Exploiting CSI-MIMO for Accurate and Efficient Device Identification

Laxima Niure Kandel, Zhuosheng Zhang, Shucheng Yu
Department of Electrical and Computer Engineering, Stevens Institute of Technology
Email: {lniureka, zzhang97, shucheng.yu}@stevens.edu

Abstract*—Due to the inherent broadcast nature of the wireless medium, Wireless Local Area Networks (WLANs) are targets of a variety of malicious attacks, for example, MAC identity spoofing, rogue AP attack, and network freeloading. These attacks invite security and privacy threats and hinder the worry-free deployment of WLAN networks. To thwart these attacks, existing research has proposed to use hardware-specific imperfections as a unique unforgeable fingerprint for the APs and/or clients. Unfortunately, existing solutions are limited to static and stable environments or use customized hardware preventing their wide-scale adoption. To overcome the limitations, in this work, we propose to use the distribution of relative phase differences between MIMO-radio transmitter oscillators as a distinguishing trait or fingerprint. More specifically, we show that the nonidealities of the multiple RF chains on a single MIMO-OFDM (Multiple Input Multiple Output-Orthogonal Frequency Division Multiplexing) transmitter can be extracted and utilized as a reliable device fingerprint. Each transmitter RF chain has a random initial phase offset, and their difference relative to one another is stable over time, differs uniquely for each transmitter device and cannot be altered by the adversary without significant effort and cost. Our functional prototype measures these unknown phase differences using PHY-layer Channel State Information (CSI) of the in-band channel obtained from off-the-shelf hardware. Our design eliminates expensive custom-built hardware, is invariant to environmental variations and supports device mobility making it practical and deployable in real indoor settings. Experimental evaluation using 17 Intel Network Interface Cards (NICs) resulted in 97% and 92% device identification accuracy for static and mobile device states respectively. Such promising results with identical model and manufacturer devices wherein underlying manufacturing variations are typically low showcase the effectiveness of our design and suggest even higher accuracy across multi-model and multi-manufacturer cards because of the higher manufacturing variations.

***Keywords*—**Fingerprinting, CSI, Carrier Phase Offset (CPO), Device identification and authentication

I. Introduction

Wireless networks are becoming increasingly prevalent and are playing an increasingly important role in our daily lives. As WiFi usage continues to surge, associated threats and security breaches continue to emerge. WiFi networks are particularly vulnerable because of their inherent open medium and easy programmability. Among all WiFi security threats, the rogue APs are the most perilous. A rogue AP is an unauthorized access point masquerading as a trusted original AP, created for launching malicious attacks. When the victim connects to a rogue AP, the adversary can eavesdrop and manipulate user's traffic stealing sensitive and confidential data such as login credentials and bank account information. To counter such identity (impostor) attacks, WLAN administrators rely on cryptographic mutual authentication schemes between clients and APs (e.g. 802.11i RSNA). While these measures do strengthen security, unfortunately, they are not free from vulnerabilities as pointed out by previous studies [1]–[3]. For this reason, many research studies have used indispensable but benign transmitter imperfections manifested in the emitted signal and measurable remotely, as an additional mechanism for device authentication. Certainly, this is a promising direction because the cost of forging hardware impairments is the deterrent thereupon providing reliable and robust means for identification [4].

Limitations of Prior Art: Over the past decade, multiple solutions have been proposed to utilize the hardware imperfections as a means for distinguishing the identity of the users. For instance, ref [5] uses IQ offset and SYNC correlation as an identification feature. They reported 99% identification accuracy using custom hardware (VSA, USRP). However, customized hardware hinders the wide-scale deployment and usability of the system. Another system [3] identifies wireless transmitters by measuring imperfections of a digital-to-analog converter (DAC) and the power amplifiers (PA). The nonlinearities of the PA are measured using a commercial power amplifier, but nonlinear variations of the DAC were simulated. Although simulation provides new knowledge without hands-on experiments, it is difficult to validate the usability in real applications. Recently, Hua et. al. [2] found a way to use custom hardware for device identification by mining carrier frequency offset (CFO) from CSI measurements. CFO is a hardware-specific feature that arises because of the mismatch of carrier frequency between TX and RX oscillators. It is distinct for different wireless devices. They eliminate the need for custom hardware and achieve a high identification accuracy of 94%. Unfortunately, their system is sensitive to channel fluctuations and device movement. This is because, they use consecutive packets to filter the channel and during the measurement process, if the channel is changing the estimated CFO will be corrupted by the channel residues. Yet another constraint of their system is the stationarity of TX and RX. These constraints make the authentication process uncomfortable and error-prone in real-life settings. The restraint in movement results because in addition to the mismatch between oscillator carrier frequencies, the Doppler effect also contributes to CFO, thus making it variable and sensitive to movement.

Motivation and Proposed Approach: To make the system

978-1-7281-0962-6/19/$31.00 ©2019 IEEE

robust to fluctuating channel and movement, in this study we propose an alternative but insensitive hardware noise for fingerprinting. Specifically, we propose to use the difference of relative phase differences of multiple RF oscillators on a single commodity transmitter as a distinctive identifying feature. Modern commodity cards support multiple antennas, for example, Intel 5300 card has three antenna ports each with a different analog front-end. The RX and TX local oscillators (LO) are not perfectly synchronized in time, frequency and phase. However, according to research on phased-array localization [6]–[8], RF oscillators on a single commodity wireless NIC are frequency-and time-locked preventing their relative phases drifting over time (packets) and frequency (OFDM subcarriers). But, across antennas (space) they have unknown, absolute phase offset relative to one another. Our insight is to exploit this relative phase difference as the signature of the transmitter device. This hardware signature is buried in the raw CSI data of the in-band channel measured at the receiver. It serves as an attractive feature for fingerprinting since it is unaffected by mobility and time. In particular, multiple RF chains within one system experience the same randomness due to movement or channel fluctuations as illustrated in Fig. 2. We extract this transmitter RF phase difference remotely at the receiver using commercial off-the-shelf (COTS) hardware and additionally support mobility in contrast to previous solutions. To the best of our knowledge, no previous study can provide both benefits simultaneously, i.e., support commodity (non-custom) hardware and tolerance to movements within a single system.

Our Contribution: The following summarizes the main contributions of this paper:

- We design the first system that extracts the relative phase differences across multiple RF oscillators within a single commodity TX NIC as a unique device signature.
- We build our system using inexpensive commodity devices and eliminate the use of expensive custom hardware.
- We conducted comprehensive experiments in diverse real environmental settings and results show that our approach is highly effective in determining the device identity even when the devices are moving.
- Our algorithm, using 17 Intel NICs achieves accuracy of 97% and 92% for static and mobile device states respectively.

The rest of the paper is organized as follows. In Section II, we present an overview of CSI and various sources of hardware impairments. Based on this understanding, Section III explains the new technique to generate the fingerprint. In Section IV, we present our experimental results and discuss the effectiveness of the proposed method. Finally, Section V presents future research direction and Section VI concludes the paper.

II. Overview of CSI and Sources of Errors

Our prototype uses COTS 802.11n hardware platform supporting three TX and RX antennas/RF chains as shown in Fig. 1. OFDM receivers continuously monitor wireless channel variations using a fine-grained PHY-layer information (CSI) measured just after the Inverse Fast Fourier Transform (IFFT) block (see Fig. 1). It characterizes the channel properties of the communication link between TX and RX antennas for each OFDM subcarrier. More specifically, if N_{TX} and N_{RX} are the number of transmit and receive antennas respectively, then for Intel 5300 card, CSI is reported for selected 30 OFDM subcarriers resulting in a measurement matrix dimension of $N_{TX} \times N_{RX} \times 30$ for each successfully decoded receiver packet. The received OFDM complex signal vector is modeled as $Y = HX + N$. H is the channel frequency response (*or true CSI*), X is the transmitted symbol vector and N is the AWGN complex noise vector. In an ideal scenario, the matrix H captures the amplitude and phase distortion ($H = |H|e^{-j\psi}$) caused by a wireless channel. But in practice, it is mixed with a variety of phase noises contributed by hardware imperfections and signal processing delays. Previous research studies [9]–[11] corroborate that the reported measurements are mixed with the following hardware errors (also shown in Fig. 1):

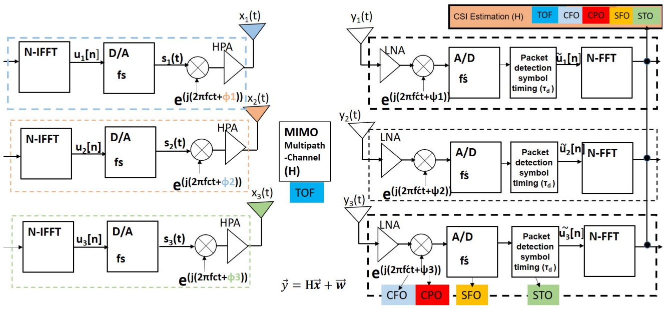


Fig. 1: Illustration of basic components of wireless transreceiver; imperfections of each component adds to the total phase noise.

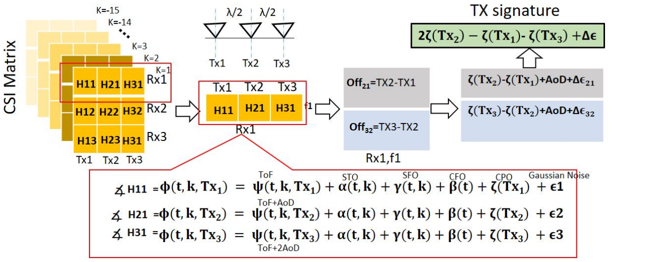

CSI Matrix
K=-15
K=-14
K=3
K=2
K=1
H11 H21 H31 Rx1
H12 H22 H32 Rx2
H13 H23 H31 Rx3
Tx1 Tx2 Tx3
λ/2 λ/2
Tx1 Tx2 Tx3
H11 H21 H31
f1
Rx1
Off21=TX2-TX1
Off32=TX3-TX2
Rx1,f1
ζ(Tx2)-ζ(Tx1)+AoD+Δϵ21
ζ(Tx3)-ζ(Tx2)+AoD+Δϵ32
TX signature
2ζ(Tx2) − ζ(Tx1)- ζ(Tx3) +Δϵ
∡ H11 =ϕ(t, k, Tx1) = ψ(t, k, Tx1) + α(t, k) + γ(t, k) + β(t) + ζ(Tx1) + ϵ1
∡ H21 =ϕ(t, k, Tx2) = ψ(t, k, Tx2) + α(t, k) + γ(t, k) + β(t) + ζ(Tx2) + ϵ2
∡ H31 =ϕ(t, k, Tx3) = ψ(t, k, Tx3) + α(t, k) + γ(t, k) + β(t) + ζ(Tx3) + ϵ3
ToF
ToF+AoD
ToF+2AoD
STO
SFO
CFO
CPO
Gaussian Noise

Fig. 2: The framework for isolating the TX signature by removing the effects of ToF, CFO, SFO and STO.

$$\hat{H}_{t,k,s} = |\hat{H}|_{t,k,s} e^{-j\phi_{t,k,s}} \tag{1}$$

$$\phi_{t,k,s} = \underbrace{\psi_{t,k,s}}_{\text{ToF}} + \underbrace{\alpha_{t,k}}_{\text{STO}} + \underbrace{\gamma_{t,k}}_{\text{SFO}} + \underbrace{\beta_t}_{\text{CFO}} + \underbrace{\zeta_s}_{\text{CPO}} + \underbrace{\epsilon}_{\text{AWGN}} \tag{2}$$

where, $\hat{H}_{t,k,s}$ is the reported *noisy CSI* matrix. $\phi_{t,k,s}$ is the total phase measured that characterizes both channel and hardware noise for a given packet (t), subcarrier index (k) and

Phase Error Sources	CPO	SFO,STO	CFO
Time	constant	variable	variable
Frequency	constant	linear	constant
Space	variable	constant	constant

TABLE I: Dimension vs phase error across multiple RF chains for a single commodity device.

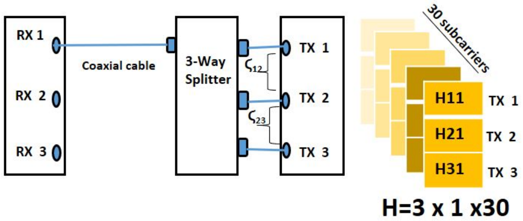


Fig. 3: Wired experimental setup in order to measure the ground truth phase difference for individual NICs .

RF antenna (s). Although the first term due to Time of Flight (ToF) ($\psi_{t,k,s}$) is usually the dominant term of the sum, other summands are non-negligible. Below we briefly explain each of the noise terms. Refer to papers [2], [6], [9]–[11] for more elaborate phase noise information.

$\boldsymbol{\psi_{t,k,s}}$ **:** it is the phase shift introduced by the air, also known as the ToF. This phase varies with time even when the TX-RX are stationary due to diverse multipath fading. It linearly increases with the subcarrier index k. Due to the physical separation of antennas, each antenna receives a slightly delayed version of the signal, i.e., the signal arrives with a different phase resulting in the phase offset across antennas. This offset is a function of antenna separation, the frequency of the carrier signal and the angle of arrival (AoA) and angle of departure (AoD) of the received and the transmitted signal.

$\boldsymbol{\alpha_{t,k}}$ **:** it is the phase shift due to Sampling Frequency Offset (SFO). It is caused by a mismatch of the sampling frequencies of the sender and receiver DAC and analog to digital converter (ADC) respectively. SFO linearly increases with the subcarrier index. It is given by $\alpha_{t,k} = 2\pi k\tau_o/N$, where τ_o is the delay due to sampling frequency mismatch and N is the IFFT length.

$\boldsymbol{\gamma_{t,k}}$ **:** Due to lack of tight time-synchronization between sender and receiver, Symbol Time Offset (STO) occurs. Within, a single device, STO varies linearly with the subcarrier index, is constant across antenna arrays but again varies across samples or time [8]. It is given by, $\gamma_{t,k} = 2\pi k\tau_d/N$, where τ_d is the symbol samples offset.

$\boldsymbol{\beta_t}$ **:** The receiver must lock to the carrier frequency of the TX for decoding the message correctly. The central frequencies cannot be perfectly synchronized. The offset between the TX-RX carrier frequency is termed CFO. It can be modeled as $\beta_t = 2\pi\Delta f_c t$. This quantity is not a function of subcarrier index (k) and is same across 3 receiver antenna elements, but varies across time or frames.

$\boldsymbol{\zeta_s}$ **:** Apart from frequency and time mismatch, the TX and RX mismatch in the initial carrier phase and is termed as carrier phase offset (CPO). Multiple RF elements in a single commodity TX have different initial phase shifts [9] leading to relative constant difference across time and subcarrier frequency. This difference causes a problem in WiFi localization algorithms. Ref. [9] calibrated this error by using equal length coaxial cables as shown in Fig. 3. Another study [7] used specialized vector network analyzer (VNA) equipment for precisely measuring the CPO error. Table I shows the relationship of various phase errors with time, frequency and space for multiple RF chains within a single commodity device.

III. Methodology

As discussed above, the measured phase using commodity hardware is a complex mixture of phase shift caused by the propagation path (medium) as well as noise-induced by a variety of hardware components at sender and receiver devices. Previous research methods based on hardware-specific fingerprinting utilize a single or combination of these hardware noises to fingerprint. For example, most recent work [2] used CFO as the fingerprint of a device. They have an elegant system design. However, the time-sensitivity of CFO restricts mobility hindering usability. We note from Eq. (2) that, excluding CPO all other phase terms vary either with time and/or frequency. Only CPO is constant for a given RF oscillator with time and frequency. When a single TX chain is used, it is difficult to filter out CPO from the received phase mixture. However, modern transmitters and receivers support multiple chains that are frequency and time locked. We exploit this extra spatial dimension offered by modern MIMO devices to extract the relative difference of CPO as our fingerprint. We filter out other time-varying phase factors and keep only the relative phase offset solely contributed by the multiple RF chains within a single transceiver as a device signature. Since this offset is constant with time and frequency, it is an attractive choice for fingerprinting.

A. *Design Rationale: Physical Modeling of MIMO channel*

Transmitter sends three streams per symbol time $[x1(t), x2(t), x3(t)]$ as shown in the block diagram Fig.1. Transmission rate such as 0x1c911 forces all three TX chains to be used for sending the data. Geographically-separated transmit antennas causes different AoD of the transmitted signal. Similarly, the antenna separation at the receiver, causes AoA at the receiver. For MIMO channel, with spatially separated antennas the channel matrix H incorporates the extra phase due to AoA and AoD. Since, we are interested in measuring the phase difference across the transmitter antennas, we slice the measured CSI matrix as shown in Fig. 2. The total phase for each antenna can be modeled as:

$$\phi_{t,k,1} = \psi_{t,k,1} + \alpha_{t,k} + \gamma_{t,k} + \beta_t + \zeta_1 + \epsilon_1 \tag{3}$$

$$\phi_{t,k,2} = \psi_{t,k,2} + \alpha_{t,k} + \gamma_{t,k} + \beta_t + \zeta_2 + \epsilon_2 \tag{4}$$

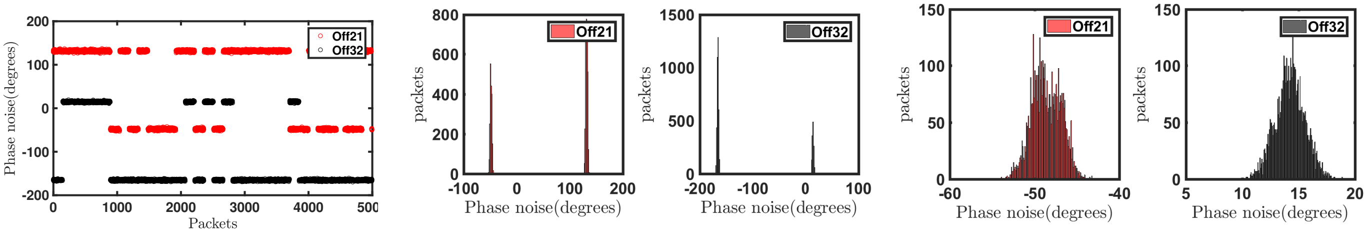
$$\phi_{t,k,3} = \psi_{t,k,3} + \alpha_{t,k} + \gamma_{t,k} + \beta_t + \zeta_3 + \epsilon_3 \tag{5}$$

Please refer to Section II for meaning of each of the symbols in the above equations. When there is no separation between antennas or channel is highly correlated, there is no AoA or AoD, and the phase due to channel is the same for all antennas i.e. $\psi_{t,k,1} = \psi_{t,k,2} = \psi_{t,k,3}$. This implies, that the relative difference between the TX chains can be calculated just by taking difference of CSI across MIMO antennas.

$$\Delta\phi_{t,k,21} = \phi_{t,k,2} - \phi_{t,k,1} = \zeta_2 - \zeta_1 + \Delta\epsilon_{21} \tag{6}$$

$$\Delta\phi_{t,k,32} = \phi_{t,k,3} - \phi_{t,k,2} = \zeta_3 - \zeta_2 + \Delta\epsilon_{32} \tag{7}$$

Eq. (6) and (7) contains relative hardware phase noise mixed with some added normal white noise. To access this hardware



(a) (b) (c)

Fig. 4: Wired experiment: phase offset between RF chains. (a)The measured phase difference between antenna 1 and 2 (Off21), and antenna 2 and 3 (Off32) for 5000 packets. Note the phase shift of ±π. (b) Histogram of phase difference before preprocessing (c) Histogram of measured phase difference after preprocessing step.

noise is dominant and extract-able, we observe the distribution of a large number of samples using multipath free wired experiments. If this metric is differentiable from Gaussian noise, it should manifest a steady structure across packets while the Gaussian noise is likely to have a more random structure. To test our hypothesis, we conduct preliminary wired experiments which we describe next.

B. *Observation with Wired Experiments*

We conducted controlled wired experiments using three-way power splitter and coaxial cables with a setting shown in Fig. 3, wherein complex multipath is not present (or minimized). To ensure that the splitter and cables did not contribute extra phase noise in our measurements, we tested them using VNA. This step is not necessary and is used just for verifying that no extra noise was being added by these components. We transmitted 5000 packets using a carrier frequency of 5.59 GHz (channel 116 HT 40+) using packet injection mode. We repeated the experiment with 9 Intel Mini card and 8 Intel Half Mini card form factor (see Fig. 6(c)). From our experiment results, we could see stable phase difference between antennas, however, they clustered in different bands as shown by Fig. 4. We noticed these bands were ± π apart (see Fig. 4(a)). A similar observation was made in [12], [13]. The cause of this ambiguity is specific to Intel 5300 card. Its firmware reports the phase of the channel modulo $\pi/2$ (instead of the modulo 2π) as reported by [9], [14]. To fix this ambiguity we simply add or subtract $\pm\pi$ from the phase difference between the two antennas, if the measured phase difference is smaller or bigger than the maximum possible phase difference range of [-$\pi/2$ +$\pi/2$]. After this preprocessing step, only one cluster remains as shown in Fig. 4(c). We calculate the phase difference for 17 NICs using Eq. (6) and Eq. (7) and visualize the result via 2D plot (see Fig. 5). From visual inspection, we see that the Mini and Half Mini Intel NICs form two different clusters and are distinguishable. Also within each cluster, most of the devices have different features and are separable. Only a few of them overlap considerably and we use a standard neural network to separate their identity with higher accuracy. While the wired setup is not practical for real-world device identification, it suggests a promising direction toward using the relative phase difference of RF oscillators as a unique MIMO-device identification feature.

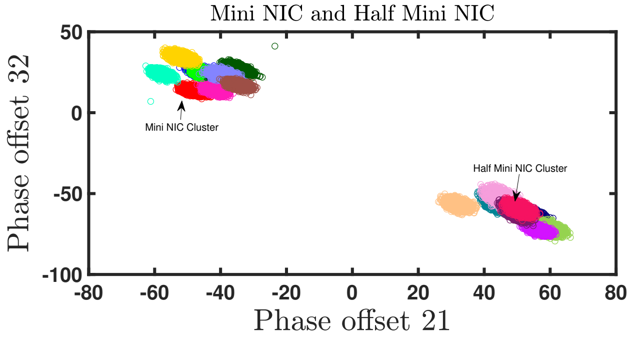


Fig. 5: Estimated phase difference Off21 (TX2 - TX1) and Off32 (TX3 - TX2) for 9 Intel Mini card and 8 Half Mini card. The bottom cluster corresponds to the Half Mini card.

C. *Cancellation of Multipath Effects*

In indoor, multipath rich setting, with perfect antenna separation of $\lambda/2$, Eq. (6) and Eq. (7) changes to following:

$$\Delta\phi_{t,k,21} = \sum_{l=1}^{L} \pi sin(\Theta_l) + \zeta_2 - \zeta_1 + \Delta\epsilon_{21} \tag{8}$$

$$\Delta\phi_{t,k,32} = \sum_{l=1}^{L} \pi sin(\Theta_l) + \zeta_3 - \zeta_2 + \Delta\epsilon_{32} \tag{9}$$

where, L represent number of multipaths, and Θ_l is the angle of departure of the multipath signal l. From above Eq. (8)-(9), it is clear that we cannot directly use the relative phase offset as our fingerprint because it is influenced by the spatial signature or AoD of the transmitted signal. To get rid of the influence of the AoD, we subtract Eq. (8) from Eq. (9) and use this remaining residue as our input to the neural network.

$$TX\ Signature, \Delta\phi = 2\zeta_2 - \zeta_1 - \zeta_3 + \Delta\epsilon \tag{10}$$

Above Eq. (10), is the transmitters fingerprint and in deriving it, we assume that antennas have perfect equal separation and that they receive same set of multipaths. In reality, there may be minute difference in distance between antennas and each antenna may see slightly different set of multipaths. These unavoidable errors may hurt extraction of our signature process and therefore such modeling errors must be compensated for.

D. *Fully connected Neural Network for RF fingerprinting*

We use a standard fully connected deep neural network to do the classification. We calculate higher-order statistical

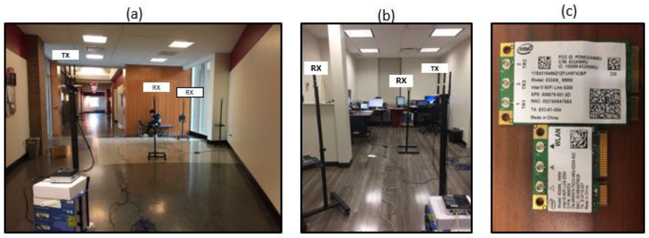


Fig. 6: Wireless experimental setup a) Indoor hallway. b) Small office room (c) Intel adaptor with PCIe Mini Card and Half Mini Card form factor used for data collection.

parameters mean, variance, skewness, and kurtosis for each receiver antenna. These parameters are calculated using a group of 20 samples. Distortions in a metric due to transmitter hardware should manifest themselves consistently across multiple packets, while channel-specific noise and Gaussian thermal noise are likely to have more random structure. Therefore, averaging 20 random samples, we expect to amplify the features caused by the hardware impairments while reducing the effects of the wireless channel and ambient noise. Before feeding this higher-order data, we normalize it using standard score ($\frac{X-\mu}{\sigma}$). The input layer of the neural network is thus a one-dimensional vector that has 12 float numbers:*(RX1: mean, variance, skewness, kurtosis; RX2: mean, variance, skewness, kurtosis; RX3: mean, variance, skewness, kurtosis)*. There are five fully connected hidden layers with the Relu activation function. The output layer uses Softmax activation function and is a one dimensional vector that has probability for each device:*(prob(device1),prob(device2),... prob(device17))*.

It is worth pointing out that it was not our goal to find the best-performing algorithm for classification. Instead, we used a simple structure as a proof of concept. In the future, we shall conduct more extensive experiments and we plan to explore the best performing neural network for classification.

IV. Results and Evaluation Methodology

Settings: Wireless experiments are more challenging as compared to the wired due to the complex multipath environment. To appropriately handle multiple noise sources we transmitted 100,000 packets and used spatial multiplexing (injection code of 0x1c911) to extract the relative phase between the TX antennas. We used 85,000 samples for training and 15,000 for prediction. We experienced, $\pm\pi$ phase uncertainty similar to wired case and employed the same preprocessing technique described earlier. We conducted static, non-line-of-sight (NLOS) and mobile experiments in different indoor room environments (e.g. a hallway, small office room). For our experiments, we manually move the receiver while the transmitter is transmitting packets. When transmitter and receiver are not moving, we obtain an accuracy of 97-98 % while distinguishing among all 17 MIMO transceivers in static indoor settings. And for the mobile case, we obtain 92 % device identification accuracy. Fig. 7 shows the training and validation loss for static and mobile experiments conducted in different indoor rooms. We present the accuracy in Table II.

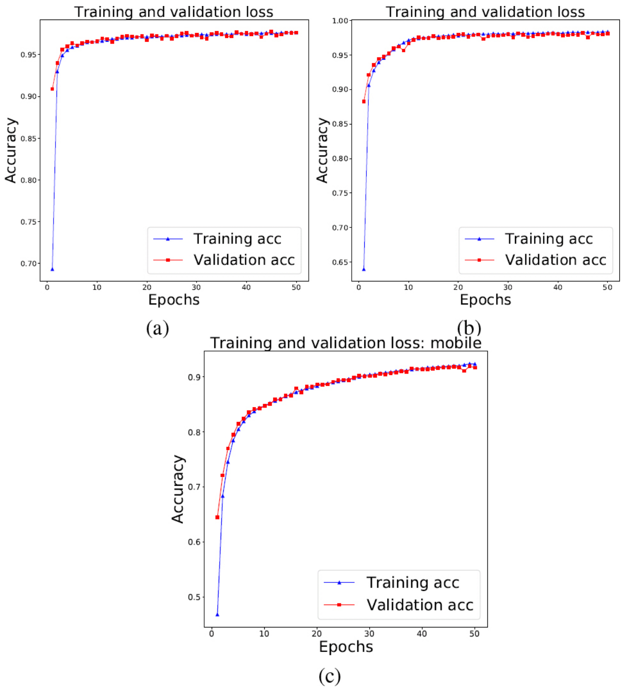


Fig. 7: Wireless results a) Accuracy vs Epochs for Hallway (distance between RX-TX is 8m). b) Accuracy for small office room (distance between RX-TX is 4m). c) Accuracy when the device is mobile (distance between the RX-TX is 3-4m).

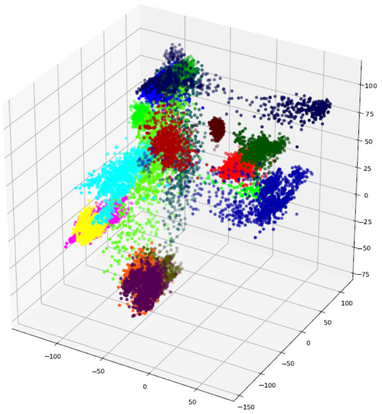


Fig. 8: Visualization of the raw wireless data. Each color represents a different Intel NIC card and each axes represents the residue phase of each RX antenna.

The 3D visualization of the raw data in Fig. 8, clearly shows a structure similar to our wired experiment.

Experiment Setting	Accuracy
Hallway LOS (8 m distance)	97 %
Hallway LOS (4 m distance)	97 %
Small Room NLOS (4 m distance)	98 %
Small Room LOS (4 m distance)	98 %
Small Room, device mobile (4m distance)	92%

TABLE II: Identification accuracy using 17 Intel TX NICs.

V. Related Work

A wide variety of hardware imperfections have been used for fingerprinting and different extracting methods lead to different approaches. In [15], [16], authors use the received signal strength (RSS) to differentiate devices to detect MAC spoofing. They use the received power as a parameter to fit the Gaussian mixture models. In another work [17], authors use a black-box based fingerprinting approach. Here, the input to the black box (AP) is a packet train, and the output is the same packet train shifted in time, shifting pattern being unique to each AP. Although the results were promising the experiments were conducted using emulated traffic. Authors in [18], [19], utilized network traffic features such as data rate, inter-arrival time, frame size e.t.c. for classifying devices. These features however are not related to the device itself and can be exploited by the adversary. In [20] small deviations of the clock skews are proposed as a unique parameter for characterizing physical devices. They use custom hardware for measuring the clock skews. In [21], followed the hardware fingerprinting approach and used machine learning tools on collected modulation data to train classifiers that are then able to distinguish wireless cards, even when produced by the same vendor. Another system called PriLa [22], extracts the CFO and spatial signatures to verify the truthfulness of the users in LBS systems. Most recent work on device fingerprinting [2], mines CFO from CSI eliminating the need for custom hardware and has good accuracy. However, their system is intolerant to the movement and dynamic multipath channel.

VI. Discussion and Future Work

We have investigated a novel approach for fingerprinting utilizing neural networks. The current investigation showcased promising results using a basic neural network. But, the design of the neural network to accommodate different vendors and other real-world impairments during the fingerprinting process should be a matter of further investigation. In future work, we aim to construct a comprehensive database using multiple vendors and do extensive field experiments.

VII. Conclusion

In this work, we presented a new wireless fingerprinting technique for device identification for commodity WiFi equipment supporting the 802.11n protocol. Our results undoubtedly indicate the practical potential of using the difference of the TX chain carrier phase offset as a valid feature for differentiating wireless devices. We fixated on a single vendor as an initial step towards using the phase difference between the antenna chains as a signature. Our optimistic results open up the door to do follow-on studies. In the future, we would like to validate the experimental results with more field experiments, see the effect of aging, temperatures and try out different vendors showing that the system is robust and works in all settings.

VIII. Acknowledgments

This work was funded in part by the US National Science Foundation under grants ECCS -1817463 and CNS-1817438.

References

[1] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 449–462, 2010.

[2] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong, "Accurate and efficient wireless device fingerprinting using channel state information," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*. IEEE, 2018, pp. 1700–1708.

[3] A. C. Polak, S. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE Journal on selected areas in communications*, vol. 29, no. 7, pp. 1469–1479, 2011.

[4] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*. IEEE, 2007, pp. 9–14.

[5] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, 2008, pp. 116–127.

[6] J. Gjengset, J. Xiong, G. McPhillips, and K. Jamieson, "Phaser: Enabling phased array signal processing on commodity wifi access points," in *Proceedings of the 20th annual international conference on Mobile computing and networking*. ACM, 2014, pp. 153–164.

[7] E. Soltanaghaei, A. Kalyanaraman, and K. Whitehouse, "Multipath triangulation: Decimeter-level wifi localization and orientation with a single unaided receiver," in *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 2018, pp. 376–388.

[8] Y. Xie, J. Xiong, M. Li, and K. Jamieson, "md-track: Leveraging multi-dimensionality in passive indoor wi-fi tracking," *arXiv preprint arXiv:1812.03103*, 2018.

[9] J. Xiong and K. Jamieson, "Arraytrack: A fine-grained indoor location system," in *Presented as part of the 10th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 13)*, 2013, pp. 71–84.

[10] M. Kotaru and S. Katti, "Position tracking for virtual reality using commodity wifi," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2017, pp. 68–78.

[11] L. N. Kandel and S. Yu, "Indoor localization using commodity wi-fi aps: Techniques and challenges," in *2019 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2019, pp. 526–530.

[12] M. Schüssel, "Angle of arrival estimation using wifi and smartphones," in *Proceedings of the International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2016, p. 7.

[13] A. Tzur, O. Amrani, and A. Wool, "Direction finding of rogue wi-fi access points using an off-the-shelf mimo–ofdm receiver," *Physical Communication*, vol. 17, pp. 149–164, 2015.

[14] D. Vasisht, S. Kumar, and D. Katabi, "Decimeter-level localization with a single wifi access point," in *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*, 2016, pp. 165–178.

[15] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 mac layer spoofing using received signal strength," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*. IEEE, 2008, pp. 1768–1776.

[16] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Transactions on Parallel and Distributed systems*, vol. 24, no. 1, pp. 44–58, 2013.

[17] K. Gao, C. Corbett, and R. Beyah, "A passive approach to wireless device fingerprinting," in *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*. IEEE, 2010, pp. 383–392.

[18] C. L. Corbett, R. A. Beyah, and J. A. Copeland, "Passive classification of wireless nics during active scanning," *International Journal of Information Security*, vol. 7, no. 5, pp. 335–348, 2008.

[19] C. Neumann, O. Heen, and S. Onno, "An empirical study of passive 802.11 device fingerprinting," in *2012 32nd International Conference on Distributed Computing Systems Workshops*. IEEE, 2012, pp. 593–602.

[20] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 2, pp. 93–108, 2005.

[21] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, 2008, pp. 116–127.

[22] W. Wang, Y. Chen, and Q. Zhang, "Privacy-preserving location authentication in wi-fi networks using fine-grained physical layer signatures," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1218–1225, 2016.