

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

Khandaker Foysal Haque*, Francesca Meneghello§, Francesco Restuccia*

*Northeastern University, US

§ University of Padova, Italy



- Motivation and general idea
- Background concepts
- **Wi-BFI** overview
- Examples of application



- The **channel frequency response (CFR)** is a necessary information for the correct functioning of wireless networks
 - recently it is being leveraged also to deliver sensing services through Wi-Fi
- **Challenge:** The CFR is not not made available outside the Wi-Fi devices

Current approach

- custom tailored tools (AX-CSI, NEXMON-CSI, Atheros CSI, Intel CSI extractors)

AX-CSI nexmon

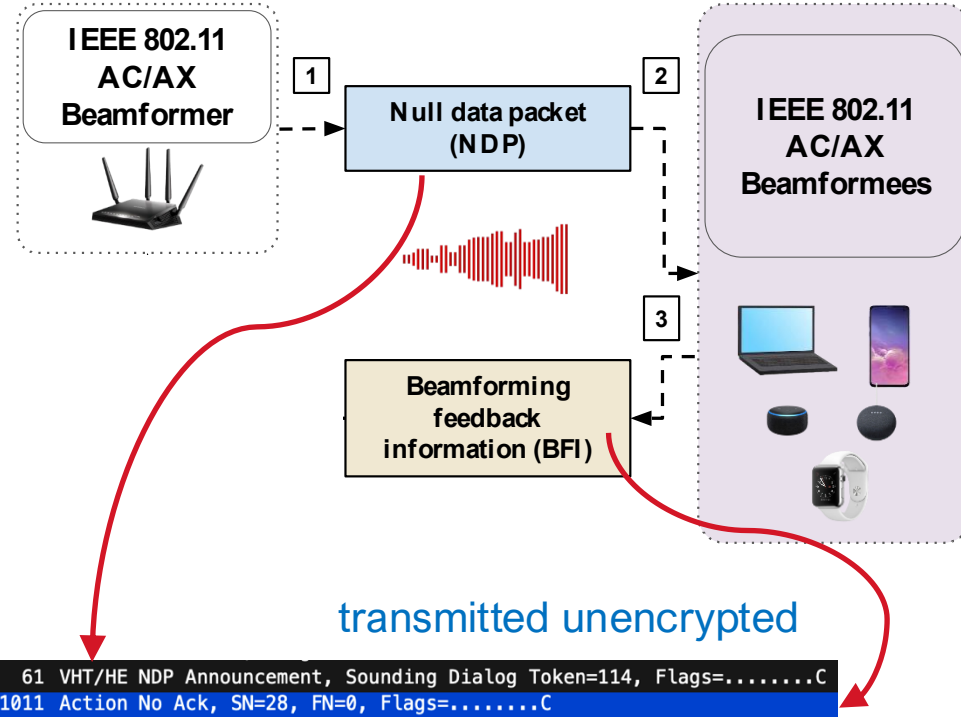
- **Wi-BFI** main idea

- use the **MIMO beamforming feedback information (BFI)** as a proxy for the CFR

Background: from CFR to BFI

For each subcarrier k , **each beamformee**

- Estimates the CFR H_k
- Obtains the **beamforming feedback matrix** through SVD of the CFR
- **Compresses** the matrix to obtain transformation angles $\phi_{k,\ell,i}$ $\psi_{k,\ell,i}$ (**beamforming feedback angles**)
- **Quantizes** the angles
- Transmits the information to the beamformer



```
52 0.032155 BeijingX_76:65:3e ... 1a:e0:65:4e:ea:ca ... 802.11 61 VHT/HE NDP Announcement, Sounding Dialog Token=114, Flags=.....C
53 0.033717 1a:e0:65:4e:ea:ca BeijingX_76:65:3e 802.11 1011 Action No Ack, SN=28, FN=0, Flags=.....C
```

Beamforming feedback matrices

Wireshark - Packet 53 - 1696427454

> Frame 53: 1011 bytes on wire (8088 bits), 1011 bytes captured (8088 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Action No Ack, Flags:C
v IEEE 802.11 Wireless Management
v Fixed parameters
Category code: HE (30)
v HE Action: HE Compressed Beamforming And CQI (0)
Total length: 947
> HE MIMO Control: 0x0712008099
> Average Signal to Noise Ratio
v Feedback Matrices
SCIDX: -500, phi11:0, phi21:1, phi31:3, psi21:8, psi31:4, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -496, phi11:3, phi21:0, phi31:2, psi21:4, psi31:4, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -492, phi11:3, phi21:0, phi31:2, psi21:4, psi31:4, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -488, phi11:2, phi21:0, phi31:1, psi21:4, psi31:4, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -484, phi11:2, phi21:0, phi31:1, psi21:0, psi31:4, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -480, phi11:1, phi21:0, phi31:1, psi21:0, psi31:4, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -476, phi11:1, phi21:0, phi31:0, psi21:0, psi31:4, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -472, phi11:1, phi21:0, phi31:0, psi21:0, psi31:4, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -468, phi11:0, phi21:0, phi31:0, psi21:12, psi31:7, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -464, phi11:0, phi21:0, phi31:3, psi21:15, psi31:7, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -460, phi11:0, phi21:0, phi31:3, psi21:15, psi31:7, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -456, phi11:0, phi21:0, phi31:3, psi21:15, psi31:7, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -452, phi11:0, phi21:0, phi31:3, psi21:15, psi31:7, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -448, phi11:3, phi21:3, phi31:3, psi21:15, psi31:7, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -444, phi11:3, phi21:3, phi31:3, psi21:15, psi31:7, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -440, phi11:3, phi21:3, phi31:3, psi21:11, psi31:7, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0
SCIDX: -436, phi11:3, phi21:3, phi31:3, psi21:11, psi31:7, psi41:2, phi22:0, phi32:0, psi32:0, psi42:0

transmitted unencrypted

0040	00 12 07 32 80 34 92 00	c0 48 24 00 30 12 09 00	...2.4...H\$.0...
0050	48 44 02 00 12 90 00 04	04 24 00 10 00 09 00 04	HD....@.\$.....
0060	40 02 00 00 9f 00 00 fc	27 00 00 ff 09 00 c0 7f	@.....'.....
0070	02 00 f0 9f 00 c0 ff 27	00 f0 ff 09 00 fc 7b 02	'.....{.
0080	00 ff 9e 00 c0 bf 27 00	e0 ef 09 00 fc 7b 02 00	'.....{.
0090	fe 9e 00 80 bf 27 00 e0	ef 09 00 f8 7b 02 00 fd	'.....{.
00a0	8e 00 40 bf 23 00 00 ef	08 00 f4 3b 02 00 fd 8e	..@.#.....;
00b0	00 40 83 23 00 d0 ef 08	00 34 38 02 00 0d 8e 01	..@.#.....48.....
00c0	40 87 63 00 c0 e2 18 00	b0 38 06 00 3c 8e 01 00	@.c.....8.<..<..
00d0	93 63 00 c0 e5 18 00 70	39 06 00 5c 8e 01 00 97	.c.....p 9..\'..
00e0	63 00 c0 e5 14 00 70 39	05 00 5c 4e 01 00 9b 53	c.....p9 ..\'N...S

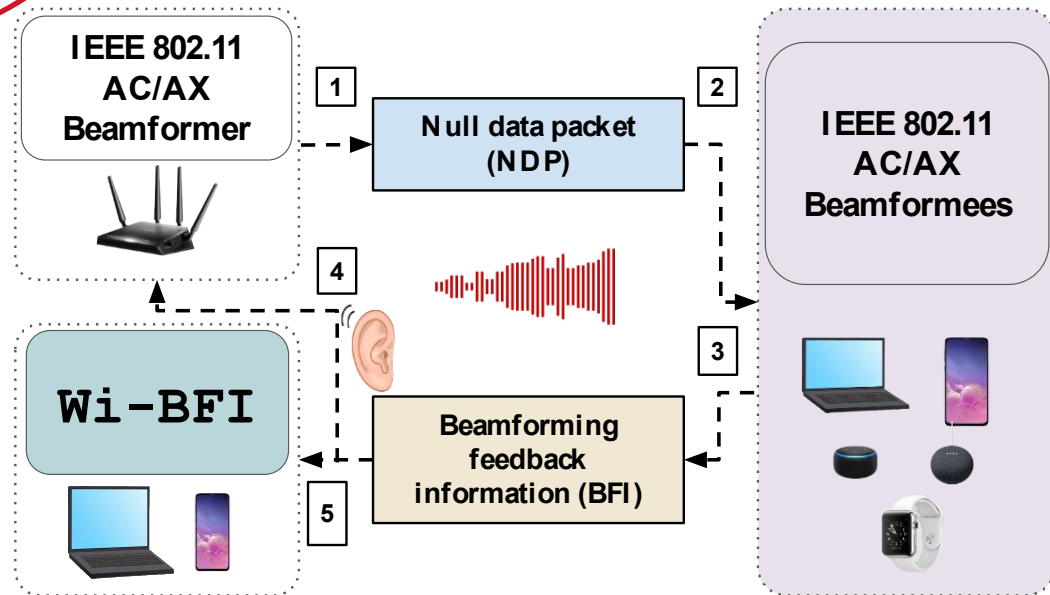
☒ Show packet bytes

Help Close

Wi-BFI operations

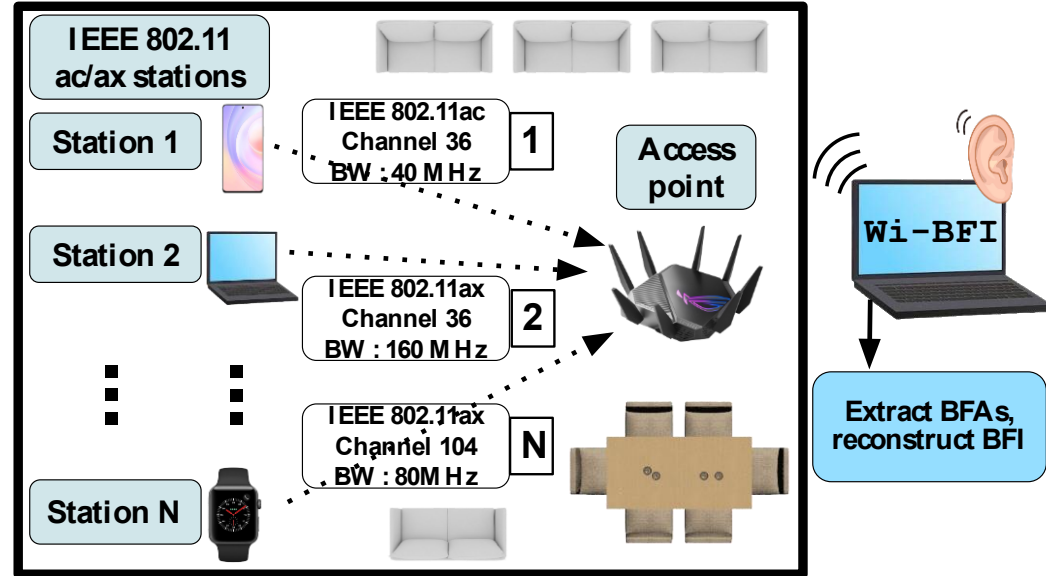
```
52 0.032155 BeijingX_76:65:3e ... 1a:e0:65:4e:ea:ca ... 802.11 61 VHT/HE NDP Announcement, Sounding Dialog Token=114, Flags=.....C
53 0.033717 1a:e0:65:4e:ea:ca BeijingX_76:65:3e 802.11 1011 Action No Ack, SN=28, FN=0, Flags=.....C
```

1. **Capture** the beamforming feedback packet
2. **Decode** the **Wi-Fi BFAs** based on the network configuration
3. **Reconstructing** the beamforming feedback matrix

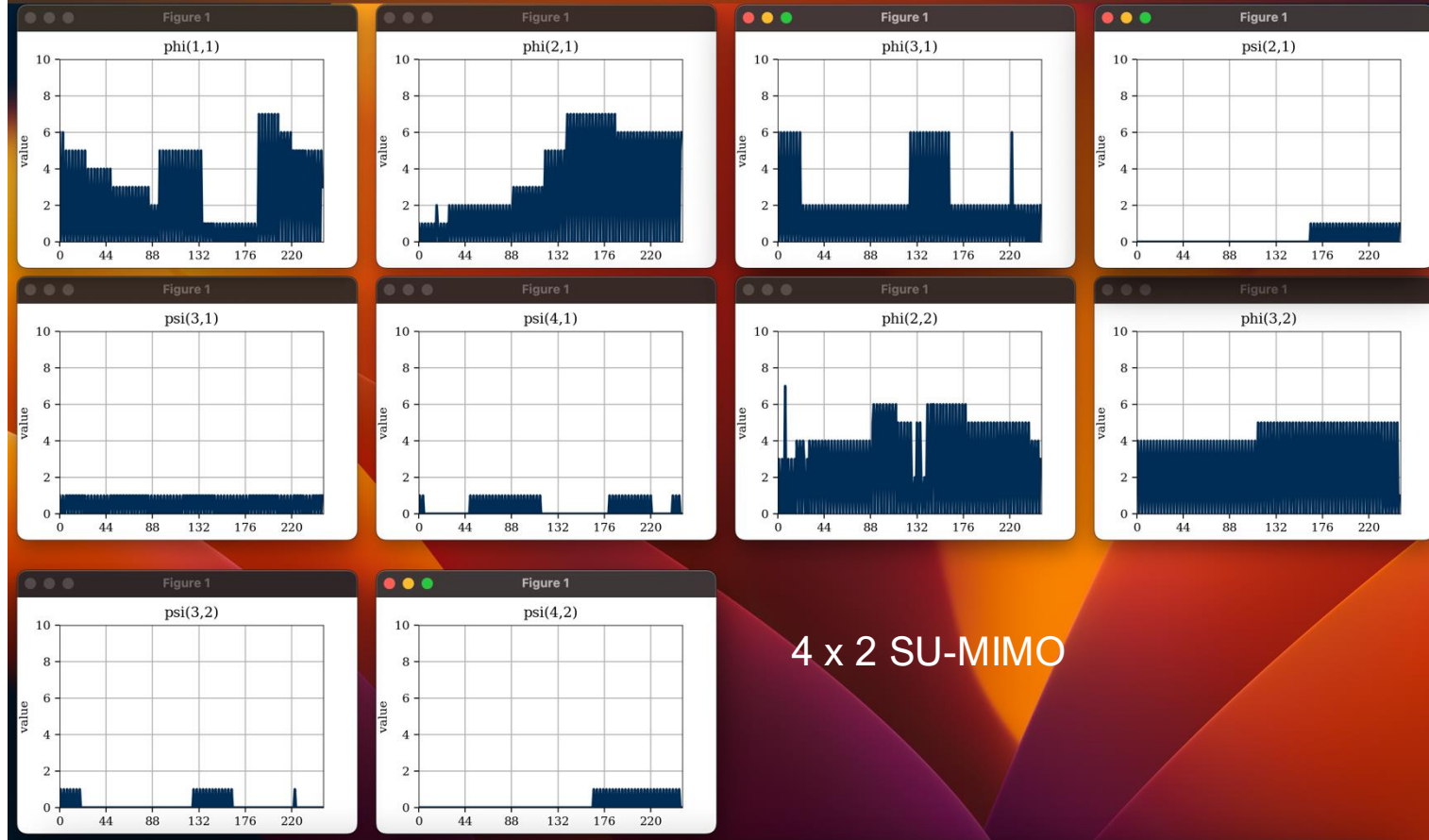


Wi-BFI features

- IEEE 802.11**ac** and 802.11**ax** networks
- Radio channels with **160/80/40/20 MHz** bandwidth
- Single-user and multi-user MIMO
- Real-time and offline extraction and storage

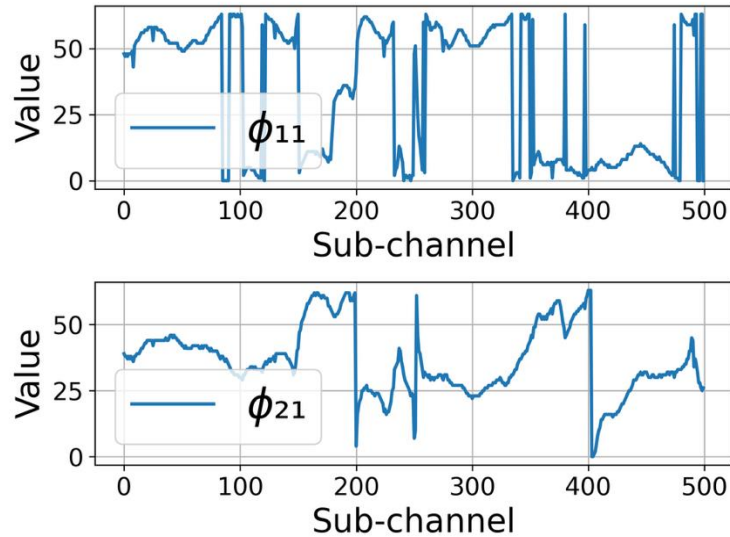


Real-time angles visualization

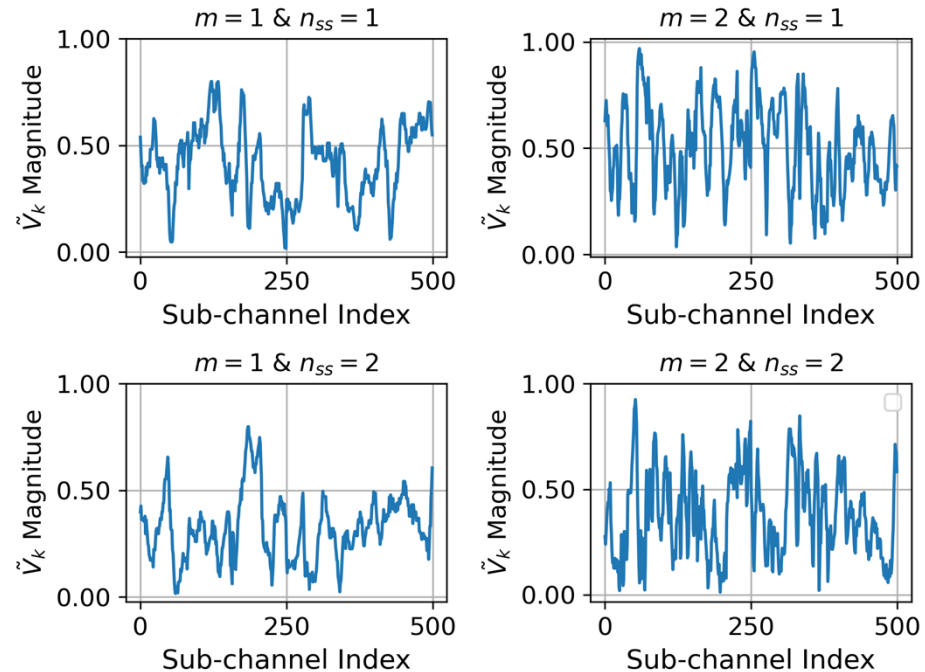


Example of captures and processing offline

Raw beamforming feedback angles

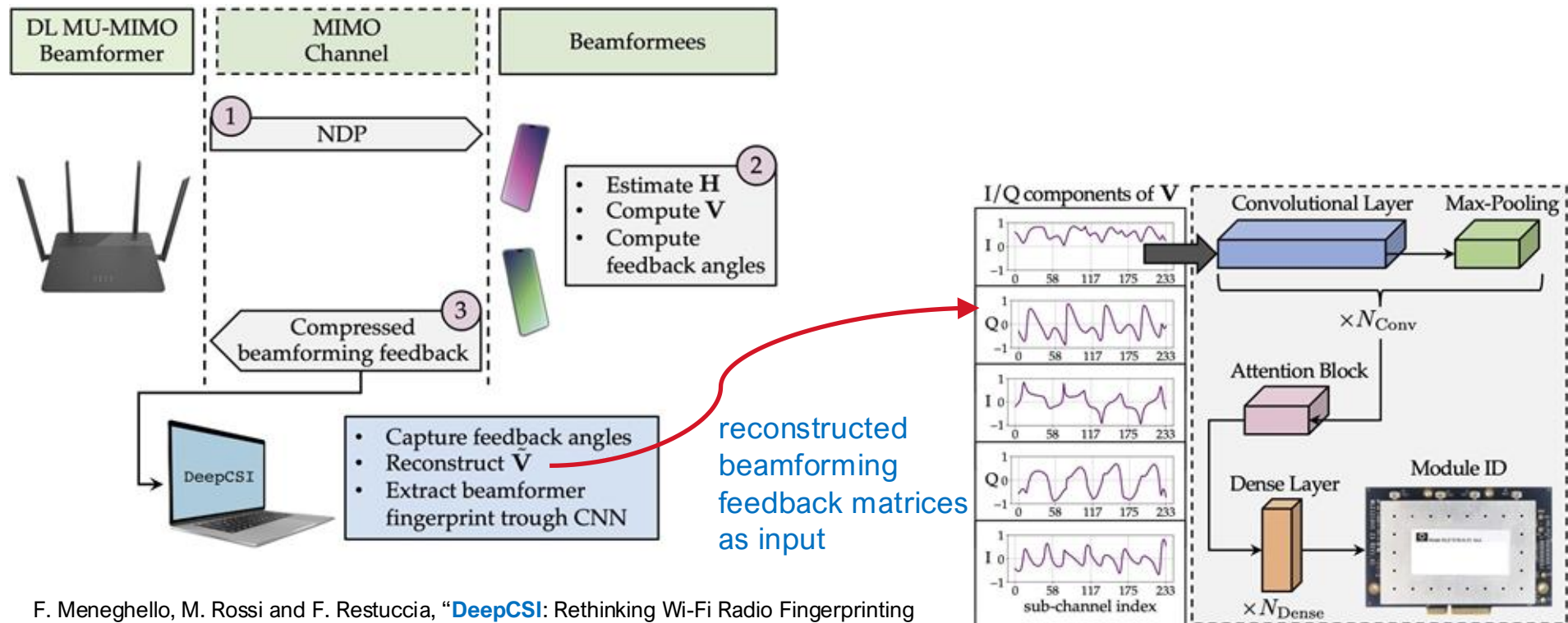


Reconstructed beamforming feedback matrix
for different antennas (m) and streams (n_{ss})



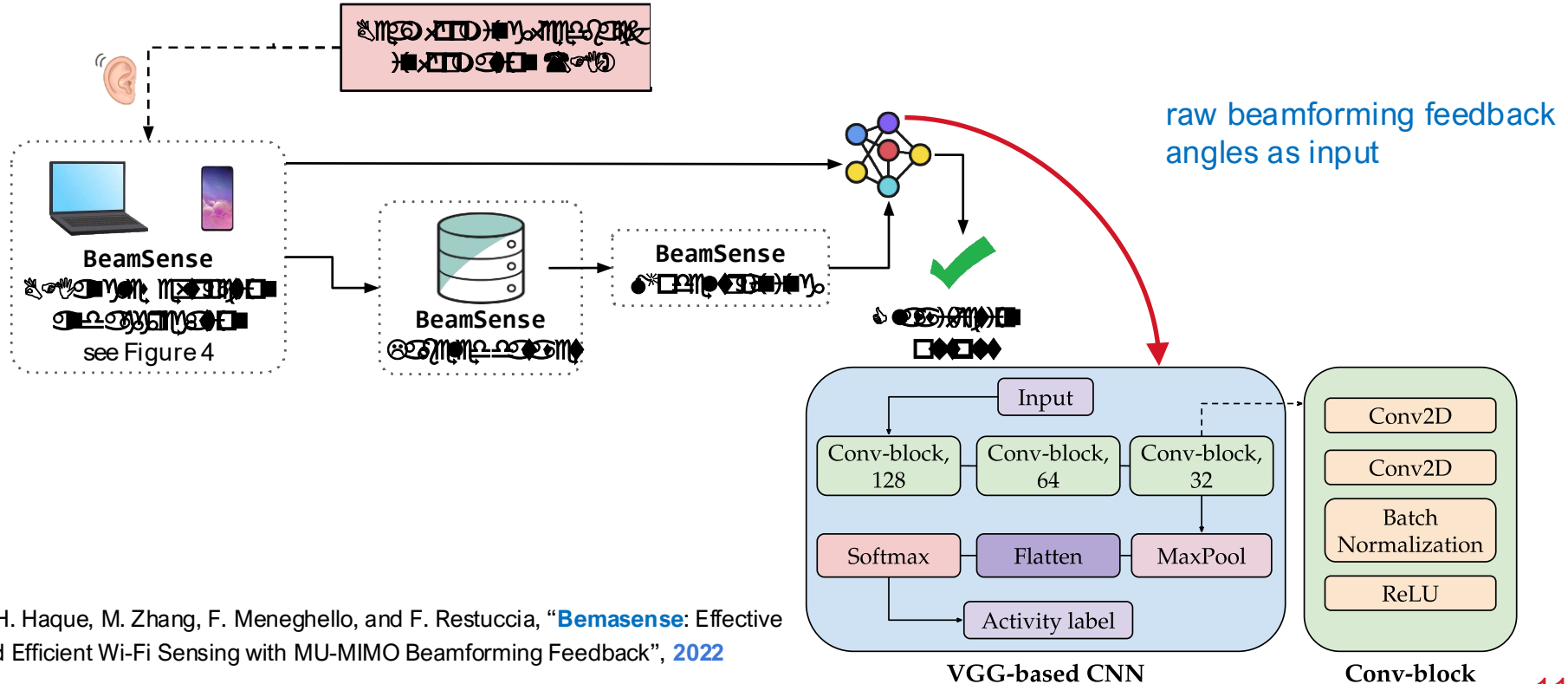
Example of application - DeepCSI

Objective: obtain a **fingerprint of the beamformer** for 802.11 device authentication



Example of application - BeamSense

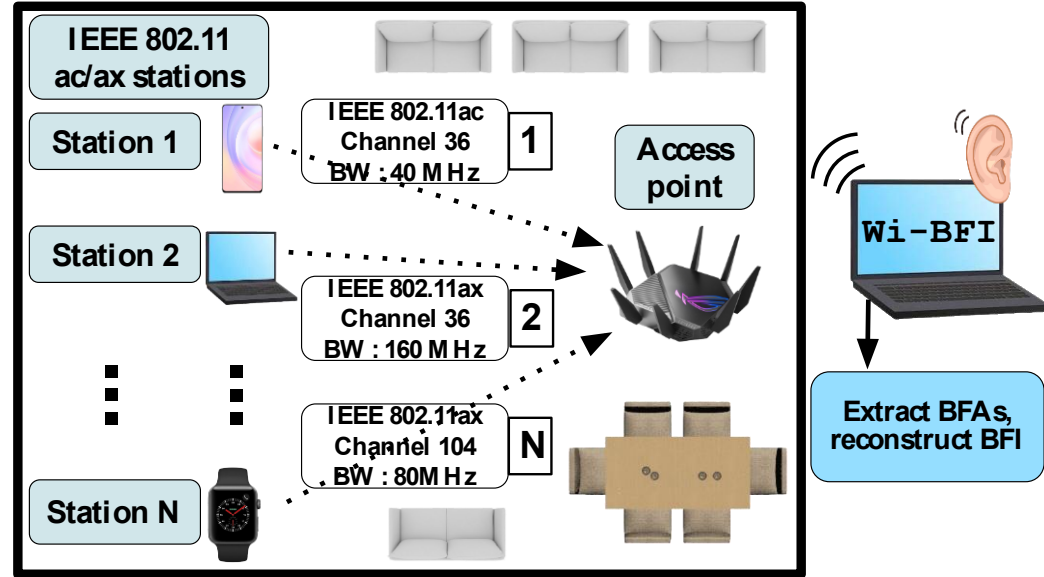
Objective: human activity recognition through 802.11ac/ax **beamforming feedback**



K. H. Haque, M. Zhang, F. Meneghello, and F. Restuccia, "**Bemasense**: Effective and Efficient Wi-Fi Sensing with MU-MIMO Beamforming Feedback", 2022

Concluding remarks

- First tool that allows capturing and decoding the **beamforming feedback angles**, and reconstructing the **beamforming feedback matrices**
- Works with packets transmitted with 20/40/80/160 MHz BW
- Works at multiple bands simultaneously
- SU- and MU-MIMO are supported
- 802.11ac and 802.11ax support



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

Khandaker Foysal Haque*, Francesca Meneghello§, Francesco Restuccia*

*Northeastern University, US

§ University of Padova, Italy

