sensors

MDPI

Article

Inter-Frame-Relationship Protected Signal: A New Design for Radio Frequency Fingerprint Authentication

Xufei Li [1,*], Shuiguang Zeng [2] and Yangyang Liu [1]

[1] School of Computer Science and Technology, Xidian University, Xi'an 710071, China; liuyangyang@stu.xidian.edu.cn
[2] College of Computer and Cyber Security, Hebei Normal University, Shijiazhuang 050024, China; sgzeng@hebtu.edu.cn
* Correspondence: chinalixufei@gmail.com

Abstract: Utilizing a multi-frame signal (MFS) rather than a single-frame signal (SFS) for radio frequency fingerprint authentication (RFFA) shows the advantage of higher accuracy. However, previous studies have often overlooked the associated security threats in MFS-based RFFA. In this paper, we focus on the carrier-sense multiple access with collision avoidance channel and identify a potential security threat, in that an attacker may inject a forged frame into valid traffic, making it more likely to be accepted alongside legitimate frames. To counter such a security threat, we propose an innovative design called the inter-frame-relationship protected signal (IfrPS), which enables the receiver to determine whether two consecutively received frames originate from the same transmitter to safeguard the MFS-based RFFA. To demonstrate the applicability of our proposition, we analyze and numerically evaluate two important properties: its impact on message demodulation and the accuracy gain in IfrPS-aided, MFS-based RFFA compared with the SFS-based RFFA. Our results show that the proposed scheme has a minimal impact of only −0.5 dB on message demodulation, while achieving up to 5 dB gain for RFFA accuracy.

Keywords: radio frequency fingerprint authentication; CSMA/CA; inter-frame-relationship; carrier frequency offset

check for updates

Citation: Li, X.; Zeng, S.; Liu, Y. Inter-Frame-Relationship Protected Signal: A New Design for Radio Frequency Fingerprint Authentication. *Sensors* **2023**, *23*, 6948. https://doi.org/10.3390/s23156948

Academic Editors: Mikael Gidlund, Zheng Yan, Qinghua Wang and Rahim Rahmani

Received: 13 June 2023
Revised: 28 July 2023
Accepted: 1 August 2023
Published: 4 August 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Radio frequency fingerprint authentication (RFFA) is a novel approach that leverages the inherent randomness of radio frequency hardware imperfections to authenticate transmitters. These hardware imperfections, including carrier frequency offset (CFO) [1], in-phase/quadrature (I/Q) imbalance [2], and I/Q origin offset [3], possess inherent, unique, and non-reproducible properties. Thus, they can be used for identity authentication without the need for traditional credentials such as tokens or digital signatures. As a result, RFFA has emerged as a prominent technology for identity authentication in future wireless networks [4–6].

Although RFFA has been extensively studied over the past few decades, achieving high accuracy remains a significant challenge. To address this issue, many researchers have devoted themselves to two approaches. The first approach is to explore potential hand-crafted features according to underlying hardware imperfections. For instance, the authors in [7] first proposed five features, and the authors in [6] proposed a new feature called fractal dimension that can be used for RFFA. The second approach is to utilize machine learning techniques to automatically extract and apply the features for RFFA. For example, the authors in [8] proposed a machine learning-based method to dynamically determine the feature decision threshold in RFFA, and the authors in [9] proposed an incremental learning method to continuously realize the feature extraction. The complicated computation involved in the second approach has also been of concern; for example, the authors in [10] proposed a transfer learning method to reduce the computation

required for edge nodes while accurately extracting the feature. Note that, for both of these two approaches, applying a multi-frame signal (MFS) performs with higher accuracy than a single-frame signal (SFS) as the input of the authenticator. This is because the MFS-based RFFA leverages the integration of multiple frames to mitigate the adverse noise effect. This approach is practical to implement, since one communication session typically involves multiple frames serving as candidates for constructing the MFS. As a brilliant study, the authors in [7] demonstrated that, by increasing the number of frames involved in the signal from 1 to 10, the RFFA accuracy improved from 30% to 90%. Despite the benefits touted by many researchers regarding this approach, they have frequently overlooked the potential security threats associated with it.

In this paper, we address a security threat associated with the aforementioned approach. Our observation is that, if an attacker injects a forged frame into the valid traffic, the forged frame can potentially blend in with other legitimate frames during the authentication process, as illustrated in Figure 1. Intuitively speaking, this may increase the likelihood of the forged frame being accepted, in a way that is even more pronounced compared with that of the single-frame signal (SFS)-based RFFA. To validate this intuition, we also conducted a Proof-of-Concept experiment (see Section 3.3), and the results clearly demonstrated this security threat. Regrettably, conducting such an injection attack is relatively straightforward for carrier-sense multiple access with collision avoidance (CSMA/CA). This is because that attackers can arbitrarily employ an idle channel to conduct the traffic injection by modifying the Backoff time [11]. Given the widespread application of CSMA/CA, it becomes crucial to address this security threat when promoting the adoption of MFS-based RFFA.

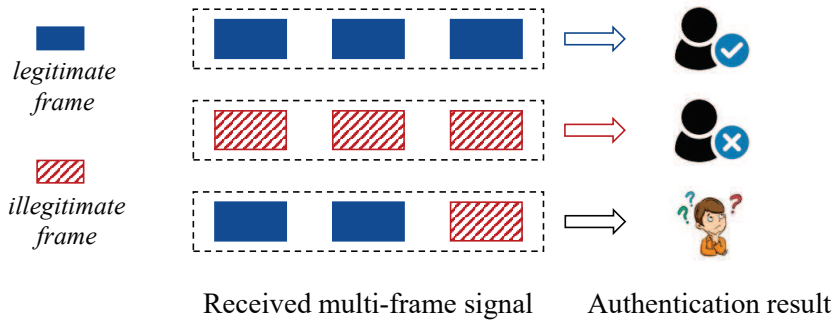

Figure 1. Three traffic types of received frames: all frames are legitimate, all frames are illegitimate, and some frames are legitimate while the rest are illegitimate. Each type of traffic is regarded as a whole in MFS-based RFFA.

To provide an MFS-based RFFA scheme overriding the above security threat, we propose an innovative design called the inter-frame-relationship protected signal (IfrPS). The core concept of IfrPS is to bind each pair of consecutively transmitted frames' signal with unique information, which can be used by the receiver to determine whether two consecutively received frames originate from the same transmitter. Meanwhile, frames that do not conform to the inter-frame relationship are excluded from the MFS-based RFFA process. Note that the unique information is randomly generated for each pair of consecutively transmitted frames and, thus, it cannot be forged by the attacker. Note that the proposed IfrPS-aided, MFS-based RFFA is applicable to these CSMA/CA communication systems, such as IEEE 802.15.4 and IEEE 802.11, in which a security level is required.

To demonstrate the applicability of our proposition, we considered two properties: efficiency and effectiveness. Efficiency evaluates the impact of IfrPS on message communication, while effectiveness quantifies the accuracy improvement achieved by IfrPS-aided, MFS-based RFFA compared to an SFS-based one. The main contributions of this paper are summarized as follows:

1. This study is the first to identify a security threat associated with MFS-based RFFA. In the CSMA/CA scenario, an attacker can inject forged frames into legitimate traffic. The MFS-based RFFA would be compromised when such an injection is not detected. We further substantiate this security threat through a Proof-of-Concept experiment;
2. To address this security threat and provide a robust MFS-based RFFA scheme, we propose the IfrPS design. The designed IfrPS can be integrated into the MFS-based RFFA to enable the receiver to detect injected frames within valid traffic. Moreover, IfrPS requires no pre-shared key between the transceiver and is compatible with old receivers because it does not need to authenticate the transmitter;
3. We analyze the potential impact of the IfrPS design on message demodulation for different constellations, including BPSK, QPSK, and 16QAM. Theoretical analysis and numerical evaluations demonstrate that the IfrPS design causes minimal degradation to message demodulation, with approximately -0.5 dB observed for the BPSK modulation system;
4. To quantify the accuracy improvement in the IfrPS-aided, MFS-based RFFA compared with the SFS-based one, we conducted a case study using CFO as the authentication feature. Through theoretical analysis and numerical evaluations, we assessed the false reject ratio (FRR) at different false accept ratio (FAR) levels. The results indicate that the proposed approach can achieve up to 5 dB gain compared to the SFS-based RFFA.

The remainder of this paper is organized as follows. Related work is introduced in Section 2. Section 3 presents the system model and security threat. In Section 4, we present the designed IfrPS and the IfrPS-aided, MFS-based RFFA scheme. In Section 5, we study the efficiency of the IfrPS design, and, in Section 6, we study the effectiveness of the IfrPS-aided, MFS-based RFFA. This paper is concluded in Section 7.

The abbreviations used in this paper are summarized in Table 1.

Table 1. Summary of abbreviations.

Abbreviation	Full Name
MFS	Multi-frame signal
SFS	Single-frame signal
RFFA	Radio frequency fingerprint authentication
CSMA/CA	Carrier-sense multiple access with collision avoidance
IfrPS	Inter-frame-protected signal
I/Q	In-phase/quadrature
BPSK	Binary phase shift keying
QPSK	Quadrature phase shift keying
16QAM	16-quadrature amplitude modulation
CFO	Carrier frequency offset
FRR	False reject rate
FAR	False accept rate
SNR	Signal-to-noise rate
HMAC	Hash message authentication code
ACK	Acknowledgment
MAC	Medium access control
IP	Internal protocol

2. Background

2.1. RFFA

As listed in Table 2, there are two approaches in RFFA research. To the best of our knowledge, [7] is the first approach for exploiting hardware imperfections to serve as the wireless device identity for RFFA. The work in [7] adopted five features (i.e., frequency error, synchronization correlation, I/Q origin offset, magnitude error, and phase error) extracted from IEEE 802.11 frame signal to distinguish different NICs. The experiment results from an indoor wireless test-bed environment demonstrated that PARADIS could differentiate more than 130 NICs with an accuracy greater than 99%. Additionally, the authors in [12] exploited

the non-linearity characteristic in the digital-to-analogue converter for device authentication and reported an authentication accuracy of 60% in their simulation with 100 devices and a signal-to-noise ratio (SNR) of 30 dB. The CFO was studied in [9] to distinguish 30 Xbee devices, and the experimental results reported an authentication accuracy of 95%. In addition, I/Q imbalance was investigated in [13] to distinguish four Zigbee devices, and an authentication accuracy of 100% was reported. In recent years, the authors in [5] explored a new feature, named visibility graph, of wireless signals and experimentally demonstrated that it could enhance the RFFA accuracy by being involved with the five features proposed in [7]. Furthermore, the authors in [6] proposed a new feature, named fractal dimension, of wireless signals and also theoretically analyzed and experimentally evaluated its effectiveness in RFFA. It can be seen from the literature that exploring new features has been an appealing research field to enhance the RFFA accuracy. Except for the above hand-draft feature-based RFFA, there is also another approach that utilizes the deep learning technique to automatically extract the "deep" fingerprint. In such an approach, the authors in [14] explored the device imperfections of controller area networks and found that, by applying the deep learning technique, the achieved RFFA accuracy increased from 92% to 96%. Moreover, the authors in [15,16] adopted convolutional neural networks to reduce the training complexity in RFFA and reported that the computation resources can be greatly reduced by using the CNN without affecting the accuracy. Towards this direction, the authors in [17] proposed to combine the signal samples from different receivers, which can reduce the required complexity in the neural networks, since it can obtain a benefit to accuracy from the data augmentation.

Table 2. Classification of researches on RFFA.

Class	Description	Reference
Hand-craft feature	Extracting features with artificially designed algorithms	[5–7,9,12,13]
Deep feature	Extracting features automatically using neural networks	[14–17]

2.2. Traffic Anomaly Detection

Our considered security threat in MFS-based RFFA arises from the fact that an attacker may inject one forged frame into valid traffic, which compromises the MFS-based RFFA if such injected is not detected. Note that such an injection causes a traffic anomaly, and there exist two types of solutions in the literature for traffic anomaly detection, as listed in Table 3.

Table 3. Classification of research on traffic anomaly detection.

Class	Description	Reference
Detection-based	Detect the appearance of anomalous traffic	[18–23]
Prevention-based	Detect the injected frame for discarding	[24,25]

The first type of solution is detection-based, which aims to detect the appearance of anomalous traffic. The basic idea is to utilize the well-defined relationship between different frames: once a forged frame is injected, the relationship is corrupted and, thus, can be detected. The most widely studied inter-frame relationship is the sequence number [18,19]. Sequence number is a 16-bit sequence control field starting at 0, which is then incremented by one for each non-fragmented frame. Thus, a forged frame signal causes non-continuity of the sequence number (here, it is assumed that an attacker cannot prevent the communication between a valid transceiver pair). However, the sequence number is easy to predict and forge by the attacker using soft wireless card or by techniques proposed in [20]; in addition, the sequence number is not available for control and management frames. Except for the sequence number, the relationships, including received signal strength [21], arrival time [22], and channel response [23], are also studied in previous

research. Although these anomaly detection techniques can provide lightweight detection of traffic anomaly, they cannot guarantee normal communication when such attacks occur. In other words, the receiver can only know the presence of a traffic anomaly but cannot locate the injected frame(s).

The second type of solution is prevention-based, which aims to detect the injected frame and then discard it to guarantee normal communication, even when the attack occurs. The most commonly utilized prevention-based solutions include the digital signature [24] and hash message authentication code (HMAC) [25]. The basic idea is that attackers do not know the key and, thus, cannot generate the correct digital signature or HAMC. However, such prevention-based solutions usually require pre-shared key between the transceiver. Accordingly, for scenarios where establishing the pre-shared key between the transceiver is too difficult or unavailable, we do not follow the prevention-based solutions in this paper.

3. System Model & Security Threat

3.1. Preliminary Knowledge to CSMA/CA

In the CSMA/CA protocol, following Section 5.1.4 in [26], devices initially synchronize with the network coordinator using beacon signals. A general transmission mechanism through a multiple-access channel was introduced in [26] as follows. When a device wants to transmit data, it senses the channel to check for ongoing activity. If the channel is busy, it continues sensing until the channel becomes idle in the next time slot. Next, the device waits for a short additional period called the distributed inter-frame spacing (DIFS), prioritizing frames with higher priority, such as real-time or urgent data. Once the DIFS expires and the channel remains idle, the device generates a random Backoff interval before transmitting. This random Backoff mechanism prevents multiple devices from transmitting simultaneously, thus avoiding collisions. For each time slot, the Backoff time counter is decremented by 1 as long as the channel is sensed idle, stopped when a transmission is detected on the channel, and reactivated when the channel is sensed idle again for more than a DIFS. When the Backoff time counter reaches zero and the channel is still idle, the device begins data transmission. Following this protocol ensures efficient communication among devices, reducing collision risks and optimizing data transfer within the network.

3.2. System Model

We consider the communication model depicted in Figure 2, where Alice and Carol act as transmitters, while Bob acts as the receiver. In this model, both Alice and Carol utilize the CSMA/CA protocol to access the channel. Bob responds with an ACK frame when he has successfully received a frame. Additionally present in the communication model is an impersonation attacker named Eve. Eve possesses knowledge about Alice, including her MAC address, IP address, and communication protocol. Eve's objective is to transmit forged frames by impersonating Alice, with the intention of pursuing invalid interests.

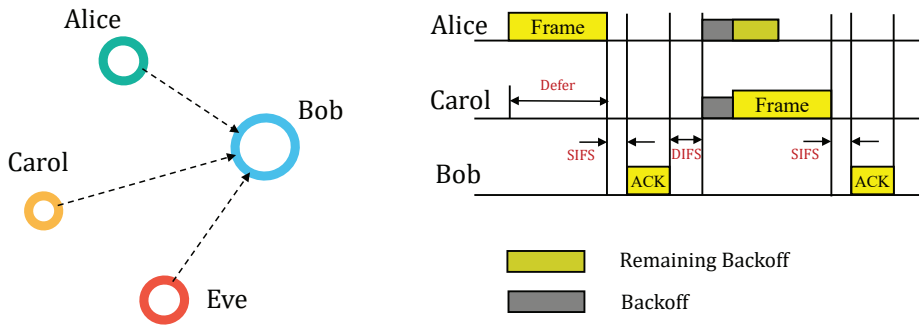

Figure 2. Communication model, where Alice and Carol communicate with Bob through a CSMA/CA channel. Eve aims to impersonate Alice to deceive Bob.

To prevent the impersonation attack, when Bob has received M ($M > 1$) frames claimed to be from Alice, Bob employs the MFS-based RFFA to determine whether the received M frames originate from Alice or Eve. We denote the M received frames signal by a matrix $\boldsymbol{Y} = [\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_M]$, where each element correspond to a frame signal. Bob first estimates the desired feature, denoted by $\hat{f}_{m(1 \leqslant m \leqslant M)} \in R^n$, from each received frame signal $\boldsymbol{y}_m$. The M feature estimates constitute a feature estimate vector $\hat{\boldsymbol{f}} = \left[\hat{f}_1, \hat{f}_2, \ldots, \hat{f}_M\right]^T$. Furthermore, we consider that Bob knows a reference feature of Alice, denoted as f. The MFS-based RFFA scheme can be formulated as the following binary hypothesis test:

$$\begin{cases} H_0: & |\boldsymbol{\alpha} \cdot \hat{\boldsymbol{f}} - f| \leqslant \delta \\ H_1: & |\boldsymbol{\alpha} \cdot \hat{\boldsymbol{f}} - f| > \delta \end{cases}, \tag{1}$$

where $\boldsymbol{\alpha} = [\alpha_1, \alpha_2, \ldots, \alpha_n]$ represents the weight of different feature estimates, and δ represents the decision threshold. If H_0 is accepted, it implies that the received multi-frame signal $\boldsymbol{Y}$ originates from Alice. Conversely, if H_1 is accepted, it indicates that the received multi-frame signal $\boldsymbol{Y}$ originates from Eve, thus implying an impersonation attack.

3.3. Security Threat

In CSMA/CA, Eve can inject a forged frame into valid traffic by modifying its Backoff time. As shown in Figure 3, Eve can arbitrarily activate injection by setting the Backoff time to zero, or deactivate injection by setting the Backoff time to the maximum value. This strategic control allows Eve to manipulate the channel access and, thus, the forged frame injection opportunity and ratio in valid traffic. As a result, the forged frame is blended with legitimate frames in the MFS-based RFFA.

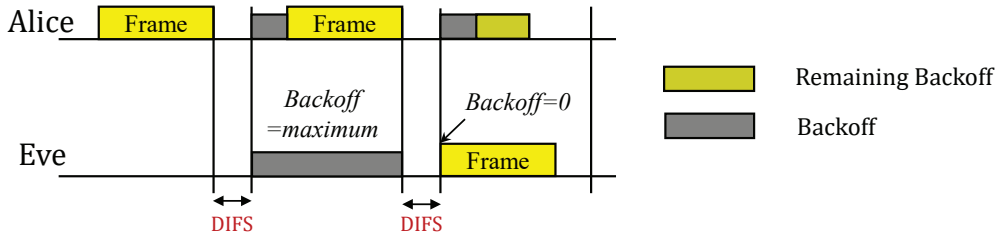

Figure 3. Arbitrary injection of a forged frame into valid traffic by Eve through modifying the Backoff time.

To demonstrate the impact of the aforementioned forged frame injection on the MFS-based RFFA, we conducted a Proof-of-Concept experiment to measure the averaged feature estimate with multiple frames in the presence and absence of the aforementioned injection. For this purpose, we first developed a frame signal collection platform, as shown in Figure 4, in which we utilized a universal software radio peripheral (USRP) as the receiver to collect frames signal by setting the Network Interface Card (NIC) as the transmitter. Next, 10^4 frame signals from two NICs, which represent Alice and Eve, were alternately sampled. We estimated, normalized, and recorded the CFO for each collected frame. Subsequently, we combined these CFO estimates to form a group of M samples comprising M_e elements randomly originating from Eve and the remaining $M - M_e$ elements randomly originating from Alice. We then calculated the average CFO estimate for each group type by setting $\boldsymbol{\alpha} = \underbrace{[1, 1, \ldots, 1]}_{M}$.

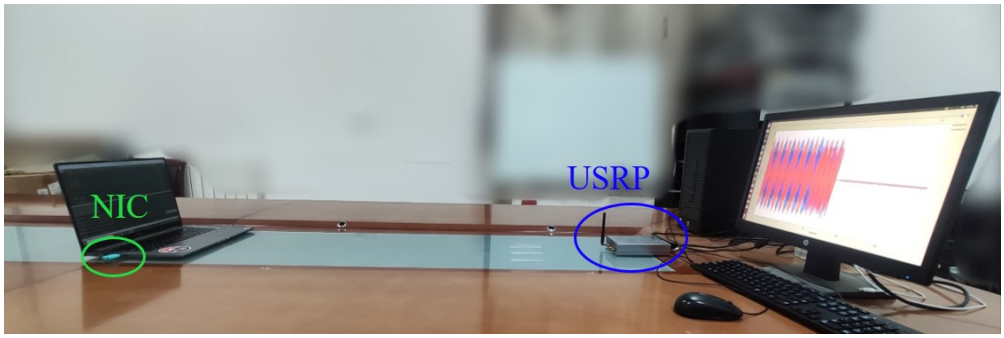

Figure 4. Experimental deployment.

To analyze the statistical distribution in the averaged CFO estimate, we set $M = 10$, and M_e varied from 0 to 10 to form 11 group classes. For each group class, we generated 10^3 samples, calculated the corresponding averaged CFO estimate of each sample, and used box plots, as illustrated in Figure 5, to represent the statistical characteristics of the averaged CFO estimate. The results in Figure 5 show that the averaged CFO estimate for classes $M_e = 0$ and $M_e = 10$ (green and red) exhibited the largest distinction, indicating that, if we can ensure all of the 10 frames originate from the same transmitter, the MFS-based RFFA can achieve the highest accuracy. However, as M_e decreased from nine to one, the distribution of the averaged CFO estimate gradually became more and more similar to that of $M_e = 0$. In particular, when $M_e = 1$, more than half of the averaged CFO estimate overlapped with that of $M_e = 0$. This suggests that, when Eve injects only one forged frame into valid traffic, the forged frame is much more likely to be accepted by the MFS-based RFFA. Overall, the results presented in Figure 5 demonstrate the severity of the identified injection attack in the MFS-based RFFA.

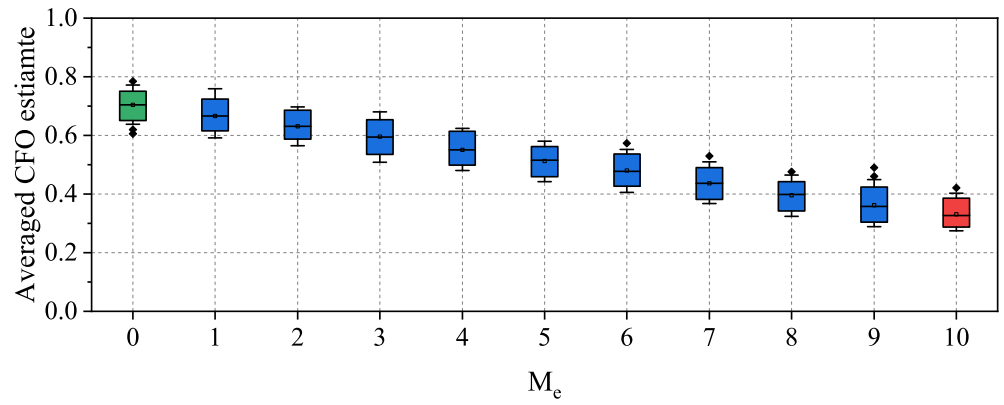

Figure 5. Box plots of averaged CFO estimates for different group classes, with the size $M = 10$ and M_e varying from 0 to 10. We show the 5th and 95th percentiles.

4. IfrPS Design and IfrPS-Aided, MFS-Based RFFA Scheme

In this section, we propose the IfrPS design and the IfrPS-aided, MFS-based RFFA scheme. At the end, we give a brief discussion of the security properties of our propositions.

4.1. IfrPS Design

The rationale behind the designed IfrPS is to associate each transmitted frame with unique information that cannot be forged by attackers. To this end, the transmitter attaches an HMAC to each transmitted frame signal and then discloses the key in the next transmitted frame signal (see the flow diagram of the IfrPS design illustrated in Figure 6). To elaborate further, we summarize the IfrPS design in three key steps.

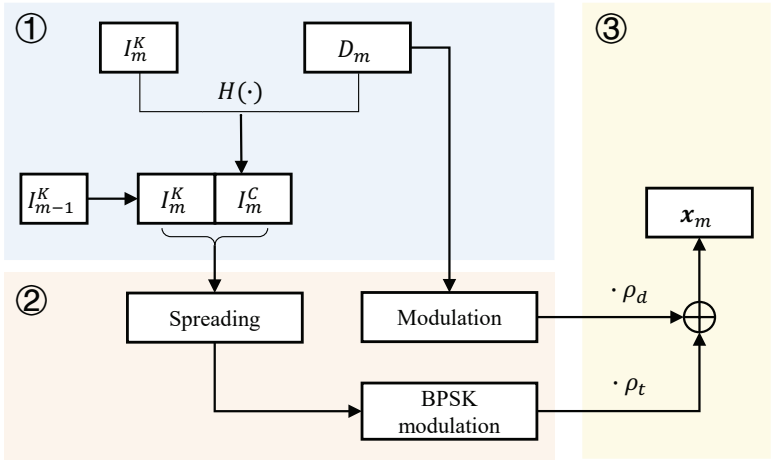

Figure 6. Flow diagram of the IfrPS design involving three steps ①, ② and ③. D_m is the frame data to be transmitted, $\boldsymbol{x}_m$ is the IfrPS obtained from D_m and unique information $\left(I_m^K, I_m^C\right)$.

First, we generate the unique information that needs to be attached in each transmitted frame signal. Let us denote the message data of the m-th frame by D_m, where m is interpreted as the frame index. It is worth noting that the re-transmitted frame is considered to have the same index m. Then, we can denote the unique information of the m-th frame by $\left(I_m^K, I_m^C\right)$. Here, I_m^K satisfies

$$I_{m-1}^C = H\left(D_{m-1}, I_m^K\right), \tag{2}$$

and I_m^C is obtained by

$$I_m^C = H\left(D_m, I_{m+1}^K\right), \tag{3}$$

where $H(\cdot)$ represents the hash function. Note that, for each value of m, the transmitter randomly generates I_m^K, and I_{m+j}^K and I_{m+j}^K are independent of each other when $i \neq j$. Based on the above, the receiver can detect whether two received frames, with signals $\boldsymbol{y}_{m-1}$ and $\boldsymbol{y}_m$, originate from the same transmitter by calculating whether the demodulated unique information and message satisfy Equation (2).

Second, we convert the unique information $\left(I_m^K, I_m^C\right)$ into symbols before attaching it to the transmitted frame signal, as shown in Figure 6. Since the bit sizes of I_m^K and I_m^C are, at most, 128, which is a number less than the frame length in most applications, we spread the unique information $\left(I_m^K, I_m^C\right)$ to match the frame length. To this end, we use the spreading code, denoted by $\boldsymbol{s} = \left[s_1, s_2, \ldots, s_{N/N_I}\right]$, with each element as aj or $-aj$ (j is the complex symbol), where N represents the frame length and N_I represents the bit size of I_m^K and I_m^C. To simplify the description, we assume that N is a multiple of N_I. Let us denote the converted symbols I_m^K and I_m^C by $\boldsymbol{t}_m^K$ and $\boldsymbol{t}_m^C$, respectively. $\boldsymbol{t}_m^K$ and $\boldsymbol{t}_m^C$ are given by

$$\begin{cases} \boldsymbol{t}_m^K[n] &= I_m^K[n|(N/N_I)] \cdot \boldsymbol{s}[n \mod (N/N_I)] \\ \boldsymbol{t}_m^C[n] &= I_m^C[n|(N/N_I)] \cdot \boldsymbol{s}[n \mod (N/N_I)] \end{cases}, \tag{4}$$

where "|" and "mod" are the symbols for division and modulus, respectively.

Third, we attach the converted BPSK symbols of $\left(I_m^K, I_m^C\right)$ into the modulated frame symbols. Let us denote the m-th frame without unique information being attached by $\boldsymbol{d}_m = [d_{m,1}, d_{m,2}, \ldots, d_{m,N}]$, and its version with unique information being attached by $\boldsymbol{x}_m$. Here, $\boldsymbol{x}_m$ is given by

$$\begin{cases} \boldsymbol{x}_m[n] = \rho_d \cdot \boldsymbol{d}_m[n] + \rho_t \cdot \boldsymbol{t}_m^K[n], & n < N/2 \\ \boldsymbol{x}_m[n] = \rho_d \cdot \boldsymbol{d}_m[n - \frac{N}{2}] + \rho_t \cdot \boldsymbol{t}_m^C[n - \frac{N}{2}], & n \geqslant N/2 \end{cases}. \tag{5}$$

where ρ_d and ρ_t represent the power allocation for the message and unique information, respectively. Due to power constraint, we have $\rho_d^2 + \rho_t^2 = 1$. To provide readers with a clearer understanding of the attaching method, we also present, in Figure 7, an illustrative example of the message being modulated with BPSK.

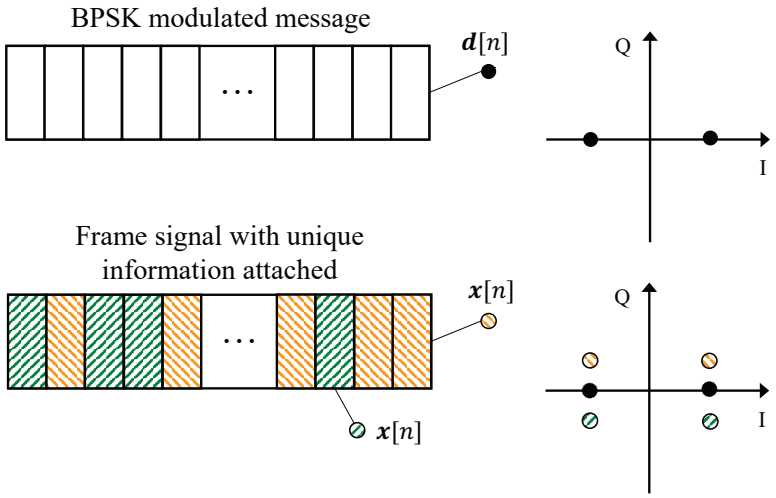

Figure 7. An illustrative example of attaching unique information into the frame signal where the message is modulated using BPSK.

4.2. IfrPS-Aided, MFS-Based RFFA Scheme

Considering that the transmitter has sequential frames for transmission, denoted by $\boldsymbol{X} = [\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \ldots]$, and taking into account the retransmission mechanism at the MAC layer, we assume that all these frames can be successfully received and demodulated by the receiver, denoted by $\boldsymbol{Y} = [\boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{y}_3, \ldots]$. However, each of the received frames may be forged and injected. In the IfrPS-aided, MFS-based RFFA scheme, the receiver needs to select the frames in $\boldsymbol{Y}$ that originate from the same transmitter as the first frame $\boldsymbol{y}_1$ and construct a selected frames set denoted as $\boldsymbol{Y}_s$. The receiver then inputs $\boldsymbol{Y}_s$ into Equation (1) to obtain the authentication result of the first frame $\boldsymbol{y}_1$. Similarly, for authenticating $\boldsymbol{y}_m$, the receiver selects frames from $\boldsymbol{Y} - \{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{m-1}\}$ and constructs the corresponding $\boldsymbol{Y}_s$. We summarize the procedure for leveraging the property of IfrPS to obtain $\boldsymbol{Y}_s$ for the authentication of $\boldsymbol{y}_1$ by using an M-frame signal as follows. This method can be extended to the authentication of other frames.

$\boldsymbol{Y}_s$ is initialized as $\boldsymbol{Y}_s = \{\boldsymbol{y}_1\}$. Frames in $\boldsymbol{Y}$ are, in turn, examined to be appended to $\boldsymbol{Y}_s$ or not. We use $\boldsymbol{y}_1$ and $\boldsymbol{y}_2$ as an example to explain how to examine the IfrPS relationship between two consecutively frames. Note that each entry of $\boldsymbol{y}_1$ and $\boldsymbol{y}_2$ is given by

$$y_{m,n} = h_{m,n} \cdot x_{m,n} + w_{m,n}, \ m \in \{1, 2\} \tag{6}$$

where $h_{m,n} \sim \mathcal{N}\left(0, \frac{1}{2}\right)$ represents the channel fading, and $w_{m,n} \sim \mathcal{N}(0, \sigma_w^2)$ represents the Gaussian noise. We assume block fading, so $h_{m,n}$ remains constant for the same value of m and varies independently across different values of m. Similarly, $w_{m,n}$ varies independently across different values of m and n. To extract the unique information attached in $\boldsymbol{y}_m$, the receiver first equalizes $\boldsymbol{y}_m$ and demodulates the message $\boldsymbol{d}_m$. Then, it demodulates the unique information using

$$\hat{\boldsymbol{t}}_m = \frac{\boldsymbol{h}_m^H}{|\boldsymbol{h}_m|^2} \cdot \boldsymbol{y}_m - \boldsymbol{d}_m, \tag{7}$$

where we assume accurate estimation of $\boldsymbol{h}_m$ and decoding of $\boldsymbol{d}_m$. Based on the obtained $\hat{\boldsymbol{t}}_m$ from Equation (7), the receiver can obtain the unique information through BPSK demodulation and de-spreading. Let $\hat{I}_m^C$ and $\hat{I}_m^K$ represent the estimated HMAC and key, respectively. The receiver can determine whether $\boldsymbol{y}_1$ and $\boldsymbol{y}_2$ originate from the same transmitter using the following binary hypothesis test:

$$\begin{cases} H_0: & \mathcal{D}\left[\hat{I}_1^C, H\left(D_1, \hat{I}_2^K\right)\right] = 0 \\ H_1: & \mathcal{D}\left[\hat{I}_1^C, H\left(D_1, \hat{I}_2^K\right)\right] > 0 \end{cases}, \tag{8}$$

where $\mathcal{D}$ represents the code distance. If H_0 is accepted, the receiver appends $\boldsymbol{y}_2$ to $\boldsymbol{Y}_s$; otherwise, $\boldsymbol{y}_2$ is not appended to $\boldsymbol{Y}_s$. The receiver iteratively examines the last element in $\boldsymbol{Y}_s$ and the first element in $\boldsymbol{Y} - \boldsymbol{Y}_s$, until either the size of $\boldsymbol{Y}_s$ is M or the pair of frames to be examined has already been examined.

Remarks: In our proposed IfrPS-aided, MFS-based RFFA scheme, we focus on authenticating the first frame $\boldsymbol{y}_1$. This differs from previous MFS-based RFFA schemes where the authentication result is used for all frame signals. This is because we cannot ensure whether the previous frame originates from the same transmitter by testing the IfrPS, as Eve, with significant computational resources, can deduce I_{m+1}^K by listening to I_m^C and D_m (see the detailed discussion in the previous subsection).

4.3. Security Property

In this subsection, we discuss the security property of the designed IfrPS, to demonstrate its ability to counter forged frame injection in MFS-based RFFA.

In MFS-based RFFA, where one forged frame is injected into valid traffic, there are two favorable cases for Eve in constructing the MFS. The first case occurs when the forged frame blends in with past valid frames, while the second case occurs when the forged frame blends in with the following valid frames. We have found that the proposed IfrPS design cannot prevent the first case, but it can effectively prevent the second case. Refer to Figure 8 for an illustrative explanation, where the marked numbers represent the frame index. In the following discussion, we analyze the security of the IfrPS design against these two cases separately.

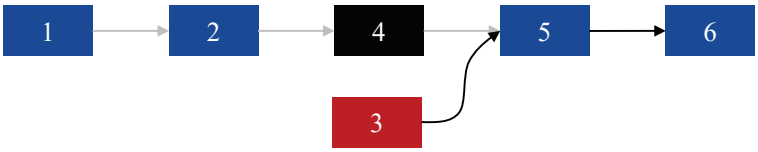

Figure 8. Forged frame injection in forming the MFS, where the forged frame cracks the inter-frame relationship between the 4th and 5th frames.

The injected frame may blend in with the following two legitimate frames for MFS-based RFFA. This can be achieved if the conveyed I^C in the third frame matches the I^K conveyed in the fourth frame. However, this scenario cannot be achieved, since Eve has to transmit the third frame before the fourth frame. It is important to note that, if the third frame is transmitted after the fourth frame, the receiver will discard the third frame due to the incorrect sequence number. Thus, Eve cannot obtain any knowledge about the I^K conveyed in the fourth frame to crack it. In other words, Eve has no way to generate the correct I^C that should conveyed by the third frame for a successful injection.

Overall, we observe that the IfrPS design can prevent the injected frame from blending in with the following valid frames in MFS-based RFFA. Therefore, we deduce that our proposed IfrPS-aided, MFS-based RFFA scheme is secure, since the receiver explores the following frames to form the MFS for each received frame.

5. Efficiency

Since the designed IfrPS requires a portion of transmission power to convey the unique information, the message demodulation BER will inevitably be affected. We measured the efficiency of the IfrPS design by evaluating its impact on message demodulation error. To this end, we considered the BPSK, QPSK, and 16QAM, with the constellation with IfrPS design shown in Figure 9, and performed both theoretical analysis and numerical evaluation towards these three modulation systems to assess the efficiency of the IfrPS design.

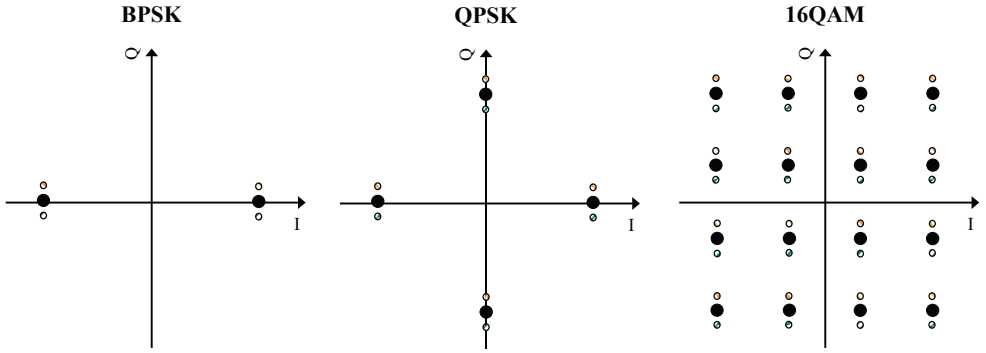

Figure 9. Constellation of superimposed symbols at the physical layer for the BPSK, QPSK, and 16QAM, respectively.

With perfect channel estimation, the n-th received frame signal after channel compensation, denoted by $\boldsymbol{y}_n^c$, can be expressed as

$$\boldsymbol{y}_n^c = \rho_d \cdot \boldsymbol{d}_n + \rho_t \cdot \boldsymbol{t}_n + \frac{1}{|h_n|} \cdot \boldsymbol{w}_n, \tag{9}$$

where we define $\frac{E_s}{E_n} = \frac{\mathbb{E}\left(d_n \cdot d_n^H\right)}{\mathbb{E}\left(w_n \cdot w_n^H\right)} = \frac{\mathbb{E}\left(t_n \cdot t_n^H\right)}{\mathbb{E}\left(w_n \cdot w_n^H\right)}$ to denote the transmission symbol-to-noise power ratio. On the basis, we have the transmission bit-to-noise power ratio of $\frac{E_b}{E_n} = \frac{E_s}{E_n}$ for BPSK, $\frac{E_b}{E_n} = \frac{1}{2} \cdot \frac{E_s}{E_n}$ for QPSK, and $\frac{E_b}{E_n} = \frac{1}{4} \cdot \frac{E_s}{E_n}$ for 16QAM. Let us denote the message demodulation BER of the IfrPS for BPSK, QPSK, and 16QAM systems by $P_{IfrPS,b}^{BPSK}$, $P_{IfrPS,b}^{QPSK}$, and $P_{IfrPS,b}^{16-QAM}$, respectively. By considering the Gray code mapping (refer to [27]), we can derive $P_{IfrPS,b}^{BPSK}$, and approximate $P_{IfrPS,b}^{QPSK}$ and $P_{IfrPS,b}^{16-QAM}$ by

$$P_{IfrPS,b}^{BPSK} = \frac{1}{2} \cdot \left(1 - \sqrt{\frac{\rho_s^2 E_b}{\rho_s^2 E_b + E_n}}\right), \tag{10}$$

$$P_{IfrPS,b}^{QPSK} \approx \frac{1}{2} - \frac{1}{4}\left[\sqrt{\frac{(\rho_s + \rho_t)^2 E_b}{(\rho_s + \rho_t)^2 E_b + E_n}} + \sqrt{\frac{(\rho_s - \rho_t)^2 E_b}{(\rho_s - \rho_t)^2 E_b + E_n}}\right], \tag{11}$$

and

$$\begin{aligned} P_{IfrPS,b}^{16QAM} \approx & \\ & = \frac{3}{8} - \frac{3}{32}\left[\sqrt{\frac{(\rho_s + \rho_t)^2 E_b}{(\rho_s + \rho_t)^2 E_b + E_n}} + \sqrt{\frac{(\rho_s - \rho_t)^2 E_b}{(\rho_s - \rho_t)^2 E_b + E_n}}\right] \\ & - \frac{3}{16}\sqrt{\frac{E_b}{E_b + E_n}}, \end{aligned} \tag{12}$$

respectively.

We present both theoretical and numerical results for the message demodulation BER of IfrPS in the presence of BPSK, QPSK, and 16QAM modulations, as well as the BER of the normal signal (without IfrPS), for comparison. Figure 10 illustrates these results.

The first observation from the figure is that the theoretical and numerical results for the message demodulation BER of IfrPS exhibit a small discrepancy. This suggests that our theoretical analysis serves as a reliable predictor for the message demodulation BER of IfrPS. The second observation is that the message demodulation BER of IfrPS is only slightly higher than that of the normal signal across various signal-to-noise ratio (SNR) levels. When $\rho_d^2 = 0.99$, the obtained BERs are nearly identical. This indicates that IfrPS introduces only a minor performance degradation in message demodulation, making it suitable for applications with stringent requirements on demodulation accuracy. The third observation is that the message demodulation BER of IfrPS is influenced by ρ_d^2, where a larger ρ_d^2 results in a higher BER. This implies that we can adapt the parameter ρ_d^2 to meet different requirements for message demodulation BER in practical applications. The fourth observation is that, under the same system parameters, the impact of IfrPS on the message demodulation BER varies across different modulation systems. For example, when $\rho_d^2 = 0.90$, the equivalent SNR degradation in message demodulation is approximately 0.45 dB for BPSK, whereas it is around 2 dB for 16QAM. This suggests that the effect of IfrPS on BER is less pronounced in low-order modulation systems.

In summary, the results in Figure 10 demonstrate the effectiveness of IfrPS, as the message demodulation BER is only slightly increased when ρ_d^2 is appropriately set. In the next section, we further explore the resulting accuracy gain in RFFA using the same ρ_d^2 setting for IfrPS.

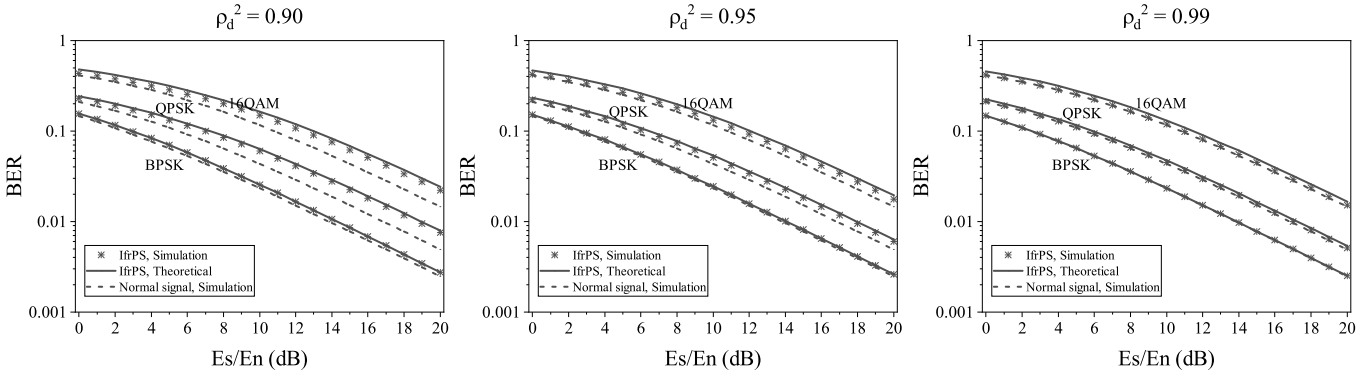

Figure 10. Theoretical and numerical results of the message demodulation BER of the IfrPS, where the message demodulation BER of the normal signal is also plotted for comparison.

6. Effectiveness

The ability to securely construct an MFS inevitably affects the accuracy of an MFS-based RFFA scheme. Thus, we evaluate the effectiveness of the IfrPS-aided, MFS-based RFFA scheme in terms of the resultant RFFA accuracy that can be achieved. To measure the effectiveness, we define two types of error as follows:

- *FRR:* FRR represents the ratio of valid samples that are incorrectly classified as invalid;
- *FAR:* FAR represents the ratio of invalid samples that are incorrectly classified as valid.

Note that these two types of error affect both the processes of IfrPS detection and RFFA at the receiver side, i.e., the Equations (1) and (8). In the context of IfrPS detection, a valid sample refers to a frame signal originating from the same transmitter as the previous frames, while an invalid sample refers to a frame signal originating from a different transmitter. In the context of RFFA, a valid sample refers to a frame signal originating from Alice, while an invalid sample refers to a frame signal originating from Eve. In the following, we first

analyze and evaluate these two types of error for the IfrPS detection process and then, on that basis, analyze and evaluate these for the RFFA process.

6.1. FRR and FAR in IfrPS Detection

We derived the closed-form expression of the FRR and the numerical solution of the FAR in the IfrPS detection process.

Theorem 1. *The FRR in IfrPS detection, denoted by* P_{FRR}^{IfrPS}*, is given by*

$$\begin{aligned} P_{FRR}^{IfrPS} &= 1 - \int_0^\infty \int_0^\infty \left[1 - \frac{1}{2} erfc\left(h_1\sqrt{L}\rho_t\sqrt{\frac{E_s}{E_n}}\right)\right]^{\frac{N}{2L}} \\ &\cdot \left[1 - \frac{1}{2} erfc\left(h_2\sqrt{L}\rho_t\sqrt{\frac{E_s}{E_n}}\right)\right]^{\frac{N}{2L}} \cdot \exp(-h_1) \cdot \exp(-h_2) \\ &\cdot dh_1 \cdot dh_2 \end{aligned} \tag{13}$$

and the FAR of IfrPS, denoted by P_{FAR}^{IfrPS}*, is given by*

$$P_{FAR}^{IfrPS} = \left(\frac{1}{2}\right)^{\frac{N}{2L}}. \tag{14}$$

Proof. For two consecutively received frame signals originating from the same transmitter, let us denote the channel fading coefficient of the first frame signal by h_1 and that of the second frame by signal h_2. We can express the probability that the unique information attached into these two frames are accurately demodulated by

$$P_{correct,1} = \left[1 - \frac{1}{2} erfc\left(h_1\sqrt{L}\rho_t\sqrt{\frac{E_s}{E_n}}\right)\right]^{\frac{N}{2L}}, \tag{15}$$

and

$$P_{correct,2} = \left[1 - \frac{1}{2} erfc\left(h_2\sqrt{L}\rho_t\sqrt{\frac{E_s}{E_n}}\right)\right]^{\frac{N}{2L}}, \tag{16}$$

respectively. Then, by integrating $P_{correct,1}$ and $P_{correct,1}$, we can obtain the probability that these two frames signal match with the demodulated unique information by

$$\begin{aligned} P_{match,1,2} = \; & \int_0^\infty \int_0^\infty P_{correct,1} \cdot P_{correct,1} \cdot \exp(-h_1) \\ & \cdot \exp(-h_2) \cdot dh_1 \cdot dh_2. \end{aligned} \tag{17}$$

Substituting $P_{FRR}^{IfrPS} = 1 - P_{match,1,2}$ into Equation (17), we can prove Theorem 1. □

We plot the theoretical and numerical results of the FRR and FAR in IfrPS detection process in Figure 11. The first observation is that the theoretical results match the numerical results well, which indicates that our theoretical expressions can be used to predict the performance. The second observation is that the resultant FRR and FAR perform a trade-off relationship over N and L. This indicates that, in practical applications, the values of N and L need to be optimized to achieve the required FRR and FAR levels. The third observation is that the resultant FRR and FAR can be refined with a larger E_s/E_n and a smaller ρ_d^2. This indicates that, for a communication with larger SNR and tolerance on message demodulation degradation, we can always obtain better performance in IfrPS detection.

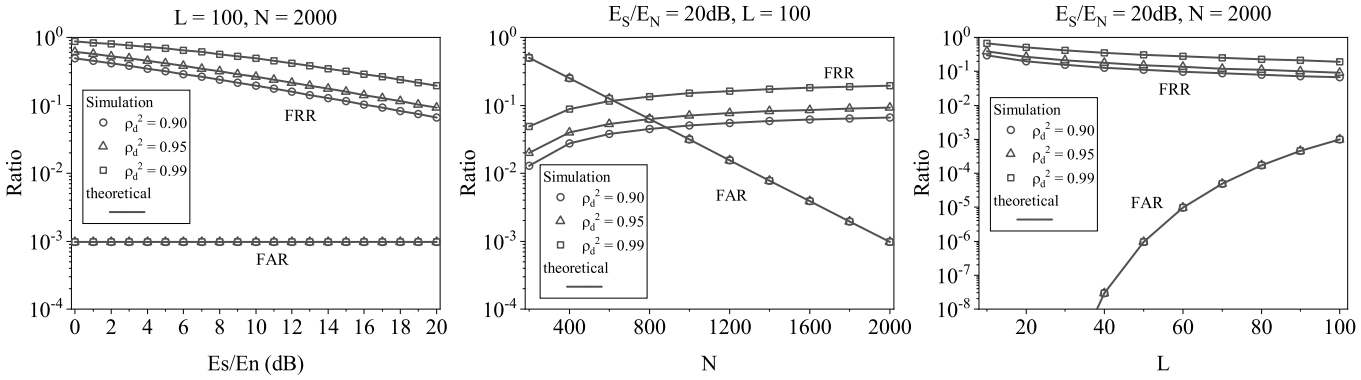

Figure 11. Theoretical and numerical results of FRR and FAR in the IfrPS detection process.

Furthermore, to provide a visual presentation of the IfrPS detection performance, we calculate the expected sequence length of the detected MFS, denoted by M. Note that the calculation can be expressed by

$$M = \sum_{m=1}^{\infty} \left(1 - P_{FRR}^{IfrPS}\right)^{m-1} \cdot P_{FRR}^{IfrPS} \cdot m. \tag{18}$$

Additionally, we plot the results in Figure 12. The first observation is that the expected sequence length increases over E_s/E_n and decreases over ρ_d^2. This is easy to understand, since we have demonstrated above that the IfrPS detection performance is positive in relation to E_s/E_n and negative to ρ_d^2. The second observation is that, for different levels of FAR in IfrPS detection, the obtained M has quite a significant value. For instance, when the FAR is fixed at 0.0001, i.e., the attacker can only compromise the IfrPS detection with the probability of 0.0001, the obtained M is more than 10 when $N = 2000$ and $\rho_d^2 = 0.90$. Since such parameters are easy to satisfy in practical applications, whereas the corresponding parameter ($\rho_d^2 = 0.90$) results in only about 2 dB degradation to message demodulation, the results in Figure 12 demonstrate the potential of enhancing the RFFA by adopting the IfrPS design and using the MFS-based approach.

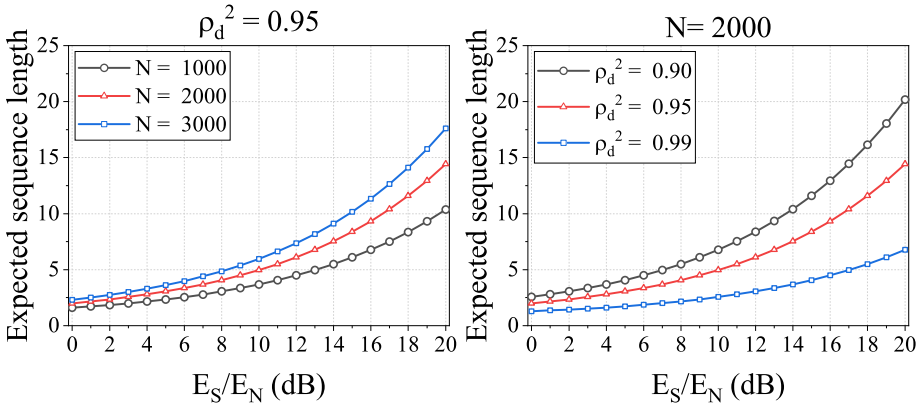

Figure 12. *Cont.*

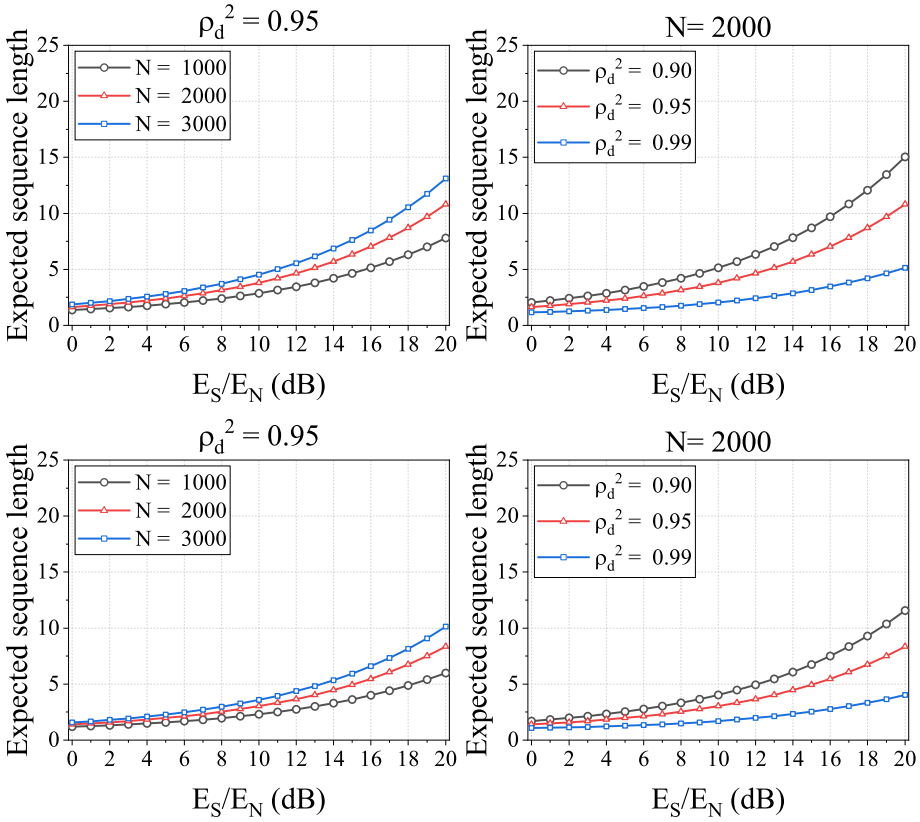

Figure 12. Simulation results of expected sequence length. Tested under the FAR of IfrPS set to be 0.01 (the top figures), 0.001 (the middle figures) and 0.0001 (the bottom figures).

6.2. FRR and FAR in RFFA

To quantify the FRR and FAR in RFFA, we used the CFO as the authentication feature as a case study. Following [28,29], we know that the CFO estimates follow the Gaussian distribution $\mathcal{N}\left(\epsilon, \frac{1}{4\pi^2 L_s^3 (N_s-1)\gamma}\right)$, where ϵ represents the expectation of CFO estimate, γ represents the received SNR, and L_s and N_s are two parameters in CFO estimation following $L_s \cdot N_s = N$. In this study, we fixed $L_s = 2$ and calculated N_s by $N_s = N/L_s$. Moreover, we can deduce that the averaged CFO estimate with M frames follows the distribution $\mathcal{N}\left(0, \frac{1}{4\pi^2 L_s^3 (N_s-1)\bar{\gamma}}\right)$, where $\bar{\gamma} = \frac{1}{M} \cdot \sum_{m=1}^{M} \gamma_m$.

We consider that the CFO of the randomly selected attacker follows the uniform distribution $\mathcal{U}(0, R)$, where R denotes the allowable CFO range, which we set to be 0.02π [28]. Thus, we can express the FAR in RFFA by

$$P_{FAR}^{SFS} = \frac{2\delta}{0.02\pi} \tag{19}$$

for the SFS-based RFFA, and by

$$P_{FAR}^{MFS} = P_{FAR}^{IfrPS} + \left(1 - P_{FAR}^{IfrPS}\right) \cdot \frac{2\delta}{0.02\pi} \tag{20}$$

for the MFS-based RFFA.

Theorem 2. *With the threshold δ, the FRR in the IfrPS-aided, MFS-based RFFA can be expressed by*

$$\begin{aligned} P_{FRR} &= \sum_{m=1}^{\infty} p(m) \cdot P_{FRR}(m) \\ &= \sum_{m=1}^{\infty} \left(1 - P_{FRR}^{IfrPS}\right)^{m-1} \cdot P_{FRR}^{IfrPS} \cdot P_{FRR}(m), \end{aligned} \tag{21}$$

where P_{FRR}^{IfrPS} *is given in Theorem 1, and* $P_{FRR}(m)$ *follows*

$$P_{FRR}(m) = erfc\left(\frac{\delta}{2\pi L_s^{1.5}\sqrt{(N_s-1)\bar{\gamma}}}\right). \tag{22}$$

To prove the above theorem, we illustrate, in Figure 13, both the theoretical and numerical FRR in RFFA, where we fix $N = 2000$, $L = 100$, and $\rho_d^2 = 0.95$. It can be observed from Figure 13 that the theoretical results of FRR in RFFA match the numerical results well. This indicates that our theoretical result can be used for predicting the FRR in IfrPS-aided, MFS-based RFFA. From Equations (19) and (20), we know that using a smaller threshold in IfrPS-aided, MFS-based RFFA system can achieve the same FAR as that using a smaller threshold in the SFS-based RFFA system, which indicates that we need to use a smaller threshold to ensure a smaller FRR at the same FAR level in RFFA through the IfrPS-aided, MFS-based one than the SFS-based one.

Lemma 1. *To ensure the same FAR level of RFFA in the IfrPS-aided, MFS-based RFFA as that in the SFS-based one, and minimize the achieved FRR, the transmitter needs to optimize L.*

To prove the feasibility of using the above method for optimizing L and, thus, to reduce the FRR under the same FAR levels, we illustrate in Figure 14 the obtained FRR by searching the optimal L. Note that the optimal L is numerically searched using the FRR and FAR expressions in Equations (20) and (21). The first observation from Figure 14 is that the searched L is the optimal one since it leads to the minimal FRR for both the theoretical and numerical results. The second observation is that the relationship between FRR and L is the convex function and, thus, we can always search the optimal L.

Finally, in oder to demonstrate the FRR gain in IfrPS-aided, MFS-based RFFA over the MFS-based RFFA, we illustrate the numerical results under different levels of FAR in Figure 15. The first observation from Figure 15 is that we can always achieve a positive FRR gain. Furthermore, the FRR gain increases with a smaller ρ_d^2. The second observation from Figure 15 is that equivalent SNR gain is mainly related to ρ_s^2 rather than N. This is because using a larger N requires a larger L to ensure the FAR level, which inevitably limits the improvement in RFFA achieved by a larger N. The third observation from Figure 15 is that the equivalent SNR gain is about 5 dB when $\rho_d^2 = 0.90$, $N = 1500$, and $E_s/E_n = 20$ dB. Note that the corresponding equivalent SNR degradation to message demodulation is only 2 dB for 16QAM, 1 dB for QPSK, and 0.5 dB for BPSk. This demonstrates the effectiveness of the proposed IfrPS-aided, MFS-based RFFA scheme in securely improving the RFFA accuracy.

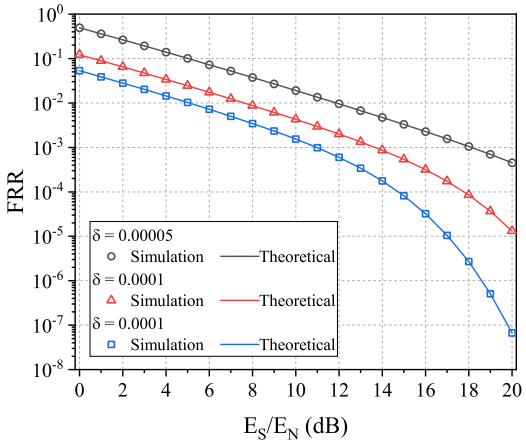

Figure 13. Theoretical and simulated FRR in the IfrPS-based multi-frame signal-based RFFA. Tested under $N = 2000$, $L = 100$, $\rho_s^2 = 0.90$.

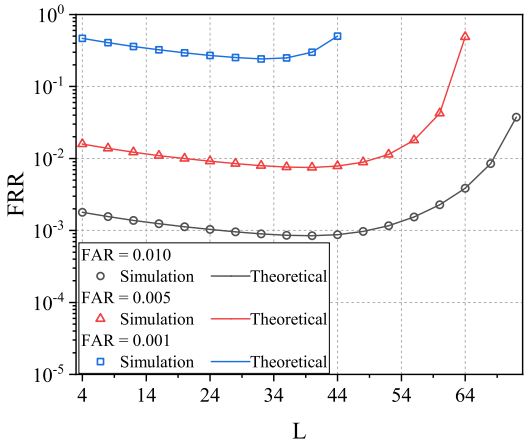

Figure 14. Theoretical and simulated FRR in the IfrPS-based multi-frame signal-based RFFA, with different FAR values. Tested under $N = 1000$, $\rho_d^2 = 0.95$.

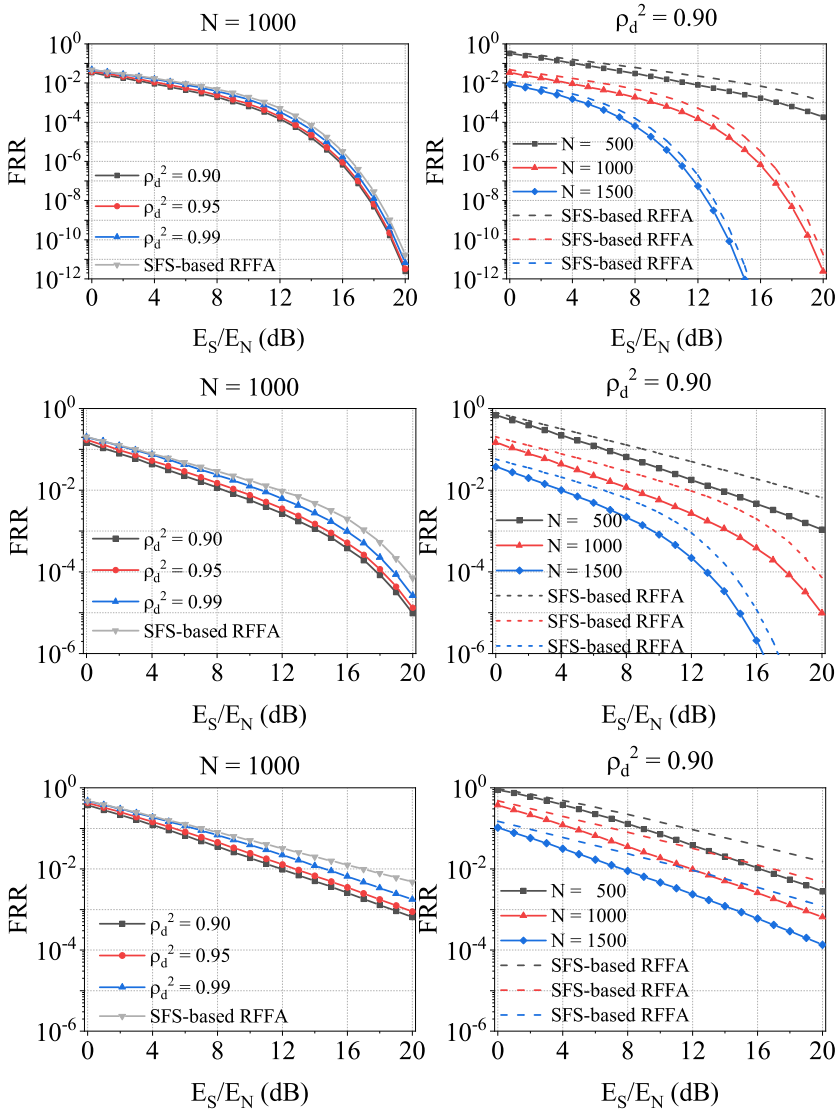

Figure 15. Numerical results of the minimal FRR achieved by the IfrPS-aided, MFS-based RFFA, tested under FAR levels of 0.01 (the top figures), 0.001 (the middle figures) and 0.0001 (the bottom figures).

7. Conclusions

In this paper, we have identified a security threat associated with the MFS-based RFFA in CSMA/CA. To counter this security threat, we propose an IfrPS-aided, MFS-based RFFA scheme. We conducted a comprehensive study to evaluate the security, efficiency, and effectiveness of the proposed scheme and conducted simulations to evaluate its performance. We note that the proposed scheme can counter the identified security threat with no pre-shared key required between the transceiver, and can be applied to various communication systems while only causing minor impact on message demodulation. Overall, our contributions advance the field of RFFA techniques by, for the first time, highlighting a new but critical viewpoint of the security threat when utilizing a multi-frame signal for RFFA in the CSMA/CA system. Additionally, we provide a foundation for further research and development in this area to securely utilize the multi-frame signal in RFFA in the CSMA/CA system without requirements for pre-shared keys.

Author Contributions: Conceptualization, X.L.; methodology, X.L.; software, S.Z.; validation, Y.L.; formal analysis, X.L.; investigation, Y.L.; writing—original draft preparation, X.L.; writing—review and editing, S.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Jinan "20 New Colleges and Universities" Introduction and Innovation Team (No. 2021GXRC064).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used can be obtained from the authors upon reasonable request.

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

References

1. Topal, O.A.; Kurt, G.K. Physical Layer Authentication for LEO Satellite Constellations. In Proceedings of the 2022 IEEE Wireless Communications and Networking Conference (WCNC), Austin, TX, USA, 10–13 April 2022; pp. 1952–1957.
2. Du, R.; Zhen, L.; Liu, Y. Physical Layer Authentication based on Integrated Semi-Supervised Learning in Wireless Networks for Dynamic Industrial Scenarios. *IEEE Trans. Veh. Technol.* **2022**, *72*, 6154–6164. [CrossRef]
3. Zou, Y.; Valkama, M.; Renfors, M. Analysis and Compensation of Transmitter and Receiver I/Q Imbalances in Space-Time Coded Multiantenna OFDM Systems. *Eurasip J. Wirel. Commun. Netw.* **2008**, *2008*, 1–16. [CrossRef]
4. Liao, R.; Wen, H.; Wu, J.; Pan, F.; Xu, A.; Jiang, Y.; Xie, F.; Cao, M. Deep-learning-based physical layer authentication for industrial wireless sensor networks. *Sensors* **2019**, *19*, 2440. [CrossRef] [PubMed]
5. Zeng, S.; Chen, Y.; Li, X.; Zhu, J.; Shen, Y.; Shiratori, N. Visibility Graph Entropy based Radiometric Feature for Physical Layer Identification. *Hoc. Netw.* **2022**, *127*, 102780.
6. Li, X.; Chen, Y.; Zhu, J.; Zeng, S.; Shen, Y.; Jiang, X.; Zhang, D. Fractal Dimension of DSSS Frame Preamble: Radiometric Feature for Wireless Device Identification. *IEEE Trans. Mob. Comput.* **2023**, 1–15. [CrossRef]
7. 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, New York, NY, USA, 14–19 September 2008; pp. 116–127.
8. Pan, F.; Wen, H.; Liao, R.; Jiang, Y.; Xu, A.; Ouyang, K.; Zhu, X. Physical layer authentication based on channel information and machine learning. In Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 9–11 October 2017; pp. 364–365.
9. Bari, M.F.; Chatterjee, B.; Sen, S. Dirac: Dynamic-irregular clustering algorithm with incremental learning for rf-based trust augmentation in iot device authentication. In Proceedings of the 2021 IEEE International Symposium on Circuits and Systems (ISCAS), Virtual, 22–28 May 2021; pp. 1–5.
10. Chen, Y.; Ho, P.; Wen, H.; Chang, S.Y.; Real, S. On Physical-Layer Authentication Via Online Transfer Learning. *IEEE Internet Things J.* **2021**, *9*, 1374–1385. [CrossRef]
11. Yamazaki, T.; Iwagami, S.; Miyoshi, T. Ant-inspired Backoff-based Opportunistic Routing for Ad Hoc Networks. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019; pp. 1–4.
12. Polak, A.C.; Dolatshahi, S.; Goeckel, D.L. Identifying wireless users via transmitter imperfections. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 1469–1479. [CrossRef]
13. Lin, Y.; Tu, Y.; Dou, Z.; Chen, L.; Mao, S. Contour stella image and deep learning for signal recognition in the physical layer. *IEEE Trans. Cogn. Commun. Netw.* **2020**, *7*, 34–46. [CrossRef]

14. Xiao, L.; Lu, X.; Xu, T.; Zhuang, W.; Dai, H. Reinforcement Learning-based Physical-layer Authentication for Controller Area Networks. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 2535–2547. [CrossRef]
15. Sankhe, K.; Belgiovine, M.; Zhou, F.; Angioloni, L.; Restuccia, F.; D'Oro, S.; Melodia, T.; Ioannidis, S.; Chowdhury, K. No Radio Left Behind: Radio Fingerprinting Through Deep Learning of Physical-layer Hardware Impairments. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *6*, 165–178. [CrossRef]
16. Al-Shawabka, A.; Restuccia, F.; D'Oro, S.; Jian, T.; Rendon, B.C.; Soltani, N.; Dy, J.; Ioannidis, S.; Chowdhury, K.; Melodia, T. Exposing the Fingerprint: Dissecting the Impact of the Wireless Channel on Radio Fingerprinting. In Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications, Toronto, ON, Canada, 6–9 July 2020; pp. 646–655.
17. Liao, R.; Wen, H.; Chen, S.; Xie, F.; Pan, F.; Tang, J.; Song, H. Multiuser Physical Layer Authentication in Internet of Things with Data Augmentation. *IEEE Internet Things J.* **2019**, *7*, 2077–2088. [CrossRef]
18. Fal, S.; Ton, V.D.; Sandeep, K. A ZigBee intrusion detection system for IoT using secure and efficient data collection. *Internet Things* **2020**, *12*, 100306.
19. Agrawal, K.; Alladi, T.; Agrawal, A.; Chamola, V.; Benslimane, A. NovelADS: A Novel Anomaly Detection System for Intra-Vehicular Networks. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 22596–22606. [CrossRef]
20. Bellardo, J.; Savage, S. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In Proceedings of the 12th Conference on USENIX Security Symposium, Washington, DC, USA, 4–8 August 2003; Volume 12, p. 2.
21. Chen, X.; Xu, W.; Wang, S.; Li, Y.; Lin, Z. An Anomaly Detection Scheme with K-means aided Extended Isolation Forest in RSS-based Wireless Positioning System. In Proceedings of the 2022 IEEE Wireless Communications and Networking Conference (WCNC), Austin, TX, USA, 10–13 April 2022; pp. 1910–1915.
22. Yang, Z.; Ying, J.; Shen, J.; Feng, Y.; Chen, Q.A.; Mao, Z.M.; Liu, H.X. Anomaly Detection Against GPS Spoofing Attacks on Connected and Autonomous Vehicles Using Learning From Demonstration. *IEEE Trans. Intell. Transp. Syst.* **2023**, 1–14. [CrossRef]
23. Tedeschini, B.C.; Nicoli, M.; Win, M.Z. On the Latent Space of mmWave MIMO Channels for NLOS Identification in 5G-Advanced Systems. *IEEE J. Sel. Areas Commun.* **2023**, *41*, 1655–1669. [CrossRef]
24. Hathal, W.; Cruickshank, H.; Sun, Z.; Maple, C. Certificateless and Lightweight Authentication Scheme for Vehicular Communication Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 16110–16125. [CrossRef]
25. Bansal, G.; Sikdar, B. Beyond Traditional Message Authentication Codes: Future Solutions for Efficient Authentication of Message Streams in IoT Networks. *IEEE Internet Things Mag.* **2022**, *5*, 102–106. [CrossRef]
26. *IEEE Std 802.15.4-2011*; IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). Revision of IEEE Std 802.15.4-2006. IEEE: New York, NY, USA, 2011; pp. 1–314.
27. Xu, Z.; Yuan, W. Watermark BER and Channel Capacity Analysis for QPSK-Based RF Watermarking by Constellation Dithering in AWGN Channel. *IEEE Signal Process. Lett.* **2017**, *24*, 1068–1072. [CrossRef]
28. Young, R.H.; Sang-Rok, M.; Ki, L.J.; Seung-Hyun, C. Novel phase and CFO estimation DSP for photonics-based sub-THz communication. *J. Light. Technol.* **2022**, *40*, 2710–2716.
29. Li, X.; Zeng, S.; Tong, W. Enhancing Carrier Frequency Offset Authentication via Fractal Dimension. In Proceedings of the 2018 International Conference on Networking and Network Applications (NaNA), Xi'an, China, 12–15 October 2018; pp. 137–142.

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