INFOCOM 2025 1571052184

How to BREAK MU-MIMO Precoding in IEEE 802.11 Wi-Fi Networks

Francesca Meneghello*, Francesco Gringoli†‡, Marco Cominelli§, Michele Rossi*¶, and Francesco Restuccia‖
*Dept. of Information Eng., University of Padova, Italy, †Dept. of Information Eng., University of Brescia, Italy,
‡CNIT - National Inter-University Consortium for Telecommunications, Italy, §Dept. of Electronic, Information and Bioeng., Polytechnic of Milan, Italy, ¶Dept. of Mathematics "Tullio Levi-Civita", University of Padova, Italy,
‖Institute for the Wireless Internet of Things, Northeastern University, United States

***Abstract*—This work reveals a critical vulnerability of the Wi-Fi standard that if unaddressed, might lead to serious security issues and compromise the performance of several billions of Wi-Fi devices. Specifically, this paper introduces and validates with commercial off-the-shelf Wi-Fi devices a new Beamforming Report Eavesdropping Attack (BREAK), which leverages the MU-MIMO channel estimation procedure used by Wi-Fi to decrease the throughput of the entire network without being detected. Through rigorous mathematical optimization, we compute the poisoned feedback that a BREAK adversary needs to send to the access point to reduce the throughput of legitimate users. Through extensive experimental evaluation with commercial Wi-Fi routers and smartphones in multiple network configurations, we show that through BREAK, an adversary may decrease the throughput at legitimate stations by 65% modifying only about 17% of its feedback without being detected. For replicability, we shared the code implementing the attack together with the modified firmware to be used at the adversary node. A video demonstration of BREAK is also available[1].**

***Index Terms*—Wi-Fi, MU-MIMO, adversarial attack, feedback poisoning, channel sounding, precoding.**

I. Introduction

Wi-Fi is among the most successful wireless technologies ever invented. From its humble beginnings in 1990 as a low-cost replacement for Ethernet, it has nowadays become a technology providing seamless Internet connectivity in any public or private space. As Wi-Fi becomes increasingly ubiquitous in our daily lives, investigating its security vulnerabilities becomes a compelling necessity.

In this paper, we experimentally demonstrate for the first time a critical security weakness regarding multi-user multi-input multi-output (MU-MIMO) transmissions of Wi-Fi devices. MU-MIMO is a key operation that allows increasing the network throughput without increasing the bandwidth [1]. Specifically, in a MU-MIMO transmission, several data streams are simultaneously sent by the access point (AP) to different stations (STAs) through the use of precoding weights. Such weights are computed based on the channel estimates performed by the STAs and fed back to the AP as control information during the so-called *channel sounding phase*. However, a major weakness in this approach is that the AP assumes that all the estimates fed back by the STAs are reliable when processing the information to obtain the precoding. *As the AP does not have any direct control over how the feedback is computed at the STAs, a STA can arbitrarily modify the feedback content without being detected.*

[1]https://youtu.be/SeVt0PWZZ8o

Critically, we show that an adversary can modify such feedback to substantially decrease the throughput at legitimate STAs connected to the same AP, as depicted in Figure 1. Indeed, an adversary that monitors the clear-text MU-MIMO feedback from other STAs (step 1 in Figure 1) can craft malicious feedback (2) that alters the precoding on the AP (3), thwarting the entire network's throughput (4). In other words, *malicious feedback can "break" MU-MIMO operations*.

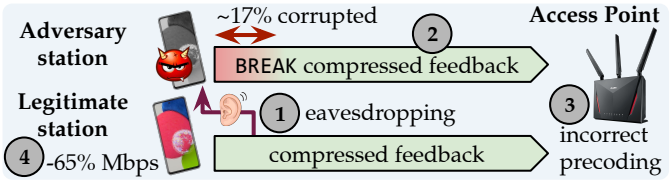

Fig. 1: BREAK overview. The adversary modifies about 17% of its feedback to decrease the legitimate STA throughput by over 65%. The numbers represent the steps of the attack.

Prior work has shown that by transmitting altered feedback, an adversary can obtain a higher share of the network resources or remove other STAs from the transmission [2], [3]. However, such attacks have only been tested through simulations or deploying custom and fully controllable experimental testbeds. *Most importantly, they make the unrealistic assumption that the adversary can gain complete and perfect knowledge of the channel frequency response (CFR) estimated by the STAs in the network*, which can only be acquired by having physical access to the STAs. On the contrary, the STAs feedback transmitted to the AP contains only a *compressed and quantized version* of the CFR estimate (the *beamforming feedback angles*). To highlight the difference between the two attack design approaches, in Figure 2, we show the impact of poisoning an increasing number of sub-channels on the bit error rate (BER) at a legitimate node when using the complete CFR and the compressed beamforming angles in the attack design. The evaluation has been performed through simulations using the Matlab IEEE 802.11ac implementation for an 80 MHz channel (234 orthogonal frequency-division multiplexing (OFDM) data sub-channels) and modulation and coding scheme (MCS) 4. We considered a two-STA Wi-Fi network (one legitimate node and an adversary) and used the WINNER II channel model for Indoor Office with signal-to-noise ratio (SNR) 20. The results – obtained as the average of 200 simulations – show that using the complete CFR leads to overestimating the impact of the attack with respect to what is practically achievable with the available information. This

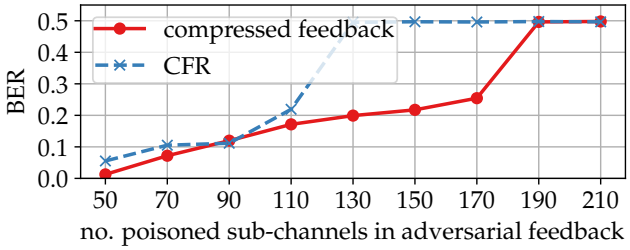

Fig. 2: BER at the victim when using the compressed feedback or the CFR to obtain the malicious feedback.

confirms that the assumption made by previous attacks makes them not implementable on standard-compliant Wi-Fi devices.

In this work, we design, prototype, and evaluate BREAK (*Beamforming Report Eavesdropping AttacK*), the first standard-compliant system that poisons the compressed beamforming feedback used for Wi-Fi MU-MIMO precoding to reduce the network-wide performance of legitimate STAs. In stark opposition with previous work, we have tested BREAK on commercial-of-the-shelf Wi-Fi routers and smartphones, proving that BREAK effectively disrupts ongoing MU-MIMO transmissions without being detected. Additionally, while previous attacks entirely modified the adversary feedback to perform the malicious action, BREAK relies on a partial corruption of it, as shown in Figure 1. To obtain the portion of feedback to be corrupted and the specific corruption to be applied, a novel constrained minimization problem is formulated. Formulating and solving this problem entailed a comprehensive mathematical analysis accounting for the entire MU-MIMO procedure.

Summary of Novel Contributions

- We propose BREAK, a new system to compromise MU-MIMO transmissions in Wi-Fi networks. BREAK leverages the vulnerabilities of the channel feedback process to degrade the throughput of legitimate STAs in a Wi-Fi network. While previous work (see Section II) proposes to modify the beamforming feedback entirely, BREAK is the first system that is capable of negatively affecting the victim throughput by *partially* modifying the feedback (about 17% of data). Moreover, BREAK reduces the throughput of legitimate STAs without radically preventing them from receiving data. BREAK is entirely *implementation-independent* as it relies only on standard-compliant physical layer (PHY) features.
- We formulate a constrained optimization problem for designing malicious feedback. We derive a surrogate problem that solely relies on the beamforming feedback packets from the STAs in the network. These packets can be captured and decoded by any wireless-enabled device without having to decrypt them. Malicious feedback is thus obtained via mathematical optimization by identifying a proper initialization point that ensures fast convergence toward the solution.
- We evaluate BREAK on a real-world Wi-Fi network featuring commercial-off-the-shelf IEEE 802.11ac Wi-Fi devices, including Asus RT-AC86U routers and a Samsung A52S smartphone. Our experimental results demonstrate that BREAK leads to a major decrease in the network throughput (by 65%, on average), even when the feedback of the malicious user is only partially poisoned (e.g., 17% of the sub-channels). Note that the proposed attack only requires one to modify the malicious node by loading the BREAK malicious firmware. Moreover, with commercially available devices, the modified feedback from the adversary goes undetected by the AP. **This work reveals a fundamental vulnerability that can compromise the performance of several billion Wi-Fi devices, which we believe needs to be addressed in future Wi-Fi standards.**

II. Background and Related Work

Prior research on MU-MIMO vulnerabilities has mainly focused on *jamming attacks*. In [4], the authors design a smart jammer that destroys *uplink* MU-MIMO transmissions of a legitimate system by optimally allocating the power budget to damage the sounding and data transmission phases. The effectiveness of the attack is assessed through simulations considering a cellular network with 10 users. Instead, our **BREAK attack aims at stealthily disrupting *downlink* transmissions** from the AP to the legitimate STAs. Even if jamming can also be effective in this case, its implementation would require the jammer to be synchronized with the AP, making the system design highly complex [5]. On the contrary, **BREAK does not require the adversary to synchronize with any device in the network**. Moreover, jamming is an *active* attack that requires the transmission of additional waveforms. In stark contrast, **BREAK modifies the content of standard-compliant control packets that are normally transmitted.** In [6], the authors propose to jam the null data packet (NDP) that is used for channel sounding (see Section III), which leads to imprecise channel estimation and, in turn, to imprecise precoding. This attack has been tested in a one-STA Wi-Fi network implementing the jammer through a universal software radio peripheral (USRP). However, for it to be effective, all the equipment (access point, adversary and victim node) must be correctly placed, and the NDP transmission time must be precisely estimated. [7] shows that the jammer should be closer to the victim than the distance between the victim and the AP for jamming to be effective. In stark contrast, **BREAK relies on the transmission of beamforming feedback packets; thus, adversaries can be placed anywhere in the environment**.

Only a few prior contributions have addressed the inherent vulnerabilities of MU-MIMO systems. The authors in [2], [8] designed malicious feedback that increases the adversary's throughput. The key idea is to deceive the AP into thinking that the adversary has a worse channel than its actual one. This forces the AP to increase the power toward the malicious node or to change the grouping policy, prioritizing the adversary in the transmissions. The attack in [2] has been tested on custom WARP boards. The efficacy of the attack in [8] has instead been tested using simulations for a massive MIMO cellular network with 32 users. However, the attacks in [2], [8] are not implementable on commercial Wi-Fi devices as they assume complete knowledge of the channel matrix, which is unavailable in Wi-Fi. Moreover, they have a different objective than BREAK as they aim at increasing the adversary's throughput and not decreasing a target STA's throughput.

More sophisticated attacks account for the feedback information of the other STAs in the network. However, all of them make the unrealistic assumption that the complete CFR is fed back and available at the adversary. *Sniffing attacks* [2], [9]–[11] shape the feedback to eavesdrop the data transmitted by the AP to the victim. While sniffing attacks might degrade privacy, they do not aim to cause any throughput degradation. Instead, MUSTER [3] prevents a victim from participating in a communication round by subverting the user selection procedure. This leads the AP to select the malicious node instead of the victim for transmission. Similarly to our work, in MUSTER [3] the adversary aims to prevent the transmission to the victim rather than increase its own throughput. Indeed, the malicious node cannot properly decode data directed to it since the malicious feedback does not match the adversary channel. However, MUSTER is not implementable on commercial Wi-Fi devices as it assumes knowledge of the complete channel matrix, whereas the Wi-Fi standard uses compressed feedback. Moreover, it requires knowing the grouping procedure in advance, which is implementation-dependent and not revealed by chip manufacturers. Indeed, MUSTER's learning-based inference is trained on grouping procedures proposed in the literature. Since they are implementation-dependent, there is no guarantee that commercial devices will actually implement them. In addition, MUSTER has been tested through a custom Wi-Fi experimental testbed based on USRPs. On the contrary, **BREAK is entirely implementation-independent as it solely relies on standard-compliant features, and has been implemented on off-the-shelf Wi-Fi devices**.

III. System Model

Following the IEEE 802.11 standard, the process to set up a MU-MIMO transmission in Wi-Fi involves three phases: *channel sounding*, *precoding*, and *interference cancellation*, as hereafter detailed. We consider a Wi-Fi MU-MIMO network where the AP is equipped with M antennas. We indicate with N_i the number of antennas at STA i, and with $N_{\text{ss},i}$ the number of spatial streams directed to such STA. The total number of receiver antennas and spatial streams, summed over all the STAs, is denoted by $N = \sum_i N_i$ and $N_{\text{ss}} = \sum_i N_{\text{ss},i}$, respectively. With K, we indicate the number of OFDM data sub-channels. We refer to $\mathbf{x}_{k,i}$ as the $N_{\text{ss},i} \times 1$-dimensional vector containing the k-th OFDM sample of the signal transmitted to STA i and with $\mathbf{x}_k$ as the $N_{\text{ss}} \times 1$-dimensional vector collecting $\mathbf{x}_{k,i}$ for all the STAs. Finally, $\mathbf{H}_{k,i}$ represents the $N_i \times M$-dimensional matrix collecting the CFR of the k-th OFDM sub-channel for the i-th STA. Henceforth, we will use * and $\dagger$ to indicate the complex conjugate and the complex conjugate transpose operations, respectively, and $[\mathbf{C}]_{l,j}$ to indicate the element at row l and column j of matrix $\mathbf{C}$.

Channel Sounding. The AP triggers the channel estimation by transmitting a sounding packet (the NDP) to the STAs. Each STA i uses the known training field in the NDP to estimate the CFR $\mathbf{H}_{\gamma,k,i}$. Note that we will use the sub-script γ to indicate the CFR that is estimated through the NDP and utilized at the AP for the computation of the precoding matrix $\mathbf{W}_k$. The CFR estimated on data packets and used at the STAs for decoding is without γ. We adopt the same notation for the matrices respectively derived from $\mathbf{H}_{\gamma,k,i}$ and $\mathbf{H}_{k,i}$. The CFR $\mathbf{H}_{\gamma,k,i}$ is then compressed for efficient transmission to the AP [12], [13]. At first, the CFR is decomposed via singular value decomposition (SVD):

$$\mathbf{H}_{\gamma,k,i} = \mathbf{U}_{\gamma,k,i} \mathbf{S}_{\gamma,k,i} \mathbf{Z}^{\dagger}_{\gamma,k,i}, \tag{1}$$

where $\mathbf{S}_{\gamma,k,i}$ is an $N_i \times M$ diagonal matrix collecting the singular values of $\mathbf{H}_{\gamma,k,i}$, while $\mathbf{U}_{\gamma,k,i}$ and $\mathbf{Z}_{\gamma,k,i}$ are $N_i \times N_i$ and $M \times M$ unitary matrices, respectively. The first $N_{\text{ss},i}$ columns of $\mathbf{Z}_{\gamma,k,i}$ are referred to as the *beamforming feedback matrix* $\tilde{\mathbf{V}}_{\gamma,k,i}$. Such matrix is further compressed through Givens rotations obtaining the so-called *beamforming feedback angles*. The angles are then quantized to minimize the overhead [14] and transmitted to the AP for precoding.

Precoding. Using ZF precoding, the $M \times N_{\text{ss}}$ *precoding matrix* $\mathbf{W}_k$ writes as [15]

$$\mathbf{W}_k = \tilde{\mathbf{V}}_{\gamma,k} \left(\tilde{\mathbf{V}}^{\dagger}_{\gamma,k} \tilde{\mathbf{V}}_{\gamma,k} \right)^{-1}, \tag{2}$$

where $\tilde{\mathbf{V}}_{\gamma,k}$ is the $M \times N_{\text{ss}}$ matrix obtained by concatenating the $M \times N_{\text{ss},i}$ $\tilde{\mathbf{V}}_{\gamma,k,i}$ matrices reconstructed from the quantized beamforming feedback angles received by all the STAs. Hence, the transmitted signal is obtained as $\mathbf{W}_k \mathbf{x}_k$. Eq. (2) enforces the ℓ-th column of $\mathbf{W}_k$ to be orthogonal to the j-th column of $\tilde{\mathbf{V}}_{\gamma,k}$, with $j \neq \ell$. The orthogonality propriety makes it possible to minimize the inter-stream interference (ISI) at each STA i and inter-user interference (IUI) between STAs. As detailed in Section IV, BREAK aims to destroy such orthogonality.

Interference Cancellation. The signal collected at the N_i antennas of STA i is $\mathbf{Y}_{k,i} = \mathbf{H}_{k,i} \mathbf{W}_k \mathbf{x}_k + \mathbf{n}_k$, where $\mathbf{n}_k$ is the additive noise. To retrieve the transmitted signal $\mathbf{x}_{k,i}$, each STA i applies an *interference cancellation matrix* $\mathbf{G}_{k,i}$ obtained as $\mathbf{G}_{k,i} = \mathbb{I}_{N_{\text{ss},i} \times N_{\text{ss}}} \tilde{\mathbf{H}}^{\dagger}_{k,i} (\tilde{\mathbf{H}}_{k,i} \tilde{\mathbf{H}}^{\dagger}_{k,i} + \mathbf{R}_{n,k})^{-1}$, where $\mathbf{R}_{n,k}$ is the noise covariance matrix and $\tilde{\mathbf{H}}_{k,i} = \mathbf{H}_{k,i} \mathbf{W}_k$ is the $N_i \times N_{\text{ss}}$-dimensional CFR of the beamformed channel, estimated on the training fields in the data packet [16]. Hence, the estimate $\hat{\mathbf{x}}_{k,i}$ of the transmitted signal is obtained as

$$\hat{\mathbf{x}}_{k,i} = \mathbf{G}_{k,i} \mathbf{Y}_{k,i}. \tag{3}$$

Ideally, when $\mathbf{R}_{n,k} = 0$ and there is no inter-stream interference, $\mathbf{G}_{k,i} \mathbf{H}_{k,i} \mathbf{W}_k = \mathbb{I}_{N_{\text{ss},i} \times N_{\text{ss}}}$, and, in turn, $\hat{\mathbf{x}}_{k,i} = \mathbf{x}_{k,i}$, i.e., STA i exactly retrieves its $N_{\text{ss},i}$ streams.

IV. BREAK Problem Formulation

For the following analysis, we define the complex matrix $\tilde{\mathbf{V}}_{\gamma,\text{all},i} = \left[\tilde{\mathbf{V}}_{\gamma,0,i} \ \dots \ \tilde{\mathbf{V}}_{\gamma,K-1,i} \right]$ ($K \times M \times N_{\text{ss},i}$ dimensional), collecting the beamforming feedback matrices $\tilde{\mathbf{V}}_{\gamma,k,i}$ of user i for all the sub-channels $k \in \mathcal{K}$, with $\mathcal{K} = \{0, \dots, K-1\}$ representing the set of OFDM sub-channels. We will use index $i = a$ to indicate the adversary node and index $i = \ell$ to indicate the legitimate nodes. Note that, as done also in previous work (Section II), we reasonably assume that the adversary is connected to the AP. This is especially feasible when considering Wi-Fi networks deployed in public places. If this is not the case, the adversary can mount a preliminary attack to gain access to the network [17].

Considering Eq. (3), the throughput of legitimate users can be decreased by forcing $\mathbf{G}_{k,\ell}\mathbf{H}_{k,\ell}\mathbf{W}_k$ to be as different as possible from the generalized identity matrix $\mathbb{I}_{N_{\mathrm{ss},\ell}\times N_{\mathrm{ss}}}$. To this purpose, the BREAK adversary node can modify its beamforming feedback matrix $\tilde{\mathbf{V}}_{\gamma,\mathrm{all},a}$ (and, in turn, the beamforming feedback angles transmitted to the AP) to compromise the precoding matrix $\mathbf{W}_k$ computed at the AP. As $\mathbf{W}_k$ is obtained by combining the feedback from all the STAs (see Eq. (2)), the adversary leverages the knowledge of the compressed feedback of the legitimate STAs to compute effectively harmful feedback. From a mathematical standpoint, BREAK maximizes the mean-square-error (MSE) between $\mathbf{G}_{k,\ell}\mathbf{H}_{k,\ell}\mathbf{W}_k$ and $\mathbb{I}_{N_{\mathrm{ss},\ell}\times N_{\mathrm{ss}}}$:

General Problem Definition

$$\max_{\tilde{\mathbf{V}}_{\gamma,\mathrm{all},a}} \sum_{k\in\mathcal{K}}\sum_{\ell} \mathrm{MSE}\Big(\mathbf{G}_{k,\ell}\mathbf{H}_{k,\ell}\mathbf{W}_k,\ \mathbb{I}_{N_{\mathrm{ss},\ell}\times N_{\mathrm{ss}}}\Big) \quad \text{subject to } P\le P_{\max} \tag{4}$$

where $P=\sum_{k\in\mathcal{K}}\mathrm{Tr}\big[\mathbf{W}_k\mathbf{W}_k^{\dagger}\big]$ and $P_{\max}$ are the transmit power (at the AP) in units of energy per OFDM symbol and its maximum value, respectively ([18], [19]). Once $\tilde{\mathbf{V}}_{\gamma,k,a}$ is obtained for $k\in\{0,\dots,K-1\}$, by solving Eq. (4), the adversary computes and quantizes the feedback angles and sends them to the AP to trigger the change of the precoding weights and infer the desired damage to the legitimate nodes.

Rewriting the objective function in Eq. (4)**.** The problem in Eq. (4) involves the uncompressed CFR matrices $\mathbf{H}_{k,\ell}$. However, *we recall that the adversary cannot access the complete CFR estimated by the legitimate STAs*; it can only reconstruct the matrices $\tilde{\mathbf{V}}_{\gamma,k,\ell}$ from the captured compressed feedback. Thus, the adversary cannot solve the problem in Eq. (4) without physical access to all the STAs. In the following, we derive a *surrogate optimization problem* that the adversary can solve only knowing the compressed beamforming feedback. For the sake of clarity, we consider a two-STA network where the adversary and the legitimate nodes have a single antenna, i.e., $N_a=N_{\mathrm{ss},a}=1$, $N_\ell=N_{\mathrm{ss},\ell}=1$, and the AP has two transmitting antennas, $M=\sum_i N_{\mathrm{ss},i}=2$ – an example of the derivation for the general case can be found in [20]. For this setup, the MSE in Eq. (4) takes the form

$$\mathrm{MSE}\big(\,\cdot\,\big)=(\det[\mathbf{\Omega}])^{-1}\mathbf{w}_{k,a}^{\dagger}\mathbf{H}_{k,\ell}^{\dagger}\mathbf{R}_{n,k}^{-1}\mathbf{H}_{k,\ell}\mathbf{w}_{k,a}, \tag{5}$$

where $\mathbf{w}_{k,a}$ is the 2×1 precoding vector associated with the adversary. To make explicit the contribution of the control variable $\tilde{\mathbf{v}}_{\gamma,k,a}$ (see Eq. (4)), we decompose the 1×2 dimensional channel matrix $\mathbf{H}_{k,\ell}$ via SVD, as presented in Eq. (1) for $\mathbf{H}_{\gamma,k,i}$. Note that here we consider the CFR estimated on the training fields of the data packets (notation without γ, see Section III). We have $\mathbf{H}_{k,\ell}=u_{k,\ell}\mathbf{S}_{k,\ell}\mathbf{Z}_{k,\ell}^{\dagger}$, where $u_{k,\ell}$ is a complex number with $u_{k,\ell}^{*}u_{k,\ell}=1$, $\mathbf{S}_{k,\ell}$ is a 1×2 vector collecting the singular value $\sigma_{k,\ell}$ of $\mathbf{H}_{k,\ell}$, i.e., $\mathbf{S}_{k,\ell}=\begin{bmatrix}\sigma_{k,\ell} & 0\end{bmatrix}$, and $\mathbf{Z}_{k,\ell}$ is a 2×2 unitary matrix. We refer to the first $N_{\mathrm{ss},\ell}=1$ column of $\mathbf{Z}_{k,\ell}$ as $\tilde{\mathbf{v}}_{k,\ell}$ (see Section III). Hence, $\mathbf{H}_{k,\ell}=u_{k,\ell}\sigma_{k,\ell}\tilde{\mathbf{v}}_{k,\ell}^{\dagger}$, and Eq. (5) becomes

$$\mathrm{MSE}\big(\,\cdot\,\big)=(\det[\mathbf{\Omega}])^{-1}\sigma_{k,\ell}^{*}\sigma_{k,\ell}\mathbf{w}_{k,a}^{\dagger}\tilde{\mathbf{v}}_{k,\ell}\mathbf{R}_{n,k}^{-1}\tilde{\mathbf{v}}_{k,\ell}^{\dagger}\mathbf{w}_{k,a}. \tag{6}$$

Rewriting the optimization problem in Eq. (4)**.** The term in Eq. (6) is associated with the inter-user interference caused by the adversary to the victim and should approach zero in the ideal case. Specifically, the term that goes to zero if the precoding is built properly is $\mathbf{w}_{k,\mathrm{a}}^{\dagger}\tilde{\mathbf{v}}_{k,1}$. In turn, the adversary can focus on making this term differ from zero. Using Eq. (2) to rewrite $\mathbf{w}_{k,a}$, we obtain

$$\mathbf{w}_{k,a}^{\dagger}\tilde{\mathbf{v}}_{k,\ell}=\frac{-\tilde{\mathbf{v}}_{\gamma,k,a}^{\dagger}\tilde{\mathbf{v}}_{\gamma,k,\ell}\tilde{\mathbf{v}}_{\gamma,k,\ell}^{\dagger}\tilde{\mathbf{v}}_{k,\ell}+\tilde{\mathbf{v}}_{\gamma,k,\ell}^{\dagger}\tilde{\mathbf{v}}_{\gamma,k,\ell}\tilde{\mathbf{v}}_{\gamma,k,a}^{\dagger}\tilde{\mathbf{v}}_{k,\ell}}{\det\big[\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\big]}, \tag{7}$$

with $\tilde{\mathbf{V}}_{\gamma,k}=\begin{bmatrix}\tilde{\mathbf{v}}_{\gamma,k,\ell} & \tilde{\mathbf{v}}_{\gamma,k,a}\end{bmatrix}$ and

$$\begin{aligned}\det\big[\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\big]=\ &\tilde{\mathbf{v}}_{\gamma,k,\ell}^{\dagger}\tilde{\mathbf{v}}_{\gamma,k,\ell}\tilde{\mathbf{v}}_{\gamma,k,a}^{\dagger}\tilde{\mathbf{v}}_{\gamma,k,a}\\ &-\tilde{\mathbf{v}}_{\gamma,k,\ell}^{\dagger}\tilde{\mathbf{v}}_{\gamma,k,a}\tilde{\mathbf{v}}_{\gamma,k,a}^{\dagger}\tilde{\mathbf{v}}_{\gamma,k,\ell}.\end{aligned} \tag{8}$$

To derive a surrogate problem of Eq. (4), we analyze Eq. (7). At first, we note that if the CFR estimated on the NDP (with γ) equals the CFR estimated on data packets (without γ), i.e., $\tilde{\mathbf{v}}_{\gamma,k,\ell}=\tilde{\mathbf{v}}_{k,\ell}$, the numerator in Eq. (7) becomes zero *independently* of $\tilde{\mathbf{v}}_{\gamma,k,a}$. In turn, $\mathbf{w}_{k,a}^{\dagger}\tilde{\mathbf{v}}_{k,\ell}=0$ and there is no inter-user interference as $\mathbf{w}_{k,a}$ and $\tilde{\mathbf{v}}_{k,\ell}$ are orthogonal (see Section III). However, the $\tilde{\mathbf{v}}_{\gamma,k,\ell}$ and $\tilde{\mathbf{v}}_{k,\ell}$ estimates are obtained in subsequent time instants on the NDP and the data packet. Given the variability of the wireless channel, they slightly differ in practice ($\tilde{\mathbf{v}}_{\gamma,k,\ell}\neq\tilde{\mathbf{v}}_{k,\ell}$), and, in turn, $\mathbf{w}_{k,a}$ and $\tilde{\mathbf{v}}_{k,\ell}$ are *nonorthogonal*. Interestingly, this makes Eq. (7) dependent on $\tilde{\mathbf{v}}_{\gamma,k,a}$. BREAK leverages this dependency to enhance the non-orthogonality between $\mathbf{w}_{k,a}$ and $\tilde{\mathbf{v}}_{k,\ell}$, thus increasing the MSE in Eq. (6). Our intuition is as follows. The numerator in Eq. (7) cannot be significantly modified by tuning $\tilde{\mathbf{v}}_{\gamma,k,a}$, as it is proportional to $\tilde{\mathbf{v}}_{\gamma,k,a}$, but the multiplying factor is small due to $\tilde{\mathbf{v}}_{\gamma,k,\ell}$ approaching $\tilde{\mathbf{v}}_{k,\ell}$. Moreover, we remind that only $\tilde{\mathbf{v}}_{\gamma,k,\ell}$ is accessible when designing $\mathbf{W}_k$, while $\tilde{\mathbf{v}}_{k,\ell}$ is associated with the transmission that occurs after the precoding matrix definition and, in turn, cannot be used by the adversary to shape the feedback. On the contrary, the denominator in Eq. (8) only depends on the feedback matrices, available to the adversary. Thus, the adversary can effectively modify $\tilde{\mathbf{v}}_{\gamma,k,a}$ to decrease the absolute value of the denominator as much as possible. Following this intuition, we replace the problem in Eq. (4) by the following constrained minimization problem

BREAK Problem Definition

$$\min_{\tilde{\mathbf{V}}_{\gamma,all,a}} \sum_{k\in\mathcal{K}}\det\Big[\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\Big] \quad \text{subject to } \det\Big[\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\Big]\neq 0,\forall k;\ P\le P_{\max} \tag{9}$$

The objective function of the BREAK problem is hereafter indicated with F, i.e., $F=\sum_{k\in\mathcal{K}}\Big(\det\Big[\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\Big]\Big)\in\mathbb{R}_{\ge 0}$. The solution to the BREAK problem is referred to as $\tilde{\mathbf{V}}_{\gamma,\mathrm{all},a}^{\mathrm{BREAK}}$ and represents the adversarial beamforming feedback matrix that the adversary should use to minimize the throughput at the legitimate receivers. *Note that the BREAK problem is written in the most general form, which holds for any number of devices, antennas, and streams. Hence, it applies to any network setup.*

V. Crafting BREAK Feedback

We solved the BREAK problem in Eq. (9) using interior-point optimization. Through our preliminary evaluations (see also the simulation results in [20]), we realized that the adversary does not need to modify the complete compressed beamforming feedback matrix $\tilde{\mathbf{V}}_{\gamma,\text{all},a}$ – i.e., for all the K OFDM sub-channels – to inflict damage to the legitimate STAs in the network. The modification of a sub-set $\hat{\mathcal{K}}$ of $\hat{K}$ sub-channels suffices to modify the precoding and create interference at the legitimate receivers. Therefore, the adversary can keep the feedback matrix $\tilde{\mathbf{V}}_{\gamma,k,a}$ for $k \in \mathcal{K} \setminus \hat{\mathcal{K}}$ unchanged, thus making harder for the AP to detect the attack. Here, the challenge is selecting the set $\hat{\mathcal{K}}$ of sub-channels to poison. One possibility is to select the sub-channels at random. However, this does not assure the modification of those sub-channels that have the *highest impact on the precoding performance*. Hence, we designed a strategy that selects the best sub-channels to be poisoned based on the problem in Eq. (9). The procedure is described in Section V-A. The complete routine is summarized in Figure 3, and detailed in Section V-B and Algorithm 1 .

A. Poisoned OFDM Sub-channels Selection

We select the OFDM sub-channels to be poisoned as those that have the highest impact on the minimization of the BREAK objective function (F) in Eq. (9). We note that F is obtained by *summing K contributions*, one for each sub-channel. Hence, the best strategy for the adversary to *minimize* F is to change the sub-channels k of $\tilde{\mathbf{V}}_{\gamma,\text{all},a}$ that contribute the most to this sum. To identify such sub-channels, the adversary first computes the gradient of F with respect to $\tilde{\mathbf{V}}_{\gamma,\text{all},a}$ and evaluates it at the unmodified $\tilde{\mathbf{V}}_{\gamma,\text{all},a}$ matrix – $\nabla F(\tilde{\mathbf{V}}_{\gamma,\text{all},a})$. Hence, for each of the transmitter antennas (rows of $\tilde{\mathbf{V}}^{\text{BREAK}}_{\gamma,\text{all},a}$) over each of the spatial streams (columns of $\tilde{\mathbf{V}}^{\text{BREAK}}_{\gamma,\text{all},a}$), the adversary selects the set $\hat{\mathcal{K}}_{m,s_a}$ of sub-channels to be poisoned as those corresponding to the entries in $\nabla F(\tilde{\mathbf{V}}_{\gamma,\text{all},a})$ with the highest absolute values (lines 3-4 of Algorithm 1).

B. Optimization Routine

For all transmitter antennas $m \in \{0,\ldots,M-1\}$ and spatial streams $s_a \in \{0,\ldots,N_{\text{ss},a}-1\}$ (line 3 of Algorithm 1), BREAK adversary node selects the set $\hat{\mathcal{K}}_{m,s_a}$ of sub-channels to be modified through the procedure in Section V-A (line 4). The elements of $\tilde{\mathbf{V}}^{\text{BREAK}}_{\gamma,\text{all},a}$ on sub-channels $k \in \mathcal{K} \setminus \hat{\mathcal{K}}_{m,s_a}$ are set to their original values (line 5). The perturbation for the elements on sub-channels $k \in \hat{\mathcal{K}}_{m,s_a}$ is obtained by solving the minimization problem in Eq. (9) (line 9), using the values on the $k \in \hat{\mathcal{K}}_{m,s_a}$ sub-channels (for all antennas $m \in \{0,\ldots,M-1\}$ and spatial streams $s_a \in \{0,\ldots,N_{\text{ss},a}-1\}$) as the control variables (line 6). Note that although $\hat{K}$ is fixed, the set $\hat{\mathcal{K}}_{m,s_a}$ differs for each pair of antenna $m \in \{0,\ldots,M-1\}$ and spatial stream $s_a \in \{0,\ldots,N_{\text{ss},a}-1\}$, as each sub-channel can have a different impact on the objective function for different m and s_a. Once obtained $\tilde{\mathbf{V}}^{\text{BREAK}}_{\gamma,\text{all},a}$, the adversary computes and quantizes the beamforming feedback angles and transmits them to the AP through the IEEE 802.11 procedure (line 10).

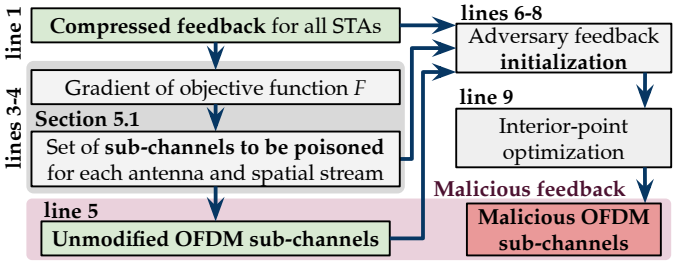

Fig. 3: Procedure for BREAK malicious feedback crafting. The line numbers refer to Algorithm 1.

Algorithm 1 Crafting BREAK malicious feedback solving Eq. (9) at the adversary

1: **Input:** $\tilde{\mathbf{V}}_{\gamma,\text{all},i}$ reconstructed from the captured quantized feedback angles for all STAs; no. sub-channels to be poisoned $\hat{K}$.
2: **Output:** BREAK malicious beamforming feedback angles.
3: **for all** $m \in \{0,\ldots,M-1\}$ transmit antennas, and $s_a \in \{0,\ldots,N_{\text{ss},a}-1\}$ adversary streams **do**
4: Define set $\hat{\mathcal{K}}_{m,s_a}$ as the $\hat{K}<K$ sub-channels associated with highest $\left[\|\nabla F(\tilde{\mathbf{V}}_{\gamma,k,a})\|\right]_{m,s_a}$ values, $k \in \{0,\ldots,K-1\}$
5: Fix the values for the unmodified sub-channels $\left[\tilde{\mathbf{V}}^{\text{BREAK}}_{\gamma,k,a}\right]_{m,s_a} \leftarrow \left[\tilde{\mathbf{V}}_{\gamma,k,a}\right]_{m,s_a}$ for $k \in \mathcal{K} \setminus \hat{\mathcal{K}}_{m,s_a}$
6: Set $\left[\tilde{\mathbf{V}}_{\gamma,k,a}\right]_{m,s_a}$, $k \in \hat{\mathcal{K}}_{m,s_a}$, as optimization control variables
7: Define $\boldsymbol{\eta}$ as a $\hat{K}$ dimensional matrix which elements follow a Gaussian distribution $\boldsymbol{\eta}_k \sim \mathcal{N}(0,1)$, and $\alpha > 0$
8: Define the initialization point for the BREAK malicious sub-channels $\left[\tilde{\mathbf{V}}^{\text{BREAK}}_{\gamma,k,a}\right]_{m,s_a} \leftarrow \left[\tilde{\mathbf{V}}_{\gamma,k,\ell}\right]_{m,s_a} + \alpha\left[\boldsymbol{\eta}_k\right]_{m,s_a}$ for $k \in \hat{\mathcal{K}}_{m,s_a}$ and legitimate STA ℓ
9: Obtain $\tilde{\mathbf{V}}^{\text{BREAK}}_{\gamma,\text{all},a}$ though interior-point optimization.
10: Compute and quantize the feedback angles from $\tilde{\mathbf{V}}^{\text{BREAK}}_{\gamma,\text{all},a}$.

Initialization. To enforce fast convergence toward the minimum, BREAK uses one of the unconstrained minima of the objective function as the solver initialization point. The objective function F reaches its unconstrained minimum when *i)* $\tilde{\mathbf{V}}^{\text{BREAK}}_{\gamma,k,a} = 0$ or *ii)* $\tilde{\mathbf{V}}^{\text{BREAK}}_{\gamma,k,a} = \tilde{\mathbf{V}}_{\gamma,k,\ell}$, $\forall k \in \mathcal{K}$. These solutions are infeasible as they do not meet the two BREAK constraints: the determinant is at the denominator of Eq. (7) and hence it can neither be zero (first constraint) nor arbitrarily small, as otherwise $\mathbf{W}_k$ would not satisfy the power constraint (second constraint). In our previous work [20], we obtained malicious feedback starting from unconstrained solution *i)*. However, we only considered an *emulated scenario* for the evaluation. Instead, we select unconstrained solution *ii)* as BREAK initialization point (lines 7-8 of Algorithm 1) as from some preliminary *experiments* with commercial devices we saw that this leads to the greatest damage to the legitimate STAs. Gaussian noise is added to make the solution feasible for proper initialization. We set $\alpha = 0.1$ in our evaluations.

Complexity of the proposed solution. The time complexity of the attack depends on Algorithm 1 and, in turn, on the complexity of the optimization in line 9. The computation complexity of evaluating the objective function F is $\mathcal{O}(2 \times \hat{K} \times N_{\text{ss}}^3 + \hat{K} \times M \times N_{\text{ss}}^2)$. On average, Algorithm 1 converges in about 10 iterations evaluating function F about 600 times per iteration. Using $\hat{K} = 256$ (IEEE 802.11ac at 80 MHz),

$M = N_{ss} = 2$, and a 4-core machine with CPU frequency of 3 GHz, the execution time is about 1 ms. If channel sounding is performed approximately every 10 ms (as recommended in [21]), the adversarial feedback obtained in one instant can be successfully used at the subsequent sounding episode (after 10 ms). For a typical human walking speed of 5.1 km/h, in 10 ms the device moves about 0.014 m, which is half of $\lambda/2$ (Wi-Fi channel 157), so we reasonably assume that the impact of mobility is modest for a Rayleigh fading channel.

C. BREAK Countermeasures

Preventing BREAK adversary action requires rethinking the way MU-MIMO is implemented in Wi-Fi. The vulnerabilities leveraged by BREAK are linked with the IEEE 802.11 MU-MIMO procedure that relies on *explicit feedback from the STAs* to obtain the precoding at the AP. This procedure must be followed by every Wi-Fi-compliant STA and AP. Hence, an adversary can always gain knowledge of the feedback transmitted by legitimate STAs and hamper the precoding efficacy by transmitting malicious feedback, building on the known AP precoding procedure. The fact that the feedback is transmitted *unencrypted* simplifies the adversary's effort. The feedback shall not be encrypted according to the most recent IEEE 802.11 standard documents since they are transmitted through specific "Not Robust Action Frames". Indeed, encrypting the feedback would have increased processing latency, energy consumption, and system complexity. Although future Wi-Fi standards may encrypt Action Frames, all devices compliant with 802.11ac/ax/be (more than 21 billion devices [22]) will still be vulnerable to BREAK as Wi-Fi standards must be backward compatible. Newly proposed data-driven sounding methods (e.g., [23], [24]) could make it harder for an adversary to estimate the effects of transmitting malicious feedback, as the parameters used for feedback compression at the STAs and precoding at the AP are not deterministically obtained using the 802.11 procedure. Yet, this does not solve the inherent vulnerability of explicit feedback transmission. Hence, *solving BREAK remains an open problem to secure next-generation Wi-Fi* and exploring countermeasures deserves a separate study.

VI. Experimental Setup

We evaluated the BREAK's effectiveness on commercial-off-the-shelf IEEE 802.11ac Wi-Fi devices in a real environment. The devices operated on the IEEE 802.11ac channel 157 using 80 MHz of bandwidth. In this configuration, the total number of sub-channels in the feedback, i.e., the number of data sub-channels removing the pilots, is $K = 234$. The experimental testbed is shown in Figure 4 together with a schematic of the placement of the nodes. The nodes in positions $S1$ and $S2$ are sniffers and allowed us to monitor the attack. The AP, the adversary node, and the legitimate STA were implemented and placed as follows. Note that our experiments were not conducted in a controlled environment, as other Wi-Fi devices were concurrently operating and transmitting traffic.

AP. The AP is a commercial 4-antenna Asus RT-AC86U (unmodified) and is placed on the South wall of the room. Only three antennas are visible in the pictures, as one is internal.

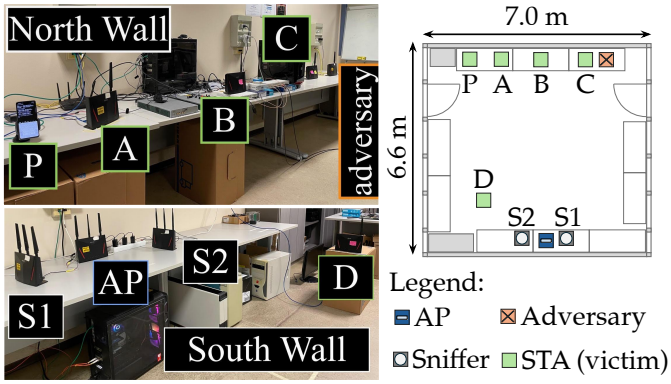

Fig. 4: Picture and layout of the experimental testbed.

Adversary. This is implemented on another Asus RT-AC86U by applying the firmware modifications described in Section VI-A. The adversary is placed in the North-East corner of the room, and a single antenna is enabled on the device.

Legitimate STAs for the evaluations in Sections VII-A-VII-B. The victims for the first sets of experiments are unmodified Asus RT-AC86U devices configured in STA mode and with a single enabled antenna. These nodes are placed in the locations labeled with a letter from A to D in Figure 4.

Legitimate STA for the evaluation in Section VII-C. We also evaluated BREAK using a Samsung A52S smartphone as the victim. The smartphone is in position P in Figure 4.

A. BREAK Implementation on a Commercial Wi-Fi Device

Implementing the BREAK attack on a commercial device requires modifying firmware-level functionalities to enable the transmission of custom beamforming feedback angles. This is challenging as Wi-Fi device vendors do not provide access to the firmware features. Hence, we reverse-engineered the channel sounding procedure implemented on Asus RT-AC86U Wi-Fi devices. The Wi-Fi chipset in such devices is the Broadcom BCM4365, featuring a D11 microcontroller whose behavior can be modified using the Nexmon framework [25]. The D11 core is responsible for managing all the time-critical operations [26], including the ones associated with MU-MIMO. During the channel sounding phase (see Section III), the content (angles) of the feedback is computed by the hardware upon reception of the NDP and stored in an internal read-only memory region. Afterward, the D11 core schedules the transmission of the feedback by configuring the transmission engine to retrieve the feedback from that memory. We modified this part of the procedure with Nexmon so that the content is fetched from another memory that we control. The attack is hence a three-step process: (i) by leveraging a user-space utility that we developed, we extract the content of the hardware-computed feedback from the adversary device where we also use the monitor mode for collecting the feedback packet(s) transmitted by the victim(s); (ii) next, we copy the captured feedback packets to a workstation where we use a Matlab script to craft the BREAK malicious feedback; (iii) finally, we transfer the BREAK malicious feedback to the adversary device where it is then transmitted to the AP.

Our firmware modification is based on the Nexmon tool; hence, the adversary is only required to install Nexmon and load the BREAK firmware that we will make available. The process only takes a few minutes. We point out that the AP and the other STAs (victims) are legitimate nodes that have not been modified, i.e., they operate following the routines defined in the IEEE 802.11 standard or designed by the chip's manufacturer (for implementation-dependent features).

VII. Experimental Results

We set the maximum transmission power parameter in Eq. (9) to $P_{\max} = 1 \times 10^5$ units of energy per OFDM symbol, according to what we observed in ordinary transmissions. To evaluate the effect of the attack, we established `iperf` sessions between the AP and each of the connected STAs (legitimate or malicious). UDP packets (1500 byte-long) were transmitted saturating the channel capacity. The bars in the following plots represent the 25-75 percentile interval, the red horizontal lines within the bars represent the median value, and the whiskers span over the 5-95 percentile interval. The horizontal lines with markers in the plots indicate the throughput before the attack, averaged across the experiments.

A. Two-STA Evaluation

We carried out a first evaluation deploying a two-STA network consisting of a legitimate STA (unmodified Asus RT-AC86U) and an adversary node (modified Asus RT-AC86U) connected to the AP. We considered two different locations for the victim (STA A and STA D in Figure 4) and we carried out 10 different experiments for each location, collecting the MU-MIMO performance metrics, at a 1 Hz rate, before the attack and for 20 s after performing the adversary action, i.e., `BREAK` malicious feedback angles transmission.

Random Attack. To confirm the need for `BREAK`'s optimization, we first evaluate the effect of poisoning the feedback by randomly corrupting $\hat{K}$ sub-channels, without using `BREAK`. We considered two options for the sub-channel selection: (v1) randomly select $\hat{K}$ out of K sub-channels, and (v2) randomly select a group of $\hat{K}$ contiguous sub-channels. We placed the victim in position A (see Figure 4) and observed the throughput before and after the attack. The results as a function of $\hat{K}$ are depicted in Figure 5 and show that randomly corrupting the feedback (even increasing $\hat{K}$) does not decrease the victim's throughput. This is because the random feedback transmitted by the adversary does not disrupt the transmissions to the victim: The data stream transmitted to the adversary is correctly precoded to be orthogonal to the channel between the AP and the victim and, in turn, it does not create interference at the victim's receiver. The random attacks only lead to completely destroying MU-MIMO transmissions directed to the adversary as its reported channel used for precoding differs from the actual one. In Figure 5 we also note a slight increase in the victim's throughput with respect to the average throughput before the attack (indicated by the horizontal lines in the plot). We analyzed this unexpected behavior and found that it is linked with a reduction of the traces transmitted in single-user multi-input, multi-output (SU-MIMO) mode. This frees spectrum resources, which are used to transmit more MU-MIMO frames. The reason why the rate controller at the AP decides to do this is implementation-specific.

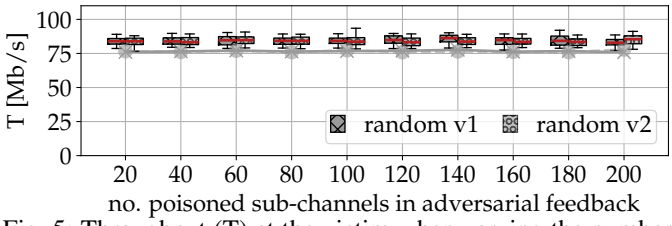

Fig. 5: Throughput (T) at the victim when varying the number of poisoned sub-channels randomly.

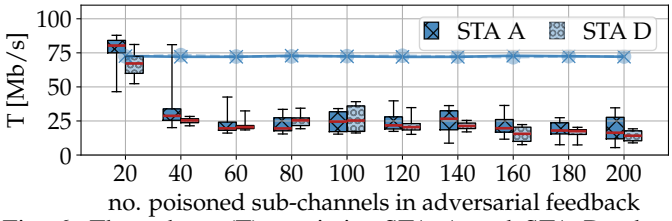

Fig. 6: Throughput (T) at victim STA A and STA D when varying the number of poisoned sub-channels $\hat{K}$ using `BREAK`.

Changing the Number of Poisoned Sub-Channels $\hat{K}$ and the Victim Position. Figure 6 shows the impact of poisoning, using `BREAK`, an increasing number of OFDM sub-channels $\hat{K}$ on the throughput at the legitimate STA. We consider two different placements for the victim node: positions A and D in Figure 4, i.e., far away and close to the AP. The results indicate that it is sufficient to poison $\hat{K} = 40$ out of the $K = 234$ sub-channels, which is 17% of the feedback values, to attain a 65% decrease in the victim's throughput, for both placements. This suggests that `BREAK` is effective independently of the respective positions of the victim, the adversary, and the AP.

To evaluate whether such degradation is linked with the inability of the legitimate STA to decode the precoded data or to a decrease in the packets transmitted by the AP, we captured all the MU-MIMO frames received at the STA and checked whether the total number of frames (decoded and failed) varies before and after the attack. The corresponding results are shown in Figure 7, where we consider $\hat{K} = 40$ poisoned sub-channels. This plot shows the number of frames that pass and fail the frame check sequence (FCS) check, along with their total number. The attack is initiated after 45 seconds; beyond this point, the number of frames processed at the receiver that fail the FCS check increases, the number of successful frames decreases, whereas their total number remains constant. This demonstrates that, after the `BREAK` attack, the AP continues to operate in MU-MIMO mode at the same packet transmission rate as before. The figure also shows that the attack is highly effective, as about 65% of the frames become undecodable.

To complete the analysis, we computed the packet error rate (PER) – number of frames that do not pass the FCS check over the total number of frames – at the victim STA, by varying the number of poisoned sub-channels and the victim's position. The results, reported in Figure 8, confirm the above discussion showing an increase of the PER starting from $\hat{K} = 40$.

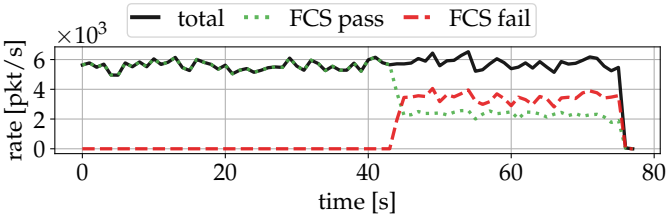

Fig. 7: Total number of MU-MIMO frames received by victim STA A ('total') versus the number of correct ('FCS pass') and incorrect ('FCS no pass') frames, when $\hat{K} = 40$.

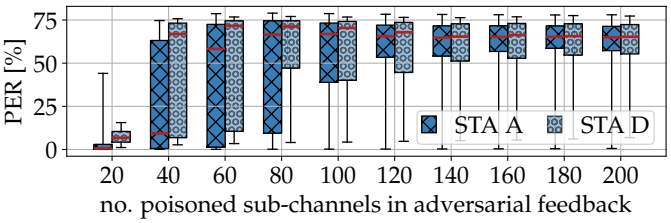

Fig. 8: MU-MIMO PER at the victim when varying the number of poisoned sub-channels $\hat{K}$.

Note that BREAK also decreases the malicious node's throughput, as the attack increases the interference among the legitimate STAs and the adversary. However, we recall that the adversary's objective is solely to break the precoding mechanism, irrespective of its receiving performance. The same reasoning has been adopted to design other attacks, such as MUSTER [3]. Moreover, we believe that by using more antennas or modifying its decoding process, the adversary would be able to retrieve its streams. This intuition is supported by the results we obtained capturing the MU-MIMO traffic directed to the adversary through a four-antenna sniffer. We noticed that the large majority of MU-MIMO frames passed the FCS check performed by such device, meaning that they are decodable.

Insights on the BREAK Malicious Feedback Crafting. In Figure 9, we plot (on the left) an example of the absolute value of the victim feedback matrix ($\tilde{\mathbf{V}}_{\gamma,\text{all},\ell}$) – reconstructed by the adversary from the quantized beamforming angles – along with the uncorrupted adversary feedback matrix ($\tilde{\mathbf{V}}_{\gamma,\text{all},a}$) and the adversarial feedback obtained using BREAK ($\tilde{\mathbf{V}}^{\text{BREAK}}_{\gamma,\text{all},a}$) with $\hat{K}=40$ (the minimum $\hat{K}$ that leads to a 65% reduction in the victim's throughput, see Figure 6). The plot refers to the first transmitter antenna, i.e., the first row of the aforementioned matrices. On the right plot, we also depict the cumulative number of poisoned sub-channels of the adversary feedback. The figure shows that the feedback matrix obtained by BREAK (the orange curve) for the poisoned sub-channels, tends to approach the victim's beamforming feedback matrix (the blue curve), which is the unconstrained solution to Eq. (9). The small differences between these two are required to ensure that the BREAK optimization problem constraints are satisfied, i.e., that the maximum transmission power is not exceeded.

Impact of BREAK on the AP MU-MIMO Rate Controller. In Figure 10, we show the MCS distribution obtained by analyzing the MCS of the frames received at the victim. We account for all MU-MIMO frames, i.e., with both FCS pass and fail ('total' in Figure 7). The results show that the MU-

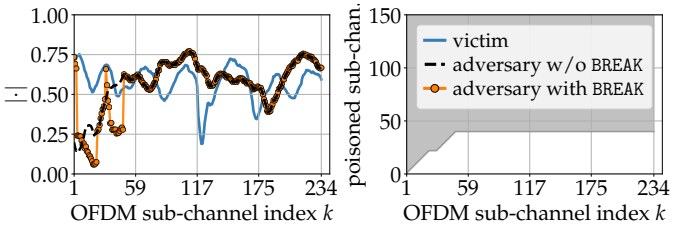

Fig. 9: Example of the feedback matrices (absolute value) of the victim and the adversary without and with BREAK, for the first transmitter antennas, with $\hat{K} = 40$. The cumulative number of poisoned sub-channels is shown on the right plot.

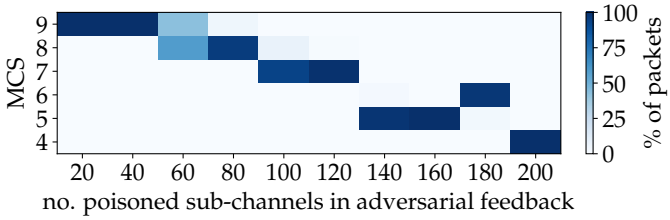

Fig. 10: MCS distribution at the victim (STA A).

MIMO rate controller at the AP reduces the MCS, i.e., reduces the rate, based on the failures (see Figure 8). This allows maintaining an almost constant throughput of about 25 Mb/s when increasing the number of poisoned sub-channels as shown in Figure 6. However, more resilient modulation and coding schemes at low rates (low MCS) are insufficient to compensate for the degradation caused by BREAK.

B. Four-STA Evaluation

We evaluated the attack on a multi-STA scenario considering a 4-STA network with three legitimate STAs (positions A, B, C in Figure 4) and a malicious node. To assess the impact of the initialization of the optimization algorithm (lines 7-8 of Algorithm 1), we carried out three different experimental campaigns featuring six experiments each. For each campaign, we used the feedback matrix $\tilde{\mathbf{V}}_{\gamma,k,\ell}$ of a different STA for the initialization (line 8 of Algorithm 1). The results are reported in Figure 11. Each row of plots refers to one of the three experimental campaigns. The different plots in each row show the throughput at each of the legitimate STAs. Overall, the throughput decrease is smaller than in the two-STA case, as the impact of the malicious feedback is reduced. Specifically, the AP receives three legitimate feedback and one malicious feedback ($1/4$ malicious) while in the two-STA case the AP receives one legitimate and one malicious feedback ($1/2$ malicious). Interestingly, the reduction in the throughput is higher for the STA that is considered for the initialization of the optimization algorithm (plots in the diagonal of Figure 11). This is especially true for STAs A and B, highlighted in green in Figure 11, and suggests that the adversary action can be targeted to a specific victim by selecting its feedback for initializing the optimization. The attack is less effective on STA C (see the plot highlighted in orange in Figure 11) with respect to the other STAs (plots highlighted in green). This is because such STA is close to the adversary and changing the feedback at the adversary does not substantially increase the interference with respect to the situation before the attack.

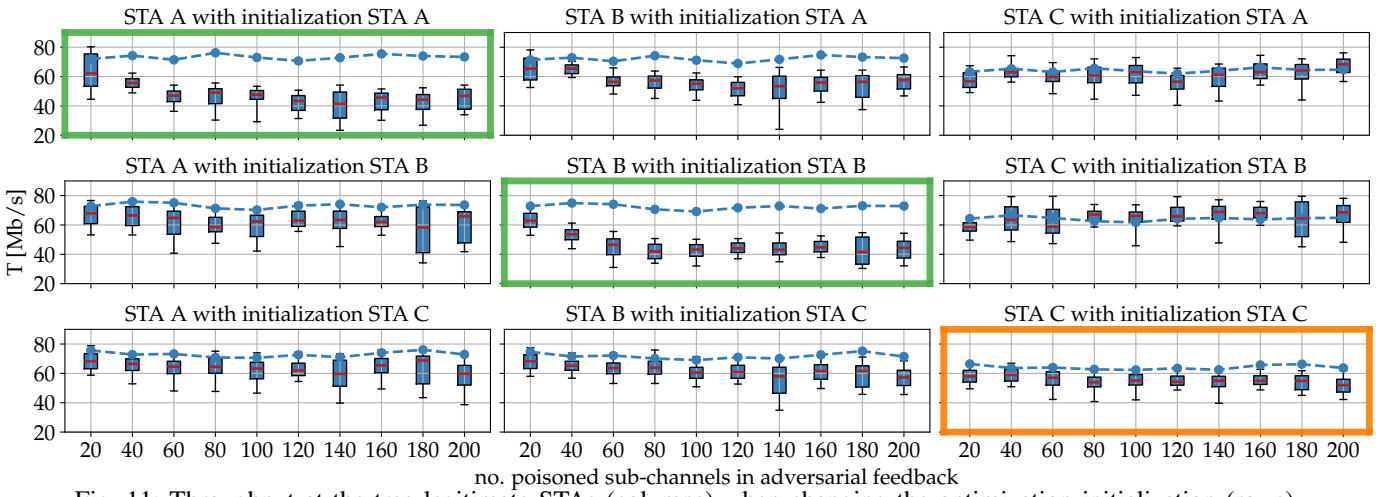

Fig. 11: Throughput at the tree legitimate STAs (columns) when changing the optimization initialization (rows).

C. Evaluation with a Smartphone

In this evaluation, we tested the efficacy of BREAK in decreasing the throughput at a Samsung A52S smartphone (P in Figure 4). The BREAK adversary (implemented on the Asus RT-AC86U) captures the smartphone beamforming feedback angles and obtains the malicious beamforming feedback by poisoning $\hat{K} = 40$ OFDM sub-channels of its feedback. Figure 12 shows a screen capture of the smartphone showing the `iperf` session running on the device. The decrease in throughput is clearly visible when the attack starts at 59 seconds from the beginning. Specifically, the throughput is about 70 MB/s before the attack and drops to about 20 MB/s after the attack. To better visualize the results, we plot the time evolution of the throughput at the smartphone in Figure 13, where the red bar indicates the starting point of the attack. This further confirms that BREAK is highly effective in decreasing the throughput of STAs involved in MU-MIMO transmissions.

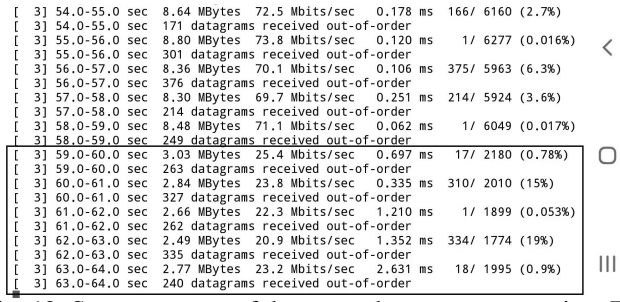

Fig. 12: Screen capture of the smartphone `iperf` session. The throughput decrease is visible during the attack (black box).

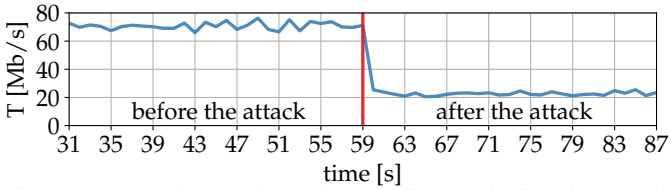

Fig. 13: Smartphone's throughput before and after the attack.

VIII. Conclusions and Summary of Impact

In this paper, we have designed and implemented BREAK, a novel attack vector toward MU-MIMO transmissions that degrades network performance. BREAK only relies on the *beamforming feedback angles* of the devices in the network that represent the only information available to the adversary to compute malicious feedback. This information is promptly retrieved from the feedback packets transmitted *without encryption* by the STAs to the AP as part of the IEEE 802.11 channel sounding procedure. In turn, BREAK does not require any physical access to the victim's node or the AP. We have implemented and tested BREAK on commercial devices and conducted an extensive experimental campaign. The results indicate that the victim's throughput may be decreased by 65% with only a limited feedback modification (17%).

We believe this paper has broken new ground in the field of wireless security and may open several additional lines of research. Among others, an intriguing direction could be to explore how STAs can obfuscate their feedback to decrease the adversary's ability to perform the attack while avoiding a substantial performance decrease. **We hope that this paper will stimulate follow-up discussions in both the Wi-Fi research and standardization communities and lead to more secure procedures for MU-MIMO networking.** The authors have provided public access to their code and data at https://github.com/francescamen/BREAK_INFOCOM2025.

Acknowledgments

This work was supported by the European Union - Next Generation EU under the Italian National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.3, CUP C93C22005250001 and E63C22002070006, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART"), CUP D33C22001300002, partnership on "SEcurity and RIghts In the CyberSpace" (PE00000014 - program "SERICS"), and Investment 1.2, CUP C93C24004880002, project "CAMELIA"; by the EU project Robust-6G "Smart, Automated and Reliable Security Service Platform for 6G" (Grant no. 101139068); by the National Science Foundation (NSF) grant CNS-2134973, ECCS-2229472, ECCS-2329013; by the Air Force Office of Scientific Research under contract number FA9550-23-1-0261; and by the Office of Naval Research under award number N00014-23-1-2221.

REFERENCES

[1] A. Goldsmith, *Wireless Communications*. Cambridge Univ. Press, 2005.

[2] Y.-C. Tung, S. Han, D. Chen, and K. G. Shin, "Vulnerability and Protection of Channel State Information in Multiuser MIMO Networks," in *Proc. of ACM SIGSAC Conference on Computer and Communications Security*, (New York, NY, USA), 2014.

[3] T. Hou, S. Bi, T. Wang, Z. Lu, Y. Liu, S. Misra, and Y. Sagduyu, "MUSTER: Subverting user selection in MU-MIMO networks," in *Proc. of IEEE INFOCOM*, (London, UK), 2022.

[4] H. Pirzadeh, S. M. Razavizadeh, and E. Björnson, "Subverting massive MIMO by smart jamming," *IEEE Wireless Communications Letters*, vol. 5, no. 1, pp. 20–23, 2015.

[5] Z. Shen, K. Xu, and X. Xia, "Beam-domain anti-jamming transmission for downlink massive MIMO systems: A Stackelberg game perspective," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2727–2742, 2021.

[6] G. Patwardhan and D. Thuente, "Jamming beamforming: A new attack vector in jamming IEEE 802.11 ac networks," in *2014 IEEE Military Communications Conference*, pp. 1534–1541, IEEE, 2014.

[7] D. S. Berger, F. Gringoli, N. Facchi, I. Martinovic, and J. B. Schmitt, "Friendly jamming on access points: Analysis and real-world measurements," *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 6189–6202, 2016.

[8] Z. Zhang, Y. Sun, A. Sabharwal, and Z. Chen, "Impact of channel state misreporting on multi-user massive MIMO scheduling performance," in *Proc. of IEEE INFOCOM*, (Honolulu, HI, USA), 2018.

[9] X. Wang, Y. Liu, X. Lu, S. Lv, Z. Shi, and L. Sun, "On eavesdropping attacks and countermeasures for MU-MIMO systems," in *Proc. of IEEE MILCOM*, (Baltimore, MD, USA), 2017.

[10] S. Wang, Z. Chen, Y. Xu, Q. Yan, C. Xu, and X. Wang, "On user selective eavesdropping attacks in MU-MIMO: CSI forgery and countermeasure," in *Proc. of IEEE INFOCOM*, (Paris, France), 2019.

[11] Y. Yang, Y. Chen, W. Wang, and G. Yang, "Securing channel state information in multiuser MIMO with limited feedback," *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3091–3103, 2020.

[12] 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 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz," *IEEE Std 802.11ac-2013 (Amendment to IEEE Std 802.11-2012)*, 2013.

[13] 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.

[14] 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.

[15] C. Peel, B. Hochwald, and A. Swindlehurst, "A vector-perturbation technique for near-capacity multiantenna multiuser communication-part I: channel inversion and regularization," *IEEE Transactions on Communications*, vol. 53, no. 1, pp. 195–202, 2005.

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

[17] K. Ramezanpour, J. Jagannath, and A. Jagannath, "Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective," *Computer Networks*, vol. 221, p. 109515, 2023.

[18] D. Palomar, J. Cioffi, and M. Lagunas, "Joint Tx-Rx beamforming design for multicarrier MIMO channels: a unified framework for convex optimization," *IEEE Transactions on Signal Processing*, vol. 51, no. 9, pp. 2381–2401, 2003.

[19] H. Sampath, P. Stoica, and A. Paulraj, "Generalized linear precoder and decoder design for MIMO channels using the weighted MMSE criterion," *IEEE Transactions on Communications*, vol. 49, no. 12, pp. 2198–2206, 2001.

[20] F. Meneghello, F. Restuccia, and M. Rossi, "WHACK: Adversarial Beamforming in MU-MIMO Through Compressed Feedback Poisoning," *IEEE Transactions on Wireless Communications*, vol. 23, no. 11, pp. 17252–17265, 2024.

[21] M. S. Gast, *802.11 ac: a survival guide: Wi-Fi at gigabit and beyond*. "O'Reilly Media, Inc.", 2013.

[22] Wi-Fi Alliance, "Value of Wi-Fi." https://www.wi-fi.org/discover-wi-fi/value-of-wi-fi, 2024.

[23] M. B. Mashhadi, Q. Yang, and D. Gündüz, "Distributed deep convolutional compression for massive MIMO CSI feedback," *IEEE Transactions on Wireless Communications*, vol. 20, no. 4, pp. 2621–2633, 2020.

[24] N. Bahadori, Y. Matsubara, M. Levorato, and F. Restuccia, "SplitBeam: Effective and Efficient Beamforming in Wi-Fi Networks Through Split Computing," in *2023 IEEE 43rd International Conference on Distributed Computing Systems (ICDCS)*, pp. 864–874, IEEE, 2023.

[25] M. Schulz, D. Wegemer, and M. Hollick, "Nexmon: The C-based Firmware Patching Framework," 2017.

[26] M. Schulz, D. Wegemer, and M. Hollick, "The Nexmon firmware analysis and modification framework: Empowering researchers to enhance Wi-Fi devices," *Computer Communications*, vol. 129, pp. 269–285, 2018.