sensors

MDPI

*Article*

# Radio Frequency Fingerprint-Based Intelligent Mobile Edge Computing for Internet of Things Authentication †

**Songlin Chen [1], Hong Wen [2,*], Jinsong Wu [3,4], Aidong Xu [5], Yixin Jiang [5], Huanhuan Song [1] and Yi Chen [1]**

[1] National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China
[2] School of Aeronautics and Astronautics, University of Electronic Science and Technology of China, Chengdu 611731, China
[3] School of Artificial Intelligence, Guilin University of Electronic Technology, Guilin 541004, China
[4] Department of Electrical Engineering, Universidad de Chile, Av Tupper 2007, Santiago 8370451, Chile
[5] EPRI, China Southern Power Grid Co. Ltd., Guangzhou 510080, China
* Correspondence: sunlike@uestc.edu.cn
† This paper is the expanded version of "A Novel Terminal Security Access Method Based on Edge Computing for IoT" published in the Proceedings of the 2018 International Conference on Networking and Network Applications (NaNA), Xi'an, China, 12–15 October 2018.

Received: 10 June 2019; Accepted: 16 August 2019; Published: 19 August 2019

**Abstract:** In this paper, a light-weight radio frequency fingerprinting identification (RFFID) scheme that combines with a two-layer model is proposed to realize authentications for a large number of resource-constrained terminals under the mobile edge computing (MEC) scenario without relying on encryption-based methods. In the first layer, signal collection, extraction of RF fingerprint features, dynamic feature database storage, and access authentication decision are carried out by the MEC devices. In the second layer, learning features, generating decision models, and implementing machine learning algorithms for recognition are performed by the remote cloud. By this means, the authentication rate can be improved by taking advantage of the machine-learning training methods and computing resource support of the cloud. Extensive simulations are performed under the IoT application scenario. The results show that the novel method can achieve higher recognition rate than that of traditional RFFID method by using wavelet feature effectively, which demonstrates the efficiency of our proposed method.

**Keywords:** Mobile edge computing; IoT; RF Fingerprinting; authentication

## 1. Introduction

In recent years we have seen an innovative Internet-of-Things (IoT) paradigm, which combines mobile edge computing (MEC) with traditional IoT architecture [1–3]. MEC is used as a bridge between IoT devices and remote cloud devices to provide edge intelligent services to meet the critical needs of industry digitization in terms of agile connectivity, real-time services, data optimization, application intelligence, security and privacy protection, which are key issues for the industry control applications [4–6]. However, such new architecture has aroused many security protection requirements, including security access authentication, security transmission, and data privacy etc., in which the most important one is security access authentication [7]. Due to constraints of terminals under the IoT system, and resource constraints of the existing authentication methods that rely on

encryption, some lightweight and effective security access authentication measurements [8,9] are necessary. Recently, many researchers have turned to using the physical (PHY) layer information to enhance wireless security [10–12]. MEC operates on the wireless media. The innovative PHY-layer security designs can cope with the unique PHY layer weakness of the MEC in which physical characteristics, such as the channel responses between communication peers, the hardware property of the wireless transmitter, have been explored as a form of fingerprint in the scenario of wireless security.

Many scholars have made contributions to the development of physical layer security [13–15]. RFFID is of vital importance to physical layer security technology. In fact, radiofrequency fingerprints (RFF), which embody the hardware property of the wireless transmitter to be identified and have the characteristics difficult to be cloned, are a good candidate to be used to enhance device identification [16–21]. Additionally, RFFID is a lightweight authentication method for the transmitters, because the authentication algorithm is mainly performed on receivers and transmitters that do almost nothing. Therefore, it is especially suitable for the source-constrained terminals of IoT to perform access identification.

The RFFID method is different from the device signal authentication method proposed in [22]. The stochastic features of dynamic watermarking signal are used as identity information. Hall et al. [23] first proposed RF fingerprinting technology in Bluetooth wireless network device identification research in 2003. After that, studies have found that the transmitter can also be identified by transmitting the steady-state portion of the signal. Hu et al. [24] utilized RF signals to identify mobile phones in a mobile cellular network. Hall et al. [23] and Ureten et al. [25,26] used RF fingerprinting technology to achieve wireless positioning and access control for wireless network. In order to further improve the authentication rate of RFFID, a machine learning algorithm has been introduced in extensive research as the classification algorithm of RFFID [27–29]. However, a machine learning algorithm needs a certain amount of computing resources to ensure a higher recognition and authentication rate. Especially in offline training, the number of offline training samples will affect the effect of machine learning. With available computing resources, MEC can perform limited tasks in offline training of machine learning. When a large number of samples need to be trained, while uploading these computing cost tasks to cloud computing platform, the authentication rate can be expected to be further improved. In this article, we propose an efficient and flexible RFFID-MEC authentication method, in which RFFID is combined with MEC and the cloud, making full use of the characteristics of MEC-IoT framework to establish the two-layer model. The first layer provides data collection, extraction of RF fingerprint features, dynamic data storage and access authentication decision, which consumes less limited computing resources running at the MEC platform. The second-layer provides powerful computing for more complex and resource-consuming tasks in the remote cloud, such as feature learning, generating decision model, and establishing a machine learning algorithm. Since the authentication algorithm is mainly performed on the MEC, the terminals do almost nothing. The novel model, the edge computing, and cloud computing work collaboratively to ensure that the method has strong computing resources and improve the authentication rate. Compared with the conventional physical authentication method [10–12,30–33], our method makes efficient use of the characteristics of edge computing to collect transmitting signals and computing support of the cloud, and performs the fast identity authentication of terminals in the IoT scenario with asymmetric computing resources. Therefore, our proposed novel authentication scheme is light-weight to the IoT terminals. Our contributions can be summarized as follows:

(1) To the best of our knowledge, we are the first to propose the radio frequency fingerprint-based authentication, that combines physical characteristics of wireless device radio frequency and machine learning algorithms under the collaborative work of edge computing and cloud computing to achieve fast and efficient authentication.
(2) We present the typical scenario that uses an RFFID-MEC method for IoT devices authentication applications and demonstrate the effectiveness of the algorithm.

The rest of this article is organized as follows. In Section 2, we introduce the related work about the background information of MEC-IoT architecture and RFFID. The secure access authentication method based on RFFID- MEC is proposed in Section 3. Section 4 includes the application of the novel

method to typical scenario and the evaluation of the proposed methods via experiments. Finally, the conclusions are given in Section 5.

## 2. Background of RFFID-MEC

### *2.1. MEC Architecture in IoT*

The emergence of MEC brings a high-performance computing platform that provides data preprocessing, storage, and edge intelligent services [2]. As shown in Figure 1, the MEC-IoT architecture encompasses three different layers, the IoT devices, MEC, and the remote cloud platform. Each layer is characterized by different constraints on computation ability, memory, and energy availability. Among them, the computation ability of IoT terminals is the weakest. The MEC layer can perform limited tasks with available computing resources and the cloud layer provides strong computing support to the other two layers.

A key transformation is to perform information processing based on servers at network edge, applying the concepts of cloud computing. MEC can be seen as a cloud server running at the edge of a mobile network and performing specific tasks that are necessary to some scenarios, such as agile connectivity, real-time services, security and privacy protection, which could not be achieved with traditional IoT network infrastructure [1]. In addition, IoT devices are connected with MEC that provide (when needed) the computational resources for more complex and resource-demanding application or processing tasks. MEC devices are interconnected through MEC networking and linked to the remote cloud depending on application needs. As the traditional cloud-centered IoT architecture, MEC-IoT architecture is also confronted with security problems. Meanwhile, access authentication is envisioned as the primary problem to be solved. As a physical layer security technology, RFFID is regarded as a lightweight access authentication method, and applicable to the MEC-IoT architecture.

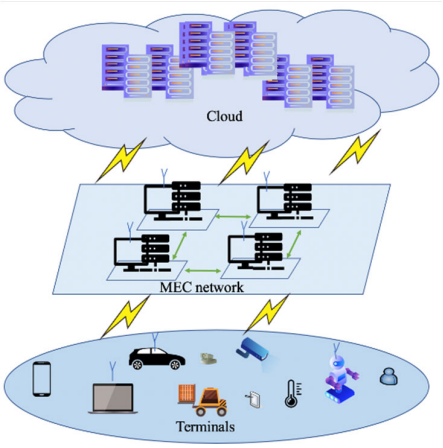



**Figure 1.** Mobile edge computing-Internet-of-Things (MEC-IoT) architecture.

### *2.2. Radio Frequency Fingerprinting Identification (RFFID)*

The RFFID method refers to identification based on the radio frequency signal fingerprint of the wireless devices to confirm the access of the legal wireless devices, thereby realizing the identity authentication of the wireless devices. The RFFID, which embodies the hardware property of the wireless transmitters, is difficult to be cloned and can be used for non-cryptographic authentication for the wireless transmitters. Cobb et al. [30] made a further explanation of the mechanism of RFF and introduced electronic component tolerances due to differences in hardware devices, such as printed circuit board traces, integrated circuit internal components, and RF front-end circuits. The electronic component tolerance effect of wireless transmitters is the main reason for generating RFF.

Since the hardware of any two wireless devices is different and hard to be faked, it is feasible to uniquely identify electronic components by RF signal fingerprinting.

As shown in Figure 2, the RFFID method consists of six steps: Signal collection, signal analysis and process, feature extraction and classification, fingerprint database, and identification. RFFID mainly includes two processes. The first one is offline to establish a fingerprint database for legitimate wireless devices by implementing, analyzing and processing the radiation signals after collecting the signals of legitimate devices. The second process is an online authentication process. The signals of the wireless devices to be identified are collected and the fingerprint features are extracted through signal analysis and processing. Then, matching and recognition are carried out in the existing legitimate fingerprint database.

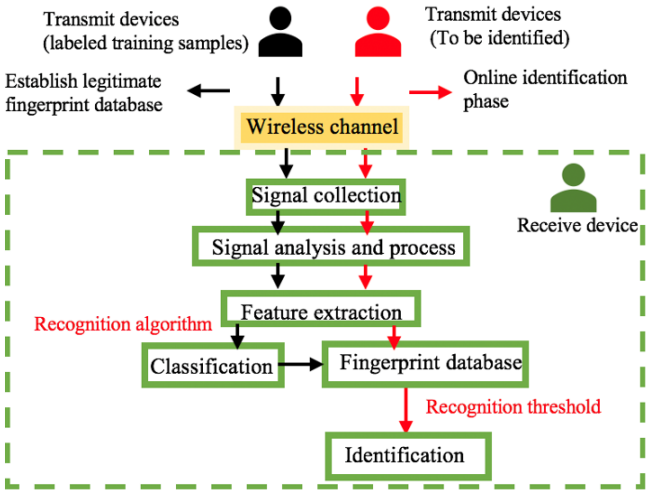



**Figure 2.** Radio frequency fingerprinting identification (RFFID) authentication method.

Recently, in order to further improve the authentication rate of RFFID, machine learning method is taken as a recognition algorithm [27–29]. However, this method consumes resources in offline samples learning due to a large number of samples training required to ensure the authentication effect. Otherwise, the authentication rate will be compromised if only limited training samples are used. Therefore, abundant computing resources are necessary to guarantee the authentication rate of RFFID. When the computing power of MEC devices is inadequate, it can upload tasks to the cloud platform. By this means, MEC can rationally get computational resources to support and fully ensure the accuracy of tasks. Therefore, a combination of the RFFID method, MEC and cloud can strengthen hardware resource guarantee.

## 3. Security Access Authentication Method Based on RFFID-MEC

In this section, we propose a lightweight algorithm for resource-constrained terminals to accomplish access authentication with a satisfied authentication rate. This algorithm that combines the mobile edge computing with the cloud may improve the accuracy of the authentication-based RFFID. The architecture of the proposed RFFID-MEC authentication consists of two layers: The first layer provides signal collection, signal analysis, and process, feature extraction and classification, and establish fingerprint feature database, which will be performed on the MEC layer. The second layer includes learning features, generating decision models, and implementing machine learning algorithms for recognition, which need the powerful computing support for much more complex and resource-consuming tasks, will be implemented on the remote cloud due to the limited computing resources of MEC. Figure 3 shows a detailed logical flow of this authentication process. The authentication process includes two processes that are an offline training process and an online decision-making process.

In the offline training authentication process, a terminal initiates an access request to the MEC platform. After that, the MEC platform collects the signal of the terminal with the identity information, and then performs feature extraction and establishes dynamic fingerprint feature database. The feature information is transmitted to the cloud computing platform. The cloud computing platform makes use of the machine learning algorithm to generate the authentication decision-making model, and transmits the resulted decision model that meets the target authentication rate back to the MEC platform. At this time, the offline training authentication process ends. In the online decision-making authentication process, a terminal initiates an access request to the MEC platform, and the MEC platform collects signals, extracts features, and performs fast identity authentication through the trained authentication model that was established from the previous step.

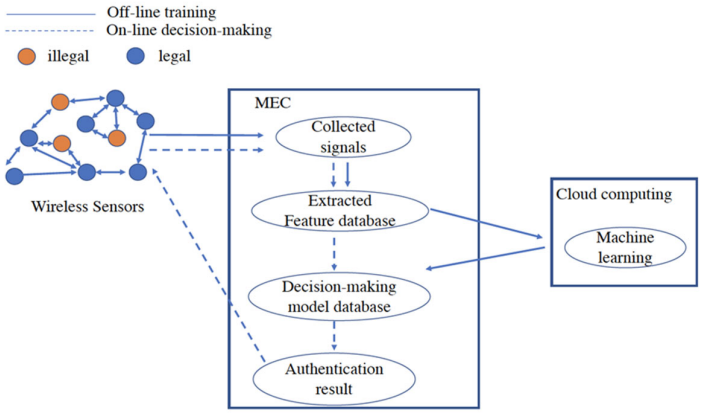



**Figure 3.** Detailed authentication process.

The RFFID-MEC algorithm is illustrated in Figure 4. Notations of frequently-used variables are described in Table 1 for steps. Steps 1–3, 5, 6 are carried out by the first layer, meanwhile Step 4, including Steps 4.1–4.6, are carried out by the second layer.

**Table 1.** Notations of frequently-used variables.

| Symbol | Description |
|---|---|
| $i$ | The $i$-th terminal |
| $N$ | Discrete points of signal acquisition |
| $x_i^{<l>T}$ | The $l$-th collection of the $i$-th terminal's vector |
| $X_i^{<l>T}$ | The total $l$-th times collection of the $i$-th terminal's set |
| $x_i^{<m>T}$ | The vector after remove the outline from the $x_i^{<l>T}$ |
| $X_i^{<m>T}$ | The set after remove the outline from the set $X_i^{<l>T}$ |
| $\overline{x_i^{<m>T}}$ | The data normalization of vector $x_i^{<m>T}$ |
| $\overline{X_i^{<m>T}}$ | The data normalization of set $X_i^{<m>T}$ |
| $\overline{\overline{x_i^{<m>T}}}$ | The vector $\overline{x_i^{<m>T}}$ generated after DTWT |
| $\overline{\overline{X_i^{<m>T}}}$ | The set $\overline{X_i^{<m>T}}$ generated after DTWT |
| $T$ | The training data set |
| $y_i$ | The category of the instance |

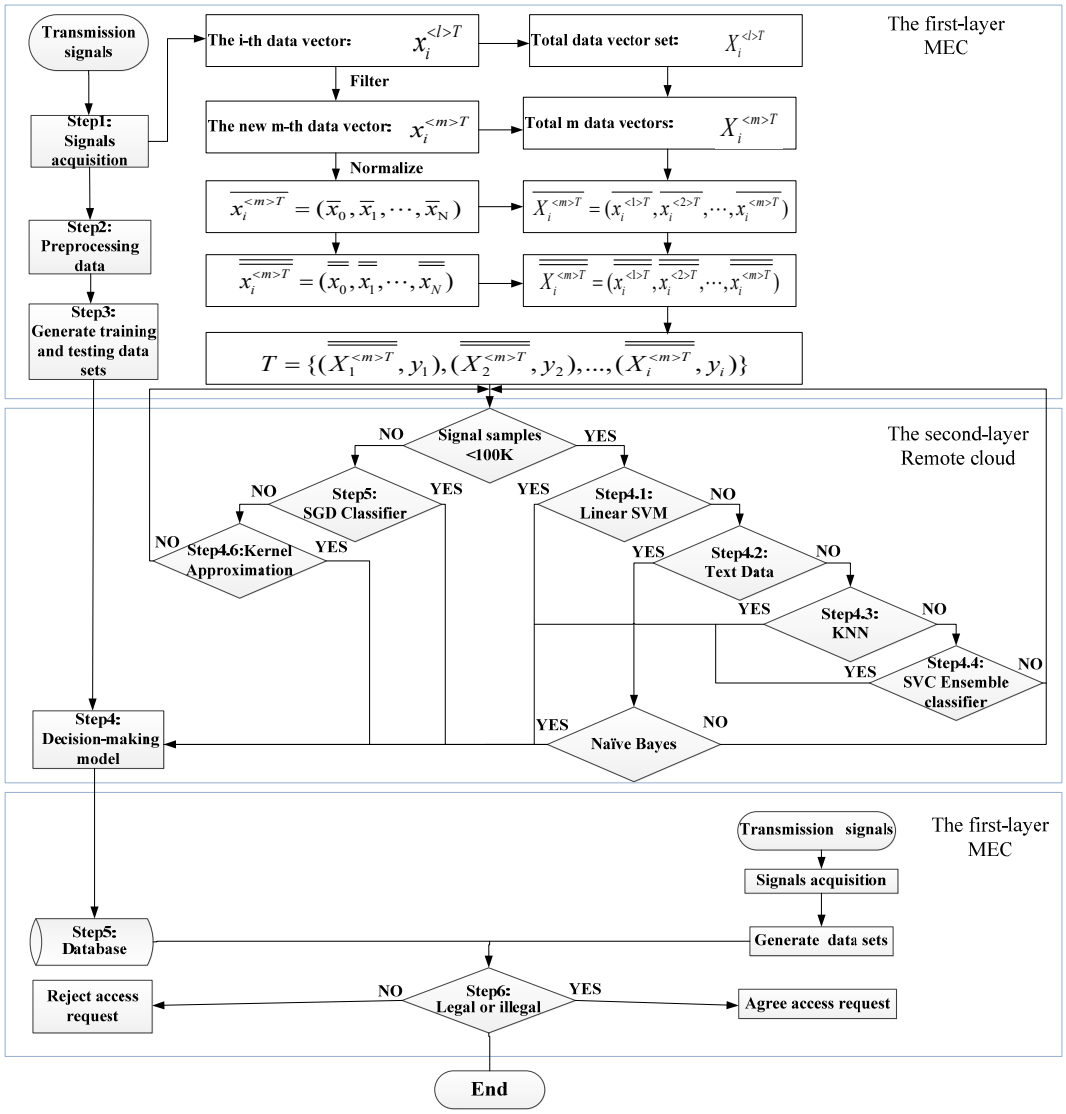



**Figure 4.** Flow chart of RFFID-MEC method algorithm.

Step 1: The MEC platform continuously acquires signals:
The MEC platform collects the RF signals of the IoT devices with identity tags:

1. The vector of the $l-th$ collection of the $i-th$ terminal device is: $x_i^{<l>T} = (x_0, x_1, \ldots, x_N)$,(N represents the discrete sample points of the collected signals)
2. The data set of the total $L$ acquisitions of the $l-th$ terminal devices is: $x_i^{<l>T} = (x_i^{<1>T}, x_i^{<2>T}, \ldots, x_i^{<L>T})$, $l = (1, 2, \cdots, L)$

Step 2: Data preprocessing in MEC platform:
The MEC platform preprocesses data sets for filtering and normalizing.

1 According to the data set, we obtain the mean $E(X_i^{<l>T})$ and, standard deviation $\sigma_{X^{<l>T}}$, and remove the outliers from the data set $X_i^{<l>T}$. Then $x_i^{<l>T}$ and, $X_i^{<l>T}$ were changed to: $x_i^{<m>T} = (x_0, x_1, \cdots, x_N)$ and, $X_i^{<m>T} = (x_i^{<1>T}, x_i^{<2>T}, \cdots, x_i^{<m>T})$, $m = (1, 2, \cdots, M)$, $M < L$.

2 $x_i^{<m>T} = (x_0, x_1, \cdots, x_N)$ was normalized to new value:

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i, i = 1, 2, 3, \cdots, N \quad (1)$$

$$\sigma^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2 \tag{2}$$

$$\overline{x_i} = \frac{x_i - \bar{x}}{\sigma} \tag{3}$$

$x_i^{<m>T}$ and, $X_i^{<m>T}$ were changed to:

$$\overline{x_i^{<m>T}} = (\overline{x_0}, \overline{x_1}, \cdots, \overline{x_N})$$

and

$$\overline{X_i^{<m>T}} = (\overline{x_i^{<1>T}}, \overline{x_i^{<2>T}}, ..., \overline{x_i^{<m>T}})$$

where $\overline{x_i^{<m>T}}$ has a standard normal distribution with mean zero and unit variance.

Step 3: The MEC platform generates training and testing data sets:

The normalized data sets $\overline{X_i^{<m>T}}$ are used by MEC platform to generate the feature vector as the training and testing data sets $T$ as follows:

$\overline{x_i^{<m>T}}$ are changed to $\overline{\overline{x_i^{<m>T}}}$

$$\begin{gathered} \varphi_{ik(n)} = f_i(n - 2^{i+1}k), (i = 0, 1, \cdots, J-2) \\ \overline{x_i^{<m>T}} = \sum_i \sum_k \overline{\overline{x_i^{<m>T}}} \varphi_{ik}(n) \end{gathered} \tag{4}$$

$\overline{X_i^{<m>T}}$ are changed to $\overline{\overline{X_i^{<m>T}}}$.

$$\overline{\overline{x_i^{<m>T}}} = (\overline{\overline{x_0}}, \overline{\overline{x_1}}, \cdots, \overline{\overline{x_N}})$$

$$\overline{\overline{X_i^{<m>T}}} = (\overline{\overline{x_i^{<1>T}}}, \overline{\overline{x_i^{<2>T}}}, \cdots, \overline{\overline{x_i^{<m>T}}})$$

T is the final generated training data sets given by:

$$T = \{(\overline{\overline{X_i^{<m>T}}}, y_1), (\overline{\overline{X_2^{<m>T}}}, y_2), ..., (\overline{\overline{X_i^{<m>T}}}, y_i)\}$$

$$m = (1, 2, ..., M), y_i \in Y = \{+1, -1\}$$

(+1 is represented as a legal terminal device, −1 is an illegal terminal device.)

Step 4: The cloud platform generates a decision-making model.

Step 4.1: When the number of sample data <100 K, we will choose a support vector machine (SVM) classification algorithm to generate a decision-making model:

$$\begin{gathered} \min \frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N}\alpha_i\alpha_j y_i y_j K(x_i, x_j) - \sum_{i=1}^{N}\alpha_i \\ s.t \sum_{i=1}^{N}\alpha_i y_i = 0, C \geq \alpha_i \geq 0, i = 1, 2, ..., N \end{gathered} \tag{5}$$

The decision-making model using the linear kernel function $K(\vec{x}, \vec{z}) = \vec{x} \bullet \vec{z}$, is applied to the linear classification of large data sets to find the optimal solution: $\vec{\alpha}^* = (\alpha_1^*, \alpha_2^*, \cdots, \alpha_N^*)^T$, $\vec{w}^* = \sum_{i=1}^{N}\alpha_i^* y_i \vec{x_i}$, choosing $C > \alpha_j^* > 0$, $b^* = y_j - \sum_{i=1}^{N}\alpha_i^* y_i K(\overline{\overline{X_i^{<m>T}}}, \overline{\overline{X_j^{<m>T}}})$.

The decision-making model is defined by:

$$f(\vec{x}) = sign(\sum_{i=1}^{N} \alpha_i^* y_i K(\overline{\overline{X_i^{<m>T}}}, \overline{\overline{X_j^{<m>T}}}) + b^*) \quad (6)$$

According to the training data sets testing model, if it can satisfy the correct target recognition rate, the current model is the decision-making model and transmitted to the MEC platform database, otherwise the algorithm will jump into Step 4.2.

Step 4.2: The cloud platform determines whether the data sets are text data. (a) If they are text data, using Naive Bayes, which can achieve the correct target recognition rate, then the current model is the decision-making model and transmitted to the MEC platform database, otherwise the algorithm will jump to Step 4. (b) If it is not text data, the algorithm will jump to Step 4.2.

Step 4.3: The cloud platform uses the (k-nearest neighbor) KNN classification algorithm to determine whether the correct recognition rate is greater than the preset one.

(a) Input the training data set T:

$$T = \{(\overline{\overline{X_1^{<m>T}}}, y_1), (\overline{\overline{X_2^{<m>T}}}, y_2), \cdots, (\overline{\overline{X_i^{<m>T}}}, y_i)\}$$

$\overline{\overline{X_i^{<l>T}}} \in \chi \subset R^n$ is the feature of the instance, and $y_i \in Y = \{+1\ -1\}$ is the category of the instance.

(b) Calculate the Euclidean distance:

$$L_p(\overline{\overline{X_i^{<m>T}}}, \overline{\overline{X_j^{<m>T}}}) = (\sum_{m=1}^{M} \left| \overline{\overline{x_i^{<m>T}}} - \overline{\overline{x_j^{<m>T}}} \right|^2)^{\frac{1}{2}} \quad (7)$$

(c) Find the k samples closest to $\overline{\overline{x_i^{<m>T}}}$ in the training data sets T, let the neighborhood of this t point be $N_t(\overline{\overline{x_i^{<m>T}}})$.

(d) Determine the category of $\overline{\overline{x_i^{<m>T}}}$ in $N_t(\overline{\overline{x_i^{<m>T}}})$, according to the classification decision is $y_i$:

$$\begin{aligned} y &= \arg\max_{C_j} \sum_{\overline{\overline{x_i^{<m>T}}} \in N} I(y_s = c_j) \\ &(s = 1, 2, \cdots, M * i; j = 1, 2) \end{aligned} \quad (8)$$

where $I$ is the indicator function. If $y_s = c_j$, then $I(y_s = c_j)$ is 1. By a similar argument, if $y_s \neq c_j$, then $I(y_s = c_j)$ is 0.

According to the training data sets testing model, if it can satisfy the correct recognition of the target, the current model is the decision model and transmitted to the MEC platform database, otherwise the algorithm will jump to Step 4.4.

Step 4.4: The cloud platform uses the integrated classifier to determine whether the correct recognition rate is greater than the preset. Integrated classifier, using a variety of existing learning algorithms from the training data to generate individual learners and based on Adaboost binary classification algorithm process, is as follows:

(a) Input the training data set T:

$$T = \{(\overline{\overline{X_1^{<m>T}}}, y_1), (\overline{\overline{X_2^{<m>T}}}, y_2), \cdots, (\overline{\overline{X_i^{<m>T}}}, y_i)\}$$

(b) Initialize the weight distribution of training data

$$D_1 = (w_{11} w_{12} \cdots w_{1q} \cdots, w_{1i}), w_{1q} = \frac{1}{i} q = 1, 2, \cdots, i$$

(c) Use the $D_h(h=1,2,\cdots,H)$ training data set with weights to learn to get the basic classifier

$$G_h(\overline{\overline{x_i^{<m>T}}}):X\to\{-1,+1\}$$

Calculate the classification error rate of $G_h(\overline{\overline{x_i^{<m>T}}})$ on the training data set given by:

$$\begin{aligned} e_h &= P(G_h(\overline{\overline{x_i^{<m>T}}})\neq y_i) \\ &= \sum_{q=1}^{i} w_{hq} I(G_h(\overline{\overline{x_i^{<m>T}}})\neq y_i) \end{aligned}$$

Calculate the coefficients of $G_h(\overline{\overline{x_i^{<m>T}}})$

$$\alpha_h = \frac{1}{2}\log\frac{1-e_h}{e_h} \tag{9}$$

Update the weight distribution of the training data sets:

$$\begin{aligned} &D_{h+1} = (w_{h+1,1}\cdots w_{h+1,q}\cdots, w_{m+1,i}) \\ &w_{h+1,q} = \frac{w_{hq}}{z_h}\exp(-\alpha_h y_q G_h(\overline{\overline{x_i^{<m>T}}})) \\ &(q=1,2,\cdots,i) \end{aligned} \tag{10}$$

$z_h$ is a normalization factor:

$$z_h = \sum_{q=1}^{i} w_{hq}\exp(-\alpha_h y_q G_h(\overline{\overline{x_i^{<m>T}}})) \tag{11}$$

It makes $D_{h+1}$ a probability distribution.

(d) Build a linear combination of basic classifiers:

$$f(x) = \sum_{h=1}^{H}\alpha_h G_h(\overline{\overline{x^{<m>T}}}) \tag{12}$$

(e) Get the final classifier:

$$\begin{aligned} G(\overline{\overline{x^{<m>T}}}) &= \mathrm{si}\,gn(f(x)) \\ &= \mathrm{si}\,gn(\sum_{h=1}^{H}\alpha_h G_h(\overline{\overline{x^{<m>T}}})) \end{aligned} \tag{13}$$

According to the testing set of test models, if it can satisfy the correct target recognition rate, the current model is the decision-making model and transmitted to output the MEC platform database, otherwise the algorithm will jump to Step 4.

Step 4.5: When the number of sample data is greater than 100 K, the SVM classification algorithm based on stochastic gradient descent is selected and the cost model is optimized by stochastic gradient descent method given by:

$$\begin{aligned} J(\theta) &= \frac{1}{s}\sum_{i=1}^{s}\frac{1}{2}(y^i - h_\theta(x^i))^2 \\ &= \frac{1}{s}\sum_{i=1}^{s}\cos t(\theta,(x^i,y^i)) \end{aligned} \tag{14}$$

The final decision-making model is an SVM algorithm based on the multi-class linear kernel. According to the testing data sets testing model, if it satisfies the correct target recognition rate, the current model is a decision-making model and transmitted to the MEC platform database, otherwise the algorithm will jump to Step 4.6 and continue to select the classification algorithm.

Step 4.6: Kernel approximation is a nonlinear classification model. Nonlinear SVM is a classification model based on linear SVM. Different kernel functions are used to realize the transformation of high-dimensional space map to low-dimensional space. The optional kernel functions are:

$$\begin{aligned} k(\vec{x},\vec{z}) &= (\gamma(\vec{x}\vec{z}+1)+r)^p \\ k(\vec{x},\vec{z}) &= \exp(-\gamma\left\|\vec{x}-\vec{z}\right\|^2) \\ k(\vec{x},\vec{z}) &= \tanh(\gamma(\vec{x}\vec{z})+r) \\ k(x,y) &= \sum_i \frac{2x_i y_i}{x_i+y_i} \\ k(x,y) &= \prod_i \frac{2\sqrt{x_i+c}\sqrt{y_i+c}}{x_i+y_i+2c} \end{aligned} \tag{15}$$

According to the testing set test model, if it satisfies the correct target recognition rate, the current model is the decision-making model and transmitted to the MEC platform database, otherwise the algorithm will jump to Step 4.

Step 5: The MEC platform stores the decision-making model and data set in the database.

Step 6: The MEC platform implements access authentication to determine whether it is legal.

Step 7: The MEC platform continuously collects the RF signals of the IoT devices with identity tags: The MEC platform collects the signal and preprocesses the data, and then passes the processed data and the training data set in the database through the decision model to judge whether the terminal identity is legal. If it is the legal device, MEC platform consents the access request. If it is not legal, the MEC platform refuses to access the request.

The main features of the RFFID-MEC architecture are:

1. Low-complexity: There is no need for encryption algorithm at the terminal node, and all the identification algorithms are completed by MEC. Therefore, the novel authentication method is especially beneficial to the terminals that are resource-constrained.
2. Low-latency: As the decision-making model has been generated by cloud computing and transmitted to MEC platform, it considerably reduces decision latency. This becomes particularly important for IoT scenarios, for example, when dealing with a large number of legitimate users' access requests that need low latency and real-time access authentication such as a driverless scenario.
3. Universality: This method is suitable for interconnection of resource-constrained IoT devices in 5G networks. Meanwhile, it has the characteristics of low computational complexity and high authentication accuracy.

## 4. RFFID-MEC Authentication Method Evaluation

We demonstrate a typical application scenario of RFFID-MEC Authentication method, as illustrated in Figure 5. IoT terminals are many NRF24Les nodes. More specifically, NRF24LE is a single RF transceiver chip and the operating frequency range is from 2.4 to 2.525 GHz. Its internal components include frequency synthesizer, power amplifier, crystal oscillator, GFSK modulator, and filters. NRF24LE chip is characterized by small power consumption, monolithic and small size. It is widely used in home automation and factory control [34]. MEC platform was composed of Universal Radio Software Peripheral (USRP). USRP is an open-source software-defined radio platform, which is consisted of a mother-board equipped with a dual 14-bit analog to digital converter (ADC) operating at 100 MHz and dual 16-dit digital to analog converter (DAC) operating at 400 MHz, and two UBX160 daughter boards and vert2450 antennas. UBX160 transceiver daughter boards that act as a front end and have a frequency range from 10 MHz to 6 GHz, which allows transmitting and

receiving in the 2.4 GHz industrial, scientific, and medical radio band (ISM band) [35]. Cloud server is taken as a cloud platform.

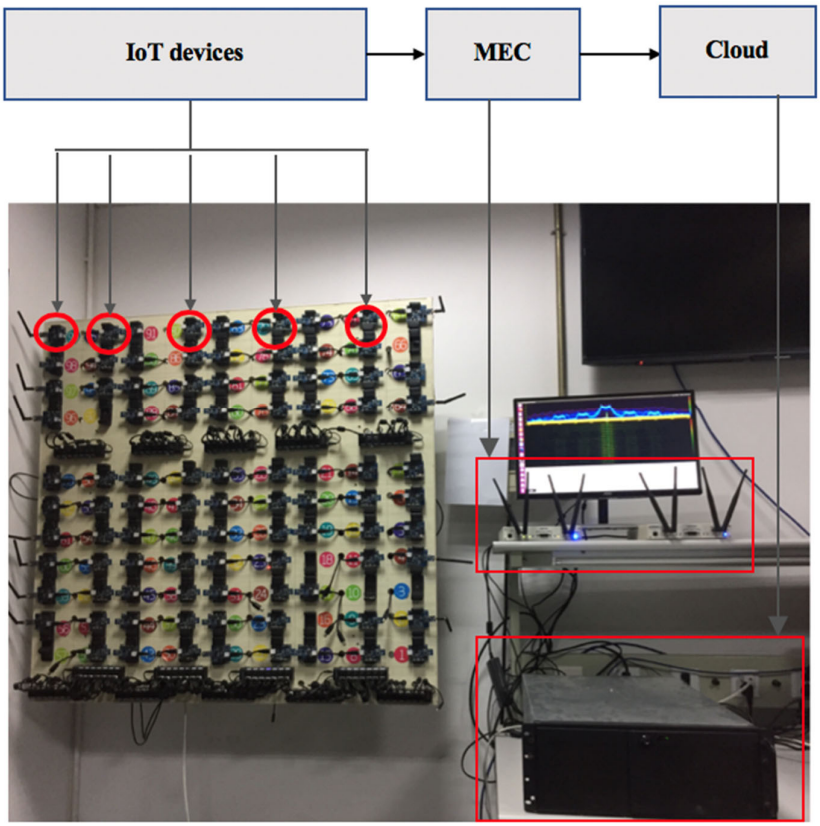



**Figure 5.** Typical application scenarios of RFFID-MEC authentication method.

There are several steps in our experiment:

The steps of the offline training authentication are as follows.

Step 1: Two terminal nodes with identity tags (illegal, legal) send signals to MEC platform, then the MEC platform collects the signals;

Step 2: The MEC platform preprocesses the collected signals to establish a fingerprint feature database;

Step 3: The MEC platform generates training and testing data sets, which are transmitted to the cloud platform;

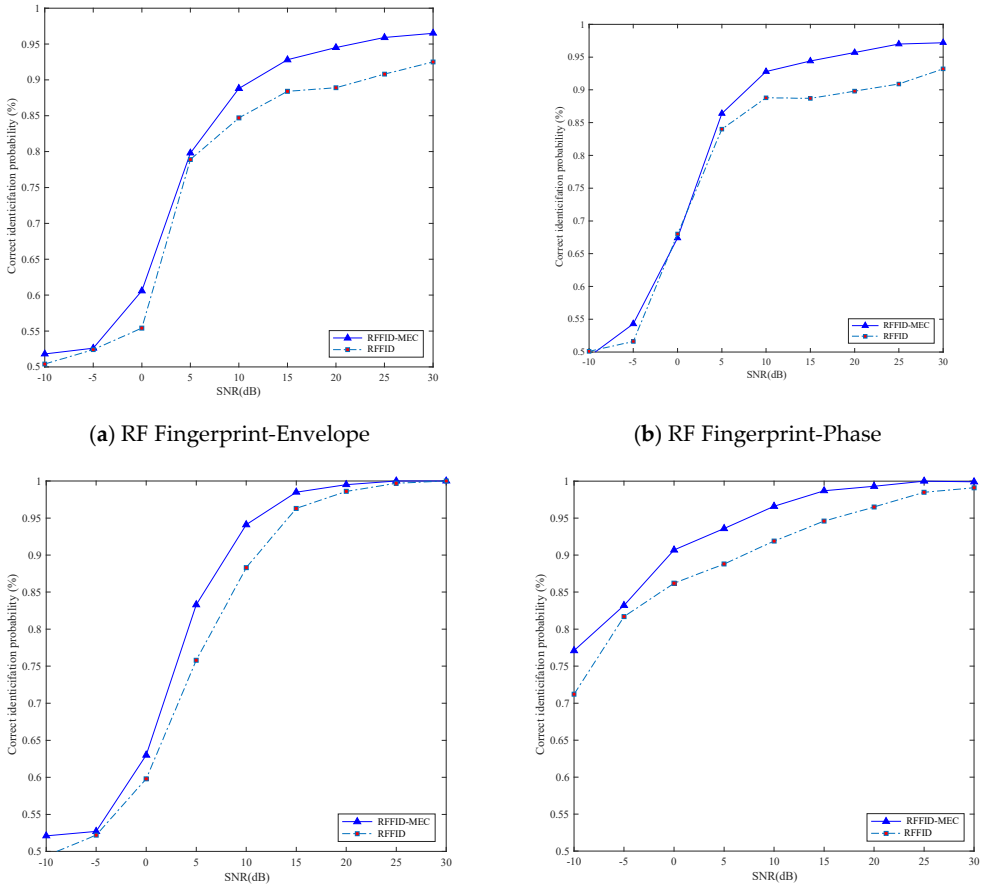
Step 4: The cloud platform performs the training processing and generates a decision-making model, which is transmitted back to the MEC platform;

Step 5: The MEC platform stores the decision-making model. Online decision-making authentication includes one step as follows:

Step 6: Terminals (illegal, legal) send signals to the MEC platform. The MEC platform generates feature data sets and determines whether it is legal or not via a previously trained model.

In addition, we have compared RFFID-MEC with traditional RFFID methods. Our simulation utilizes each of four kinds of RF fingerprint features to verify the authentication effect under different SNR. Compared with the traditional RFFID method, the RFFID-MEC method takes advantage of the cloud computing platform to increase the number of offline training samples in a machine learning algorithm. As shown in Figure 6, from the four simulation results, it can be seen that whether using envelope, phase, STFT, or wavelet feature, the correct identification probability of RFFID-MEC method is higher than that of RFFID method at different SNR. Besides, the simulation indicates that the correct identification probability of wavelet feature clearly outperforms the other ones and

achieves a higher correct identification rate at low SNR, because the fingerprint of wavelet transform possesses strong anti-noise characteristics [36]. Therefore, we demonstrate the effectiveness of the proposed RFFID-MEC method choosing wavelet RF feature, which can be applied to security authentication.




(**a**) RF Fingerprint-Envelope (**b**) RF Fingerprint-Phase

(**c**) RF Fingerprint-STFT (**d**) RF Fingerprint-wavelet

**Figure 6.** Correct identification probability versus SNR for RFFID-MEC and RFFID using four different RF fingerprint features including: Envelope, phase, STFT, and wavelet feature.

## 5. Conclusions

The paper has developed a lightweight RFFID-MEC authentication method by taking advantage of attributes-based MEC, cloud, and non-encryption RFFID for IoT terminals. The presented two-layer model is extremely suitable for the MEC-based IoT paradigms. Compared with the traditional RFFID security access authentication, our light-weight RFFID-MEC authentication method has achieved higher authentication accuracy and improved the work efficiency of IoT terminals, in which all the computing burdens are taken by the edge devices and the cloud. Subsequently, we put this method into an application scenario. Our simulations have demonstrated the effectiveness of this method in actual IoT environments.

**Author Contributions:** S.C. and H.S. contributed to the main results and code implementation. H.W. and J.W. organized the work, and revised the draft of the paper. S. C. and H. W. designed the experiments. S.C., H.S. and Y.C. performed the experiments. S.C. and H. W. analyzed the experimental results. S.C., H.W., A.X., Y.J., H.S., and Y.C. discussed the results. S.C. wrote the original manuscript.

**Funding:** This research was supported by National Key R&D Program of China (2018YFB0904900, 2018YFB0904905). This research was also supported in part by Chile CONICYT FONDECYT Regular Project 1181809

**Conflicts of Interest:** The authors declare no conflicts of interests.

## References

1. Chiang M.; Zhang T. Fog and IoT: An overview of research opportunities. *IEEE Internet Things J.* **2016**, *3*, 854–864.
2. Mao Y.; You C.; Zhang J.; Huang K.; Letaief K.B. A survey on mobile edge computing: The communication perspective. *IEEE Commun. Surv. Tuts.* **2017**, *19*, 2322–2358.
3. Xie Y.; Wen H.; Wu B.; Jiang, Y.; Meng, J. A Modified Hierarchical Attribute-Based Encryption Access Control Method for Mobile Cloud Computing. *IEEE Trans.Cloud Comput.* **2015**, *7*, 383–391.
4. Zhang, K.; Leng, S.; He, Y.; Maharjan, S.; Zhang, Y. Mobile edge computing and networking for green and low-latency internet of things. *IEEE Commun. Mag.* **2018**, *56*, 39–45.
5. Chen, S.; Wen, H.; Wu, J.; Lei, W.; Hou, W.; Liu, W.; Xu, A.; Jiang, X. Internet of Things Based Smart Grids Supported by Intelligent Edge Computing. *IEEE Access* **2019**, *7*, 74089–74102.
6. Pan, F.; Pang, Z.; Wen, H.; Luvisotto, M.; Xiao, M.; Liao, R.F.; Chen, J. Threshold-Free Physical Layer Authentication Based on Machine Learning for Industrial Wireless CPS. *IEEE Trans. Indus. Inf.* **2019**. doi:10.1109/TII.2019.2925418.
7. Pan, F.; Pang, Z.; Luvisotto, M.; Jiang, X.; Jansson, R.N.; Xiao, M.; Wen, H. Authentication Based on Channel State Information for Industrial Wireless Communications. In Proceedings of IECON the 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 21–23 October 2018.
8. Jing, Q.; Vasilakos, A.V.; Wan, J.; Lu, J.; Qiu, D. Security of the internet of things: Perspectives and challenges. *Wirel. Networks* **2014**, *20*, 2481–2501.
9. Zhang, K.; Liang, X.; Lu, R.; Shen, X. Sybil attacks and their defenses in the internet of things. *IEEE Internet Things J.* **2014**, *1*, 372–383.
10. Chen, Y.; Wen, H.; Song, H.; Chen, S.; Xie, F.; Yang, Q.; Hu, L. Lightweight one-time password authentication scheme based on radiofrequency fingerprinting. *IET Commun.* **2018**, *12*, 1477–1484.
11. Wen H.; Li S.; Zhu X.; Zhou, L. A framework of the PHY-layer approach to defense against security threats in cognitive radio networks. *IEEE Network* **2013**, *27*, 34–39.
12. Wen, H.; Wang, Y.; Zhu, X. Physical layer assist authentication technique for smart meter system. *IET Commun.* **2013**, *3*, 189–197.
13. Wen, H.; Ho, P.H.; Qi, C.; Gong, G. Physical layer assisted authentication for distributed *ad hoc* wireless sensor networks. *IET Inf. Secur.* **2010**, *4*, 390–396.
14. Rehman S.U.; Sowerby K.; Coghill C. RF fingerprint extraction from the energy envelope of an instantaneous transient signal. In Proceedings of the Australian Communications Theory Workshop (AusCTW), Wellington, New Zealand, 30 January–2 February 2012.
15. Dubendorfer C.K.; Ramsey B.W.; Temple M.A. An RF-DNA verification process for ZigBee networks. In Proceedings of the IEEE Military Communications Conference, Orlando, FL, USA, 29 October–1 November 2012.
16. Patel H. Non-parametric feature generation for RF-fingerprinting on ZigBee devices. In Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), Verona, NY, USA, 26–28 May 2015.
17. Baldini G.; Giuliani R.; Steri G.; Neisse R. Physical layer authentication of internet of things wireless devices through permutation and dispersion entropy. In Proceedings of the Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017.
18. Chen S.; Wen H.; Wu J.; Chen, J.; Liu, W.; Hu, L.; Chen, Y. Physical layer channel authentication for 5G via machine learning algorithm. *Wirel. Commun. Mob. Comput.* **2018**. doi:10.1155/2018/6039878.
19. Xie, F.; Wen, H.; Li, Y.; Chen, S.; Hu, L.; Chen, Y.; Song, H. Optimized coherent integration-based radio frequency fingerprinting in internet of things. *IEEE Internet Things J.* **2018**, *5*, 3967–3977.
20. Ferdowsi A.; Saad W. Deep Learning for Signal Authentication and Security in Massive Internet-of-Things Systems. *IEEE Trans. Commun.* **2019**, *67*, 1371–1387.
21. Hu, L.; Wen, H.; Wu, B.; Pan, F.; Liao, R.F.; Song, H.; Tang, J.; Wang, X. Cooperative jamming for physical layer security enhancement in internet of things. *IEEE Internet Things J.* **2018**, *5*, 219–228.

22. Hu, L.; Wen, H.; Wu, B.; Tang, J.; Pan, F.; Liao, R.F. Cooperative jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers. *IEEE Trans. Veh. Technol.* **2018**, *67*, 2108–2117.
23. Hall J.; Barbeau M.; Kranakis E. Detection of transient in radio frequency fingerprinting using signal phase. *Wirel. Opt. Commun.* **2003**, 13–18. doi:10.1155/2018/6039878.
24. Hu N.; Yao Y. Identification of legacy radios in a cognitive radio network using a radio frequency fingerprinting based method. In Proceedings of the IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 10–15 June 2012.
25. Ureten O.; Serinken N. Bayesian detection of wi-fi transmitter RF fingerprints. *Electron. Lett.* **2005**, *41*, 373–374.
26. Ureten O.; Serinken N. Wireless security through RF fingerprinting. *Can. J. Electr. Comput. Eng.* **2007**, *32*, 27–33.
27. Merchant K.; Revay S.; Stantchev G.; Nousain B. Deep Learning for RF Device Fingerprinting in Cognitive Communication Networks. *IEEE J. Sel. Top. Signal Process.* **2018**, *12*, 160–167.
28. Youssef K.; Bouchard L.; Haigh K.; Silovsky J.; Thapa B.; Valk C.V. Machine Learning Approach to RF Transmitter Identification. *IEEE J. Radio Freq. Identif.* **2018**, *2*, 197–205.
29. McGinthy J.M.; Wong L.J.; Michaels A.J. Groundwork for Neural Network-Based Specific Emitter Identification Authentication for IoT. *IEEE Internet Things J.* **2019**, *4*, 6429–6440.
30. Weiner M.; Jorgovanovic M.; Sahai A.; Nikolié, B. Design of a low-latency, high-reliability wireless communication system for control applications. In Proceedings of the IEEE International Conference on Communications (ICC), Sydney, Australia, 10–14 June 2014.
31. Cobb W.E.; Laspe E.D.; Baldwin R.O.; Temple, M.A.; Kim, Y.C. Intrinsic physical-layer authentication of integrated circuits. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 14–24.
32. Suski II, W.C.; Temple, M.A.; Mendenhall, M.J.; Mills, R.F. Using spectral fingerprints to improve wireless network security. In Proceedings of the IEEE Global Telecommunications Conference, New Orleans, LO, USA, 30 November–4 December 2008.
33. Pan, F.; Pang, Z.; Xiao, M.; Wen, H.; Liao, R.F. Clone detection based on physical layer reputation for proximity service. *IEEE Access*, **2019**, *7*, 3948–3957.
34. Nordic, Nordic Semiconductor-nrf24 Series. Available online: https://www.nordicsemi. com/Products/Low-power-short-range-wireless/nRF24-series (accessed on 29 January 2019).
35. Ettus Research, Universal Software Radio Peripheral. Available online: https://www.ettus. com/ (accessed on 29 January 2019).
36. Klein R.W.; Temple M.A.; Mendenhall M.J. Application of wavelet-based RF fingerprinting to enhance wireless network security. *J. Commun. Networks* **2009**, *11*, 544–555.