Wi-BFI: Extracting the IEEE 802.11 Beamforming Feedback Information from Commercial Wi-Fi Devices

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

ABSTRACT

Recently, researchers have shown that the beamforming feedback angles (BFAs) used for Wi-Fi multiple-input multiple-output (MIMO) operations can be effectively leveraged as a proxy of the channel frequency response (CFR) for different purposes. Examples are passive human activity recognition and device fingerprinting. However, even though the BFAs report frames are sent in clear text, there is not yet a unified open-source tool to extract and decode the BFAs from the frames. To fill this gap, we developed `Wi-BFI`, the first tool that allows retrieving Wi-Fi BFAs and reconstructing the beamforming feedback information (BFI) – a compressed representation of the CFR – from the BFAs frames captured over the air. The tool supports BFAs extraction within both IEEE 802.11ac and 802.11ax networks operating on radio channels with 160/80/40/20 MHz bandwidth. Both multi-user and single-user MIMO feedback can be decoded through `Wi-BFI`. The tool supports real-time and offline extraction and storage of BFAs and BFI. The real-time mode also includes a visual representation of the channel state that continuously updates based on the collected data. **`Wi-BFI` code is open source and the tool is also available as a pip package[1].**

CCS CONCEPTS

• **Networks** → **Network experimentation**; **Network measurement**; • **Hardware** → **Wireless devices**.

KEYWORDS

Wi-Fi, beamforming, compressed beamforming feedback, multiple-input multiple-output (MIMO)

[1]https://github.com/kfoysalhaque/Wi-BFI

ACM WiNTECH' 23, October 6, 2023, Madrid, Spain

ACM ISBN 979-8-4007-0340-9/23/10…$15.00
https://doi.org/10.1145/3615453.3616514

ACM Reference Format:
Khandaker Foysal Haque[†], Francesca Meneghello[*] and Francesco Restuccia[†] . 2023. `Wi-BFI`: Extracting the IEEE 802.11 Beamforming Feedback Information from Commercial Wi-Fi Devices. In *The 17th ACM Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization 2023 (ACM WiNTECH' 23), October 6, 2023, Madrid, Spain.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3615453.3616514

1 INTRODUCTION

Wi-Fi is the technology of choice for plug-and-play Internet connectivity in indoor environments such as homes, offices, shopping malls, and university campuses. Around 19.5 billion of Wi-Fi devices are currently deployed worldwide and their number is expected to increase with around 3.8 billion of devices shipped annually [1].

To support the increasing demand for connectivity, modern Wi-Fi systems rely on multiple-input multiple-output (MIMO) technology that allows concurrently transmitting several data streams to multiple receivers (*beamformees*). MIMO leverages the channel frequency response (CFR) estimate performed by the beamformees during channel sounding to obtain precoding parameters for each data stream at each transmitter antenna. The estimate is referred to as the beamforming feedback information (BFI) and is transmitted by the beamformees to the transmitter (*beamformer* in a compressed form – the beamforming feedback angles (BFAs) (see Section 2.1). Interestingly, *the BFAs are transmitted in clear text* and, in turn, can be captured by any network analyzer, e.g., Wireshark, and decoded without the need for decryption. This characteristic makes the *compressed BFAs an appealing proxy to the CFR* to obtain information about the radio propagation channel. In turn, BFAs (and BFI) can be used for a wide range of applications that span from network optimization to wireless sensing.

To enable this new paradigm, we developed `Wi-BFI`, the first tool that allows parsing the BFAs frames to extract the beamforming angles, and reconstruct the BFI. An overview of `Wi-BFI` is depicted in Figure 1. `Wi-BFI` can concurrently extract the BFAs transmitted by devices implementing different Wi-Fi standards, and operating on channels with different bandwidths. For example, `Wi-BFI` can simultaneously extract the BFAs of an IEEE 802.11ac compliant device at

40 MHz (station 1 in Figure 1), and an IEEE 802.11ax compliant device at 160 MHz (station 2 in Figure 1) through a single capture. `Wi-BFI` does not require access to the monitored devices in the MIMO network. Contrarily, extracting the CFR requires physical access and firmware modifications of the monitored devices [2]. Because of this, state-of-the-art work has shown significant interest in BFI [3, 4]. Recent work has demonstrated that BFAs/BFI can be successfully used in various applications like wireless human sensing [5] and radio-fingerprinting [6]. While in previous work the procedure to extract the BFAs/BFI was customized to the specific network setup, **`Wi-BFI` can be used with any network configuration** thus enabling further research in the area.

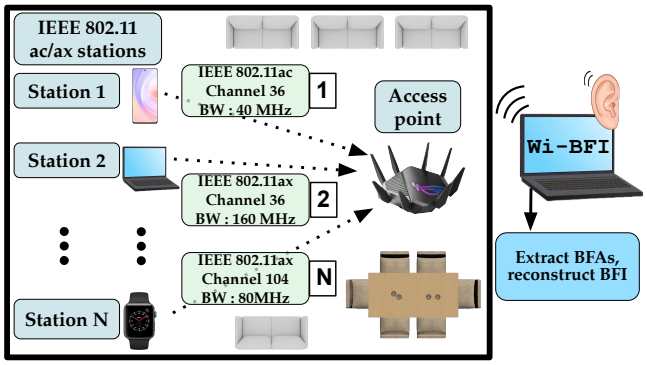

Figure 1: `Wi-BFI` overview.

Summary of Paper Contributions

This work provides the following contributions.

• We propose `Wi-BFI`, an open source python-based tool to extract 802.11ac/ax BFAs in the wild and reconstruct the BFI. `Wi-BFI` is compatible with any network configurations and operating systems.

• We enable the extraction of BFAs and reconstruction of BFI from multiple devices simultaneously, without any physical access to them. The monitored devices can implement different standards and operate on different bands.

• We provide both real-time plotting and saving of the extracted BFAs and reconstructed BFI from live capture or any prior collected traces.

• We present a use case entailing human activity classification with BFAs collected from IEEE 802.11ac devices operating at 80 MHz. By leveraging spatial diversity, the BFAs-based classifier achieves up to 99.28% of accuracy.

2 SYSTEM ARCHITECTURE OF `Wi-BFI`

In the following, we will use the superscripts T and $\dagger$ to denote the transpose and the complex conjugate transpose (i.e., the Hermitian). We define with $\angle\mathbf{C}$ the matrix containing the phases of complex-valued matrix $\mathbf{C}$. Moreover, $\text{diag}(c_1, \ldots, c_j)$ indicates the diagonal matrix with elements $(c_1, \ldots, c_j)$ on the main diagonal. The (c_1, c_2) entry of matrix $\mathbf{C}$ is defined by $[\mathbf{C}]_{c_1,c_2}$, while $\mathbb{I}_c$ refers to an identity matrix of size $c \times c$ and $\mathbb{I}_{c\times d}$ is a $c \times d$ generalized identity matrix.

2.1 `Wi-BFI` Operation Principle

`Wi-BFI` leverages the way MIMO is implemented in Wi-Fi networks following the mechanism standardized in IEEE 802.11. To enable MIMO, the beamformer *pre-codes* the data packets by linearly combining the signals to be simultaneously transmitted to the different beamformees. To do so, the beamformer uses a precoding matrix $\mathbf{W}$ which is derived from the CFR matrix $\mathbf{H}$, describing how the environment modifies the irradiated signals in their path to the receiver. The CFR needs to be estimated by each beamformee and fed back to the beamformer to allow proper pre-coding.

The CFR estimation process is called *channel sounding* and is depicted in Figure 2. The procedure is triggered by the beamformer that periodically broadcasts a null data packet (NDP) to estimate the MIMO channel between itself and the connected beamformees (**step 1** in Figure 2). Since its purpose is to sound the channel, the NDP *is not beamformed*. This is particularly advantageous as the resulting *CFR estimation is not affected by inter-stream or inter-user interference.*

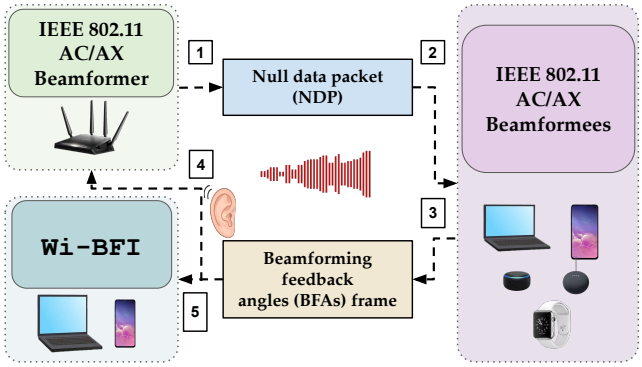

Figure 2: `Wi-BFI`– overall system architecture.

The NDP is a packet containing sequences of bits – named long training fields (LTFs) – the decoded version of which is known by the beamformees. The LTFs are transmitted over the different beamformer antennas in subsequent time slots, thus allowing each beamformee to estimate the CFR of the links between its receiver antennas and the beamformer transmitter antennas. The LTFs are modulated – as the data fields – through orthogonal frequency-division multiplexing (OFDM) by dividing the signal bandwidth into K partially overlapping and orthogonal sub-channels spaced apart by $1/T$. The input bits are grouped into OFDM symbols, $\mathbf{a} = [a_{-K/2}, \ldots, a_{K/2-1}]$ where a_k is named OFDM sample. The K OFDM samples are digitally modulated and transmitted through the K OFDM sub-channels in a parallel fashion

thus occupying the channel for T seconds. Thus, the transmitted LTF signal is

$$s_{\text{tx}}(t) = e^{j2\pi f_c t} \sum_{k=-K/2}^{K/2-1} a_k e^{j2\pi kt/T}, \tag{1}$$

where f_c is the carrier frequency. The NDP is received and decoded by each beamformee (**step 2** in Figure 2) to estimate the CFR $\mathbf{H}$. The different LTFs are used to estimate the channel over each pair of transmitter (TX) and receiver (RX) antennas, for every OFDM sub-channels. This generates a $K \times M \times N$ matrix $\mathbf{H}$ for each beamformee, where M and N are respectively the numbers of TX and RX antennas. Next, the CFR is compressed – to reduce the channel overhead – and fed back to the beamformer. Using $\mathbf{H}_k$ to identify the $M \times N$ sub-matrix of $\mathbf{H}$ containing the CFR samples related to sub-channel k, the *compressed beamforming feedback* is obtained as follows ([7], Chapter 13). First, $\mathbf{H}_k$ is decomposed through singular value decomposition (SVD) as

$$\mathbf{H}_k^T = \mathbf{U}_k \mathbf{S}_k \mathbf{Z}_k^\dagger, \tag{2}$$

where $\mathbf{U}_k$ and $\mathbf{Z}_k$ are, respectively, $N \times N$ and $M \times M$ unitary matrices, while the singular values are collected in the $N \times M$ diagonal matrix $\mathbf{S}_k$. Using this decomposition, the complex-valued beamforming matrix $\mathbf{V}_k$ is defined by collecting the first $N_{\text{SS}} \leq N$ columns of $\mathbf{Z}_k$. Such a matrix is used by the beamformer to compute the pre-coding weights for the N_{SS} spatial streams directed to the beamformee. Hence, $\mathbf{V}_k$ is converted into polar coordinates to avoid transmitting the complete matrix. Specifically, $\mathbf{V}_k$ is decomposed as the product of $\mathbf{D}_{k,i}$ and $\mathbf{G}_{k,\ell,i}$ matrices, which are defined as

$$\mathbf{D}_{k,i} = \begin{bmatrix} \mathbb{I}_{i-1} & 0 & \dots & 0 \\ 0 & e^{j\phi_{k,i,i}} & 0 & \dots \\ \vdots & 0 & \ddots & 0 \\ & \vdots & 0 & e^{j\phi_{k,M-1,i}} \\ 0 & \dots & 0 & 1 \end{bmatrix}, \tag{3}$$

$$\mathbf{G}_{k,\ell,i} = \begin{bmatrix} \mathbb{I}_{i-1} & 0 & \dots & 0 \\ 0 & \cos\psi_{k,\ell,i} & 0 & \sin\psi_{k,\ell,i} \\ \vdots & 0 & \mathbb{I}_{\ell-i-1} & 0 \\ & -\sin\psi_{k,\ell,i} & 0 & \cos\psi_{k,\ell,i} \\ 0 & \dots & 0 & \mathbb{I}_{M-\ell} \end{bmatrix}, \tag{4}$$

where the values of the ϕ and ψ angles are obtained through the procedure detailed in Alg. 1. The number of ϕ and ψ angles depends on the specific network configuration, i.e., the number of transmitter antennas and spatial streams. Using these matrices and $\tilde{\mathbf{D}}_k$ (see line 2 in Alg. 1), $\mathbf{V}_k$ can be written as $\mathbf{V}_k = \tilde{\mathbf{V}}_k \tilde{\mathbf{D}}_k$, with

$$\tilde{\mathbf{V}}_k = \prod_{i=1}^{\min(N_{\text{SS}},M-1)} \left(\mathbf{D}_{k,i} \prod_{l=i+1}^{M} \mathbf{G}_{k,l,i}^T \right) \mathbb{I}_{M \times N_{\text{SS}}}, \tag{5}$$

Algorithm 1: $\mathbf{V}_k$ matrix decomposition

1 Require: $\mathbf{V}_k$;
2 $\tilde{\mathbf{D}}_k = \text{diag}(e^{j\angle[\mathbf{V}_k]_{M,1}}, \dots, e^{j\angle[\mathbf{V}_k]_{M,N_{\text{SS}}}})$;
3 $\Omega_k = \mathbf{V}_k \tilde{\mathbf{D}}_k^\dagger$;
4 **for** $i \leftarrow 1$ *to* $\min(N_{\text{SS}}, M-1)$ **do**
5 $\quad \phi_{k,\ell,i} = \angle\,[\Omega_k]_{\ell,i}$ with $\ell = i, \dots, M-1$;
6 $\quad$ compute $\mathbf{D}_{k,i}$ through Eq. (3);
7 $\quad \Omega_k \leftarrow \mathbf{D}_{k,i}^\dagger \Omega_k$;
8 $\quad$ **for** $\ell \leftarrow i+1$ *to* M **do**
9 $\quad\quad \psi_{k,\ell,i} = \arccos\left(\frac{[\Omega_k]_{i,i}}{\sqrt{[\Omega_k]_{i,i}^2 + [\Omega_k]_{\ell,i}^2}} \right)$;
10 $\quad\quad$ compute $\mathbf{G}_{k,\ell,i}$ through Eq. (4);
11 $\quad\quad \Omega_k \leftarrow \mathbf{G}_{k,\ell,i} \Omega_k$;

where the products represent matrix multiplications. In the $\tilde{\mathbf{V}}_k$ matrix, the last row – i.e., the feedback for the M-th transmitter antenna – consists of non-negative real numbers by construction. Using this transformation, the beamformee is only required to transmit the ϕ and ψ angles to the beamformer as they allow reconstructing $\tilde{\mathbf{V}}_k$ precisely. Moreover, it has been proved (see [7], Chapter 13) that the beamforming performance is equivalent at the beamformee when using $\mathbf{V}_k$ or $\tilde{\mathbf{V}}_k$ to construct the steering matrix $\mathbf{W}$. In turn, the feedback for $\tilde{\mathbf{D}}_k$ is not fed back to the beamformer.

To further reduce the channel occupancy, the angles are quantized using b_ϕ bits for ϕ and $b_\psi = b_\phi - 2$ bits for ψ, as follows:

$$[\phi, \psi] = \left[\pi \left(\frac{1}{2^{b_\phi}} + \frac{q_\phi}{2^{b_\phi - 1}} \right), \left(\frac{1}{2^{b_\psi + 2}} + \frac{q_\psi}{2^{b_\psi + 1}} \right) \right]. \tag{6}$$

In IEEE 802.11ac/ax, $b_\phi = \{9, 7\}$ bits and $b_\phi = \{6, 4\}$ bits are used for multi-user multi-input multi-output (MU-MIMO) and single-user multi-input multi-output (SU-MIMO) systems respectively. The quantized values – $q_\phi = \{0, \dots, 2^{b_\phi} - 1\}$ and $q_\psi = \{0, \dots, 2^{b_\psi} - 1\}$ – are packed into the compressed beamforming frame (**step 3** in Figure 2) and such *BFAs frame* is transmitted to the beamformer (**step 4** in Figure 2). The b_ϕ and b_ψ can be read in the VHT/HE MIMO control field, together with other information like the number of columns (N_{SS}) and rows (M) in the beamforming matrix and the channel bandwidth (see Figure 3). Each BFI contains A angles for each of the K OFDM sub-channels for a total of $A \times K$ angles each. We remark that, since MU-MIMO requires fine-grained channel sounding – around every 10 milliseconds, according to [8] – it is fundamental to process the BFI in a fast manner at the beamformer. For this reason, and since cryptography would lead to excessive delays, *the angles are currently transmitted over-the-air unencrypted.*

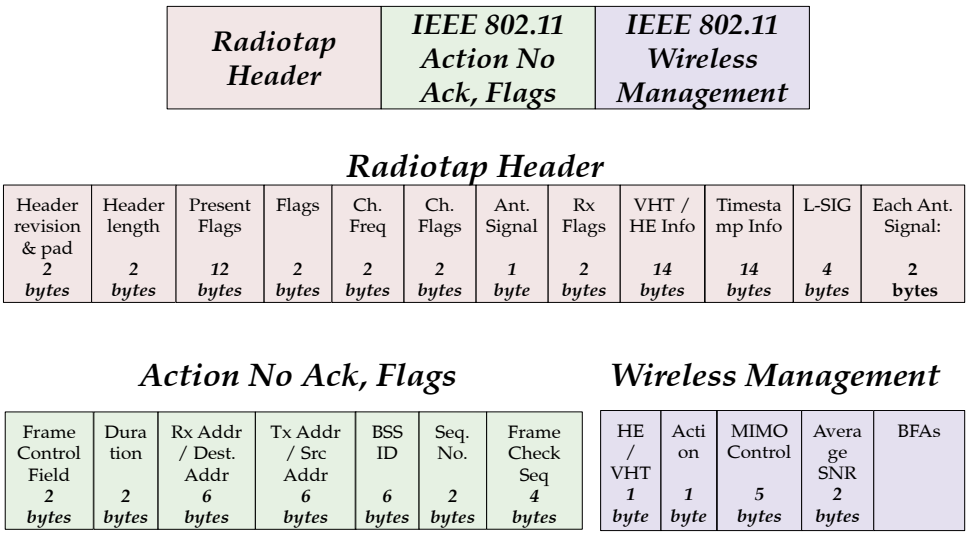

Figure 3: IEEE 802.11ac/ax BFI report frame structure.

`Wi-BFI` captures the BFAs frames (**step 5** in Figure 2) with the python-based network monitoring tool `Pyshark`. However, any other network monitoring tool like `tcpdump` or `Wireshark` can also be used with `Wi-BFI`.

Note that the beamformer continuously triggers the channel sounding procedure on the connected beamformees. This makes *the BFI contain very rich, reliable, and spatially diverse information*. Moreover, as BFAs frames are broadcasted by the beamformees, the information for all the beamformees *can be collected with a single capture* by any Wi-Fi-compliant device. `Wi-BFI` leverages this procedure to collect the BFAs frames from multiple devices operating on different bands with a single capture, and reconstruct the BFI from the extracted BFAs. Thus, `Wi-BFI` does not need any direct access to the beamformees or any hardware-specific tool, ultimately reducing the complexity of the data collection procedure.

`Wi-BFI` consists of four main steps as depicted in Figure 4. Firstly, in **step I**, `Wi-BFI` groups the BFAs frames based on the following arguments: **(i)** the standard: IEEE 802.11ac or IEEE 802.11ax; **(ii)** the bandwidth: 20 MHz, 40 MHz, 80 MHz, or 160 MHz; **(iii)** the device, through the MAC address.

After grouping the BFAs frames from any live capture or earlier captured trace, `Wi-BFI` performs bit-wise parsing through the frames to extract the BFAs (**step II** in Figure 4). For that, we follow the IEEE 802.11 BFAs frame structure, presented in Figure 3. Specifically, a BFAs frame has three main parts: **(i)** *Radiotap Header*, **(ii)** *IEEE 802.11 Action No Ack, Flags*, and **(iii)** *IEEE 802.11 Wireless Management*. The fields of each part of a BFAs frame, along with the corresponding byte values, are mentioned in Figure 3. `Wi-BFI` parses through each of the fields of the BFAs frame to extract the corresponding information including the BFAs. The BFAs

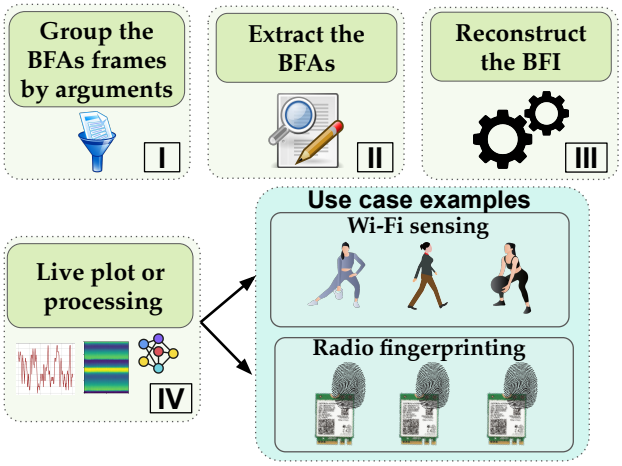

Figure 4: Main steps of the `Wi-BFI` tool.

are structured in a matrix of dimension is $P \times K \times A$, where P represents the total number of packets in the capture. As an example, considering a 4×2 IEEE 802.11ax SU-MIMO system operating on a 160 MHz bandwidth channel, with the beamformer having four antennas and the beamformee having two antennas, each BFAs frame has K =500 OFDM data sub-channels with A =10 BFAs each. For this setup, Figure 5 depicts the first two BFAs (ϕ_{11} and ϕ_{21}) for each of the OFDM sub-channels (x-axis) for one BFAs frame.

Note that, according to the standard, the number of sub-channels changes with the change in operating standards and transmission bandwidth [9]. Moreover, we remind that the number of BFAs depends on the network configuration, i.e., the number of transmit antennas M, and the number of spatial streams N_{SS}. The number and order of BFAs for some network configurations are reported in Table 1.

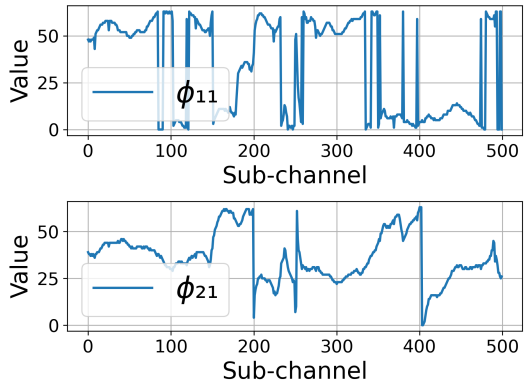

Figure 5: BFAs (ϕ_{11} and ϕ_{21}) of each sounded sub-channel of a 4×2 IEEE 802.11ax system at 160 MHz.

MIMO	No. angles	Order of the angles
2×1	2	ϕ_{11}, ψ_{21}
2×2	2	ϕ_{11}, ψ_{21}
3×1	4	$\phi_{11}, \phi_{21}, \psi_{21}, \psi_{21}$
3×2	6	$\phi_{11}, \phi_{21}, \psi_{21}, \psi_{21}, \phi_{22}, \psi_{32}$
3×3	6	$\phi_{11}, \phi_{21}, \psi_{21}, \psi_{21}, \phi_{22}, \psi_{32}$
4×1	6	$\phi_{11}, \phi_{21}, \phi_{31}, \psi_{21}, \psi_{31}, \psi_{41}$
4×2	10	$\phi_{11}, \phi_{21}, \phi_{31}, \psi_{21}, \psi_{31}, \psi_{41}, \phi_{22}, \phi_{32}, \psi_{32}, \psi_{42}$
4×3	12	$\phi_{11}, \phi_{21}, \phi_{31}, \psi_{21}, \psi_{31}, \psi_{41}, \phi_{22}, \phi_{32}, \psi_{32}, \psi_{42}, \phi_{33}, \psi_{43}$
4×4	12	$\phi_{11}, \phi_{21}, \phi_{31}, \psi_{21}, \psi_{31}, \psi_{41}, \phi_{22}, \phi_{32}, \psi_{32}, \psi_{42}, \phi_{33}, \psi_{43}$

Table 1: Order of BFAs in the BFI report frame in Figure 3 for different MIMO configurations.

After extracting the BFAs, `Wi-BFI` reconstructs the $\tilde{\mathbf{V}}_k$ matrix following Equation 5 (see **step III** of Figure 4). The dimension of the reconstructed $\tilde{\mathbf{V}}_k$ matrix is $P \times K \times M \times N_{SS}$. For the above mentioned 4×2 IEEE 802.11ax system at 160 MHz, the reconstructed $\tilde{\mathbf{V}}_k$ has K=500, M=4 and N_{SS}= 2 making the dimension $P \times 500 \times 4 \times 2$. The $\tilde{\mathbf{V}}_k$ matrices reconstructed by `Wi-BFI` from the captured angles for the first two transmitter antennas are depicted in Figure 6, i.e., for $(m = 1, n_{SS} = 1)$, $(m = 1, n_{SS} = 2)$, $(m = 2, n_{SS} = 1)$, and $(m = 2, n_{SS} = 2)$, with $m \in \{0, \ldots, M-1\}$ and $n_{SS} \in \{0, \ldots, N_{SS} - 1\}$) being the transmitter antenna and the spatial stream indices, respectively. Figure 6 reports $\tilde{\mathbf{V}}_k$ for a single frame. Figure 7 depicts the time evolution of $\tilde{\mathbf{V}}_k$ (multiple frames).

As the final step, as depicted in **step IV** of Figure 4, `Wi-BFI` either plots or saves the extracted BFAs and the $\tilde{\mathbf{V}}_\mathbf{k}$ matrix (BFI). For further visual representations of the BFAs, please refer to our `Wi-BFI` demonstration video.[2]

[2] `Wi-BFI` demonstration available at https://youtu.be/0k7uYRCmMBw

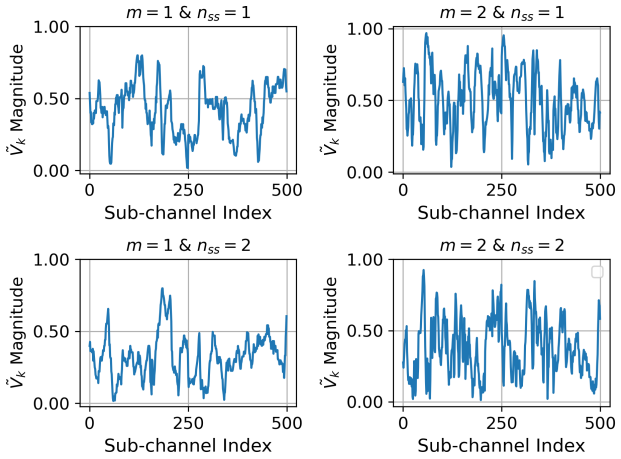

Figure 6: Magnitude of $\tilde{\mathbf{V}}_\mathbf{k}$ of each sounded sub-channel for different transmit antennas $m \in \{0, \ldots, M-1\}$ and spatial streams $n_{SS} \in \{0, \ldots, N_{SS} - 1\}$ of a 4×2 IEEE 802.11ax system at 160 MHz.

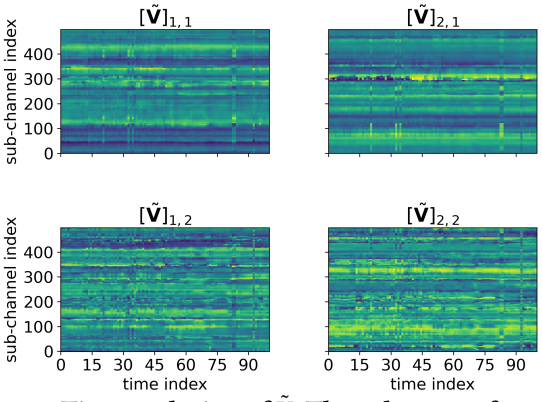

Figure 7: Time evolution of $\tilde{\mathbf{V}}$. The columns refer to the transmit antenna and rows to the spatial streams.

3 `WI-BFI` USE CASE: SENSING WITH BFAs

Beyond connectivity, the unprecedented rise in the number of smartphones, laptops, and many other Wi-Fi-enabled devices [10] will pave the way to revolutionary Wi-Fi sensing applications including activity recognition [5], and radio-fingerprinting [6], among others [11].

The vast majority of such applications leverage the uncompressed CFR measurements obtained from pilot symbols in the Wi-Fi packets to characterize the propagation channel. Despite leading to good performance, CFR-based techniques require manual extraction and recording of the CFR, which is currently not supported by the IEEE 802.11 standard. This has led to the usage of CFR extractor tools running custom-tailored firmware [2, 12]. Even if 802.11 could eventually support CFR extraction in the future, (i) it would require additional device-specific processing to extract it from the

chip, thus increasing energy consumption; (ii) multi-device sensing would require tight synchronization among collectors to align the time of the individual CFR measurements. On top of these, most of the existing CFR tools need direct access to the device and only work on devices implementing specific standards and operating on channels with certain bandwidths. This limits different applications to leverage the Wi-Fi signals opportunistically and hinders mass adoption at the same time.

On the contrary, we argue that the BFI, and, in turn, the BFAs, are more effective metrics for developing sensing applications. In this section, we show how BFAs can be leveraged for human activity classification through IEEE 802.11ac MU-MIMO systems operating on channels with 80 MHz of bandwidth. A comparison of BFAs and traditional CFR based approach along with domain generalization capability of BFAs are presented in [5].

3.1 Learning Architecture

Owing to its excellent performance, convolutional neural network (CNN) is a popular choice in a wide range of applications including wireless sensing [5, 13]. The convolutional layer is the basis of CNN which performs convolution operations on the elements of the input data to extract features. Thus, for demonstrating the potential of BFAs in Wi-Fi sensing tasks like activity classification, we leverage a CNN architecture based on only three VGG-based blocks [14]. Specifically, the network stacks three convolutional blocks (`conv-block`) and a max-pooling (`MaxPool`) layer as detailed in Figure 8. The output of the `MaxPool` layer is flattened and then the Softmax activation function is used to obtain the probability distribution over the activity labels.

Each `conv-block` consists of two 2-dimensional convolutional layers. Inspired by the design of VGG block, we use a kernel size of 3×3 and a step size of 1 in each of the convolutional layer [14]. We use batch normalization and rectified linear units (ReLU) activation function in each `conv-block` to avoid gradient explosion or vanishing and to have non-linearity in the network respectively. Our VGG-based CNN consists of three of such `conv-blocks` with 32, 64, and 128 filters respectively.

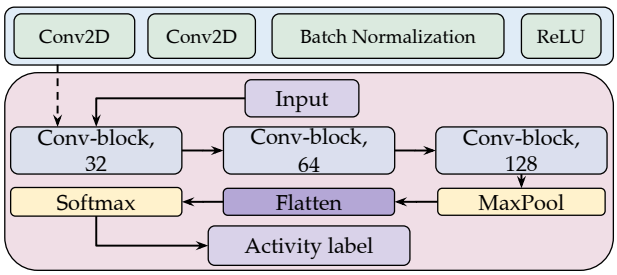

Figure 8: CNN-based learning architecture.

3.2 Experimental Setup

The experiments are conducted in three indoor scenarios with three different subjects as presented in Figure 9.

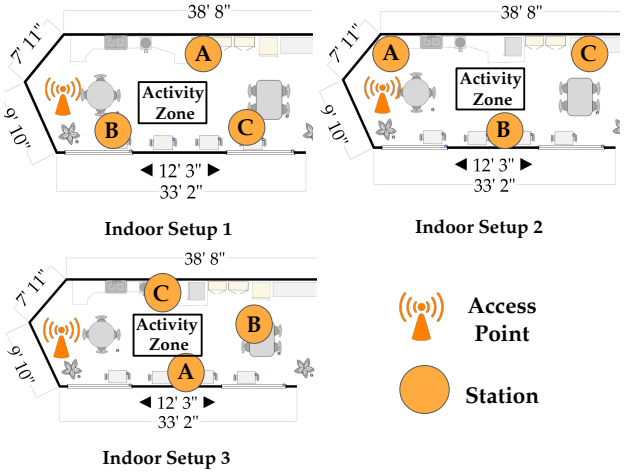

Figure 9: Experimental setup for activity classification with BFAs.

In each of the setups, we have a 3×3 IEEE 802.11ac MU-MIMO system operating on channel 153 with center frequency f_c = 5.77 GHz, with 80 MHz of bandwidth. Each of the systems has one beamformer and three beamformees (stations (STAs)) with M=3 and N=1 antennas enabled respectively. We use off-the-shelf Netgear Nighthawk X4S AC2600 routers both as beamformer and beamformees to set up the network. We consider three human subjects performing ten different activities: *walking, standing, rotating, waiving, drinking, hands up and down, reading a book, jogging, boxing, and clapping*. UDP data streams are sent from the beamformer to the beamformees in the downlink direction to trigger the channel sounding. We record the BFAs frames of all three stations with a single capture with `Wi-BFI` and extract the BFAs associated with each beamformees. For training the model we capture the BFAs frames for 3 minutes for each activity performed by each subject. Hence, for each of the beamformees we divide the extracted BFAs into non-overlapping windows of 10 packets each. The windows are fed one at a time to the learning block. To obtain the ground truth, we also capture the video streams of the subjects performing the activities. The experimental setup and the snaps from the ground truth video streams with three different subjects and activities are shown in Figure 10.

3.3 Sensing Performance with BFAs

Figure 11 presents the classification performance of BFAs with baseline CNN when we consider a different number of STAs. The average classification accuracies are respectively 94.35%, 98.59%, and 99.28% when we use the data from only

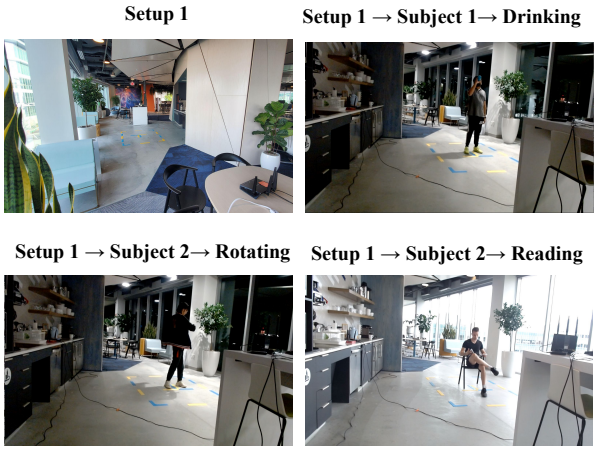

Figure 10: Experimental setup for activity classification with BFAs.

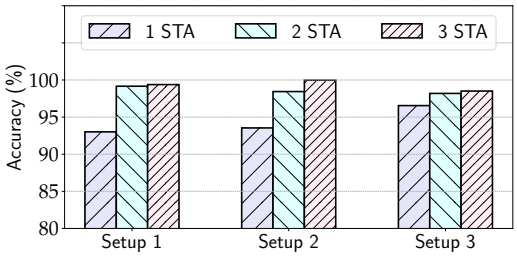

Figure 11: Classification performance with BFAs for different number of STAs.

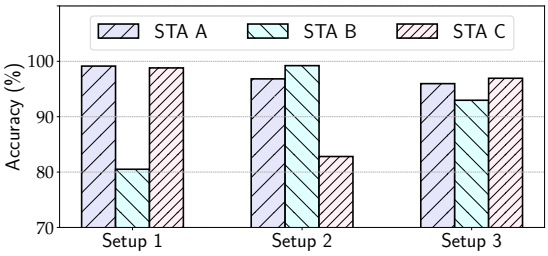

Figure 12: Classification performance with BFAs for each individual STA.

one STA, two STAs combined, and three STAs combined. It is noticeable that the performance is comparatively poor when we have only one STA.

To further investigate this aspect, we report the classification performance of each individual beamformees in Figure 12. We notice that, in different setups, the individual performance of the beamformees varies significantly. For example, in setup 1, STA B performs worse with an accuracy of around 80%. On the other hand, in setup 2 and setup 3 STA C and STA B perform worse with an accuracy of 82.81% and 92.97% respectively. This is due to the fact that the physical location of the STA may cause the channel between

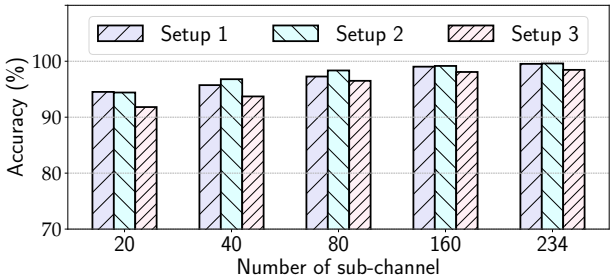

Figure 13: Classification performance considering different number of OFDM sub-channels

that particular STA and the beamformer to be in deep fade, making the model perform poorly. However, this can be improved by considering more than one beamformees for the classification as presented in Figure 11.

To evaluate the impact of the sub-channel granularity on the activity classification accuracy, we report in Figure 13 the performance of the CNN based model, presented in Figure 8, when we consider different numbers of OFDM sub-channels. The average performance over all the setups considering all 234 data sub-channels at 80 MHz bandwidth is 99.19%. Even though the overall performance degrades when the number of sub-channels decreases, the reduction in the performance is not significant. On the other hand, a decrease in the number of sub-channels results in a significant reduction of the computational burden. For example, the performance decreases by only 0.44% and 1.83% when the number of sub-channels is decreased to 160 and 80, respectively. However, it reduces the computational burden by 1.46 and 2.92 times respectively. Considering only 20 sub-channels, the overall performance is 93.58% with an 11.7 times reduction of the computational burden. This gives us an idea of the trade-off between the performance and computational burden.

Overall, the performance analysis shows that BFAs-based sensing performs comparatively with the CFR based sensing works of the literature [11]. BFAs-based sensing can leverage spatial diversity gained through MU-MIMO system which most CFR-based approaches cannot.

4 RELATED WORK

Over the last few years, a few efforts have been made to leverage BFAs frames for various applications including radio-fingerprinting [6] and Wi-Fi sensing [3–5, 15]. Meneghello et al. leveraged $\tilde{\mathbf{V}}_\mathbf{k}$ matrices to perform Wi-Fi radio fingerprinting on the move which is based on the intuition that, imperfections in the transmitter's radio circuitry percolate onto the BFI [6]. Kanda et al. extracted $\tilde{\mathbf{V}}_\mathbf{k}$ matrices from BFAs frames to perform respiratory rate estimation [3]. Kondo et al. evaluate the sensing ability of uni-directional and bi-directional BFI and demonstrate that BFI computed from the

access point (uplink beamforming) has better sensitivity in comparison to the BFI computed by the stations (downlink beamforming) [4]. Itahara et al. leveraged BFI to estimate the angle of departure for multiple propagation paths and achieved comparable performance to that of CFR based approaches [15]. Haque et al. performed sensing by classifying 20 different human activities with compressed BFAs [5].

Even though there has been increased interest in BFI-based research, there are no unified open-sourced tools to extract BFAs and reconstruct BFI from the captured BFAs. This limits the research community to investigate further this field. Thus we developed `Wi-BFI` to extract BFAs and reconstruct the $\tilde{\mathbf{V}}_\mathbf{k}$ matrices from any IEEE 802.11 device with all possible bandwidths and network configurations.

5 CONCLUSIONS AND REMARKS

In this paper, we have proposed `Wi-BFI`, the first tool to extract IEEE 802.11ac/ax beamforming feedback angles (BFAs) and reconstruct the beamforming feedback information (BFI) in the wild from both SU-MIMO and MU-MIMO systems operating at 20 MHz/40 MHz/80 MHz/160 MHz bandwidth and with any network configuration. `Wi-BFI` operates at multiple bands and with multiple Wi-Fi standards simultaneously without the need for any direct access to the beamformer or beamformees. We provided an example of leveraging BFAs for one of the most popular wireless sensing tasks, i.e., human activity recognition, achieving up to 99.28% recognition accuracy. Other BFI use cases include radio-fingerprinting, Wi-Fi localization, and optimization of the resource allocation in MU-MIMO networks, among others. To further promote BFI-based research we have made the `Wi-BFI` tool compatible with any operating system and we open-sourced it together with a detailed explanation of the operations and practical examples of use.

ACKNOWLEDGMENTS

This work is funded in part by the National Science Foundation (NSF) grant CNS-2134973, CNS-2120447, and ECCS-2229472, 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, and by the Fulbright Schuman Program, administered by the Fulbright Commission in Brussels and jointly financed by the U.S. Department of State, and the Directorate-General for Education, Youth, Sport and Culture (DG.EAC) of the European Commission. The views and opinions expressed in this work are those of the authors and do not necessarily reflect those of the funding institutions.

REFERENCES

[1] Wi-Fi Alliance. The Economic Value of Wi-Fi: A Global View (2018 and 2023). https://tinyurl.com/EconWiFi, 2021.

[2] Francesco Gringoli, Marco Cominelli, Alejandro Blanco, and Joerg Widmer. Ax-csi: Enabling csi extraction on commercial 802.11ax wi-fi platforms. In *Proceedings of the 15th ACM Workshop on Wireless Network Testbeds, Experimental Evaluation & CHaracterization*, page 46–53, New York, NY, USA, 2022. Association for Computing Machinery.

[3] Takamochi Kanda, Takashi Sato, Hiromitsu Awano, Sota Kondo, and Koji Yamamoto. Respiratory Rate Estimation Based on WiFi Frame Capture. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, pages 881–884, online, 2022. IEEE.

[4] Sota Kondo, Sohei Itahara, Kota Yamashita, Koji Yamamoto, Yusuke Koda, Takayuki Nishio, and Akihito Taya. Bi-directional beamforming feedback-based firmware-agnostic WiFi sensing: An empirical study. *IEEE Access*, 10:36924–36934, 2022.

[5] Khandaker Foysal Haque, Milin Zhang, Francesca Meneghello, and Francesco Restuccia. BeamSense: Rethinking Wireless Sensing with MU-MIMO Wi-Fi Beamforming Feedback, 2023.

[6] Francesca Meneghello, Michele Rossi, and Francesco 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)*, pages 1062–1072, Bologna, Italy, 2022. IEEE.

[7] Eldad Perahia and Robert Stacey. *Next Generation Wireless LANs: Throughput, Robustness, and Reliability in 802.11n.* Cambridge Univ. Press, Cambridge, UK, 2008.

[8] Matthew S Gast. *802.11 ac: A Survival Guide: Wi-Fi at Gigabit and Beyond.* " O'Reilly Media, Inc.", Sebastopol, CA, USA, 2013.

[9] 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, 2021.

[10] IoTForAll.com. The Role of WiFi in the IoT. https://www.iotforall.com/wifi-role-iot, 2020.

[11] Yongsen Ma, Gang Zhou, and Shuangquan Wang. Wifi sensing with channel state information: A survey. *ACM Comput. Surv.*, 52(3), jun 2019.

[12] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. Tool release: Gathering 802.11n traces with channel state information. *SIGCOMM Comput. Commun. Rev.*, 41(1):53, Jan. 2011.

[13] Khandaker Foysal Haque, Milin Zhang, and Francesco Restuccia. Simwisense: Simultaneous multi-subject activity classification through wi-fi signals. In *2023 IEEE 24th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pages 46–55, 2023.

[14] Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition, 2014.

[15] Sohei Itahara, Sota Kondo, Kota Yamashita, Takayuki Nishio, Koji Yamamoto, and Yusuke Koda. Beamforming feedback-based model-driven angle of departure estimation toward legacy support in WiFi sensing: An experimental study. *IEEE Access*, 10:59737–59747, 2022.