
46. Ohigashi, T.; Morii, M. A practical message falsification attack on WPA. In Proceedings of the 2009 Joint Workshop on Information Security, Kaohsiung, Taiwan, 6–7 August 2009.
47. Paar, C.; Pelzl, J. *Understanding Cryptography: A Textbook for Students and Practitioners*; Springer: Berlin/Heidelberg, Germany, 2011; ISBN 9783642041006.
48. Elliott, C. Quantum Cryptography. *IEEE Secur. Priv.* **2004**, *2*, 57–61. [CrossRef]
49. Wang, J.; Liu, Y.; Niu, S.; Song, H.; Jing, W.; Yuan, J. Blockchain Enabled Verification for Cellular-Connected Unmanned Aircraft System Networking. *Future Gener. Comput. Syst.* **2021**, *123*, 233–244. [CrossRef]
50. Shwartz, O.; Mathov, Y.; Bohadana, M.; Elovici, Y.; Oren, Y. Opening Pandora's Box: Effective Techniques for Reverse Engineering IoT Devices. In Proceedings of the Smart Card Research and Advanced Applications: 16th International Conference, CARDIS 2017, Lugano, Switzerland, 13–15 November 2017; pp. 1–21. [CrossRef]
51. Lakew, Y.F.; Singh, A.K.; Bhatia, S. Assessing and Exploiting Security Vulnerabilities of Unmanned Aerial Vehicles. In *Smart Systems and IoT: Innovations in Computing*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 701–710. [CrossRef]
52. Schiansky, P.; Kalb, J.; Sztatecsny, E.; Roehsner, M.-C.; Guggemos, T.; Trenti, A.; Bozzio, M.; Walther, P. Demonstration of Quantum-Digital Payments. *Nat. Commun.* **2023**, *14*, 3849. [CrossRef]
53. Wang, W.; Sun, Z.; Piao, S.; Zhu, B.; Ren, K. Wireless Physical-Layer Identification: Modeling and Validation. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2091–2106. [CrossRef]
54. Brik, V.; Banerjee, S.; Gruteser, M.; Oh, S. Wireless Device Identification with Radiometric Signatures. In Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, San Francisco, CA, USA, 14 September 2008; ACM: New York, NY, USA, 2008; pp. 116–127. [CrossRef]
55. Communication Network Interdependencies in Smart Grids: Methodology for the Identification of Critical Communication Network Links and Components. Available online: https://www.enisa.europa.eu/publications/communication-network-interdependencies-in-smart-grids (accessed on 1 October 2023).
56. Kimani, K.; Oduol, V.; Langat, K. Cyber Security Challenges for IoT-Based Smart Grid Networks. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 36–49. [CrossRef]
57. Wang, W.; Lu, Z. Cyber Security in the Smart Grid: Survey and Challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
58. Yousaf, A.; Loan, A.; Babiceanu, R.F.; Yousaf, O. Physical-layer Intrusion Detection System for Smart Jamming Attacks. *Trans. Emerg. Telecommun. Technol.* **2017**, *28*, e3189. [CrossRef]
59. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. A Comparative Study of LPWAN Technologies for Large-Scale IoT Deployment. *ICT Express* **2019**, *5*, 1–7. [CrossRef]
60. Perez, M.; Sierra-Sanchez, F.E.; Chaparro, F.; Chaves, D.M.; Paez-Rueda, C.-I.; Galindo, G.P.; Fajardo, A. Coverage and Energy-Efficiency Experimental Test Performance for a Comparative Evaluation of Unlicensed LPWAN: LoRaWAN and SigFox. *IEEE Access* **2022**, *10*, 97183–97196. [CrossRef]
61. Hossain, M.I.; Markendahl, J.I. Comparison of LPWAN Technologies: Cost Structure and Scalability. *Wirel. Pers. Commun.* **2021**, *121*, 887–903. [CrossRef]
62. The Full Story on UK Smart Meters. Available online: https://www.smartme.co.uk/smets-2.html (accessed on 20 September 2023).
63. Agung Enriko, I.K.; Zaenal Abidin, A.; Noor, A.S. Design and Implementation of LoRaWAN-Based Smart Meter System for Rural Electrification. In Proceedings of the 2021 International Conference on Green Energy, Computing and Sustainable Technology (GECOST), Miri, Malaysia, 7 July 2021; pp. 1–5. [CrossRef]
64. Gallardo, J.L.; Ahmed, M.A.; Jara, N. LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid. *IEEE Access* **2021**, *9*, 124295–124312. [CrossRef]
65. Rawlinson, K. HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. Available online: https://www.proquest.com/docview/1549571608 (accessed on 3 December 2023).
66. Brar, H.S.; Kumar, G. Cybercrimes: A Proposed Taxonomy and Challenges. *J. Comput. Netw. Commun.* **2018**, *2018*, 1798659. [CrossRef]
67. Bouzidi, M.; Amro, A.; Dalveren, Y.; Alaya Cheikh, F.; Derawi, M. LPWAN Cyber Security Risk Analysis: Building a Secure IQRF Solution. *Sensors* **2023**, *23*, 2078. [CrossRef]
68. Bouzidi, M.; Mohamed, M.; Dalveren, Y.; Moldsvor, A.; Cheikh, F.A.; Derawi, M. Propagation Measurements for IQRF Network in an Urban Environment. *Sensors* **2022**, *22*, 7012. [CrossRef] [PubMed]
69. *EN 300 220-1 V2.4.1*; Technical Characteristics and Test Methods. European Committee for Electrotechnical Standardization: Brussels, Belgium, January 2012.

70. Shi, Y.; Davaslioglu, K.; Sagduyu, Y.E. Generative Adversarial Network for Wireless Signal Spoofing. In Proceedings of the ACM Workshop on Wireless Security and Machine Learning, Miami, FL, USA, 15 May 2019; ACM: New York, NY, USA, 2019; pp. 55–60. [CrossRef]
71. Li, G.; Yu, J.; Xing, Y.; Hu, A. Location-Invariant Physical Layer Identification Approach for Wi-Fi Devices. *IEEE Access* **2019**, *7*, 106974–106986. [CrossRef]
72. Sankhe, K.; Belgiovine, M.; Zhou, F.; Riyaz, S.; Ioannidis, S.; Chowdhury, K. ORACLE: Optimized Radio Classification through Convolutional Neural Networks. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019.