Radio Frequency Fingerprint Identification for Narrowband Systems, Modelling and Classification

Junqing Zhang, Roger Woods, *Senior Member, IEEE,* Magnus Sandell, *Senior Member, IEEE,* Mikko Valkama, *Senior Member, IEEE,* Alan Marshall, *Senior Member, IEEE,* and Joseph Cavallaro, *Fellow, IEEE*

***Abstract*—Device authentication is essential for securing Internet of things. Radio frequency fingerprint identification (RFFI) is an emerging technique that exploits intrinsic and unique hardware impairments as the device identifier. The existing RFFI literature focuses on experimental exploration but comprehensive modelling is missing. This paper systematically models impairments of transmitter and receiver in narrowband systems and carries out extensive experiments and simulations to evaluate their effects on RFFI. The modelled impairments include oscillator imperfections, imbalance of inphase (I) and quadrature (Q) branches of mixers and power amplifier (PA) nonlinearity. We then propose a convolutional neural network-based RFFI protocol. We carry out experimental measurements over three months and demonstrate that oscillator imperfections are not suitable for RFFI due to their unpredictable time variation caused by temperature change. Our simulation results show that our protocol can classify 50 and 200 devices with uniformly and randomly distributed IQ imbalances and PA nonlinearities with high accuracy, namely 99% and 89%, respectively. We also show that the RFFI has some tolerance on different receiver imbalances during training and classification. Specifically, the accuracy is shown to degrade less than 20% when the residual receiver's gain and phase imbalances are small. Based on the experimental and simulation results, we made recommendations for designing a robust RFFI protocol, namely compensate carrier frequency offset and calibrate IQ imbalances of receivers.**

***Index Terms*—Device authentication, radio frequency fingerprint identification, RF impairment, narrowband, convolutional neural network**

I. Introduction

Internet of things (IoT) has digitally transformed our everyday life which aims to connect everything and everyone. Many exciting IoT applications such as smart home, smart cities, connected healthcare, industry 4.0, etc. are enabled by a wide range of IoT devices [1]. Cisco predicts that there will be 300 billion IoT devices by 2030[1], mainly connected wirelessly thanks to the easy installation and deployment. However, the broadcast nature of wireless transmissions makes device authentication challenging as any malicious users can access the network. Devices are conventionally authenticated by cryptographic schemes, which rely on a commonly pre-shared key and software address. However, key management and distribution become challenging for IoT devices, as many of them will be low-cost and distributed in remote areas [2]. Software address, such as MAC/IP address, is not encrypted and can be spoofed easily.

A new and secure device authentication method is thus urgently needed and should be designed to be tamper-proof. It should ideally be lightweight, because many IoT devices are low-cost with limited computational and power resources and some are required to work for over 10,000 hours on a coin cell battery [3]. Radio frequency fingerprint identification (RFFI) has emerged as a promising candidate [4], [5], which exploits the unique hardware features of transceiver devices as their identifiers. These features are produced because of the manufacturing process variations, which cannot be eliminated even with advanced manufacturing technologies. The hardware features deviate from the nominal values and will slightly affect the waveform of wireless transmissions, but the deviation is within such a small range that it does not affect the normal communication operation. As these impairments are unique, stable and difficult to tamper with, they can be extracted as device identifiers.

Many IoT techniques, for example, ZigBee, Bluetooth, LoRa, and Sigfox, only require a low communication rate as the payload is short. These techniques are usually narrowband. For example, LoRa only occupies a bandwidth of 125, 250 or 500 kHz, and supports a bit rate ranging from 0.24 - 37.5 kbps[2]. It can be used to transmit environmental monitoring information such as temperature. RF impairments of narrowband techniques consist of oscillator imperfections such as carrier frequency offset (CFO) and phase noise, mixer imperfections including inphase (I) and quadrature (Q) imbalance, power amplifier (PA) nonlinearity as well as antenna patterns [6]. The

Manuscript received xx, 2020; accepted xx, 2020. Date of publication xx, 2020; date of current version xx, 2020. The work was supported in part by the UK Royal Society Research Grants under grant ID RGS/R1/191241 and in part by the National Key Research and Development Program of China under grant ID 2020YFE0200600. The associate editor coordinating the review of this paper and approving it for publication was xxx. *(Corresponding author: Junqing Zhang.)*

J. Zhang and A. Marshall are with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom. (e-mail: junqing.zhang@liverpool.ac.uk; alan.marshall@liverpool.ac.uk)

R. Woods is with the School of Electronics, Electrical Engineering and Computer Science at the Queen's University Belfast, Belfast, BT9 5AG, United Kingdom. (e-mail: r.woods@qub.ac.uk)

M. Sandell is with the Bristol Research and Innovation Laboratory, Toshiba Research Europe Ltd., Bristol BS1 4ND, United Kingdom. (e-mail: magnus.sandell@toshiba-bril.com)

M. Valkama is with the Tampere University, 33720 Tampere, Finland. (e-mail: mikko.valkama@tuni.fi)

J. Cavallaro is with the Department of Electrical and Computer Engineering, Rice University, Houston, USA. (e-mail: cavallar@rice.edu)

Digital Object Identifier xxx

[1]https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/big-data/solution-overview-c22-740248.html

[2]https://www.semtech.com/products/wireless-rf/lora-transceivers/sx1272

emitted signal of IoT devices will be distorted by the above transmitter impairments. A receiver will capture the physical waveform and extract these impairments to infer the device identity.

Modelling RF impairments is important to understand the behavior of hardware impairments and the capacity of RFFI. While there is detailed general RF impairments modelling [6]–[9], the modelling for RFFI is rather limited or only partially complete. For example, the work in [10], [11] modelled RF impairments but did not examine their individual and overall impacts on the RFFI. In addition, other work focused on only one single transmitter impairment, for example, CFO [12]–[15], IQ imbalance [11], [12], [16], PA nonlinearity [17]–[21], antenna pattern [22], [23]. However, transmitter impairments are twisted with each other and coexist in practical systems. The overall effects of these impairments require further investigation. Finally, there is very limited work on receiver impairments [11], [24]. In practice, different receivers may be used for RFFI and their impairments will interfere with the extraction of transmitter impairments. This important aspect is not properly modelled and explored yet. However, if we are to achieve progress and create a system to efficiently exploit RFFI, we need an effective model that is backed up and based on solid research.

In summary, this paper starts to address the need for the design of a robust RFFI protocol by providing a comprehensive study of RF impairments modelling in the RFFI context. This paper carries out a systematic modelling of both transmitter and receiver impairments in narrowband systems as well as comprehensive experimental and simulation validation for their effects on RFFI. Specifically, we create a model that involves the major RF impairments that are exploited for RFFI in the literature, including oscillator imperfections [12]–[15], IQ gain and phase imbalances [11], [12], [16], and PA nonlinearity [17]–[21]. We study the impact of individual and overall impairments as well as other relevant configurations such as the transmission power (backoff level of PA), signal-to-noise ratio (SNR), payload pattern and length. We finally make design guidelines for a practical and robust RFFI system. Our detailed contributions are as follows.

- We carry out six experiments over three months using five LoRa devices and demonstrate that CFO is time-varying and not suitable for classifying low-cost IoT devices. In addition, we show that CFO interferes with other RF impairments.
- Extensive simulations are carried out to validate the effects of transmitter impairments including IQ imbalances and PA nonlinearities. We show that our RFFI protocol can classify 50 devices of uniformly distributed impairments with accuracies as high as 99% at SNR of 20 dB.
- Extensive simulations are carried out to study the effects of receiver impaired by IQ imbalances. It demonstrates that, for the first time, when the receiver IQ imbalances are within a limited range, that is, the gain and phase imbalances were within the range of [-0.2 0.2] dB and [-1 1] degree, respectively, the classification accuracy is compromised by less than 20%.

As the RF impairments cannot be reconfigured or customized, the following recommendations have been identified for designing a robust RFFI protocol:

- Estimate and compensate CFO before RFFI in order to avoid CFO interfering with other RF impairments.
- Calibrate IQ imbalance of the receiver in advance for obtaining low residual IQ imbalances to minimize the impact of different receivers.

The rest of the paper is organized as follows. Section II introduces the related work. Section III presents the overview of RFFI systems, which consists of transmitter and receiver impairments and the RFFI protocol. Specifically, transmitter impairments are modelled in Section IV while Section V models the receiver impairments and introduces the RFFI protocol. Section VI explains the simulation setup. The experimental and simulation results are given in Section VII. Section VIII concludes the paper.

II. Related Work

RFFI research can be generally categorized into experimental-based studies and model-based work. The former constitutes the majority of the current literature, which uses IoT devices as devices under test (DUTs) and software defined radio (SDR) platforms, for example, universal software radio peripheral (USRP) or high specification equipment such as oscilloscope as receivers. RFFI has been applied to ZigBee [24]–[26], WiFi [12], [14], [15], [27]–[29], and LoRa [30]. These research efforts validate the practicability of RFFI.

RFFI is a multi-class classification problem and state-of-the-art machine learning and deep learning algorithms can be leveraged. Specifically, classic machine learning algorithms such as support vector machine (SVM) [12], [30], random forest and decision tree [27], [31], are used. However, the work usually relies on the handcrafted features, which will be twisted with each other and accurate estimation of individual feature will be challenging in some cases. It also requires a good understanding of the underlying communication protocols. On the other hand, deep learning algorithms can take the raw signals directly and extract the hidden features, which can significantly decrease the development overhead and difficulty. Deep learning is hence widely used for RFFI, including convolutional neural network (CNN) [26], [29], [30], [32], [33], long short-term memory (LSTM) [11], [34], and gated recurrent units (GRU) [34].

The transmitter impairments are the intrinsic and unique features of each device that RFFI aims to exploit as device identifiers. Specifically, CFO has been extracted to classify WiFi devices [15]. Wong *et al.* [16] designed an IQ imbalance-based RFFI. Hanna *et al.* [18] used the Saleh model to depict the PA nonlinearity in narrowband systems while Polak *et al.* [17] used Volterra series to represent the memory effects of a PA in a wideband system. The Taylor polynomial model has also been used to model the PA memory effects [19]–[21]. The radiation patterns of antennas have also been explored for RFFI [22], [23].

The receiver impairments also affect the RFFI performance. In practical applications, the manufacturers may carry out the

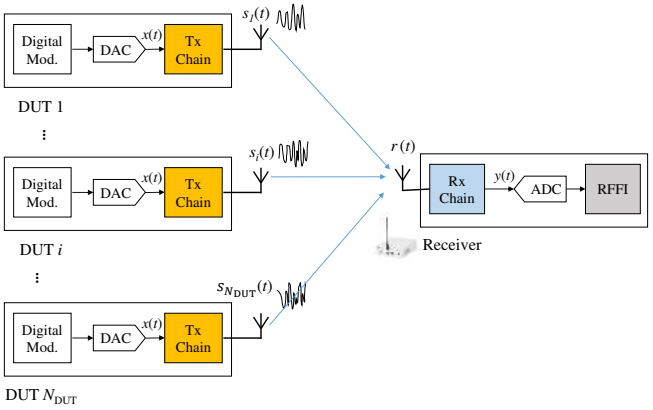


Fig. 1. System overview.

RFFI training using a high specification receiver to capture wireless signals, and provide the training information to customers. The users are likely to use their own receivers for classification. Another example is that roaming IoT devices will access the network from different base stations/access points, hence the RFFI will be carried out via different receivers. However, because received signals will be impacted by receiver impairments, different receivers will probably interfere with the recognition of the transmitter impairments. There are very few efforts on this challenge. He *et al.* [11] employed multiple distorted receivers and used information fusion to combine their results. However, the same receiver sets were used for training and classification. Peng *et al.* [24] used two different USRP SDR platforms for training and classification and demonstrated the performance is only slightly affected. Nevertheless, proper modelling of the receiver impairments is missing and the effect of different receivers for training and classification on the RFFI is not clear.

III. System Overview

The overview of an RFFI system is shown in Fig. 1. There are N_{DUT} DUTs with different hardware impairments, such as IQ mismatch and PA nonlinearity. The i^{th} DUT will emit modulated signals, $s_i(t)$, which will be captured by a receiver. Based on the received signal, $r(t)$, the receiver tries to identify the slight differences among the RF impairments and deduce the transmitter identity using the RFFI protocol.

For each DUT, the transmitted signal is first modulated digitally, for example, using 16 quadrature amplitude modulation (16QAM) or quadrature phase shift keying (QPSK). It is then converted to the analog domain by a digital-to-analog converter (DAC). The analog signal, $x(t)$, further undergoes upconversion and power amplification, and is finally emitted by an antenna. The overall effects of these analog processes can be expressed as

$$s_i(t) = \mathcal{F}_i(x(t)), \tag{1}$$

where $\mathcal{F}_i(\cdot)$ denotes combined effects of the transmitter chain of i^{th} DUT. Each DUT is subject to hardware impairments during the manufacturing process and this paper focuses on modelling and analyzing oscillator imperfections, IQ mismatch and PA nonlinearity as they are the most common impairments for RFFI, which will be done in Section IV.

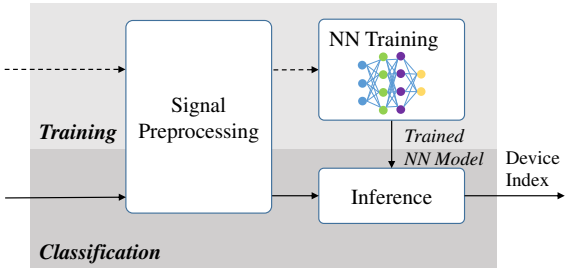


Fig. 2. A deep learning-based RFFI protocol.

The signal reaching the receiver will undergo channel effects. In a narrowband system, the received signal can be given as

$$r(t) = h(t)s_i(t) + n(t), \tag{2}$$

where $h(t)$ is the channel effect and $n(t)$ is the additive white Gaussian noise (AWGN), that is, $n(t) \sim \mathcal{CN}(0, \sigma_n^2)$.

Once the receiver captures the signal $r(t)$, it is processed by the receiver chain in the analog domain such as downconversion and demodulation, which yields

$$y(t) = \mathcal{G}(r(t)), \tag{3}$$

where $\mathcal{G}(\cdot)$ represents the overall receiver chain effect. The receiver impairments are modelled in Section V-A.

Based on the received signal $y(t)$, the receiver aims to infer the identity of the DUT using RFFI. As shown in Fig. 2, a deep learning-based RFFI protocol consists of two stages, namely training and classification. During the training stage, a receiver, acting as an authenticator, will collect sufficient packets from each DUT and use these packets to train a neural network (NN) model. The training only needs to be done offline and for one time. Signal preprocessing algorithms are adopted consisting of packet detection and synchronization, CFO estimation and compensation. At the classification stage, a DUT will emit a wireless signal and the receiver will classify the origin based on the received waveform and the pre-trained NN model. A CNN-based RFFI protocol will be designed in Section V-B. Compared with traditional schemes, CNN-based RFFI protocol does not need handcrafted features. In addition, CNN has been applied with great success in image classification, speech recognition, natural language processing, etc. Its excellent classification capability can also be leveraged for RFFI.

IV. Transmitter Impairments

The architecture of the direct (homodyne) conversion transmitter is portrayed in Fig. 3. The impairment modelling is based on the general RF impairments modelling for a direct conversion transmitter [6], [8], [35]–[37], with a special focus on the oscillator imperfection including CFO and phase noise, mismatch of I and Q branches, and PA nonlinearity, as they are the main features studied for RFFI.

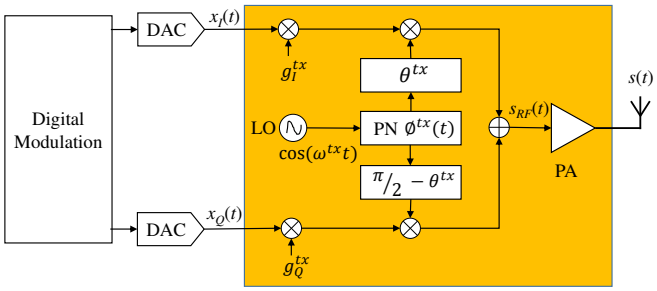


Fig. 3. Transmitter chain with hardware impairments.

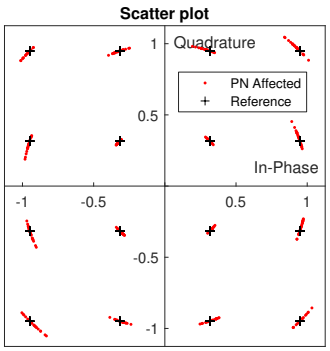


Fig. 4. Phase noise effect. Constellation change due to phase noise.

A. Oscillator Imperfection

A crystal local oscillator (LO) generates sinusoidal waves with the required carrier frequency, which is used for upconversion at the transmitter. It usually employs a phase-locked loop (PLL) circuit to synthesize the carrier frequency.

The frequency stability, δf, represents the variation of the frequency output of a LO, which can be quantified in the parts per million (ppm). The frequency offset will satisfy [38]

$$-\frac{\delta f}{10^6} \times f_c^0 \leq \Delta f \leq +\frac{\delta f}{10^6} \times f_c^0, \tag{4}$$

where f_c^0 is the reference nominal frequency. The output frequency can then be given as

$$f_c = f_c^0 + \Delta f. \tag{5}$$

Besides the frequency offset, the LO is also affected by the phase noise, $\phi(t)$. The phase noise can be characterized by single sideband noise spectral density and has the unit of decibels below the carrier per Hertz (dBc/Hz). It can be modelled as a filtered Gaussian noise. Both CFO and phase noise will bring a phase shift to the constellation points. For example, the effect of phase noise is shown in Fig. 4.

Based on the above analysis, the carrier at the transmitter side can be mathematically expressed as

$$\Omega^{tx}(t) = \cos(\omega^{tx}t + \phi^{tx}(t)), \tag{6}$$

where

$$\omega^{tx} = 2\pi(f_c^0 + \Delta f^{tx}), \tag{7}$$

and Δf^{tx} is the frequency offset of the transmitter.

B. IQ Imbalance at Mixer

The transmitter uses a quadrature mixer to upconvert the signals from the baseband to the RF band. There will often be mismatch/imbalance between the I and Q branches.

The transmitter will digitally modulate the payload using, for example, QAM, and convert the modulated signals by a DAC to

$$x(t) = x_I(t) + jx_Q(t), \tag{8}$$

where $x_I(t)$ and $x_Q(t)$ are the modulated signals at I and Q branches, respectively. The signal is upconverted from the baseband to the RF band. The RF band signal at the mixer in the presence of IQ imbalance and oscillator imperfections can be given as [39]

$$\begin{aligned} s_{RF}(t) =& g_I^{tx} x_I(t)\cos(\omega^{tx}t + \phi^{tx}(t) + \theta^{tx}) - \\ & g_Q^{tx} x_Q(t)\sin(\omega^{tx}t + \phi^{tx}(t) - \theta^{tx}), \end{aligned} \tag{9}$$

where g_I^{tx} and g_Q^{tx} are the I and Q gains, respectively, $\psi^{tx} = 2\theta^{tx}$ is the IQ phase mismatch. The IQ gains in the linear scale at the transmitter can be given as [40]

$$g_I^{tx} = 10^{\left(0.5\frac{G^{tx}}{20}\right)}, \tag{10}$$

$$g_Q^{tx} = 10^{\left(-0.5\frac{G^{tx}}{20}\right)}, \tag{11}$$

where G^{tx} is the gain imbalance in dB at the transmitter.

The equivalent baseband signal of $s_{BB}(t)$ can be given as

$$s_{BB}(t) = s_I(t) + js_Q(t). \tag{12}$$

The signal in (9) can be rewritten as

$$\begin{aligned} s_{RF}(t) &= s_I(t)\cos(\omega^{tx}t + \phi^{tx}(t)) - s_Q(t)\sin(\omega^{tx}t + \phi^{tx}(t)) \\ &= \Re\{s_{BB}(t)e^{j(\omega^{tx}t + \phi^{tx}(t))}\}, \end{aligned} \tag{13}$$

where $\Re\{\cdot\}$ denotes the real part operation, and

$$s_I(t) = g_I^{tx} x_I(t)\cos(\theta^{tx}) + g_Q^{tx} x_Q(t)\sin(\theta^{tx}), \tag{14}$$

$$s_Q(t) = g_I^{tx} x_I(t)\sin(\theta^{tx}) + g_Q^{tx} x_Q(t)\cos(\theta^{tx}). \tag{15}$$

The baseband signal can be rearranged as

$$s_{BB}(t) = g_I^{tx} x_I(t)e^{j\theta^{tx}} + jg_Q^{tx} x_Q(t)e^{-j\theta^{tx}}. \tag{16}$$

In the simulation of wireless transmissions, complex forms of the signal and channel are more commonly used because of the elegant mathematical expression. Therefore, from now on, we denote the signal of the RF band as

$$s_{RF}(t) = s_{BB}(t)e^{j(\omega^{tx}t + \phi^{tx}(t))}. \tag{17}$$

The effect of the IQ imbalance is illustrated in Fig. 5. As shown in Fig. 5(a), a positive/negative gain imbalance will bring a horizontal/vertical stretch. The phase imbalance will result in constellation rotation, which can be observed in Fig. 5(b).

As shown in Figs. 5(c) and 5(d), when the gain imbalance of a transmitter, G^{tx}, is within [-5 5] dB, or the phase imbalance, ψ^{tx}, is within [-30 30] degree, these imbalances do not cause a severe impact on the bit error rate (BER) for a 16QAM system at an SNR of 10 dB. In addition, the BER when there are both gain and phase imbalances is given in Figs. 5(e) and 5(f). The

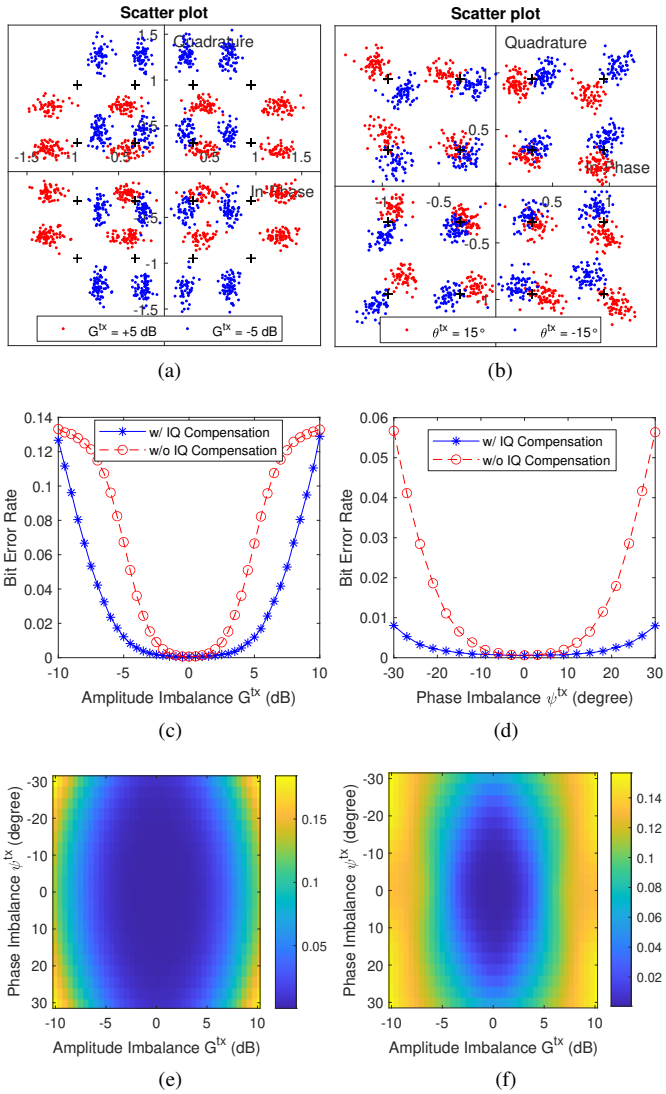


Fig. 5. IQ imbalance of mixers impairment. (a) Constellation change with gain imbalances. SNR $\gamma = 20$ dB. (b) Constellation change with phase imbalances. SNR $\gamma = 20$ dB. (c) BER versus gain imbalance. SNR $\gamma = 10$ dB. (d) BER versus phase imbalance. SNR $\gamma = 10$ dB. (e) BER versus gain and phase imbalance with IQ compensation. (f) BER versus gain and phase imbalance without IQ compensation.

BER is only compromised by 1% when IQ compensation is adopted [41].

It should be noted that IQ compensation will always be adopted by a receiver in practical systems [41]. However, as the IQ imbalances are part of the intrinsic hardware impairments that we aim to exploit for RFFI, we employ raw signals without IQ compensation, which can be implemented independently from, and in parallel with, normal receiver operations.

C. Power Amplifier Nonlinearity

The PA is an indispensable part of the transmitter that amplifies a low-power signal to a higher power one. It is, however, usually nonlinear. The memoryless nonlinear effects of a PA in a narrowband system can be modelled as amplitude/amplitude (AM/AM) and amplitude/phase (AM/PM) characteristics [6].

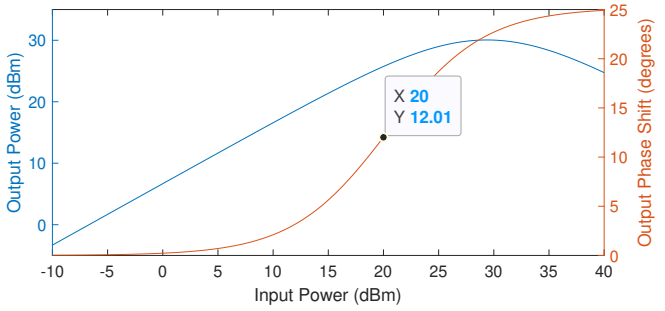


Fig. 6. AM/AM and AM/PM characteristics of the Saleh model. $[\alpha_A = 2.1587, \beta_A = 1.1517, \alpha_\Phi = 4.0033, \beta_\Phi = 9.1040]$.

As the relation $|s_{RF}(t)| = |s_{BB}(t)|$ holds, where $|\cdot|$ calculates the amplitude, the combined effects of the PA can be written as

$$s(t) = A(|s_{BB}(t)|)e^{j(\varphi+\Phi(|s_{BB}(t)|))}, \tag{18}$$

where $A(\cdot)$ and $\Phi(\cdot)$ denote the AM/AM and AM/PM effects, respectively, $\varphi = \angle s_{BB}(t) + \omega^{tx}t + \phi^{tx}(t)$.

There have been several behavioural models proposed, such as the Saleh, Rapp and Ghorbani models, etc. [6]. For example, the AM/AM and AM/PM characteristics of the Saleh model can then be defined as

$$A(|s_{BB}(t)|) = \frac{\alpha_A|s_{BB}(t)|}{1+\beta_A|s_{BB}(t)|^2}, \tag{19}$$

$$\Phi(|s_{BB}(t)|) = \frac{\alpha_\Phi|s_{BB}(t)|^2}{1+\beta_\Phi|s_{BB}(t)|^2}, \tag{20}$$

respectively, where α_A, β_A, α_Φ, and β_Φ are the corresponding coefficients. The AM/AM and AM/PM characteristics are shown in Fig. 6. When the input power increases to a certain level, the PA enters the non-linear region, which should be avoided. The backoff is a level below the saturation point. The larger it is, the further the PA is from the saturation point.

The effect of the PA is given in Fig. 7. Regarding the same Saleh model used for Fig. 6, the constellation is rotated about 10 degrees due to the AM/PM effect, when the input power is 20 dBm, as shown in Fig. 7(a). This matches Fig. 6 as the AM/PM effect is 12.01 degrees for a 20 dBm input power. As can be observed in Fig. 7(b), BER for a 16QAM system at 10 dB SNR significantly decreases with the backoff level, especially when the PA leaves away from the nonlinear region. We further configured different PA models by setting their parameters with a change of $\pm 10\%$ to the default values, that is, $[\alpha_A = 2.1587, \beta_A = 1.1517, \alpha_\Phi = 4.0033, \beta_\Phi = 9.1040]$. Fig. 7(c) demonstrates that the BER remains stable for different PA parameters when the backoff level is fixed.

D. Summary

After the above hardware modulation and processing, the transmitted signal is ready and will be emitted by an antenna. For the simplification of notation, we rewrite (18) as

$$s(t) = s'(t)e^{j(\omega^{tx}t+\phi^{tx}(t))}, \tag{21}$$

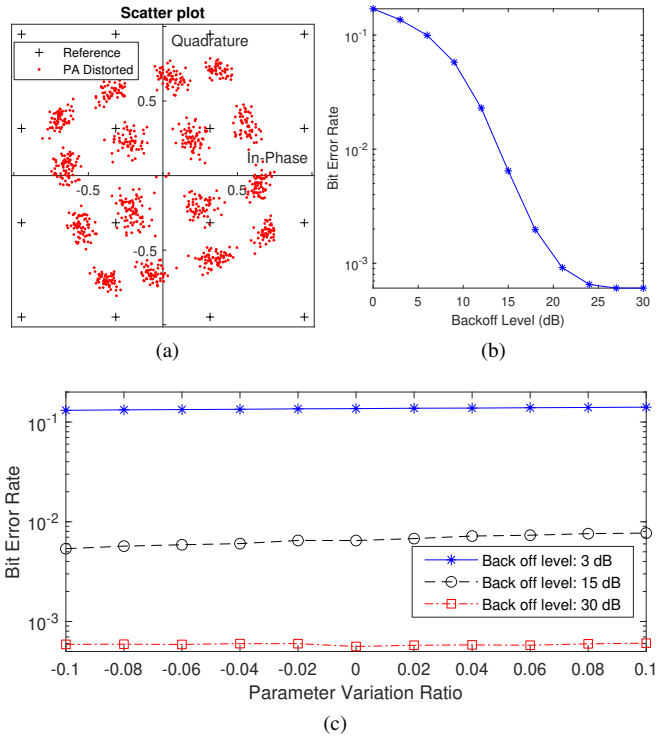


Fig. 7. PA impairment. SNR $\gamma = 10$ dB. (a) Constellation change with PA distortions. (b) BER versus back off level of a PA. (c) BER versus varied PA parameters.

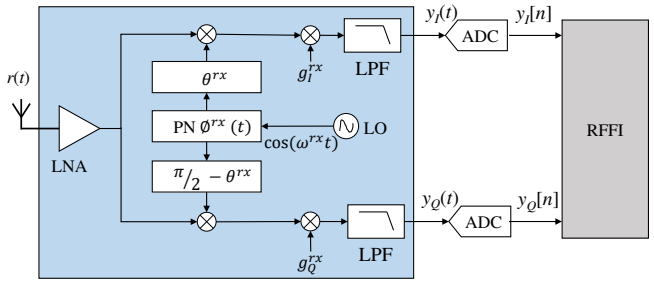


Fig. 8. Receiver chain with hardware impairments.

where

$$s'(t) = A(|s_{BB}(t)|)e^{j(\angle s_{BB}(t)+\Phi(|s_{BB}(t)|))}. \quad (22)$$

This completes the transmitter modulation and processing.

V. RFFI System

As shown in Fig. 8, the receiver will capture the signal via an antenna, downconvert it from the RF band to the baseband, and carry out IQ demodulation, which will be introduced in Section V-A. The processed analog signals are then converted to digital sequences and fed into the RFFI protocol, which will be explained in Section V-B.

A. Receiver Chain With RF Impairments

Similar to the transmitter, the receiver will also have RF impairments. The receiver oscillator is subject to frequency offset, Δf^{rx}, and phase noise, $\phi^{rx}(t)$. The receiver uses a mixer to downconvert received signals from the RF band to the baseband, which will also have imbalanced I and Q branches. The gains of I and Q branches in the linear scale at the receiver can be defined as [40]

$$g_I^{rx} = 10^{\left(0.5\frac{G^{rx}}{20}\right)}, \quad (23)$$

$$g_Q^{rx} = 10^{\left(-0.5\frac{G^{rx}}{20}\right)}, \quad (24)$$

respectively, where G^{rx} is the gain imbalance in dB at the receiver.

Considering these effects, the receiver's carrier can be given as

$$\Omega^{rx}(t) = K_1^{rx}e^{-j(\omega^{rx}t+\phi^{rx}(t))} + K_2^{rx}e^{j(\omega^{rx}t+\phi^{rx}(t))}, \quad (25)$$

where

$$K_1^{rx} = \frac{g_I^{rx}e^{-j\theta^{rx}} + g_Q^{rx}e^{j\theta^{rx}}}{2}, \quad (26)$$

$$K_2^{rx} = \frac{g_I^{rx}e^{j\theta^{rx}} - g_Q^{rx}e^{-j\theta^{rx}}}{2}, \quad (27)$$

and

$$\omega^{rx} = 2\pi(f_c^0 + \Delta f^{rx}), \quad (28)$$

and $\theta^{rx} = \frac{\psi^{rx}}{2}$, ψ^{rx} is the IQ phase mismatch at the receiver.

The received signal at the antenna (RF band) can be written as

$$r(t) = h(t)s(t) = h(t)s'(t)e^{j(\omega^{tx}t+\phi^{tx}(t))}. \quad (29)$$

After the downconversion and low pass filter, the received signal (baseband) becomes

$$\begin{aligned} y(t) &= r(t)\Omega^{rx}(t) \\ &= K_1^{rx}h(t)s'(t)e^{j\Delta C} + K_2^{rx}(h(t)s'(t))^*e^{-j\Delta C}, \end{aligned} \quad (30)$$

where

$$\Delta C = 2\pi(\Delta f^{tx} - \Delta f^{rx})t + \phi^{tx}(t) - \phi^{rx}(t). \quad (31)$$

It can be observed that the signal $y(t)$ possesses all the RF impairments of both the transmitter and receiver.

When a receiver without gain and phase imbalances is considered, (30) can be simplified as

$$y(t) = h(t)s'(t)e^{j\Delta C}. \quad (32)$$

Finally, $y(t)$ is sampled by the analog-to-digital converter (ADC), which produces a complex sequence, $y[n]$, with N_s symbols. The sequence is fed into the RFFI protocol for training and classification.

B. A CNN-based RFFI Protocol

As RFFI is a multi-class classification problem, we can leverage state-of-the-art deep learning algorithms to classify these devices. Specifically, CNN has been widely used in RFFI to learn the correlation within the IQ samples [26], [29], [30], [32], [33], which is also adopted in this paper.

The CNN architecture is shown in Fig. 9, which is designed based on the famous AlexNet CNN architecture [42]. AlexNet has five convolutional layers and achieves excellent performance on the ImageNet dataset. The complex IQ samples,

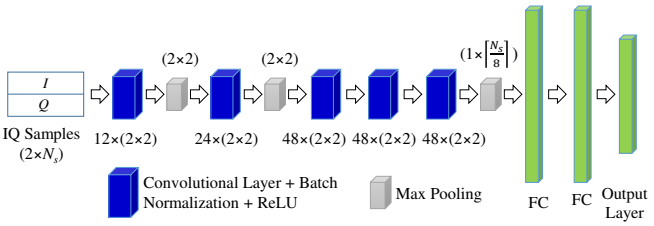


Fig. 9. The architecture of the adopted CNN model.

$y[n]$, are stacked as a new matrix, $\begin{pmatrix} y_I[n] \\ y_Q[n] \end{pmatrix}$, with a size of $2 \times N_s$. The sequences are then fed into the CNN model. Each convolutional layer contains batch normalization and uses ReLU as the activation function. The number of filters and size of the filter are marked in Fig. 9.

Following the configurations of other similar deep learning-based RFFI work [29], [33], we used the Adam optimizer with an initial learning rate of 1×10^{-4} for training CNN. The maximum number of epochs is 100 but the training will stop when the condition for patience of validation stopping is met, which is set to 20 in this paper. MATLAB Deep Learning Toolbox[3] was used to build the CNN model. The simulation was carried out on a node powered with two Nvidia Quadro P4000 GPUs, which is part of the high performance computing facilities at the University of Liverpool.

VI. Simulation Setup

This section will introduce the simulation setup in terms of the transmitter and receiver impairments as well as the channel model.

A. Transmitter

We configure N_{DUT} DUTs with different IQ imbalance and PA nonlinearity. Oscillator imperfection was not included as a suitable impairment for RFFI, which will be explained in Section VII-A.

As shown in Table I, we considered five cases. Cases T1-T4 represented individual transmitter impairment, namely gain imbalance, phase imbalance, gain & phase imbalances, and PA nonlinearities, respectively, while case T5 included all the above impairments. The ranges of the impairments are selected as follows.

- IQ Imbalance: From the literature, the absolute gain imbalance ranges from 0.02 to 0.82 and the phase imbalance varies from 2 degrees to 11.42 degrees [16], [34]. Therefore, we set the ranges of gain and phase imbalances as [-1 1] dB and [-5 5] degree, respectively. Based on the BER simulation results in Fig. 5, the IQ mismatches in the above ranges do not impact the BER.
- PA nonlinearity: The Saleh model was used. Each parameter, namely $[\alpha_A, \beta_A, \alpha_\Phi, \beta_\Phi]$, was varied within $\pm 5\%$ of the default values, $[\alpha_A = 2.1587, \beta_A = 1.1517, \alpha_\Phi = 4.0033, \beta_\Phi = 9.1040]$.

For cases T1, T2 and T3, the same Saleh PA model with the default values were used.

[3]https://mathworks.com/help/deeplearning/

TABLE I
Transmitter and Receiver Impairments

Transmitter	Case T1: All the DUTs have gain imbalances, G^{tx}, which follows a uniform random distribution within the range [-1 1] dB.
	Case T2: All the DUTs have phase imbalances ψ^{tx}, which follows a uniform random distribution within the range [-5 5] degree.
	Case T3: All the DUTs have both gain and phase imbalances. G^{tx} and ψ^{tx} follow the same distributions as the cases T1 and T2.
	Case T4: All the DUTs have PA nonlinearities. Saleh model was used. Each parameter, namely $[\alpha_A, \beta_A, \alpha_\Phi, \beta_\Phi]$, was varied within $\pm 5\%$ of the default values, $[\alpha_A = 2.1587, \beta_A = 1.1517, \alpha_\Phi = 4.0033, \beta_\Phi = 9.1040]$.
	Case T5: All the DUTs have gain and phase imbalances as well as PA nonlinearities. Their parameters follow the same distributions as the case T3 and T4.
Receiver	Case R0: The classification receiver has no RF impairment.
	Case R1: The classification receiver has gain imbalances within the range [-1 1] dB.
	Case R2: The classification receiver has phase imbalances within the range [-5 5] degree.
	Case R3: The classification receiver has both gain and phase imbalances whose ranges are [-1 1] dB and [-5 5] degree, respectively.

We also studied the effect of the payload pattern on classification performance. The payload, $x(t)$, is not part of RF impairments, but will lead to different modulated signals, hence affect the extraction of RF impairments. We simulated both the same data payload and random data payload to study the effect of the data pattern. All the data was modulated by QPSK.

B. Channel

As shown in (30), the channel effect will interfere with RF impairments, which has been experimentally validated by [43]. As this paper focuses on the device-specific hardware features, we adopted an AWGN channel. The channel impairments can be potentially solved by data augmentation [44], [45] or using channel-independent features [29].

Different SNR levels were simulated to evaluate the noise effects.

C. Receiver

The training and classification stages of RFFI require a receiver to capture wireless transmissions. RFFI with the same receiver at these stages allows us to investigate the effects of the hardware impairments at DUTs.

However, RFFI may not use the same receiver for these stages in practice, as we discussed in Section II. Hence, RFFI with different receivers is a more practical setup, which has not been comprehensively investigated. In this paper, we simulated both scenarios, that is, RFFI with the same receiver and RFFI with different receivers of varied IQ imbalances. Specifically, we considered the receiver at the training stage has no RF

impairment. Regarding the receiver at the classification stage, the cases in Table I were considered.

We built our RF impairments model using the MATLAB Communications Toolbox and based on a MATLAB example simulating a QAM system with RF impairments[4].

D. Metric

We used the overall classification accuracy and confusion matrix to evaluate the RFFI performance during the classification stage. In particular, classification accuracy is defined as the percentage of correctly identified packets over the total packets. Confusion matrix is an effective method to visualize the machine learning classification results. The row and column of the matrix represent the instances in a predicted class and the ones in an actual class, respectively.

VII. Experimental and Simulation Results

This section will present the experimental and simulation results of RFFI with different transmitter and receiver impairments. The system configurations differ in the number of DUT, N_{DUT}, transmitter impairments (case T1 to T5), SNR, data pattern and length, as well as the receiver impairments (case R0 to R3). For each configuration, we train a CNN model whose architecture is shown in Fig. 9. We generate 1,000 packets for each DUT, among which 90% are used for CNN training and the rest 10% are for validation; we further generate another 1,000 packets for CNN testing (classification).

In order to exclusively study the transmitter impairments, Section VII-A and Section VII-B considers the same receiver for both training and classification stages, that is, $G^{rx} = 0$ and $\psi^{rx} = 0$. Frequency offset is affected by working environmental conditions such as temperature. There is no suitable mathematical expression to describe the variation of frequency offset against temperature. Hence we designed experiments to estimate the frequency offset, and demonstrated oscillator imperfections are not suitable for RFFI due to their time-varying nature in Section VII-A. On the other hand, IQ imbalance and PA nonlinearity are time-invariant and can be described mathematically. In order to carry out comprehensive studies on their individual and overall effects, simulation allows us to tune the parameters. Hence, Section VII-B presents the effects of IQ imbalance and PA nonlinearity using simulation. Finally, Section VII-C evaluates the impact of different receivers for training and classification stages by simulation.

A. RFFI Experiments with Oscillator Imperfections

The oscillator imperfections are not ideal for RFFI as they are not stable and may interfere with other transmitter impairments. We use $N_{\text{DUT}} = 5$ DUTs as a case study to investigate the CFO effect in this section.

[4]https://uk.mathworks.com/help/comm/examples/end-to-end-qam-simulation-with-rf-impairments-and-corrections.html

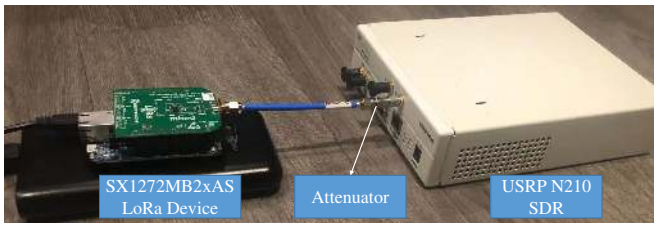


Fig. 10. Experimental setup for measuring CFO. The LoRa device and USRP SDR were connected using an attenuator.

1) CFO Variation: Oscillators are subject to temperature change and aging. For example, FTR5123-B is a crystal oscillator used in LoRa devices[5]; its frequency variation over -20 to +70 °C is ±10 ppm and its aging effect is ±10 ppm over 10 years.

As it is difficult to get mathematical expressions of the oscillator drift, we carried out measurements to obtain CFO variations using five SX1272MB2xAS LoRa shields[6], which are equipped with FTR5123-B oscillators. As shown in Fig. 10, we connected each LoRa end device with a USRP N210 SDR platform using an attenuator, which brought a 40 dB power attenuation but had no effect on the frequency offset, hence the channel effect was avoided. USRP SDR platforms are commonly used for RFFI as a receiver to collect raw IQ samples [10], [14], [26], [29]. The frequency accuracy of the USRP N210 platform is 2.5 ppm[7], which is smaller than that of the LoRa devices. In addition, the same USRP board was always used to minimize its effect on the estimation of the transmitter frequency offset. Compared to sophisticated equipment such as spectrum analyzers, USRP N210 is a low-end receiver. Using USRP as the testbed will provide insights into whether low-end receivers will be eligible for RFFI. High-end receivers will be too expensive to be widely used in practical applications.

We carried out six measurements over three months, with two tests each in August, September and October 2020. Each measurement lasted about one hour and 1,000 packets were collected. The CFOs estimated from these packets are shown in Fig. 11, which shows that CFO is not stable in neither short nor long term. Within the one hour collection on each day, CFOs of each DUT were varying, perhaps due to the self-heating. They also varied over three months, especially DUT4 and DUT5, which is probably due to the environmental temperature changes.

2) CFO-based RFFI: As shown in (32), the varying CFO and phase noise will cause phase rotation to the signal. In order to evaluate the CFO effect on the RFFI, we adopted a hybrid method of integrating experimentally estimated CFO with the simulation model. We first generated 1,000 packets without any RF impairments, by configuring $G^{tx} = 0$, $\psi^{tx} = 0$, and PA with the default parameter in the simulation. We

[5]https://lora-alliance.org/sites/default/files/showcase-documents/FTR5123-B0.pdf

[6]https://os.mbed.com/components/SX1272MB2xAS/

[7]https://www.ettus.com/wp-content/uploads/2019/01/07495_Ettus_N200-210_DS_Flyer_HR_1.pdf

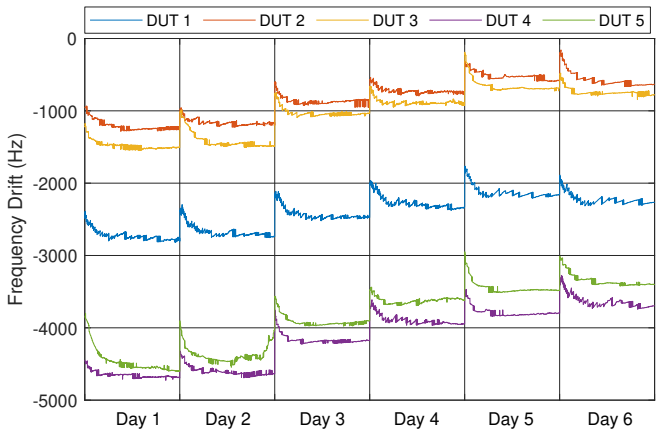
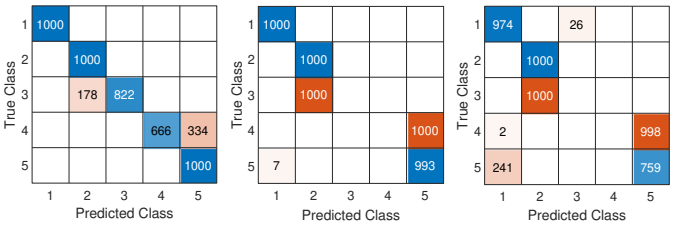


Fig. 11. Frequency drift variations in six days: Day 1 and Day 2 in August, Day 3 and Day 4 in September and Day 5 and Day 6 in October 2020.



(a) (b) (c)

Fig. 12. Confusion matrix of CFO-based RFFI. CFOs from Day 1 were used for training. (a) Overall accuracy, 89.76%. CFOs from Day 2 as test data. (b) Overall accuracy, 59.86%. CFOs from Day 3 as test data. (c) Overall accuracy, 54.66%. CFOs from Day 4 as test data.

converted the estimated CFOs from day 1 in August to ΔC and applied them to packets one by one using (32). These CFO impaired packets were used as the training data. The test data was generated similarly but the estimated CFOs were from a different day. Fig. 12 shows the confusion matrices when the test data was generated using CFOs from day 2 in August, day 3 and 4 in September 2020.

As can be observed from Figs. 12(b) and 12(c), the results are not promising as some DUTs are completely misclassified. Take DUT3 as an example. As the CFOs of DUT3 on day 3, August are very similar to the CFO of DUT2 on day 1, August, they cannot represent reliable device identifier anymore. The CNN thus made a wrong classification, as shown in Fig. 12(b).

3) CFO Interference to Other RF Impairments: While Section VII-A2 only involved CFO impairment, this section will investigate CFO co-existence with other transmitter impairments to explore whether CFO will interfere with them.

Similar to Section VII-A2, we combined the simulation data with different RF impairments and CFO estimated from experiments. Regarding training data, we generated 1,000 packets with RF impairments and applied the CFO from day 1, August. Another 1,000 packets were generated and applied with the CFOs from day 2 to day 6 as the test data. We carried out the above process for the cases T1 to T5 involving different transmitter impairments. We also did the simulation when there was no CFO impairment which can be regarded as references. The results are given in Fig. 13.

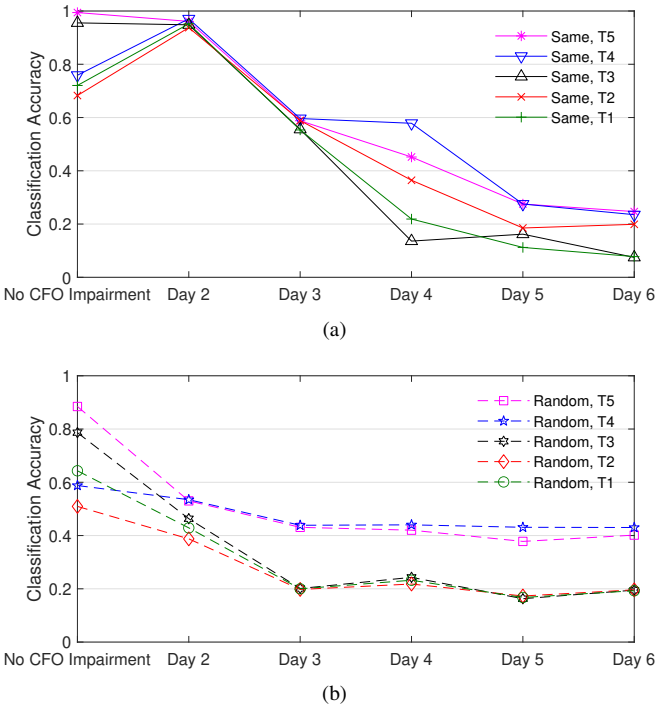


Fig. 13. CFO Interference. "No CFO Impairment" means no CFO applied to training and test data. "Day n" indicates that the Day 1 CFO was applied to the training data and the CFO from the Day n was applied to the test data. $N_{\text{DUT}} = 5$, SNR, $\gamma = 10$ dB. $N_s = 600$. (a) Same data payload. (b) Random data payload.

As can be observed, the CFO effect on RFFI is not stable. For some cases and test data, for example, cases T1, T2 and T4 of day 2 in Fig 13(a), the classification accuracies were improved. This is probably because these RF impairments are distinguishable and CFO adds another dimension of feature variations, even though CFOs of several devices are quite similar. On the other hand, CFO may compromise RFFI, for example, cases T1 to T5 with day 3 - day 6 test data as shown in Fig. 13(a) and all the results in Fig. 13(b). As we are not able to predict the CFO effect in advance, it is suggested to compensate the CFO impairment to avoid potential performance reduction.

4) Discussion: More CFO measurement results and its effect on RFFI have been experimentally shown in [46]. This paper advances the work in [46] by taking a hybrid method to combine experimentally measured CFO with the simulated RF impairments, which allows the investigation of CFO interfering with other RF impairments.

As many IoT devices use cheaply made components in order to reduce the cost and we are not able to control environmental temperature, frequency drift of an oscillator may not be a stable parameter for RFFI. In addition, apart from the oscillator drift, the estimated CFO may also include Doppler shift in a mobile channel, although its value may be small in slow fading channels. For example, it has been analyzed in [13] that the Doppler shift is only about 1% of oscillator frequency drift. Phase noise changes quickly from packet to packet. While it is possible to calculate the statistical features of the phase noise as the device characteristics [47], this method requires collecting numerous signals, which cannot be done

on a per-packet basis. Finally, it should be noted both CFO and phase noise can be estimated and compensated for reliable communications. However, their time-varying nature makes them not suitable for RFFI.

While there is existing work exploiting CFO and phase noise for RFFI [15], [48], we reckon their oscillators may be more sophisticated, which is not the case for low-cost IoT. In addition, long-term experiments involving temperature and aging are not available. Hence, their stability over time and environment changes are unknown, which is one of the most essential metrics for a device authentication scheme.

Recommendation One: Always estimate and compensate CFO before RFFI. In any practical wireless communication systems, we will often employ repeated preambles for CFO estimation and compensation, for example, the popular Schmidl-Cox algorithm [49]. Hence, we do not consider the oscillator imperfections in the following of this paper.

B. RFFI Simulation with IQ Imbalance and PA Nonlinearity

In the simulation of this subsection, we simulated $N_{\text{DUT}} = 50$ DUTs with RF impairments, except in Section VII-B5. The same receiver without RF impairments is used for training and classification, that is, case R0.

1) IQ Imbalance (T1 - T3 & R0): As shown in Fig. 14, the classification accuracies of case T3 (with both gain and phase imbalances) with the same data are about three times of the accuracies of case T1 (with gain imbalance only) and case T2 (with phase imbalance only). The effects of gain and phase imbalances are complementary, and their co-existence can significantly increase the feature space.

The effect of the number of symbols of each packet is shown in Fig. 14(a). Intuitively, more symbols will lead to higher classification accuracy, as the packet contains more information, which is validated by the simulation results. A physical layer waveform usually has much more than 800 symbols. For example, a ZigBee physical layer packet with 120 bytes will be modulated into about 16,000 symbols.

The effect of SNR on RFFI accuracy is given in Fig. 14(b). When the SNR increases, the signal has a better quality. Hence, the small variations among devices are more visible and can be learned easier by CNN. The accuracy is not promising in low SNR scenarios as the signal is swamped by noise. Signal pre-processing algorithms can be adopted to improve the SNR, for example, the denoising algorithm in [50].

2) Power Amplifier Nonlinearity (T4 & R0): Figs. 14(a) and 14(b) show the classification accuracies of PA nonlinearities regarding number of symbols and SNR, respectively.

Fig. 15 demonstrates that a smaller backoff level will have a better classification accuracy, because the nonlinear effect is more severe. However, as shown in Fig. 7(b), backoff level that is too small will result in a higher BER, which should be avoided. We used a 30 dB backoff level in this paper, which is the worst case for RFFI as the PA nonlinearity is the least.

3) Overall Effect (T5 & R0): We consider the case T5 that $N_{\text{DUT}} = 50$ DUTs have both gain & phase imbalances and PA nonlinearities. As shown in Fig. 14(a), the accuracy with the same data payload becomes relatively stable when there are 800 symbols.

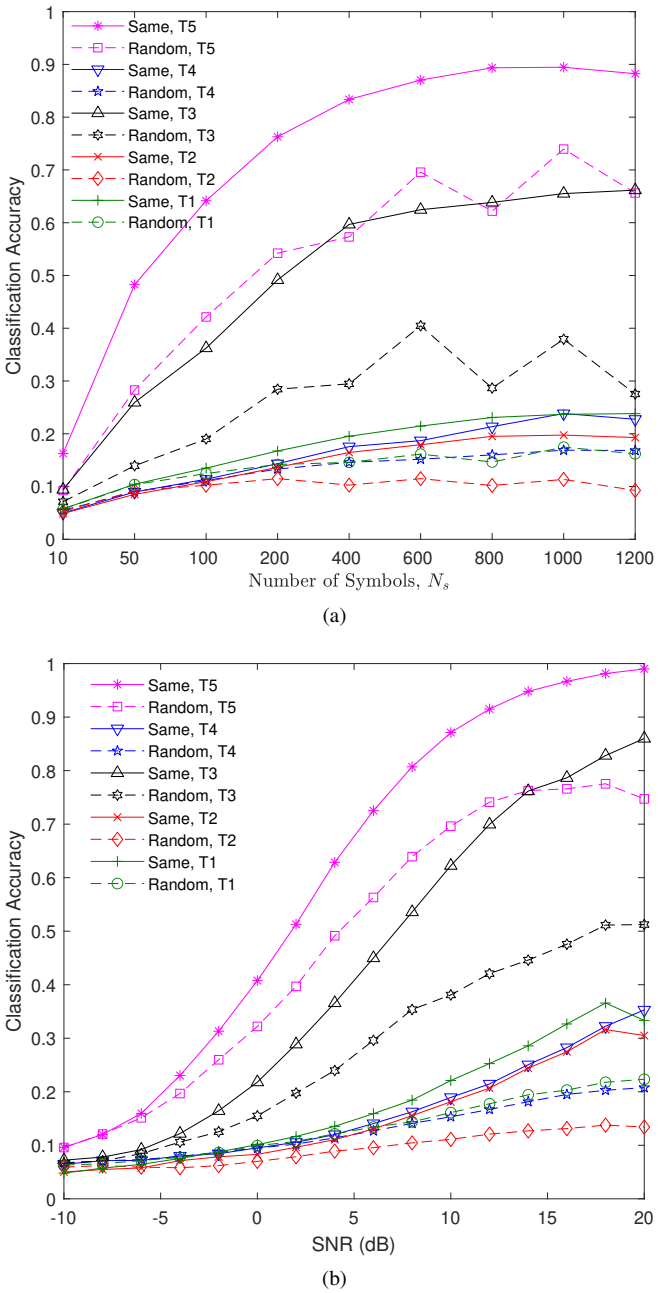


Fig. 14. Effects of different transmitter impairments on classification accuracy. Number of devices $N_{\text{DUT}} = 50$. (a) Classification accuracy versus the number of symbols per packet. SNR, $\gamma = 10$ dB. (b) Classification accuracy versus SNR. Number of symbols per packet, $N_s = 600$.

As can be observed from Fig. 14(b), with a packet length of 600 symbols, the classification accuracy is 87.1% when SNR is 10 dB, which is a reasonable level for a practical system. It can be boosted to 99% for a 20 dB SNR. These accuracies are quite high and very promising for developing RFFI as a matured solution.

4) Data Pattern: From Figs. 14(a) and 14(b), it can be observed that the same data payload always achieves better accuracy than random data payload, which is not surprising. Random payload brings another dimension of the variation,

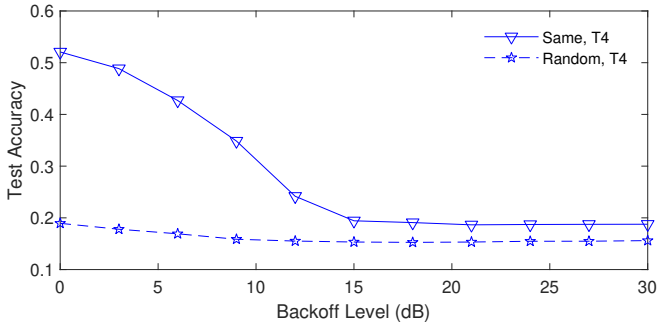


Fig. 15. Effects of PA nonlinearity, classification accuracy versus backoff levels. Number of devices $N_{\text{DUT}} = 50$. Number of symbols per packet, $N_s = 600$. SNR, $\gamma = 20$ dB.

TABLE II
CLASSIFICATION ACCURACY AND INITIAL LEARNING RATE VERSUS NUMBER OF DUT. NUMBER OF SYMBOLS PER PACKET, $N_s = 600$. SNR, $\gamma = 20$ DB.

		$N_{\text{DUT}} = 50$	$N_{\text{DUT}} = 100$	$N_{\text{DUT}} = 200$
Same Data	Classification Accuracy	99.0%	94.8%	89.3%
	Initial Learning Rate	1×10^{-4}	3×10^{-5}	1×10^{-5}
Random Data	Classification Accuracy	74.7%	81.1%	64.3%
	Initial Learning Rate	1×10^{-4}	1×10^{-4}	3×10^{-5}

hence it is more difficult for CNN to find patterns incurred by the RF impairments. The simulation results in Fig. 14 matches those in [18], regarding the observation that the same data payload achieves better classification accuracy than random payload for classifying PA nonlinearities.

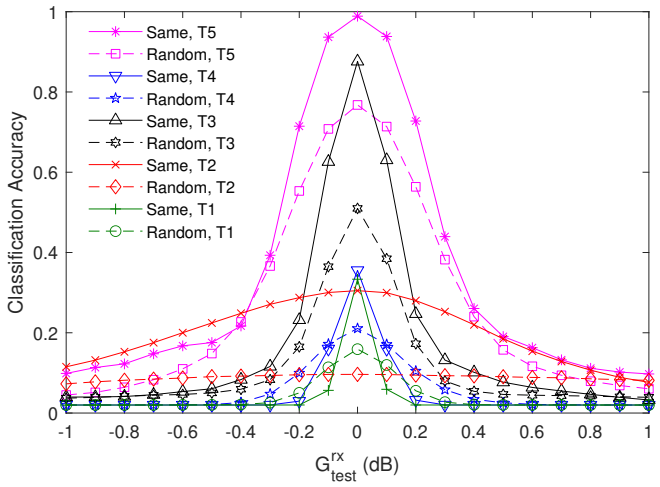
5) Number of DUT (T5 & R0): Intuitively, it is more difficult to classify more DUTs when their RF impairments are within the same range, because their features will be closer to each other. We carried out more simulation with $N_{\text{DUT}} = 100$ and $N_{\text{DUT}} = 200$ with all the transmitter impairments and the results are shown in Table II. When there are more DUTs, smaller initial learning rates are used.

As can be observed, when there are 200 DUT with the same data payload and 20 dB SNR, the classification accuracy is only slightly decreased to 89.3%.

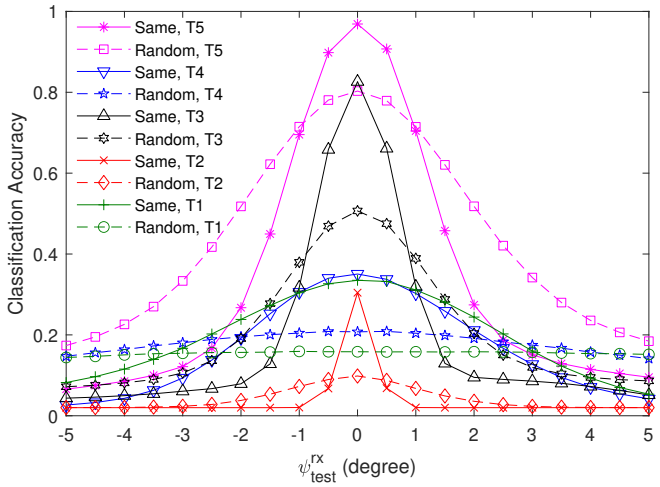
C. RFFI Simulation with Different Receivers

This section will demonstrate the effects of different receivers used for training and classification stages, that is, cases R1, R2 and R3. Specifically, in the simulation setup, we configure the receiver at the training stage as $G^{rx}_{train} = 0$ and $\psi^{rx}_{train} = 0$. We consider the receiver at the classification stage with IQ imbalances, G^{rx}_{test} and ψ^{rx}_{test}.

1) Receiver Gain and Phase Imbalance (T1 - T5 & R1 and R2): We first investigated the individual effects of gain and phase imbalances of receivers. Specifically, we considered $N_{\text{DUT}} = 50$ DUTs with impairments configured as cases T1 to T5 and the receiver cases R1 and R2 in order to independently study receiver's gain and phase imbalances.



(a)



(b)

Fig. 16. Effects of a different classification receiver on classification accuracy. Number of devices $N_{\text{DUT}} = 50$. Number of symbols per packet, $N_s = 600$. SNR, $\gamma = 20$ dB. (a) R1, classification accuracy versus gain imbalances of receivers. $\psi^{rx}_{test} = 0$. (b) R2, classification accuracy versus phase imbalances of receivers. $G^{rx}_{test} = 0$.

As shown in Fig. 16, the effects of the gain and phase imbalances are complementary. For example, when there are only gain imbalances at DUTs (case T1), that is, $\psi^{tx} = 0$:

- the gain imbalances at the receiver (R1) will affect the classification accuracy, as shown in Fig 16(a);
- the phase imbalances at the receiver (R2) will affect the classification accuracy in a slighter manner, as shown in Fig 16(b). There is no effect when random data is used.

This is because the gain and phase imbalances affect the signal modulation and constellation differently, as shown in (16) and Figs. 5(c) and 5(d).

2) Overall Effect (T5 & R3): In practice, DUTs will include all the impairments and the receiver will also have both gain and phase imbalances. Hence, we carried out further simulations with DUTs configured with IQ imbalances and PA nonlinearities, that is, case T5, and the classification receiver with both gain and phase imbalances, that is, case R3.

As shown in Fig. 17, the accuracy gradually drops when

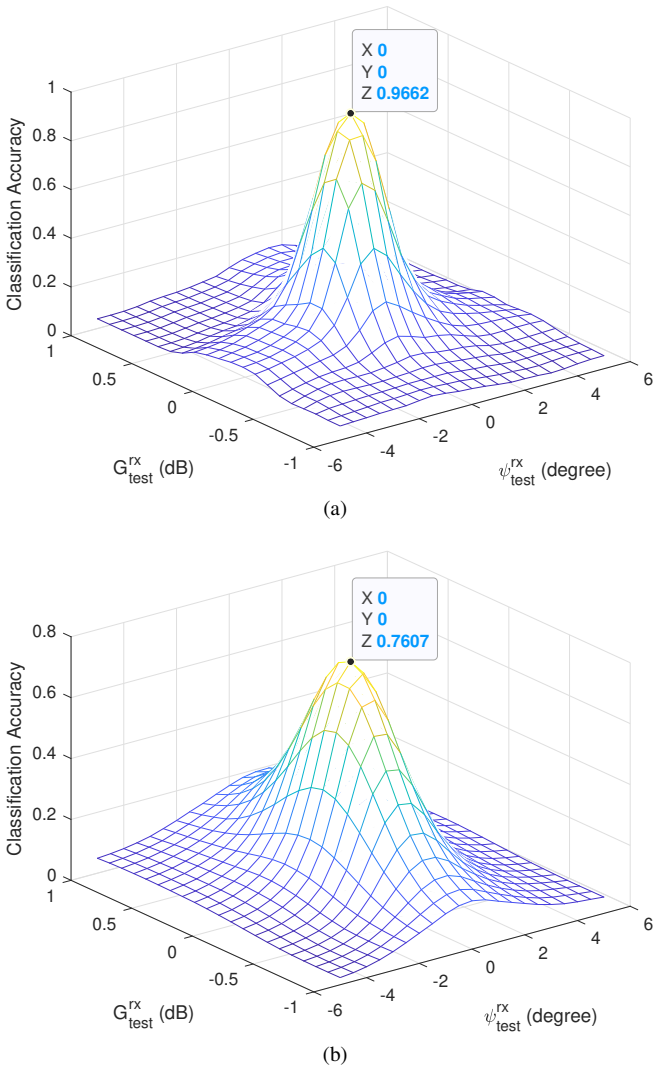


Fig. 17. R3, effects of a different classification receiver on classification accuracy. Number of devices $N_{\text{DUT}} = 50$. Number of symbols per packet, $N_s = 600$. SNR, $\gamma = 20$ dB (a) Same data payload. (b) Random data payload.

the classification receiver deviates from the training receiver in terms of the gain and phase imbalances. The accuracies dropped less than 20%, when the gain and imbalances were in a small range, for example, G^{rx}_{test} and ψ^{rx}_{test} within the range of [-0.2 0.2] dB and [-1 1] degree, respectively.

Recommendation Two: The receiver should carry out IQ estimation and calibration in advance before RFFI [51]–[53]. Hence, when the residual imbalances after calibration are limited to a small range, the classification performance will not be significantly compromised.

VIII. Conclusion

This paper carried out systematic modelling on the hardware impairments of a narrowband transmitter and receiver as well as extensive experimental and simulation validation of their effects on the RFFI. Specifically, hardware impairments involve oscillator imperfections, phase and gain imbalances at mixer and PA nonlinearity. Through our experimental campaign over three months, we found that oscillator imperfections are not stable and interfere with other impairments. Our extensive simulations demonstrated phase and gain imbalances, as well as PA nonlinearities, are suitable for RFFI and we should exploit all of them to achieve the optimal classification accuracy. Our proposed protocol can classify 50 and 200 DUTs that have uniformly and randomly distributed transmitter impairments with high accuracy, namely 99.0% and 89.3%, respectively, at SNR of 20 dB when the same data payload was used. We also modelled the receiver impairments and analyzed their effect on the RFFI when different receivers were used for training and classification stages. The accuracy dropped less than 20% when the residual gain and phase imbalances of the classification receiver were within the range of [-0.2 0.2] dB and [-1 1] degree, respectively. Based on the experimental and simulation results, we recommend that we should compensate CFO and calibrate IQ imbalances at receivers in order to design a robust RFFI protocol. Our future work will study the effect of different modulation schemes on the RFFI.

Acknowledgement

The detailed simulation was undertaken on Barkla, part of the High Performance Computing facilities at the University of Liverpool, UK.

References

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, 2017.

[2] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138 406–138 446, 2020.

[3] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Security & Privacy*, vol. 13, no. 1, pp. 14–21, 2015.

[4] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys*, vol. 45, no. 1, p. 6, 2012.

[5] S. Riyaz, K. Sankhe, S. Ioannidis, and K. Chowdhury, "Deep learning convolutional neural networks for radio identification," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 146–152, 2018.

[6] Z. Zhu, H. Leung, and X. Huang, "Challenges in reconfigurable radio transceivers and application of nonlinear signal processing for RF impairment mitigation," *IEEE Circuits Syst. Mag.*, vol. 13, no. 1, pp. 44–65, 2013.

[7] L. Anttila, M. Valkama, and M. Renfors, "Blind moment estimation techniques for I/Q imbalance compensation in quadrature receivers," in *Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Communications*, Helsinki, Finland, Sep. 2006, pp. 1–5.

[8] M. Valkama, A. Springer, and G. Hueber, "Digital signal processing for reducing the effects of RF imperfections in radio devices—an overview," in *Proc. IEEE Int. Symp. Circuits and Systems*, Paris, France, May/Jun. 2010, pp. 813–816.

[9] L. Smaini, *RF Analog Impairments Modeling for Communication Systems Simulation*. Wiley Online Library, 2012.

[10] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: Modeling and validation," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2091–2106, 2016.

[11] B. He and F. Wang, "Cooperative specific emitter identification via multiple distorted receivers," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3791–3806, 2020.

[12] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. 14th ACM Int. Conf. Mobile Computing and Networking*, San Francisco California USA, Sep. 2008, pp. 116–127.

[13] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658–1667, 2014.

[14] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, "Fingerprinting Wi-Fi devices using software defined radios," in *Proc 9th ACM Conf. Security & Privacy in Wireless and Mobile Networks*, Darmstadt, Germany, Jul. 2016, pp. 3–14.

[15] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong, "Accurate and efficient wireless device fingerprinting using channel state information," in *Proc. IEEE INFOCOM*, Honolulu, HI, USA, Oct. 2018, pp. 1700–1708.

[16] L. J. Wong, W. C. Headley, and A. J. Michaels, "Specific emitter identification using convolutional neural network-based IQ imbalance estimators," *IEEE Access*, vol. 7, pp. 33 544–33 555, 2019.

[17] A. C. Polak, S. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, pp. 1469–1479, 2011.

[18] S. S. Hanna and D. Cabric, "Deep learning based transmitter identification using power amplifier nonlinearity," in *Proc. Int. Conf. Computing, Networking and Communications*, Honolulu, HI, USA, Feb. 2019, pp. 674–680.

[19] J. Zhang, F. Wang, O. A. Dobre, and Z. Zhong, "Specific emitter identification via Hilbert–Huang transform in single-hop and relaying scenarios," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1192–1205, 2016.

[20] U. Satija, N. Trivedi, G. Biswal, and B. Ramkumar, "Specific emitter identification based on variational mode decomposition and spectral features in single hop and relaying scenarios," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 581–591, 2018.

[21] J. Gong, X. Xu, and Y. Lei, "Unsupervised specific emitter identification method using radio-frequency fingerprint embedded InfoGAN," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2898–2913, 2020.

[22] M. W. Lukacs, A. J. Zeqolari, P. J. Collins, and M. A. Temple, ""RF-DNA" fingerprinting for antenna classification," *IEEE Antennas Wireless Propag. Lett.*, vol. 14, pp. 1455–1458, 2015.

[23] S. Balakrishnan, S. Gupta, A. Bhuyan, P. Wang, D. Koutsonikolas, and Z. Sun, "Physical layer identification based on spatial–temporal beam features for millimeter-wave wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1831–1845, 2020.

[24] L. Peng, A. Hu, J. Zhang, Y. Jiang, J. Yu, and Y. Yan, "Design of a hybrid RF fingerprint extraction and device classification scheme," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 349–360, 2019.

[25] T. J. Bihl, K. W. Bauer, and M. A. Temple, "Feature selection for RF fingerprinting with multiple discriminant analysis and using ZigBee device emissions," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1862–1874, 2016.

[26] L. Peng, J. Zhang, M. Liu, and A. Hu, "Deep learning based RF fingerprint identification using differential constellation trace figure," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 1091–1095, 2019.

[27] Y. Shi and M. A. Jensen, "Improved radiometric identification of wireless devices using MIMO transmission," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 4, pp. 1346–1354, 2011.

[28] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1180–1192, 2015.

[29] K. Sankhe, M. Belgiovine, F. Zhou, L. Angioloni, F. Restuccia, S. D'Oro, T. Melodia, S. Ioannidis, and K. Chowdhury, "No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments," *IEEE Trans. on Cogn. Commun. Netw.*, vol. 6, no. 1, pp. 165–178, 2019.

[30] P. Robyns, E. Marin, W. Lamotte, P. Quax, D. Singelée, and B. Preneel, "Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning," in *Proc. ACM WiSec*, 2017, pp. 58–63.

[31] H. J. Patel, M. A. Temple, and R. O. Baldwin, "Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting," *IEEE Trans. Rel.*, vol. 64, no. 1, pp. 221–233, 2015.

[32] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep learning for RF device fingerprinting in cognitive communication networks," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 1, pp. 160–167, 2018.

[33] F. Restuccia, S. D'Oro, A. Al-Shawabka, M. Belgiovine, L. Angioloni, S. Ioannidis, K. Chowdhury, and T. Melodia, "DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms," in *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Catania, Italy, Jul. 2019, pp. 51–60.

[34] D. Roy, T. Mukherjee, M. Chatterjee, E. Blasch, and E. Pasiliao, "RFAL: Adversarial learning for RF transmitter identification and classification," *IEEE Trans. on Cogn. Commun. Netw.*, vol. 6, no. 2, pp. 783 – 801, Jun. 2020.

[35] L. Anttila, M. Valkama, and M. Renfors, "Frequency-selective I/Q mismatch calibration of wideband direct-conversion transmitters," *IEEE Trans. Circuits Syst. II*, vol. 55, no. 4, pp. 359–363, 2008.

[36] M. Aziz, F. M. Ghannouchi, and M. Helaoui, "Blind compensation of I/Q impairments in wireless transceivers," *Sensors*, vol. 17, no. 12, p. 2948, 2017.

[37] M. C. Sanchez, A. Segneri, A. Georgiadis, S. A. Kosmopoulos, G. Goussetis, and Y. Ding, "System performance evaluation of power amplifier behavioural models," in *Active and Passive RF Devices Seminar 2018*, 2018.

[38] (2013) Silicon oscillator frequency characteristics and measurements. Accessed on 11 March 2021. [Online]. Available: https://www.sitime.com/api/gated/Feb-25-26-Webinar-Frequency-Measurement-Techniques.pdf

[39] Z. Zhu, X. Huang, M. Caron, and H. Leung, "Blind self-calibration technique for I/Q imbalances and DC-offsets," *IEEE Trans. Circuits Syst. I*, vol. 61, no. 6, pp. 1849–1859, 2013.

[40] Apply i/q imbalance to input signal. Accessed on 11 March 2021. [Online]. Available: https://www.mathworks.com/help/comm/ref/iqimbal.html

[41] L. Anttila, M. Valkama, and M. Renfors, "Blind compensation of frequency-selective I/Q imbalances in quadrature radio receivers: Circularity-based approach," in *Proc. IEEE ICASSP*, vol. 3, Honolulu, HI, USA, 2007, pp. 245 – 248.

[42] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Proc. Int. Conf. Neural Information Processing Systems*, Lake Tahoe, NV, Dec. 2012, p. 1097–1105.

[43] A. Al-Shawabka, F. Restuccia, S. D'Oro, T. Jian, B. C. Rendon, N. Soltani, J. Dy, S. Ioannidis, K. Chowdhury, and T. Melodia, "Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting," in *Proc. IEEE INFOCOM*, Toronto, ON, Canada, Jul. 2020, pp. 646–655.

[44] N. Soltani, K. Sankhe, J. Dy, S. Ioannidis, and K. Chowdhury, "More is better: Data augmentation for channel-resilient RF fingerprinting," *IEEE Commun. Mag.*, vol. 58, no. 10, pp. 66–72, 2020.

[45] M. Cekic, S. Gopalakrishnan, and U. Madhow, "Robust wireless fingerprinting: Generalizing across space and time," *arXiv preprint arXiv:2002.10791*, 2020.

[46] G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, "Radio frequency fingerprint identification for LoRa using spectrogram and CNN," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Virtual Conference, May 2021, pp. 1–10. [Online]. Available: https://arxiv.org/abs/2101.01668

[47] A. Ali and G. Fischer, "The phase noise and clock synchronous carrier frequency offset based RF fingerprinting for the fake base station detection," in *Proc. IEEE 20th Wireless and Microwave Technology Conference (WAMICON)*, Cocoa Beach, FL, USA, Apr. 2019, pp. 1–6.

[48] A. C. Polak and D. L. Goeckel, "Wireless device identification based on RF oscillator imperfections," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2492–2501, 2015.

[49] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Trans. Commun.*, vol. 45, no. 12, pp. 1613–1621, 1997.

[50] Y. Xing, A. Hu, J. Zhang, L. Peng, and G. Li, "On radio frequency fingerprint identification for DSSS systems in low SNR scenarios," *IEEE Commun. Lett.*, vol. 22, no. 11, pp. 2326–2329, 2018.

[51] M. Valkama, M. Renfors, and V. Koivunen, "Advanced methods for I/Q imbalance compensation in communication receivers," *IEEE Trans. Signal Process.*, vol. 49, no. 10, pp. 2335–2344, 2001.

[52] A. Kiayani, L. Anttila, Y. Zou, and M. Valkama, "Advanced receiver design for mitigating multiple RF impairments in OFDM systems: Algorithms and RF measurements," *J. Electrical and Computer Engineering*, vol. 2012, 2012.

[53] C.-J. Hsu and W.-H. Sheen, "Joint calibration of transmitter and receiver impairments in direct-conversion radio architecture," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 832–841, 2012.