WideScan: Exploiting Out-of-Band Distortion for Device Classification Using Deep Learning

Abdurrahman Elmaghbub, Bechir Hamdaoui, Arun Natarajan
School of Electrical Engineering and Computer Science, *Oregon State University*
{elmaghba, hamdaoui, nataraja}@oregonstate.edu

***Abstract*—Wireless device classification techniques play a vital role in supporting spectrum awareness applications, such as spectrum access policy enforcement and unauthorized network access monitoring. Recent works proposed to exploit distortions in the transmitted signals caused by hardware impairments of the devices to provide device identification and classification using deep learning. As technology advances, the manufacturing impairment variations among devices become extremely insignificant, and hence the need for more sophisticated device classification techniques becomes inescapable. This paper proposes a scalable, RF data-driven deep learning-based device classification technique that efficiently classifies transmitting radios from a large pool of bit-similar, high-end, high-performance devices with same hardware, protocol, and/or software configurations. Unlike existing device classification techniques, the novelty of the proposed approach lies in exploiting both the in-band and out-of-band distortion information, caused by inherent hardware impairments, to enable scalable and accurate device classification. Using convolutional neural network (CNN) model for classification, our results show that the proposed technique substantially outperforms conventional approaches in terms of both classification accuracy and learning times. In our experiments, the testing accuracy obtained under the proposed technique is about 96% whereas that obtained under the conventional approach is only about 50% when the devices exhibit very similar hardware impairments. The proposed technique can be implemented with minimum receiver design tuning, as radio technologies, such as cognitive radios, can easily allow for both in-band and out-of-band sampling.**

***Index Terms*—Wireless device classification, device fingerprinting, hardware impairments, deep learning.**

I. Introduction

Deep learning based wireless device classification techniques have emerged as potential solution approaches for supporting spectrum access awareness applications, such as permitting spectrum regulatory agencies to enforce their access policy and allowing network administrators to monitor and control unauthorized access to their wireless networks. More recently, there has been a focus on exploiting distortions in the transmitted signals that are caused by hardware impairments during the manufacturing process to provide unique features and signatures of the devices that can be leveraged to improve the accuracy of device classification (e.g., [1], [2]). The training/testing accuracy of these deep learning based approaches decreases, however, with the decrease in the impairment variability among the wireless devices. Therefore, it is difficult for these deep learning approaches to achieve accurate device classification when the devices exhibit very similar (i.e., indistinguishable) hardware distortions. For instance, high-end, bit-similar software-defined radios (SDRs), such as USRP X310 radios, are made with hardware components with low impairment variability, making them not easy to identify using existing deep learning based methods. Oracle [1], for example, intentionally introduces artificial impairments in the signal to increase the differentiability among devices while maintaining a tolerable bit error rate (BER) for each device. DeepRadioID [2], on the other hand, uses a carefully-optimized digital finite response filter (FIR) at the transmitter's side to slightly modify the baseband signal to compensate for current channel condition. These methods showed considerable improvement and resiliency against high similarity among transmitters and high channel condition variability. However, they suffer from scalability issues, since the set of artificial impairment values that can be added without exceeding the tolerable BER level is limited. Additionally, it is not practical to integrate additional hardware, such as FIR filters, into each transmitter's circuit that desires to interact with the network.

In this paper, we propose `WideScan`, a novel, deep learning-based device classification technique that uses IQ samples collected from the RF signals to efficiently identify and classify high-performing transmitters with the *same, minimally-distorted* hardware components. `WideScan` (1) is scalable in that it can distinguish among a large number of minimally-distorted devices, regardless of their protocol/software configurations, (2) is robust against signature cloning and modification, (3) requires no changes at the transmitters, and (4) incurs minimal extra processing at the receiver side that can be performed with existing hardware. The novelty of the proposed technique lies in considering both the *in-band* and *out-of-band* (OOB) spectrum emissions of the received signals to capture hardware signatures and features, which are then used to uniquely and efficiently discriminate among devices, even when devices have same hardware with significantly reduced distortions [3]. OOB emissions are those that predominate the out-of-band domain, defined as the frequency range separated from the assigned emission frequency by less than 250% of the message bandwidth [4]. OOB emissions are mainly caused by the modulation and the nonlinearity of the RF transceiver front-end, which result in in-band distortions as well as in an interference into adjacent channels. Despite the endless efforts to reduce OOB emissions, there will always be some inevitable amounts of OOB emissions, which can be

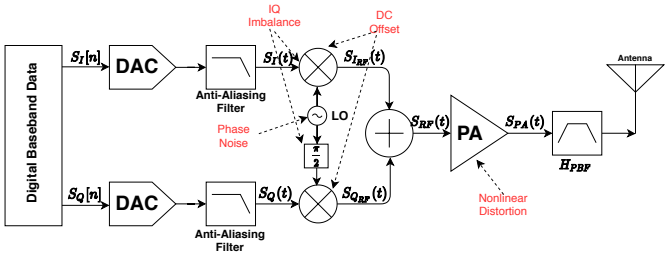


Fig. 1: Typical transceiver with main RF impairments

tolerated by standards but our proposed technique also exploits to provide unique device signatures. Our results show that `WideScan` substantially outperforms existing approaches that only consider the in-band distortion information by achieving significantly higher performances in terms of both classification accuracy and learning time, even when considering minimally-distorted devices with very similar hardware impairments. In our experiments, the testing accuracy obtained under `WideScan` is about **96%** whereas that obtained under the conventional approach is only about **50%** when the devices exhibit very similar hardware impairments.

The rest of the paper is organized as follows. Section II presents the key hardware impairments of a typical transmitter and illustrates their impacts on out-of-band spectrum emissions. Section III presents the proposed technique, and Section IV presents the performance results and analysis. Finally, Section V concludes the paper.

II. Transmitter Hardware Impairments

Transmitter hardware impairments, acquired during manufacturing and assembly stages, cause transmitted RF signals to deviate from their ideal values, thus establishing unique signatures for their corresponding transmitter devices. Despite the efforts aimed at designing hardware techniques that can eliminate/limit these hardware impairments so that they fall within tolerable ranges, these impairments cannot be eliminated completely. Therefore, since our focus in this paper is on exploiting such impairments to enable efficient device classification, we begin in this section by taking a closer look at the sources, modeling, and impact of the most significant transmitter-specific impairments, with more emphasis on the OOB distortions that these impairments cause. Fig. 1, showing these impairments, will be used throughout for illustration.

A. DC Offset

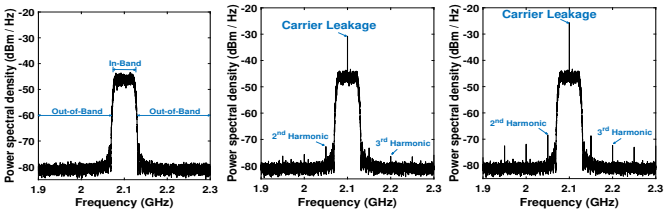
Direct-conversion transmitters like the one shown in Fig. 1 leverage the quadrature mixer configuration to implement the upconversion of the baseband signal without the need for filtering. It does so by separately (in parallel) upconverting, at the carrier frequency w_c, the two in-phase (I) baseband modulated, $S_I(t) = A(t)\cos(\phi(t))$, and quadrature (Q) baseband modulated, $S_Q(t) = A(t)\sin(\phi(t))$, components with two independent mixers fed by a local oscillator (LO) tone shifted by 90° from one another. Each mixer outputs the product of the baseband signal (I or Q component) and the carrier signal coming from the LO port. For *ideal* mixers, the output consists of two terms, one appearing at the summation and one appearing at the difference of the two multiplied/mixed frequencies. However, due to hardware impairments, *real* mixers also produce some other unwanted emissions at different frequencies. Of particular importance is an undesired spike, known as carrier leakage spike, that appears at the center of the desired signal and cannot be easily filtered out. This results in distortion of the signal constellation, as well as in an increase in the error vector magnitude.

There are two main sources of DC offsets: carrier leakage and second-order nonlinearity. Carrier leakage stems from the LO leakage due to the poor isolation between the LO and RF output ports of the mixer. Thus, a strong LO signal can leak through unintended paths toward the mixer output port and appear at the middle of the desired signal spectrum [5]. For example, when mixing the in-phase baseband component $S_I(t)$, because of this LO leakage, the mixer output becomes $S_{I_{RF}} = S_I(t)\cos(w_c t) + v_{lo}\cos(w_c t)$, where $v_{lo}\cos(w_c t)$ is the unwanted carrier term resulting from LO's leakage through the mixer output port and appearing at the middle of the spectrum, and v_{lo} is a hardware-specific quantity that varies from a mixer to another.

The second source of DC offsets is the second-order nonlinearity. When passing single-tone signals through a system with second-order nonlinearity, the output signal contains frequency components at integers multiple of the input frequency. To illustrate, let's feed the in-phase baseband component to the mixer while considering only the nonlinearity up to the second-order and ignoring the LO leakage effect. The output of the mixer in this case becomes $S_{I_{RF}}(t) = \alpha_1 S_I(t)\cos(w_c t) + \alpha_2 S_I^2(t)\cos^2(w_c t)$, where α_1 and α_2 are the coefficients that model and capture the mixer 's first- and second-order nonlinearity terms. When replacing $S_I(t)$ by its expression $A(t)\cos(\phi(t))$, the second-order nonlinearity term—the one responsible for the DC component—can be written as

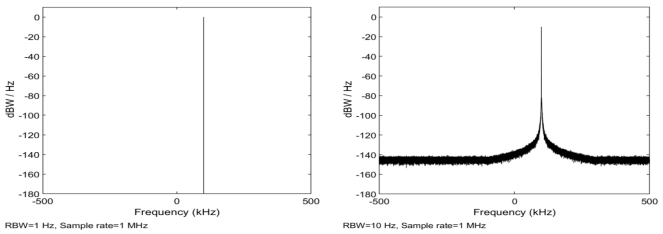
$$\alpha_2 S_I^2(t)\cos^2(w_c t) = \frac{\alpha_2 A^2(t)}{4} + \frac{\alpha_2 A^2(t)}{8}\big[2\cos(2w_c t) + 2\cos(2\phi(t)) + \cos(2(\phi(t) - w_c t)) + \cos(2(\phi(t) + w_c t))\big] \quad (1)$$

Note that the first term in Eq. (1) represents the DC component, and it is affected by the nonlinearity distortion captured by the parameter α_2. Beside the relatively large carrier leakage component at the center of the signal spectrum, the nonlinearity of the mixer also introduces other undesired harmonic spurs in the out-of-band domain. The amplitude of the carrier leakage spike and its harmonics depend on both the silicon-level circuitry of the mixer and the second-order nonlinearity distortion of the device. This can be clearly observed in Fig. 2, which compares the amplitudes of the carrier leakage spikes shown through the PSD of three simulated devices. Here, device 1 mimics an ideal mixer (i.e., zero DC offset), while device 2 and device 3 mimic real mixers with in-phase DC offset values of 0.9 and 0.5 and quadrature offset values of 0.9 and 0.5, respectively. The figure clearly shows that while the output of the ideal mixer (Device 1) has neither a carrier



(a) Device 1 (b) Device 2 (c) Device 3

Fig. 2: DC Offset Effect: Device 1 (ideal mixer, DC offset = 0); Device 2 (DC offset: I=Q=0.9); Device 3 (DC offset: I=Q=0.5)



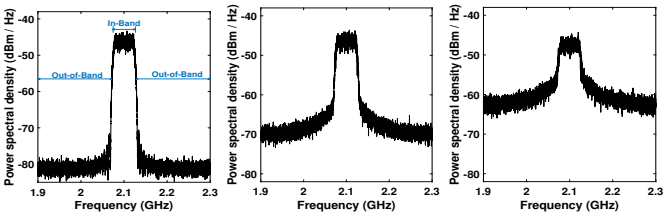
(a) Ideal Local Oscillator. (b) Real Local Oscillator.

Fig. 3: Phase Noise Effect

leakage spike nor harmonic spurs, real mixers (Devices 2 and 3) cause DC offset spikes (carrier leakage and the harmonic spurs) to appear not only in the center of the message spectrum, but also in its out-of-band surroundings. Also, observe that for the two real devices, the amplitudes of the spikes are quite different from one device to another even though the difference between their DC offset values is insignificant. Therefore, the carrier leakage and the harmonic spurs caused by mixer impairments can potentially be leveraged for providing unique device signatures that can be used for device classification. Furthermore, providing the classifier with out-of-band information capturing the differences between the DC offset harmonic spurs can increase device separability and classification accuracy.

B. Phase Noise

In RF transmitter architectures, Local Oscillators (LOs) are responsible for generating periodic oscillating signals that can be used by the mixer to upconvert the baseband signal at the carrier frequency. In an ideal LO, this periodic signal can be represented as a pure sinusoidal waveform $\cos(w_c t)$, which allows to upconvert baseband signals at the carrier frequency w_c while preserving their original spectrum shape. This is illustrated in Fig. 3a, which upconverts a baseband tone to 100KHz using an ideal LO. In real LOs, the time domain instability of the generated signals causes random phase fluctuations that result in expansion or regrowth of the signal spectrum in both sides of the carrier frequency. The real LO oscillating signal can thus be represented as $\cos(w_c t + \theta(t))$, where $\theta(t)$ is the phase deviation or noise term. The impact of this noise, commonly known as *phase noise*, is illustrated in Fig. 3b, which shows the upconversion of the same tone—whose upconversion using ideal LO is shown in Fig. 3a—using real LO signal.



(a) Device 1 (b) Device 2 (c) Device 3

Fig. 4: Phase Noise Effect: Device 1 (ideal LO); Device 2 (phase noise = -80 dBc/Hz); Device 3 (phase noise = -72 dBc/Hz); at 1MHz frequency offset.

The phase noise manifests in a random rotation in the receiver signal constellation, thereby increasing the symbol detection error [6] as well as the out-of-band noise level. To illustrate this, consider mixing the in-phase baseband signal, $S_I(t)$, with the real LO signal, $\cos(w_c t + \theta(t))$; here $\theta(t)$ represents the phase noise. Now applying the Fourier transform to the mixer output, i.e., the upconverted/modulated signal $S_{I_{RF}}(t) = S_I(t)\cos(w_c t + \theta(t))$, yields

$$\mathcal{F}[S_{I_{RF}}(t)] = \frac{1}{2}\{\bar{S}_I(f-f_c) * \mathcal{F}[e^{j\theta(t)}] + \bar{S}_I(f+f_c) * \mathcal{F}[e^{-j\theta(t)}]\} \quad (2)$$

where $f_c = \frac{w_c}{2\pi}$, $\bar{S}_I(f) = \mathcal{F}[S_I(t)]$, and $\mathcal{F}[.]$ and * are the Fourier transform and convolution operators. From Eq. (2), we observe that the phase noise $\theta(t)$ results in a bandwidth expansion beyond the original signal's spectrum around the carrier frequency f_c, which comes from the convolution of the spectrum of the bandpass (upconverted) signal, $\bar{S}_I(f+f_c)$, and that of the phase noise, $\mathcal{F}[e^{-j\theta(t)}]$.

Now since the spectrum expansion (or regrowth) depends on the LO phase noise, different devices will exhibit different out-of-band distortions. This can be clearly seen in Fig. 4, where the PSD of three simulated devices, each with a different phase noise value but all with the same frequency offset, are displayed. Device 1 mimics an ideal LO (i.e., zero phase noise value), while device 2 and device 3 mimic real LOs with phase noise values of -80 and -72 dBc/Hz, respectively, at the same frequency offset, 1MHz. The figure clearly shows that the out-of-band spectrum shapes for device 2 and device 3 are different from one another and from device 1. Therefore, like DC offsets, a transmitter's phase noise caused by its LO impairments can potentially be leveraged for providing unique device signature that can too be used for device classification. Additionally, considering the out-of-band information makes the spectra of devices more discernible and thus enhances the performance of the classifier.

C. Power Amplifier (PA) Nonlinearity Distortion

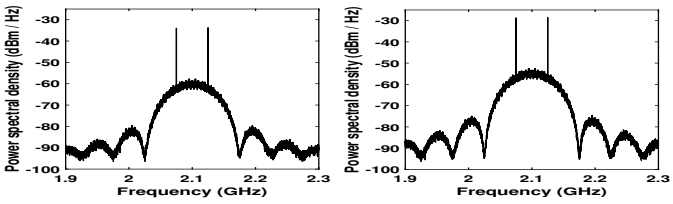
The majority of circuit nonlinearity is attributed to PAs as they provide the modulated RF signals with the required radiation power to reach their destination. When a PA operates in the linear region, its I/O characteristics is linear and an acceptable performance is ensured. However, operating in that region leads to more power consumption due to the associated lower power efficiency. Since PAs dominate power consumption, transmitters typically drive PAs to work near the

saturation region for higher power efficiency. Unfortunately, power efficiency and linearity conflict one another in that signals would suffer severely from the nonlinearity of the PA when operating in the saturation region. Such nonlinear distortions result in amplitude compression, as well as in high adjacent channel power leakage as a result of the bandwidth expansion, aka spectral regrowth. Although many methods have been proposed to minimize the distortion, PAs still exhibit some nonlinearity behaviors.

PA nonlinearity distortion is typically captured through the instantaneous amplitude and phase output responses to changes in the amplitude of the PA input signal, respectively known as Amplitude-to-Amplitude (AM-AM) and Amplitude-to-Phase (AM-PM) distortion curves. Using complex power series [7], the nonlinear PA output modelling the AM-AM and AM-PM distortions in response to the PA input signal $S_{RF}(t)$ can be expressed as [8] $S_{PA}(t) = \tilde{\alpha}_1 S_{RF}(t) + \tilde{\alpha}_3 S^3_{RF}(t) + \tilde{\alpha}_5 S^5_{RF}(t) + ...$, where $\tilde{\alpha}_i$s are the complex coefficients of the model. As we can infer from the equation, only the odd terms can be determined from single-tone complex compression characteristics, but fortunately, the odd-order terms are the most important as they produce intermodulation distortion in-band and adjacent to the desired signal [9]. To illustrate the impact of PA nonlinearity on out-of-band spectrum distortions, suppose the PA input signal $S_{RF}(t) = A(t)\cos(w_c t + \phi(t))$ and consider looking at the effect of the third-order nonlinearity term only; i.e., the term

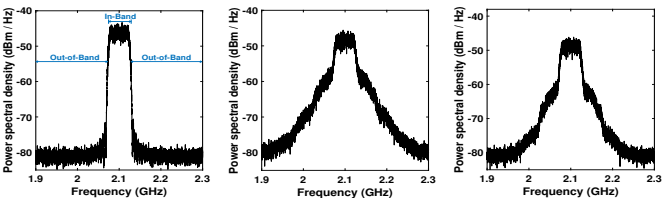
$$\tilde{\alpha}_3 S^3_{RF}(t) = \frac{\tilde{\alpha}_3 A^3(t)}{4}\left[3\cos(w_c t + \phi(t)) + \cos(3w_c t + 3\phi(t))\right]$$

Now provided that the out-of-band component at $3w_c$ is located sufficiently far away from the center frequency, w_c, and that the bandwidth of the original signal is much less than w_c, this out-of-band component can easily be filtered out without causing any bandwidth regrowth around the original message spectrum. However, the first term at w_c can lead to spectrum regrowth. For instance, in the case of constant-envelope modulation schemes such as BPSK where the amplitude $A(t)$ is constant, the spectrum of the modulated signal in the vicinity of w_c remains unchanged. This can be shown in Fig. 5 where the spectrum of a BFSK modulated signal has not changed after passing through a nonlinear PA. Note that the shape of the spectrum is the same under both linear and nonlinear PAs. However, for variable-envelope modulation schemes such as 16QAM where the amplitude $A(t)$ varies over time, nonlinearity causes a spectral regrowth of the original signal spectrum in that the $\frac{\tilde{\alpha}_3^3 A^3(t)}{4}$ term generally exhibits a broader spectrum than $A(t)$ itself. For this case of modulation, the severity of the spectral growth also depends on the nonlinearity model parameter $\tilde{\alpha}_3$. To illustrate, we show in Fig. 6 the case of a 16QAM modulated signal passing through a linear PA (Fig. 6a) and two nonlinear PAs (Figs. 6b and 6c) each under slightly different nonlinearity parameters. Two key observations we make from these results. First, observe that the nonlinearity of PA leads to an out-of-band spectrum growth (or distortion). Second, even a slight difference in the



(a) Linear PA (b) Nonlinear PA

Fig. 5: Nonlinearity effect under BFSK modulation



(a) Linear PA (b) Nonlinear PA 1 (c) Nonlinear PA 2

Fig. 6: Nonlinearity effect under 16QAM modulation

nonlinearity impairments causes a considerable differences in the amplitude of the frequency components in the out-of-band spectrum, as can be observed from the indicated amplitudes of the spikes. That is, different PA nonlinearity impairments cause different out-of-band spectrum distortions. Therefore, we argue that out-of-band spectrum distortion information due to PA nonlinearity can potentially be exploited to increase device distinguishability, thereby enhancing the accuracy and scalability of device classification.

D. IQ Mismatch

As shown in Fig. 1, the I and Q baseband components, $S_I(t) = A(t)\cos(\phi(t))$ and $S_Q(t) = A(t)\sin(\phi(t))$, are upconverted at the carrier frequency w_c with two mixers, and the two outputs of the mixers are summed up, yielding, for real mixers, the bandpass modulated signal

$$S_{RF}(t) = A(t)\cos(\phi(t))\cos(w_c t) - A(t)\sin(\phi(t))\sin(w_c t)$$

However, DAC and mixer hardware impairments manifest in amplitude mismatch, $\Delta\alpha$, and phase deviation, $\Delta\theta$, between the I and Q paths. This IQ mismatch, aka IQ imbalance, leads to imperfect image cancellation and results in residual energy at the mirror frequency $-w_c$, causing interference and SNR degradation. Considering an amplitude and a phase imbalances of $\Delta\alpha$ and $\Delta\theta$ when upconverting the baseband signal, the distorted bandpass signal can be expressed as:

$$S_{RF}(t) = (1-\Delta\alpha)S_I(t)\cos(w_c t) - S_Q(t)\sin(w_c t + \Delta\theta)$$

Now assuming an ideal power amplifier and an ideal direct-conversion receiver, the distorted complex baseband signal $\tilde{R}(t) = S_{RF}(t)e^{-jw_c t}$ received at the receiver after downconversion can be expressed as (after some math manipulations and clearing the terms appearing at twice the carrier frequency)

$$\tilde{R}(t) = \left(\frac{1-\Delta\alpha}{2}\right)S_I(t) + j\left(\frac{\sin(\Delta\theta) - j\cos(\Delta\theta)}{2}\right)S_Q(t)$$

Clearly, IQ imbalances cause in-band and out-of-band signal distortions that can be extracted and used for increasing device signature separability and device classification.

III. Leveraging Out-of-Band Distortions for Robust Device Classification

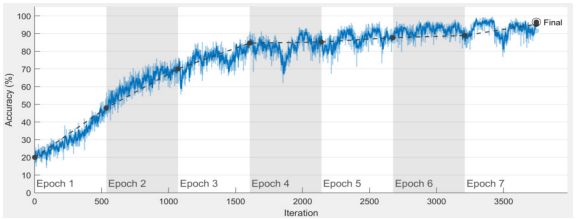
A. `WideScan`: *The Proposed Technique*

Based on the aforementioned description of the relationship between the out-of-band emissions and the hardware impairments of RF front-end components, and the observations we made from our simulations, we found that we are missing valuable indicative information when we process and leverage only the (in-band) message bandwidth for providing device signatures. Therefore, we propose in this paper to consider both the in-band and out-of-band spectra by oversampling the captured signals at the receiver with an appropriate factor. Without any further processing, the raw IQ values obtained from the oversampled signals are then fed into a deep convolutional neural network (CNN) for device identification and classification. It is worth mentioning that technology advancements of transceiver designs nowadays (e.g., software defined and cognitive radios) can easily allow for sampling the captured signals in the out-of-band region, and therefore, the proposed technique, `WideScan`, can be implemented without requiring newly/sophisticated receiver designs.

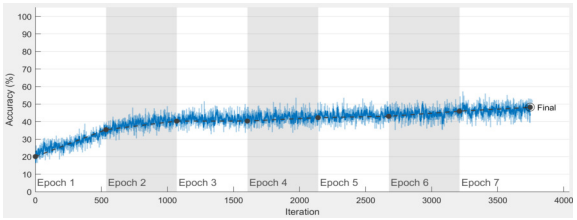
B. *CNN Classifier Architecture*

We use a variation of the CNN architecture used in [10], where each IQ input sequence is represented as a two-dimensional (I and Q components) real-valued tensor of size 2×1024. The input is fed to the first convolutional layer (Conv1), which consists of 16 filters, each of size 1x4. Each filter learns 4-sample variations in time over the I or Q dimension separately to generate 16 distinct feature maps over the complete input sample. Each ConvLayer is followed by a Batch normalization layer, a Rectified Linear Unit (ReLU) activation, and a maximum pooling (MaxPool) layer with filters of size 1x2 and stride [1 2] to perform a pre-determined non-linear transformation on each element of the convolved output, except the last ConvLayer, which is followed by an Average Pooling (AP) layer with a dimension 1x32. The output of the AP layer is then provided as an input to the Fully Connected (FC) layer, which has 5 neurons. Then, the output of the FC is finally passed to a classifier layer. To overcome overfitting, we set the dropout rate to 0.5 at the dense layers. A softmax classifier is used in the last layer to output the probabilities of each frame being fed to the CNN.

The weights of the network are trained using stochastic gradient descent with momentum (SGDM) optimizer with an initial learning rate of $l = 0.02$ and a learning rate drop factor of 0.1 with a learning rate drop period of 9. We minimize the prediction error through back-propagation, using categorical cross-entropy as a loss function computed on the classifier output. We implement our CNN architecture in MATLAB using the Deep Learning Toolbox running on a system with intel Corei7 8th Gen CPU.



(a) Our proposed method: `WideScan`.



(b) Conventional method: In-band only.

Fig. 7: Training and validation accuracy

IV. Performance Evaluation and Analysis

Using MATLAB's Communications toolbox, we designed a simulation model of a typical full wireless communications processing chain for 5 wireless devices. Different RF impairments blocks have been used to introduce hardware impairments to the ideal blocks of the simulation. The impairments that have been considered in this experiment are the following: IQ imbalance, DC offset, carrier frequency offset, phase noise, and PA nonlinearity distortion. Each device represents a transmitter that sends 16QAM modulated signals over an AWGN channel. For each transmitter, we collect the raw IQ values of two different bandwidths, 2.075 - 2.125 GHz, which represents the bandwidth of the message (in-band), and 1.9 - 2.3 GHz, which includes both in-band (message bandwidth) and out-of-band domain. We generate $200,000$ samples for each of the five devices, divided into training, validation, and test sets, to be used in the classification task.

Our simulation model emulates the RF front-end of 5 impaired wireless devices with all the relevant impairments to assess the performance of the two methods: the proposed method, `WideScan`, leveraging both in-band and out-of-band spectrum distortion information, and the conventional method using in-band distortion information only. We set the impairments values very similar across the devices to resemble the bit-similar radios and to make the identification task even harder. Table I shows the RF impairment values used for this experiment. The generated dataset is divided into three sets: 80% of data used for training, 10% of data used for validation, and 10% of data used for testing.

Fig. 7 shows that the training accuracy (blue curve) of the proposed `WideScan` outperforms the conventional classification approach that uses in-band information only. These results show that considering out-of-band distortion information in addition to in-band information increases the classification accuracy substantially. Our experiments show that the out-of-band additional processing exploited in our proposed technique does not incur an increase in the computation time of

RF	IQ-amp(dB)	IQ-phase(deg)	I-DC offset	Q-DC offset	AM-AM	AM-PM	Phase noise(dBc/Hz)	Freq offset(Hz)
Dev1	0.08	0.1	0.1	0.15	[2.178 1.12157]	[4.0893 9.2040]	[-60, -80]	[20, 200]
Dev2	0.1	0.09	0.109	0.1	[2.197 1.16157]	[4.13 9.2540]	[-60, -80]	[20, 200]
Dev3	0.09	0.09	0.1	0.1	[2.16 1.10157]	[4.0933 9.2840]	[-59.9, -80]	[20, 200.9]
Dev4	0.109	0.108	0.1	0.1	[2.17 1.12157]	[4.113 9.2040]	[-60, -80.1]	[20, 200]
Dev5	0.1	0.099	0.099	0.1	[2.1587 1.15157]	[4.133 9.2040]	[-60, -80]	[20.1, 200]

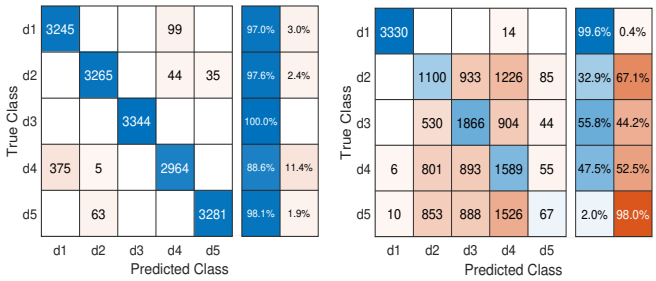
TABLE I: RF impairments: IQ-amp and IQ-phase are amplitude mismatch and phase deviation. I-DC and Q-DC are the in-phase and quadrature DC offsets. AM-AM and AM-PM distortions are represented by the alpha and beta parameters of Saleh model [11]. LO phase noise is introduced by a filtered Gaussian noise using a spectral mask specified by noise level and the frequency offset vectors.

the method; the running times of the reported results are 97.38 and 96.35 minutes for the in-band only and the proposed technique, respectively. Also, from the validation accuracy (the black dotted line in the figure), we can infer that our technique does not suffer from overfitting.

In Fig. 8, we show the confusion matrices of classification accuracy under each of the two methods where di indicates device i. The figure shows that the proposed method, `WideScan`, substantially surpasses the in-band only method in terms of classification accuracy. The testing accuracy obtained under the proposed method across the five tested devices is **96.2%** whereas that obtained under the in-band only method is only **48.6%**. It is worth mentioning that similar results are also obtained when considering the 8-PSK modulation scheme as opposed to the 16QAM scheme.

The main reason for why `WideScan` achieves such a high accuracy is because it leverages, in addition to the in-band distortion information already exploited by prior methods, out-of-band distortion information caused by the different radio hardware components, which, as explained in the previous sections, provide unique device signatures that lead to substantial increase in device separability.

Another point that is also worth mentioning is that our experiments indicated that this accuracy gab between our proposed technique and the prior in-band only method is inversely proportional to the hardware impairments variability among devices, meaning that both techniques enjoy high classification accuracy when the devices exhibit relatively high impairment values. However, we strongly argue that as technology advancements continue to reduce such impairments, the variability among these impairments across different devices will continue to shrink, making the reliance on in-band only information for device classification inefficient. Our proposed technique, leveraging out-of-band distortion in addition to in-band information, becomes in this case increasingly compelling and suitable for providing robust and scalable device separability performance.



(a) `WideScan`. (b) In-band only.

Fig. 8: Confusion matrices: di indicates device i

V. Conclusion

We proposed `WideScan`, a scalable, deep learning based technique that exploits both the in-band and out-of-band signal information to enable efficient device classification. We presented the models and the impact of the main hardware RF transmitter impairments in considerable depth and insight, with more emphasis on the out-of-band signal distortions and their potentials and contributions to providing unique device signatures and features that can increase devices' separability. Experimental results showed that our proposed technique increases the device classification accuracy significantly, especially in realistic scenarios where the variability of hardware impairment values among the different devices is insignificant, which is the case of high-end, high-performance radios.

References

[1] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "Oracle: Optimized radio classification through convolutional neural networks," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 2019, pp. 370–378.

[2] 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. of the Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2019, pp. 51–60.

[3] A. Elmaghbub and B. Hamdaoui, "Leveraging hardware-impaired out-of-band information through deep neural networks for robust wireless device classification," *arXiv preprint arXiv:2004.11126*, 2020.

[4] M. Tanaka, H. Sakamoto, M. Kobayashi, and Y. Kitayama, "Unwanted emissions of multi-carrier transmitter in spurious domain," in *26th Intn'l Communications Satellite Systems Conference (ICSSC)*, 2008.

[5] R. Svitek and S. Raman, "Dc offsets in direct-conversion receivers: Characterization and implications," *IEEE Microwave Magazine*, vol. 6, no. 3, pp. 76–86, 2005.

[6] M. R. Khanzadi, D. Kuylenstierna, A. Panahi, T. Eriksson, and H. Zirath, "Calculation of the performance of communication systems from measured oscillator phase noise," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 5, pp. 1553–1565, 2014.

[7] N. Blachman, "Band-pass nonlinearities," *IEEE Transactions on Information Theory*, vol. 10, no. 2, pp. 162–164, 1964.

[8] K. G. Gard, L. E. Larson, and M. B. Steer, "The impact of rf front-end characteristics on the spectral regrowth of communications signals," *IEEE Transactions on Microwave Theory and Techniques*, vol. 53, no. 6, pp. 2179–2186, 2005.

[9] K. G. Gard, H. M. Gutierrez, and M. B. Steer, "Characterization of spectral regrowth in microwave amplifiers based on the nonlinear transformation of a complex gaussian process," *IEEE Transactions on Microwave Theory and Techniques*, vol. 47, no. 7, pp. 1059–1069, 1999.

[10] X. Liu, D. Yang, and A. El Gamal, "Deep neural network architectures for modulation classification," in *2017 51st Asilomar Conference on Signals, Systems, and Computers*. IEEE, 2017, pp. 915–919.

[11] A. A. Saleh, "Frequency-independent and frequency-dependent nonlinear models of twt amplifiers," *IEEE Transactions on communications*, vol. 29, no. 11, pp. 1715–1720, 1981.