

Dissertation for Doctor of Philosophy

Radio Frequency Fingerprinting:
Deep Learning-based Approaches

Jusung Kang

School of Electrical Engineering and Computer Science

Gwangju Institute of Science and Technology

2024

박사학위논문

전파 신호 식별 시스템:
딥러닝 기반 접근법

강주성

전기전자컴퓨터공학부

광주과학기술원

2024

Radio Frequency Fingerprinting: Deep Learning-based Approaches

Advisor: Professor Heung-No Lee

by

Jusung Kang

School of Electrical Engineering and Computer Science

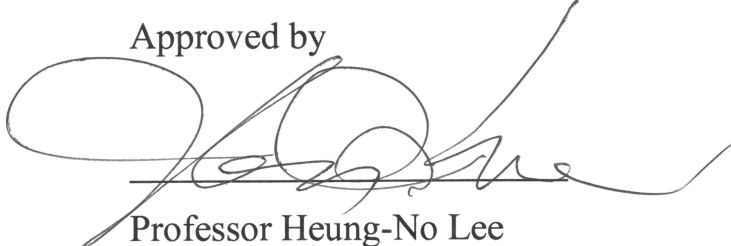
Gwangju Institute of Science and Technology

A dissertation submitted to the faculty of the Gwangju Institute of Science and Technology in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Electrical Engineering and Computer Science

Gwangju, Republic of Korea

May 14, 2024

Approved by

A handwritten signature in black ink, appearing to read 'Heung-No Lee', written over a horizontal line.

Professor Heung-No Lee

Committee Chair

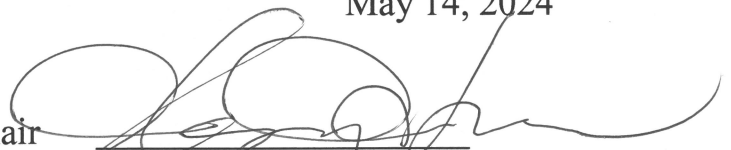
Radio Frequency Fingerprinting: Deep Learning-based Approaches

Jusung Kang

Accepted in partial fulfillment of the requirements for
the degree of Doctor of Philosophy

May 14, 2024

Committee Chair



Prof. Heung-No Lee

Committee Member



Prof. Jong Won Shin

Committee Member



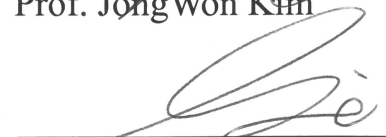
Prof. Euseok Hwang

Committee Member



Prof. Jong Won Kim

Committee Member



Prof. Young-Sik Kim
(DGIST)

Dedicated to my family

Abstract

In this dissertation, we focus on the authentication issues that arise when numerous Radio Frequency (RF) devices are wirelessly connected in an Internet of Things (IoT) environment. Modern cryptographic key-based Media Access Control (MAC) layer authentication systems pose significant security threats if keys are lost and require complex algorithms that are not suitable for IoT environments. To address these issues, RF Fingerprinting technology, which authenticates devices using unique RF signal characteristics at the physical layer, has gained attention. RF Fingerprinting starts from the premise that it is significantly more costly to replicate the unique characteristics of RF signals, thereby playing a crucial role in enhancing the security of wireless networks.

This dissertation presents two significant research findings related to RF Fingerprinting and discusses the challenges and future research directions for achieving system integrity.

The first study proposes an RF Fingerprinting method capable of identifying signal transmitters in a frequency-hopping spread spectrum (FHSS) network, one of the best existing RF security systems. To achieve this, Signal Fingerprints (SF) of the hopping signals were extracted and transformed into spectrograms representing the time-frequency behavior of the SFs. These spectrograms were then trained using a designed Deep Inception Network (DIN)-based signal classifier. As a result, the system was able to identify signal transmitters with 97% accuracy for hopping signals, and the algorithm for detecting network attackers showed an Area Under the Receiver Operating Characteristic (AUROC) curve performance of 0.99.

The second study emphasizes the importance of public key management in IoT environments and introduces an RF-based Public Key Generator (RF-PubKG) model. The proposed model, by projecting RF feature clusters into cryptographic sequences, achieved 97.2% accuracy at a 20dB Signal-to-Noise Ratio (SNR), which further improves to 99.6%

in noiseless conditions. Furthermore, low-correlation analysis of the generated public key sets confirmed the reliability and independence of the learning-based public key system, and a proof of concept of the RF-PubKG-based Rivest–Shamir–Adleman (RSA) digital signature system demonstrated that it could effectively operate as Public Key Cryptography (PKC) without the need for Public Key Infrastructure (PKI). These results are expected to simplify public key management in IoT environments and significantly improve the efficiency of the digital signature verification process.

Finally, we discuss the challenges and future research directions for the integrity of the RF Fingerprinting system. The contribution of this study spans from existing methods operating with analog feature keys in the real domain to the RF-PubKG based on public keys operating in the finite field. Furthermore, the research direction includes the development of sensor intelligence systems based on digitized analog feature keys operating in the digital domain. This involves discussing the challenges of public operation in the current system and proposing future research directions to overcome these challenges.

©2024
Jusung Kang
ALL RIGHTS RESERVED

국 문 요 약

본 논문은 IoT 환경에서 수많은 RF 기기들이 무선으로 연결될 때 발생하는 인증 문제에 초점을 맞춘다. 현대의 암호학 키 기반 MAC 계층 인증 시스템은, 키 분실 시 보안에 심각한 위협을 초래하며, IoT 환경에 적합하지 않은 복잡한 알고리즘이 요구된다. 이러한 문제를 해결하기 위한 방안으로, Physical 계층에서 기기의 고유한 RF 신호 특징을 이용하여 인증하는 RF Fingerprinting 기술이 주목받고 있다. RF Fingerprinting 은 RF 신호의 고유 특성을 복제하는 데 상당한 비용이 발생한다는 점에서 출발하며, 무선 네트워크의 보안을 강화하는데 중요한 역할을 수행할 수 있다.

본 논문은 RF Fingerprinting 관련 두 가지 연구 결과를 소개하며, 시스템 완성을 위한 Challenge 및 Future research direction 에 대해 논한다.

첫 번째 연구는 현존하는 최고의 RF 보안 시스템 중 하나인 주파수 도약 확산 스펙트럼 네트워크에서 신호 송출원 식별이 가능한 RF Fingerprinting 방법을 제안한다. 이를 위해 도약 홉 신호에 대한 SF 를 추출하여 시간-주파수 행동을 나타내는 스펙트로그램으로 변환하고, 이를 설계된 Deep Inception Network (DIN) 기반 신호 분류기에 학습시켰다. 그 결과, 도약 홉 신호에 대한 97%의 정확도로 신호 송출원을 식별할 수 있었으며, 네트워크 공격자 탐지를 위한 알고리즘은 AUROC 커브 0.99 의 성능을 확인하였다.

두 번째 연구는 IoT 환경의 공개 키 관리의 중요성을 강조하며, RF 기반 공개 키 생성기 (i.e., RF-PubKG) 모델을 소개한다. 제안하는 모델은 RF 특성 cluster 를 암호 시퀀스로 투영하는 방법으로서, 20dB SNR 에서 97.2%의 정확도를 달성하고, 노이즈가 없는 환경에서는 99.6%로 향상되는 것을 확인하였다. 나아가 생성된 공개 키 셋의 낮은 상관관계 분석을 통해 학습 기반 공개 키 시스템의 신뢰성과 독립성을 확보하였으며, RF-PubKG 기반 RSA 디지털 서명 시스템 구현을 통해 PKI 없는 PKC 로도 효과적으로 작동할 수 있음을

실증하였다. 이러한 결과는 IoT 환경에서의 공개 키 관리를 간소화하고 디지털 서명 검증 과정의 효율성을 크게 향상시킬 것으로 기대한다.

마지막으로, RF Fingerprinting 시스템의 완성을 위한 Challenge 및 Future research direction 에 대해 논한다. Real domain 으로부터 Analog Feature key 로 동작하는 기존 방법에서, Finite field 에서 동작하는 Public key 기반 RF-PubKG 로 이어지는 본 연구 기여에 대해 논한다. 여기서 나아가 Digital domain 에서 동작하는 Digitized Analog Feature key 기반 Sensor Intelligence 시스템으로의 연구 방향에 대해 논한다. 이에 현재 시스템에서의 범용적 동작을 위한 도전 과제에 대해 논하고, 이를 극복하기 위한 향후 연구 방향에 대해 논하고자 한다.

©2024
강 주 성
ALL RIGHTS RESERVED

List of Contents

Abstract	6
List of Contents	10
List of Tables	12
List of Figures	13
Chapter 1. Introduction	16
1.1. Physical layer Authentication in IoT environment	16
1.2. Radio Frequency (RF) Fingerprinting	18
1.2.1. Definition of RF Fingerprinting	18
1.2.2. Signal Fingerprints (SFs)	19
1.2.3. Related Works	21
1.2.4. Custom Data Acquisition (DA) System	23
1.2.5. RF Fingerprinting Usage Examples	24
1.3. Contributions and Outline of this Dissertation	25
Chapter 2. [Classification] RF Fingerprinting for FH Emitter Identification	28
2.1. Motivations	28
2.2. Introduction	28
2.3. Problem Formulation	33
2.3.1. Frequency Hopping (FH) Signals of Frequency Hopping Spread Spectrum (FHSS) Network	33
2.3.2. User Authentication in FHSS Networks	34
2.3.3. Emitter Identification based User Authentication in FHSS Networks	35
2.4. Proposed RF Fingerprinting-based Emitter Identification (RFEI) method	37
2.4.1. Signal Fingerprint Extraction	38
2.4.2. Time–Frequency Feature Extraction	39
2.4.3. User Emitter Classification	41
2.4.4. Base Classifier: Deep Inception Network Classifier	42
2.4.5. Ensemble Approach for Multimodal Signal Fingerprints	45
2.4.6. Attacker Emitter Detection	47
2.5. Baseline Algorithms for RF Fingerprinting Method	49
2.6. Experimental Setups	52
2.7. Results and Discussions	55
2.7.1. Emitter Identification Accuracy	55
2.7.2. Efficiency of the Inception Blocks	57
2.7.3. Class Activation Map (CAM) Analysis of the DIN Classifier	59
2.7.4. Outlier Detection Performance	61
2.7.5. Discussion	64
2.8. Summary	65
Chapter 3. [Cryptography] RF Public Key Generator for Digital Application	67
3.1. Motivations	67
3.2. Introduction	67

3.3. Background Knowledge.....	71
3.3.1. Target Radio Frequency Features	71
3.3.2. Radio Frequency Fingerprinting	72
3.3.3. Digital Signature scheme	75
3.3.4. Certificates and Public Key Infrastructure (PKI).....	76
3.4. Proposed RF based Public Key Generator (RF-PubKG) method	78
3.4.1. Radio Frequency Public Key Generator	78
3.4.2. RF-PubKG Based Hashed RSA scheme.....	81
3.5. Experimental Setups	83
3.5.1. RF feature dataset description.....	83
3.5.2. Evaluated RF Fingerprinting Models.....	84
3.5.3. Ensemble RF-PubKG.....	85
3.6. Results and Discussions	86
3.6.1. Public Key Estimation results	87
3.6.2. Reliability of the Cryptographic Sequences.....	91
3.6.3. PubKGs in hashed RSA scheme	94
3.6.4. Discussion.....	95
3.7. Summary	97
Chapter 4. Summary of Contributions and Future Research Direction.....	99
4.1. Summary of Contributions.....	99
4.2. Challenges and Future research directions for Public usage of RF Fingerprinting.....	100
Chapter 5 Conclusions	103
Bibliography	105
Curriculum Vitae	117
Acknowledgement	122

List of Tables

Table 1.1 Literatures of the RF Fingerprintings.	21
Table 2.1 Non-replicable authentication system for the physical layer of the FHSS network.....	36
Table 2.2 Structure of the base classifier: the DIN classifier.	44
Table 2.3 Proposed RFEI algorithm.	49
Table 2.4 Details of the FH dataset.....	53
Table 2.5 Implemented parameter settings.	54
Table 2.6 Emitter identification accuracy.	55
Table 2.7 Averaged confusion matrix of the ensemble approach based proposed method.	57
Table 2.8 Identification accuracies of the residual and inception blocks.....	58
Table 2.9 Averaged confusion matrix of the outlier detectors based on the proposed method.	63
Table 2.10 Averaged confusion matrix of the outlier detectors based on baseline 3.	63
Table 3.1 Proposed RF-PubKG algorithm, $F_{RF-PubKG}$	81
Table 3.2 Hashed RSA algorithm based on RF-PubKG.	83
Table 3.3 RF Feature Dataset	84
Table 3.4 Architecture of the RF-PubKG model (Based on DIN model in [2])	84
Table 3.5 Key Estimation Accuracy*	87
Table 3.6 Key Estimation Time	88
Table 3.7 Correlation Matrix for Key Sets Generated by Distinct RF-PubKG Models.....	93
Table 3.8 Quantification Analysis of RF-PubKG Based Digital Signature Scheme Implemented by Hashed RSA Algorithm	93

List of Figures

Figure 1.1 Physical layer authentication in Internet of Things (IoT) environment [11].	16
Figure 1.2 User authentication approaches in Open System Interconnection (OSI) model.	17
Figure 1.3 Way to utilize the RF Fingerprinting.	18
Figure 1.4 Example of Signal Fingerprints (SF).	19
Figure 1.5 Custom-made data acquisition (DA) system.	23
Figure 1.6 Example of tracking an un-authenticated user.	24
Figure 2.1 Non-replicable authentication scenario based on the RFEI method.	31
Figure 2.2 FH signals in two FHSS networks	33
Figure 2.3 Block diagram of the RFEI-based non-replicable authentication system.	36
Figure 2.4 Examples of the SFs: (a) RT, (b) SS, and (c) FT signals.	39
Figure 2.5 Examples of the spectrograms: (a) RT, (b) SS, and (c) FT signals.	41
Figure 2.6 Basic block for constructing the deep learning classifier used in this study: (a) the residual block [69] and (b) the inception block [70].	42
Figure 2.7 Examples of the spectrograms: (a) RT, (b) SS, and (c) FT signals.	44
Figure 2.8 Stacking ensemble approach for the multimodal SF signals.	46
Figure 2.9 Attacker detection scheme based on stacking ensemble approach.	47
Figure 2.10 Emitter identification accuracy at different signal-to-noise ratios (SNRs).	56
Figure 2.11 Identification accuracies of the residual and inception blocks at different SNRs.	58
Figure 2.12 Examples of GCAM of the DIN classifier: (a) AGCAM for target emitters, (b) positive sample with an inference score greater than 0.99, and (c) negative sample with an inference score less than 0.30.	60

Figure 2.13 PLCP frame format for FHSS networks in the 802.11 standard [57].	61
Figure 2.14 Histogram of the output vectors.	62
Figure 2.15 Receiver operating characteristic (ROC) curves.	64
Figure 3.1 An overview of the user authentication scheme in IoT Environments: (a) ID/PW-based authentication; (b) authentication based on IP and MAC addresses utilizing PKC; (c) authentication using RF features based on RFF; and (d) (RF-PubKG) the proposed method for authentication using IP and MAC addresses combined with RF features through PKC.	68
Figure 3.2 The overall RF Fingerprinting process is depicted with (a) the Pre-processing step and (b) the RF Fingerprinting step illustrating the conventional RFF, followed by (c) (Proposed) the Key Generator step representing the proposed RF-PubKG method.	72
Figure 3.3 System overview of Digital Signature schemes: (a) Traditional scheme with a certificate management system from the PKIs, illustrating the process of certificate issuance; (b) Trustworthy scheme based on the RF-PubKGs, utilizing the RFF for key generation to eliminate the need for a centralized certificate authority, thus simplifying the overall certificate management system.	76
Figure 3.4 The proposed RF-PubKG structure: The KeyGen layer is located at the highest hidden layer, which processes outputs to generate and estimate the public key, as depicted in (3.10) to (3.14).	78
Figure 3.5 Ensemble approach of RF-PubKGs: The raw key outputs from each RF-PubKG are combined in stacked manner in (3.20).	86
Figure 3.6 Key estimation accuracy of the RF-PubKG under AWGN channel conditions. The RF-PubKG achieves 97.2% at 20dB SNR, rising to 99.0% with improved channel conditions.	90
Figure 3.7 Frame error rate of the RF-PubKG under AWGN channel conditions. The RF-PubKG achieves 5.6% at 20dB SNR, 2.0% at 25dB SNR, and decreased to less than 1.0% in noise-free conditions.	90

Figure 3.8 Clustering results of estimated public keys, k_{estimate} , from RF features with the public key set \mathbf{K}_{pub} : (a) Demonstrated centrality within the training dataset; (b) Consistency maintained within the testing dataset. The public key set accurately establishes cluster centers during training and preserves center integrity in testing. 91

Figure 3.9 Correlation Matrix of the RF-PubKG. Public key correlations remain below 0.24, indicating the uniqueness of the generated public keys among RF transmitters. 92

Figure 4.1 SFs-based application in the Digital Signal Processing domain. 99

Figure 4.2 Challenges in Network Usage of the RF Fingerprinting System 100

Figure 4.3 Proposed network system for public usage of the RF Fingerprinting 102

Chapter 1. Introduction

1.1. Physical layer Authentication in IoT environment

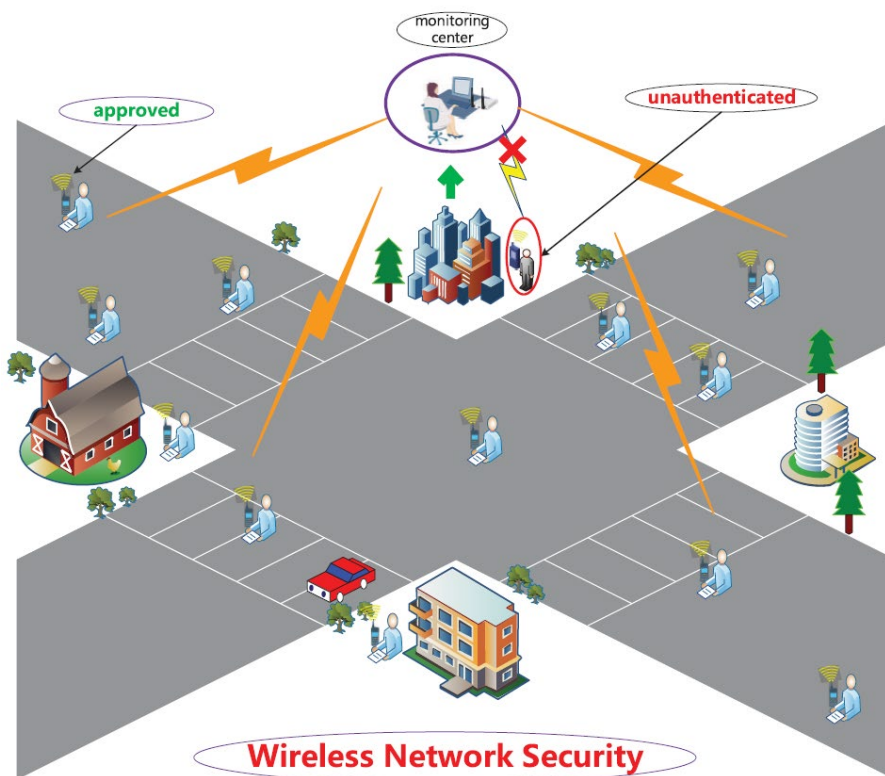


Figure 1.1 Physical layer authentication in Internet of Things (IoT) environment [11].

The Internet of Things (IoT) comprises an extensive network with interconnected devices, each requiring robust security protocols that enable safe and efficient communication. These devices are connected to application servers, which provide the necessary intelligence for their operations. Due to their huge volume of devices and distributed nature, the IoT environment demands an authentication process that is not only effective but also scalable and simple to implement.

Figure 1.1 presents an example scenario of the device authentication process in an IoT environment. These characteristics are required for authentication in IoT environments.

- **Connectivity and Scale:** IoT environments characteristically consist of thousands of devices connected over air. This extensive connectivity necessitates a streamlined yet secure method of authentication.
- **Simplicity and Efficiency:** The communication protocols used must be straightforward to accommodate the wide range of device capabilities and to facilitate easy deployment and maintenance.
- **Effective Authentication:** Ensuring that each device is authenticated before it can interact with others or access the network is crucial for maintaining system integrity and security.

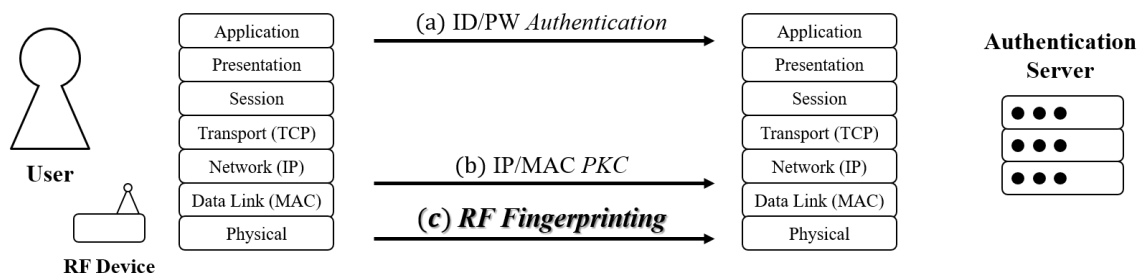


Figure 1.2 User authentication approaches in Open System Interconnection (OSI) model.

The conventional user authentication method in the Open System Interconnection (OSI) model is presented in figure 1.2. In IoT environment, these methods are commonly used for ensuring secure device authentication:

- **Encryption Key-Based Approaches:** Typically used at the MAC layer, these methods rely on secure key management and may require complex cryptographic algorithms, making them suitable for environments where additional security layers are critical.
 - ✓ ID/PW Authentication: Traditional username and password authentication which operates at the application level.
 - ✓ IP/MAC PKC: Utilizing Public Key Cryptography (PKC) at the IP and MAC address levels to secure device communications.

- **Physical Layer Authentication:** This method has gained attention for its simplicity and effectiveness. It serves as a pre-authentication step, utilizing the unique characteristics of physical RF signals emitted by devices to verify their authenticity.
 - ✓ RF Fingerprinting: A approach that uses the unique RF signal characteristics of each device to identify and authenticate it, ensuring a secure connection at the physical layer.

In conclusion, implementing robust authentication protocols in IoT environments is essential for securing the network against unauthorized access and ensuring the integrity of communications between devices. By employing a combination of traditional cryptographic methods and innovative solutions like RF Fingerprinting, IoT systems can achieve both security and efficiency.

1.2. Radio Frequency (RF) Fingerprinting

1.2.1. Definition of RF Fingerprinting

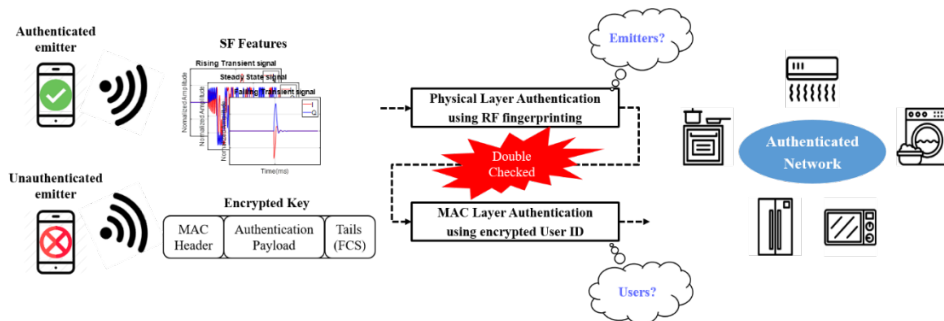


Figure 1.3 Way to utilize the RF Fingerprinting.

Radio Frequency (RF) Fingerprinting is a sophisticated identification technique employed in the range of IoT security. It leverages the unique Signal Fingerprint (SF) inherent in the RF signals emitted by devices to pinpoint their distinct transmission sources. This method is crucial for authenticating devices at the physical layer, thereby enhancing network security.

One way to utilize the RF Fingerprinting is presented in Figure 1.3. RF Fingerprinting operates by analyzing specific features of the RF signal emitted by each device, such as the steady state signal and transient changes over time. These characteristics, unique to each device due to minor imperfections in hardware manufacturing, act as an unintentional signature. By extracting and comparing these features, RF Fingerprinting can accurately identify and authenticate legitimate devices while blocking signals from unauthenticated sources. The description of the double-checking mechanism based on RF Fingerprinting is as follows:

- **Step 1) Physical Layer Authentication:** This initial step involves the direct analysis of the physical RF signal characteristics. The system captures and evaluates the signal's unique features to determine if the emitter is authenticated.
- **Step 2) MAC Layer Authentication:** Following the physical layer check, the device undergoes authentication at the MAC layer using an encrypted user ID. This double-check mechanism ensures that only devices verified at both the physical and MAC layers can access the network.

RF Fingerprinting is an effective and innovative authentication technique that ensures the integrity and security of communications within IoT networks. By utilizing the unique signal characteristics of each device, it provides a reliable method for physical layer security that complements traditional encryption-based security measures.

1.2.2. Signal Fingerprints (SFs)

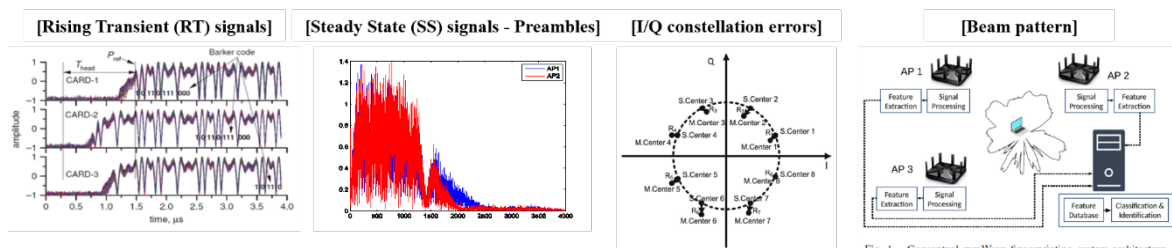


Figure 1.4 Example of Signal Fingerprints (SF).

Signal Fingerprints (SF) are numerical values derived from the RF signals emitted by devices, which uniquely identify each emitter's RF ID. These fingerprints arise due to inherent variances in the components and manufacturing process of the emitters. Even slight differences in power amplifiers (PA), frequency oscillators (FO), analog-to-digital converters (ADC), and other components can introduce unique characteristics in the signal's time domain that are challenging to duplicate or fabricate. The examples of the SFs in Figure 1.4 can be defined as follows:

- **Temporal Variations[3, 16]** : The fingerprints can be observed in the time domain from the rising transient (RT), falling transient (FT), and steady-state (SS) signal components.
- **Demodulation Characteristics[36]** : On the demodulation domain, I/Q constellation errors introduce another layer of unique identifiers which are derived from the way signals are modulated and demodulated.
- **Spatial Characteristics[49]** : Differences in the beam pattern of beacon signals also contribute to the uniqueness of the RF fingerprint.

The unique nature of these fingerprints makes them non-replicable in hardware (H/W) configurations, ensuring a high level of security against duplication attempts. Recent advancements in GAN-based duplication methods in software (S/W) manners have been reported ([27], [29]), which attempt to replicate these fingerprints digitally, but physical layer characteristics remain robust against such attacks.

SF are utilized for physical layer authentication in IoT and wireless communication systems, ensuring that only authenticated devices can access the network. The reliability of SF-based authentication is crucial for maintaining the integrity and security of communications within these networks.

SF offer a robust mechanism for device identification and authentication in radio frequency environments. By exploiting the inherent and unalterable physical properties of emitted RF signals, this method provides a secure and effective way to guard against unauthorized access and ensure network security.

1.2.3. Related Works

Table 1.1 Literatures of the RF Fingerprintings.

Signal Fingerprints Feature Extraction	RT	SS		FT
		Region Of Interest (ROI)		
		Preamble	Datagram	
Hand-craft features	[14], [45], [50]	[44], [33]	[34], [40], [52]	
Time domain (raw) signal	[51]	[47]	[21], [24], [42]	
Frequency domain signal	[3], [46]	[3]		[3]
Time-Frequency domain signal	[43]		[38], [41]	
Other approaches: - I/Q Connotation domain: [30], [48] - GAN approach: [37], [39] - Beam pattern approaches : [49]				

RF Fingerprinting has become a core technology in securing wireless communications by identifying devices based on inherent and unique characteristics of their emitted signals. Recent research has focused extensively on two key aspects: the derivation of SF and the methodologies for Feature Extraction from these fingerprints. Literature results are presented in Table 1.1.

SFs are critical in the domain of RF Fingerprinting for their role in uniquely identifying device emissions. These fingerprints are derived from various aspects of the signal such as RT, SS, and FT phases. The primary methods for extracting these features can be broadly categorized into:

- **Hand-craft Features:** Sophisticated features that require in-depth understanding of signal properties, typically calculated manually or with minimal automation.
- **Machine Learning Techniques:** Utilizing deep learning classifiers to automate feature extraction and improve identification accuracy.

Literature has shown a diversity in approach, focusing on temporal, frequency, and time-frequency domains to derive these features, as evidenced by references such as [14][45][50] for hand-crafted features, [51] for time-domain signals, and [3][46] for frequency-domain signals.

Feature Extraction in RF Fingerprinting can be segmented based on the signal characteristics:

- **Transient Signal Approach:** Focuses on features from signal transients including amplitude, phase, and frequency variations. Common extraction techniques include Principal Component Analysis (PCA) and statistical feature extraction such as mean and variance ([3, 12-19], [14, 15]).
- **Steady State Signal Approach:** These approaches concentrate on sustained signal parts or the decay phase of signals, respectively, with methodologies ranging from Differential Constellation Trace to entropy and energy-based features ([29], [34], [35]).
- **Advanced Categorizations:** Incorporating methods such as log spectral energy features, Mutual Information for frequency, and Maximum Cross Correlation results to refine the extraction process ([25, 26], [31], [32]).

The literature categorizes and references a vast array of methods and signal aspects, illustrating the depth and breadth of the field. For instance, transient signals are explored through various facets, from basic amplitude and phase trajectories to complex wavelet transform coefficients and Fourier Transform-based techniques ([15], [17]). Steady state signals benefit from advanced data information methods like the I/Q constellation trace figure features and matched filter coefficients ([30], [33]).

Moreover, FT signals, a less commonly studied feature, have seen methodologies developed around their unique properties, such as frequency offset features and constellation tract figure features ([3], [30]).

The field of RF Fingerprinting is evolving, with a rich literature base exploring various feature extraction techniques across different signal domains. The continuous development in statistical and machine learning approaches is particularly promising, offering paths to more robust and automated systems that can enhance security measures in wireless networks.

1.2.4. Custom Data Acquisition (DA) System

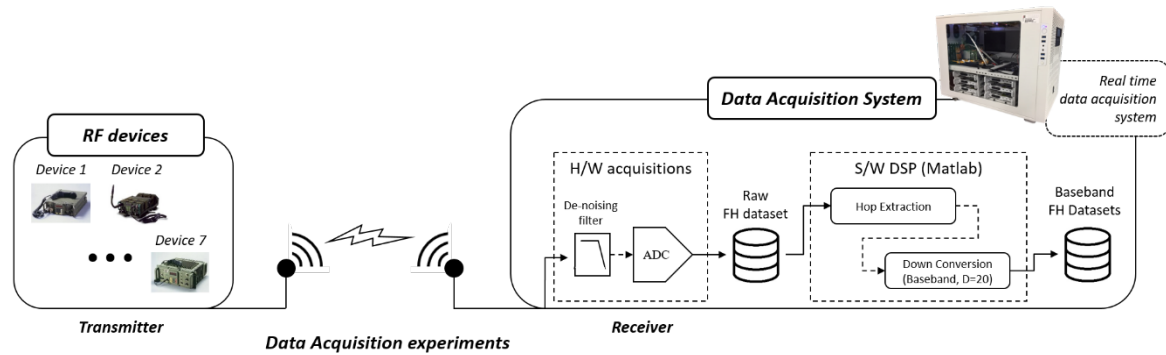


Figure 1.5 Custom-made data acquisition (DA) system.

To effectively capture and analyze RF signals in our research, we developed a custom-made Data Acquisition (DA) system. Architecture of DA system is presented in Figure 1.5. This system is engineered to handle high-speed data capture and processing, enabling us to analyze RF signals in real-time.

The DA system consists of several key components:

- **High-Speed Digitizer:** The core of our DA system is the PXI14400 digitizer, which supports sampling rates up to 400 MHz with a 14-bit resolution. This high-speed digitizer is crucial for capturing RF signals with high fidelity.
- **Storage System:** We employed a RAID-0 configuration with six Solid State Drives (SSDs) to ensure fast data writing speeds of up to 1.6 GB/s. This setup allows for the real-time streaming and storage of large amounts of data.
- **Software for Data Processing:** Data processing is conducted using MATLAB and DSP techniques implemented in software. These processes include the decoding and extraction of RF features from the raw dataset.

The RF signal capture process begins with the transmission of the RF signal from RF emitters. The signal is then received and down-converted to an Intermediate Frequency (IF) using a combination of the Nagoya NL-R2 UHF antenna, an RF mixer, and the E4438C ESG vector signal generator. The down-converted IF signal is sampled by the PXI14400 digitizer.

Following this, Digital Signal Processing (DSP) techniques are applied to extract the RF burst from the IF signal. We utilized an energy detection approach, as described in reference [2], to detect these RF bursts. The signal is then further processed to down-convert it to the baseband with a decimation factor, forming the baseband RF burst dataset used for feature extraction.

This custom DA system provides a robust platform for capturing and analyzing RF signals, supporting advanced research in RF Fingerprinting and other wireless communication technologies. The integration of high-speed digitization with real-time data processing capabilities allows for effective handling and analysis of RF data, critical for developing new security protocols and understanding RF signal behaviors.

1.2.5. RF Fingerprinting Usage Examples

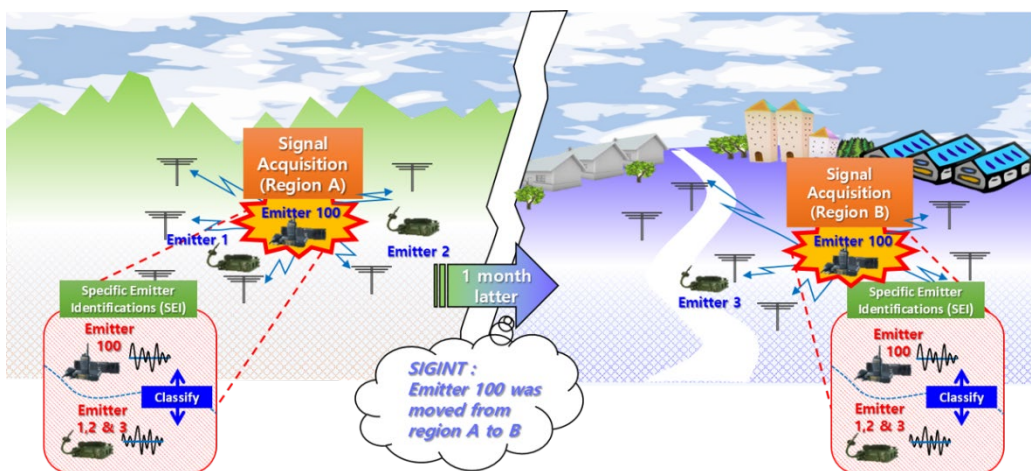


Figure 1.6 Example of tracking an un-authenticated user.

RF Fingerprinting is a powerful technology that can significantly enhance the security and management of wireless communications in public spaces. By identifying unique transmission sources, RF Fingerprinting supports both the authentication of legitimate devices and the tracking of unauthorized emitters. Example of tracking scenario is presented in Figure 1.6.

RF Fingerprinting utilizes distinct characteristics inherent in the RF signals emitted by each device to determine its identity. This unique identification process is crucial in

environments where secure communication is paramount, such as in IoT networks spanning public infrastructures.

- **Secured Communication for Authenticated Users:** In IoT environments, ensuring that communication happens between authenticated devices is essential. RF Fingerprinting aids this process by providing a reliable means to verify if communication originates from a legitimate source. This not only helps in maintaining data integrity but also protects the network from potential cyber threats.
- **Tracking and Locating Unauthorized Emitters:** Unauthenticated devices can pose significant security risks. RF Fingerprinting enables network administrators to detect and locate unauthorized emitters. Once an unauthenticated signal source is identified, it can be isolated, and appropriate security measures can be enacted to prevent any malicious activities or breaches.

RF Fingerprinting offers a robust solution for enhancing security in wireless networks. By enabling precise identification and tracking of RF emitters, this technology plays a crucial role in securing IoT environments and other public communication networks. The ability to differentiate between authenticated and unauthenticated signals ensures that only trusted devices participate in the network, maintaining overall system integrity and security.

1.3. Contributions and Outline of this Dissertation

This dissertation delves into the application of RF Fingerprinting within IoT environments, addressing both theoretical and practical implications. The primary contributions are:

- **Development of an RF Fingerprinting System:** Proposing an RF Fingerprinting framework working at the identification of Frequency Hopping (FH) signals, ensuring high-security standards and system integrity.

- **Abnormal/Outlier Detection Algorithm:** Introducing an advanced algorithm for detecting anomalies in RF signals. This algorithm is designed for scalability and integrates incremental learning techniques, enhancing adaptability in dynamic environments.
- **Integration of RF Fingerprinting with Public Key Infrastructure:** By merging RF Fingerprinting techniques with public key-based cryptography, the dissertation proposes novel SF-based digital signature algorithms that do not rely on traditional PKI systems.

These contributions are supported by extensive research and are detailed further in the following subsequent chapters. Chapter 2 delves into the classification of RF Fingerprinting for identifying FH emitters, detailing problem formulations, proposed methods for emitter identification, and various RF Fingerprinting techniques, including feature extraction and classification algorithms. Chapter 3 shifts focus to cryptographic applications of RF Fingerprinting, proposing a new RF-based Public Key Generator (RF-PubKG) and discussing its implementation and providing a detailed examination of the experimental setups and results. This includes evaluations of RF Fingerprinting models and an ensemble approach for enhancing the system's robustness. Chapter 4 discusses the challenges for public operation of the RF Fingerprinting system, and proposing future research directions to overcome these challenges. Finally, Chapter 5 concludes the dissertation, summarizing the key findings and suggesting future research directions. The dissertation also includes a comprehensive bibliography, a curriculum vitae, and acknowledgements, detailing the academic contributions and the collaborative efforts behind the research.

Several key publications have emerged from this research, contributing significantly to the field of RF Fingerprinting:

- [1] Jusung Kang et al., "Radio Frequency Public Key Generator for Digital Application," IEEE Access, 2023.
- [2] Jusung Kang et al., "Radio Frequency Fingerprinting for Frequency Hopping Emitter Identification," Applied Sciences, 2021.

- [3] Kiwon Yang et al., "Multimodal Sparse Representation-Based Classification Scheme for RF Fingerprinting," IEEE Communications Letters, 2019.
- Additional references [4]-[10] detail various aspects and applications of RF Fingerprinting explored throughout this dissertation.

These publications underscore the dissertation's impact and its foundational role in advancing RF Fingerprinting technologies.

Chapter 2. [Classification] RF Fingerprinting for FH Emitter Identification

The studies in this chapter have been published in Applied Sciences [2].

2.1. Motivations

In a frequency hopping spread spectrum (FHSS) network, the hopping pattern plays an important role in user authentication at the physical layer. However, recently, it has been possible to trace the hopping pattern through a blind estimation method for FH signals. If the hopping pattern can be reproduced, the attacker can imitate the FH signal and send the fake data to the FHSS system. To prevent this situation, a non-replicable authentication system that targets the physical layer of an FHSS network is required. In this study, a radio frequency fingerprinting-based emitter identification method targeting FH signals was proposed. A SF was extracted and transformed into a spectrogram representing the time-frequency behavior of the SF. This spectrogram was trained on a deep inception network-based classifier, and an ensemble approach utilizing the multimodality of the SFs was applied. A detection algorithm was applied to the output vectors of the ensemble classifier for attacker detection. The results showed that the SF spectrogram can be effectively utilized to identify the emitter with 97% accuracy, and the output vectors of the classifier can be effectively utilized to detect the attacker with an area under the receiver operating characteristic curve of 0.99.

2.2. Introduction

The most important task in user authentication of a wireless communication system is to identify the emitter information of RF signals. A common way to confirm the emitter

information, that is, the emitter ID, is to decode the address field of the medium access control (MAC) frame [53]. However, under this digitized information-based authentication process on a MAC layer, an attacker can possess the address information and imitate it as an authenticated user. To prevent this weakness, a physical layer authentication process, namely RF Fingerprinting, has been studied in recent years [54].

RF Fingerprinting is an identification technique that utilizes a SF to identify the unique emitter source of an RF signal. In the manufacturing of RF components inside an emitter, process tolerance is inevitable. These tolerances affect subtle differences in the features of the emitted RF signal. Because these process tolerances are not reproducible, an SF can act as the fingerprint of an emitter. It can also be utilized as a non-replicable authentication key to identify the authenticated user [55].

RF Fingerprinting can be used to distinguish SFs in RF signals [3, 14, 21, 33, 38]. A conventional approach is to design a handcrafted feature from the SFs based on domain knowledge. In [14], the statistical moment and entropy were calculated from spectrograms of the transient signal to identify Bluetooth devices. In [33], statistical moments were calculated from preamble signals to identify Bluetooth devices. In [3], the principle components of the transient and steady state signals using sparse representation were proposed to identify Walkie-Talkies. A recent approach is to train SFs directly using a deep learning-based classifier. In [21], the signal difference between the received signal and the ideally encoded signal was calculated as the SF. It was trained using a one-dimensional convolutional neural network (CNN)-based ensemble classifier to identify ZigBee devices. In [38], the Hilbert spectrogram of the SF was utilized to train a residual-based classifier.

The FHSS is a highly secure communication protocol frequently used in secure communication systems [56]. With an FHSS system, the FH signal rapidly hops from one frequency to another in a predefined pseudo-random fashion. This hopping pattern is known only to the transmitter–receiver pair. Thus, an attacker who does not possess the hopping pattern cannot pretend to be an authenticated user. In this case, the hopping pattern is a key for the authentication process on the physical layer of the FHSS network.

However, in recent days, attackers may have possessed the predefined hopping

patterns. Especially for the FHSS network in the industry–science–medical (ISM) band as the hopping sequence is described in the IEEE 802.11 standard [57]. Scholars have also estimated the hopping pattern as a blind estimation condition [58–60]. In [58], the hopping sequence was extracted from the USRP device, and an attack model based on the extracted hopping sequence was discussed. In [59], a real time hopping frequency tracking model based on the autoregressive moving average was proposed. In [60], the FH signals were sorted based on the power and hopping time information. From these studies, hopping patterns are expected to be traceable today and reproduced in the future.

Recently, a frequency hopping network based on non-orthogonal multiple access (NOMA) was proposed [61]. In the NOMA system, the probability that the attacker intercepts the FH signal can be reduced through the two stage relay communication [62], the additive artificial noise method [63], and the optimization of the power allocation for the beamforming scheme [64]. However, this antiinterception capability is closely related to the outage probability of the NOMA users, closely related to the signal power. This means that if the attacker is closely located to the near user side with a high SNR value, the attacker can intercept the FH signal and trace the hopping pattern.

Once a hopping pattern is reproducible, an attacker can generate FH signals similar to those of the authenticated user. The two hopping patterns become undiscernible and the attacker can pretend to be the user. In this case, the received signal can be demodulated to proceed to the MAC layer inspection step. The MAC layer authentication system should discern the attacker unless even the digital key is exposed to the attacker. That is, if the attacker knew the digital key of the network system, the attacker would be able to pretend to be the authenticated user, which is the case in deceptive jamming attacks [65] or man-in-the-middle attacks [66]. These attacks are not easily detectable and can flood fake data to mislead the network system [65]. To prevent such attacks, a non-replicable authentication system that can detect an attacker who even knows the digital key is required.

This study aims to propose an enhanced solution to the physical layer authentication problem in the case in which the attacker can reproduce the hopping pattern. The scenario of the problem is shown in Figure 2.1. It is assumed that the user, attacker, and receiver exist in the FHSS network. The goal of the attacker is to deceive the receiver by emitting the

imitated FH signal based on the replicated hopping pattern. The primary goal of the receiver is to decide if the signal received came from the user or from the attacker.

The novel receiver algorithm we propose in this study is an RF Fingerprinting-based emitter identification (RFEI) method that targets the physical layer of the FHSS network. By examining the emitter ID on the received FH signal, the receiver can decide if the current FH signal is emitting from one of the allowed users. If the emitter ID of the current FH signal is not included in the set of authenticated user IDs, the receiver can reject the current FH signal before it is passed to the MAC layer. The RFEI method can achieve system enhancement by being applied to the user authentication process. As the key of the RFEI method, that is, the SF, is generated by the process tolerances during the manufacturing process, the attacker cannot reproduce it. By detecting these attackers based on the SFs, non-replicable authentication systems can be achieved wherein the receiver can reject FH signals even if an attacker knows the hopping pattern and the digital key.

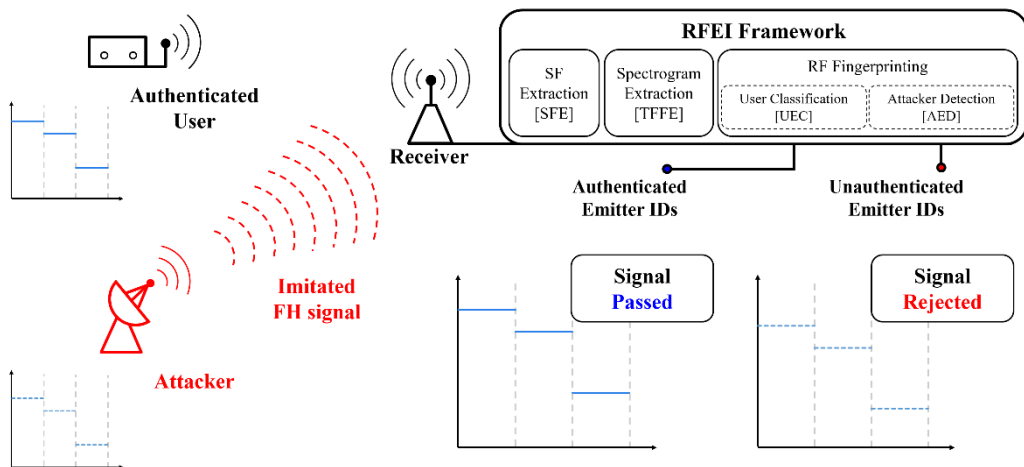


Figure 2.1 Non-replicable authentication scenario based on the RFEI method.

The RFEI method consists of four steps: SF extraction (SFE, Chapter 2.4.1), time–frequency feature extraction (TFFE, Chapter 2.4.2), user emitter classification (UEC, Chapter 2.4.3 to 2.4.5), and attacker emitter detection (AED, Chapter 2.4.6). As a preprocessing step, the target hop signal is down-converted to the baseband based on the hopping pattern known to the receiver. The baseband hop signal is passed to the SFE step to extract the analog SFs, i.e., RT, SS, and FT signals are extracted. The SF is provided to the

TFFE step to transform the SF into the time–frequency domain, i.e., the spectrogram. The spectrogram is provided to the UEC stage to train and test the spectrogram on a custom deep inception network (DIN)-based classifier. In addition, the ensemble approach is applied to exploit the multimodality of the analog SFs. Finally, the classifier output vector is provided to the AED step in which a detection algorithm is applied to detect the FH signal of the attacker. The novelties of this study are that (1) RF Fingerprinting methods were evaluated targeting for FH signals, (2) the ensemble approach was applied to utilize the multimodality of SFs, and (3) the RFEI framework was employed to identify users and detect attackers simultaneously.

The RFEI algorithm was evaluated on a few SFs and ensemble-based approaches. The algorithm compares to well designed baselines inspired by recent approaches described in the RF Fingerprinting literature [14, 21, 33, 38]. The experiments were performed using an actual FH dataset to evaluate the reliability of the algorithm. The results confirm that the proposed DIN classifier could improve the emitter ID identification accuracy by more than 1% compared to the baseline (Chapter 2.7.1). In addition, the multimode SF ensemble approach proved to be the most effective, achieving the best results with 97.0% identification accuracy for the seven FHSS emitters (Chapter 2.7.2). Regarding the detection performance, the classifier output vector of the outliers exhibited a much lower value than those of the training sample. By utilizing these differences, the detector based on the DIN-based ensemble classifier can improve the area under the receiver operating characteristic curve (AUROC) from 0.97 to 0.99 compared to the baseline. This result indicates that the classifier output vectors can effectively be used to detect the attacker signal input (Chapter 2.7.4).

The remainder of this study is organized as follows. The problem formulation is presented in Chapter 2.3. The details of the RFEI method are described in Chapter 2.4, and the baseline algorithms are explained in Chapter 2.5. The results, a discussion, and other details of the experiments are described in Chapter 2.6 and 2.7. The conclusion is presented in Chapter 2.8.

2.3. Problem Formulation

2.3.1. Frequency Hopping (FH) Signals of Frequency Hopping Spread Spectrum (FHSS) Network

In this study, we consider an FHSS network in which K FH signals are observed in a single receiver. To consider the ability of attackers to imitate FH signals similar to those of an authenticated user, we assume that the h th hopping times of the k th FH signals t_h^k have the same value, that is, the FH signals hop simultaneously. An example of an FHSS network with the two different FH signals is presented in Figure 2.2.

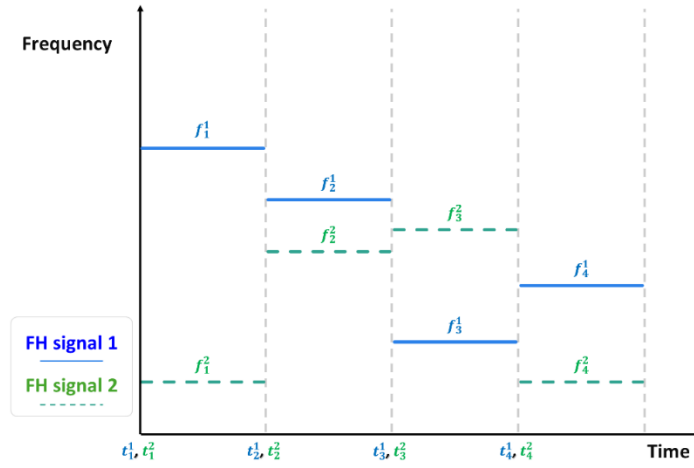


Figure 2.2 FH signals in two FHSS networks

A single FH signal is defined as follows

$$x^k(t) = a^k e^{j2\pi(f^k(t)t + \varphi^k(t))} \quad (2.1)$$

where $x^k(t)$ is the FH signal emitted by the k th emitter, a^k is the amplitude and is the hopping frequency of the k th FH signal $x^k(t)$, and $\varphi^k(t)$ is the phase difference modulated by the k th message signal $m^k(t)$. When the message signal is modulated with frequency modulation (FM), the phase difference is defined as follows

$$\varphi^k(t) = \int_{-\infty}^t m^k(\alpha) d\alpha \quad (2.2)$$

From Equation (2.1), all the K FH signals simultaneously observed by a single receiver can be defined as follows

$$y(t) = \sum_{k=1}^K x^k(t) + n(t) \quad (2.3)$$

where $y(t)$ is the observed RF signal and $n(t)$ is the additive white Gaussian noise (AWGN) present in the channel environment.

The FH signal is observed during the observation time T . During this time, a total of H hops are observed. Within a single hop duration of the h th hop signal, $t_h \leq t < t_{h+1}$, the hopping frequency $f^k(t)$ is held constant at f_h^k , denoting the h th hopping frequency of the k th FH signal. Thus, Eqs (2.1) and (2.3) can, respectively, be reformulated as follows

$$x_h^k(t) = A e^{j2\pi(f_h^k t + \varphi_h^k(t))}, \text{ for } t_h \leq t < t_{h+1} \quad (2.4)$$

$$y_h(t) = \sum_{k=1}^K x_h^k(t) + n(t), \text{ for } t_h \leq t < t_{h+1} \quad (2.5)$$

where $x_h^k(t)$ is the h th hop signal of the k th FH signal and $y_h(t)$ is the observed RF signal during the h th hop duration, $t_h \leq t < t_{h+1}$, where a total of K hop signals exist.

2.3.2. User Authentication in FHSS Networks

In an FHSS network, the core process for user authentication can be performed in two steps: (1) determining whether or not the appropriate hopping frequency is measured, and (2) determining whether or not the header information of the MAC frame is correct.

Because we assume that the attacker can reproduce the predefined hopping pattern $\mathbf{f}^k = [f_1^k, f_2^k, \dots, f_H^k]$, the imitated FH signal will display the same hopping frequency pattern. The imitated FH signal will be demodulated and passed through the MAC layer, that is, Step 1 is disabled. The process of inspecting the address field in the MAC header remains. However, because this address information has been digitized, the attacker can possess and imitate this address field. If an attacker sends an address field similar to an authenticated emitter, there is no way to detect and prevent it. Therefore, the emitter identification process based only on header information of the MAC frame is not sufficient to reject the imitated FH signal.

2.3.3. Emitter Identification based User Authentication in FHSS Networks

We propose a non-replicable authentication system that operates on the physical layer of the FHSS network presented in Figure 2.3 and Table 2.1 (i.e. Algorithm 1). By adding the emitter identification framework within the authentication process, we can achieve an enhanced physical layer authentication system for the FHSS network by verifying (1) whether or not the appropriate hopping frequency is measured, (2) whether the emitter ID of the current FH signal is an authenticated user or attacker, and (3) whether or not the header information of the MAC frame is correct.

In this study, our target was to evaluate the RFEI framework for the FH signals corresponding to Step 2 of Algorithm 1. We intended to develop an algorithm to estimate the emitter ID from the baseband FH signal such that

$$s_h^k(t) = Ae^{j2\pi\phi_h^k(t)}, \text{ for } t_h \leq t < t_{h+1} \quad (2.6)$$

$$\tilde{k} = F_{RFEI}(s_h^k(t)) \quad (2.7)$$

where $s_h^k(t)$ is the baseband hop signal down-converted from the hop signal $x_h^k(t)$ and \tilde{k} is the emitter ID estimated from the RFEI algorithm F_{RFEI} .

As the receiver knows the hopping frequency, f_h^k , the target hop signal, $x_h^k(t)$ can

be extracted from the observed FH signal, $y_h(t)$. This approach is reasonable as the FH signal must be demodulated to an IF or baseband and passed to the MAC layer to decode the digital data modulated by the message signal, $m^k(t)$. The SFs are non-replicable differences dependent on the manufacturing process of the emitter. Therefore, the SFs are independent of the hopping frequency and should be in the baseband of the hop signal, $s_h^k(t)$.

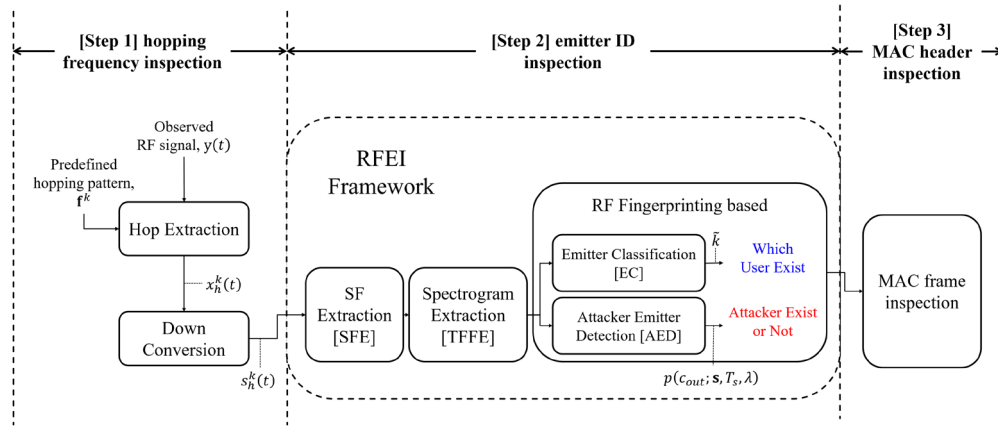


Figure 2.3 Block diagram of the RFEI-based non-replicable authentication system.

Table 2.1 Non-replicable authentication system for the physical layer of the FHSS network.

Algorithm 1. Non-replicable authentication system for the physical layer of the FHSS network.

Input: The observed RF signal $y(t)$

For each hop duration, $t_h \leq t < t_{h+1}$ **do:**

Step1: Extract and down-convert the target hop signal $x_h^k(t)$ to the baseband hop signal $s_h^k(t)$ from the observed signal $y_h(t)$ based on a predefined hopping pattern f_h^k .

If RFEI is activated **do:**

Step 2-1: Estimate the emitter ID based on the RFEI algorithm on (2.7)

Step 2-2: Pass the hop signal $x_h^k(t)$ when the emitter ID k is an authenticated emitter ID.

Step 2-3: Reject the hop signal $x_h^k(t)$ when the emitter ID k is an attacker's emitter ID.

Step 3: Send all passed baseband hop signals $s_h^k(t)$ to the next step, i.e., the MAC frame inspection.

Output: The authenticated baseband signal $x^k(t)$.

2.4. Proposed RF Fingerprinting-based Emitter Identification (RFEI) method

The RFEI algorithm is implemented as follows.

- **SF extraction:** An SF is an RF signal that contains feature information for emitter ID identification. It can be any signal involved in the demodulation process for communication. However, the SF used in this study focused on analog SF, i.e., RT, SS, and FT signals.
- **Time–frequency feature extraction:** A feature is a set of values containing physical measurements that can ensure robust classification. Any feature having a physical meaning can be applied from statistical moments to a raw preamble signal. In this study, a spectrogram of the SF was considered.
- **User emitter classification:** Classification is a decision process in which an emitter ID can be estimated from an input feature. A classifier was trained and tested on a large set of extracted features. Subsequently, the emitter ID was estimated from the classifier output vector. In this study, we consider a discriminative classifier model from a support vector machine (SVM) to a DIN-based ensemble classifier.
- **Attacker emitter detection:** This detection process enables the classifier to search whether the input feature has been trained for the classifier. The difference between the classifier output characteristics of the trained and outlier samples can be utilized. In this study, a simple but effective threshold based approach was applied.

The RFEI method can be formulated as a classification problem using the following expression

$$\mathbf{y} = F_{RFEI}(\mathbf{s}) \quad (2.8)$$

where $\mathbf{s} = [s(T_s), s(2T_s), \dots, s(NT_s)] \in \mathbb{C}^{N \times 1}$ is a baseband hop signal sampled by the sampling period T_s . The vector representation of the signal is now used in this study for convenience. Further, N is the length of a complex valued baseband hop signal, F_{RFEI} is a mapping function from the signal space to the ID space referencing the RFEI algorithm, and $\mathbf{y} \in \mathbb{R}^{C \times 1}$ is the output vector of the algorithm containing the emitter ID information, where C is the number of emitters trained on the algorithm.

2.4.1. Signal Fingerprint Extraction

The SF can be defined as any subtle differences in the demodulation and decoding of the FH signal, which can uniquely identify the emitter ID. However, in this study, our objective was to identify the emitter ID before passing through the MAC layer. Thus, we targeted the analog SF that could pass the physical layer in the form of RT, SS, and FT signals. We represent them by

$$\mathbf{s}_{SF} = \mathbf{g}_{SF}(\mathbf{s}) \quad (2.9)$$

where \mathbf{g}_{SF} is the extraction function of the SF, and $\mathbf{s}_{SF} \in \mathbb{C}^{N_{SF} \times 1}$ is the SF selected from a set of possible lists, that is, $SF \in \{RT, SS, FT\}$. Here, N_{SF} is the length of the SFs.

Based on the definition of the SF signal in [3], the RT signal is defined as an increasing RF signal that increases from the noise level to the designed level. The SS signal is defined as a region of the RF signal that contains a modulated signal with a designed energy level, and the FT signal is defined as an inverse case of the RT signal, decreasing the RF signal from the designed energy level to the noise level.

For accurate extraction, the extraction procedure is structured based on the energy variation of the SFs. For the windowed vector $\mathbf{s}_n = s[i + (n-1)/2 \times W_E : i + (n+1)/2 \times W_E]$ with the extraction window size W_E and its L_2 norm energy E_n , the detection rule for the transient signals can be expressed as follows

$$\begin{cases} E_n \geq (1 + \delta) \times E_{n-1}; & T^{RT} \leftarrow [T^{RT} \quad i] \\ E_n \leq (1 - \delta) \times E_{n-1}; & T^{FT} \leftarrow [T^{FT} \quad i] \end{cases} \quad (2.10)$$

where δ is the threshold value for detecting the energy variance and T^{RT} and T^{FT} are the detected time indices for the RT and FT signals, respectively.

A sliding window method is applied to monitor the energy variation of the incoming signal, which is then used to detect the RT and FT signals. The RT signal is detected as a signal in which the L_2 -norm energy of the window is increased by 10% or more. The FT signal is defined as a decreasing case. After detecting the RT and FT signals, the SS signal can be defined as the signal between the RT and FT signals using the following definitions:

$$\begin{aligned} \mathbf{s}_{RT} &= s [T^{RT} [1]:T^{RT} [-1]] \\ \mathbf{s}_{SS} &= s [T^{RT} [-1]:T^{FT} [1]] \\ \mathbf{s}_{FT} &= s [T^{FT} [1]:T^{FT} [-1]] \end{aligned} \quad (2.11)$$

The extraction results for the SFs are presented in Figure 2.4.

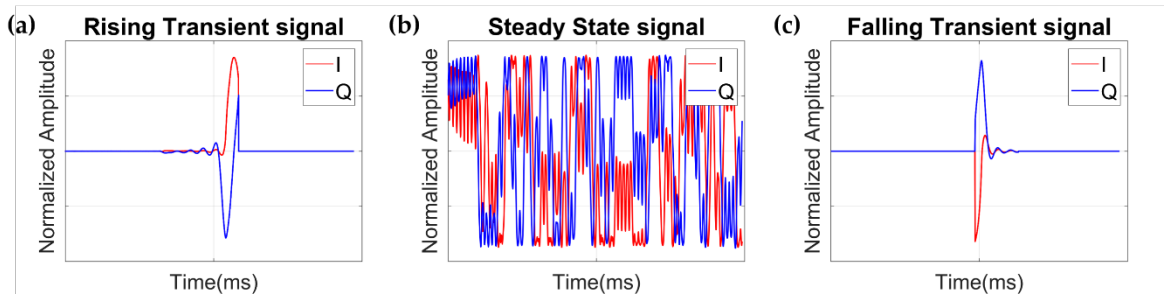


Figure 2.4 Examples of the SFs: (a) RT, (b) SS, and (c) FT signals.

2.4.2. Time–Frequency Feature Extraction

The next step is to design a feature from the SF. The purpose of this step is to transform the SF domain into a specific feature domain in which the physical measurements between different emitters could be well distinguished. In conventional approaches [3, 14, 33], the

designed handcrafted features are calculated from signal characteristics of the SFs. In this case, the goal is to obtain a feature domain that can ensure robust classification results. However, in more recent approaches [21, 38], the purpose of this step is slightly modified. The SFs are transformed into domains that can express the signal characteristics of the SFs, and the identification of a feature domain that can ensure robust classification is entrusted to the classification step based on a deep learning-based classifier. The relevant procedure is expressed as follows

$$\mathbf{s}_{Feature} = \mathbf{q}_{SF}(\mathbf{s}_{SF}) \quad (2.12)$$

where \mathbf{q}_{SF} is the transform function for the designed feature domain, $\mathbf{s}_{Feature} \in \mathbb{R}^{N_{SF}^f \times N_{SF}^t}$, where N_{SF}^f and N_{SF}^t are the sizes of the frequency and time indices, respectively, of the spectrogram transformed from the SF.

In this study, the time–frequency distribution of the FH signals, that is, the spectrogram, was analyzed. The spectrogram is a well-known time–frequency analysis method used to visualize the variation of the frequency components calculated from nonstationary signals [67]. The feature design strategy used in this study requires analysis of the power density behavior of the SFs in the time–frequency domain. The key idea of the FHSS system is that the carrier frequency of the FH signal hops within a predefined frequency range. Therefore, the signal characteristics must be implied in the distribution of the time–frequency domains.

A discrete-time short-time Fourier transform (STFT) is applied to compute the spectrogram of the SFs. With the sliding window $w[n]$ with a size of W_{STFT} , the STFT of the SFs can be calculated as follows

$$\text{STFT}_{s_{SF}}[m, p] = \sum_{n=-N_{SF}}^{N_{SF}} s_{SF}[n] w[n-m] e^{-j2\pi pm} \quad (2.13)$$

where $m = 1, 2, \dots, K_{SF}^t$ is the time sampling point along the time axis and $p = 1, 2, \dots, K_{SF}^f$

is the frequency sampling point along the frequency axis. We set N_{SF} as a sufficiently large value.

Next, the power density behavior of the spectrogram can be represented as the magnitude squared of the STFT such that

$$\text{spectrogram}\{\mathbf{s}_{SF}\} = \left| \text{STFT}_{s_{SF}}[m, p] \right|^2 \quad (2.14)$$

The spectrogram results are presented in Figure 2.5.

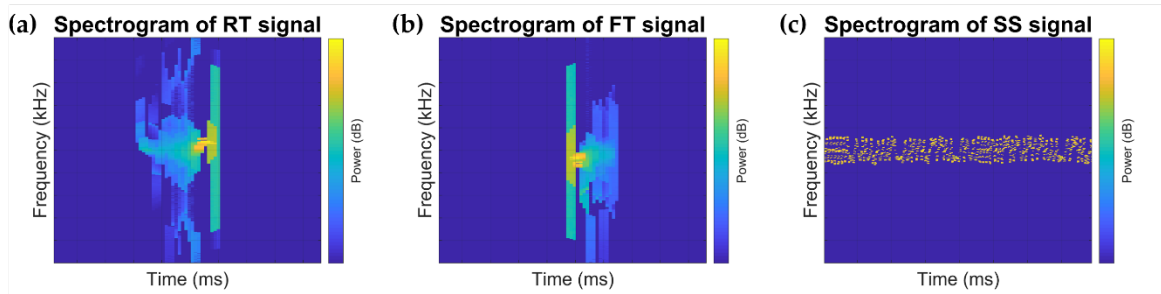


Figure 2.5 Examples of the spectrograms: (a) RT, (b) SS, and (c) FT signals.

2.4.3. User Emitter Classification

The third step is to identify the emitter ID from the designed feature. The goal is to design a classification algorithm that can learn spectrograms for robust classification results. Owing to recent research in the field of deep learning, deep neural networks are well known for their abilities to extract spatial or temporal features with nonlinear computational capabilities [68]. Thus, we aimed to construct a deep learning-based classifier to train the spectrogram of the SFs. The classification process can be obtained using

$$\mathbf{y} = \mathbf{f}_{Classifier}(\mathbf{s}_{Feature}) \quad (2.15)$$

where $\mathbf{f}_{Classifier}$ is the deep learning-based classification algorithm, and the output vector \mathbf{y} implies the emitter ID information k .

2.4.4. Base Classifier: Deep Inception Network Classifier

There are two main blocks to construct the custom deep learning-based classifier: a residual block [69] and an inception block [70]. The residual block is designed to enable flexible training as the depth of the network increases. In the case of the inception block, the main purpose is to filter out input features with different receptive field sizes.

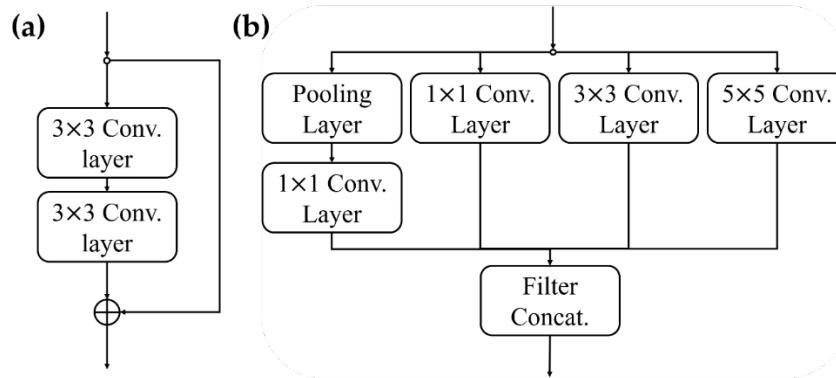


Figure 2.6 Basic block for constructing the deep learning classifier used in this study: (a) the residual block [69] and (b) the inception block [70].

The custom deep learning-based classifier utilized in our study consists of two main blocks: a residual block [69] and an inception block [70]. The architecture of these blocks is shown in Figure 2.6.

The design strategy of the residual block is to handle the degradation problem as the network goes deeper [69]. The residual block contains skip connections between adjacent convolutional layers and helps mitigate the vanishing gradient problem. The goal of the residual network is to allow flexible training of the features as the network depth increases.

The design strategy of the inception block involves calculating features with different filter sizes in the same layer [70]. The inception block contains parallel convolutional layers with different filter sizes. The results for each layer are concatenated in the filter axis and pass through the next layer. These parallel connections can extract features with multiple receptive field sizes, which are useful when the features vary in location and size.

The spectrogram contains the physical measurements of the SF signals. It represents the power densities of the SF signals along the time–frequency axes. To train these two-dimensional density behaviors of the SF signals, we aimed to filter the spectrogram on multiple filter scales in the temporal and spatial domains by applying inception blocks.

The spectrogram consists of physical measurements calculated from the SF signals. It represents the power densities of the SFs along the time–frequency axes. Thus, the subtle differences exhibited by the SFs can be anywhere on the time–frequency axes of the spectrogram, and the size of the features can be varied. To train these SFs, we aimed to filter the spectrogram on multiple scales in the temporal and spatial domains by applying inception blocks to construct a custom deep learning classifier.

We utilized the inception-A and reduction-A blocks to construct the base classifier: the DIN classifier. The inception-A and reduction-A blocks are the basic blocks for constructing the Inception-v4 models [71]. The role of the inception-A block is to filter the input features with multiple receptive field sizes and concatenate them as the filter axis, thereby expanding its dimensions. The role of the reduction-A block is to downsize the feature map on the grid side, that is, the time–frequency axes of the spectrogram. It can effectively manage the number of weights inside the classifier, similar to the pooling layer.

We adopted the inception-A and reduction-A blocks, as shown in Figure 2.7. The structures of the blocks are the same as defined in [71]. However, the filter sizes N_F of the sublayers were set to 32 and 64, adjusted by the experiments. Batch normalization [72] and rectified linear unit activation units were applied immediately after every convolutional layer. The inception-A block was applied twice to expand the filter axis, and the reduction-A block was applied once to resize the feature map on the grid axis. We applied these block sequences twice, adjusted by heuristic experiments. The total structure of the DIN classifier is provided in Table 2.2.

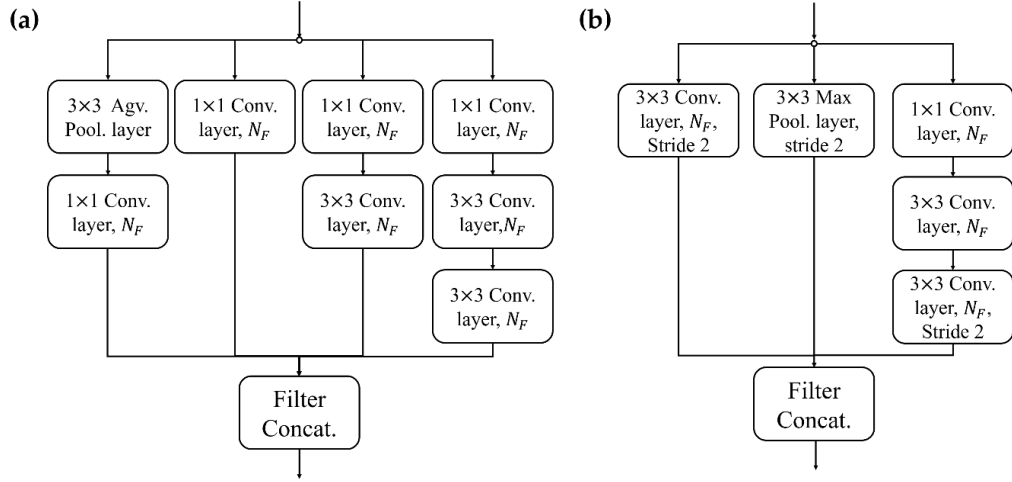


Figure 2.7 Examples of the spectrograms: (a) RT, (b) SS, and (c) FT signals.

Table 2.2 Structure of the base classifier: the DIN classifier.

Type	Filter Size/Stride/Padding	Output Shape (for the SS Input)
Input signal	-	$205 \times 340 \times 1$
Conv_1	$3 \times 3/2/0$	$102 \times 169 \times 32$
Conv_2	$3 \times 3/1/0$	$100 \times 167 \times 32$
Conv_3	$3 \times 3/1/1$	$100 \times 167 \times 32$
Max. pool	$3 \times 3/2/0$	$49 \times 83 \times 32$
2 × inception	Inception-A [$N_F = 32$]	$49 \times 83 \times 128$
1 × reduction	Reduction-A [$N_F = 32$]	$24 \times 41 \times 192$
2 × inception	Inception-A [$N_F = 64$]	$24 \times 41 \times 256$
1 × reduction	Reduction-A [$N_F = 64$]	$20 \times 11 \times 384$
Avg. pool	Adaptive avg. pooling	$1 \times 1 \times 384$
Linear	Logits	$1 \times 1 \times 7$

Finally, we obtained the deep learning classification framework, as in Equation (2.15). From the M training samples in $\mathbf{S} = [\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_M]$ and output samples $\mathbf{Y} = [\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_M]$, the cross-entropy loss, was applied such that loss function can be expressed as follows

$$\text{loss} = -(1/M) \sum_{i=1}^M \log \left(e^{y_i[c_k]} / \sum_{j=1}^C e^{y_i[c_j]} \right) \quad (2.16)$$

where c_k is the true label of sample \mathbf{y}_i with the k th emitter ID, $\mathbf{y}_i[c_j]$ is the j th element of output sample \mathbf{y}_i . Based on the cross-entropy losses, the Adam optimizer [73] is utilized to update the weights of our DIN classifier.

After finishing the training of the DIN classifier, the emitter ID of input sample \mathbf{y}_i can be estimated as follows

$$\begin{aligned} p(c_l; \mathbf{s}_{SF}) &= \text{softmax}(\mathbf{y})_{c_l} \\ &= \frac{e^{\mathbf{y}[c_l]}}{\sum_{j=1}^C e^{\mathbf{y}[c_j]}} \end{aligned} \quad (2.17)$$

$$\begin{aligned} \tilde{k} &= \underset{c_j \in C}{\text{argmax}} \left(p(c_j; \mathbf{s}_{SF}) \right) \\ &= \underset{c_j \in C}{\text{argmax}} \left(\text{softmax}(\mathbf{y})_{c_j} \right) \end{aligned} \quad (2.18)$$

where $p(c_l; \mathbf{s}_{i,SF})$ is the probability that the emitter ID of the input sample is c_l , which can be defined as the softmax output of sample \mathbf{y}_i . In this probability, the estimated emitter ID \tilde{k} is defined as the maximum probability that input samples will be included in a particular emitter ID c_j (see the Equation (2.18)).

2.4.5. Ensemble Approach for Multimodal Signal Fingerprints

The ensemble approach is a well-known method that ensures better generalization performance of classification models [74]. It combines the results of multiple base classifiers trained on the same training dataset and makes a final decision based on these results. Stacking is a combined method that uses the final model to combine the outputs of the base model [74]. It is useful when multimodal features are present in applications such as video signal processing where audio, video, and text segments exist simultaneously [75]. It was reported that multiple SFs, that is, the RT, SS, and FT signals, can be considered as multimodal features for an accurate RF Fingerprinting model [3]. To utilize the multimodality features of the SFs, we adapted the stacking ensemble approach to the DIN

model as presented in Figure 2.8. The SFs \mathbf{s}_{SF} were extracted from hop signal \mathbf{s} in Equation (2.10). These SFs can act as independent features for emitter identification. Thus, each of the SFs, i.e., RT, SS, and FT, is assumed to be independent of the others. For the ensemble approach, the probability that the emitter ID is c_j can be defined as follows

$$p(c_j; \mathbf{s}) = \prod_{SF \in \{RT, SS, FT\}} p(c_j; \mathbf{s}_{SF}) \quad (2.19)$$

According to the DIN classifier trained on the RT, FT, and SS signals presented in Chapter 2.4.4, the final decision was performed by a linear combination of each base classifier (i.e., DIN classifier) such that

$$\begin{aligned} \tilde{k} &= \underset{c_j \in C}{\operatorname{argmax}} p(c_j; \mathbf{s}) \\ &= \underset{c_j \in C}{\operatorname{argmax}} \prod_{SF \in \{RT, SS, FT\}} p(c_j; \mathbf{s}_{SF}) \\ &= \underset{c_j \in C}{\operatorname{argmax}} \prod_{SF \in \{RT, SS, FT\}} \operatorname{softmax}(\mathbf{y}_{SF})_{c_j} \end{aligned} \quad (2.20)$$

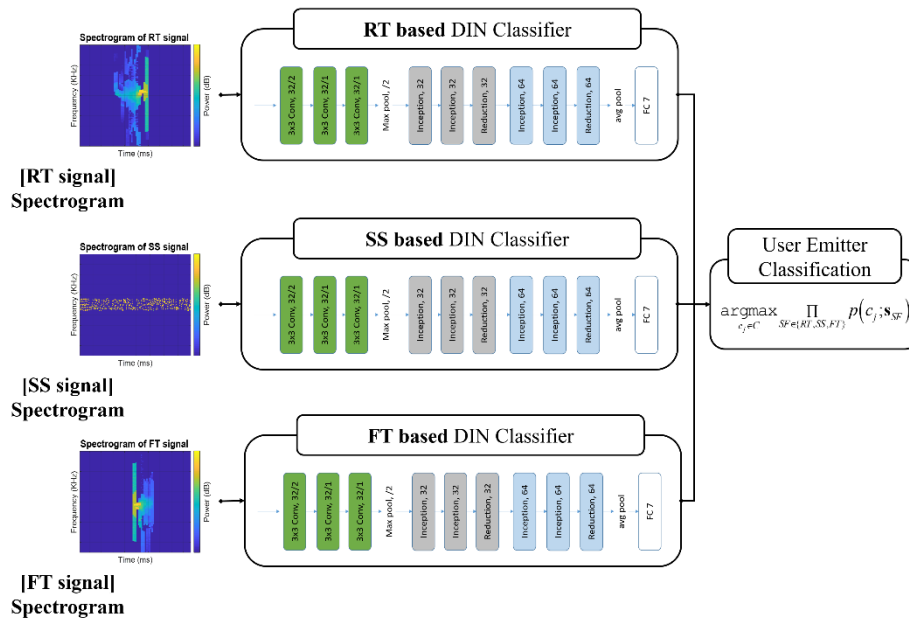


Figure 2.8 Stacking ensemble approach for the multimodal SF signals.

2.4.6. Attacker Emitter Detection

The last step of the RFEI method is an outlier detection step implemented to detect the imitated FH signal. An outlier is a sample included in specific emitter IDs that is not considered during training. In this study, the imitated FH signal was the outlier. This step is aimed at detecting the differences in the classifier output characteristics between the outputs of the classifier when the trained and outlier samples are input. This objective can be achieved by comparing the classifier outputs [76–78], exposing the outliers during the training step to magnify the differences between the trained and outlier samples [79,80], and analyzing the likelihood of the inputs from a generative adversarial network [81,82].

The proposed outlier detection scheme is presented in Figure 2.9. We considered the outlier detection framework proposed in [77]. Temperature scaling [83] and the opposite application of an adversarial attack [84] have been reported to be effective in detecting outlier samples. After preprocessing the input sample, outliers can be detected when the maximum probability of the output vector is lower than the threshold. The key idea of this approach is that the output vector of the outlier represents a much smaller value than the output vector of the trained sample.

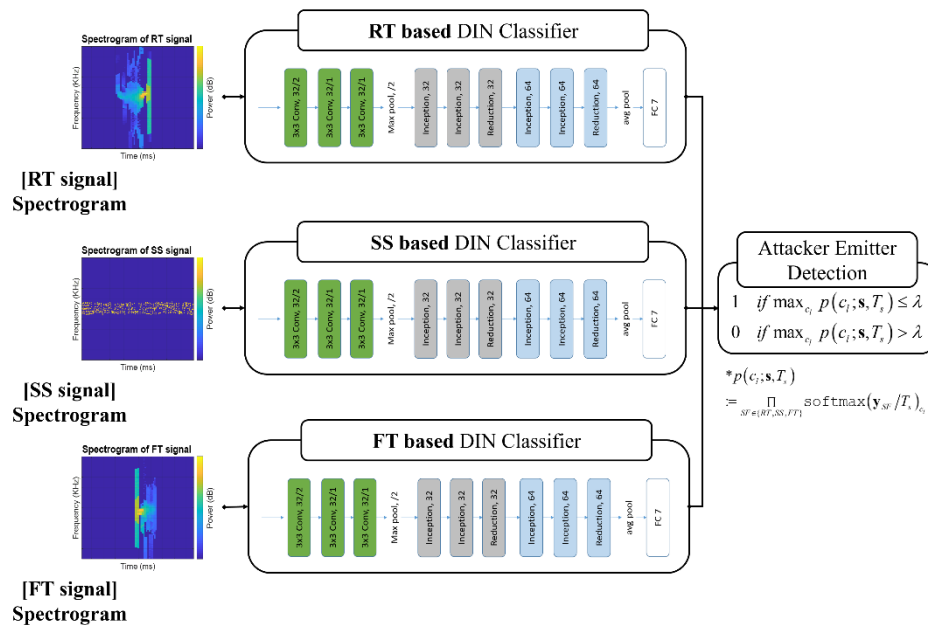


Figure 2.9 Attacker detection scheme based on stacking ensemble approach.

Utilizing this approach, we constructed the outlier detector to alert the signal input when the imitated FH signal was input by performing two steps: (1) calibration of the output vector of the classifier by a temporal scaling factor, T_s , and (2) comparison of the maximum probability of the output vector to the outlier detection threshold, λ . In this study, opposite application of the adversarial attack was not performed because a small perturbation of the input sample may affect the SFs, defined as subtle differences in the FH signal.

Mathematically, the temporal scaling process was applied to Equation (2.17) such that

$$\begin{aligned} p(c_l; \mathbf{s}_{SF}, T_s) &= \text{softmax}(\mathbf{y}/T_s) \\ &= \frac{\exp(\mathbf{y}[c_l]/T_s)}{\sum_{j=1}^C \exp(\mathbf{y}[c_j]/T_s)} \end{aligned} \quad (2.21)$$

In the case of the ensemble approach, the probability in Equation (2.19) was modified as the temporal scaled version as follows

$$\begin{aligned} p(c_l; \mathbf{s}, T_s) &= \prod_{SF \in \{RT, SS, FT\}} p(c_l; \mathbf{s}_{SF}, T_s) \\ &= \prod_{SF \in \{RT, SS, FT\}} \text{softmax}(\mathbf{y}_{SF}/T_s)_{c_l} \end{aligned} \quad (2.22)$$

Based on the scaled output probability, the detection rule for the outlier sample can be defined as follows

$$p(c_{out}; \mathbf{s}, T_s, \lambda) := \begin{cases} 1 & \text{if } \max_{c_l} p(c_l; \mathbf{s}, T_s) \leq \lambda \\ 0 & \text{if } \max_{c_l} p(c_l; \mathbf{s}, T_s) > \lambda \end{cases} \quad (2.23)$$

where $p(c_{out}; \mathbf{s}, T_s, \lambda)$ is the probability that the current input sample is an outlier. This detection rule is a binary classifier with trained class c_{train} and outlier class c_{out} . Thus, parameters T_s and λ were optimized experimentally based on the minimum false positive rate (i.e., the part of the actual outliers that were misdetected as trained samples, FPR) when

the true positive rate (i.e., the part of the actual trained samples that were detected as trained samples, TPR) was higher than 95%.

The final version of the algorithm used for our proposed RFEI process is presented in Table 2.3 (i.e., Algorithm 2).

Table 2.3 Proposed RFEI algorithm.

Algorithm 2. Proposed RFEI algorithm.

Input: The target baseband hop signal $s_h^k(t)$

Initialize: $i = 1$, $T^{RT} = T^{FT} = \{ \}$ for time periods, W_E and bandwidth of interest (BOI) BW_{BOI} .

Step 1: (Extract the target SF)

while do:

Detect the transient signal with Equation (2.10).

Extract the target SF s_{SF} with Equation (2.11).

Set $i \leftarrow i + 0.5 \times W_E$

Step 2: (Calculate the spectrogram)

Calculate the spectrogram $s_{Feature}$ of the SF with Equation (2.13) with respect to the BOI, BW_{BOI} .

Step 3: (Perform emitter classification) $i + W_{Ext.} < length(\mathbf{s})$

Estimate the emitter IDs from the decision rule using either the base classifier (2.18) or ensemble approaches in Equation (2.20).

Step 4: (Perform outlier detection)

Scale the output vector for temporal scaling factor T_s with Equation (2.22) and detect the outliers with Equation (2.23)

Output: Return the authenticated baseband hop signals $s_h^k(t)$

2.5. Baseline Algorithms for RF Fingerprinting Method

In this study, for performance comparison, three other baseline methods were carefully designed and implemented based on algorithms from the literature [14, 21, 33, 38].

Before describing the details, we note that the signal preprocessing steps, such as preamble extraction [33] and signal difference calculation after signal decoding [21], are not covered in this study. The goal of this study was to identify the emitter ID in the physical

layer of the FHSS network. Therefore, we focused on analog SFs that can be obtained from the physical layer of the system. To this end, all baseline SFs were set to RT, SS, and FT, and the feature extraction and classification processes were designed to reflect the approaches in the literature.

Baseline 1: Statistical Moments based RF Fingerprinting The first baseline aims to reflect the conventional RF Fingerprinting approaches based on handcrafted features. It was designed for statistical moments of the SFs, similar to that in [14, 33].

The SF extraction process was the same as that of the proposed method described in Section 3.1.

For feature extraction, the SFs were segmented using N_{seg} . Because the RT and FT signals were too short to be segmented, segmentation was applied only to the SS signal.

$$\mathbf{s}_{SF} = \left[\mathbf{s}_{SF|1}, \mathbf{s}_{SF|2}, \dots, \mathbf{s}_{SF|N_{seg}} \right] \quad (2.24)$$

where $\mathbf{s}_{SF|n}$ is the n th segment of SF. For each segmented SF, a total of six sub-features were considered. The instantaneous amplitude, phase, and frequency, described in [33], were calculated as sub-features, and the time, frequency, and time–frequency axes of the spectrogram, identified as good features in [14], were applied as sub-features. Subsequently, the statistical moments (i.e., mean m , variance σ^2 , skewness γ , and kurtosis κ) and entropy H were calculated for each sub-feature. Thus, a total of 30 features were calculated and arranged in a vector form such that

$$\mathbf{s}_{Feature|\mathbf{s}_{SF|n}} = \left[(m, \sigma^2, \gamma, \kappa, H)_1, (m, \sigma^2, \gamma, \kappa, H)_2, \dots, (m, \sigma^2, \gamma, \kappa, H)_6 \right] \quad (2.25)$$

where $\mathbf{s}_{Feature|\mathbf{s}_{SF|n}} \in \mathbb{R}^{1 \times 30}$ is the vector form of the handcrafted features calculated from the n th segments of the SF. Finally, the composite handcrafted feature $\mathbf{s}_{Feature} \in \mathbb{R}^{N_{SF}^{stats} \times 1}$ can be defined as follows

$$\mathbf{s}_{Feature} = [\mathbf{s}_{Feature|s_{SF1}}, \mathbf{s}_{Feature|s_{SF2}}, \dots, \mathbf{s}_{Feature|s_{SF|N_{seg}}}] \quad (2.26)$$

where N_{SF}^{stats} was the size of the statistic moments vector.

For classification, a linear SVM from [14] was applied. Random forest or multi-class AdaBoost from [33] and linear discriminant analysis from [14] were also investigated. We compared these algorithms when applied to our FH signal dataset, and the linear SVM showed the best classification results.

Baseline 2: Raw Signal-based RF Fingerprinting The second baseline aims to reflect the recent methods of RF Fingerprinting based on raw signal processing. It was designed to train raw SF signals directly in the ensemble approaches of the deep learning classifiers described in [21].

As described at the beginning of Chapter 2.5, the SF extraction process was the same as that of the proposed method described in Chapter 2.4.1.

For feature extraction, the SFs were segmented using N_{seg} in Equation (2.24). The core idea of this approach was to train the raw signals in the ensemble classifiers, and the RT and FT were also segmented in this case. The feature vectors of each segment were set to a two-channel I/Q vector $\mathbf{s}_{Feature|s_{SF|n}} \in \mathbb{R}^{N_{SF}^{raw} \times 2}$ such that

$$\mathbf{s}_{Feature|s_{SF|n}} = \begin{bmatrix} \text{Re}(\mathbf{s}_{SF|n}) \\ \text{Im}(\mathbf{s}_{SF|n}) \end{bmatrix} \quad (2.27)$$

where N_{SF}^{raw} is the size of each segment $\mathbf{s}_{SF|n}$.

For the ensemble classification approach, the base classifier was set to a one-dimensional CNN as an identification network for outdoor data in [14]. After training each base classifier using segmented feature $\mathbf{s}_{Feature|s_{SF|n}}$, classification was performed using an ensemble approach, as in [21]

$$\tilde{k} = \underset{c_j \in C}{\operatorname{argmax}} \prod_{n \in N_{\text{seg}}} p\left(c_j; \mathbf{s}_{\text{Feature}|\mathbf{s}_{\text{SF}|n}}\right) \quad (2.28)$$

Baseline 3: Spectrogram-based RF Fingerprinting The third baseline aims to reflect the recent approach in [38], which is based on the SF spectrogram. As described in [38], the author trained the Hilbert spectrum of the received hop signal in a residual unit-based deep learning classifier. To reflect this approach in baseline 3, the algorithm was designed to train an SF spectrogram directly in the residual-based deep learning classifier.

The SF extraction and feature extraction processes were the same as those of the proposed method described in Chapter 2.4.1 and 2.4.2.

For classification, the classifier structure was set to the residual-based deep learning classifier described in [38]. After training the classifier, classification was performed using Equation (2.18).

2.6. Experimental Setups

This section describes the experimental investigation of the emitter identification performance of the proposed RF Fingerprinting method. Before discussing the results, several experimental setups are discussed.

We collected FH signals from a real experiment to determine the reliability of the algorithm. Seven FHSS devices were used to experiment. Each device utilized the same hopping rate for secure voice communication. The FH signal was frequency-modulated, and the carrier frequency was set to hops in the very high frequency range. The exact hopping rate and frequency range will not be disclosed owing to security issues. The FHSS device was connected under laboratory environmental conditions. The FH signal was acquired at a 400 MHz sampling rate and stored as raw FH data in the DA system.

Target hop extraction and down-conversion were performed on the stored raw training FH data. Because we assumed the predefined hopping pattern to be known, an energy

detection approach was applied to the exact hopping frequency f_h^k and the target hop samples \mathbf{x}_h^k were extracted from the observed RF signal \mathbf{y} . Subsequently, the hop sample was down-converted to the baseband using a decimation factor of 20, i.e., 20M sample rate baseband hop signals \mathbf{s}_h^k were acquired. These were stored as baseband FH training data in the DA system. This down-conversion approach is reasonable because the FH signals were also demodulated to the IF or baseband to decode the digital data modulated by the message signal $m^k(t)$ as in Equation (2.2). As the SFs depend on the component characteristics of the emitter, the SFs also should exist in the baseband hop signal, \mathbf{s}_h^k .

Another set of FH signals was acquired to prepare an outlier dataset. Two more FHSS devices were recruited, and the FH signals were acquired on different dates compared with those of the training dataset. The emitter specifications were the same as those of the training emitter. However, in this experiment, the FH signal was down-converted to baseband and stored as outlier FH data with a sampling rate of 2.34 MHz. For fair comparison, the sampling rate of the signal was resampled using the Fourier-domain based sampling rate conversion method, which can improve the accuracy and computational cost compared to the time domain-based method [85]. These outlier data were considered only in the outlier detection experiment described in Chapter 2.7.4.

Table 2.4 Details of the FH dataset.

Dataset	Emitters	Emitter Type	Number of Acquisitions	Number of Samples
Training dataset	Emitter 1	Model 1	5 times	170
	Emitter 2	Model 1		168
	Emitter 3	Model 1		170
	Emitter 4	Model 1		171
	Emitter 5	Model 2		160
	Emitter 6	Model 2		169
	Emitter 7	Model 2		168
Outlier dataset	Emitter 8	Model 3	10 times	308
	Emitter 9	Model 3		312
Total emitters		9	Total samples	1796

An average of 168 hop FH signals were obtained for each training emitter, and an average of 310 hop FH signals were obtained for each outlier emitter; a total of 1796 samples from nine emitters were obtained. The details are presented in Table 2.4.

The results were obtained using the experimental setup as follows. For the training and testing datasets, the FH dataset was partitioned according to a 7:3 ratio; a total of 823 samples were trained, and a total of 353 samples were tested from seven emitters. In the outlier detection experiment, the test dataset for training emitters and the outlier dataset for outlier emitters were considered; a total of 353 samples from seven training emitters were tested, and a total of 620 outlier samples from two outlier emitters were tested. All the results were tested 10 times, and the average performance was presented. The experiments were conducted with an Intel i7-6850K CPU unit and an NVIDIA Titan RTX GPU unit. The dataset generation task in Figure 9 was performed using MATLAB 2018a, and all RF Fingerprinting algorithms were implemented in Python 3.6 with PyTorch 1.6.0. The implemented parameters of the RF Fingerprinting algorithms performed at our experiments are described in Table 2.5.

Table 2.5 Implemented parameter settings.

Algorithm	Parameters	Values
Proposed algorithm	Number of FH signals, K	7
	Number of emitters trained on the classifier, C	7
	Length of the FH signal, N	194,475
	Length of the SFs, N_{SF}	38,895 for RT and FT 175,027 for SS
	Extraction window size, W_E	1945
	Energy variance detection threshold, δ	0.1
	Length of the frequency axis in the spectrogram, N_{SF}^f N_{SF}^{stats}	205 for all SFs
	Length of the time axis in the spectrogram, N_{SF}^t	74 for RT and FT 340 for SS
	STFT window size, W_{STFT}	1024
	Number of segmented SFs, N_{seg}	10
Baseline 1 algorithm	Length of the handcrafted feature vector, N_{SF}^{stats}	30 for RT and FT 300 for SS
Baseline 2 algorithm	Length of the raw vector segmented by the FH signal,	3889 for RT and FT 17,502 for SS

2.7. Results and Discussions

2.7.1. Emitter Identification Accuracy

We firstly investigated the emitter identification performance of the proposed RFEI algorithm and the baselines. All algorithms were applied to all SFs, and the mean and standard deviation of the experimental values were investigated. The results are listed in Table 2.6.

Table 2.6 Emitter identification accuracy.

	RT	SS	FT
	Mean Accuracy (%) \pm Standard Deviation		
Statistical moments *	61.8 \pm 0.0	92.6 \pm 0.0	66.4 \pm 0.0
Raw signal **	17.7 \pm 1.3	89.5 \pm 0.7	20.4 \pm 2.1
Spectrogram-residual ***	83.7 \pm 2.1	93.7 \pm 1.2	93.9 \pm 1.2
Spectrogram-DIN †	84.6 \pm 1.5	95.3 \pm 1.2	92.8 \pm 1.1
Ensembles †		97.0 \pm 0.6	

*: (Baseline 1) statistical moments approach in [14,33]. **: (Baseline 2) raw signal approach in [21]. ***: (Baseline 3) spectrogram and residual block-based approach in [38]. †: (Proposed) spectrogram, DIN classifier, and ensemble-based approach in the proposed method.

Table 2.6 demonstrates the efficiency of the proposed RFEI algorithm showing that the proposed algorithm for identifying the emitter ID based on the SS spectrogram and DIN base classifier performs with an accuracy of 95.3%, which is better than other baseline algorithms. In addition, the ensemble approach of RT, FT, and SS based on the proposed algorithm yielded an accuracy of 97.0%, demonstrating its efficiency with a higher identification accuracy than other baseline algorithms.

In terms of the SF efficiency, the results show that the SS signal is the most effective SF, as it is more accurate than the RT and FT signal-based results. In addition, in terms of the efficiencies of the feature extraction and classification approaches, the spectrogram feature is effective for representing the differences in the SF for each emitter. The most effective means of identifying the emitter ID in the FH signals is to ensemble the multimodal SFs, i.e., the RT, FT, and SS, trained by a DIN.

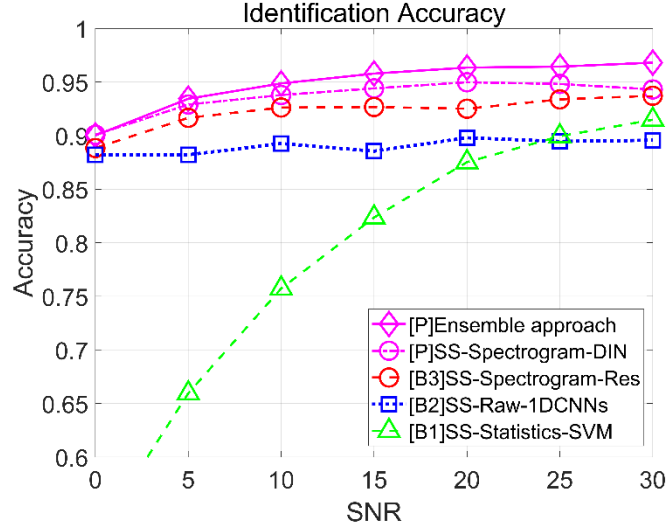


Figure 2.10 Emitter identification accuracy at different signal-to-noise ratios (SNRs).

The emitter identification performance at SNRs is shown in Figure 2.10. The AWGN signal $n(t)$ can be artificially added to the received hop signal \mathbf{s} as follows

$$SNR = 10 \log_{10} \left(\frac{\|\mathbf{s}\|_2^2}{N\sigma_n^2} \right) \quad (2.29)$$

where N and σ_n^2 are the length and variance of the noise signal $n(t)$, respectively.

We found that the classification accuracy obtained by applying the proposed method to the SS signal was nearly 3% above baselines 1 and 2 and at least 1% above baseline 3 over the entire range of SNRs. In addition, the ensemble approach of the proposed algorithm can improve the accuracy by more than 1% compared to the proposed method. In particular, applying the proposed method to the SS signal at 20 dB SNR, which is the typical operating SNR of the FHSS network [86], yielded an accuracy of more than 95.0%. For the ensemble approach, the identification accuracy was measured to be greater than 96.4%, making it the most effective algorithm. These accuracies are higher than those of baseline 1 (87.5%), baseline 2 (89.8%), and baseline 3 (92.5%).

The validity of the proposed algorithm was verified again. At low SNR, the accuracy of baseline 1 decreases dramatically, whereas the other algorithms maintain their accuracies. Baseline 2, Baseline 3, and the proposed method work well when applied to the SS signal, even at low SNRs. However, the proposed method outperforms the baselines, and the ensemble approaches outperform the other algorithms at all SNRs. These findings imply that a deep learning-based classifier at baselines 2 and 3 can learn the differences in the SFs for RF Fingerprinting, but our proposed algorithm (i.e., using the spectrogram and DIN classifier) with the ensemble approach is more effective than the baselines.

The confusion matrix of the ensemble approach based on the proposed method is presented in Table 2.7. The confusion matrix is a specific metric for a classifier that can represent the relationship of each emitter. This matrix can be obtained by simply counting the results of the test samples with their true label information. The rows of the matrix indicate the true emitter IDs, and the columns indicate the predicted emitter IDs. The diagonal terms in the confusion matrix represent the correct classification result cases, and the offdiagonal terms represent the incorrect classification result cases. Thus, Table 2.7 shows that our ensemble approach based on the proposed method can identify the FH emitters with more than 94.6% accuracy without confusion between emitters.

Table 2.7 Averaged confusion matrix of the ensemble approach based proposed method.

		Predicted Emitter (%)						
		1	2	3	4	5	6	7
Actual Emitter (%)	1	100.0	0	0	0	0	0	0
	2	0.2	98.6	0	0.2	0.4	0	0.6
	3	0	0	98.0	0.2	0	1.8	0
	4	0	1.6	0.6	95.5	0.6	0.4	1.4
	5	0	0.2	1.9	0.4	96.0	1.0	0.4
	6	0	0	2.6	0	1.0	95.8	0.6
	7	0.6	1.0	0.4	2.8	0.6	0	94.6

2.7.2. Efficiency of the Inception Blocks

We constructed the DIN classifier based on the inception blocks. To confirm the efficiency of the inception blocks, the identification accuracy of the proposed method was compared with that of baseline 3. The difference between the proposed method and baseline 3 lies in the classifier. As in baseline 3, the classifier was set to the residual-based classifier

described in [38]. Two experiments were performed for comparison. One was conducted to identify the emitter ID from the received hop signal s without the SF extraction, and the other was performed to identify the emitter ID from the ensemble approach of the SFs. The results are presented in Table 2.8 and Figure 2.11.

Table 2.8 Identification accuracies of the residual and inception blocks.

	Hop Signal without SF Extraction	Ensemble Approach with SF Extraction
	Mean Accuracy (%) \pm Standard Deviation	Standard Deviation
Spectrogram—Residual ***	94.4 \pm 1.1	96.4 \pm 0.7
Spectrogram—DIN \dagger	95.1 \pm 1.0	97.0 \pm 0.6

***: (Baseline 3) spectrogram approaches in [38]. \dagger : (Proposed) spectrogram approach of SF.

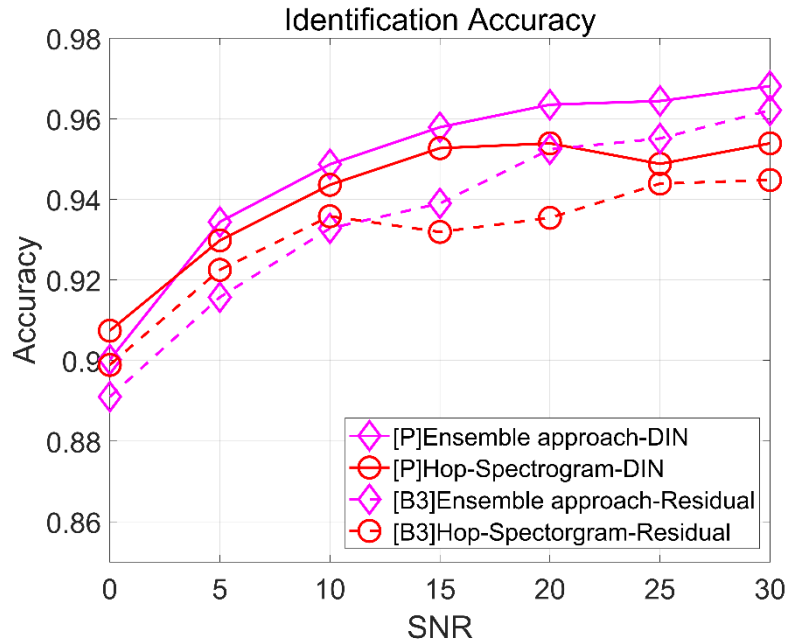


Figure 2.11 Identification accuracies of the residual and inception blocks at different SNRs.

Table 2.8 presents the identification accuracies of the proposed algorithm and baseline 3. The identification accuracy results at different SNRs are presented in Figure 2.11. Both sets of results demonstrate the efficiency of the inception blocks. Table 2.8 reveals that the DIN-based approach can produce higher accuracies than the residual-based approach. This result is also shown in Figure 2.11. As the SNR changes, the accuracy of the DIN-based approach is superior to that of the residual block-based approach, except when the ensemble approach of the residual-based method overcomes the hop and DIN-based method in

environments with SNRs of 20 dB or more. However, if we focused on the classifier structure, i.e., compared the performance between hops approaches or ensemble approaches, the performance of the residual network could not overcome the performance of the inception blocks. As described in Chapter 2.4.4, this result may stem from the fact that filtering features with different receptive field sizes can help train SFs within deep learning architectures.

2.7.3. Class Activation Map (CAM) Analysis of the DIN Classifier

We investigated the feature map of the DIN classifier to understand why the DIN-based model works well. To this end, we applied a gradient-weighted CAM (GCAM) to visualize the feature map. The GCAM is a well-known feature visualization that identifies parts of the input signal that positively influence the class decision [87]. This can be achieved by backpropagating the gradient of the inference to the input layer and highlighting the input parts using positive gradient values.

The GCAM is a feature visualization method that identifies parts of the input signal that positively influence the class decision [87]. It can be obtained by performing the following steps. (1) Firstly, the gradient of the inference score from the target class c_j , that is, the j th element of the model output \mathbf{y} , is back-propagated to the last convolutional layer of the model, which is the last reduction-A block of the DIN. (2) Secondly, global average pooling of the back-propagated values on the grid axis, that is, the time and frequency axes of the feature map, is performed. This value serves as a weight to infer the importance of the current filter result. (3) With the linear combination of the entire filter map, the Grad-CAM for the input sample \mathbf{s} and decision class c_j is obtained. Specifically, it follows

$$a_f^{c_j} = \frac{1}{P} \sum_z \sum_k \frac{\partial \mathbf{y}[c_j]}{\partial A_{zk}^f} \quad (2.30)$$

$$GCAM(\mathbf{s}, c_j) = \text{ReLu} \left(\sum_f a_f^{c_j} A^f \right) \quad (2.31)$$

where A_{zk}^f is the grid point (z, k) of the f th filter map existing on the last convolutional layer of the classifier model, P is the size of the f th filter map, and A^f and $a_f^{c_j}$ are the neuron importance weights of the f th filter map when the target class c_j is decided.

Finally, the GCAM is averaged for the positive samples that record the correct identification results. The positive sample dataset $\mathbf{S}_{True} = [\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_{M_{True}}]$ is collected when the classification result of the input sample \mathbf{s}_j in Equation (2.15) is true. For the positive sample \mathbf{s}_j and its true decision class c_j , the GCAM can be averaged as follows

$$AGCAM(c_j) = \frac{1}{M_{True}} \sum_{\mathbf{x}_i \in \mathbf{S}_{True}} GCAM(\mathbf{s}_i, c_j) \quad (2.32)$$

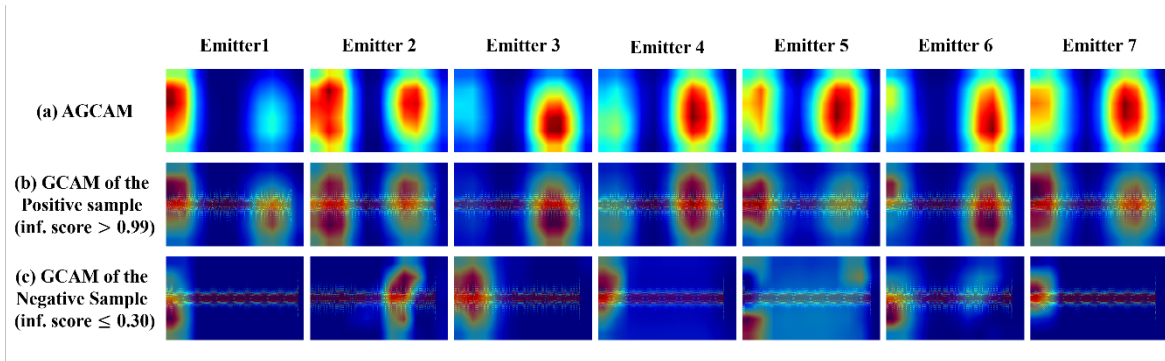


Figure 2.12 Examples of GCAM of the DIN classifier: (a) AGCAM for target emitters, (b) positive sample with an inference score greater than 0.99, and (c) negative sample with an inference score less than 0.30.

The average GCAM (AGCAM) results are presented in Figure 2.12. Interestingly, for each emitter classification, we found that the activated region of the AGCAM is the location at which the head and tail of the signal are located. The GCAM of the positive sample with an inference score of 0.99 or higher is shown in Figure 2.12.(b). These results show that when the classifier model correctly identifies the emitter ID, the filter maps of the model are activated similarly to the AGCAM of the target emitter. In other words, the intensity of the activated region differs from that of the AGCAM, but the shape and location of the activated region are similar to those in the AGCAM results. Conversely, the GCAM of the negative

sample with an inference score of 0.30 or less is shown in Figure 2.12.(c). The results demonstrate that when the model misidentifies the emitter ID, the activated region of the filter maps is completely different from those of the target emitter and other emitters.

To verify the meaning of the activated region in Figure 2.12, the physical layer convergence protocol (PLCP) frame format for the FHSS network as defined in the 802.11 standard [57] is presented in Figure 2.13. It can be verified that the preamble field is located at the head part of the frame, and the frame body is located at the tail part of the frame.

The preamble is a sequential signal for synchronization between the transmitter and receiver. Therefore, duplicated sync sequences must be transmitted repeatedly. When the data sequence contained in the frame is identical for each emitter, only the differences in SFs remain, which is helpful in RF Fingerprinting. Consequently, many researchers have applied additional preprocessing steps to extract preamble signals [3, 33]. However, the proposed method based on the DIN classifier can automatically learn the preamble field without additional preprocessing steps.

In the cases of the frame body, the GCAM is activated in this region because the FH signal dataset is collected in a laboratory environment; hence, the data sequences contained in the frame body are similar to each other. This similarity of the data sequences can help identify the differences in the SFs of the emitters. Again, the proposed method can automatically learn the fields in which the emitter IDs can be identified.

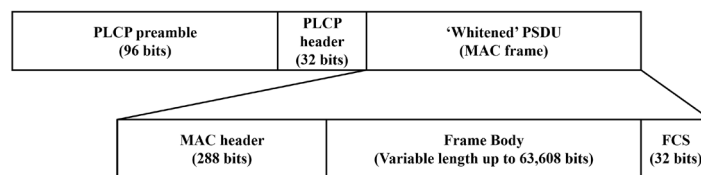


Figure 2.13 PLCP frame format for FHSS networks in the 802.11 standard [57].

2.7.4. Outlier Detection Performance

We evaluated the outlier detection performance of the proposed algorithm and baseline 3. The experimental dataset was prepared using the test dataset for trained emitters and the

outlier dataset for outlier emitters. Before executing the experiment, the detector-related parameters, that is, the temporal scaling factor T_s and detection threshold λ , were optimized. For $T_s \in [1, 2, 3, 4, 5, 10, 15, 20]$ and $0 \leq \lambda \leq 0.3$, the parameters were set to $T_s = 2$ and $\lambda = 0.07$ for the proposed algorithm and $T_s = 1$ and $\lambda = 0.05$ for proposed baseline 3. These values were selected by finding the minimum FPR when the TRP was higher than 95%.

As discussed in Chapter 2.4.6, the key idea of the outlier detector is based on the fact that the maximum probability of the output vectors from the outlier samples has a smaller value than the maximum probability of the output vectors from the trained samples. To verify this idea, we plotted a histogram in Figure 2.14 showing the maximum probabilities of the output vectors obtained from the proposed method, i.e., the output vectors of the ensemble approach in the DIN. Evidently, the maximum probability values of the outlier samples occur at positions < 0.1 . Conversely, the values of trained samples mostly exist at position ≥ 0.2 . These results demonstrate that the differences between the characteristics of the outliers and trained samples are easily identified and can be utilized to detect the outlier samples.

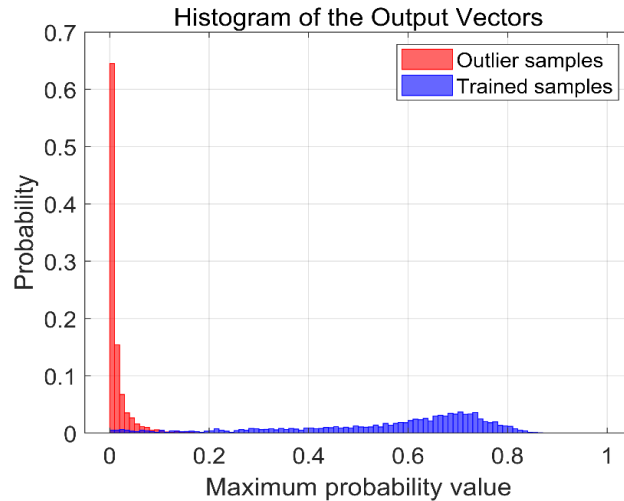


Figure 2.14 Histogram of the output vectors.

We present the confusion matrices of the outlier detectors based on the proposed method and baseline 3 in Tables 2.9 and 2.10. As we optimized our parameters based on the FPR values when the TPR was higher than 95.0%, both TPRs yielded similar rates in the

detection of the actual trained samples. However, in the case of the true negative ratio, which represents the actual outlier sample detection ability, the proposed method can achieve a rate of 95.6%, which is 6.6% higher than that of baseline 3 (89.0%). In other words, the proposed method can reduce the FPR from 11.0% to 4.4%. These results indicate that the DIN classifier-based approach is useful for training SF features in FH signals and can effectively detect outlier samples by using these trained features.

Table 2.9 Averaged confusion matrix of the outlier detectors based on the proposed method.

		Predicted Emitter (%)	
		Learned Classes	Outlier Classes
Actual emitter (%)	Learned classes	96.6	3.4
	Outlier classes	4.4	95.6

Table 2.10 Averaged confusion matrix of the outlier detectors based on baseline 3.

		Predicted Emitter (%)	
		Learned Classes	Outlier Classes
Actual emitter (%)	Learned classes	96.8	3.2
	Outlier classes	11.0	89.0

Figure 2.15 plots the ROC curve and compares the AUROCs. All values were averaged over 10 experiments. The ROC metric describes the relationship between the probability of detection (i.e., TPR) and the probability of a false alarm (i.e., FPR). This result can be achieved by plotting the FPR together with the TPR at different detector thresholds λ . Additionally, this ROC metric is known as the cost–benefit relationship in decision theory. Thus, when a high benefit is obtained at a low cost, i.e., when the probability of false alarms is low, high detection rates should be obtained. In other words, if the curve moves toward the upper left with a high AUROC, the model possesses strong detection ability. The results confirm that the proposed method can clearly improve the ROC curve compared with baseline 3. The AUROC also improves from 0.97 to 0.99. These results provide clear evidence that the proposed DIN-based ensemble method is more effective than the residual block-based method.

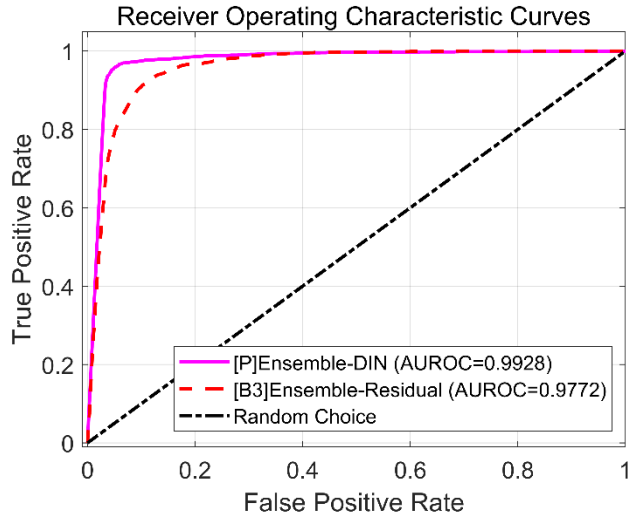


Figure 2.15 Receiver operating characteristic (ROC) curves.

2.7.5. Discussion

PUF, Uniqueness, and Repeatability of the FH signals: FH signals satisfy the characteristics of Physical Unclonable Function (PUF), uniqueness, and repeatability. Since the RF emitter components in FH signals are identical, the theoretical basis for the existence of SFs is clear, which has been heuristically proven in this paper. SFs have been reported to be duplicated using learning-based methods in GAN-based software techniques [37]. However, there has been no report of successfully replicating the duplicated RF signal in a real-world scenario using hardware components. The theoretical basis for this is that in the hardware reproduction of RF signals, another SF can emerge, making differentiation possible. For instance, studies on RF Fingerprinting have shown that individual distinctions can be made in USRP-based software-defined radio (SDR) devices [39]. Therefore, while FH signals themselves can be repeatable [59, 118-120], the SFs within FH signals are non-repeatable, satisfy uniqueness, and thus meet the characteristics of PUF.

Noise Susceptibility of the FH signals: We assume the simplest AWGN channel model. This is the channel model commonly addressed in most RF Fingerprinting papers, with other channel models such as multi-hop relaying-based Rayleigh channel environments also being discussed [38]. This approach is taken because RF Fingerprinting technology is still in its early research stages, and due to the noise susceptibility of SFs, the research has been conducted in a way that minimizes the impact of the channel. In other words, it is argued

that RF Fingerprinting can be sufficiently utilized even after applying existing receiver techniques that compensate for channel noise and then analyzing the SFs. While this logic is plausible, it remains unproven, indicating that further research is needed to address noise susceptibility. Future research should consider issues such as multi-path channels and DSP key-based channel coding.

Product based ensemble decision rule: We applied a product-based decision rule to individual DIN classifiers. This heuristic approach involved applying various methods such as addition, product, log product, and argmax product, and selecting the method that showed the best performance. This approach treats the results of each DIN for individual SFs as independent entities, assuming a linear relationship. However, in reality, since the SFs are output from the same RF emitter, it is difficult to determine that such an assumption leads to an optimal ensemble decision. Therefore, further research is needed to find the optimal ensemble decision rule, such as weight-based approaches [121] and additional ensemble layer-based methods [122].

2.8. Summary

In this study, an RFEI method that targets the physical layers of FHSS networks was proposed with the objective of directly identifying emitter IDs from received FH signals. An analog SF extraction process, SF spectrogram features, a DIN-based classifier for emitter classification, and an outlier detector algorithm for attacker detection were proposed and applied to the target hop signals. In addition, the ensemble approach that utilized multimodality SFs was evaluated for robust classification. The results showed that the SF spectrogram extracted from the received FH signal can be effectively analyzed using the DIN-based classifier, and the classification accuracy was improved by at least 1.00% compared with those of other baselines. In addition, the multimodal SF ensemble approach, that is, the use of RT, FT, and SS, achieved the best results with a classification accuracy of 97.0% for the seven real FHSS emitters. In addition, the inception block-based approach was more effective than the residual block-based approach owing to its filtering ability at different receptive field sizes. From the analysis of the GCAM for each FH emitter, we found

that the classifier model can train the region wherein the differences in the SFs can be maximized. In addition, the outlier detection performance of the proposed method was evaluated. We found that the output characteristics of the outliers differed from those of the training samples, and this property can be used by the detector to identify attacker signals with an AUROC of 0.99.

These results support that the proposed RFEI method can identify emitter IDs of the FH signals emitted by authenticated users and can detect the existence of the FH signals emitted by attackers. Because the SFs cannot be reproduced, it is possible to configure non-replicable authentication systems in the physical layer of the FHSS network. This study focused on evaluating the RFEI method, one of the components of the overall authentication system. Our future study will consider system improvement by utilizing the GCAM to detect misclassification cases.

As another future study, we will consider the property of the outliers in the RFEI system. We believe that further distinctions of the outliers, namely the detection of multi-labeled outliers, may be possible. We expect that this future consideration will help prevent the malicious application of the RFEI system, such as when eavesdroppers utilize the RFEI system. If the eavesdropper can successfully prepare the target FH sample, it can be used as a signal tracking method to decode the actual FH signal transmission. Our future study will consider the ways to prevent this malicious scenario by generating artificial outliers that can imitate authentication users.

Chapter 3. [Cryptography] RF Public Key Generator for Digital Application

The studies in this chapter have been published in IEEE Access [1].

3.1. Motivations

In IoT environments, effective public key management is crucial for managing numerous devices. RF features, primarily considered analog features within physical layer authentication by RF Fingerprinting (RFF) processes, present a novel approach to key management. In this research, we introduce a novel RF-based Public Key Generator (RF-PubKG) model that maps RF features into cryptographic sequences by incorporating a Key Generation (KeyGen) layer into the RFF model. The RF-PubKG demonstrates superior performance, achieving 97.2% accuracy at a 20dB SNR and further improving to 99.6% in noise-free conditions with a Frame Error Rate (FER) below 1%. The generated public key sets exhibit negligible correlation, with intra-key-set correlations not exceeding 0.24 and inter-model correlations falling below 0.04, highlighting the reliability of the RF-PubKG model. The integration with the Rivest–Shamir–Adleman (RSA) algorithm provides proof-of-concept for the RF-PubKG-based digital signature scheme, effectively simplifying the Certificate Authorities (CAs) management and, consequently, reducing Public Key Infrastructure (PKI) complexity. This simplification promises effective public key management within the Public Key Cryptography (PKC), thereby enhancing the efficiency of digital signature verification processes.

3.2. Introduction

In an Internet of Things (IoT) environment, accepting messages from trusted users is

a crucial task. A common method to authorize users is to check the device's address, such as the Media Access Control (MAC) or Internet Protocol (IP) address, encoded as digital bits in message packets. However, if these addresses are transmitted without cryptographic encryption, eavesdroppers can sniff and modify the addresses using software-defined approaches [88].

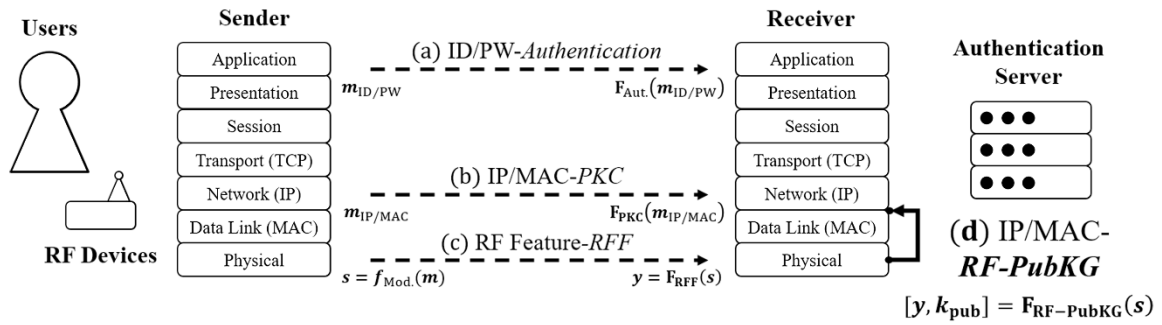


Figure 3.1 An overview of the user authentication scheme in IoT Environments: (a) ID/PW-based authentication; (b) authentication based on IP and MAC addresses utilizing PKC; (c) authentication using RF features based on RFF; and (d) (RF-PubKG) the proposed method for authentication using IP and MAC addresses combined with RF features through PKC.

One of the efficient solutions to solve this problem is to insert a valid authentication code in message packets. An overview of the user authentication scheme in IoT environments is presented in Fig. 3.1. In recent decades, several network security protocols, such as IEEE 802.1X [89], MACsec [90], or IPsec [91], have been proposed to secure network channels. These methods encrypt and decrypt user datagrams using cryptographic algorithms, making it impossible for eavesdroppers to sniff the user address without access to the public and private key details.

To secure communication between the numerous devices in IoT environments, a reliable key management system is essential. Public Key Cryptography (PKC) can be an effective solution due to its effective public key management structure. In PKC, the sender's datagrams are encrypted using a private key, allowing any receiver to verify both the integrity of the datagrams and the sender's identity. This approach simplifies key management, as each IoT device needs only a single public and private key, whereas a unique key for each pair of devices is required in private key cryptography.

Digital certificates are primarily used to verify the trustworthiness of the public key. These certificates are centrally managed in the Public Key Infrastructure (PKI) for key authentication, certificate issuance, and management [92]. However, establishing a trusted PKI involves significant financial and resource allocations for trusted third parties, which is not feasible for IoT environments. An alternative key management system for ensuring the trustworthiness of the public keys is required.

Radio Frequency Fingerprinting (RFF) can be an alternative approach for verifying the authenticity of IoT devices. The RFF is one of the physical layer authentication approaches that utilizes a unique RF feature present in analog RF signals. The inherent nonlinearity in the RF components of the transmitter, such as the Digital Analog Converter, Frequency Oscillator, or Power Amplifier, arises from manufacturing variations [20]. These effects accumulate and manifest as a distinct feature in the transmitted RF signal, which can serve as a unique authenticated key referred to as the RF feature.

Research on RF features is both extensive and multifaceted. For instance, the time-frequency energy properties of transient signals generated at the beginning of RF transmission have been used to identify twenty Bluetooth devices [21]. Multi-sampled steady state signals, capturing variations in RF transmission of preamble data, have been directly trained into a convolutional neural network for 54 ZigBee devices under line-of-sight conditions [22]. Spectrograms of falling signals observed during the decline of RF transmission have been used to identify seven frequency-hopping transmitters [2]. More recently, multi-faceted RF features have been considered with advanced deep learning approaches. For Wi-Fi devices, IQ, carrier frequency offset, Fourier coefficients, and time-frequency coefficients are incorporated into an attention-based deep learning model [93]. Similarly, magnitude, phase, and power spectral density of steady-state signals of the Bluetooth devices have been considered with an embedding-attention framework [94].

The RF features are renowned for their non-replicable key characteristics, largely attributed to practical challenges [54]. The randomness and uniqueness of these RF features stem from the natural variations introduced during the manufacturing process. Replicating these key features would require tighter control over the varied components at the analog level. However, it is widely recognized that achieving such control is either prohibitively

expensive or virtually impossible in real-world scenarios [95]. Owing to the inherent randomness and uniqueness of the RF features, they can be effectively utilized as non-replicable public keys in user authentication schemes.

Our research goal is to utilize the non-replicable RF features as public keys for the PKC. To achieve this goal, the RF feature must be converted into a finite cryptographic sequence. Recent research on RFF has concentrated on capturing RF features as digitized signals in the real domain [2, 14, 47, 93, 94, 96-98]. These features are segmented directly from the RF signal and transformed into feature domains to enhance the distinction between different RF transmitters. Subsequently, these RF features have mainly been processed using AI models for identification, rather than for cryptographic computations. Conversely, cryptographic schemes based on PKC depend on complex mathematical problems conducted within the finite field domain [99]. Although cryptographic calculation in the real domain is feasible, it requires hardware capabilities that are expensive and unsuitable for IoT environments. Therefore, further research is required to establish a mapping relationship between RF features and cryptographic sequences.

In this paper, we propose a novel RFF process for a Radio Frequency based Public Key Generator (RF-PubKG) to utilize RF features as cryptographic sequences. In the process of RFF model training, we introduce a key generation layer to map the RF features into cryptographic sequences. By considering these cryptographic sequences as users' public keys, we can simplify the PKI structure in the PKC, enhancing the efficiency of the public key management system. The specific contributions of this paper are detailed as follows:

- **(RF-based Cryptographic sequences)** We propose the RF-PubKG for mapping RF features to cryptographic sequences. This unique mapping of the RF feature to a cryptographic sequence enables integrated authentication with RFF and PKC. This aspect of the research paves the way for addressing cryptographic problems based on RF features.
- **(RF-based Digital Signature)** As proof of concept, we evaluate the RF-PubKG-based digital signature scheme along with the hashed RSA algorithm. This result demonstrates the simplification of the PKI structure by relying on

the trustworthiness of the public key, which is inferred from non-replicable RF features.

The structure of this paper is as follows: Chapter 3.3 describes the background knowledge related to RFF and the digital signature scheme for PKC. Chapter 3.4 presents the proposed RF-PubKG scheme and the conceptual structure for the RF-PubKG-based digital signature scheme implemented by RSA algorithm. Chapter 3.5 details the dataset and experimental setup, while Chapter 3.6 presents the results and discussions. Chapter 3.7 concludes the paper by summarizing the findings of this research.

3.3. Background Knowledge

3.3.1. Target Radio Frequency Features

The RF features are distinct characteristics that can be differentiated within the RF domain. Selecting the appropriate target RF feature is crucial for the design of the RFF. While various methods exist to calculate the RF features from RF signals, in this work, we adopt the definition outlined in our previous research [2]. The simple descriptions for each feature are as follows:

- **(Rising Transient, RT)** The RT feature is a signal property that rises from the noise level to the desired communication level, illustrating the process of RF signal emission when the device is activated.
- **(Steady State, SS)** The SS feature refers to the property of the signal region that contains the RF-modulated digital data for message transmission. This illustrates the process of RF modulation during data transmission.
- **(Falling Transient, FT)** The FT feature represents the signal property that decreases from the communication level to the noise level. This illustrates the attenuation of the RF signal when the device is deactivated.

The most crucial aspect of utilizing the RF features as public keys is ensuring that it

cannot be forged by a third party. In [100], it was reported that the statistical analysis of the RT feature is more resilient to impersonation attacks compared to the I/Q constellation error calculation in the SS feature.

Additionally, we aim to replace certificates with RF features. From the definition of the RF features, the RT and FT features are independent of the modulated digital data, and they can be directly utilized as unique features over an extended period. On the other hand, the SS feature undergoes significant variations depending on the modulated digital data. These data dependencies can be eliminated through additional computational costs, such as extracting the ideal modulated RF signal from the received RF signal [22]. However, these post-processing costs may compromise the effectiveness of the system configuration.

For this reason, in this research, we focus on the RT and FT features as RF features, aiming to create characteristics that have no dependencies on the digital contents of the certificate.

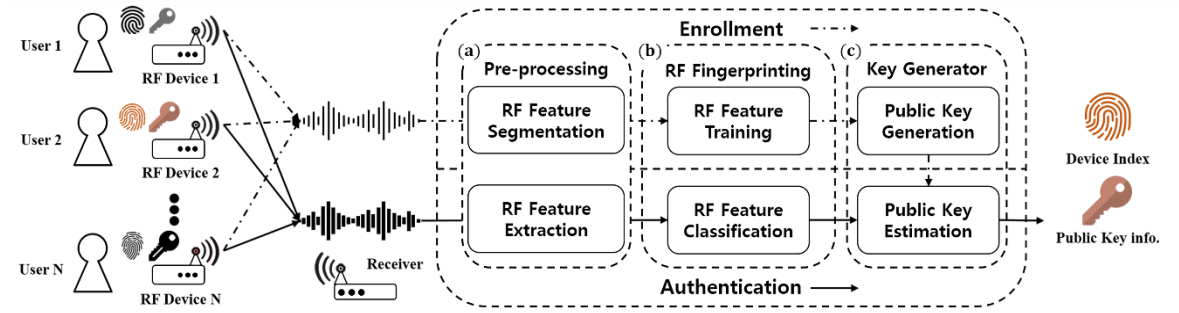


Figure 3.2 The overall RF Fingerprinting process is depicted with (a) the Pre-processing step and (b) the RF Fingerprinting step illustrating the conventional RFF, followed by (c) (Proposed) the Key Generator step representing the proposed RF-PubKG method.

3.3.2. Radio Frequency Fingerprinting

The overall scheme for the RFF process is presented in Fig. 3.2, along with the proposed RF-PubKG structure. This subsection describes the detailed RFF process,

including the pre-processing step and the RFF model training process. The proposed RF-PubKG scheme is described in Chapter 3.4.

The details of the RFF process are conducted in three steps: 1) RF feature segmentation, 2) RF feature extraction, and 3) RF feature training and classification.

The overall RFF process is formulated as a classification problem for given RF features. The mathematical description is as follows:

$$\mathbf{y} = F_{\text{RFF}}(\mathbf{s}) \quad (3.1)$$

where $\mathbf{s} \in \mathbb{C}^{N_{\text{Sig}} \times 1}$ is a down-converted RF signal acquired from the receiver operation. N_{Sig} is the length of a complex-valued signal \mathbf{s} . F_{RFF} is the RFF algorithm that maps the input signal \mathbf{s} from the RF signal space to the device ID space. Finally, $\mathbf{y} \in \mathbb{R}^{N_c \times 1}$ is the result of the RFF that contains the device ID information, where N_c represents the number of transmitters used to train the RFF algorithm.

The RF feature segmentation is the step for extracting the target RF features from the received RF signal. This procedure can be represented by the following equation:

$$\mathbf{s}_{\text{Seg}} = g_{\text{Seg}}(\mathbf{s}) \quad (3.2)$$

where g_{Seg} is the function for segmenting the RF features $\mathbf{s}_{\text{Seg}} \in \mathbb{C}^{N_{\text{Seg}} \times 1}$. It is defined on the target RF feature list, i.e., $feature \in \{RT, FT\}$. N_{Seg} is the length of the segmented RF features \mathbf{s}_{Seg} . In this paper, g_{Seg} is designed based on the energy variation of the RF feature. We adopt a windowed energy detection approach to monitor the energy fluctuation, with $E_n \geq (1 + \delta)E_{n-1}$ indicating a rise for RT and $E_n \leq (1 - \delta)E_{n-1}$ indicating a fall for FT. The specific details are further described in [2].

As a next step, the RF feature extraction aims to transform the signal space of RF features into other domains, thereby enhancing the differentiation between the RF features from different transmitters. The extraction procedure is expressed as follows:

$$\mathbf{s}_{\text{Trans}} = h_{\text{Trans}}(\mathbf{s}_{\text{Seg}}) \quad (3.3)$$

where h_{Trans} is the function for domain transform of the RF features. $\mathbf{s}_{\text{Trans}} \in \mathbb{R}^{N_{\text{Trans}}^i \times N_{\text{Trans}}^j}$ is the transformed RF feature, where N_{Trans}^i and N_{Trans}^j are the sizes of each transformed indices, i and j , respectively. The function h_{Trans} can be defined in many different ways. It can transfer to the I/Q constellation domain [101], can calculate the properties in the statistics domain [33], or can be directly processed into the AI models for deep learning classifiers [23]. In this paper, the discrete-time short-time Fourier transform (STFT) is applied to convert the signal domain into multi-dimensional spaces, i.e., time and frequency axis. In this case, i and j are t and f ; the details are described in [2].

As a last step, the RF feature training and classification aims to assign transmitter IDs from the RF features, ensuring robust classification through effective training. The classification results can be obtained by:

$$\mathbf{y} = \mathbf{f}_{\text{Classify}}(\mathbf{s}_{\text{Trans}}) \quad (3.4)$$

where $\mathbf{f}_{\text{Classify}}$ is the classification algorithm, and the output \mathbf{y} implies the transmitter ID information. Thanks to recent research in deep learning, $\mathbf{f}_{\text{Classify}}$ is commonly defined as a deep learning-based classifier, such as Convolutional Neural Network (CNN) based classifiers [102–104] or Generative Adversarial Network (GAN) based approaches [27, 105]. This paper utilizes the Deep Inception Network (DIN), which reported its effectiveness in understanding the RF features in our previous work [2], as the main RFF model. The structure details are described in Table 3.4 of Chapter 3.5.

To obtain the classification from (3.4), we must train the RFF model $\mathbf{f}_{\text{Classify}}$ for robustness. From the given training dataset $\mathbf{S} = [\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_M]$ of M samples and their relative labels $\mathbf{Y} = [\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_M]$, our DIN model for RFF can be trained with the cross-entropy loss and Adam optimizer [73] as follows:

$$loss = -\left(\frac{1}{M}\right) \sum_{i=1}^M \log \left(\frac{e^{y_i[c_k]}}{\sum_{j=1}^C e^{y_i[c_j]}} \right) \quad (3.5)$$

where k is the true transmitter ID relative to an output label y_i , and $y_i[c_j]$ is the value of the j th element in y_i .

3.3.3. Digital Signature scheme

A Digital Signature (DS) scheme is one of the PKC applications used to verify the authenticity and integrity of a digital message [106]. It involves using a private key to generate a unique signature for the sending message, which can be verified using the corresponding public key. The signature verifies that the message is not tampered with and is indeed sent by the claimed sender.

The DS scheme involves the following steps:

- **(Key Generation, *Gen*)** The signer generates a pair of keys; a private key, k_{pri} , and a corresponding public key, k_{pub} . k_{pri} is kept secret and used only by the signer, while k_{pub} is made public and can be shared with the verifier.

$$[k_{\text{pri}}, k_{\text{pub}}] = \text{Gen}(1^n) \quad (3.6)$$

- **(Signature Generation, *Sign*)** To sign the message m which has been hashed with the hash function h , the signer applies a one-way cryptographic function to the hashed message.

$$\sigma = \text{Sign}(k_{\text{pri}}, h(m)) \quad (3.7)$$

- **(Signature Verification, *Vrfy*)** The verifier with the public key, k_{pub} , and the signature, σ , can verify the authenticity of the sending message m . Verification is done by applying a verification function defined as follows:

$$\text{Vrfy}(k_{\text{pub}}, h(m), \sigma) = b \quad (3.8)$$

where b is 1 if the signature is valid, and 0 if the signature is invalid

The digital signature can be verified by anyone who has access to the valid public key. However, calculating the private key solely from the public key and forging a valid signature using the estimated private key is extremely challenging due to cryptographic complexity. These properties make digital signature schemes fundamental tools for ensuring the integrity of digital data and emphasize the need for valid public key management.

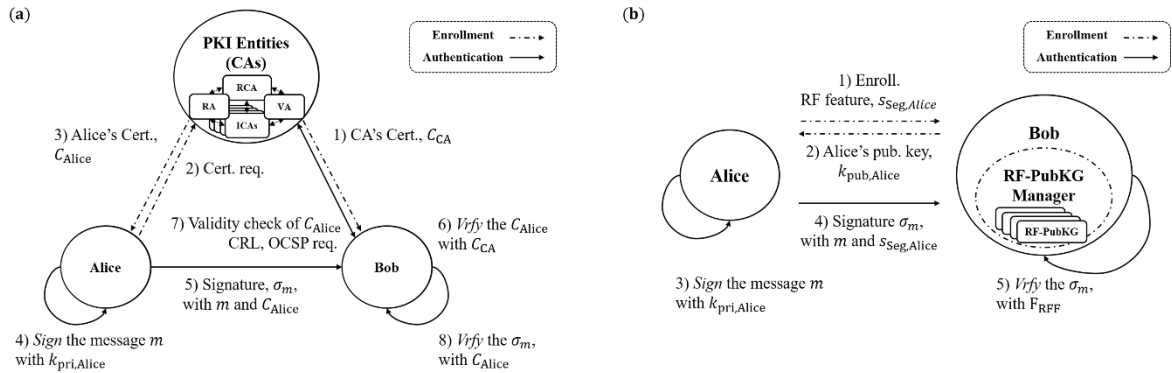


Figure 3.3 System overview of Digital Signature schemes: (a) Traditional scheme with a certificate management system from the PKIs, illustrating the process of certificate issuance; (b) Trustworthy scheme based on the RF-PubKGs, utilizing the RFF for key generation to eliminate the need for a centralized certificate authority, thus simplifying the overall certificate management system.

3.3.4. Certificates and Public Key Infrastructure (PKI)

The trustworthiness of the public keys is crucial in digital signature schemes. If third parties generate invalid signatures and fake public keys, the verifier may struggle to determine signature validity. To prevent this, the digital certificate is used to verify the authenticity of the user's public key. These certificates are strictly managed in the PKI system to ensure integrity and authenticity [107].

We present the system overview of the digital signature scheme with the PKIs in Fig. 3.3.(a). The Certificate Authority (CA) is a core entity of the PKI structure, constructed as a

trusted entity responsible for ensuring the authenticity of the certificates. The certificate contains a digital signature with a user's public key and identity information. The CA signs this certificate with the CA's private key and commits it to Alice and Bob within a secured channel. By verifying Alice's certificate with the CA's public key, Bob can trust the integrity of Alice's public key.

The CA is responsible for the revocation and renewal of the certificates. The CA must publish the Certificate Revocation Lists (CRLs) or operate the Online Certificate Status Protocol (OCSP) to inform users of the up-to-date status of the certificates. Bob needs to check these lists to ensure that Alice's public key is current.

The CAs are organized in a hierarchical model, where the intermediate CA (ICA) authenticates users, and the ICAs are authenticated by the root CA (RCA). This structure ensures the certificate's credibility by tracing back to the credibility of all CAs. However, this structure requires significant resource allocation to maintain the secure channel for the commitment of the certificates. Effective architecture to reduce these management costs must be considered [92].

In this paper, we aim to propose the RF-PubKG, which the public keys are directly derived from the RFF models.

$$[\mathbf{y}, k_{\text{pub}}] = F_{\text{RF-PubKG}}(\mathbf{s}) \quad (3.9)$$

We present an overview of the digital signature scheme with the RF-PubKG in Fig. 3.3.(b). The uniqueness and non-replicability of RF features allow the RF features to serve as unique public keys, replacing the role of digital certificates. By transforming the RF features into finite cryptographic sequences, i.e., unique public keys, the trustworthiness of the public key can be ensured, a role previously fulfilled by certificates. This approach can simplify the PKI architecture in the digital signature scheme. It allows the RF-PubKG model manager, which originally operates at the receiver in the RFF process, to manage the enrollment of RF features for authentication. Therefore, this approach can simplify the hierarchical model required by focusing on managing the RFF models within the RF-PubKG manager, thus reducing the complexity of the traditional certificate infrastructure.

3.4. Proposed RF based Public Key Generator (RF-PubKG) method

3.4.1. Radio Frequency Public Key Generator

Originating from the conventional RFF process outlined in Chapter 3.3.2, the RF-PubKG includes an additional feature map layer to enhance cryptographic key reliability. The underlying principles and algorithmic approaches of the RF-PubKG are described in this section.

The feature map was first introduced as an intermediate computation result of the CNN model [108]. It is used to detect and extract specific features from the input data. Each value of the feature map in the data represents the interaction between a particular feature and its location information. This feature map helps to understand how the deep learning model can recognize essential features within the data.

From research analyzing the feature maps learned by each layer, it is well-known that higher layers can learn complex features to make decisions [109]. Applying this understanding to the RFF model, we can infer that the higher layers of the RFF model learn the crucial features from RF signals to estimate the device ID information. The proposed RF-PubKG is derived from this inference.

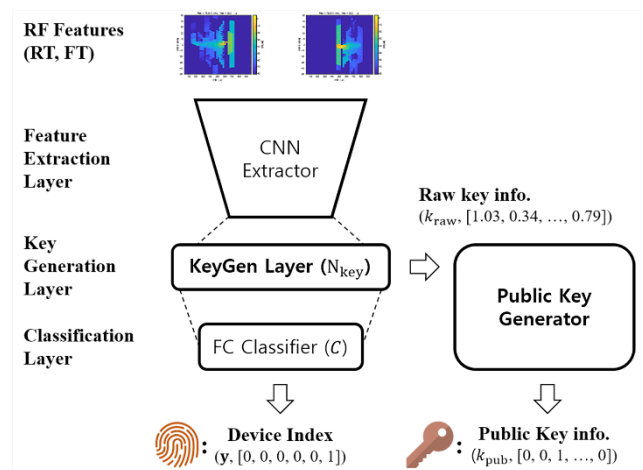


Figure 3.4 The proposed RF-PubKG structure: The KeyGen layer is located at the highest hidden layer, which processes outputs to generate and estimate the public key, as depicted in (3.10) to (3.14).

The RF-PubKG scheme is depicted in Fig. 3.4 . Based on the definition of the RFF classification model in (3.4), we define the output of the Key Generation (KeyGen) Layer as follows:

$$[\mathbf{y}, k_{\text{raw}}] = f_{\text{Classify,KeyGen}}(\mathbf{s}_{\text{Trans}}) \quad (3.10)$$

where $k_{\text{raw}} \in \mathbb{R}^{N_{\text{key}} \times 1}$ is the raw key derived from the input RF feature $\mathbf{s}_{\text{Trans}}$, and is considered as an intermediate output produced by the additional KeyGen layer. $f_{\text{Classify,KeyGen}}$ is the classification algorithm for RF-PubKG, which extends the RFF model with the KeyGen layer. In this research, the KeyGen layer is located at the highest hidden layer of the RFF model, i.e., just before the final classification layer.

The raw key, k_{raw} , is computed within the real domain, \mathbb{R} . To apply the cryptographic scheme, the raw key needs to be converted into a cryptographic sequence that operates within the finite field domain. To transfer the real domain into the target finite field with q elements, we define a mapping function as follows:

$$k_{\text{estimate}} = \text{round} \left((q-1) \times \frac{k_{\text{raw}} - \min(k_{\text{raw}})}{\max(k_{\text{raw}} - \min(k_{\text{raw}}))} \right) \quad (3.11)$$

where $k_{\text{estimate}} \in \mathbb{N}^{N_{\text{key}} \times 1}$ is the estimated cryptographic key working with the Galois Fields with q elements, i.e., $GF(q)$. This research assumes a binary field, $GF(2)$. The round function is a mathematical function that maps a real number to the nearest integer number.

The phase of the RF-PubKG is divided into two parts, i.e., Enrollment and Authentication, similar to the RFF as described in Fig. 3.2. Enrollment is the training phase in which the classification model is trained from the pre-enrolled RF features of the target transmitters. Authentication is the testing phase in which the input RF feature is classified as one of the trained transmitter sets.

Based on this description, we set the public key of the RF transmitters as a sample mean of the pre-enrolled RF features, which can be obtained during the Enrollment phase.

The detail is as follows:

$$k_{\text{pub},c_i} = \text{round} \left(\frac{\sum k_{\text{estimate,Train},c_i}}{n_{\text{Train},c_i}} \right) \quad (3.12)$$

where $k_{\text{pub},c_i} \in \mathbb{N}^{N_{\text{key}} \times 1}$ is the public key of the i th target device c_i , $k_{\text{estimate,Train},c_i}$ is the sample cryptographic key estimated from the pre-enrolled RF features, and n_{Train,c_i} is the number of the pre-enrolled samples.

The public key setting step can be done by calculating the public keys as in (3.12) for all of the target transmitters.

$$\mathbf{K}_{\text{Pub}} = [k_{\text{pub},c_1}, k_{\text{pub},c_2}, \dots, k_{\text{pub},c_N}] \quad (3.13)$$

where $\mathbf{K}_{\text{Pub}} \in \mathbb{N}^{N_{\text{key}} \times N_C}$ is the public key set of all target transmitters, which can be used as a reference for the public key generators.

To authenticate the public key from the input RF feature during the Authentication phase, a key estimation method is required to estimate a public key from a given public key set. We consider the similarity of the cryptographic sequences; Hamming distance is a valuable metric that measures the similarity of the two input sequences [110]. We can estimate the public key as follows:

$$\hat{k}_{\text{pub}} = \underset{k_{\text{pub},c_i}}{\text{Argmin}} H(k_{\text{pub},c_i}, k_{\text{estimate,Test}}) \quad (3.14)$$

where $k_{\text{estimate,Test}}$ is the cryptographic key estimated from the test RF feature, H is the Hamming distance between the public key and estimated key, and $\hat{k}_{\text{pub}} \in \mathbb{N}^{N_{\text{key}} \times 1}$ is the final estimated public key of the test RF feature during the Authentication phase.

By referencing (3.10) and (3.14), we can obtain the formulation of the RF-PubKG as represented by (3.9). The whole procedure for the RF-PubKG is presented in Table 3.1 (i.e., Algorithm 1).

Table 3.1 Proposed RF-PubKG algorithm, $F_{\text{RF-PubKG}}$.

Algorithm 1. Proposed RF-PubKG algorithm, $F_{\text{RF-PubKG}}$.

Input: The received RF signal \mathbf{s} .

Step1: Segment and Transform the target RF signal \mathbf{s} to the segmented RF feature \mathbf{s}_{seg} on (3.2) and the transformed RF feature $\mathbf{s}_{\text{Trans}}$ on (3.3).

If *phase* is *Enrollment* **do:**

Step 2-1: Train the RF-PubKG model $f_{\text{Classify,KeyGen}}$ on (3.10) with the loss function on (3.5)

Step 2-2: Set the public keys \mathbf{K}_{pub} on (3.12) and (3.13).

else if *phase* is *Authentication* **do:**

Step 2-1: Estimate the device ID, c_i from the model output \mathbf{y} , described in (3.10).

Step 2-2: Estimate the public key, \hat{k}_{pub} , based on the key estimation equation in (3.14).

Output: The estimated device ID, c_i , the estimated public key, \hat{k}_{pub} .

3.4.2. RF-PubKG Based Hashed RSA scheme.

In this chapter, we aim to prove the effectiveness of the proposed RF-PubKG system. As a proof of concept, we demonstrate the RF-PubKG-based digital signature scheme with the simplified PKI configuration by replacing the CAs with the RF-PubKGs.

This paper considers the hashed RSA algorithm as a digital signature scheme. The RSA algorithm is currently the most widely used PKC algorithm. The RSA is based on the mathematical fact that the factorization of the sufficiently large number is difficult to solve [111]. T, represented as follows:

$$n = P \cdot Q \quad (3.15)$$

where P and Q are prime numbers, and n is the product of these two primes. The factorization of the sufficiently large n into the unknown prime numbers, P and Q , is a complicated problem. However, if one of the two primes is known, calculating the other remaining prime becomes an easy problem.

The RSA key generation process utilizes the above relationship to generate the public and private key pair. In this work, we aim to generate an RSA private key, k_{pri} , satisfying the following two conditions when the estimated public key, k_{pub} , is given from Algorithm 1.

$$\gcd(\varphi(n), k_{\text{pub}}) = 1 \quad (3.16)$$

$$k_{\text{pri}} \cdot k_{\text{pub}} \equiv 1 \pmod{\varphi(n)} \quad (3.17)$$

where $\varphi(n) := (P-1) \cdot (Q-1)$ is Euler's totient function of n in (3.13).

We detail the hashed RSA algorithm based on the RF-PubKG in Table 3.2 (i.e., Algorithm 2). To integrate the RF-based estimated public key into the RSA algorithm, the following two modifications are made to the conventional hashed-RSA algorithm:

$$\text{LSB}(k_{\text{pub}}) = 1 \quad (3.18)$$

$$\hat{k}_{\text{pub}} = F_{\text{RF-PubKG}}(\mathbf{s}) \quad (3.19)$$

where (3.18) reflects the public key for RSA key pairs that need to be odd numbers, and (3.19) is the expected public key that should be utilized in the verification step.

The remaining steps align with the standard RSA algorithm; the signer signs the message m with its private key k_{pri} , denoted by RSA signature σ_m , and the verifier verifies the signature σ_m with its public key k_{pub} in verification scheme. The 'Hash-and-Sign' paradigm, referred to as hashed RSA algorithm [106], employs a one-way hash function h to convert variable-length input message m to a fixed-length hash value \hat{m} . This conversion is computationally challenging to reverse, making it useful for constructing efficient and secure signatures. In this paper, SHA-256 is applied, which is well known to provide random oracle properties [112]. The system structure is presented in Fig. 3.3.(b).

Table 3.2 Hashed RSA algorithm based on RF-PubKG.

Algorithm 2. Hashed RSA algorithm based on RF-PubKG.

Input: The public key k_{pub} , the user identity m , the received RF signal s and the RF-PubKG algorithm

$F_{\text{RF-PubKG}}$.

function $Gen(k_{\text{pub}})$

1. Set the LSB of the k_{pub} as 1 (for odd number)
2. Set the large P and Q as prime numbers (with the size of $N_{\text{key}}/2$ bits).
3. Compute $n = P \cdot Q$ and $\varphi(n) = (P-1) \cdot (Q-1)$.
4. Check that $\text{gcd}(\varphi(n), k_{\text{pub}}) = 1$
 - 4.1 If not, do again from 2 to 4.
5. Compute k_{pri} where $k_{\text{pri}} \cdot k_{\text{pub}} \equiv 1 \pmod{\varphi(n)}$

Output: Public key $\{k_{\text{pub}}, n\}$ and Private key $\{k_{\text{pri}}, n\}$.

function $Sign(k_{\text{pri}}, m)$

1. Hash the input message, m , i.e. $\hat{m} \leftarrow SHA_{256}(m)$
2. Sign the hashed message \hat{m} , i.e. $\sigma_m \leftarrow \hat{m}^{k_{\text{pri}}} \pmod{n}$

Output: The signature σ_m of the message m .

function $Verify(s, m, \sigma_m)$

1. Estimate the public key, \hat{k}_{pub} , from $F_{\text{RF-PubKG}}$ as depicted in Algorithm 1
- if** $SHA_{256}(m) = \sigma_m^{\hat{k}_{\text{pub}}} \pmod{n}$ **then**
 return True
else:
 return False
-

3.5. Experimental Setups

3.5.1. RF feature dataset description

We collected a set of RF signals from real RF transmitters. Six Ultra High Frequency (UHF) walkie-talkie transmitters were prepared; four were the SL1M Motorola, and two were the BD358 Hytera. All transmitters adhered to the Digital Mobile Radio (DMR) standard [40], which followed the two-slot Time-Division Multiple Access (TDMA) and four-level Frequency Shift Keying (4FSK) modulation protocol. The RF signal consisted of repeated RF bursts. These bursts occurred at intervals of 30ms. Each RF burst was constructed from the RT, SS, and FT features described in Chapter 3.3.1. We considered the RT and FT features as the target RF features in this research.

The details of the RF feature dataset are presented in Table 3.3. An average of 664 RF

bursts were measured for each transmitter, resulting in 3982 bursts from six transmitters. The RF dataset was divided into training and testing datasets at a ratio of 7:3, meaning that 2790 bursts were used for training, while 1192 bursts were reserved for testing.

Table 3.3 RF Feature Dataset

Class	Model Type	# of Signal Acquisitions	# of RF bursts
Device 1	Model 1	35 times	665
Device 2	Model 1		665
Device 3	Model 1		665
Device 4	Model 1		665
Device 5	Model 2		661
Device 6	Model 2		661
Total classes	6	Total bursts	3982

3.5.2. Evaluated RF Fingerprinting Models

In this paper, we aim to demonstrate the effectiveness of the key generation approach rather than evaluating the classifier model. We describe the architectures of the main and baseline RFF models evaluated in this paper.

There are three approaches to constructing the custom deep learning classifier: a vgg block in VGG [113], a residual block in ResNet [69], and an inception block in Inception-v4 [71]. We have evaluated the RFF models with these construction approaches to demonstrate the generality of the RF-PubKG.

Table 3.4 Architecture of the RF-PubKG model (Based on DIN model in [2])

Type	Filter size / Stride / padding	Output Shape
Input signal	-	205x124x1
Conv_1	3x3 / 2 / 0	102x61x32
Conv_2	3x3 / 1 / 0	100x59x32
Conv_3	3x3 / 1 / 1	100x59x32
Max Pool	3x3 / 2 / 0	49x29x32
2 x Inception	Inception-A [$N_F = 32$]	49x29x128
1 x Reduction	Reduction-A [$N_F = 32$]	24x14x192
2 x Inception	Inception-A [$N_F = 64$]	24x14x256
1 x Reduction	Reduction-A [$N_F = 64$]	11x6x384
Avg. Pool	Adaptive Avg. Pooling	384
Key Gen Layer	logits	N_{key}
Linear	logits	6

We constructed the main RFF model based on the inception block. The architecture detail is presented in Table 3.4. The design strategy of the inception block is to filter out input features using different receptive field sizes. This strategy was successfully demonstrated to be useful for understanding RF features in our previous work [2]. Based on this result, we adopted the DIN classifier from [2] as the main RFF model, utilizing the inception-A and reduction-A blocks of the inception-v4 model [71]. The only modification made was the introduction of the KeyGen layer as the highest hidden layer of the model, serving as the public key generator, as described in Chapter 3.4.1.

A first baseline model is established using a set of vgg blocks. The design strategy of the vgg block employs a repeated pattern of a simple and homogeneous topology, proven effective in extracting complex features as the network deepens [113]. To ensure fairness in comparison with the main model, we simplified the VGG11 model in [113], originally composed of 5 vgg blocks, to just 2 vgg blocks with channel depths of 32 and 64. Similar to the main model, we introduced the KeyGen layer just before the FC-1000 layer.

A second baseline model is established using the residual block. The residual block is designed to alleviate the vanishing gradient problem that occurs as the network goes deeper, through the use of a skip connection [69]. This strategy is well-reflected in [38], where the Hilbert spectrum of the SS feature is effectively trained by repeating 2 residual blocks. Baseline 2 is constructed from the RFF model structure in [38] by introducing the KeyGen layer just before the fc5 layer.

The third baseline represents a conventional RFF model constructed using a CNN architecture. In [21], the SS features were calculated by removing the ideally encoded signal from the received RF signal, and these features were learned using an RFF model constructed with a 1D convolutional network. For the Baseline 3 model, we adapted the identification network from [21], converting the 1D convolutional layer to 2D, and added a KeyGen layer just before the final Dense layer.

3.5.3. Ensemble RF-PubKG

An ensemble approach is a well-known method to enhance the generalization performance of the classifier [74]. It aggregates the results of the multiple base classifiers to

make a final decision. It was reported that the stacking ensemble of the multiple RF features can improve the accuracy of RFF [2].

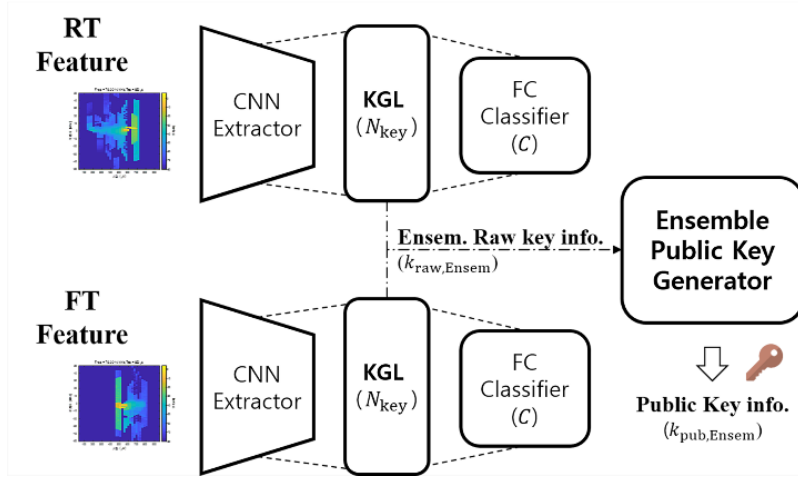


Figure 3.5 Ensemble approach of RF-PubKGs: The raw key outputs from each RF-PubKG are combined in stacked manner in (3.20).

We construct a stacking ensemble key generator as shown in Fig. 3.5. From the definition of the raw key with a single classifier in (3.10), the ensemble raw key $k_{raw,Ensem}$ for the input RF features $\mathbf{s}_{Trans,feature}$ can be defined as follows:

$$k_{raw,Ensem} = \frac{1}{|feature|} \sum f_{KeyGen,Classify}(\mathbf{s}_{Trans,feature}) \quad (3.20)$$

where $feature \in \{RT, FT\}$ is the target feature of interest for stacking the ensemble classifier, and the other key generation algorithms in (3.10) to (3.14) operate on this ensemble raw key $k_{raw,Ensem}$.

3.6. Results and Discussions

This chapter describes the results and discussion related to the proposed RF-PubKG method. Accuracy and Frame Error Rate (FER) are examined across various signal-to-noise ratio (SNR) channel conditions to evaluate the effectiveness of the RF-PubKG. To evaluate

system reliability, we measure clustering results for RF-PubKG outputs and the correlation between different public keys or RF-PubKG models. Furthermore, we quantify the size and time consumption of the RSA algorithm based on RF-PubKG, serving as a proof of concept for the RF-PubKG-based digital signature scheme, as illustrated in Fig. 3.3. These metrics, which will be discussed in the following subsections, provide a comprehensive evaluation of the proposed RF-PubKG’s performance and reliability.

3.6.1. Public Key Estimation results

First, we evaluate the key estimation accuracy and key estimation time of the proposed RF-PubKG method. Accuracy is determined by the correctness of the estimated public key, as defined in (3.14). Time is measured as the public key generation time from (3.10) to (3.14). We assume that the public key set in (3.13) is already established during the Enrollment phase and committed to the receiver in the Authentication phase. The results are presented in Tables 3.5 and 3.6.

Table 3.5 Key Estimation Accuracy*

RF-PubKG models		Key Size			
		1024	2048	4096	8192
<i>[P] Incep.</i>	RT	98.3±0.2	98.2±0.4	98.2±0.4	97.9±0.8
	FT	96.0±0.7	95.1±1.0	94.9±0.8	93.7±1.7
	Ensem.	99.7±1.0	99.5±0.2	99.6±0.3	99.4±0.4
[B1] VGG	RT	92.0±4.1	95.7±1.1	96.7±1.2	97.0±0.5
	FT	84.5±1.8	84.4±1.8	85.8±1.3	85.8±1.0
	Ensem.	97.2±0.7	97.6±1.1	97.6±1.0	97.9±0.8
[B2] Res.	RT	97.1±0.9	97.2±0.3	96.5±0.8	96.0±0.6
	FT	91.2±0.8	91.5±1.1	90.6±1.2	90.8±1.2
	Ensem.	99.1±0.4	99.0±0.4	98.4±1.0	99.1±0.4
[B3] CNN	RT	65.6±11.7	73.2±7.7	79.2±4.4	81.9±5.4
	FT	78.3±2.1	76.6±6.4	78.6±3.3	78.5±3.6
	Ensem.	82.3±5.8	86.4±5.1	90.1±3.0	91.4±2.4

* Mean Accuracy (%) ± Standard Deviation, as derived from (3.14)

Table 3.5 illustrates the public key estimation accuracy related to variations in key size. The FT feature achieved an average mapping accuracy of 94.9% to cryptographic sequences, while the RT feature achieved 98.1% accuracy. The Ensemble of RF Features yielded a 99.6% accuracy in mapping to cryptographic public keys. This result indicates that there were just five rejections out of 1192 RF bursts in the test dataset. In other words, one rejection per every 7.5 seconds will occur in the DMR transaction.

When compared to the baselines, Baseline 2 achieved an accuracy that was 0.7% lower than the inception block, highlighting the residual block's efficiency. However, the inception block maintained higher accuracy than Baseline 2 across all key size variations. This is consistent with the findings in [2] that the consideration of different receptive filter sizes in the inception block is more efficient. While Baseline 1, utilizing the vgg blocks, showed similar estimation efficiency, it had a nearly 2% decrease in performance. Regarding Baseline 3, the CNN-based RFF model, it achieved an accuracy of only 87.6%. We analyzed this result due to its limited structure for training RT and FT features.

Table 3.6 Key Estimation Time

RF-PubKG models		Estimation Time*	# of parameters	# of branches
[P] Incep.	RT / FT	5.6 ± 0.1	1.1 M	4
	Ensem.	10.8 ± 0.1	2.3 M	
[B1] VGG	RT / FT	1.7 ± 0.0	25.8 M	1
	Ensem.	2.6 ± 0.1	51.5 M	
[B2] Res.	RT / FT	2.2 ± 0.0	0.3 M	2
	Ensem.	3.8 ± 0.0	0.5 M	
[B3] CNN	RT / FT	1.5 ± 0.0	0.8 M	1
	Ensem.	2.2 ± 0.0	1.7 M	

* Mean Estimation Time (ms) \pm Standard Deviation, as measured from (3.10) to (3.14)

Table 3.6 presents the key estimation time for the RF feature-based public key. Using a single feature, the inception RF-PubKG results in an average estimation time of 5.6ms, while the ensemble approach results in 10.8ms. These values are greater than those of the other baselines, such as 2.2 ms for Baseline 3, 2.6 ms for Baseline 1, and 3.8 ms for Baseline 2.

Upon analysis, we observe that the time degradation is primarily correlated with the number of branches in RFF models, rather than with the number of parameters. For instance, the ResNet and inception blocks contain 2 and 4 branches, respectively. While these branches may appear to be calculated in parallel within the system structure, they are serially computed and combined in S/W implementations. This means that the inception blocks require 4 times as many calculations as other baselines. Even in that case, the results of the inception RF-PubKGs remain competitive, considering the one-slot duration of the DMR transaction is 30ms. We expect that the ensemble RF-PubKGs can be optimized in time by utilizing multiple GPU units for parallel input features.

As a next step, we estimate the key estimation accuracy against SNR variation according to the AWGN channel. From (3.1), the received signal, including the AWGN channel noise, is defined as follows:

$$\hat{\mathbf{s}} \leftarrow \mathbf{s} + \mathbf{n} \quad (3.21)$$

where $\hat{\mathbf{s}}$ is a noisy RF burst to which AWGN channel noise \mathbf{n} generated proportionally from normal RF burst \mathbf{s} is applied. SNR formulation for the AWGN noise \mathbf{n} is defined as follows:

$$SNR = 10 \log_{10} \left(\frac{\|\mathbf{s}\|_2^2}{|\mathbf{n}| \sigma_n^2} \right) \quad (3.22)$$

where $|\mathbf{n}|$ represents the length of the \mathbf{n} , and σ_n^2 represents its variation.

As a next evaluation metric, we evaluate the FER of the proposed method. According to the frame definition in the TDMA protocol of the DMR standard [40], one frame consists of two RF burst signals. Since the RF-PubKGs operate on units of the RF burst signal, we can compute the probability of two RF bursts being received without error. The probabilities are defined as follows:

$$BER = 1 - Accuracy \quad (3.23)$$

$$FER = (1 - BER)^2 \quad (3.24)$$

where the Burst Error Rate (BER) is the probability of an RF burst being rejected.

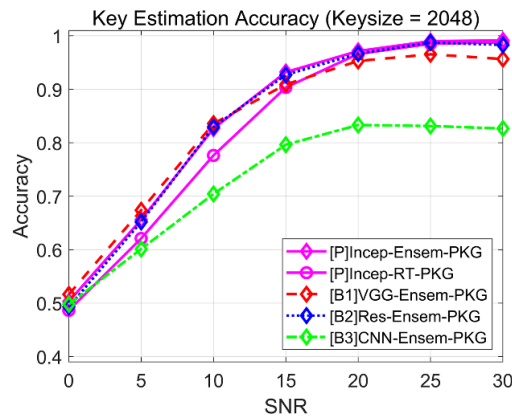


Figure 3.6 Key estimation accuracy of the RF-PubKG under AWGN channel conditions. The RF-PubKG achieves 97.2% at 20dB SNR, rising to 99.0% with improved channel conditions.

The estimation accuracy results in relation to SNR variation are presented in Fig. 3.6. With SNR over 20dB, which is generally assumed to be a good channel condition, the ensemble method achieved over 97.2% key estimation accuracy. This represents a performance improvement of more than 0.5% compared to 96.6% of the RT, 95.3% of the Baseline 1, and 96.7% of the Baseline 2. Baseline 3 only achieved an 83.3% accuracy, a degradation in performance. Especially at 25dB or higher, the inception RF-PubKGs achieved over 99.0% accuracy, uniquely achieving a BER of less than 1% compared to the other baselines.

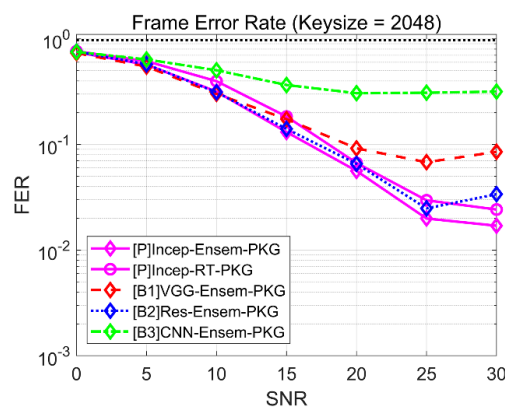


Figure 3.7 Frame error rate of the RF-PubKG under AWGN channel conditions. The RF-PubKG achieves 5.6% at 20dB SNR, 2.0% at 25dB SNR, and decreased to less than 1.0% in noise-free conditions.

Fig. 3.7 presents the FER results. At SNR levels exceeding 20dB, the ensemble approach achieves an FER of 5.6%. This value decreases to 2.0% at 25dB SNR and drops further to less than 1.0% in noise-free conditions where no AWGN noise is added. Conversely, the baselines do not reach below 1.0% FER, with the lowest value being 1.9% for Baseline 2 in noise-free conditions. We emphasize that these results reflect the raw FER without the application of Error Correction Coding (ECC), a technique commonly utilized to enhance FER performance. We anticipate that future improvements in performance through ECC will be possible.

3.6.2. Reliability of the Cryptographic Sequences

To evaluate the reliability of the proposed RF-PubKG, we conduct a comparative analysis of the estimated public keys derived from both training and test datasets. To facilitate this comparison, we apply t-distributed Stochastic Neighbor Embedding (t-SNE) to our RF dataset. t-SNE is a nonlinear dimensionality reduction method to transfer a high-dimensional data structure into a lower-dimensional space while preserving the similarity relationships of the data points [114]. It is primarily used for visualization and can be useful for discovering patterns or clusters in complex data domains. The results of the t-SNE are presented in Fig. 3.8.

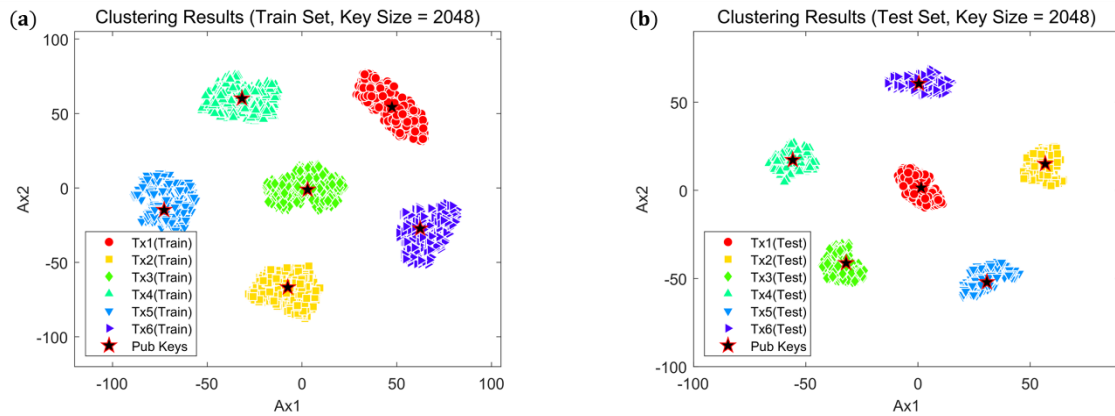


Figure 3.8 Clustering results of estimated public keys, k_{estimate} , from RF features with the public key set \mathbf{K}_{Pub} : (a) Demonstrated centrality within the training dataset; (b) Consistency maintained within the testing dataset. The public key set accurately establishes cluster centers during training and preserves center integrity in testing.

Fig. 3.8.(a). illustrates the clustering results between the public key sets \mathbf{K}_{Pub} and the public keys k_{estimate} estimated from the training dataset. The results show that the public key estimation scheme in (3.12) is simple but effectively identifies the center of each cluster. The key consideration for this evaluation is how well this pre-enrolled public key set aligns with the public keys estimated from the test dataset. The clustering result is illustrated in Fig 3.8.(b). The result shows that the given public key set retains the centrality of the clusters in the test dataset. It confirms that, as described in (3.14), accurate and unique public key estimation is achievable through a Hamming distance-based estimation approach, when using the provided public key set.

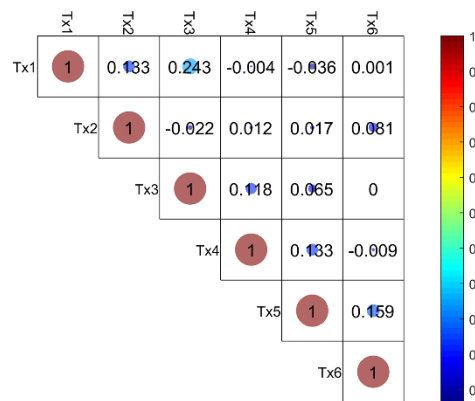


Figure 3.9 Correlation Matrix of the RF-PubKG. Public key correlations remain below 0.24, indicating the uniqueness of the generated public keys among RF transmitters.

In Fig. 3.9, a correlation matrix of the public key sets is calculated to confirm the stability of the generated public cryptographic key sets. The result shows that the correlation between the generated Public Key of each transmitter is not significantly large, and the largest correlation is 0.24 between Tx1 and Tx3. This is a reasonable result considering that the AI model trains the dataset for optimizing the clusters with sufficient distance. This result confirms that the RF-PubKGs can generate unique public key sets with sufficiently different cryptographic sequences between the RF transmitters.

Table 3.7 Correlation Matrix for Key Sets Generated by Distinct RF-PubKG Models

RFF Models	Classes					
	Tx 1	Tx 2	Tx 3	Tx 4	Tx 5	Tx 6
Trial 1	1	1	1	1	1	1
Trial 2	0.01	-0.03	0.03	-0.01	-0.03	-0.02
Trial 3	0.00*	0.02	0.01	0.02	0.02	0.00*
Trial 4	0.00*	-0.04	0.00*	0.04	0.04	0.02
Trial 5	-0.02	0.00*	0.00*	-0.02	0.02	-0.01
Trial 6	-0.01	0.01	-0.01	0.00*	0.00*	0.01
Trial 7	0.00*	0.01	-0.04	-0.02	-0.02	-0.02
Trial 8	0.02	-0.01	0.00*	0.00*	0.00*	0.00*
Trial 9	-0.03	0.04	-0.02	-0.01	-0.01	0.03
Trial 10	-0.03	0.01	0.01	-0.02	-0.02	-0.03

* Correlation values are lower than 0.01

Another significant aspect of evaluating the reliability of the key generator is to examine the variance in generated public key sets when new RFF models are being trained. Table 3.7 evaluates the correlations for the generated public key sets across the different trained RFF models. The result shows that the correlation remains consistently low, not exceeding 0.04. This implies that the activated node positions in the KeyGen layer are established through the random distribution. This observation confirms that the periodical re-training approach of the RFF model can enhance the overall security of the PKC system.

Table 3.8 Quantification Analysis of RF-PubKG Based Digital Signature Scheme Implemented by Hashed RSA Algorithm

Model	Key Size	Cert. File Size (Bytes)		Cert. Gen. time (ms)		Digital Signature processing time (ms)														
		CA	Sender	CA	Sender	Gen	Sign	KeyGen	CA Cert. Vrfy	Sender Cert. Vrfy										
Incep.-RSA	1024	Not Required**				157.1	20.1	21.9	Not Required	1.3										
	2048					1188.9	64.5	21.4		7.7										
	4096					11990.4	314.9	22.3		56.7										
	8192					195872.1	1970.7	22.9		437.2										
VGG-RSA	1024					Not Required**				153.5	19.9	16.0	Not Required	1.3						
	2048									1186.1	65.1	17.0		7.7						
	4096									15130.7	365.7	23.2		65.8						
	8192									225352.5	2286.1	28.9		505.9						
Res.-RSA	1024									Not Required**				151.0	19.9	6.9	Not Required	1.3		
	2048													1064.3	64.6	7.1		7.7		
	4096													15844.0	365.6	9.2		65.9		
	8192													245305.9	2290.9	10.2		508.0		
RSA*	1024	1159	969	9.6	1.7									129.8	18.1	Not Required		1.3	0.3	
	2048	1513	1322	48.5	2.4									970.4	50.2			1.2	0.7	
	4096	2566	2348	495.0	6.4									13335.4	239.0			1.2	2.4	
	8192	4182	3960	5974.7	32.9									194467.5	1289.5			1.6	8.3	

* Conventional hashed RSA algorithm (i.e., k_{pub} is 65537)

** Public keys are directly estimated from the RF-PubKG; certificate management is NOT required.

3.6.3. PubKGs in hashed RSA scheme

As a proof of concept for the RF feature-based digital signature schemes, the implementation performance was evaluated using a hashed RSA algorithm based on the RF-PubKG. The results for size and time consumption are presented in Table 3.8. We implemented a hashed RSA digital signature scheme based on the X509 certificate for the PKI management system using the PyCryptodome[115] and pyOpenSSL[116] libraries. The system overview is depicted in Fig. 3. PyCryptodome, a Python library for cryptographic operations that complies with the Digital Signature Standard (DSS) standard documents NIST FIPS 186-4 [117], is utilized to implement the RSA signature scheme. Meanwhile, the pyOpenSSL library, a wrapper for OpenSSL in Python, is used to construct the digital signature scheme with a single CA for PKIs using the X509 object packages in pyOpenSSL. The evaluation included evaluations of certificate file sizes and scheme operation time, thus confirming the concept for the proposed RF-PubKGs.

In our evaluation, we assume that the training procedure for the RF-PubKG has already completed the Enrollment phase as defined in Algorithm 1. This implies that the RF-PubKG function F_{RFF} and Public Key Set \mathbf{K}_{pub} have been committed to the sender and receiver before RF transmission. We artificially generate a 12-digit MAC address as a user identity message and evaluate the implemented signature scheme to verify this address. Our focus is on the analysis of time consumption and file size for constructing the PKIs. Specifically, we measure the time required for the Gen, Sign, and Vrfy processes as defined in Algorithm 2. In addition, we measure the time needed for CA certificate verification, the file size for PKI configuration, and the certificate generation time.

Consequently, the proposed RF-based RSA signature is identical to the conventional RSA signature method except for the public key generation process from the RF-PubKGs. For this reason, it was confirmed that the time consumption is similar to that of the conventional RSA algorithm, and it even increased as the key size increased. This result can be anticipated, given that the method involves a larger key size than general RSA key pairs, which utilize a fixed public key, i.e., k_{pub} is 65537.

The proposed RF-based RSA signature scheme presents an advantage in simplifying the PKI structure. Through the previous discussion, we confirmed that a public key can be uniquely derived from the non-replicable RF features. This means that the PKI, a system for maintaining and managing certificates, can be simplified because the reliability of the public key can be sufficiently secured. As a result of the actual experiment, it is confirmed that Alice's signature could be verified from the public keys estimated from the received RF feature, and a certificate for Alice is not required to verify the public key in this process. We note that one person only needs a few Kbytes and tens of milliseconds, but these amounts can increase exponentially as the number of people managed by PKIs increases.

This evaluation illustrates that the hierarchical model of CAs described in Chapter 3.3.4 can be sufficiently simplified. The complexity can be minimized, as the structure solely necessitates a RFF model manager responsible for the systematic updates of the RFF models.

3.6.4. Discussion

We have successfully evaluated the effectiveness and reliability of RF-PubKG and validated the concept of an RF-PubKG-based digital signature scheme using the RSA algorithm. This subsection discusses the impact and future work related to RF-PubKG, along with its drawbacks.

Effectiveness of the RF-PubKG: RF-PubKG is a novel RFF process designed to generate trustworthy public keys from non-replicable RF features. It allows for the integrity verification of the public key, based on the device's authenticity at the physical layer. We believe that RF-PubKG can enhance the efficiency of cryptographic system structures by being integrated into key verification processes.

As demonstrated in Chapter 3.6.3, we implemented an RF-PubKG-based digital signature scheme using the RSA algorithm. This scheme efficiently validates the signature directly from the trustworthy public key derived from the RF-PubKG, thereby making certificates redundant and reducing the need for third-party CA management. Consequently, as depicted in Fig. 3.3, RF-PubKG considerably simplifies the operational complexities and resources required for PKI entities. We believe this potential application to simplify PKC structures holds promise for a wide range of key-based cryptography.

Replaceability of the PKI structure: The RF-PubKG proposed in this paper demonstrates potential as a replacement for PKI. The RF-PubKG achieved a key estimation accuracy of over 99.4% and a FER of less than 1.0%. While this performance is superior to other baselines, it falls short of 100%, making it insufficient to replace PKI entirely. This subsection will discuss the system's limitations and possible application environments.

The advantage of RF-PubKG lies in its ability to simplify the complex PKI structure, even though frame drops may occur at a rate of 1.0% FER. In other words, RF-PubKG is suitable for application environments where the benefits of a simplified PKI can be maximized, despite the occurrence of slight data drops.

First of all, it is suitable for simplifying PKI systems in IoT environments. In IoT settings, where various sensors periodically transmit data via RF communication, there is a need for lightweight PKI solutions within limited network resources [123]. For example, in the case of RF communication using Walkie Talkie, as demonstrated in this paper, a drop of approximately 30ms did not cause any issues in communication. Moreover, it is expected to be used in various IoT environments for lightweight PKI structures, such as Industrial IoT [124], smart cities, and wireless sensor networks [125].

Outside of IoT environments, it can also be utilized to streamline PKI structures in the medical [124, 126] and financial [124] sectors. Traditional PKI structures are overly complex and slow, making them unsuitable for the fast and efficient security systems required in fields like healthcare and finance. Therefore, RF-PubKG's simplified but robust PKI system has significant potential for efficient use. However, given the nature of data in the financial and medical sectors, a 1% frame drop rate is insufficient and can cause serious issues in the event of errors. Hence, further research is needed to implement dual security measures or error correction mechanisms to minimize these risks.

Future enhancement of the RF-PubKG: Future work will focus on addressing the inefficiencies of the RF-PubKG-based digital signature scheme in the context of cryptography. As a proof-of-concept, we employed a cascade structure that combines RF-PubKG and the existing RSA algorithm. Although this approach shows feasibility, it was not optimally efficient from a cryptographic aspect, as demonstrated by the increased time

consumption shown in Table 3.8. These inefficiencies are drawbacks for real-world applications that necessitate further research into more effective cryptographic algorithms for managing the RF-PubKGs.

Additionally, further research is needed to enhance the reliability of RF-PubKG. For the replacement of PKI systems discussed in the previous section, it is necessary to improve key estimation accuracy performance through dual security mechanisms or ECC-based error correction mechanisms to ensure reliable system operation at lower SNR levels.

3.7. Summary

In this research, we have investigated the novel application of RF features in generating trustworthy cryptographic sequences, demonstrating the promising potential of RF features at the physical layer to enhance the efficiency of digital security. We proposed RF-PubKG, which utilizes a key generation layer within the RFF model to effectively map analog RF features to digital cryptographic key sequences. This work establishes a novel paradigm for public key generation.

We evaluated the effectiveness of RF-PubKG. We achieved key estimation accuracy of over 99% for various cryptographic key lengths, with a generation time of only 10.8ms. In AWGN channels with an SNR level over 20 dB, these results maintained a 97.2% accuracy along with a 5.6% FER, which decreased below 1% as channel conditions improved.

We corroborated the reliability of the RF-PubKG by validating the consistency and clustering centrality of the public key sets when compared to the testing dataset. We confirmed the independence among public keys by measuring correlation values lower than 0.24. Notably, the ability to generate distinct key sets with updates to the RFF model was demonstrated by correlation values lower than 0.04, emphasizing the dynamic and adaptable nature of the RF-PubKG scheme.

As a proof-of-concept, we have validated the RF-PubKG-based digital signature

scheme using an RSA algorithm. This scheme enhances PKI efficiency by generating reliable public keys directly from unique RF features, thus avoiding the complexities of third-party CA management. These results validate the signature verification directly from the RF-derived public keys, making certificates redundant. Such simplification could reduce the operational complexities and resource demands for PKIs, enhancing the efficiency of digital signature applications by simplifying the PKI entities. This process of verification could become less complex and resource-intensive when managing a large number of identities.

This research is a pioneering exploration into utilizing RF features as cryptographic sequences, thereby substantiating the cryptographic viability of the proposed method. Research findings not only evaluate the efficiency and reliability of the RF-PubKG but also its applicability to real-world cryptographic scenarios.

As a direction for future research, we plan to further improve our research findings by integrating ECC to improve FER rates and expanding the application of PKC to simplify complex hierarchical systems of cryptography. We will continue to pave the way for more secure and efficient cryptographic solutions derived from the potential of RF signal features.

Chapter 4. Summary of Contributions and Future

Research Direction

4.1. Summary of Contributions

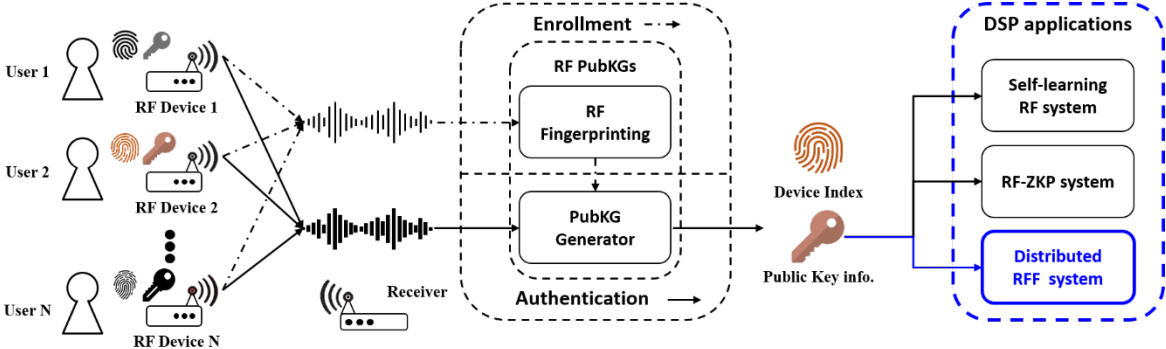


Figure 4.1 SFs-based application in the Digital Signal Processing domain.

Earlier chapters detailed foundational research in RF Fingerprinting, which primarily operated with the analog feature key in the real domain and extended into cryptographic public keys in finite fields. This chapter explores the challenges and future research directions for ensuring the integrity of RF Fingerprinting systems for public use. The evolution from RF-based physical layer authentication to cryptographic sequence generation lays the groundwork for addressing more complex and distributed environments that are typical in modern IoT digital applications. Figure 4.1 presents the conceptual motivation for future SFs-based IoT digital applications.

The first research in this dissertation, as presented in Chapter 2, focused on exploiting the intrinsic imperfections of RF emitters as an analog SF feature key to authenticate devices at the physical layer. This work achieves technical contributions by proposing an RF Fingerprinting system for physically secured FH signals, focusing on a detailed analysis of SFs feature key operations in the real domain. The RF Fingerprinting operation of the SFs in real domain has proven effective through direct application at the physical layer.

The second research in this dissertation proposed an RF-PubKG method that maps the analog SFs feature key operating in the real domain, \mathbb{R} , to a public key operating in the finite field, \mathbb{N} . This work achieves technical contributions by enabling the analysis of SFs in the finite field domain, $GF(2)$, and shows its potential by proving that it can be used in cryptographic applications such as public key cryptography.

We believe that we have paved the way for the development of trustworthy IoT applications using non-replicable digitized analog feature keys. Through our research, we have been able to extend SFs signal processing, which mainly operated in the real domain, to the finite domain, and we believe it should further extend to operation in the digital domain, i.e., DSP applications. This method is expected to address existing issues of RF Fingerprinting such as noise susceptibility, emitter scalability, and the difficulty of operating additional security systems except for the hardware non-replicable feature of the SFs. In the next sub-chapter, we will discuss the issues that need to be considered for the public use of RF Fingerprinting and future research directions.

4.2. Challenges and Future research directions for Public usage of RF Fingerprinting

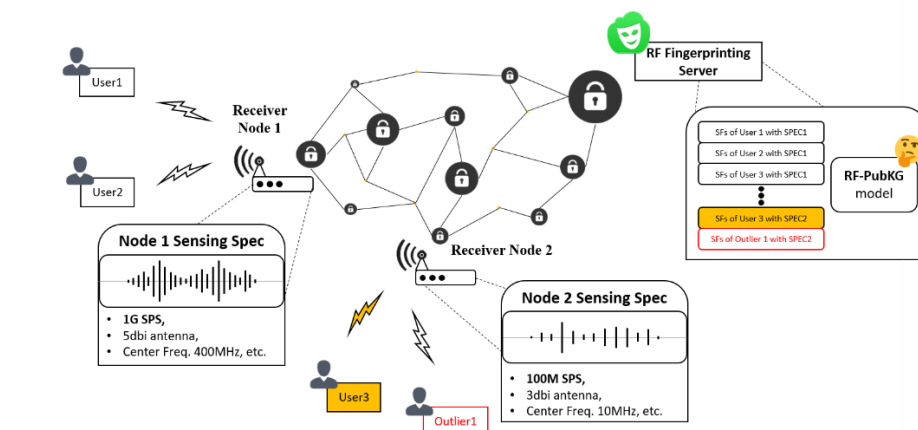


Figure 4.2 Challenges in Network Usage of the RF Fingerprinting System

For the public usage of RF Fingerprinting, it is impractical to equip every local environment that requires authentication with an RF Fingerprinting system; therefore, a

network system-based remote RF Fingerprinting system is necessary. The concept figure illustrating the challenges that could arise during the operation of a network system is shown in Figure 4.2. To ensure operation within a network system, it is necessary to consider the various specifications of different RF sensing nodes. In this section, we discuss the intrinsic difficulties that arise from the public usage of the RF Fingerprinting system on a network structure and describe possible strategies for handling these difficulties.

To operate RF Fingerprinting within a network system, the following challenges should be considered.

- **Emitter Scalability:** For public usage of RF Fingerprinting, it is necessary to consider a self-learning system that detects and relearns when a new emitter connects. Existing systems have difficulty detecting unlearned emitter signals. As mentioned in Chapter 2.4.6, single-label detection makes it relatively easy to consider detection and relearning, but multi-label detection and incremental learning are much more challenging and require further research.
- **Difficulty in Additional security:** The security of the RF Fingerprinting system starts from the non-replicable feature of SFs. While this is robust, it is still insufficient to guarantee a 100% perfect security system. Therefore, further research is needed to add additional security processing methods, such as ECC-based RF-PubKG and Zero Knowledge Proof, to enhance the security level.
- **Interoperability for Unified RF Fingerprinting Framework:** Within a network system, emitters can exist in various locations along with nodes having different RF sensing specifications. A straightforward method for unified operation is to prepare a sufficient number of RF samples for all possible emitter-sensing node combinations, but this is impractical. Therefore, research is needed on a robust feature extraction method that can compensate for this variability, and on a distributed AI learning method for a unified RF Fingerprinting framework that operates by transmitting only the emitter ID information.

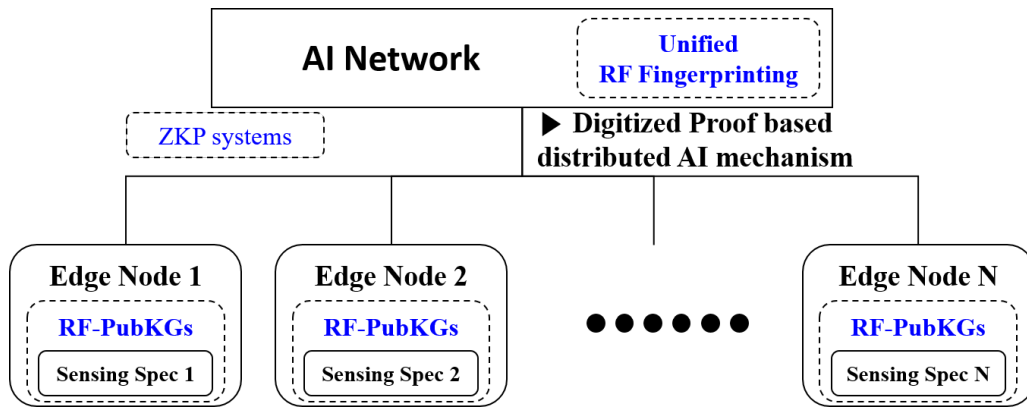


Figure 4.3 Proposed network system for public usage of the RF Fingerprinting

The concept structure of the proposed network system for public usage of RF Fingerprinting is illustrated in Figure 4.5. For the system implementation, the following research ideas need to be addressed:

- **Self-Learning System:** This system should be capable of detecting and adapting to new emitters as they connect, ensuring continuous learning and updating of the RF Fingerprinting database.
- **Zero Knowledge Proof:** Implementing cryptographic methods to ensure secure communication between nodes and the central system without revealing sensitive information.
- **Network-Based Distributed AI System:** A framework where AI models are distributed across various nodes, allowing for efficient processing and analysis of diverse RF emitter specifications.

The implementation of a PubKG-based RF Fingerprinting network system represents a significant advancement in handling the inherent challenges of developing network-based trustworthy IoT applications. By compensating RF signal processing algorithms across diverse sensing specifications, the proposed system aims to enhance the scalability, security, and efficiency of RF Fingerprinting applications in IoT and other future digital applications.

Chapter 5 Conclusions

This dissertation has focused on the application of RF Fingerprinting within IoT environments, with the primary goal of enhancing security through innovative identification and authentication strategies. Throughout this research, we have developed systems that adapt RF Fingerprinting to tackle modern digital and network challenges, resulting in several notable contributions and findings.

The research successfully proposed and developed the RFEI system, which is capable of identifying emitters operating with highly secured FH signals. This system represents a significant advancement in emitter identification technology, offering robust security measures suitable for IoT environments. Additionally, an anomaly detection algorithm was designed specifically for the RFEI system. This algorithm enhances the system's robustness by effectively identifying unusual patterns, thereby increasing its practical applicability in real-world scenarios.

Moreover, this dissertation introduced new digital signature algorithms that utilize SFs to streamline the PKI of PKC systems. These algorithms make the cryptographic operations both more efficient and secure. A pivotal achievement of this research was the successful transformation of SFs from the analog domain to cryptographic sequences in the digital domain. This transformation is essential for integrating RF Fingerprinting into digital communication systems and paves the way for its broader application across various digital platforms.

Moving forward, future research should address several key areas to further enhance RF Fingerprinting systems. Developing self-learning systems capable of detecting and learning from new emitters autonomously is essential, as current systems struggle with untrained emitter signals, particularly in multi-label detection and incremental learning scenarios. Additionally, investigating methods like Zero Knowledge Proof to enhance the security of RF Fingerprinting systems is crucial. While SFs provide a non-replicable feature, additional security layers are necessary for robust protection.

Moreover, exploring frameworks where AI models are distributed across various nodes will allow for efficient processing and analysis of diverse RF emitter specifications. This includes developing edge-based feature embedding models that standardize emitter ID information across the network.

The implementation of a PubKG-based RF Fingerprinting network system represents a significant advancement in developing trustworthy IoT applications. By compensating for RF signal processing across diverse sensing specifications, the proposed system aims to enhance the scalability, security, and efficiency in RF Fingerprinting applications. This system offers a promising direction for public usage and commercialization of RF Fingerprinting technology, paving the way for future digital infrastructures. These advancements are expected to drive the commercialization of RF Fingerprinting systems and significantly impact the development of secure and scalable IoT solutions.

Bibliography

- [1] Jusung Kang, Young-Sik Kim, and Heung-No Lee, "Radio Frequency Public Key Generator for Digital Application", IEEE Access, Vol. 11, pp. 140867 - 140880, Dec. 2023, doi: 10.1109/ACCESS.2023.3340305, (Impact factor: 3.9).
- [2] Jusung Kang, Younghak Shin, Hyunku Lee, Jintae Park, and Heung-No Lee, "Radio Frequency Fingerprinting for Frequency Hopping Emitter Identification", Applied Sciences, 11(22), 10812, Nov. 2021, doi: 10.3390/app112210812, (Impact factor: 2.679)
- [3] Kiwon Yang, Jusung Kang, Jehyuk Jang and Heung-No Lee, "Multimodal Sparse Representation-Based Classification Scheme for RF Fingerprinting," IEEE Communications Letters, Vol. 23, Issue 5, pp. 867 - 870, Mar. 2019. (Impact Factor: 2.723)
- [4] Jusung Kang, Cheolsun Kim, Younghak Shin and Heung-No Lee, "One versus All 분류기 기반 전파 신호 송출원 식별 시스템에 관한 연구", 2020 년도 전자공학회 하계 학술대회, Aug. 19~22nd, 2020.
- [5] Jusung Kang, Haewoong Choi, Jaewon Bang, Rohit Thakur, Cheolsun Kim and Heung-No Lee, "상용 Walkie-Talkie 에 대한 천이상태 신호 기반 Radio Frequency Fingerprinting 시스템", 2016 년도 한국통신학회 동계종합학술발표회, Jan 20-22, 2016.
- [6] JuSung Kang, Kiseon Kim, and Heung-No Lee, "재구성 가능한 통신기에 대한 천이상태 신호 기반 개별 통신기 분류 시스템에 관한 연구", 대한전자공학회, 2015 년 대한전자공학회 추계학술대회, pp. 873-875, Nov. 2015.
- [7] Changyun Lee, Jusung Kang and Heung-No Lee, "Radio Frequency Fingerprinting 을 위한 비 학습 데이터 검출 및 재학습 시스템", 2019 년도 대한전자공학회 추계학술대회, Nov., 22-23th, 2019.
- [8] Changyun Lee, Jusung Kang, Haeung Choi and Heung-No Lee, "CNN 을 이용한 주파수 도약 신호 기반 RF Fingerprinting 시스템", 2019 년도 대한전자공학회 하계종합학술대회, June 26-28th, 2019.
- [9] Kiwon Yang, Jusung Kang and Heung-No Lee, "합성곱 신경망을 이용한 디지털

- 통신기 분류 알고리즘”, 2019 년도 한국통신학회 동계종합학술발표회, Jan. 23-25th, 2019.
- [10] Changyun Lee, Jusung Kang and Heung-No Lee, “천이상태 신호와 정상상태 신호를 이용한 Radio Frequency fingerprinting 시스템”, 2019 년도 한국통신학회 동계종합학술발표회, Jan. 23-25th, 2019.
- [11] Kejin Sa, Dapeng Lang, Chenggang Wang, and Yu Bai, ‘Specific Emitter Identification Techniques for the Internet of Things’, IEEE Access, Special Section on Intelligent and Cognitive Techniques for Internet of Things, 2019.12
- [12] S. Taşcıoğlu, M. Köse and Z. Telatar, "Effect of sampling rate on transient based RF Fingerprinting," 2017 10th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, 2017, pp. 1156-1160.
- [13] O. H. Tekbas, N. Serinken, O. Ureten, “An experimental performance evaluation of a novel radio-transmitter identification system under diverse environmental conditions,” Canadian Journal of Electrical and Computer Engineering., vol. 29, no. 3, pp. 203–209, 2004.
- [14] A. M. Ali, E. Uzundurukan, and A. Kara, “Assessment of features and classifiers for Bluetooth RF Fingerprinting,” IEEE Access, vol. 7, pp. 50524–50535, Apr. 2019
- [15] J. Hall, M. Barbeau, and E. Kranakis, “Detecting rogue devices in bluetooth networks using radio frequency fingerprinting,” in IASTED International Conference on Communications and Computer Networks, 2006.
- [16] P. Padilla, J.L. Padilla, J.F Valenzuela-Valdes, “Radiofrequency identification of wireless devices based on RF Fingerprinting”, Electronics Letters, 2013.10
- [17] Y. Yuan, Z. Huang, H. Wu, and W. Wang, “Specific emitter identification based on Hilbert–Huang transform-based time-frequency-energy distribution features,” IET Commun., vol. 8, no. 13, pp. 2404–2412, Sep. 2014
- [18] Y.-J. Yuan, Z. Huang, and Z.-C. Sha, “Specific emitter identification based on transient energy trajectory,” Prog. Electromagn. Res. C, vol. 44, pp. 67–82, 2013.
- [19] O.Ureten and N.Serinken, “Wireless security through RF Fingerprinting,” Canadian J. Elect. Comput. Eng., vol. 32, no. 1, Winter 2007
- [20] Q. Wu et al., “Deep learning based RF Fingerprinting for device identification and wireless security,” Electron. Lett., vol. 54, no. 24, pp. 1405–1407, 2018
- [21] K. Merchant, S. Revay, G. Stantchev, and B. Noursain, “Deep learning for RF device

- fingerprinting in cognitive communication networks,” *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 1, pp. 160–167, Feb. 2018.
- [22] K. Merchant and B. Noursain, “Enhanced RF Fingerprinting for IoT devices with recurrent neural networks,” in *IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2019, pp. 590–597.
- [23] H. Jafari, O. Omotere, D. Adesina, H. Wu and L. Qian, "IoT Devices Fingerprinting Using Deep Learning," *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, Los Angeles, CA, USA, 2018.11. pp. 1-9.
- [24] K. Youssef, et al., “Machine learning approach to RF transmitter identification,” *IEEE J. Radio Freq. Identif.*, vol. 2, no. 4, pp. 197–205, Dec. 2018.
- [25] I. Kennedy, P. Scanlon, and M. Buddhikot, "Passive steady state RF Fingerprinting: a cognitive technique for scalable deployment of cochannel femto cell underlay s, " in *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on. IEEE*, 2008, pp. 1-12
- [26] Kennedy, I.O., Scanlon, Patricia, Mullany, F.J., Buddhikot, M.M., “Radio Transmitter Fingerprinting : A Steady State Frequency Domain Approach”, *VTC*, 2008.09
- [27] K. Merchant and B. Noursain, "Securing IoT RF Fingerprinting systems with generative adversarial networks," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Norfolk, VA, USA, 2019, pp. 584–589.
- [28] Kevin Merchant and Bryan Noursain, ‘Toward Receiver-Agnostic RF Fingerprint Verification’, *2019 IEEE Globecom Workshops (GC Wkshps)*, 2019.12
- [29] Y. Li, L. Chen, J. Chen, F. Xie, S. Chen and H. Wen, "A Low Complexity Feature Extraction for the RF Fingerprinting Process," *2018 IEEE Conference on Communications and Network Security (CNS)*, Beijing, 2018.05, pp. 1-2.
- [30] L. Peng et al., “Design of a hybrid RF fingerprint extraction and device classification scheme,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 349–360, Feb. 2019.
- [31] Ryan M. Gerdes, Thomas E. Daniels, Mani Mina, and Steve F. Russel. Device identification via analog signal fingerprinting: A matched filter approach. *The 13th Annual Network and Distributed System Security Symposium*, 2006.
- [32] Scanlon, Patricia, Kennedy, Irwin O., and Liu, Yongheng: ‘Feature Extraction Approaches to RF Fingerprinting for Device Identification in Femtocells’, *Bell Labs Tech. J.*, 2010

- [33] H. J. Patel, M. A. Temple, and R. O. Baldwin, "Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinctive attribute fingerprinting," *IEEE Trans. Rel.*, vol. 64, no. 1, pp. 221–233, Mar. 2015.
- [34] Y. Jia, J. Ma, L. Gan, "Radiometric Identification Based on Low-Rank Representation and Minimum Prediction Error Regularization," *IEEE Commun. Lett.*, vol. 21, no. 8, pp. 1847-1850, Aug, 2017.
- [35] Crystal Bertoncini, Kevin Rudd, Bryan Nousain and Mark Hinders, 'Wavelet Fingerprinting of Radio-Frequency Identification (RFID) Tags', *IEEE Transactions on Industrial Electronics*, 2011.12
- [36] Vladimir Brik, Suman Banerjee, Marco Gruteser, Sangho Oh, "Wireless device identification with radiometric signatures", *MobiCom*, 2008.09
- [37] J. Gong, X. Xu, and Y. Lei, "Unsupervised specific emitter identification method using radio-frequency fingerprint embedded infogan," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2898–2913, 2020.
- [38] Y. Pan, S. Yang, H. Peng, T. Li, and W. Wang, "Specific emitter identification based on deep residual networks," *IEEE Access*, vol. 7, pp. 54 425–54 434, 2019.
- [39] Debashri Roy , Tathagata Mukherjee, Mainak Chatterjee , Erik Blasch, Fellow, IEEE, and Eduardo Pasilliao, 'RFAL: Adversarial Learning for RF Transmitter Identification and Classification', *IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING*, VOL. 6, NO. 2, JUNE 2020.
- [40] "Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Digital Mobile Radio (DMR) Systems; Part 1: DMR Air Interface (AI) Protocol," Standard ETSI TS 102 361-1, European Telecommunications Standards Institute, 2016.
- [41] L. Ding, S. Wang, F. Wang, and Z. Wei, "Specific emitter identification via convolutional neural networks," *IEEE Commun. Letters*, vol. 22, no. 12, pp. 2591-2594, Sep. 2018.
- [42] Yinghui Liu, Hau Xu, Zisen Qi, and Yunhao Shi, 'Specific Emitter Identification Against Unreliable Features Interference Based on Time-Series Classification Network Structure', *IEEE Access Special Section on Internet of Things Attacks and Defense: Recent Advances and Challenges*, 2020.11
- [43] Gianmarco Baldini and Claudio Gentile, 'Transient-Based Internet of Things Emitter Identification Using Convolutional Neural Networks and Optimized General Linear

- Chirplet Transform’, IEEE Comm. Letters, Vol. 24, No. 7, Jul. 2020.
- [44] Liting Sun , Xiang Wang, Afeng Yang, and Zhitao Huang, ‘Radio Frequency Fingerprint Extraction Based on Multi-Dimension Approximate Entropy’, IEEE Signal Processing Letters, Vol. 27, 2020.
- [45] Alghannai Aghnaya, Aysha M. Ali, and Ali Kara, ‘Variational Mode Decomposition-Based Radio Frequency Fingerprinting of Bluetooth Devices’, IEEE Access, 2019. 10
- [46] Memduh Kose, Selcuk Tascioglu, and Ziya Telatar, ‘RF Fingerprinting of IoT Devices Based on Transient Energy Spectrum’, IEEE Access 2019.01
- [47] Jiabao Yu, Aiqun Hu , Guyue Li, and Linning Peng, ‘A Robust RF Fingerprinting Approach Using Multisampling Convolutional Neural Network’, IEEE Internet of Things Journal, VOL. 6, NO. 4, AUGUST 2019
- [48] Kunal Sankhe , Mauro Belgiovine, Fan Zhou , Luca Angioloni, Frank Restuccia, Salvatore D’Oro , Tommaso Melodia, Stratis Ioannidis, and Kaushik Chowdhury, ‘No Radio Left Behind: Radio Fingerprinting Through Deep Learning of Physical-Layer Hardware Impairments’, IEEE Trans. on Cognitive Communications and Networking, Vol. 6, No. 1, Mar. 2020.
- [49] Sarankumar Balakrishnan , Student Member, IEEE, Shreya Gupta, Student Member, IEEE, Arupjyoti Bhuyan , Senior Member, IEEE, Pu Wang , Dimitrios Koutsonikolas, and Zhi Sun , Member, IEEE. ‘Physical Layer Identification Based on Spatial– Temporal Beam Features for Millimeter-Wave Wireless Networks’, IEEE Transactions on Information Forensics and Security, Vol. 15, 2020
- [50] Ya Tu, Zhen Zhang, Yibing Li, Chao Wang, and Yihan Xiao, ‘Research on the Internet of Things Device Recognition Based on RF-Fingerprinting’, IEEE Access Special Section on Intelligent and Cognitive Techniques for Internet of Things, 22 Mar. 2019.
- [51] Feiyi Xie, Hong Wen , Jinsong Wu , Songlin Chen , Wenjing Hou, and Yixin Jiang , ‘Convolution Based Feature Extraction for Edge Computing Access Authentication’, IEEE Transactions on Network Science and Engineering, Vol. 7, No. 4, Oct.-Dec. 2020
- [52] Xiang Chen and Xiaojun Hao, ‘Feature Reduction Method for Cognition and Classification of IoT Devices Based on Artificial Intelligence’, IEEE Access, Special Section on Artificial Intelligence for Physical-Layer Wireless Communications, 16 Jul. 2019
- [53] Standard for Information Technology—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications IEEE Std.

- No. 802.11-2020, Feb. 2021. Available online: <https://ieeexplore.ieee.org/document/9363693> (accessed on 15 November 2021).
- [54] Soltanieh, N.; Norouzi, Y.; Yang, Y.; Karmakar, N.C. A review of radio frequency fingerprinting techniques. *IEEE J. Radio Freq. Identif.* 2020, 4, 222–233.
- [55] Kennedy, I.O.; Scanlon, P.; Mullany, F.J.; Buddhikot, M.M.; Nolan, K.E.; Rondeau, T.W. Radio transmitter fingerprinting: A steady state frequency domain approach. In *Proceedings of the IEEE 68th Vehicular Technology Conference, Calgary, AB, Canada, 21–24 September 2008*; pp. 1–5.
- [56] Stremler, F.G. *Introduction to Communication Systems*; Addison–Wesley: Reading, MA, USA, 1990; p. 658.
- [57] Standard for Information Technology—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications IEEE Std. No. 802.11-2012, Mar. 2012. Available online: <https://ieeexplore.ieee.org/document/6178212> (accessed on 15 November 2021).
- [58] Shin, H.; Choi, K.; Park, Y.; Choi, J.; Kim, Y. Security Analysis of FHSS-Type Drone Controller. In *International Workshop on Information Security Applications*; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9503, p. 240.
- [59] Liu, Z.; Huang, Z.; Zhou, Y. Hopping instants detection and frequency tracking of frequency hopping signals with single or multiple channels. *IET Commun.* 2012, 6, 84–89.
- [60] Wang, Z.; Zhang, B.; Zhu, Z.; Wang, Z.; Gong, K. Signal Sorting Algorithm of Hybrid Frequency Hopping Network Station Based on Neural Network. *IEEE Access* 2021, 9, 35924–35931.
- [61] Li, S.; Nie, H.; Wu, H. Performance Analysis of Frequency Hopping Ad Hoc Communication System With Non-Orthogonal Multiple Access. *IEEE Access* 2019, 7, 113171–113181.
- [62] Feng, Y.; Yan, S.; Liu, C.; Yang, Z.; Yang, N. Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access. *IEEE Trans. Inf. Forensics Secur.* 2018, 14, 1670–1683.
- [63] Liu, Y.; Qin, Z.; Elkashlan, M.; Gao, Y.; Hanzo, L. Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks. *IEEE Trans. Wirel. Commun.* 2017, 16, 1656–1672.

- [64] Ghous, M.; Abbas, Z.H.; Hassan, A.K.; Abbas, G.; Baker, T.; Al-Jumeily, D. Performance Analysis and Beamforming Design of a Secure Cooperative MISO-NOMA Network. *Sensors* 2021, 21, 4180.
- [65] Mpitzopoulos, A.; Gavalas, D.; Konstantopoulos, C.; Pantziou, G. A survey on jamming attacks and countermeasures in WSNs. *IEEE Commun. Surv. Tutor.* 2009, 11, 42–56.
- [66] Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. *IEEE Commun. Surv. Tutor.* 2016, 18, 2027–2051.
- [67] Oppenheim, A.V.; Ronald, W.S.; John, R.B. *Discrete-Time Signal Processing*; Prentice Hall: Hoboken, NJ, USA, 1999.
- [68] Khan, A.; Sohail, A.; Zahoor, U.; Qureshi, A.S. A survey of the recent architectures of deep convolutional neural networks. *Artif. Intell. Rev.* 2020, 53, 5455–5516.
- [69] He, K.; Zhang, X.; Ren, S.; Sun, J. Deep residual learning for image recognition. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Las Vegas, NV, USA, 27–30 June 2016; pp. 770–778.
- [70] Szegedy, C.; Liu, W.; Jia, Y.; Sermanet, P.; Reed, S.; Anguelov, D.; Erhan, D.; Vanhoucke, V.; Rabinovich, A. Going deeper with convolutions. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Boston, MA, USA, 7–12 June 2015; pp. 1–9.
- [71] Szegedy, C.; Ioffe, S.; Vanhoucke, V.; Alemi, A. Inception-v4, Inception-ResNet and the impact of residual connections on learning. In *Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence*, San Francisco, California, USA, 4–9 February 2017.
- [72] Ioffe, S.; Szegedy, C. Batch normalization: Accelerating deep network training by reducing internal covariate shift. In *Proceedings of the International Conference on Machine Learning (ICML)*, Lille, France, 6–11 July 2015; pp. 448–456.
- [73] Kingma, D.P.; Ba, J. Adam: A method for stochastic optimization. *arXiv* 2014, arXiv:1412.6980.
- [74] Ganaie, M.A.; Hu, M.; Tanveer, M.; Suganthan, P.N. Ensemble deep learning: A review. *arXiv* 2021, arXiv:2104.02395.
- [75] Guo, J.; Nie, X.; Yin, Y. Mutual Complementarity: Multi-modal enhancement semantic learning for micro-video scene recognition. *IEEE Access* 2020, 8, 29518–29524.

- [76] Hendrycks, D.; Gimpel, K. A baseline for detecting misclassified and out-of-distribution examples in neural networks. In Proceedings of the International Conference on Learning Representations (ICLR), Toulon, France, 24–26 April 2017; pp. 1–12.
- [77] Liang, S.; Li, Y.; Srikant, R. Enhancing the reliability of out-of-distribution image detection in neural networks. In Proceedings of the International Conference on Learning Representations (ICLR), Toulon, France, 24–26 April 2017; pp. 1–27.
- [78] Lee, K.; Lee, K.; Lee, H.; Shin, J. A simple unified framework for detecting out-of-distribution samples and adversarial attacks. In Proceedings of the Neural Information Processing Systems (NIPS), Montreal, QC, Canada, 3–8 December 2018; pp. 7167–7177.
- [79] Lee, K.; Lee, H.; Lee, K.; Shin, J. Training confidence-calibrated classifiers for detecting out-of-distribution samples. In Proceedings of the International Conference on Learning Representations (ICLR), Vancouver, BC, Canada, 30 April–3 May 2018; pp. 1–16.
- [80] Hendrycks, D.; Mazeika, M.; Dietterich, T. Deep anomaly detection with outlier exposure. In Proceedings of the 7th International Conference on Learning Representations (ICLR), New Orleans, LA, USA, 6–9 May 2019; pp. 1–18.
- [81] Choi, H.; Jang, E.; Alemi, A.A. WAIC, but why? Generative ensembles for robust anomaly detection. arXiv 2018, arXiv:1810.01392.
- [82] Serrà, J.; Álvarez, D.; Gómez, V.; Slizovskaia, O.; Núñez, J.F.; Luque, J. Input complexity and out-of-distribution detection with likelihood-based generative models. In Proceedings of the International Conference on Learning Representations (ICLR), Virtual Conference, 26 April–1 May 2020; pp. 1–15.
- [83] Hinton, G.; Vinyals, O.; Dean, J. Distilling the knowledge in a neural network. arXiv 2015, arXiv:1503.02531.
- [84] Goodfellow, I.J.; Shlens, J.; Szegedy, C. Explaining and harnessing adversarial examples. In Proceedings of the 3rd International Conference on Learning Representations (ICLR), San Diego, CA, USA, 7–9 May 2015; pp. 1–11.
- [85] Bi, G.; Mitra, S.K. FFT-based sampling rate conversion. In Proceedings of the IEEE Conference on Industrial Electronics and Applications (ICIEA), Singapore, 18–20 July 2012; pp. 428–431.
- [86] Sklar, B. Digital Communications; Prentice Hall: Upper Saddle River, NJ, USA, 2001;

Volume 2, pp. 773–774.

- [87] Selvaraju, R.R.; Cogswell, M.; Das, A.; Vedantam, R.; Parikh, D.; Batra, D. Grad-CAM: Visual explanations from deep networks via gradient-based localization. In Proceedings of the IEEE International Conference on Computer Vision (ICCV), Venice, Italy, 22–29 October 2017; pp. 618–626.
- [88] J. Zhang et al., "Radio frequency fingerprints vs. physical unclonable functions – are they twins, competitors or allies?" *IEEE Network*, vol. 36, no. 6, pp. 1–9, 2022.
- [89] "IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control," *IEEE Std 802.1X-2020*, 2020.
- [90] "IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Security," *IEEE 802.1 Working Group*, 2018.
- [91] K. Seo and S. Kent, "Security architecture for the Internet protocol," *Internet Eng. Task Force*, RFC 4301, Dec. 2005.
- [92] S. Khan et al., "Survey on issues and recent advances in vehicular public-key infrastructure (VPKI)," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 1574–1601, 3rd Quart., 2022.
- [93] A. Jagannath and J. Jagannath, "Embedding-assisted attentional deep learning for real-world RF Fingerprinting of Bluetooth," *IEEE Trans. Cogn. Commun. Netw.*, vol. 9, no. 4, pp. 940–949, 2023.
- [94] Y. Zeng, Y. Gong, J. Liu, S. Lin, Z. Han, R. Cao, K. Huang, and K. B. Letaief, "Multi-Channel Attentive Feature Fusion for Radio Frequency Fingerprinting," *IEEE Trans. Wireless Commun.*, Early Access, pp. 1–1, Sep. 25, 2023.
- [95] A. Jagannath et al., "A Comprehensive Survey on Radio Frequency (RF) Fingerprinting: Traditional Approaches, Deep Learning, and Open Challenges," *Computer Networks*, vol. 219, p. 109455, 2022.
- [96] K. Sankhe et al., "Oracle: Optimized radio classification through convolutional neural networks," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, IEEE, 2019, pp. 370–378.
- [97] N. Soltani et al., "RF Fingerprinting unmanned aerial vehicles with non-standard transmitter waveforms," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15518–15531, 2020.
- [98] O. M. Gul, M. Kulhandjian, B. Kantarci, A. Touazi, C. Ellement, and C. D’amours, "Secure industrial IoT systems via RF Fingerprinting under impaired channels with

- interference and noise,” *IEEE Access*, vol. 11, pp. 26289–26307, 2023.
- [99] J. Zhang et al., “Physical layer security for the Internet of Things: Authentication and key generation,” *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 92–98, Oct. 2019.
- [100] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proc. 3rd ACM Conf. Wireless Netw. Security*, 2010, pp. 89–98.
- [101] F. Zhuo, Y. Huang, and J. Chen, "Radio frequency fingerprint extraction of radio emitter based on I/Q imbalance," in *Proc. Int. Congr. Inf. Commun. Technol. (ICICT)*, 2017, pp. 472–477.
- [102] L. Peng, J. Zhang, M. Liu, A. Hu, "Deep learning based rf fingerprint identification using differential constellation trace figure," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, 2020, pp. 1091–1095.
- [103] L. Zong, C. Xu, H. Yuan, "A rf fingerprint recognition method based on deeply convolutional neural network," in *Proc. of IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)*, 2020, pp. 1778–1781.
- [104] A. Al-Shawabka, et al., "Exposing the fingerprint: dissecting the impact of the wireless channel on radio fingerprinting," in *Proc. of IEEE Conference on Computer Communications (INFOCOM)*, 2020.
- [105] D. Roy, T. Mukherjee, M. Chatterjee, E. Pasilio, "Detection of rogue rf transmitters using generative adversarial nets," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, pp. 1–7.
- [106] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Boca Raton, FL, USA: Chapman & Hall, 2007.
- [107] D. R. Stinson, *Cryptography: Theory and Practice*, 3rd ed. Boca Raton, FL, USA: CRC Press, Nov. 2005.
- [108] M. D. Zeiler and R. Fergus, “Visualizing and understanding convolutional networks,” in *Proc. Eur. Conf. Comput. Vis.*, 2014, pp. 818–833.
- [109] J. Yosinski, J. Clune, Y. Bengio, and H. Lipson, “How transferable are features in deep neural networks?,” in *Proc. 27th Int. Conf. Neural Inf. Process. Syst.*, 2014, pp. 3320–3328.
- [110] M. Norouzi et al., "Hamming distance metric learning," in *Proc. Adv. Neural Inf. Process. Syst.*, Dec. 2012, pp. 1061–1069.
- [111] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures

- and public-key cryptosystems," *Commun. ACM*, vol. 26, no. 1, pp. 96–99, Jan. 1983.
- [112] "Secure Hash Standard," FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Apr. 1995.
- [113] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," in *Proc. Int. Conf. Learn. Represent.*, 2015.
- [114] L. van der Maaten and G. Hinton, "Visualizing data using t-SNE," *J. Mach. Learn. Res.*, vol. 9, pp. 2579–2605, Nov. 2008.
- [115] "PyCryptodome Documentation.", [Online]. Available: <https://pycryptodome.readthedocs.io/en/latest/>, Accessed on: Aug. 25, 2023,
- [116] "pyOpenSSL Documentation.", [Online]. Available: <https://www.pyopenssl.org/en/latest/index.html>, Accessed on: Aug. 25, 2023,
- [117] "Digital Signature Standard (DSS)," NIST FIPS PUB 186-4, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, 2013.
- [118] Lei, Ziwei & Yang, Peng & Zheng, Linhua & Hui, Xiong & Ding, Hong. (2019). Frequency Hopping Signals Tracking and Sorting Based on Dynamic Programming Modulated Wideband Converters. *Applied Sciences*. 9. 2906. 10.3390/app9142906.
- [119] J. Ma, B. Shi, X. Guo and Y. Wang, "An Improved Frequency Tracking Algorithm for Frequency Hopping Signals Based on ARMA Model," 2019 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Dalian, China, 2019, pp. 1-5.
- [120] K. Khanikar, R. Sinha and R. Bhattacharjee, "Sparse representation based tracking of frequency hopping primary user for cognitive radio," 2014 International Conference on Signal Processing and Communications (SPCOM), Bangalore, 2014, pp. 1-6.
- [121] Mishra, Sashikala, et al. "Improving the accuracy of ensemble machine learning classification models using a novel bit-fusion algorithm for healthcare AI systems." *Frontiers in Public Health* 10 (2022): 858282.
- [122] AbaeiKoupaei, Niloufar, and Hussein Al Osman. "A multi-modal stacked ensemble model for bipolar disorder classification." *IEEE Transactions on Affective Computing* 14.1 (2020): 236-244.
- [123] AlSalem, Thanaa Saad, Mohammed Amin Almaiah, and Abdalwali Lutfi. "Cybersecurity Risk Analysis in the IoT: A Systematic Review." *Electronics* 12.18 (2023): 3958.
- [124] Mirani, Akseer Ali, et al. "Key challenges and emerging technologies in industrial IoT

- architectures: A review." *Sensors* 22.15 (2022): 5836.
- [125] Oh, JiHyeon, et al. "A secure and lightweight authentication protocol for IoT-based smart homes." *Sensors* 21.4 (2021): 1488.
- [126] Bobde, Yash, et al. "Enhancing Industrial IoT Network Security through Blockchain Integration." *Electronics* 13.4 (2024): 687.

Curriculum Vitae

Name : Jusung Kang
Birth Date : June. 14. 1988.
Birth Place : Republic of Korea
Permanent Address : 123 Cheomdangwagi-ro (Oryong-dong), Buk-gu, Gwangju
E-mail : k92492@gist.ackr, happistday@gmail.com

Research Interests

1. Radio Frequency (RF) fingerprinting
2. Classification, Outlier Detection, Incremental Learning
3. Zero Knowledge Proof, User authentication system
4. Autonomous Driving, Collision Avoidance, Path Planning, Reinforcement Learning, SLAM, Airsim
5. IR image based Classifier and Detector

Education

2013.03 – 2024.08 School of Electrical Engineering and Computer Science,
Gwangju Institute of Science and Technology (Ph.D.)
2007.03 – 2012.02 Department of Electrical and Computer Engineering,
Ajou University (B.S.)

Patent Registrations

1. 강주성, 박진태, 이창윤, 이흥노, “다중 레이블 아웃라이어 검출 방법 및 신호 송출원 식별 모델 확장 방법”, Registration number: 10-2415975, Registration date: June 28th, 2022.
2. 강주성, 박진태, 이흥노, “양상블 기반 무선 핑거프린팅 장치 및 이를 이용한 송출원 식별 방법”, Registration number: 10-2347174, Registration date: December 30th, 2021.
3. 강주성, 이흥노, “SRC 기반의 RF 핑거프린팅 장치 및 방법”, Application number: 10-2016-0112772, Patent number: 10-1858987, Registration date: May 5th, 2018.

Awards

1. 광주과학기술원 전기전자컴퓨터공학부, GUP (Global University Project) 학업 우수상 (2015.12.22)
2. 아주대학교 전자공학과, 학업우수자 선정, 다산장학 수상 (2010 년, 2011 년)

Journal Papers (International/Domestics)

1. **Jusung Kang**, Young-Sik Kim, and Heung-No Lee, "Radio Frequency Public Key Generator for Digital Application", IEEE Access, Vol. 11, pp. 140867 - 140880, Dec. 2023, doi: 10.1109/ACCESS.2023.3340305, (Impact factor: 3.9).
2. Manjit Kaur, Dilbag Singh, Mohamed Yaseen, Vijay Kumar, **Jusung Kang**, and Heung-No Lee "Computational deep air quality prediction techniques: A systematic review", Artificial Intelligence Review, Vol. 56, pp. 2053 - 2098, Aug. 2023 (Impact factor: 12.0, Top Q1 Journal)
3. **Jusung Kang**, Younghak Shin, Hyunku Lee, Jintae Park, and Heung-No Lee, "Radio Frequency Fingerprinting for Frequency Hopping Emitter Identification", Applied Sciences, 11(22), 10812, Nov. 2021, doi: 10.3390/app112210812, (Impact factor: 2.679)
4. Kiwon Yang, **Jusung Kang**, Jehyuk Jang and Heung-No Lee, "Multimodal Sparse Representation-Based Classification Scheme for RF Fingerprinting," IEEE Communications Letters, Vol. 23, Issue 5, pp. 867 - 870, Mar. 2019. (Impact Factor: 2.723)
5. 신종목, **강주성**, 이흥노, "광 대역 통신 시스템의 협 대역 간섭 제거를 위한 압축센싱 기술 (Narrow band Interference Cancellation In Wide band Communications Using Compressed Sensing)", 대한전자공학회, 전자공학회지, Vol. 41, No. 6, pp. 67 - 75, June, 2014.

Conference Papers (International/Domestics)

1. **Jusung Kang**, Cheolsun Kim, Younghak Shin and Heung-No Lee, "One versus All 분류기 기반 전파 신호 송출원 식별 시스템에 관한 연구", 2020 년도 전자공학회 하계 학술대회, Aug. 19~22nd, 2020.
2. **Jusung Kang**, Hyunjun Han, Rohit Thakur, Nakwoo Kim, Byongtak Lee and Heung-No Lee, "컬러 영상 데이터베이스를 활용한 적외선 영상 객체 분류 신경망 학습 방법에 관한 연구", 제 18 회 전자정보통신 학술대회 (CEIC 2016), Dec. 02-03rd, 2016.
3. **Jusung Kang**, Haewoong Choi, Jaewon Bang, Rohit Thakur, Cheolsun Kim and Heung-

- No Lee, “상용 Walkie-Talkie 에 대한 천이상태 신호 기반 Radio Frequency Fingerprinting 시스템”, 2016 년도 한국통신학회 동계종합학술발표회, Jan 20-22, 2016.
4. **JuSung Kang**, Kiseon Kim, and Heung-No Lee, “재구성 가능한 통신기에 대한 천이상태 신호 기반 개별 통신기 분류 시스템에 관한 연구“, 대한전자공학회, 2015 년 대한전자공학회 추계학술대회, pp. 873-875, Nov. 2015.
 5. Hyunjun Han, **Jusung Kang**, Muhammad Asif Raza and Heung-No Lee, “Learning Through Adverse Event for Collision Avoidance: A Self-Learning Approach”, The 10th International Conference on Ubiquitous and Future Networks(ICUFN 2018), Prague, Czech Republic, Jul. 3-6, 2018.
 6. Changyun Lee, **Jusung Kang** and Heung-No Lee, “Radio Frequency Fingerprinting 을 위한 비 학습 데이터 검출 및 재학습 시스템”, 2019 년도 대한전자공학회 추계학술대회, Nov., 22-23th, 2019.
 7. Changyun Lee, **Jusung Kang**, Haeung Choi and Heung-No Lee, “CNN 을 이용한 주파수 도약 신호 기반 RF Fingerprinting 시스템”, 2019 년도 대한전자공학회 하계종합학술대회, June 26-28th, 2019.
 8. Kiwon Yang, **Jusung Kang** and Heung-No Lee, “합성곱 신경망을 이용한 디지털 통신기 분류 알고리즘”, 2019 년도 한국통신학회 동계종합학술발표회, Jan. 23-25th, 2019.
 9. Changyun Lee, **Jusung Kang** and Heung-No Lee, “천이상태 신호와 정상상태 신호를 이용한 Radio Frequency fingerprinting 시스템”, 2019 년도 한국통신학회 동계종합학술발표회, Jan. 23-25th, 2019.
 10. Giljun Jung, **Jusung Kang** and Heung-No Lee, “Prediction of Survival from Disaster with Bigdata”2019 년도 한국통신학회 동계종합학술발표회, Jan. 23-25th, 2019.
 11. Rohit Thakur, **Jusung Kang**, Hyunjun Han and Heung-No Lee, “Concurrent Food Localization and Recognition using Deep Convolution Neural Network” 2017 년도 하계종합학술대회, June 29 - July 1, 2017.
 12. Hyunjun Han, **Jusung Kang**, Rohit Thakur and Heung-No Lee, “격자구조 및 그래프 모델 기반 무인이동체 자율주행 시스템 연구” 2017 년도 항공우주시스템공학회 춘계학술대회, April 26-28th, 2017.
 13. Sangjun Park, Haeung Choi, Woong-Bi Lee, Cheolsun Kim, **Jusung Kang** and Heung-No Lee, “다중 측정 벡터 모델에 관한 최신 분석 결과 소개”, 2017 년도 하계종합학술대회, June 29 - July 1, 2017.

14. Pavel S. Ni, Sangjun Park, Hwanchol Jang, Seungchan Lee, **Jusung Kang**, Heung-No Lee, “High-Resolution Image Reconstruction from Old Video Recordings via Sparse Representation” 한국통신학회, 2015 년도 하계종합학술발표회, pp. June 24-26, 2015.
15. Hyeongho Baek, Jongmok Shin, **Jusung Kang** and Heung-No Lee, “Ultra wideband channel estimation based compressive sensing and approximate message passing (AMP) algorithm” 한국통신학회, 2014 년도 동계종합학술발표회, pp.792-793 Jan 22-24, 2014.
16. Woong-Bi Lee, **Jusung Kang**, J. Oliver, and Heung-No Lee, “협력적 무선 다중 접속 망에서 네트워크 부호를 이용한 릴레이 공격 감지 방법” 2013 하계학술대회, 한국통신학회, pp.758-759 June. 19-21, 2013.

Professional Society Activity

- | | |
|---------------------|---|
| 2021.09 ~ 2024.02 | 리버밴스(주), 연구 개발팀, 책임 연구원 |
| 2019.08. | GDG Gwangju 주관, 2019 딥러닝 여름학교 내 강화학습 개론 강의 및 해커톤 진행 |
| 2019.01. | GDG (Google Developer Group) Gwangju 주관, 강화학습 윈터스쿨 내 강화학습 기초이론 강의 |
| 2018.03. ~ 2020.03. | 광주과학기술원, 인공지능 학술 동아리, A-GIST 운영위원 (비정형&시계열 팀 리더) |
| 2016.06. ~ 2016.06. | (사)한국인지과학산업협회 인지기술 튜터리얼 13-3 차 딥러닝 실습 참가 |
| 2014.03. ~ 2015.02. | 광주과학기술원 대학원생 e-멘토단 |

Project Experiences

(비고: [PM] Project Manager, 과제 실무 총괄, [선임 연구원] 연구 주관, [참여 연구원] 연구 참여)

1. LiberVance 네트워크 기술 개발 – Layer2 플랫폼
 - 중소벤처기업진흥공단 (TIPS R&D), 2022.07 ~ 2024.06, 5 억원, 참여 연구원·PM,
2. 2022 년 AI(시)제품·서비스 제작지원
 - 인공지능산업융합사업단 (AICA), 2022.06 ~ 2022.11, 0.9 억원, 선임 연구원·PM,

3. 도약 주파수 천이 상태 신호 기반 통신망 식별을 위한 RF Fingerprinting 시스템 연구
 - LIG 넥스원, 2019.03 ~ 2021.02, 2 억원, 선임 연구원·PM,
4. 3D 영상센서와 초소형 라이다(LiDAR)를 결합한 차세대 3D 인식 복합센서모듈 기술개발
 - 한국연구재단, 2016.09 ~ 2019.07, 17 억원, 선임 연구원·PM,
5. SEC 연구소에서 활용 가능한 RF Fingerprinting 목적의 SRC S/W 개발
 - SEC 연구소, 2017.04 ~ 2017.12, 0.5 억원, 참여 연구원,
6. 에너지 IoT 디바이스 진단·관리를 위한 기초 연구
 - ETRI, 2016.06 ~ 2016.11, 0.4 억원, 선임 연구원,
7. [EW11] 통신 신호 특성 분석 및 인식 알고리즘 연구
 - 국방과학연구소, 2013.11 ~ 2015.12, 3.2 억원, 선임 연구원·PM,
8. 전파신호식별 및 초분광이미징에 특화된 지능형 신호 복원 및 분류 시스템 연구
 - 한국연구재단 (중견 후속), 2021.03 ~ 2024.02, 8.9 억원, 참여 연구원,
9. 레이더, 분광기, 뇌컴퓨터 인터페이스 시스템에 특화된 지능형 신호 복원 및 분류 시스템 연구
 - 한국연구재단 (중견 후속), 2018.03 ~ 2021.02, 8.4 억원, 참여 연구원,
10. 부호 이론적 다중 압축 센싱 시스템 개발 연구 (후속)
 - 한국연구재단 (중견 후속), 2015.05 ~ 2018.04, 8.4 억원, 참여 연구원,
11. 부호 이론적 다중 압축 센싱 시스템 개발 연구
 - 한국연구재단 (중견 신규), 2013.03 ~ 2015.04, 6 억원, 참여 연구원,

Acknowledgement

13년 03월 시작하여 24년 08월 마무리 하게 된 약 10여년 간의 학위 과정은 저와는 다른 생각의 다양한 사람들과 함께 연구하고 토론하며 생각의 영역을 넓힐 수 있는 값진 경험이었습니다. 센서 지능화 솔루션 연구를 주제로 수행한 RF 신호, 이미지, 초분광 신호, 초음파 신호 등 다양한 센서를 이용한 연구 경험은 저를 졸업 후 어떤 연구에도 전념할 수 있는 탄탄한 기반 지식을 지닌 연구자로 만들었습니다. 나아가 군, 정출연, 사기업 등 다양한 소속의 연구자들과의 협업을 통해 다른 사람의 생각을 이해하고 원활한 연구 진행을 위한 중요한 점들을 깨달을 수 있었습니다. 이러한 경험에 기반하여, 마침내 길었던 학위 과정을 무사히 마칠 수 있음에 감사하며, 과정에 있어 도움을 주신 수 많은 분들께 다음과 같이 감사 인사를 드리고자 합니다.

가장 먼저, 연구자로서의 가르침을 주시고 학위 과정을 지원해주신, 지도교수 이흥노 교수님께 감사의 인사를 드립니다. 교수님께서 항상 말씀주신, ‘Read’, ‘Think’, and ‘Writing’ 원칙은 연구로 생각이 복잡할 때 마다 정리할 수 있게 도와준 핵심 원칙이 되었습니다. 자기 주장이 강한 저를 끝까지 믿고 지원해주셔서 감사합니다. 더불어 학위논문 심사위원을 흔쾌히 맡아주신 ‘신종원 교수님’, ‘황의석 교수님’, ‘김종원 교수님’, 그리고 멀리 DGIST로부터 직접 가르침을 주신 ‘김영식 교수님’께 감사의 인사를 드립니다.

학위 과정동안 동거동락하며 지낸 INFONET 구성원 여러분께 감사 인사를 드립니다. 입학하여 적응하느라 바쁠 때, 연구자로서 지녀야 할 자세에 대해 말씀해주신 환철이형, 진택이형께 감사드립니다. 두 선배님 덕분에 일찍 적응할 수 있었던 것 같습니다. 다음으로 연구 주제 및 연구실 생활에 있어서의 많은 조언을 주신, 영학이형, 웅비형께 감사의 인사를 드립니다. 두 선배님은 앞으로도 제 마음속에 사수로 간직하고자 합니다. 또한 힘들때 불평 불만을 들어주시고, 극복하기 위한 여러 말씀을 주신 상준이형, 승찬이형께도 감사를 표합니다. 마지막으로, 연구실 생활을 같이하며 여러 연구 및 실무를 같이

진행한 Pavel 형, 해웅이, 재혁이, 철순이에게도 고마움을 전하고자 합니다. 여러분이 배려해주지 않았으면 학위 과정을 무사히 마치지 못했을 것이라 생각합니다. 이밖에도 일찍 적응할 수 있도록 여러 자리를 마련해주신 정민선배, 형호형, 수길이형께 감사의 말을 전하고자 하며, 동기 및 부사수로 여러 연구를 같이 수행한 종목이, 승윤이, 기원이, 창윤이, 형주, 지오, 영인이에게도 감사를 표하고자 합니다. 더불어 현재 연구실에서 학위과정 중인 지오, 영인이, 승민이, 수민이에게도 고마움을 표합니다. 바쁘단 핑계로 많은 것을 알려주지 못하고 졸업하는 것 같아 미안함을 같이 표하며, 앞으로도 치열하게 고민하고 행동하여 결과를 만들어내 학위를 잘 마무리 할 수 있기를 응원하는 바입니다.

학위 과정동안 도움을 받은 연구실 밖에서 만난 인연들에 대해서도 감사함을 표합니다. 먼저 대학원 생활 동안 여러 어려움을 나누며 말동무가 되어주었던 동기들, 준형이형, 동원이형, 성현이, 문도, 정현이형, 종목이, 원석이에게 고마움을 표합니다. 술 한잔 나누며 이야기한 많은 것들이 학위과정 동안 생각의 사고를 넓히고 어려움을 극복하는 데 원동력이 되었던 것 같습니다. 다음으로 타 연구실임에도 불구하고 졸업후에도 후배 연구자의 어려움을 살피고 용기를 북돋아주신 충재형, 용훈이형, 효영이형에게도 큰 감사의 마음을 전하고자 합니다. 주기적으로 오셔서 해주셨던 여러 말씀과 응원은 학위 말미를 견디고 마무리하는데 큰 도움이 되었습니다. 또한 학부 시절부터 이어진 인연으로 학위과정 내내 응원과 용기를 보내준 기석이형, 강석이형에게도 깊은 고마움을 전합니다. 두 분 덕분에 과거 즐거웠던 기억을 추억하며 힘을 내어 학위 과정을 마무리 할 수 있었습니다. 마지막으로 외부 연구 커뮤니티 활동을 통해 맺은 인연에 대해서도 감사의 마음을 전합니다. 학위 말미에 GDG (Google Developer Group) Gwangju 및 A-GIST (Artificial General Intelligence Study Team) 연구 스터디 활동을 하였으며, 이 과정에서 인연을 맺은 용이님, 동현님, 형욱님, 동원이형, 종훈님, 성한님, 양우님, 락훈님, 송준호님, 최준호님에게도 감사를 표합니다. 상기 활동은 담보 상태에 있던 연구 진행에 있어 깊은 통찰을 얻는 귀중한 인연이 되었으며, 여러분을 통해

깨달은 ‘Learn to Share, Share to Learn’ 정신은 앞으로의 연구 활동에 있어 귀중한 기준점이 될 것임을 믿어 의심치 않습니다.

길어지는 학위 과정에 있어서도 온전히 저를 믿고 응원해주신 아버지, 어머니, 그리고 누나에게 깊은 감사의 마음을 표합니다. 내색하지 않으려 노력했음에도 불구하고 표가 낮을 스트레스 표출 상황에서도 같이 공감해주시며 꾸준한 응원을 보내주셨음을 인지하고 있으며, 이러한 응원이 없었으면 절대 학위과정을 마무리 하지 못했을 것임을 잘 알고 있습니다. 이 자리를 표해 가족으로부터 받은 깊은 사랑에 감사한 마음을 전하며, 앞으로 한 사람의 연구자로서 열심히 생활하며 받은 사랑에 보답할 수 있는 막내가 되겠습니다.

마지막으로, 고마우신 분들이 너무 많지만 미처 기술하지 못한 다른분들께도 양해의 말씀과 함께 이 자리를 빌어 감사의 마음을 전합니다.

2024년 06월 강주성 올림.