New Frontier of Communication Security on Radio Frequency Fingerprints Concealment

Zhisheng Yao, Yu Wang, Guan Gui, Shiwen Mao, and Xinbin Wang

Abstract

Due to device-specific defects introduced during the hardware manufacturing process, the radio frequency fingerprint (RFF) can be extracted to identify wireless devices and further avoid spoofing attacks. Many effective RFF identification methods have been proposed based on either machine learning or deep learning. However, from the perspective of communication security, if the RFF of the transmitter can be easily extracted and identified, attackers can disguise themselves as legitimate transmitters by impersonating RFF and other means, thereby undermining the security of wireless communications. Therefore, concealing the RFF of legitimate transmitters from detection and camouflage attacks has become a highly challenging issue in the field of wireless communications. This article presents an active RFF concealment (RFFC) method, which removes the nonlinear features of the transmitter system, thereby preventing attackers from obtaining the transmitter's RFF and ensuring the identity security of the transmitter. To evaluate the performance of RFF concealing technology, we simulate seven types of RFFC systems, and collect datasets without and with RFFC technology. The simulation results show that the performance of traditional transmitter identification methods decreases sharply after RFFC. Especially in low signal-to-noise ratio environments and complex multipath channel conditions, the proposed RFFC technology makes the RFF features chaotic and difficult to detect, leading to dramatically reduced effectiveness of existing transmitter identification methods.

Introduction

With the rapid development of wireless communications, many new wireless network technologies are constantly emerged and gradually integrating into various aspects of people's daily lives, which represents the arrival of the Internet of Things (IoT) era, including smart homes, smart cities, advanced healthcare, connected cars and so on, collectively constructing a world of ubiquitous connectivity [1]. With vigorous development of the fifth-generation mobile communication technology (5G) in many countries today, the emerging industries represented by the IoT are thriving. With the development of the sixth generation mobile communication technology (6G), a series of IoT applications are expected to further enhance their connectivity and achieve large-scale interconnection [2]. Wireless networks facilitate information exchange within open communication media, while this openness brings about significant information security risks. When illegal users obtain network access rights by bypassing legitimate wireless access authentication mechanisms, they can launch attacks on the wireless network, endangering communication security of legitimate users. As a result, the legitimate user information may be stolen, abused, or tampered with.

In the past decade, the field of wireless communications has been extensively studied with respect to physical layer security technologies. Various physical features, such as variations and randomness of the channel noise and the unique fingerprints of hardware devices, have been leveraged to achieve encryption, authentication, and malicious node identification at the physical layer [3]. Specifically, radio frequency fingerprinting (RFF) is considered an effective method for enhancing the security of wireless networks. RFF is caused by the tiny differences among wireless devices during manufacturing and processing, which result in subtle but unique differences when these devices' transmitted signals. These inherent and unique RFF features can be used to identify wireless devices.

In order to further investigate the process of RFF generation, researchers have attempted to model the generation process of RFF. They use theoretical analysis and construction of simulation datasets to study this field in more detail. Yu *et al.* [4]analyzed the impact of various components in the structure of a universal zero intermediate frequency digital communication transmitter on RFF and established the corresponding time-domain baseband models for RFF through MATLAB. And they provided upper and lower bounds for parameters such as DC bias, in-phase/quadrature (I/Q) gain imbalance, I/Q quadrature offset error, I/Q filter deviation, oscillator phase noise, and power amplifier (PA) nonlinearity parameters. Jia *et al.* [5] used the square integral bispectral (SIB) of the signal as the feature vector for RFF signal, and used a support vector machine (SVM) classifier for identification. Wang *et al.* [6] proposed an efficient RFF identification method based on complex-value neural network (CVCNN) and network compression technology. In the field of communication interference identification, Liu *et al.* [7] focus on the vulnerability of adversarial attacks faced by deep learning-based aviation transportation commu-

Zhisheng Yao, Yu Wang, and Guan Gui are with Nanjing University of Posts and Telecommunications, China; Shiwen Mao is with Auburn University, USA; Xianbin Wang is with Western University, Canada.

Digital Object Identifier: 10.1109/MWC.015.2300550

1536-1284/24/$25.00 © 2024 IEEE

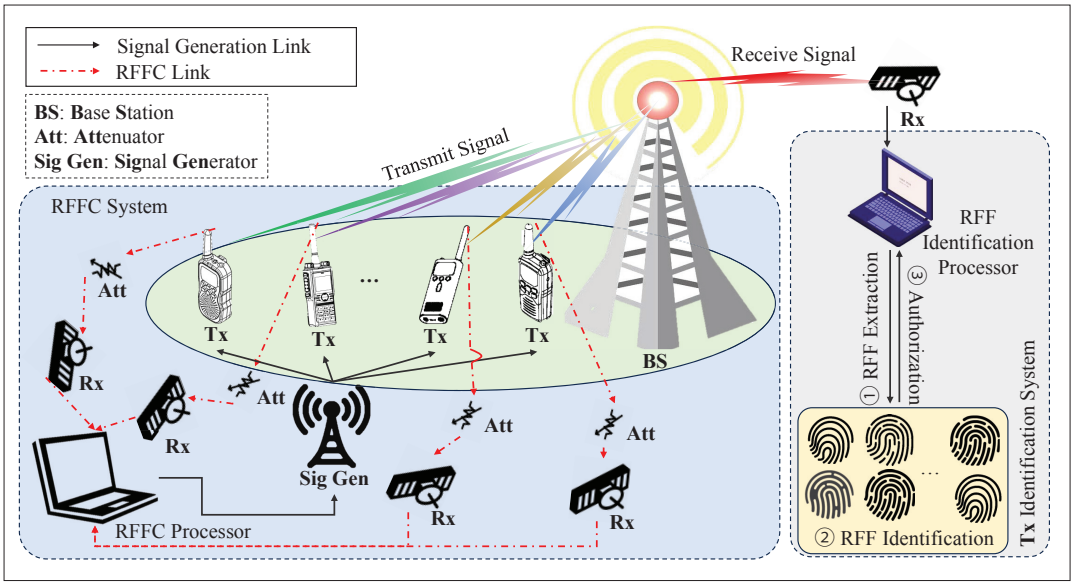

FIGURE 1. Overview of RFFC system and transmitter identification system.

nication interference identification models, and introduce a new dual layer attack method that combines dynamic iterative step size adjustment and class feature analysis to improve the effectiveness of attacks.

However, with the continuous improvement of wireless device hardware performance and the enhancement of software-defined capability, malicious users may adopt various methods to obtain the RFF of the target device, and then use signal processing and hardware reconstruction methods to disguise as the target device, thereby attacking legitimate users. Therefore, it is crucial to develop effective techniques to conceal RFF from detection and impersonation by malicious users.

In this article, we focus on how to use RFF concealment (RFFC) technology to actively conceal the RFF of transmitters, ensuring that the identity information of the transmitter be hard to identify. First, we introduce an RFFC model for wireless transmitters and use it as a basis to analyze the mechanism of RFF generation, which helps us to establish the corresponding transmitter baseband RFF model. Next, we present the proposed RFFC technique, including the principles, structures, and algorithm. Subsequently, we simulate seven different types of transmitter, and make them work separately in the original state and the state under RFFC technology. Then we evaluate the effectiveness of RFFC on transmitters identification using currently widely adopted machine learning-based and deep learning-based methods. Experimental results validate that RFFC can effectively protect RFF from detection and impersonation by malicious users, and reduce the identifiability of the transmitter. Finally, we discusse important challenge for future research.

System Model

Figure 1 shows the RFFC system and transmitter identification system of wireless transmitters. Specifically, before the baseband signal is transmitted to the base station, it is first processed by the RFFC processor, which can generate a signal with opposite RFF characteristics to the transmitter, and then input the signal that has undergone RFFC processing into the transmitter and transmit it to the base station. It is worth noting that the RFFC processor must perform RFFC processing on each baseband signal to be input to the transmitter to ensure that the opposite RFF characteristics carried by the RFFC signal are adapted to the RFF characteristics of each transmitters. Subsequently, it is necessary to obtain transmission signals from each transmitters, and use the attenuator to reduce the signal power to an acceptable range of the receiver. The receiver transmits the received signal to the RFFC processing system to assist in updating the feedback of the corresponding RFFC model for each transmitter.

In the transmitter identification system, the radio frequency (RF) signal from the base station is first received by the receiver. Then, the RFF identification processor extracts the transmitter's RFF for device identification and authentication by analyzing the transmitter's communication signal. Similar to different people having different fingerprints, different transmitters also have different RFFs, which can be used for transmitter identification and authentication. However, for signals whose RFF has been concealed, the RFF information will not be visible. Therefore, traditional RFF identification methods will not be able to identity and authenticate transmitters.

RFF Model

The yellow section in Fig. 2 shows the block diagram of a typical digital communication transmitter. Specifically, the analog circuit components of the transmitter, which are marked in gray background in the block diagram, are the primary sources of RFF. The I/Q digital baseband signals from the digital communication transmitter are converted into analog signals through a digital to analog converter (DAC), where they may have DC bias errors and a certain level of harmonic distortion. Next, the analog signals pass through the intermediate frequency (IF) filter, where the frequency response errors of both I and Q IF filters are introduced. The imbalance of this I/Q filter is usually considered frequency dependent, so the imbalance in I/Q manifests differently at different frequencies.

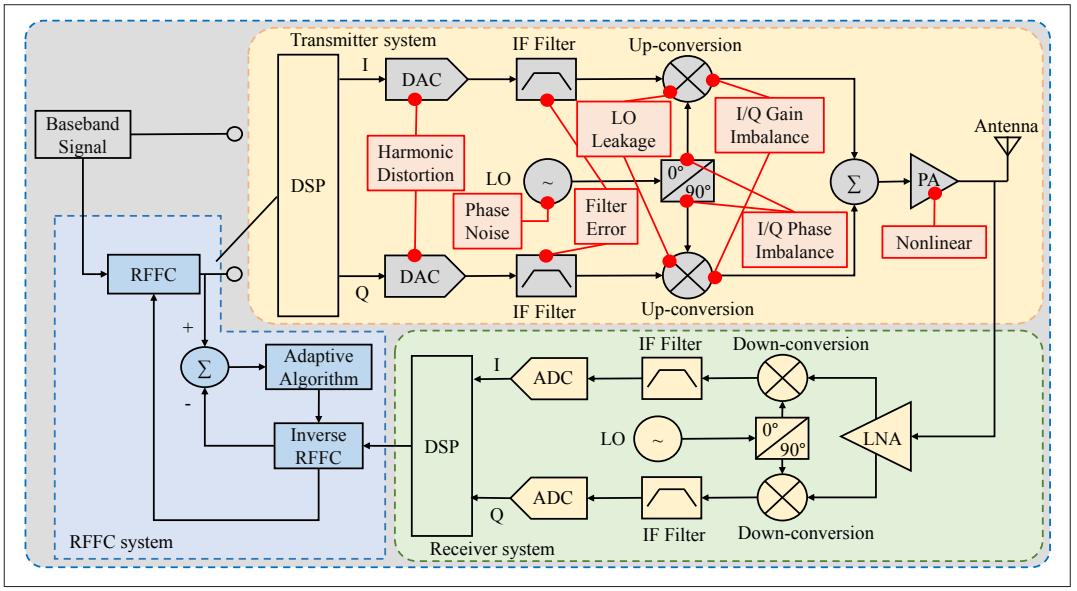

FIGURE 2. RFFC system block diagram for wireless transmitters.

Subsequently, the analog signals are up-converted to the appropriate transmission frequency range using the mixer. However, there is phase noise in the RF local oscillator of the transmitter, leading to carrier phase jitter. The carrier signal is then phase-shifted by 90 degrees to form two sets of modulated carriers, which are used to modulate the analog signals of the I and Q channels, respectively. However, in practice, due to phase deviation, the phase difference between the I/Q modulated carriers is usually not exactly 90 degrees, resulting in a certain degree of orthogonal offset error, which disrupts the orthogonality of the I and Q channels. Additionally, the mixers in the I/Q paths often exhibit gain mismatches, leading to I/Q gain imbalances of the output signals. Finally, after the I and Q signals are combined, they need to be amplified by the RF front-end PA to the appropriate output power for long-distance transmission. During the signal amplification process, PA typically brings a certain degree of nonlinear effects, resulting in out-of-band spectral proliferation, which is also a crucial factor that affects the transmitter's RFF. Ultimately, the amplified signal is radiated into the air through the antenna [4].

In summary, the distortions caused by defects in transmitter hardware are referred to as RFF. Specifically, the primary source of RFF is the nonlinear distortion of the PA in the RF front-end of the transmitter. Therefore, the modeling of transmitter RFF is often simplified as modeling the PA nonlinearity. In addition, the IQ gain imbalance caused by the mixer and the IQ phase imbalance caused by the orthogonal modulator are also important components of the transmitter RFF, and are usually considered the main source of RFF and an important part of RFF modeling.

RFFC Technology

In this section, we primarily focus on RFFC for digital communication transmitters. In Fig. 2, we demonstrate an RFFC system block diagram used in wireless transmitters, which is the block in blue. The PA, mixer and quadrature modulator play crucial roles in transmitter identification, with their nonlinearity, IQ gain imbalance, and IQ phase imbalance distortion as important sources of RFF. In recent years, several techniques have emerged to alleviate nonlinear distortion, including power back-off techniques, feedforward linearization techniques, feedback linearization techniques, and pre-distortion techniques [8]. Specifically, the pre-distortion technique has shown many advantages in mitigating nonlinear distortion [9], such as handling wider bandwidth signals, achieving high efficiency, and simplicity in implementation, making it the most popular solution for addressing nonlinear distortion. Considering the real-time and lightweight requirements of RFFC, the RFFC method in this article focuses on system linearization schemes based on digital pre-distortion (DPD).

RFFC Principle

The overall structure of Fig. 2 adopts indirect learning architecture (ILA) to learn the RFF characteristics of the transmitter for RFFC. Specifically, before feeding the signal into the transmitter, it undergoes processing through an RFFC processor with system linearization function. The design and implementation of RFFC processors are based on the principles of DPD technology. Through detailed analysis and modeling of the transmitter's RFF, a nonlinear transformation function opposite to the transmitter's RFF is designed, and the inverse model of the transmitter's behavior model is constructed to ensure that the baseband signal is processed by RFFC and generates a concealed signal with completely opposite characteristics to the transmitter's RFF. As the signal is transmitted, The RFF features carried by concealed signals cancel out the RFF features of the transmitter, making it difficult for the receiver to identify the transmitter via its RFF, thus ensuring the efficacy of RFFC.

In order to obtain an RFFC model with opposite RFF characteristics of the transmitter, it is first necessary to build a receiving feedback system to capture the RFF information in the current transmission signal. This process involves the output signal of the transmitter being attenuated by a low noise amplifier (LNA), followed by down conversion and IF filtering, and then converted into a digital signal through analog-to-digital conversion (ADC). The

digital signal is then input into the RFFC system, providing the necessary data foundation for training the RFFC model.

In the RFFC system, the transmitter's RFF is learned by analyzing the output and input signals of the transmitter, and the nonlinear behavior of the transmitter is modeled, that is, the inverse RFFC model. This inverse RFFC model undergoes optimization through adaptive algorithms to refine its effectiveness. Once the inverse RFFC model is determined, using the principle of equivalence between the inverse model and the original model, the inverse RFFC model is placed at the front end of the transmitter as an RFFC processing unit. Consequently, when the baseband signal is processed through this RFFC unit, the resultant signal emerges from the transmitter does not contain identifiable RFF characteristics, thereby preserving the confidentiality of the transmitter's identity information. The specific algorithm procedure is shown in Algorithm 1.

Require:
- Determine the structure of the RFFC model;
- Obtain the Tx inputs signals and Tx outputs signals;

[Inverse RFFC model training]:

1. Determine the structure of the inverse RFFC model;

2. Take the Tx output signal as the inverse RFFC model input, and let the inverse RFFC model predict the Tx input signal;

3. Optimize the inverse RFFC model;

[RFFC model deployment]:

1. Transform the inverse RFFC model into the forward RFFC model;

2. Deploy the RFFC model to the front end of the Tx, to let the digital baseband signal pass through the RFFC unit before Tx.

ALGORITHM 1. Training and deployment procedure of RFFC method.

RFFC Algorithm

With the development of digital processing algorithms, memory polynomials have become a common method for the nonlinear modeling of PA, utilizing adaptive algorithms for parameter fitting to learn the coefficients of these polynomials. With the development of deep learning, PA nonlinear modeling based on neural networks (NN) beginning to emerge. Based on this technology, this article first performs an inverse modeling of PA nonlinearity, namely the RFFC inverse model in Fig. 2. By inverting this inverse model as the RFFC model, the digital baseband signal intended for transmission undergoes RFFC preprocessing through this RFFC model, so that the signal entering the transmitter link has the opposite characteristics of RFF, thereby achieving RFFC.

Parameter fitting adaptive algorithms typically include algorithms such as least squares (LS) algorithm [9] and recursive least squares (RLS) algorithm [10] based on generalized memory polynomial. The LS algorithm aims to minimize the sum of squares error between measured values and theoretical values by finding the best function match of the data, thereby achieving accurate fitting of parameters. This method performs significantly well with sufficient sample size, but its accuracy is limited when the sample size is insufficient. Therefore, directly using the LS algorithm to calculate the coefficient of the RFFC model may not be suitable for actual hardware implementation. In contrast, the RLS algorithm enhances the parameter estimation process by recursively updating estimates, which markedly reduces computational complexity and accelerates the calculation process. This not only effectively overcomes the limitations of LS algorithm in terms of sample size and computational complexity, but also makes it suitable for hardware implementation.

Due to the fact that memory polynomials simulate the nonlinear characteristics of PA through polynomials, their model performance significantly decreases when dealing with strongly nonlinear of PA. In addition, the high correlation between its basis functions limits the further improvement of model performance. Therefore, considering that NN are particularly suitable for modeling strongly nonlinear devices due to their large structure, numerous parameters, and strong nonlinear fitting ability, this article explores the performance of three different NN models as RFFC models. The first model adopts a real-valued focused time-delay neural network (RVFTDNN) [11] architecture, consisting of three connected layers. The input includes the I value, Q value, and high-order variables of the current time and its past times, and the output is the predicted value of the next time. The second model is an RFFC model based on bidirectional long short term memory (BiLSTM) [12] network , which simulates the memory effect of PA through a sequence to sequence regression network, with inputs containing past and current time samples. The last model uses a real valued time delayed convolutional neural network (RVTDCNN) [13] as the backbone network, and the input data is organized into a graph containing IQ components and current and past signal envelope related terms. This model has lower complexity compared to the RVFTDNN and BiLSTM.

In order to further improve the performance of RFFC, other distortion factors such as IQ imbalance distortion caused by quadrature modulators [14], and even the distortion caused by carrier frequency offset can be considered [15]. However, concealing IQ imbalance distortion typically requires additional feedback circuits, and suppressing carrier frequency offset requires channel estimation. These are time-consuming and increases the system complexity and hardware overhead, and may also lead new errors. Considering that IQ imbalance distortion and carrier frequency offset are not the main sources of RFF, in order to reduce the complexity and hardware overhead of RFFC systems, this article does not introduce concealment algorithms specifically designed for IQ imbalance distortion and carrier frequency offset.

Data Generation and Preprocessing

We use Mathworks' simulink to simulate the RFFC system of digital communication transmitters. Specifically, we use the idealized baseband library from the RF Blockset for equivalent baseband modeling. The input signal is a complex-modulated signal containing the information to be transmitted, centered around the carrier frequency. The modules in the idealized baseband library do not consider out of band behavior or stray harmonics generated by nonlinear effects or interference signals. In addition, the modules in the idealized baseband library do not simulate impedance mismatch and assume that all modules are perfectly matched.

The simulation system includes a 16-QAM signal generator. Also, it includes I/Q modulators, PA

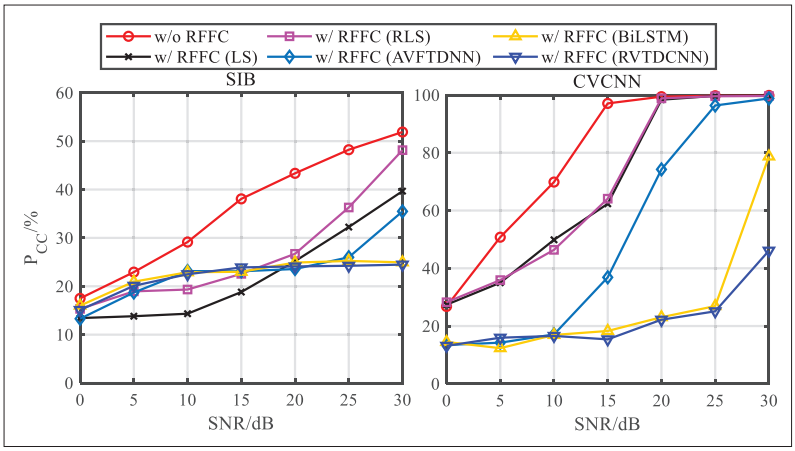

FIGURE 3. Transmitter identification performance by different transmitter identification methods under RFFC.

models, mixers, couplers, and S parameter blocks which represent antenna load effects. The receiver link performs a down-conversion from RF to low intermediate frequency. Specifically, the PA model includes Polynomial, Saleh, and Rapp. The nonlinear characteristics in different transmitters can be simulated by setting the parameters of the PA model, and the IQ gain imbalance and IQ phase imbalance characteristics in different transmitters can be simulated by setting the IQ imbalance parameters of the mixer. The filter is Butterworth filter.

In particular, this article simulates seven different types of transmitter and generated datasets using RFFC techniques based on LS, RLS, RVFTDNN, BiLSTM, and RVTDCNN, respectively, to study the impact of RFFC techniques on transmitter identification performance. Finally, 42 datasets of seven types of transmitters working on normal and RFFC states are obtained through simulation. Furthermore, we preprocess the obtained datasets to make each type of dataset contain 1000 samples, each with a length of 1000 sample points. We convert the complex values of the channel into signals composed of real and imaginary parts of two channels to meet the requirements of machine learning and deep learning model-based transmitter identification. Then, we add additive Gaussian white noise (AWGN) to the ideal simulation dataset, with the noise signal-to-noise ratio (SNR) gradually increasing from 0 dB to 30 dB in steps of 5 dB.

Experimental Results

Transmitter Identification Performance under RFFC

In this section, we focus on the transmitter identification performance under RFFC. For comparison, we use machine learning-based algorithms as benchmarks. First, we extract SIB features of the transmitter's RFF and then utilize a SVM for transmitter identification [5]. Additionally, we experiment with deep learning algorithms. We focused on the transmitter identification performance based on CVCNN [6]. Specific experimental results are presented in Fig. 3.

The experimental results show that the performance of deep learning identification methods based on CVCNN is generally better than that of machine learning identification methods based on SIB. However, at low SNR, both transmitter identification methods fail due to the increase of AWGN. After using RFFC technology, the transmitter identification performance decreases sharply, especially the RFFC method based on RVTDCNN and BiLSTM has the most significant effect, even at high SNR. Specifically, under the SIB based machine learning transmitter identification method, when the SNR is below 20 dB, the transmitter identification accuracy for various RFFC methods does not exceed 30 percent. Under the deep learning identification method based on CVCNN, the RFFC method based on RVTDCNN and BiLSTM performs the best. When the SNR is below 25 dB, the transmitter identification accuracy is only about 20 percent. The RFFC method based on RVFTDNN slightly worse, and its RFFC effect gradually manifests when the SNR is below 20 dB. The RFFC method based on LS and RLS has the worst performance, only causing a certain degree of decline in the CVCNN identification method when the SNR is below 20 dB.

The confusion matrix in Fig. 4 shows the impact of RVTDCNN-based RFFC technology on the transmitters identification performance of based on CVCNN when the SNR is 15 dB. It can be observed that after using RFFC technology, the transmitter identification method is completely ineffective, and traditional training and testing methods are no longer able to build a model that can accurately identify the transmitter. We conclude that as RFFC reduces the transmitter's identifiability and effectively safeguarding the transmitter's identity information. It is an effective security measure.

Transmitter RFF Extraction Performance under RFFC

In this section, we further explore the effectiveness of RFFC by extracting the RFF of the transmitter. As shown in Fig. 5, we demonstrate the changes in depth features extracted by CVCNN when SNR is at 15 dB and different RFFC techniques are used. It can be seen that with the gradual enhancement of RFFC technology, the intra class distance of this feature is constantly increasing, the inter class distance is constantly decreasing, the overall feature becomes more chaotic, and the discrimination between features is decreasing. At the same time, we introduce the silhouette coefficient (SC) index to evaluate the clustering effect of features, with a value range of [–1, 1]. The closer the value approaches 1, the better the cohesion and separation. From the values of SC in Fig. 5, after using RFFC, the SC values sharply decrease, indicating a significant reduction in the discriminability of RFF features.

Transmitter Identification Performance under Different Channel Conditions

Considering that the complexity and variability of wireless channels in real-world environments can have an impact on transmitter identification, this article demonstrates the performance of CVCNN-based transmitter identification methods under different multipath fading channel conditions, both without RFFC and with RVTDCNN-based RFFC, through Fig. 6. The results indicate that as the multipath effect increases, the transmitter identification performance continues to decline. Specifically, when using RFFC technology based on RVTDCNN and under

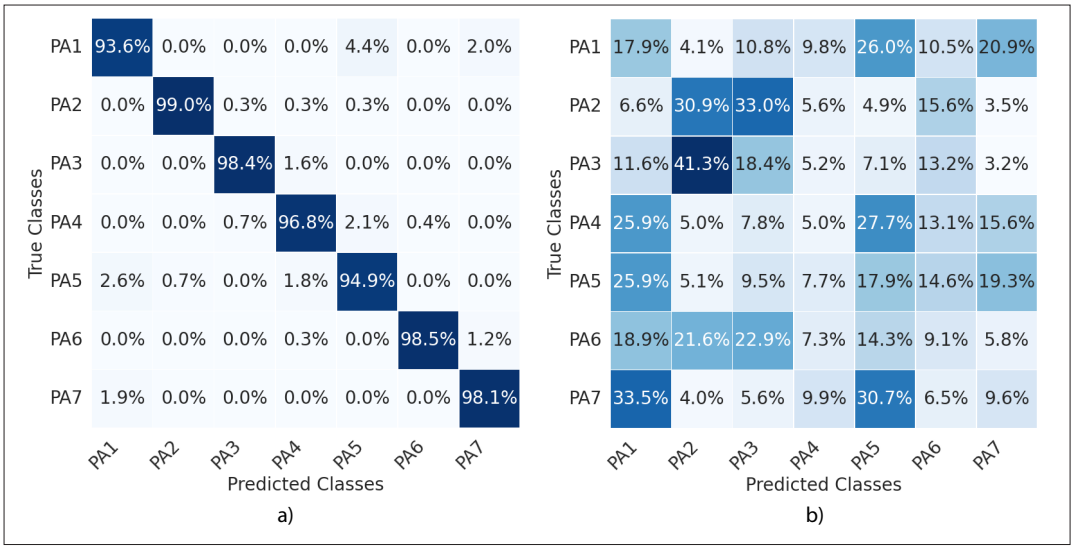

FIGURE 4. Confusion matrix for CVCNN-based transmitter identification under RVTDCNN-based RFFC technology with SNR of 15 dB. Specifically, the identification accuracy from (a) to (b) are 97.1 % to 15.4 % (↓81.7 %): a) w/o RFFC; (b) w/ RFFC (RVTDCNN).

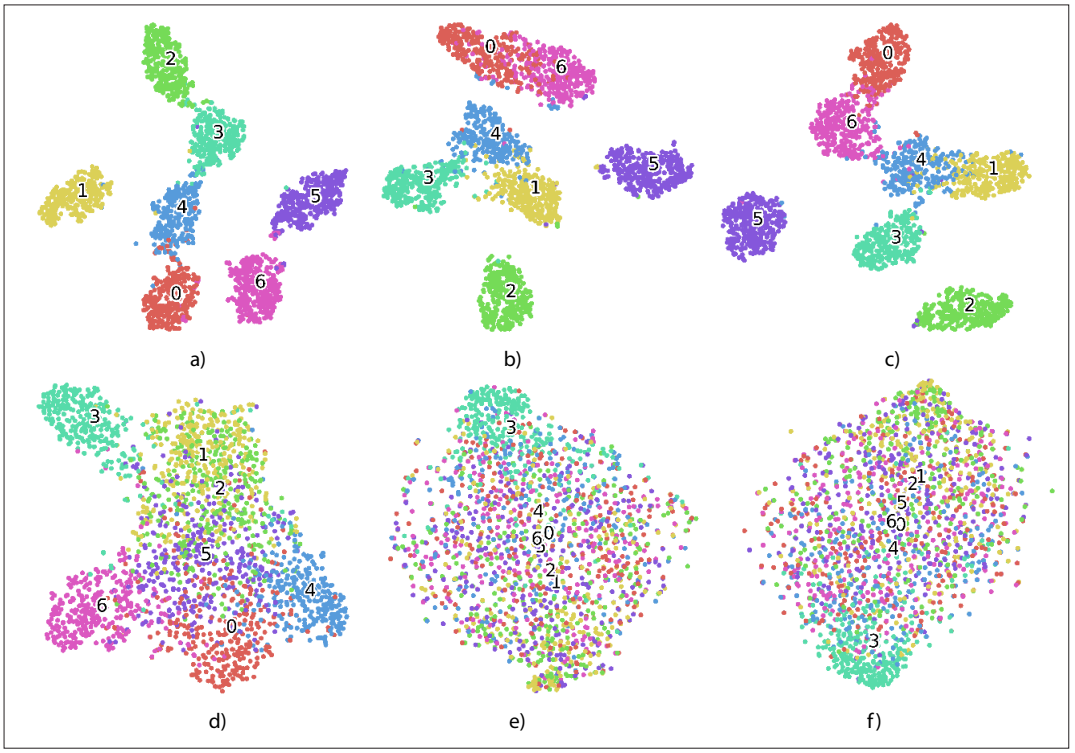

FIGURE 5. Visualization of RFF high-dimensional features by CVCNN-based transmitter identification methods under different RFFC technology with SNR of 15 dB. Specifically, their SC from (a) to (f) are 0.41, 0.30 (↓0.09), 0.33 (↓0.07), 0.01 (↓0.40), -0.03 (↓0.44) and -0.04 (↓0.45): a) w/o RFFC; b) w/ RFFC (LS); c) w/ RFFC (RLS); d) w/ RFFC (RVFTDNN); e) w/ RFFC (BiLSTM); f) w/ RFFC (RVTDCNN).

complex multipath channel conditions, the transmitter identification method based on CVCNN performs extremely poorly.

Future Research Challenges

In this section, we discuss research challenges related to the future use of RFFC to protect RFF from malicious user detection and disguise, in order to avoid transmitter identity leakage and related security.

Diversified Wireless Channel Environment

Future wireless communication environments will become increasingly diverse, with respect to different frequency bands, protocols, and device types, as well as the impact of various interference factors in the actual environment, such as multipath propagation, noise interference, signal attenuation, and so on. Channel fingerprint concealment techniques are crucial with strong adaptability and wide applicability to cope with the impact of channel diversity and maintain efficient RFFC performance.

Lightweight RFFC Techniques for Low Power and

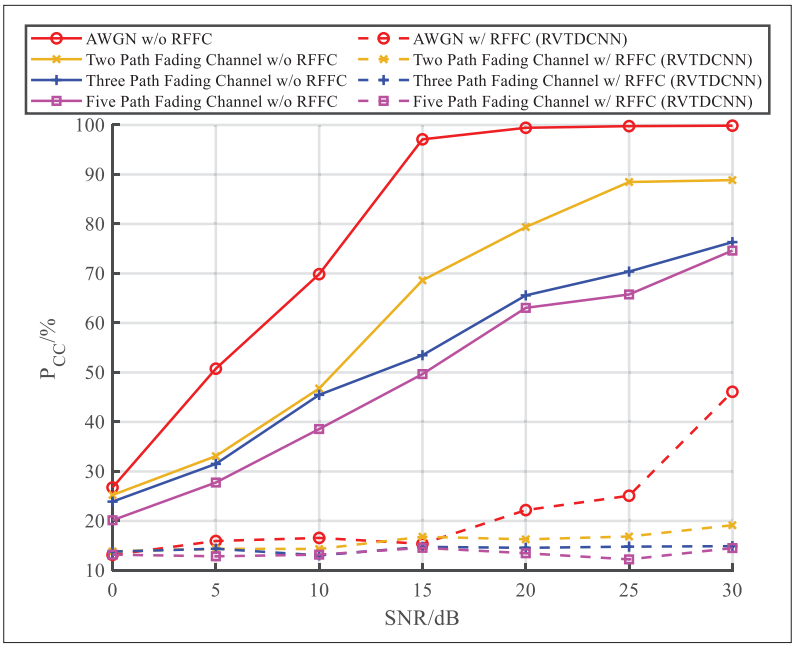

FIGURE 6. Transmitter identification performance under different channel conditions.

Resource Constrained Devices

In IoT and embedded systems, devices often have limited energy and computational resources, and RFF characteristics are constantly changing. Therefore, future research needs to address how to implement effective RFFC techniques in such resource constrained scenarios, and how to design a light and efficient algorithm for real-time RFF concealing to protect such devices from detection and spoofing attacks.

Key Management

RFFC can be integrated with key management systems, by treating the concealed RFF content as a special type of key. To ensure the security of encryption and decryption keys for communication, only devices with legitimate fingerprints can obtain access keys. Therefore, the protection of keys is of utmost importance. The key management system must ensure the security of RFF concealed content in key storage and transmission to prevent leakage or misuse.

Conclusions

This article presented an RFFC technology that effectively conceals the RFF of a transmitter, for protecting the transmitter's identity information and reducing its identifiability, which provided a fresh perspective and solution for issues related to transmitter identity protection and information security in the field of wireless communication. The article focus on the mechanism of RFF generation in digital communication transmitters, and elaborate on the principles, architecture, and algorithms of RFFC technology. Using Mathworks' Simulink, we model seven types of digital communication transmitters and conduct simulations of RFFC systems, and conduct experimental verification in different SNR environments and different channel conditions. Experimental results show that under RFFC technology, both machine learning-based and deep learning-based transmitter identification methods suffer significantly degraded, especially in low SNR environments and complex multipath channel conditions where transmitters are almost unidentifiable. Additionally, the extracted RFF high-dimensional features became more unstable and chaotic. Finally, we discuss future research challenges, including adapting to diverse wireless channel environments, developing lightweight RFFC techniques for low power and resource constrained scenarios, and emphasizing the importance of key management systems. These challenges will drive the future development in RFFC, addressing the growing demands for communication security, and ensuring the safety and privacy of communications in the era of the IoT.

References

[1] J. M. Stocchero *et al.*, "Secure Command and Control for Internet of Battle Things Using Novel Network Paradigms," *IEEE Commun. Mag.*, vol. 61, no. 5, May 2023, pp. 166–72.

[2] M. Giordani *et al.*, "Toward 6G Networks: Use Cases and Technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, Mar. 2020, pp. 55–61.

[3] N. Wang *et al.*, "Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities," *IEEE Internet of Things J.*, vol. 6, no. 5, Oct. 2019, pp. 8169–81.

[4] J. Yu *et al.*, "Time-Domain Baseband Modeling of Radio Frequency Fingerprint for Zero-If Digital Communication Transmitter," *J. Terahertz Science and Electronic Information Technology*, vol. 19, no. 4, Aug. 2021, pp. 603–16.

[5] J. Jia and L. Qi, "RF Fingerprint Extraction Method Based on Bispectrum," *J. Terahertz Science and Electronic Information Technology*, vol. 19, no. 1, 2021, pp. 107–11.

[6] Y. Wang *et al.*, "An Efficient Specific Emitter Identification Method Based on Complex-Valued Neural Networks and Network Compression," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 8, June 2021, pp. 2305–17.

[7] M. Liu *et al.*, "Adversarial Attack and Defense on Deep Learning for Air Transportation Communication Jamming," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 1, Jan. 2024, pp. 973–86.

[8] H. Li *et al.*, *Digital Front-End in Wireless Communication and Broadcasting: Introduction to Wireless Communications and Digital Broadcasting*, Cambridge UK: Cambridge University Press, 2011, pp. 3–27.

[9] D. R. Morgan *et al.*, "A Generalized Memory Polynomial Model for Digital Predistortion of RF Power Amplifiers," *IEEE Trans. Signal Process.*, vol. 54, no. 10, Oct. 2006, pp. 3852–60.

[10] Y. Qian, Q. Li, and T. Yao, "Analysis of Different Predistortion Structures and Efficient Least-Square Adaptive Algorithms," *Proc. 2003 IEEE Int'l. Conf. Acoustics, Speech, and Signal Processing*, 2003, Hong Kong, 2003, pp. II–461.

[11] M. Rawat and F. M. Ghannouchi, "A Mutual Distortion and Impairment Compensator for Wideband Ddirect-Conversion Transmitters Using Neural Networks," *IEEE Trans. Broadcast.*, vol. 58, no. 2, June 2012, pp. 168–77.

[12] J. Sun *et al.*, "Behavioral Modeling and Linearization of Wideband RF Power Amplifiers Using BiLSTM Networks for 5G Wireless Systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, June. 2019, pp. 10348–56.

[13] X. Hu *et al.*, "Convolutional Neural Network for Behavioral Modeling and Predistortion of Wideband Power Amplifiers," *IEEE Trans. Neural. Netw. Learn. Syst.*, vol. 33, no. 8, Aug. 2022, pp. 3923–37.

[14] Y. D. Kim *et al.*, "Adaptive Compensation for Power Amplifier Nonlinearity in the Presence of Quadrature Modulation/Demodulation Errors," *IEEE Trans. Signal Process.*, vol. 55, no. 9, August. 2007, pp. 4717–21.

[15] X. Wang, P. Ho, and Y. Wu, "Robust Channel Estimation and ISI Cancellation for OFDM Systems With Suppressed Features," *IEEE J. Sel. Area. Commun.*, vol. 23, no. 5, May. 2005, pp. 963–72.

Biographies

Zhisheng Yao [S] received his Bachelor's degree in Electronic Information Engineering from Nanjing University of Posts and Telecommunications in 2022. He is currently pursuing a Ph.D. at the same university. His research interests include wireless communications, physical layer security, intelligent signal processing, radio frequency fingerprinting, communication security, and digital predistortion technology.

Yu Wang [M] received the Ph.D. degree in Signal and Information Processing from Nanjing University of Posts and Telecommunications, Nanjing, China in 2023. Since 2023, he has been a specially-appointed professor with the Nanjing University of Posts and Telecommunications, Nanjing, China. He has published more 50 papers in peer-reviewed IEEE journal/conferences and received 6 best paper awards. His research interests include deep learning, optimization, and its application in wireless communications.

Guan Gui [F] received the Ph.D. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2012. From 2009 to 2014, he joined Tohoku University as a research assistant as well as a postdoctoral research fellow, respectively. From 2014 to 2015, he was an Assistant Professor at the Akita Prefectural University, Akita, Japan. Since 2015, he has been a professor at Nanjing University of Posts and Telecommunications, Nanjing, China. His recent research interests include intelligence sensing and recognition, and physical layer security. He has published more than 200 IEEE Journal/Conference papers and won several best paper awards, for example, ICC 2017, ICC 2014 and VTC 2014-Spring. He received the IEEE Communications Society Heinrich Hertz Award in 2021, the Clarivate Analytics Highly Cited Researcher in Cross-Field in 2021-2023. Since 2022, he has been a Distinguished Lecturer of the IEEE Vehicular Technology Society.

Shiwen Mao [F] received his BE and ME degrees in Electronic Engineering and a BEc in Enterprise Management from Tsinghua University. He earned an MS in Systems Engineering and a Ph.D. in Electrical Engineering from NYU Tandon. He is a Professor at Auburn University and Director of the Wireless Engineering Research and Education Center. His research interests include wireless networks, multimedia communications, and smart grid. He is a Fellow of IEEE, IET, and AAIA, has held IEEE leadership roles, and published over 200 papers with numerous awards.

Xianbin Wang [F] is a Full Professor and Tier-1 Canada Research Chair at Western University, specializing in 5G/6G, wireless security, and IoT. He received his Ph.D. from the National University of Singapore in 2001. He was a Senior Research Scientist at CRC Canada and a system designer at STMicroelectronics. He has published over 400 papers, holds over 30 patents, and received numerous awards, including multiple IEEE Best Paper Awards. He is a Fellow of IEEE, the Canadian Academy of Engineering, and the Engineering Institute of Canada.