IEEE INFOCOM 2025 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) | 979-8-3315-4370-9/25/$31.00 ©2025 IEEE | DOI: 10.1109/INFOCOMWKSHPS65812.2025.11152893

Radio Fingerprinting of Wi-Fi Devices Through MIMO Compressed Channel Feedback

Francesca Meneghello[*], Khandaker Foysal Haque[†], Francesco Restuccia[†]
[*] Department of Information Engineering, University of Padova, Italy
[†] Institute for the Wireless Internet of Things, Northeastern University, United States

***Abstract*—In this paper, we present `DeepCSIv2`, a data-driven radio fingerprinting (RFP) algorithm to characterize Wi-Fi devices acting as stations (STAs) at the physical layer. Our approach relies on STA-specific hardware impairments extracted from the multiple-input, multiple-output (MIMO) channel state information (CSI) feedback transmitted unencrypted by the STAs to Wi-Fi access points (APs) to establish MIMO transmissions. Recent work showed that such feedback can be effectively used to fingerprint devices acting as APs. In this work, we demonstrate that the same control information can be leveraged to obtain relevant features describing the STAs. Our intuition is that even tiny STA-specific hardware characteristics introduce detectable impairments in the channel estimated by the STA, and percolate in the CSI feedback – consisting of the compressed and quantized channel estimate. `DeepCSIv2` is based on a neural network architecture that automatically extracts the STA's radio fingerprint from the feedback captured over the air and identifies the device. We evaluated `DeepCSIv2` through an extensive data collection campaign using 18 commercial IEEE 802.11ax network interface cards (NICs) of the same type from the same vendor. We considered different experiment configurations, changing the propagation environment and the operational bandwidth. The results show that `DeepCSIv2` reaches an accuracy higher than 96% in identifying the 18 NICs in our dataset. We will share the dataset and RFP code with the community for reproducibility.**

***Index Terms*—Radio fingerprinting, Wi-Fi, MIMO, compressed beamforming feedback, channel sounding.**

I. Introduction

Wireless networks are the dominant approach to deliver communication services to end devices such as smartphones, personal computers, and smart home appliances. As our society becomes more and more digital, the rapid and constant increase in the number of devices requiring wireless connectivity will soon lead to a saturation of the radio spectrum. Indeed, the radio spectrum resources have to be shared among all devices exchanging information through wireless operating technologies in the same area. In this context, a specific challenge is the effective use of the *unlicensed* spectrum where Wi-Fi stations (STAs) and access points (APs) have to coordinate among them and with cellular devices that follow the new-radio unlicensed (NR-U) standard. To enable this, strict and fine-grained dynamic spectrum access (DSA) rules should be defined to allow spectrum administrators to continuously monitor *which* and *when* an unlicensed device is using the spectrum [1]. Cryptographic authentication could help to perform such operations. Still, they require the exchange of private keys among all the nodes in the network, which is challenging, especially when considering devices operating through different technologies.

Radio fingerprinting (RFP) represents a more practical and viable strategy to perform DSA. Specifically, RFP is gaining momentum for device authentication given its ability to identify devices without the need for cryptography. The main idea behind RFP is that each device has some peculiarities that uniquely characterize that specific piece of hardware and percolate in the wireless signals transmitted over the radio channel. Such features are hardware-related – e.g., the length of the radio-frequency chain – and are linked with the different devices (different vendors and/or models), and even with the wireless network interface card (NIC) manufacturing process. Indeed, tiny hardware differences can be present also among devices of the same model from the same vendor, which, in turn, are supposed to be identical as they are produced following the same specifications. Building on this idea, research work in the literature has shown that information about wireless devices can be effectively obtained by analyzing the wireless signals they emit or some related quantities such as the channel state information (CSI) [2]. While the first RFP approaches relied on manual feature extraction [3], [4], recent strategies use deep neural networks (DNNs) to automatically obtain a device fingerprint from the raw radio data [5].

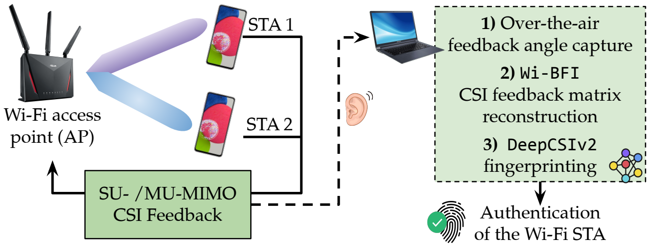

STA 1
STA 2
Wi-Fi access point (AP)
SU- /MU-MIMO CSI Feedback
1) Over-the-air feedback angle capture
2) Wi-BFI CSI feedback matrix reconstruction
3) DeepCSIv2 fingerprinting
Authentication of the Wi-Fi STA

Fig. 1: Main operations of `DeepCSIv2`. The fingerprints of the STAs are extracted from the CSI feedback transmitted unencrypted by the STAs to the AP to enable MIMO operations.

In this work, we present `DeepCSIv2`, a novel technique to fingerprint Wi-Fi multiple-input, multiple-output (MIMO) devices operating in STA mode. As depicted in Figure 1, by leveraging a DNN-based processing, `DeepCSIv2` extracts useful STA-related features and obtain the fingerprint from the CSI data fed back by the terminals to the APs at the end of each *channel sounding* round – a key procedure for enabling MIMO transmissions. The CSI feedback consists of a compressed and quantized version of the channel frequency response (CFR), which describes the way the wireless signals are modified by the radio channel between the AP and the specific STA. This information is estimated by the STA based on a sounding packet broadcasted by the AP and known as null data packet (NDP). Two key features make such CSI feedback highly appealing for RFP. At first, the CFR is obtained from data streams (the NDP) transmitted in a single-input, single-output (SISO) mode by the AP and, in turn, *the channel estimate is not affected by inter-stream or inter-user interference*. Second, *the feedback is transmitted unencrypted* from the STAs to the APs. Hence, any wireless device operating as a spectrum administrator can easily obtain and use such information to authenticate the devices.

Our RFP approach stands upon the `DeepCSI` tool presented in [5], which uses the CSI feedback to identify Wi-Fi devices operating as APs. The idea is that the AP's hardware-related features percolate in the wireless signal carrying the NDP used for the estimation of the CFR. Instead, in this work, we investigate whether such CSI feedback contains information about the specific STA that estimates the CFR. Hence, while `DeepCSI` captures imperfections related to the signal generation and wireless transmission processes, *in `DeepCSIv2` we are looking at hardware peculiarities related to the signal reception and decoding steps*. This makes `DeepCSIv2` to be a different and complementary approach to `DeepCSI`. Indeed, while `DeepCSI` is designed to be implemented on STAs to authenticate the AP, `DeepCSIv2` provides the AP with a means to continuously authenticate the connected STAs. By combining `DeepCSI` and `DeepCSIv2`, spectrum administrators can accurately map all devices in the network.

To the best of our knowledge, `DeepCSIv2` is the first tool to **fingerprint MIMO-enabled Wi-Fi STAs that operate in single-user MIMO (SU-MIMO) or multi-user MIMO (MU-MIMO) mode**, i.e., that use multiple antennas to multiplex information. Other approaches only consider STAs operating in SISO mode [6]–[10] or leveraging MIMO for diversity instead of multiplexing [11], [12]. Moreover, we stress that **our fingerprinting algorithm can run on any Wi-Fi-enabled device** as the fingerprinting primitive is extracted by capturing and analyzing the *CSI feedback transmitted unencrypted over the air*. On the contrary, previous approaches rely on expensive software-defined radios, which are usually unavailable in most scenarios. The only other work adopting a similar approach to ours is `DeepCSI` [5] that targets a different scenario as discussed above. Moreover, `DeepCSIv2` is the first RFP approach evaluated on IEEE 802.11ax-compliant devices (`DeepCSI` was evaluated considering IEEE 802.11ac).

Summary of Novel Contributions

- We devised `DeepCSIv2`, a novel RFP approach for MIMO-enabled Wi-Fi terminals. `DeepCSIv2` obtains the device's fingerprint by capturing and analyzing the CSI feedback consisting of the compressed and quantized CFR periodically (every about 10 ms) obtained by the STAs and transmitted unencrypted to the AP;
- We designed and implemented on commercial Wi-Fi devices a complete pipeline for device authentication at the physical layer using `DeepCSIv2`. The procedure does not require the use of software-defined radio (SDR) and neither to modify the firmware of the channel-monitoring device as `DeepCSIv2` only leverages wirelessly transmitted unencrypted data;
- We performed an extensive data collection campaign with IEEE 802.11ax (Wi-Fi 6) devices for performance evaluation showing that `DeepCSIv2` reaches an accuracy higher than 96% in identifying 18 different commercial-of-the-shelf NICs in different real environments.

II. Related Work

Pioneer approaches to RFP leveraged hand-extracted features obtained from radio signals [2]–[4]. However, they do not scale well with the number of devices and do not generalize to different propagation environments and network setups.

With the advancement of machine and deep learning techniques, new RFP approaches have been proposed [6]–[10]. These techniques allow avoiding manual feature extraction and enable doing it automatically in combination with the identification (classification) task. In particular, in [9], [10], the authors propose to use DNNs to fingerprint ZigBee and LoRa devices. In [7] the authors propose ORACLE, an algorithm to fingerprint Wi-Fi devices by introducing artificial impairments at the transmitter's side. A similar approach has been proposed in [8]. However, without compensation, this strategy leads to a bit error rate (BER) increase. Other contributions in the literature target the compensation of the channel impairments in fingerprinting the radio device through DNN: in [6], [13] finite impulse response (FIR) filters are proposed to do this.

Recent work proposes to leverage the system's diversity gain obtained through multiple antennas at the transmitter and receiver sides to reduce the distortion in retrieving the transmitted signal that is used for device fingerprinting [11], [12]. The authors consider devices adopting space-time block codes (STBC) at the transmitter to improve the received signal-to-noise ratio (SNR) by replicating each information symbol in space using multiple antennas and in time using pre-coding – the Alamouti and the Tarokh codes are respectively considered in the two articles. The fingerprint is then obtained from the reconstruction of the transmitted signal based on the channel estimate performed at the receiver. In particular, the authors target to fingerprint the STA in the network, considering single-user systems. Despite being promising, the proposed approaches have only been tested through MATLAB simulations, and in turn, their actual applicability is unclear. Moreover, the authors consider specific coding configurations, which make the approaches impractical for generalization purposes. Finally, the method in [11], [12] only works for devices that use MIMO to improve the diversity gain (a single data stream is transmitted). Devices that use MIMO for multiplexing, i.e., that simultaneously transmit multiple streams, can not be fingerprinted using the approaches proposed in [11], [12].

To the best of our knowledge, `DeepCSI` [5] is the only work in the literature presenting a RFP algorithm to identify devices that leverage MIMO for multiplexing. As introduced above, `DeepCSI`'s main idea is that the radio imperfections of the Wi-Fi AP percolate in the sounding packets used for channel estimation and, in turn, also affect the CFR that is fed back to the AP for precoding. Hence, `DeepCSI` uses the CSI feedback to obtain a fingerprint of the AP. Moreover,

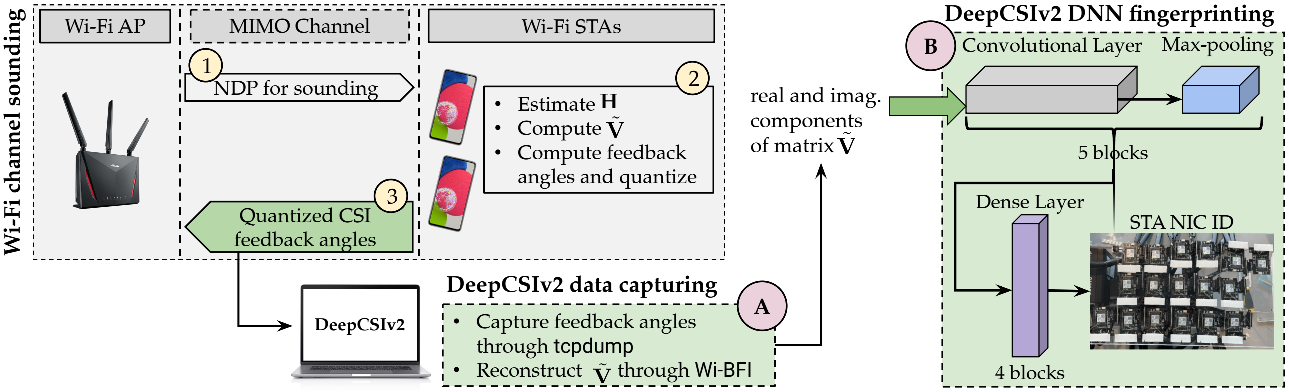

Wi-Fi channel sounding
Wi-Fi AP
MIMO Channel
Wi-Fi STAs
1
NDP for sounding
2
Estimate H
Compute Ṽ
Compute feedback angles and quantize
3
Quantized CSI feedback angles
DeepCSIv2
DeepCSIv2 data capturing
A
Capture feedback angles through tcpdump
Reconstruct Ṽ through Wi-BFI
real and imag. components of matrix Ṽ
DeepCSIv2 DNN fingerprinting
B
Convolutional Layer
Max-pooling
5 blocks
Dense Layer
STA NIC ID
4 blocks

Fig. 2: DeepCSIv2 leverages the channel sounding procedure used in IEEE 802.11 networks to enable SU- and MU-MIMO. The STA fingerprint is extracted from the CFR feedback transmitted at the end of the sounding by the STAs to the AP.

DeepCSI is the only RFP approach that can be performed by any device empowered with a Wi-Fi NIC used to monitor the wireless channel. Indeed, the other RFP approaches require the use of SDRs to analyze the radio signals and perform fingerprinting. Such expensive and very specialized equipment is not widely available in common Wi-Fi networks. However, DeepCSI has been designed and tested for fingerprinting Wi-Fi APs only, i.e., the DNN has been trained to detect the circuitry imperfections associated with the device transmitting the NDP for channel sounding (see Section III). In this work, we propose DeepCSIv2, a DNN-based framework that complements DeepCSI and enables RFP of STAs, i.e., the devices that perform the channel estimation based on the NDP.

III. System Model

We consider a Wi-Fi network following the IEEE 802.11ax standard, where an AP empowered with M antennas serves a set $\mathcal{I}$ of Wi-Fi STAs empowered with N_i antennas each. By leveraging the spatial diversity derived from the multiple transmitting and receiving antennas, the AP can simultaneously transmit multiple streams to one or multiple STAs. These transmission modes are referred to as SU-MIMO and MU-MIMO, respectively, and are key to support the increasing demand for connectivity and the growth in the number of connected devices while guaranteeing an adequate quality of service (QoS) to the end users. SU-MIMO and MU-MIMO transmissions require the AP to combine (*precode*) the data streams to be simultaneously transmitted to the connected STAs by means of specific precoding weights. This operation aims at reducing the interference among the transmitted streams enabling proper decoding at the different receivers. The main idea is to make each data stream directed to a specific STA *orthogonal* to the MIMO link between the AP and the other STAs. In this way, the channel impairments cancel out the data stream intended for a specific STA when the stream propagates through the wireless channel directed to all the other STAs. In turn, the stream will not cause interference at other STAs' receiver and each STA only receives the data directed to it. Residual interference linked with imperfect orthogonality between the streams and the channels is compensated through interference cancellation.

The precoding weights are derived by the AP from the wireless channel estimates (CFR, denoted as $\mathbf{H}_i$) of the links between itself and the connected STAs. Such estimation is performed at the STAs once triggered by the AP through the transmission of a sounding packet called NDP. The procedure, referred to as *channel sounding*, is depicted on the left part of Figure 2. The NDP (step 1 in Figure 2) is a packet that only contains training symbols, i.e., sequences of symbols that are well known by the STAs as they are defined in the IEEE 802.11 standards [14]. The NDP is decoded at each STA and used to estimate the CFR over all the orthogonal frequency-division multiplexing (OFDM) sub-channels (step 2 in Figure 2). This provides an $N_i \times M \times K$ CFR matrix $\mathbf{H}_i$, where K is the number of sub-channels considered for OFDM transmissions. *The CFR is compressed and quantized before being fed back to the AP* to reduce the time the channel is occupied with control data (airtime overhead of the channel sounding). Specifically, $\mathbf{H}_i$ is first decomposed through singular value decomposition (SVD). Hence, only the first $N_{\text{ss},i}$ columns of the right singular matrix $\tilde{\mathbf{V}}_i$ are retained and further compressed by applying Givens rotations (see Chapter 13 of [15]), where $N_{\text{ss},i} < N_i$ represents the number of spatial streams the STA is served with by the AP. The output of this procedure consists of a set of ϕ and ψ values called *feedback angles* that are quantized using a number of bits that depends on the specific device configuration and varies from a minimum of 2 to a maximum of 9 (see [16]). The number of ϕ and ψ feedback angles depends on the MIMO configuration, i.e., M and $N_{\text{ss},i}$. The quantized values are then packed into a *Not Robust Action Frame* that is transmitted without encryption to guarantee low latency (step 3 in Figure 2). Upon reception of the quantized angles, the AP reconstructs the compressed CFR $\tilde{\mathbf{V}}_i$ and uses it to obtain the precoding weights through zero forcing. We refer interested readers to [5] for a complete overview of the channel sounding procedure including feedback compression and quantization.

IV. DeepCSIv2 Radio Fingerprinting Design

Our proposed DeepCSIv2 RFP approach leverages $\tilde{\mathbf{V}}_i$ to obtain a fingerprint of STA i using DNNs. The procedure is summarized in Figure 2, which describes how the fingerprinting device takes advantage of the channel sounding procedure to authenticate the STA. Specifically, the fingerprinting device collects the Not Robust Action Frames containing the compressed and quantized CFR through a Wi-Fi NIC set in monitor mode (block A in Figure 2). Hence, the ϕ and ψ angles are extracted, decoded – no decryption is needed since the angles are transmitted unencrypted (see Section III) – and used to reconstruct the compressed $N_{\mathrm{ss},i} \times M \times K$-dimensional CFR matrix $\tilde{\mathbf{V}}_i$, which is a proxy of the CFR $\mathbf{H}_i$. We used the `Wi-BFI` tool to perform these operations [17].

At this point, the $\tilde{\mathbf{V}}_i$ matrix is processed by a DNNs-based data-driven classifier that extracts relevant STA-specific features from $\tilde{\mathbf{V}}_i$ and identifies the STA (block B in Figure 2). The classifier is depicted on the right part of Figure 2 and is described in the following. The algorithm takes as input the real and imaginary parts of $\tilde{\mathbf{V}}_i$, stacked into an $N_{\mathrm{row}} \times N_{\mathrm{col}} \times N_{\mathrm{ch}}$ matrix. Specifically, the different spatial streams are combined over the row dimension ($N_{\mathrm{row}} \leq N_{\mathrm{ss},i}$), the OFDM sub-channels over the columns ($N_{\mathrm{col}} \leq K$), and the transmit antennas over the channel dimension ($N_{\mathrm{ch}} < 2M$, where the 2 factor is for the real and imaginary parts). The DNN consists of five convolutional layers with 128 filters each, and kernel sizes of $(1, 7)$ for the first three layers, $(1, 5)$ for the fourth layer and $(1, 3)$ for the last one. The `selu` activation function [18] is used after each convolutional layer, followed by a max-pooling layer with $(1, 2)$ kernel. The output of the last max-pooling layer is forwarded through an attention block following the structure described in [5]. Thanks to this block, the algorithm learns where the most relevant information is located within the feature maps and focuses on such regions to obtain effective fingerprints. A skip connection is implemented by summing the output of the attention block with its input. The result is flattened and forwarded through three dense layers with `selu` activation. Alpha-dropout is applied between the three dense layers with a retain probability of 0.5 and 0.2, respectively. The classification is performed through a final dense layer with `softmax` activation and a number of output neurons equal to the number of STAs (NICs) to be identified.

After being trained through $\tilde{\mathbf{V}}_i$ samples collected from the different STAs to be identified, the `DeepCSIv2` algorithm allows associating an input $\tilde{\mathbf{V}}_i$ with the STA that is the most probable generator of such information.

V. Experimental Setup

The experimental evaluation of `DeepCSIv2` was conducted using the WiSEC testbed, a large-scale, multi-NICs, and multi-band platform designed for testing Wi-Fi networks. WiSEC is equipped with an ASUS B250 motherboard featuring 18 PCIex1 slots, each hosting an Intel AX210 Wi-Fi NIC implementing the IEEE 802.11ax standard. The WiSEC testbed is depicted in Figure 3, where 4 NICs are highlighted. For `DeepCSIv2` evaluation, the 18 WiSEC NICs were used as STAs. The AP was implemented through an ASUS RT-AX86U (AX5700) router (see Figure 4 on the upper left).

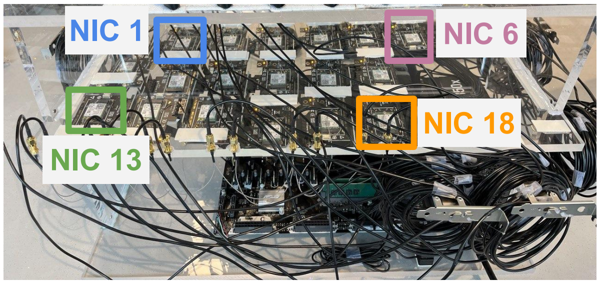
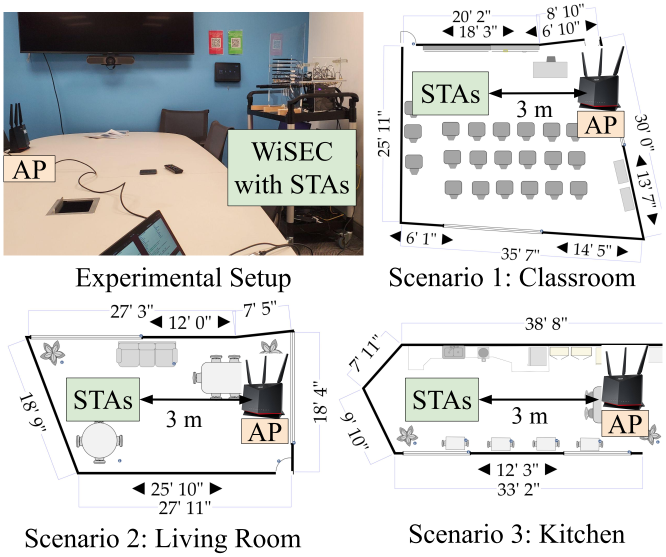


Fig. 3: WiSEC testbed consisting of 18 Intel AX210 Wi-Fi NICs. For data collection, each NIC has been connected subsequentially to the AP using the same 2 antennas and cables to avoid introducing hardware features not related to the NICs.



Experimental Setup

Scenario 1: Classroom

Scenario 2: Living Room

Scenario 3: Kitchen

Fig. 4: Experimental setup consisting of an IEEE 802.11ax AP and the WiSEC testbed for `DeepCSIv2` evaluation. The maps of the three scenarios for data collection are also reported.

A laptop PC empowered with an Intel AX200 NIC has been used as the monitor device to collect the feedback angles and retrieve the compressed $\tilde{\mathbf{V}}_i$ matrices for fingerprinting. Through this setup, *we are the first to evaluate the effectiveness of IEEE 802.11ax device fingerprinting using a commercial laptop as the monitor*. Indeed, the only other work using COTS hardware as the fingerprinting device is `DeepCSI` that considered an IEEE 802.11ac system. The `tcpdump` network analyzer tool has been used for capturing the over-the-air feedback transmission. Hence, the `Wi-BFI` tool allowed reconstructing the $\tilde{\mathbf{V}}_i$ matrices from the captured angles [17]. An example of reconstructed $\tilde{\mathbf{V}}_i$ matrix over the OFDM sub-channels for two transmitter antennas and two streams is reported in Figure 5 while Figure 6 shows the time evolution of $\tilde{\mathbf{V}}_i$ over multiple frames for the different OFDM sub-channels.

We collected the data for training the `DeepCSIv2` algorithm by considering a SU-MIMO network where only one STA (NIC) at a time was connected to the AP. However, the same data can be collected also in a MU-MIMO system. To generate traffic that triggers the transmission of CSI feedback from the STA to the AP, we established TCP `iperf` sessions from the STA to the AP, simulating typical data transmissions. *Note that for data collection we connected every NIC of WiSEC to the same pair of antennas through*

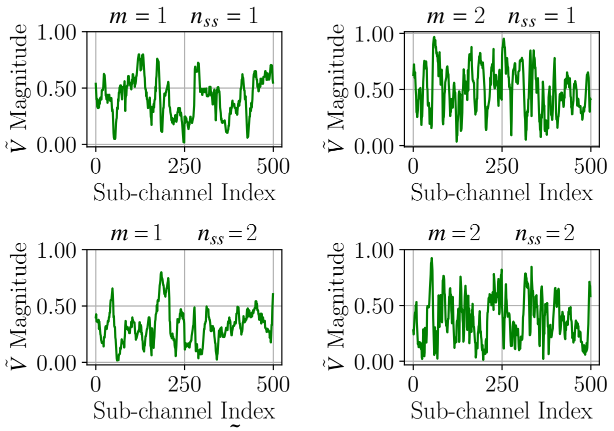


Fig. 5: Example of the $\tilde{\mathbf{V}}_\mathbf{i}$ magnitude at each sounded OFDM sub-channel for different transmit antennas $m \in \{0, \dots, M-1\}$ and spatial streams $n_{\rm SS} \in \{0, \dots, N_{\rm SS}-1\}$ for the considered 4×2 IEEE 802.11ax system operating at 160 MHz.

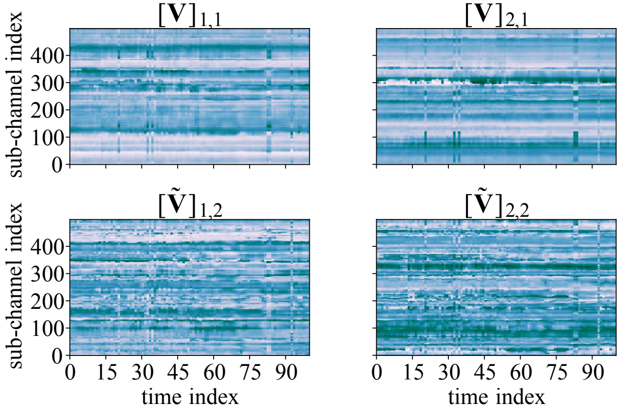
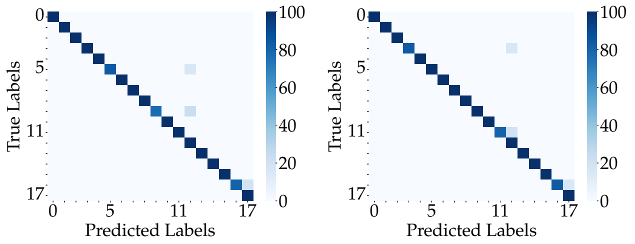


Fig. 6: Example of the time evolution of $\tilde{\mathbf{V}}$ for the considered 4×2 IEEE 802.11ax system at 160 MHz. The columns refer to different transmit antennas (first subscript of $\tilde{\mathbf{V}}$) while the rows refer to the spatial stream (second subscript of $\tilde{\mathbf{V}}$).

identical RF extension cables. Moreover, the antennas were maintained in the same physical location for all the different data collection rounds. This setting ensures consistent signal capture conditions across all the NICs. By removing any possible difference between the data collected for the different NICs, the DeepCSIv2 system is forced to extract the most characteristic features of the NICs (STAs) themselves.

As presented in Figure 4, we collected the CSI feedback of each of the STAs with the exact same setup in three different environments – a classroom, a living room, and a kitchen. In each environment, the data is collected with the same location of the AP, and the NIC's antennas. The connection was established on channel 36 for each of the NICs across the different experimental scenarios considering different operational bandwidths ranging from 20 MHz to 160 MHz. This results in a different number of OFDM sub-channels K used for data transmission and, in turn, considered for the channel estimation and included in the feedback. In each different configuration (environment and bandwidth) we collected about 1500 CSI feedback frames for each NIC.



(a) 20 MHz, 96.56% (b) 160 MHz, 99.97%

Fig. 7: Confusion matrices describing the DeepCSIv2 fingerprinting accuracy in the living room when using the first spatial stream. The percentages represent the average accuracy.

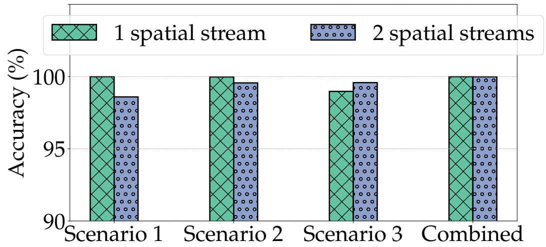


Fig. 8: Classification accuracy of DeepCSIv2 in fingerprinting 18 NICs in the three scenarios, using 160 MHz bandwidth, and considering the data for one (first) or two data streams.

VI. Performance Evaluation

We evaluated DeepCSIv2's performance on the different scenarios considering different numbers of spatial streams, bandwidths, and numbers of NICs to be identified. Each dataset have been split into training, validation, and test sets, respectively accounting for the 70%, 15%, and 15% of the data. As the datasets are balanced among the different NICs, we considered the accuracy as the performance metric.

To begin with, Figure 7 shows the confusion matrices obtained when using the first spatial stream to fingerprint the Wi-Fi STAs in the living room. The colorbar indicates the accuracy. The results, obtained considering both a 20 MHz and a 160 MHz channel, show that the average accuracy exceeds 96%. A 3% accuracy improvement is visible when expanding the bandwidth by four times as this increases the number of sub-channels that are used for fingerprinting from 242 to 1024.

The average accuracy when training and testing DeepCSIv2 in the three evaluation scenarios using only the first spatial stream ("1 spatial stream") or considering the data for both the streams ("2 spatial streams") is reported in Figure 8. The values show that obtaining the fingerprint through data associated with the first stream is in general more reliable than also accounting for the subsequent stream due to the error propagation in the compression and quantization procedure that generates the feedback (a deeper analysis can be found in [5]). This makes the second spatial stream noisier than the first one and, in turn, adding this data degrades the fingerprinting performance. As the results show, only in the third scenario performance slightly increases when adding the second stream data, while it decreases for scenarios 1 and 2. The last set of bars refers to the accuracy obtained when the fingerprinting is trained on data collected in all

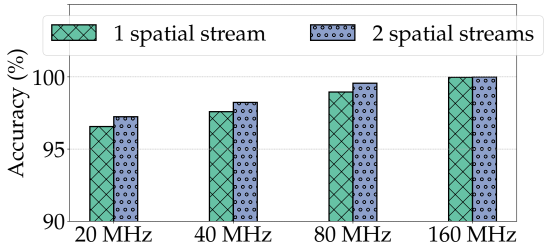


Fig. 9: Classification accuracy of DeepCSIv2 in fingerprinting 18 NICs when using different operational bandwidths, and considering the information for one (first) or two data streams. The results are averaged over all the evaluation scenarios.

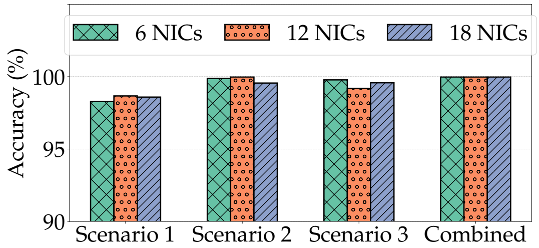


Fig. 10: Classification accuracy of DeepCSIv2 in fingerprinting 6, 12, and 18 NICs in three different scenarios in Figure 4, using a bandwidth of 160 MHz and 2 antennas.

the scenarios. By doing this, the classification accuracy approaches 100%, demonstrating an improvement in the effectiveness of the extracted fingerprints in identifying the STAs. Indeed, when trained on data collected in different propagation environments, DeepCSIv2's DNNs is forced to learn environment-independent features for fingerprinting. In turn, more effective and representative STA-specific features are extracted to build the radio fingerprint.

In Figure 9, we deepen the evaluation of the fingerprinting performance when changing the bandwidth, considering 40 MHz and 80 MHz in addition to the already mentioned 20 MHz and 160 MHz. The results considering one and both the spatial streams are reported. As introduced in Figure 7, an increase in the fingerprinting accuracy can be appreciated when increasing the bandwidth as more sub-channels allow obtaining more representative features. As a final evaluation, in Figure 10 we assess the impact of the number of NICs in the dataset on the accuracy. The results confirm that DeepCSIv2 is scalable and effectively works with different numbers of STAs to be identified. Indeed, in all the environments and when combining their data, the accuracy remains almost stable when considering different numbers of NICs.

VII. Concluding Remarks

In this work, we presented DeepCSIv2, the first tool to radio fingerprint Wi-Fi NICs operating as STAs in SU-MIMO/MU-MIMO networks. DeepCSIv2 leverages the CSI feedback transmitted unencrypted by each STA in a Wi-Fi network to enable SU-MIMO/MU-MIMO. Being computed by the STAs, the feedback is affected by small STA-specific hardware impairments and, in turn, it can be used to fingerprint the device. This allows performing RFP without specialized hardware like SDR. Indeed, DeepCSIv2 can be executed on any commercial Wi-Fi-enabled device, e.g., laptop or smartphone. We implemented DeepCSIv2 and evaluated its performance using 18 IEEE 802.11ax NICs deployed in three different environments. The proposed approach exceeds 96% accuracy in all situations.

Acknowledgments

This work is funded in part by the National Science Foundation (NSF) grant CNS-2134973, ECCS-2229472, and ECCS-2329013, by the Air Force Office of Scientific Research under contract number FA9550-23-1-0261, by the Office of Naval Research under award number N00014-23-1-2221.

References

[1] J. Horwitz, V. Beat, "Wi-Fi 6E and 5G Will Share 6GHz Spectrum to Supercharge Wireless Data." https://tinyurl.com/wyvmn5c, 2020.

[2] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, "Fingerprinting Wi-Fi Devices Using Software Defined Radios," in *Proc. of ACM WiSec*, 2016.

[3] 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 of Things Journal*, vol. 6, no. 1, pp. 349–360, 2019.

[4] T. Zheng, Z. Sun, and K. Ren, "FID: Function Modeling-based Data-Independent and Channel-Robust Physical-Layer Identification," in *Proc. of IEEE INFOCOM*, 2019.

[5] F. Meneghello, M. Rossi, and F. Restuccia, "DeepCSI: Rethinking Wi-Fi radio fingerprinting through MU-MIMO CSI feedback deep learning," in *2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS)*, pp. 1062–1072, IEEE, 2022.

[6] 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 ACM MobiHoc*, 2019.

[7] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "ORACLE: Optimized Radio clAssification through Convolutional neuraL nEtworks," in *Proc. of IEEE INFOCOM*, 2019.

[8] S. Riyaz, K. Sankhe, S. Ioannidis, and K. Chowdhury, "Deep Learning Convolutional Neural Networks for Radio Identification," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 146–152, 2018.

[9] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep Learning for RF Device Fingerprinting in Cognitive Communication Networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 160–167, 2018.

[10] R. Das, A. Gadre, S. Zhang, S. Kumar, and J. M. Moura, "A Deep Learning Approach to IoT Authentication," in *Proc. of IEEE ICC*, 2018.

[11] N. Basha, B. Hamdaoui, K. Sivanesan, and M. Guizani, "Channel-resilient deep-learning-driven device fingerprinting through multiple data streams," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 118–133, 2023.

[12] B. Hamdaoui, N. Basha, and K. Sivanesan, "Deep learning-enabled zero-touch device identification: Mitigating the impact of channel variability through MIMO diversity," *IEEE Communications Magazine*, vol. 61, no. 6, pp. 80–85, 2023.

[13] S. D'Oro, F. Restuccia, and T. Melodia, "Can You Fix My Neural Network? Real-Time Adaptive Waveform Synthesis for Resilient Wireless Signal Classification," in *Proc. of IEEE INFOCOM*, 2021.

[14] IEEE, "IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN," *IEEE Std 802.11ax-2021 (Amendment to IEEE Std 802.11-2020)*, 2021.

[15] E. Perahia and R. Stacey, *Next Generation Wireless LANs: Throughput, Robustness, and Reliability in 802.11n.* Cambridge Univ. Press, 2008.

[16] F. Meneghello, K. F. Haque, and F. Restuccia, "Evaluating the Impact of Channel Feedback Quantization and Grouping in IEEE 802.11 MIMO Wi-Fi Networks," *IEEE Wireless Communications Letters*, 2024.

[17] K. F. Haque, F. Meneghello, and F. Restuccia, "Wi-BFI: Extracting the IEEE 802.11 Beamforming Feedback Information from Commercial Wi-Fi Devices," in *Proc. of ACM WiNTECH*, 2023.

[18] G. Klambauer, T. Unterthiner, A. Mayr, and S. Hochreiter, "Self-Normalizing Neural Networks," in *Proc. of ACM NIPS*, 2017.