WHACK: Adversarial Beamforming in MU-MIMO Through Compressed Feedback Poisoning

Francesca Meneghello, *Member, IEEE*, Francesco Restuccia, *Senior Member, IEEE*, and Michele Rossi, *Senior Member, IEEE*

***Abstract*—Multi-user MIMO is a key component of modern wireless networks. As such, investigating the related security weaknesses is a compelling necessity. A major issue unveiled by existing work is that adversaries can "poison" the channel information feedback reported to the beamformer to decrease the performance experienced by a legitimate user. Prior work, however, assumes that the feedback is reported in an uncompressed fashion, which is not the case in current wireless standards such as Wi-Fi or 5G. In this work, we first show that assuming uncompressed feedback leads to overestimating the attack effectiveness by up to 60%. Next, we formulate ACFP (*Adversarial Compressed Feedback Problem*), a novel non-convex constrained optimization problem to find the *compressed feedback* that maximizes a victim's bit error rate (BER) while satisfying maximum power constraints. We propose WHACK (*Wireless Harmful Adversarial Compressed feedbacK*), a new algorithm to solve ACFP and find the malicious compressed feedback based on the convexity of the objective function and constraint using a nonlinear conjugate gradient method. WHACK has been prototyped and extensively evaluated with off-the-shelf Wi-Fi devices. Experimental results show that it maximizes the victim's BER, while modifying less than 60% of the feedback. Our dataset and code will be released for reproducibility purposes.**

***Index Terms*—Adversarial attack, beamforming feedback poisoning, MU-MIMO, digital precoding, IEEE 802.11ac/ax**

I. Introduction

Multi-user multi-input multi-output (MU-MIMO) is a key cornerstone of recent and future wireless networks. In short, MU-MIMO allows a device (beamformer) to simultaneously transmit different data streams to the connected beamformees, thus increasing data rate without increasing the bandwidth [1].

To avoid interference among the data streams, MU-MIMO systems require knowledge of the channel frequency response (CFR) between the beamformer and each beamformee. In current systems, the CFR is estimated by the beamformees and immediately fed back to the beamformer, which properly precodes the data streams making them distinguishable at the different receivers. As shown in Figure 1, this key aspect makes MU-MIMO vulnerable to attacks where *an adversary eavesdrops the information and uses it to create malicious feedback that compromises the precoding at the beamformer*. Existing work – discussed in detail in Section II – has shown that in this way, an adversary can successfully eavesdrop (with up to 99% of success rate) a node's transmission [2]–[4], grant itself a higher share (up to 20%) of network resources [5], or remove a node from the transmission [6].

Francesca Meneghello and Michele Rossi are with the Department of Information Engineering, University of Padova, Italy. Michele Rossi is also with the Department of Mathematics "Tullio Levi-Civita", University of Padova, Italy. Francesco Restuccia is with the Institute for the Wireless Internet of Things, Northeastern University, United States. e-mail: *francesca.meneghello.1@unipd.it*, *michele.rossi@unipd.it*, *frestuc@northeastern.edu*

However, previous work assumes that the adversary has complete and perfect knowledge of the CFR related to the beamformer-victim link. This is not true for currently adopted wireless standards such as IEEE 802.11 (commercially known as Wi-Fi). To reduce the feedback airtime overhead, the CFR is fed back in a *compressed* form – hereafter referred to as *compressed feedback* (see Section III) [7]. In turn, the adversary cannot gain access to the complete CFR, making the assumption made by previous work not applicable to practical scenarios. Moreover, in Section II it is shown that considering the compressed feedback makes the related optimal adversarial action inherently different from attacking the uncompressed CFR, since the adversary achieves up to 60% less BER in the same setup. *This critical aspect motivates a new study considering compressed feedback in the attack design.*

To this end, in this article, we design, prototype, and evaluate WHACK (*Wireless Harmful Adversarial Compressed feedbacK*), the first MU-MIMO beamforming attack specifically tailored for attacks on the compressed feedback. As shown in Figure 1, the adversary leverages the knowledge of the victim's compressed feedback (step 1) to generate a malicious compressed feedback (step 2) that alters the precoding (step 3). This leads the victim to experience 0.5 BER, meaning that the signal cannot be decoded (step 4).

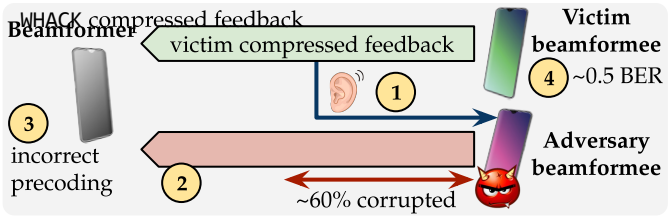

Fig. 1: WHACK overview. The adversary modifies about 60% of its feedback to make victim's data undecodable (0.5 BER).

This challenging objective has been reached through (i) the definition of a new optimization problem, called *Adversarial Compressed Feedback Problem* (ACFP), specifically targeting MU-MIMO systems using compressed feedback; and (ii) the development of a new strategy that effectively and efficiently solves ACFP to craft WHACK malicious compressed feedback. Regarding point (i), we formulated ACFP through a comprehensive mathematical derivation that accounts for the *complete* MU-MIMO processing. As for point (ii), we carried out an in-depth analysis of the ACFP problem, characterizing the convexity of the problem's objective function and constraint, and designing an iterative algorithm that approaches the optimal solution. WHACK attack strategy considers that the adversary may *partially modify* its compressed feedback to reach its objective, which has never been considered by previous work.

WHACK has been validated via an extensive experimental data collection through commercial IEEE 802.11ac devices, showing that the adversarial feedback makes the signal unintelligible with a modification of less than 60% of the original feedback.

Summary of Novel Contributions

- We propose WHACK, a new attack strategy against MU-MIMO that increases the BER of one or more victims by eavesdropping the victims' *compressed feedback* and crafting an adversarial feedback that makes the precoding incorrect. To this end, we mathematically formulate and solve ACFP, a non-convex and constrained optimization problem.
- We derived the WHACK adversarial compressed feedback by designing a custom-tailored nonlinear conjugate gradient-based solver that leverages the convexity of the problem's objective function and constraint.
- We prove that an adversary can effectively inflict damage to a victim even through a *partial perturbation of the feedback* (around 60%). This allows achieving *much better stealthiness* than previously proposed attacks that require a modification of the entire feedback. WHACK allows for an efficient and automated search of the portion of the feedback to be poisoned by directly integrating this into the solver routine.
- We assessed the WHACK performance by collecting real channel data from IEEE 802.11ac transmissions. Experimental results show that WHACK can maximize the BER of the victims while modifying only 60% of the sub-channels. **We will share our dataset and code with the community for replicability**.

Overall, we hope that our work will inform current standardization efforts in IEEE 802.11 and 3GPP on MU-MIMO security. Specifically, we focus on the vulnerability of the MU-MIMO technique that is *currently* implemented on commercially available devices to shed light on a serious security weakness affecting wireless networks ubiquitously deployed nowadays, that must be solved in upcoming standards. Recent work has proposed to replace the beamforming feedback procedure with machine learning (ML)-based approaches [8]–[11]. However, these strategies are only being investigated for possible inclusion in next-generation wireless standards – they are not implemented in current Wi-Fi or 5G networks. Moreover, ML-based techniques are also prone to adversarial attacks that degrade the CFR feedback quality [12].

II. Background and Related Work

The vulnerabilities of the current MU-MIMO beamforming feedback process have been only partially investigated. *Sniffing attacks* have been proposed [2]–[5], where the adversary gains knowledge of the data transmitted to a victim by constructing a forged feedback based on the victim's feedback. Other attacks aim at unfairly prioritizing the adversary in the transmission process. For example, in [5] the authors propose a *power attack* where the adversary pretends to have a worse channel than its actual one by underreporting the CFR, thus forcing the beamformer to increase the power of those streams that are directed to the adversary. Similarly, in [13] the CFR is underreported to change which users are considered in the same transmission block (a process also known as *grouping*), leading to performance degradation for legitimate users. These attacks do not target a specific victim and, in turn, do not leverage the knowledge of other users' CFR.

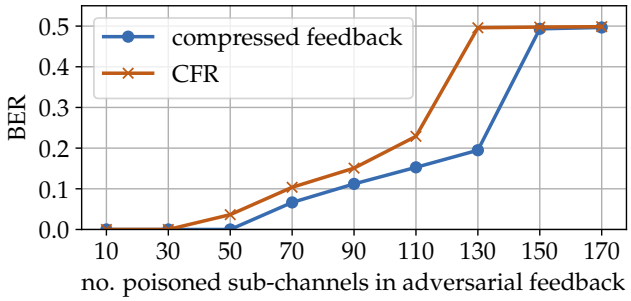

Fig. 2: WHACK BER at the victim when using the compressed feedback or the CFR.

Differently from the contributions in [2]–[5], [13] WHACK objective is to reduce the communication performance of a specific victim in the network, regardless of the goodness of the adversary link. In this view, the contribution in the literature that is most related to WHACK is MUSTER [6], where the authors propose a denial of service attack against a node, which aims at removing the victim from the group of users scheduled for the transmission. To achieve this, the malicious user designs its reported CFR based on the legitimate users' CFR. The idea is to *align the malicious feedback to the victim's feedback* and slightly modify it to reduce interference with the other users. Due to the strong inter-user interference between the victim and the adversary, the beamformer will select only one of the two for transmission. By appropriately constructing the feedback (minimizing the interference with other users), the adversary has a higher chance of being selected. Based on this attack, other two attacks were proposed where the first increases the transmission chances of a target (malicious) user, while the second decreases the throughput for legitimate users.

The key issue in MUSTER is that grouping algorithms are implementation-dependent and thus the related attacks cannot be generalized to arbitrary MU-MIMO networks. On the contrary, in this work, we design an attack operating at the *physical layer* by targeting the precoding procedure that is *univocally defined in the wireless standards*. Moreover, differently from attacks in [6], [13] that completely remove the victim from the transmission round, we propose an approach to control the level of damage inflicted on the victim's receiver by partially modifying the adversary's feedback.

Additionally, a common critical issue of existing work is to disregard that the CFR feedback is usually sent back in a *compressed form*, as discussed in Section III. This approach leads to overestimating the attack effectiveness: In Figure 2 we show that using the CFR led to underestimating the number of orthogonal frequency-division multiplexing (OFDM) sub-channels of the feedback that the adversary should modify to shape the malicious data. As an example, to reach a BER of 0.2, the adversary should poison the compressed feedback of 130 sub-channels while the CFR-based approach wrongly estimates that the perturbation of less than 110 sub-channels is sufficient. Following this analysis, here – in sharp contrast to existing work – we analyze the case where the feedback is

compressed, which is the actual case in real-world systems.

To conclude, we mention that while jamming attacks can be effectively used in single-stream transmissions, jamming MU-MIMO communication is highly complicated as it would require the jammer to be synchronized with the beamformer [14]. On the contrary, WHACK does not require any synchronization with other devices in the network.

III. System Model for MU-MIMO communications

We consider modern wireless local area networks (WLANs) operating with OFDM and MU-MIMO support, e.g., Wi-Fi [7]. We assume that the adversary device is able to operate in MU-MIMO mode and is wirelessly connected to the same network of the victim devices. This holds true for Wi-Fi networks deployed in public places. In case this is not verified, a preliminary attack can be inferred by the adversary to gain access to the network [15]. Note that we consider fully digital MU-MIMO as supported by current Wi-Fi-5G systems to increase the channel capacity, by multiplexing several data streams to different users, and improve the robustness to fading, by combining the data streams at the different antennas. This work does not consider analog or hybrid beamforming strategies for signal directionality.

Henceforth, we denote by K the number of OFDM sub-channels, by M the number of transmit antennas (at the *beamformer*), N_i represents the number of receiver antennas at user (*beamformee*) i, $N_{\text{ss},i}$ refers to the number of spatial streams directed to beamformee i, and $N = \sum_i N_i$ and $N_{\text{ss}} = \sum_i N_{\text{ss},i}$ are the total number of receiver antennas and spatial streams, respectively, summed over all the beamformees. Moreover, we refer to $\mathbf{x}_k$ as the $N_{\text{ss}} \times 1$-dimensional vector encoding the k-th element of the Fourier transform of the transmitted signal for all the spatial streams. We indicate with $\mathbf{H}_{k,i}$ the $N_i \times M$-dimensional matrix collecting the CFR of the k-th OFDM sub-channel for the i-th beamformee. The main symbols used within the paper are summarized in Table I. We use $[\mathbf{C}]_{j,\ell}$ to indicate the element at row j and column ℓ of matrix $\mathbf{C}$.

k	OFDM sub-channel index, $k \in \mathcal{K}$ with $\mathcal{K} = \{0, \dots, K-1\}$
M	no. transmitter antennas (at the beamformer)
N_i	no. receiver antennas at beamformee i, $N = \sum_i N_i$
$N_{\text{ss},i}$	no. streams directed to beamformee i, $N_{\text{ss}} = \sum_i N_{\text{ss},i}$
γ	sub-script for quantities estimated on the sounding packet
$\mathbf{H}_{k,i}$	$N_i \times M$-dimensional CFR matrix
$\tilde{\mathbf{V}}_{\gamma,k,i}$	$M \times N_{\text{ss},i}$-dimensional beamforming feedback of user i
$\tilde{\mathbf{V}}_{\gamma,k}$	$M \times N_{\text{ss}}$-dimensional, obtained concatenating $\tilde{\mathbf{V}}_{\gamma,k,i}$ $\forall i$
$\mathbf{W}_k$	$M \times N_{\text{ss}}$-dimensional precoding matrix
$\mathbf{G}_{k,i}$	$N_{\text{ss},i} \times N_i$-dimensional interference cancellation matrix

TABLE I: Summary of the symbols used in the paper.

To instantiate a MU-MIMO transmission, the beamformer obtains an $M \times N_{\text{ss}}$-dimensional *precoding matrix* $\mathbf{W}_k$ based on the knowledge of the CFR $\mathbf{H}_{k,i}$, $\forall i$. This $\mathbf{W}_k$ matrix is used to differently weigh the signals transmitted through the available antennas to compensate for the radio channel and allow for properly decoding data at each receiver.

The operations needed to obtain the precoding matrix $\mathbf{W}_k$ are illustrated in Figure 3 and are hereafter explained. At first, the CFR $\mathbf{H}_{\gamma,k,i}$ is estimated at each beamformee i using a

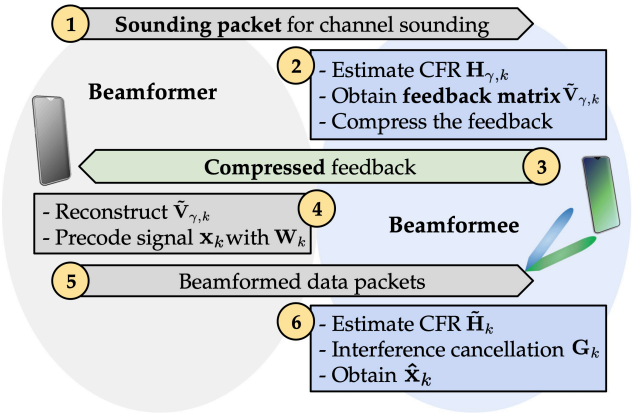

Fig. 3: Beamforming in MU-MIMO WLANs.

sounding packet, which is transmitted by the beamformer to the beamformees using an omnidirectional transmission for the specific purpose of channel estimation (**steps 1-2** in Figure 3). Note that, we will use the sub-script γ to indicate the CFR that is estimated through the sounding packet and used at the beamformer for the computation of the precoding matrix $\mathbf{W}_k$. The CFR estimated at the beamformees on data packets and used to decode data is without γ. We adopt the same notation for the matrices respectively derived from $\mathbf{H}_{\gamma,k,i}$ and $\mathbf{H}_{k,i}$.

Related work in the literature presented in Section II assume that this (uncompressed) matrix $\mathbf{H}_{\gamma,k,i}$ is fed back to the beamformer. However, to save spectrum resources, each beamformee sends the estimated CFR $\mathbf{H}_{\gamma,k,i}$ back to the beamformer in a compressed form (**steps 2-3** in Figure 3). Specifically, for singular value decomposition (SVD) beamforming, the CFR matrix estimated at beamformee i, $\mathbf{H}_{\gamma,k,i}$, is decomposed via SVD as

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

where $\dagger$ indicates the complex conjugate transpose operation, $\mathbf{S}_{\gamma,k,i}$ 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. It follows that $\mathbf{Z}_{\gamma,k,i}$ is an orthonormal basis of $\mathbb{R}^M$ and each of its (M-dimensional) columns can be used to weight the signal associated with a specific stream – thus obtaining orthogonal streams. The first $N_{\text{ss},i} \leq \min\{N_i, M\}$ columns of $\mathbf{Z}_{\gamma,k,i}$ are referred to as the *compressed feedback* $\tilde{\mathbf{V}}_{\gamma,k,i}$. Before transmission, $\tilde{\mathbf{V}}_{\gamma,k,i}$ is further compressed and quantized to reduce airtime overhead.

At the beamformer, the $M \times N_{\text{ss},i}$ $\tilde{\mathbf{V}}_{\gamma,k,i}$ matrices, obtained by all the beamformees, are concatenated to obtain an $M \times N_{\text{ss}}$ $\tilde{\mathbf{V}}_{\gamma,k}$ matrix. This latter matrix is utilized to obtain $\mathbf{W}_k$ (**step 4** in Figure 3, precoding matrix), which is in turn used to send the data packets to the beamformees (**step 5**, beamformed). Using ZF precoding, the precoding matrix is

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

where a regularization term can be added to the $\tilde{\mathbf{V}}^{\dagger}_{\gamma,k} \tilde{\mathbf{V}}_{\gamma,k}$ factor to account for the different signal-to-noise ratio (SNR) of the users (minimum mean-square-error (MMSE) precoding [16]). 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 beamformee i and inter-user interference (IUI) between beamformees.

Being $\mathbf{x}_k$ the transmitted beamformed signal, the signal collected at the N_i antennas of beamformer i is

$$\mathbf{Y}_{k,i} = \sqrt{\boldsymbol{\rho}_i/M}\ \mathbf{H}_{k,i}\mathbf{W}_k\mathbf{x}_k + \mathbf{n}_k, \tag{3}$$

where $\mathbf{n}_k$ is the additive noise, and $\boldsymbol{\rho}_i$ contains the N_i SNR values for user i (note that in the following, for clarity of exposition, we will not include the scaling factors associated with the SNR). Considering Eq. (1), if $\mathbf{H}_{k,i} = \mathbf{H}_{\gamma,k,i}$ (ideal case) only the intended $N_{\mathrm{ss},i}$ streams are collected at beamformee i. However, some residual interference is still present at the receiver due to the time variability of the channel, the channel estimation error and the compression and quantization of matrix $\tilde{\mathbf{V}}_{\gamma,k}$. Thus, for data decoding (**step 6** in Figure 3), each beamformee i estimates the $N_i \times N_{\mathrm{ss}}$-dimensional CFR of the beamformed channel, $\tilde{\mathbf{H}}_{k,i} = \mathbf{H}_{k,i}\mathbf{W}_k$, and applies an *interference cancellation matrix* $\mathbf{G}_{k,i}$ ($N_{\mathrm{ss},i} \times N_i$ dimensional) to retrieve an estimate $\hat{\mathbf{x}}_{k,i}$ of the transmitted signal, $\hat{\mathbf{x}}_{k,i}$, from the signals $\mathbf{Y}_{k,i}$ collected at the N_i antennas. Note that, the beamformed CFR $\tilde{\mathbf{H}}_{k,i}$ is estimated at the receiver for all the spatial streams, also those directed to other beamformees. $\mathbf{G}_{k,i}$ combines the $\mathbf{Y}_{k,i}$ signals to reconstruct the $N_{\mathrm{ss},i}$ spatial streams directed to user i as

$$\hat{\mathbf{x}}_{k,i} = \mathbf{G}_{k,i}\mathbf{Y}_{k,i}, \tag{4}$$

and is obtained as [17],

$$\mathbf{G}_{k,i} = \mathbb{I}_{N_{\mathrm{ss},i}\times N_{\mathrm{ss}}}\mathbf{W}_k^{\dagger}\mathbf{H}_{k,i}^{\dagger}\left(\mathbf{H}_{k,i}\mathbf{W}_k\mathbf{W}_k^{\dagger}\mathbf{H}_{k,i}^{\dagger} + \mathbf{R}_{n,k}\right)^{-1}, \tag{5}$$

where $\mathbf{R}_{n,k}$ is the noise covariance matrix. Ideally, when $\mathbf{R}_{n,k} = 0$ and there is neither inter-stream nor inter-user interference, $\mathbf{G}_{k,i}\mathbf{H}_{k,i}\mathbf{W}_k = \mathbb{I}_{N_{\mathrm{ss},i}\times N_{\mathrm{ss}}}$, and, in turn, $\hat{\mathbf{x}}_{k,i} = \mathbb{I}_{N_{\mathrm{ss},i}\times N_{\mathrm{ss}}}\mathbf{x}_k$, i.e., device i exactly retrieves its $N_{\mathrm{ss},i}$ streams.

IV. Adversarial Compressed Feedback Problem (ACFP) Formulation

The WHACK attack aims at increasing the BER experienced by a *victim beamformee* by modifying the compressed feedback that is fed back by the adversary beamformee to the beamformer. The objective of the adversary beamformee is to make $\mathbf{G}_{k,i}\mathbf{H}_{k,i}\mathbf{W}_k$ at the victim as different as possible from the generalized identity matrix $\mathbb{I}_{N_{\mathrm{ss},i}\times N_{\mathrm{ss}}}$. To this purpose, *the adversary modifies its feedback by leveraging the knowledge of the compressed feedback of the victim device. We recall that the adversary cannot access the complete CFR estimated by the victim beamformee*; it can only reconstruct matrix $\tilde{\mathbf{V}}_{\gamma,k,i}$ from the captured compressed and quantized feedback.

For the following analysis, we define the complex matrix $\tilde{\mathbf{V}}_{\gamma,\mathrm{all},i} = \left[\tilde{\mathbf{V}}_{\gamma,0,i}\ \ \ldots\ \ \tilde{\mathbf{V}}_{\gamma,K-1,i}\right]$ ($K\times M\times N_{\mathrm{ss},i}$ 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 $\mathcal{K} = \{0,\ldots,K-1\}$ representing the set of sub-channels. In what follows, and without loss of generality, we identify the victim with index $i = 1$, the adversary with index $i = \mathrm{a}$ and all other beamformees in the network with index $i = \ell$. From a mathematical standpoint, the adversary maximizes the BER experienced by the victim by maximizing the mean-square-error (MSE) between the transmitted symbol $\mathbf{x}_{k,1}$ (from beamformer to the victim) and the symbol decoded by the victim, $\hat{\mathbf{x}}_{k,1}$, that is,

General Problem Definition

$$\max_{\tilde{\mathbf{V}}_{\gamma,\mathrm{all,a}}} \sum_{k\in\mathcal{K}} \mathrm{MSE}\left(\hat{\mathbf{x}}_{k,1}, \mathbf{x}_{k,1}\right) \quad \text{subject to } P \le P_{\max} \tag{6}$$

where $P = \sum_{k\in\mathcal{K}} P_k$ with $P_k = \mathrm{Tr}\left[\left(\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\right)^{-1}\right]$ (see Appendix A for the formulation) represents the transmit power (at the beamformer) measured in units of energy per OFDM symbol [18] and $P_{\max}$ is its maximum value [19].

Once $\tilde{\mathbf{V}}_{\gamma,k,\mathrm{a}}$ is obtained for $k \in \{0,\ldots,K-1\}$, by solving Eq. (6), the adversary computes the compressed feedback and sends it to the beamformer to trigger the change of the precoding weights and infer the desired damage to the victim. However, the problem in Eq. (6) involves the actual encrypted message that the beamformer transmits to the victim $\mathbf{x}_{k,1}$ and the one decoded by the victim receiver $\hat{\mathbf{x}}_{k,1}$, both of which are not available to the adversary. Hence, Eq. (6) cannot be solved directly by the adversary. To cope with this, we formulate a surrogate problem ACFP, which can be solved by the adversary by solely using the compressed beamforming feedback that can be captured over the air. While ACFP is not mathematically equivalent to the problem in Eq. (6), it represents the best the adversary can do to degrade the victim's performance based on the information it has access to. Hence, the main idea for the following derivation is to rewrite Eq. (6) to identify the contribution of $\tilde{\mathbf{V}}_{\gamma,\mathrm{all,a}}$ to the MSE. The ACFP problem will then target the maximization of this term.

Rewriting the objective function in Eq. (6). Defining $\boldsymbol{\Lambda}_k = \hat{\mathbf{x}}_{k,1} - \mathbf{x}_{k,1}$, the MSE writes as $\mathrm{MSE}\left(\hat{\mathbf{x}}_{k,1}, \mathbf{x}_{k,1}\right) = \mathrm{Tr}\left[\boldsymbol{\Lambda}_k\boldsymbol{\Lambda}_k^{\dagger}\right]$. Using Eq. (3) and Eq. (4) we have $\boldsymbol{\Lambda}_k = \mathbf{G}_{k,1}(\mathbf{H}_{k,1}\mathbf{W}_k\mathbf{x}_k + \mathbf{n}_k) - \mathbb{I}_{N_{\mathrm{ss},1}\times N_{\mathrm{ss}}}\mathbf{x}_k$. Now, using the expression for the interference cancellation matrix in Eq. (5), and applying the Woodbury identity $\mathbf{A}^{\dagger}\left(\mathbf{A}\mathbf{A}^{\dagger}+\mathbb{I}\right)^{-1}\mathbf{A} = \mathbb{I} - \left(\mathbf{A}^{\dagger}\mathbf{A}+\mathbb{I}\right)^{-1}$ ([20]) with $\mathbf{A} = \mathbf{R}_{n,k}^{-1/2}\mathbf{H}_{k,1}\mathbf{W}_k$, we obtain

$$\mathrm{MSE}(\hat{\mathbf{x}}_{k,1}, \mathbf{x}_{k,1}) = \mathrm{Tr}\left[\mathbb{I}_{N_{\mathrm{ss},1}\times N_{\mathrm{ss}}}\left(\mathbf{W}_k^{\dagger}\mathbf{H}_{k,1}^{\dagger}\mathbf{R}_{n,k}^{-1}\mathbf{H}_{k,1}\mathbf{W}_k + \mathbb{I}_{N_{\mathrm{ss}}\times N_{\mathrm{ss}}}\right)^{-1}\mathbb{I}_{N_{\mathrm{ss}}\times N_{\mathrm{ss},1}}\right], \tag{7}$$

where we assume that $\mathbb{E}\left[\mathbf{x}_k\mathbf{x}_k^{\dagger}\right] = 1$ and that $\mathbf{x}_k$ and $\mathbf{n}_k$ are statistically independent. To separate the contributions of the victim and the adversary in Eq. (7), we write $\mathbf{W}_k$ as a block matrix $\mathbf{W}_k = \begin{bmatrix}\mathbf{W}_{k,1} & \mathbf{W}_{k,\ell} & \mathbf{W}_{k,\mathrm{a}}\end{bmatrix}$, where $\mathbf{W}_{k,1}$ collects the first $N_{\mathrm{ss},1}$ columns of $\mathbf{W}_k$ and $\mathbf{W}_{k,\ell}$ and $\mathbf{W}_{k,\mathrm{a}}$ consists of the remaining $(N_{\mathrm{ss}} - N_{\mathrm{ss},1})$ columns (the users can be changed in order without loss of generality for the formulation). Defining $\mathbf{R}_{\mathbf{H}_1} = \mathbf{H}_{k,1}^{\dagger}\mathbf{R}_{n,k}^{-1}\mathbf{H}_{k,1}$, we obtain

$$\mathrm{MSE}(\hat{\mathbf{x}}_{k,1}, \mathbf{x}_{k,1}) = \mathrm{Tr}\left[\mathbb{I}_{N_{\mathrm{ss},1}\times N_{\mathrm{ss}}}\boldsymbol{\Omega}_k^{-1}\mathbb{I}_{N_{\mathrm{ss}}\times N_{\mathrm{ss},1}}\right], \tag{8}$$

where the $\boldsymbol{\Omega}_k$ matrix describes the interference experienced

by the victim device and is expressed as

$$\mathbf{\Omega}_k = \begin{bmatrix} \mathbf{W}_{k,1}^\dagger \mathbf{R}_{\mathbf{H}_1} \mathbf{W}_{k,1} & \mathbf{W}_{k,1}^\dagger \mathbf{R}_{\mathbf{H}_1} \mathbf{W}_{k,\ell} & \mathbf{W}_{k,1}^\dagger \mathbf{R}_{\mathbf{H}_1} \mathbf{W}_{k,\mathrm{a}} \\ \mathbf{W}_{k,\ell}^\dagger \mathbf{R}_{\mathbf{H}_1} \mathbf{W}_{k,1} & \mathbf{W}_{k,\ell}^\dagger \mathbf{R}_{\mathbf{H}_1} \mathbf{W}_{k,\ell} & \mathbf{W}_{k,\ell}^\dagger \mathbf{R}_{\mathbf{H}_1} \mathbf{W}_{k,\mathrm{a}} \\ \mathbf{W}_{k,\mathrm{a}}^\dagger \mathbf{R}_{\mathbf{H}_1} \mathbf{W}_{k,1} & \mathbf{W}_{k,\mathrm{a}}^\dagger \mathbf{R}_{\mathbf{H}_1} \mathbf{W}_{k,\ell} & \mathbf{W}_{k,\mathrm{a}}^\dagger \mathbf{R}_{\mathbf{H}_1} \mathbf{W}_{k,\mathrm{a}} \end{bmatrix}. \tag{9}$$

Ideally, if $\mathbf{H}_{k,1} = \mathbf{H}_{\gamma,k,1}$ and there is no inter-streams nor inter-user interference, we have

$$\mathbf{\Omega}_k = \begin{bmatrix} \mathbb{I}_{N_{\mathrm{ss},1} \times N_{\mathrm{ss},1}} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}, \tag{10}$$

that makes the MSE in Eq. (8) equal to zero (see Appendix B).

Formulation of the ACFP optimization problem. For the sake of understanding, next we consider the case where each receiver has a single antenna, i.e., $N_1 = N_{\mathrm{ss},1} = 1$, $N_{\mathrm{a}} = N_{\mathrm{ss,a}} = 1$, and the beamformer has two transmitting antennas, $M = \sum_i N_{\mathrm{ss},i} = 2$. Interested readers can find the formulation of the ACFP problem for the general case in Appendix B. For the two-beamformees setup, $\mathbf{W}_{k,i}^\dagger \mathbf{R}_{\mathbf{H}_1} \mathbf{W}_{k,j} = \mathbf{w}_{k,i}^\dagger \mathbf{R}_{\mathbf{H}_1} \mathbf{w}_{k,j}$ is a scalar quantity for each $\{i, j\}$, with $\mathbf{w}_{k,i}$ being the 2×1 dimensional precoding vector (i.e., $\mathbf{W}_{k,i}$ when $N_{\mathrm{ss},i} = 1$), and the MSE in Eq. (8) takes the form

$$\mathrm{MSE}\big(\hat{\mathbf{x}}_{k,1}, \mathbf{x}_{k,1}\big) = \left(\det[\mathbf{\Omega}_k]\right)^{-1} \mathbf{w}_{k,\mathrm{a}}^\dagger \mathbf{R}_{\mathbf{H}_1} \mathbf{w}_{k,\mathrm{a}}. \tag{11}$$

We now rewrite the expression in Eq. (11) by decomposing the 1×2 dimensional channel matrix $\mathbf{H}_{k,1}$ in $\mathbf{R}_{\mathbf{H}_1}$ via SVD, as presented in Eq. (1) for $\mathbf{H}_{\gamma,k,i}$. We have $\mathbf{H}_{k,1} = u_{k,1} \mathbf{S}_{k,1} \mathbf{Z}_{k,1}^\dagger$, where $u_{k,1}$ is a complex number with $u_{k,1}^* u_{k,1} = 1$ (the symbol * indicates the complex conjugate operation), $\mathbf{Z}_{k,1}$ is a 2×2 unitary matrix, and $\mathbf{S}_{k,1}$ is a 1×2 vector collecting the singular value $\sigma_{k,1}$ of $\mathbf{H}_{k,1}$, i.e., $\mathbf{S}_{k,1} = \begin{bmatrix} \sigma_{k,1} & 0 \end{bmatrix}$. Adopting the same notation used in Section III, we refer to the first $N_{\mathrm{ss},1} = 1$ column of $\mathbf{Z}_{k,1}$ as $\tilde{\mathbf{v}}_{k,1}$. Hence, the $\mathbf{H}_{k,1}$ decomposition can be rewritten as $\mathbf{H}_{k,1} = u_{k,1} \sigma_{k,1} \tilde{\mathbf{v}}_{k,1}^\dagger$, and Eq. (11) becomes

$$\mathrm{MSE} = \left(\det[\mathbf{\Omega}_k]\right)^{-1} \sigma_{k,1}^* \sigma_{k,1} \mathbf{w}_{k,\mathrm{a}}^\dagger \tilde{\mathbf{v}}_{k,1} \mathbf{R}_{n,k}^{-1} \tilde{\mathbf{v}}_{k,1}^\dagger \mathbf{w}_{k,\mathrm{a}}. \tag{12}$$

The term in Eq. (12) is associated with the inter-user interference caused by the adversary transmissions to the victim's ones, and should approach zero in the ideal case. The objective of the adversary is to skillfully craft $\tilde{\mathbf{v}}_{\gamma,k,\mathrm{a}}$ to make it deviate from zero. 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. Writing $\tilde{\mathbf{V}}_{\gamma,k} = \begin{bmatrix} \tilde{\mathbf{v}}_{\gamma,k,1} & \tilde{\mathbf{v}}_{\gamma,k,\mathrm{a}} \end{bmatrix}$, we obtain

$$\mathbf{w}_{k,\mathrm{a}}^\dagger \tilde{\mathbf{v}}_{k,1} = \frac{-\tilde{\mathbf{v}}_{\gamma,k,\mathrm{a}}^\dagger \tilde{\mathbf{v}}_{\gamma,k,1} \tilde{\mathbf{v}}_{\gamma,k,1}^\dagger \tilde{\mathbf{v}}_{k,1} + \tilde{\mathbf{v}}_{\gamma,k,1}^\dagger \tilde{\mathbf{v}}_{\gamma,k,1} \tilde{\mathbf{v}}_{\gamma,k,\mathrm{a}}^\dagger \tilde{\mathbf{v}}_{k,1}}{\det[\tilde{\mathbf{V}}_{\gamma,k}^\dagger \tilde{\mathbf{V}}_{\gamma,k}]}. \tag{13}$$

Considering Eq. (13), if $\tilde{\mathbf{v}}_{\gamma,k,1} = \tilde{\mathbf{v}}_{k,1}$, the numerator becomes zero (independently of $\tilde{\mathbf{v}}_{\gamma,k,\mathrm{a}}$) and, in turn, $\mathbf{w}_{k,\mathrm{a}}^\dagger \tilde{\mathbf{v}}_{k,1} = 0$ as expected from the way $\mathbf{W}_k$ is designed (see Section III). However, as introduced before, the variability of the wireless channel prevents $\tilde{\mathbf{v}}_{\gamma,k,1} = \tilde{\mathbf{v}}_{k,1}$ to hold, making $\mathbf{w}_{k,\mathrm{a}}^\dagger \tilde{\mathbf{v}}_{k,1}$ slightly differ from zero, i.e., $\mathbf{w}_{k,\mathrm{a}}$ and $\tilde{\mathbf{v}}_{k,1}$ are *nonorthogonal* in practice. WHACK exploits this nonorthogonality to maximize the effectiveness of the attacks, i.e., to maximize $\mathrm{MSE}(\hat{\mathbf{x}}_{k,1}, \mathbf{x}_{k,1})$. Remarkably, the numerator in Eq. (13) cannot be significantly modified by tuning $\tilde{\mathbf{v}}_{\gamma,k,\mathrm{a}}$, as it is proportional to $\tilde{\mathbf{v}}_{\gamma,k,\mathrm{a}}$, but the multiplying factor is very small due to $\tilde{\mathbf{v}}_{\gamma,k,1}$ approaching $\tilde{\mathbf{v}}_{k,1}$. Moreover, only $\tilde{\mathbf{v}}_{\gamma,k,1}$ is accessible when designing $\mathbf{W}_k$, while $\tilde{\mathbf{v}}_{k,1}$ is associated with the transmission event that occurs after the definition of the precoding matrix. Given these observations, our intuition is that $\tilde{\mathbf{v}}_{\gamma,k,\mathrm{a}}$ should instead be modified with the objective of decreasing the absolute value of the denominator in Eq. (13) as much as possible, thus enhancing the non-orthogonality between $\mathbf{w}_{k,\mathrm{a}}$ and $\tilde{\mathbf{v}}_{k,1}$. Following this intuition, we replace the problem in Eq. (6) by the following problem called ACFP (*Adversarial Compressed Feedback Problem*):

ACFP Problem Definition

$$\begin{aligned} &\max_{\tilde{\mathbf{V}}_{\gamma,\mathrm{all,a}}} \sum_{k \in \mathcal{K}} \det\Big[\tilde{\mathbf{V}}_{\gamma,k}^\dagger \tilde{\mathbf{V}}_{\gamma,k}\Big]^{-1} \\ &\text{subject to} \quad \det\Big[\tilde{\mathbf{V}}_{\gamma,k}^\dagger \tilde{\mathbf{V}}_{\gamma,k}\Big] \neq 0, \quad \forall k \\ &\qquad P \leq P_{\max} \end{aligned} \tag{14}$$

The solution to the ACFP problem is hereafter indicated with $\tilde{\mathbf{V}}_{\gamma,\mathrm{all,a}}^{\mathrm{WHACK}}$ and represents the adversarial feedback matrix that the adversary should use to maximize the BER at the victim's receiver. The per-sub-carrier objective function in the ACFP problem is referred to as $F_k = \det\big[\tilde{\mathbf{V}}_{\gamma,k}^\dagger \tilde{\mathbf{V}}_{\gamma,k}\big]^{-1}$, where $\det\big[\tilde{\mathbf{V}}_{\gamma,k}^\dagger \tilde{\mathbf{V}}_{\gamma,k}\big] \in \mathbb{R}_{\geq 0}$ (see Appendix C for a proof). Note that in Eq. (14), the control variables $\tilde{\mathbf{V}}_{\gamma,k,\mathrm{a}}$ for different sub-channels $k \in \mathcal{K}$ are independent. Hence, the maximization problem in Eq. (14) is equivalent to maximizing each term (F_k) separately. Specifically, F_k is linked with the interference caused by the adversary to the victim on sub-channel k that is induced by the wrong precoding. By maximizing F_k, the adversary makes $\mathbf{\Omega}_k$ in Eq. (9) deviate from its ideal interference-free form in Eq. (10), thus increasing the MSE in Eq. (8). *Note that the ACFP 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.*

A. Discussions on the Threat Model

The ACFP problem formulated in Eq. (14) only depends on the beamforming feedback matrices $\tilde{\mathbf{V}}_{\gamma,k,i}$ of the devices in the network. This information is promptly retrieved from the *compressed feedback* transmitted by the beamformees to the beamformer as part of the channel sounding procedure. In turn, WHACK does not require any firmware modification of physical access to the victim device or to the beamformer. Note that the compressed feedback is transmitted by each beamformee *in clear text* to reduce the sounding airtime overhead (see, e.g., [7]), and it is not beamformed, i.e., is transmitted omnidirectionally. In turn, the adversary can obtain the needed information by simply capturing the ongoing Wi-Fi traffic from its wireless interface. This can be done by using any network protocol analyzer, like, e.g., Wireshark or tcpdump, and does not require any firmware modification to the adversary device. We refer the reader to [21] for a detailed description of the beamforming feedback capturing and decoding processes. WHACK only requires a modification

to the adversary device's firmware or driver to integrate the procedure to shape the malicious feedback. Hence, once the malicious feedback is obtained through the tampered procedure detailed in Section V, the information is transmitted to the beamformer through the standard compliant method for beamforming frame construction.

As discussed in Section I-II, we remark that the beamforming feedback is the only information available at the beamformer to compute the precoding matrix as the CFR (uncompressed) is not fed back. Assuming that the adversary knows the uncompressed CFR and using it to design the attack, as done in previous work, is inappropriate as it entails a strategy that can only be implemented by gaining physical access to the victim's device. Second, knowing the full (uncompressed) CFR does not provide any advantages with respect to only knowing the compressed feedback, as the malicious node would need in any case to obtain the compressed feedback to design the attack vector – as formulated in Eq. (14) – given that this is the information that the beamformer uses for precoding.

The effectiveness of the WHACK attack depends on the maximum power that can be emitted from the antenna elements at the beamformer, which is enforced by the second constraint in ACFP (Eq. (14)). From the ACFP problem formulation, it descends that WHACK implements an attack that infers the strongest damage to the victim, while meeting the physical limit on the maximum transmission power.

V. Deriving WHACK Adversarial Feedback

In Appendix C, we prove that $\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}$ is positive semidefinite. This guarantees that the ACFP objective function in Eq. (14) $F_k(\tilde{\mathbf{V}}_{\gamma,k}) = \det\left[\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\right]^{-1} : \mathbb{C}^{M\times N_{\rm ss}} \rightarrow \mathbb{R}_{\geq 0}$ is convex (see Chapter 3 of [22] and Lecture 4 of [23]). In turn, the problem in Eq. (14) corresponds to the maximization of a convex function and its solutions are at the extreme of the feasible set defined by the problem constraints. Importantly, we have that the transmit power constraint $P_k(\tilde{\mathbf{V}}_{\gamma,k}) = \mathrm{Tr}\left[\left(\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\right)^{-1}\right] : \mathbb{C}^{M\times N_{\rm ss}} \rightarrow \mathbb{R}_{\geq 0}$ is also convex when $\tilde{\mathbf{V}}_{\gamma,k} \neq 0$ (this makes $\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}$ being positive definite, see Appendix C), as the inverse of a positive definite matrix is convex and the trace is an affine transformation that maintains convexity [22]. We will leverage this convexity for designing the strategy to solve the ACFP problem in the following.

In Figure 4, we show an example of the values assumed by F_k and P_k when varying the control variable $\tilde{\mathbf{v}}_{\gamma,k,\mathrm{a}}$ for the case we considered in Section IV (single-antenna receivers, $N_{\rm a}=N_{{\rm ss},\mathrm{a}}=1$, and two-antenna transmitter, $M=\sum_i N_{{\rm ss},i}=2$). The plots refer to sub-channel $k=100$ at the first transmit antenna $m=1$ and spatial stream $s_{\rm a}=1$. Note that F_k and P_k go to infinity as $\det\left[\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\right]$ approaches zero that is a singularity point for the two functions. The average power constraint per sub-channel, obtained as $P_{k,\max}=P_{\max}/K$, is represented by the red plane in the right plot.

Main idea for solving Eq. (14) and convergence. Both the objective function and the power constraint are convex functions defined on the same domain ($\det\left[\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\right] \neq 0$) and with the same singularity point ($\det\left[\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\right] = 0$) where

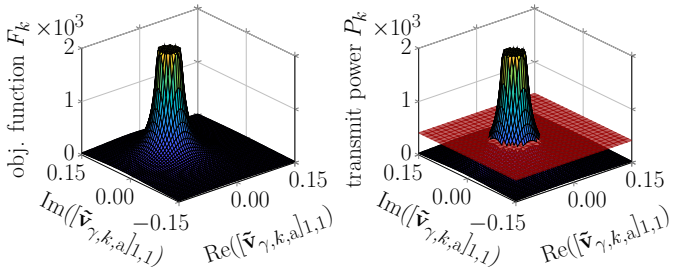

Fig. 4: Objective function F_k (left) and transmit power P_k (right) for k=100 with respect to the real and imaginary parts of the control variable $\tilde{\mathbf{v}}_{\gamma,k,\mathrm{a}}$ for the first transmit antenna $m=1$ and spatial stream $s_{\rm a}=1$ with $M=2$, $N_{\rm a}=N_{{\rm ss},\mathrm{a}}=1$. The red plane on the right plot represents the power constraint.

both functions go to infinity. Hence, considering the right plot in Figure 4, the extremes of the feasible set – i.e., the solutions to the ACFP problem in Eq. (14) – are the points $\tilde{\mathbf{V}}_{\gamma,k,\mathrm{a}}^{\texttt{WHACK}}$ at the intersection between the surface representing the transmit power and the red plane representing the power constraint. In turn, the idea is to start the search for $\tilde{\mathbf{V}}_{\gamma,k,\mathrm{a}}^{\texttt{WHACK}}, \forall k$ from a point close to the objective function's singularity point, i.e., where the surface on the left plot (objective function) in Figure 4 goes to infinity. Next, to reach the extremes of the feasible set, the candidate solution $\tilde{\mathbf{V}}_{\gamma,k,\mathrm{a}}^{\texttt{WHACK}}$ is slowly and iteratively modified to make P_k (represented by the surface on the right plot in Figure 4) approach $P_{\max}$ (the red plane). Specifically, the candidate solution $\tilde{\mathbf{V}}_{\gamma,\mathrm{all},\mathrm{a}}^{\texttt{WHACK}}$ is iteratively updated following the gradient of P_k. If the transmit power associated with the candidate solution $\tilde{\mathbf{V}}_{\gamma,\mathrm{all},\mathrm{a}}^{\texttt{WHACK}}$ violates the power constraint $P_{\max}$, the value of $\tilde{\mathbf{V}}_{\gamma,k,\mathrm{a}}^{\texttt{WHACK}}, \forall k$ is modified in the direction of decreasing the gradient of P_k. If the power constraint is met, we move in the ascending direction of the gradient as, in this case, the value of the objective function $F_k, \forall k$ can be further increased while meeting the transmit power constraint $P < P_{\max}$. *As both the objective function $F_k(\tilde{\mathbf{V}}_{\gamma,k})$ and the power constrain $P_k(\tilde{\mathbf{V}}_{\gamma,k})$ are convex function, this strategy guarantees to approach the set of optimal solutions, i.e., the boundary of the feasible set defined by the transmit power constraint.*

Based on this main idea, we designed a custom search routine that is summarized in Algorithms 1-2 and in Figure 5, and detailed next.

A. WHACK search initialization (Algorithm 1)

The adversary does not necessarily need to modify the complete $\tilde{\mathbf{V}}_{\gamma,\mathrm{all},\mathrm{a}}$ matrix – i.e., for all the OFDM sub-channels $k \in \mathcal{K}$ – to inflict damage to the victim. The modification of a sub-set $\hat{\mathcal{K}}$ of $\hat{K}$ out of K sub-channels suffices to create interference at the victim's receiver through the modification of the precoding at the beamformer. Therefore, the adversary can keep the feedback matrix $\tilde{\mathbf{V}}_{\gamma,k,\mathrm{a}}$ for $k \in \mathcal{K}\backslash\hat{\mathcal{K}}$ unchanged, thus making harder for the beamformer to detect the attack. Here, the challenge is how to select the set of sub-channels to be poisoned. One possibility is to select this set of sub-channels at random. However, this does not represent the best strategy to apply. In the following, we describe the WHACK

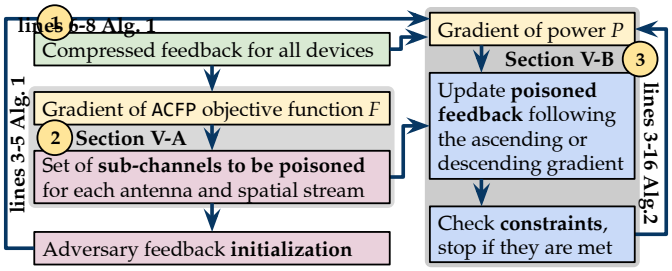

Fig. 5: Procedure for WHACK adversarial feedback crafting.

Algorithm 1 Selection of the OFDM sub-channels to be poisoned and initialization of the search matrix

1: **Input:** number of sub-channels to be poisoned $\hat{K}$
2: **Output:** search initialization matrix $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,\text{all,a}}$ and set of OFDM sub-channels to be poisoned $\hat{\mathcal{K}}_{m,s_\text{a}}$ for Algorithm 2
3: Obtain $F_k = \det\left[\tilde{\mathbf{V}}^{\dagger}_{\gamma,k}\tilde{\mathbf{V}}_{\gamma,k}\right]^{-1}$ and its gradient ∇F_k with respect to the $M \times N_{\text{ss,a}}$ elements of the control variable $\tilde{\mathbf{V}}_{\gamma,k,\text{a}}$, $\forall k$
4: **for all** $m \in \{0,\ldots,M-1\}$ transmit antennas, $s_\text{a} \in \{0,\ldots,N_{\text{ss,a}}-1\}$ adversary streams **do**
5: Select set $\hat{\mathcal{K}}_{m,s_\text{a}}$ as the $\hat{K}<K$ sub-channels associated with highest $\left[\|\nabla F_k\|\right]_{m,s_\text{a}}$ values, $k\in\{0,\ldots,K-1\}$
6: Define $\boldsymbol{\eta}_k$ as a $\hat{K}$ dimensional matrix which elements follow a Gaussian distribution $\boldsymbol{\eta}_k \sim \mathcal{N}(0,1)$, and $\alpha > 0$
7: Define starting matrix for the WHACK malicious feedback $\left[\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}}\right]_{m,s_\text{a}} \leftarrow \alpha\left[\boldsymbol{\eta}_k\right]_{m,s_\text{a}}$ for $k\in\hat{\mathcal{K}}_{m,s_\text{a}}$
8: $\left[\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}}\right]_{m,s_\text{a}} \leftarrow \left[\tilde{\mathbf{V}}_{\gamma,k,\text{a}}\right]_{m,s_\text{a}}$ for $k\in\mathcal{K}\setminus\hat{\mathcal{K}}_{m,s_\text{a}}$

approach for the poisoned sub-channels selection and detail the initialization point for the search.

Selection of the sub-set of poisoned OFDM sub-channels. In WHACK, the adversary bases the selection on the ACFP objective function in Eq. (14), $F=\sum_{k\in\mathcal{K}}F_k$. We note that the function to be *maximized* is obtained by summing K contributions, one for each of the K sub-channels in $\mathcal{K}$. Hence, the best strategy for the adversary is to change the sub-channels k that contribute the least to this sum. We detail this sub-channels selection procedure in Alg. 1. The adversary first computes the gradient of the objective function $F_k, \forall k$, with respect to $\tilde{\mathbf{V}}_{\gamma,k,\text{a}}$ and evaluates it at the unmodified $\tilde{\mathbf{V}}_{\gamma,k,\text{a}}$ matrix – ∇F_k (line 3 of Alg. 1). Hence, for each of the transmit antennas (rows of $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,\text{all,a}}$) over each of the spatial streams (columns of $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,\text{all,a}}$), the adversary selects the set $\hat{\mathcal{K}}_{m,s_\text{a}}$ of sub-channels to be poisoned as those corresponding to the highest absolute ∇F_k values (lines 4-5 of Alg. 1). The elements of $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,\text{all,a}}$ on sub-channels in set $\hat{\mathcal{K}}_{m,s_\text{a}}$ will be perturbed by the iterative procedure in Alg. 2, while the remaining elements are set to their original values and never modified during the search. We stress that although $\hat{K}$ is fixed (user-defined input parameter), the set $\hat{\mathcal{K}}_{m,s_\text{a}}$ differs for each pair of transmit antenna $m\in\{0,\ldots,M-1\}$ and spatial stream $s_\text{a}\in\{0,\ldots,N_{\text{ss,a}}-1\}$, as each sub-channel can have a different impact on the objective function for different m and s_a.

Initialization of the search. Matrix $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}}$ is initialized in lines 6-8 of Alg. 1 and is performed for each transmit antenna m and each adversary spatial stream s_a (line 4). Following the main idea above, we start the search from a point close to the objective function's singularity point. Specifically, for each of the sub-channels to be poisoned ($k\in\hat{\mathcal{K}}_{m,s_\text{a}}$) the singularity point $\det\left[\tilde{\mathbf{V}}^{\dagger}_{\gamma,k}\tilde{\mathbf{V}}_{\gamma,k}\right]=0$ can be reached by setting $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}}=\mathbf{0}$. As this solution is infeasible, we set the entries of the candidate matrix $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}}$ to arbitrary small random numbers, i.e., $\left[\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}}\right]_{m,s_\text{a}}=\alpha\left[\boldsymbol{\eta}_k\right]_{m,s_\text{a}}$ (line 7), where $\boldsymbol{\eta}_k$ is a vector of normally distributed random complex numbers and α is a non-negative scalar that should be small to generate a matrix that approaches $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}}=\mathbf{0}$ (line 6). The remaining elements of $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}}$ (for $k\in\mathcal{K}\setminus\hat{\mathcal{K}}_{m,s_\text{a}}$) are set to the values of the unperturbed adversary matrix $\tilde{\mathbf{V}}_{\gamma,k,\text{a}}$ (line 8).

Algorithm 2 Modified nonlinear conjugate gradient method for solving ACFP at the adversary and crafting WHACK

1: **Input:** search initialization matrix $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,\text{all,a}}$ and set of OFDM sub-channels to be poisoned $\hat{\mathcal{K}}_{m,s_\text{a}}$ (from Algorithm 1)
2: **Output:** WHACK adversary matrix $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,\text{all,a}}$ ($K\times M\times N_{\text{ss,a}}$) from which the adversarial feedback is obtained
3: Set iter_num $\leftarrow 0$ and $\mu_0 > 0$
4: $\det_k \leftarrow \det\left[\tilde{\mathbf{V}}^{\dagger}_{\gamma,k}\tilde{\mathbf{V}}_{\gamma,k}\right], \forall k\in\mathcal{K}$
5: $P \leftarrow \sum_{k\in\mathcal{K}} P_k$
6: $\Delta\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}} \leftarrow \nabla P_k$, $\forall k\in\hat{\mathcal{K}}_{m,s_\text{a}}$ (gradient of P_k with respect to the $M\times N_{\text{ss,a}}$ elements of the control variable $\tilde{\mathbf{V}}_{\gamma,k,\text{a}}$)
7: **while** ($\exists\, k\in\mathcal{K}$ such that $\det_k == 0$) or ($P \geq P_{\max}$) or ($P \leq \rho_{\min}P_{\max}$) **do**
8: $\boldsymbol{\delta}_k \leftarrow \text{sign}(P_{\max}-P)\Delta\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}} / \sum_{k\in\mathcal{K}}\Delta\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}}$, $k\in\hat{\mathcal{K}}_{m,s_\text{a}}$
9: iter_num $\leftarrow$ iter_num $+1$, $\mu \leftarrow \mu_0/\text{iter\_num}$
10: **for all** $m\in\{0,\ldots,M-1\}$, $s_\text{a}\in\{0,\ldots,N_{\text{ss,a}}-1\}$ **do**
11: $\left[\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}}\right]_{m,s_\text{a}} \leftarrow \left[\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}}\right]_{m,s_\text{a}} + \mu\left[\boldsymbol{\delta}_k\right]_{m,s_\text{a}}$ for $k\in\hat{\mathcal{K}}_{m,s_\text{a}}$
12: Clip Re$\left(\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,\text{all,a}}\right)$ and Im$\left(\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,\text{all,a}}\right)$ to lie in $[-\xi,\xi]$
13: $\det_k \leftarrow \det\left[\tilde{\mathbf{V}}^{\dagger}_{\gamma,k}\tilde{\mathbf{V}}_{\gamma,k}\right]$, $\forall k\in\mathcal{K}$ (using $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,\text{all,a}}$)
14: Update P_k using the new $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,\text{k,a}}$
15: $P \leftarrow \sum_{k\in\mathcal{K}} P_k$
16: $\Delta\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}} \leftarrow \nabla P_k + \boldsymbol{\beta}\Delta\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,\text{all},k}$ $\forall k\in\hat{\mathcal{K}}_{m,s_\text{a}}$

B. WHACK iterative search (Algorithm 2)

As introduced above, the solution to Eq. (14) lies on the boundary of the feasible set defined by the constraints. Hence, the objective of Alg. 2 is to modify the initial candidate solution $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,\text{all,a}}$ so that F_k is maximized and the constraint on the transmit power is meet, while guaranteeing that $\det\left[\tilde{\mathbf{V}}^{\dagger}_{\gamma,k}\tilde{\mathbf{V}}_{\gamma,k}\right]\neq 0, \forall k$. To this end, we designed a customized nonlinear conjugate gradient method [24] where the updates are performed following the direction of the gradient of P computed with respect to $\tilde{\mathbf{V}}_{\gamma,k,\text{a}}$ and evaluated at $\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,k,\text{a}}$ ($\nabla P_k, \forall k$, line 6 of Alg. 2). The updates are repeatedly applied until all constraints are met (line 7, Alg. 2). The perturbation $\boldsymbol{\delta}_k$ is obtained by normalizing the gradient over the OFDM sub-channels dimension (line 8, Alg. 2). The update direction is obtained in line 8 as $\text{sign}(P_{\max}-P)$, i.e., we follow the descending gradient if $P\geq P_{\max}$ while the ascending gradient

direction is followed if $P < \rho_{\min} P_{\max}$. The user-defined $\rho_{\min}$ parameter sets the lower bound that must be surpassed when starting from a solution for which $P < P_{\max}$, while $\mu > 0$ is the step size parameter, which decreases at each iteration of Alg. 2 (line 9). The perturbations are applied for each transmit antenna m at the beamformer and each adversary stream s_{a}, for all the $k \in \hat{\mathcal{K}}_{m,s_{\mathrm{a}}}$ sub-channels to be poisoned (line 10-11 of Alg. 2). Note that the sets $\hat{\mathcal{K}}_{m,s_{\mathrm{a}}}$ remain unchanged for the different iterations in line 7 of Alg. 2, as they are defined based on the unmodified $\tilde{\mathbf{V}}_{\gamma,\mathrm{all,a}}$. We underline that in Alg. 2, P does not have to be minimized nor maximized. We are only concerned with making it close to the power budget $P_{\max}$.

Upon obtaining a new $\tilde{\mathbf{V}}^{\texttt{WHACK}}_{\gamma,\mathrm{all,a}}$ from lines 8-11 of Alg. 2, the elements of $\tilde{\mathbf{V}}^{\texttt{WHACK}}_{\gamma,\mathrm{all,a}}$ are clipped to lie in $[-\xi, \xi]$ (with $\xi > 0$ being a hyperparameter of the algorithm) to avoid deviating from the typical values observed in the experimental evaluations. If $\det_k$ and P computed in lines 13-15 do not meet the constraints, the conjugate gradient is updated by considering the gradient evaluated on the new and the previous $\tilde{\mathbf{V}}^{\texttt{WHACK}}_{\gamma,\mathrm{all,a}}$ matrix (line 16), and the just described procedure is iterated. The weighting coefficient β is computed following the Polak–Ribière formulation [24], [25].

C. Solution timescale and channel variability

The time complexity of the attack depends on Alg. 2 that is $\mathcal{O}(\mathrm{iter\_num} \times \hat{K} \times M \times N_{\mathrm{ss}}^2)$, where $\mathrm{iter\_num}$ is the number of iterations of the loop in line 12. On average, the algorithm converges in about $\mathrm{iter\_num} = 2$ steps (or fewer). Using $K = 256$ (IEEE 802.11ac at 80 MHz), $M = N_{\mathrm{ss}} = 2$, and a CPU frequency of 3 GHz, the execution time is about 1.4 μs with the current implementation. If channel sounding is performed approximately every 10 ms (as recommended in [26]), 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 of 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. In comparison, the computation complexity of an interior point optimization [27] (used in Section VII for comparison) depends on the computation complexity of evaluating F, which is $\mathcal{O}(2 \times \hat{K} \times N_{\mathrm{ss}}^3 + \hat{K} \times M \times N_{\mathrm{ss}}^2)$.

D. WHACK Countermeasures

WHACK, as other adversarial attacks to the beamforming procedure (see Section II), relies on the fact that the beamforming feedback matrix is transmitted unencrypted from the beamformees to the beamformer and the adversary is entirely aware of the algorithm adopted by the beamformer to precode the MU-MIMO streams. These procedures are defined in the wireless standards and adopted by all the devices compliant with them. In the following, we provide some possible countermeasures to WHACK. However, note that implementing countermeasures requires major modifications to the standards: Although future versions may implement effective countermeasures to WHACK, all devices implementing older versions of the standards will still be vulnerable to the attack as the standards should be back-compatible.

Encryption. A possible way to prevent WHACK malicious action is to encrypt the compressed feedback transmitted by the beamformees to the beamformer as presented in, e.g., [2]. This would make the adversary unable to design proper malicious feedback to hamper the performance of a victim device. However, encryption would increase the complexity and latency of the channel sounding procedure. As the sounding should be performed regularly given the variability of the wireless channel, this drawback may make encryption infeasible in practical setups.

Machine learning. Another approach is to entirely substitute the deterministic channel sounding and precoding procedures with a learning-based approach. By leveraging data-driven parameters adapted to the specific setup, it would be more difficult for a malicious device to estimate the effect of corrupting its feedback. This would prevent the adversary from leveraging the precoding process to optimally shape the malicious feedback and in turn, execute the attack. Data-driven channel sounding procedures have been presented in [9], [11].

Detection. A different strategy to mitigate the effect of the attack would be to *detect* if a node is transmitting malicious feedback. This requires implementing some detection algorithms at the beamformer. In the case of time division duplex (TDD) systems, the beamformer can compare the uplink and downlink channels and check that reciprocity holds (apart from hardware impairments). When dealing with frequency division duplex (FDD) systems, the beamformer can check whether the received feedback is admissible by using signal processing-based or data-driven anomaly detection algorithms (e.g., [28], [29]). Note that these strategies would not allow preventing the WHACK attack. However, once a malicious node has been detected, the beamformer can remove it from the connected nodes and stop the adversary action.

VI. Experimental Setup

We evaluate the performance of WHACK in a Wi-Fi network deployed indoor using devices implementing the IEEE 802.11ac standard. In Wi-Fi networks, the beamforming feedback consists of some quantized rotational angles whose number depends on the MU-MIMO setting. Given how compressed feedback is built in IEEE 802.11, in addition to the ones in Eq. (14), other two constraints are needed to create standard-compliant feedback. Specifically, the elements associated with the last transmitting antenna in the feedback matrix should be real and positive, i.e., we maintain only the absolute value of the last row in $\tilde{\mathbf{V}}^{\texttt{WHACK}}_{\gamma,\mathrm{all,a}}$ before line 12 in Alg. 2.

We considered a network consisting of a fixed IEEE 802.11ac access point (AP) (beamformer), placing the beamformees in 20 different positions spaced apart by 60 cm within the evaluation environment, as depicted in Figure 6. The channel data have been collected both when the line-of-sight (LOS) between the AP and the beamformees is available and when it is blocked (non-LOS (NLOS) scenario). The beamformer and the beamformees are Asus RT-AC86U IEEE 802.11ac routers, where only one antenna was enabled at the beamformees, i.e., $N_i = N_{\mathrm{ss},i} = 1$. The data is obtained from ongoing transmissions on the 802.11ac channel 157 with an allotted bandwidth of 80 MHz, entailing 256 OFDM sub-channels.

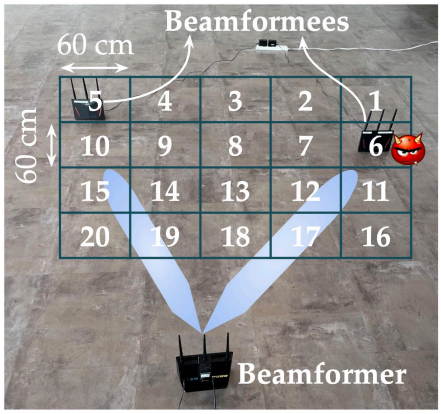

Fig. 6: Experimental setup. The victim and adversary beamformees are moved within the environment in the positions identified by indices $\{1, \ldots, 20\}$.

To collect the channel data for the beamformer-beamformees link we use the Nexmon CSI extraction tool [30]. The CFR is collected for one link at a time to allow the subsequent proper emulation of the channel sounding procedure where the CFR is estimated through the long training field (LTF) in the sounding packet that are transmitted without beamforming and, in turn, the CFR is not affected by ISI and IUI (see Section III).

VII. WHACK Performance Evaluation

To evaluate the WHACK attack effectiveness, we first focus on a scenario consisting of two beamformees served with one spatial stream each as in the example in Section IV. This represents the best-case scenario for the beamformer as it has to shape the smallest number of streams for a MU-MIMO transmission – i.e., two out of the maximum eight beams allowed by [7], [31] – making the precoding accurate. This leads to the worst-case scenario for the adversary as the naturally occurring interference among the streams is at its minimum. Through additional experiments, we also show that the WHACK attack still works increasing the number of beamformees up to four (the 802.11ac maximum), where one of them acts as the adversary implementing the attack.

Each of the distributions presented next is averaged over 2000 channel realizations, i.e., each obtained from 2000 different channel estimates collected from commercial devices as detailed in Section VI. When no otherwise specified, the distributions are obtained from the data collected in the LOS scenario and considering SNR$=25$ dB, which represents a worst-case scenario for the adversary as the victim BER approaches zero when no attacks are performed (see evaluation in Figure 15). The modulation and coding scheme (MCS) is set to the VHT-MCS 4. The number of OFDM poisoned sub-channels is set to $\hat{K}=150$, and the maximum transmission power to $P_{\max}=1\times10^5$ [units of energy per OFDM symbol], based on the average P values we observed during the transmission phase before the malicious action. To have an intuition about its physical meaning, we compute the energy for one OFDM symbols considering an average transmit power of 30 mW. As the transmit time for one OFDM symbol is $T_s = 3.2$ μs, the energy for one OFDM symbol is about 1×10^{-7} J. In turn, 10^5 units of energy per OFDM symbol corresponds to 10 mW that is in line with the expected values.

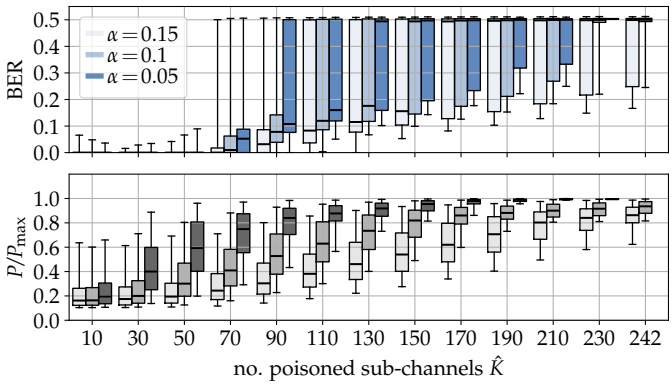

Fig. 7: Victim BER and normalized beamformer transmission power under WHACK for different initialization parameters α, varying the number of poisoned sub-channels $\hat{K}$.

The bars in the following plots cover the 25-75 percentile interval, the horizontal line within each bar represents the median value, and the whiskers span over the 5-95 percentile interval. The horizontal lines in the violin plots indicate the median values.

Hyperparameters Selection. To select the α parameter used to initialize the search algorithm (line 5, Alg. 2), we evaluate the performance of the WHACK approach under different α values. In Figure 7 we report the distribution of the victim BER and the beamformer transmission power when the adversary reports the compressed feedback matrix obtained through WHACK varying $\alpha \in \{0.05, 0.1, 0.15\}$. The results are obtained for the adversary in position 12 and the victim in position 14, and for different numbers of poisoned OFDM sub-channels. As α decreases from 0.15 to 0.1, the attack performance increases, i.e., the victim's BER approaches 0.5, because the WHACK solution is close to the singularity point. However, if α is chosen too small (0.05) the nonlinear conjugate gradient method makes the solution highly deviate from the singularity point thus leading to attack performance degradation. Therefore, we set $\alpha=0.1$ in the following evaluations. Moreover, we set $\mu_0=1$ in line 16 of Alg. 2 based on a hyperparameter search similar to that performed for α. The value for ξ (line 12 of Alg. 2) is set to $\xi = 1.1$ to reflect typical values for the compressed beamforming feedback observed in the data collected from commercial devices. The user-defined parameter $\rho_{\min}$ (see line 7 of Alg. 2) is set to 0.8.

Insights on the WHACK Solution for ACFP. In Figure 8, we plot an example of the real and imaginary parts and the absolute value of the victim beamforming feedback matrix ($\tilde{\mathbf{V}}_{\gamma,\text{all},1}$) – reconstructed by the adversary from the beamforming feedback – together with the same quantities for the uncorrupted adversarial feedback matrix ($\tilde{\mathbf{V}}_{\gamma,\text{all,a}}$) and the adversarial feedback obtained through WHACK ($\tilde{\mathbf{V}}^{\text{WHACK}}_{\gamma,\text{all,a}}$). The data is related to the first transmitter antenna, i.e., the first row of the aforementioned matrices. On the bottom right subplot of Figure 8 we also show the cumulative number of sub-channels of the original adversary feedback that are poisoned when designing the WHACK malicious feedback using the sub-channel selection strategy in Section V-A. Figure 8 shows that

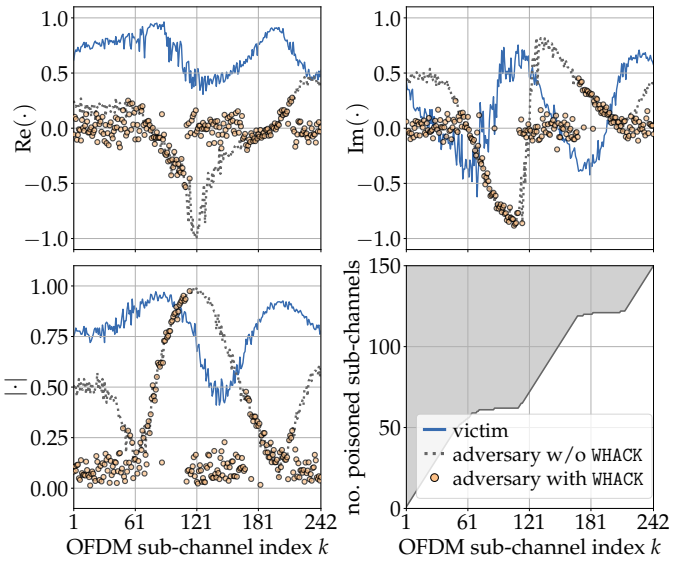

Fig. 8: Example of the feedback matrices (real and imaginary parts and absolute value) of the victim, and the adversary without and with applying WHACK, for the first transmitter antenna. On the bottom right the cumulative number of poisoned sub-channels in the WHACK adversarial feedback is shown.

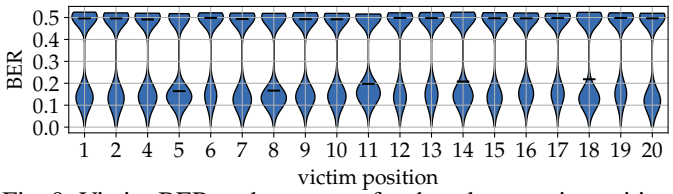

Fig. 9: Victim BER under WHACK for the adversary in position 3 and different victim positions (see Figure 6).

the WHACK solution for the adversary feedback on the $\hat{K}$ poisoned sub-channels approaches zero which is the singularity point for the objective function in Eq. (14) ($\tilde{\mathbf{V}}_{\gamma,k,\mathrm{a}} = 0$, see Section V). The small difference between the two visible in the figure allows enforcing the problem constraints. Figure 8 also allows appreciating how Alg. 1 selects the sub-channels to be poisoned (set $\hat{\mathcal{K}}$, see Section V-A). *The sub-channels that are already closed to the singularity point are maintained unchanged in the WHACK adversary feedback while the others are poisoned through the WHACK algorithm.*

Changing the Victim Position. Figs. 9 shows the distribution of the victim BER when the adversary uses WHACK to report adversarial feedback. To show a different setting for the adversary location, here we consider position 3 for the adversary (middle of the environment, see Figure 6). The victim is placed in each of the other 19 positions, to evaluate the effect of the different respective positions of the victim and the adversary. The results show that WHACK is able to shape adversarial beamforming feedback that maximizes the damage inflicted to the victim.

Changing the Number of Poisoned Sub-Channels $\hat{K}$ and the Maximum Beamformer Transmission Power $P_{\max}$. We evaluate the impact of the hyperparameters $\hat{K}$ and $P_{\max}$ in Figure 10 and Figure 11 respectively. The adversary is in position 12 and the victim is in position 14. The figures show

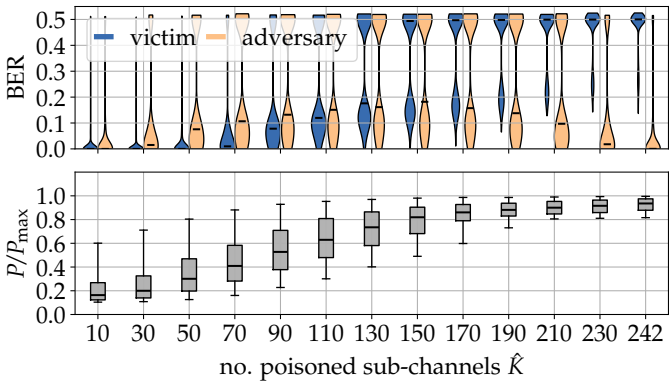

Fig. 10: Victim (left) and adversary (right) BER, and normalized beamformer transmission power under WHACK varying the number of poisoned OFDM sub-channels $\hat{K}$.

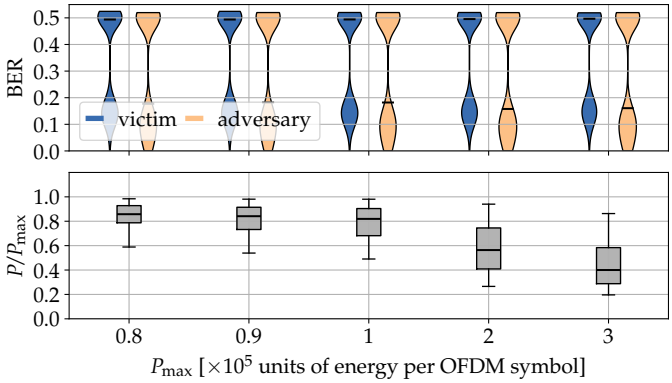

Fig. 11: Victim (left) and adversary (right) BER, and normalized beamformer transmission power under WHACK varying the limit on the transmission power $P_{\max}$.

the BER at the victim and the adversary side (upper plots) and the transmission power at the beamformer (bottom plots) when the WHACK attack is in place. Figure 10 shows that by increasing the number of poisoned sub-channels $\hat{K}$, the malicious node is able to strengthen the damage inflicted to the victim, at the cost of increasing the transmission power – even maintaining it below the limit enforced by the ACFP constraint in Eq. (14) that, in this figure is $P_{\max} = 1 \times 10^5$. Interestingly, *even modifying less than 60% of the feedback, i.e., from $\hat{K} = 150$, the adversary is able to maximize the BER at the victim's receiver. Poisoning only a portion of the sub-channels, the adversary achieves much better stealthiness than modifying the entire feedback*. The results in Figure 11 are obtained for $\hat{K} = 150$ and indicate that WHACK is always able to meet the user-defined power constraint $P_{\max}$ while maximizing the damage inflicted to the victim. For that, *the adversary only uses the power necessary to maximize the BER* without requiring high transmission power when it is not needed – see the last two bars in Figure 11, i.e., $P_{\max} = \{2, 3\} \times 10^5$, where about half of the maximum power is used.

The analysis in Figures 10-11 also shows that the BER experienced by the adversary is low on average. This suggests that *the interference cancellation (see Eq. (5)) performed by the adversary is able to compensate for the badly beamformed transmission*, as the SNR at the adversary side remains high enough for that.

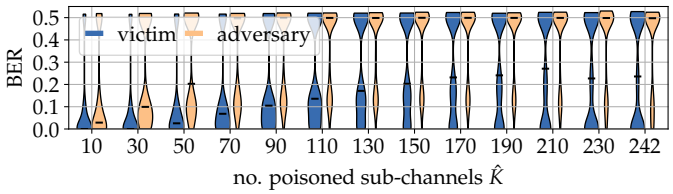

Fig. 12: Victim (left) and adversary (right) BER under WHACK varying the number of poisoned OFDM sub-channels $\hat{K}$ using the interior point optimization algorithm.

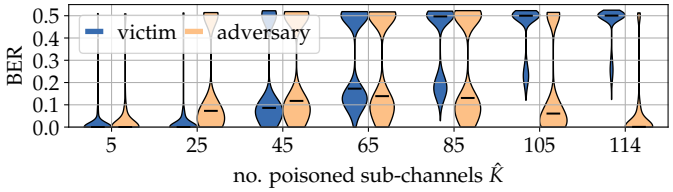

Fig. 13: Victim (left) and adversary (right) BER under WHACK varying the number of poisoned OFDM sub-channels $\hat{K}$ using a 40 MHz channel, i.e., $K = 114$.

In Figure 12 we show the performance of the WHACK attack when using the interior point optimization routine [27] to solve the ACFP problem in Eq. (14) instead of using the approach we proposed in Algorithms 1-2. The results show that this approach also allows designing proper malicious feedback. However, the BER increase is on average less than the increase we can achieve with our approach (see Figure 10). Moreover, while our approach allows keeping the BER at the adversary low, the feedback obtained through the interior point optimization strategy makes the BER at the adversary increase with the same trend of the BER at the victim device.

To evaluate the impact of the total number of OFDM data sub-channels on the attack performance, in Figure 13 we evaluate WHACK emulating a 40 MHz system varying the number of poisoned sub-channels $\hat{K}$ from the total $K = 114$ data sub-channels. The results show that WHACK leads to a 0.5 BER at the victim receiver starting from $\hat{K} = 85$, consistently with the evaluation at 80 MHz.

Evaluation in NLOS Scenario and changing the SNR. We compare the BER achieved for different values of poisoned OFDM sub-channels in the LOS scenario considered above with the results obtained in the NLOS setting. The analysis is reported in Figure 14 and shows that the WHACK attack is effective in both LOS and NLOS. The impact of the SNR is evaluated in Figure 15. We consider both the LOS and NLOS cases and we evaluate the variations in the BER when the adversary reports the uncorrupted feedback ("normal" situation) and when it reports the malicious feedback obtained through WHACK to inflict damage to the victim. *Starting from an SNR of 15 dB, WHACK succeeds in increasing the BER of the victim both in LOS and NLOS channels*. Moreover, when the SNR reaches 25-30 dB, while in a normal situation the BER approaches zero, WHACK is still able to damage the victim transmission increasing the experienced BER. The decrease in the effectiveness of WHACK when increasing the SNR is linked to the way multi-input, multi-output (MIMO) precoding works. While the precoding ensures that each beamformee does not receive information related to streams directed to different beamformees in the network, this does not imply that the streams are nullified in all the directions except the one of the receiver. In turn, when the SNR is high, the victim can still decode the stream even if the precoding is corrupted. However, in real-world situations, it is unlikely to have SNR higher than 25 dB.

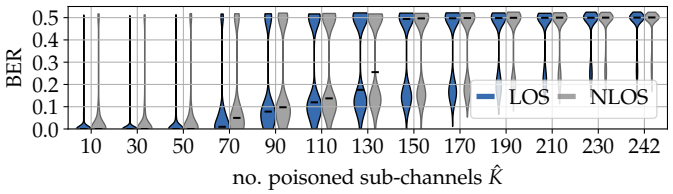

Fig. 14: Victim BER under WHACK varying the number of poisoned sub-channels in LOS (left) / NLOS (right) settings.

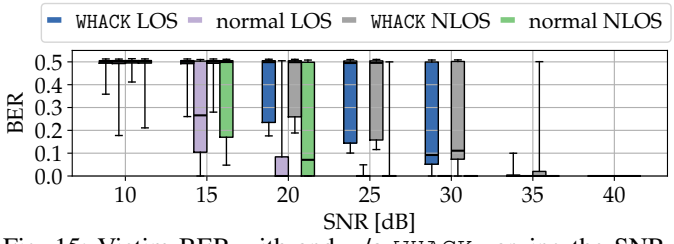

Fig. 15: Victim BER with and w/o WHACK varying the SNR.

Evaluation with multiple beamformees. In Figure 16 we report the BER (varying the number of poisoned sub-channels) experienced by four MU-MIMO devices (the maximum for 802.11ac/ax) where one of them acts as the adversary implementing the WHACK attack. The victims are in positions 8, 10, and 14, and the adversary is in position 12 (see Figure 6). The results confirm that *the WHACK attack effectively maximizes the BER of multiple beamformees in the network*. This is because the WHACK attack vector is derived from the singularity point of the objective function in ACFP, which is independent of the specific victim ($\tilde{\mathbf{V}}_{\gamma,k,\mathrm{a}} = 0$). Moreover, as the compressed feedback of all the devices is used when applying Alg. 2, the gradient descent happens in the direction that maximizes the BER for all the victims. The results also show that contrary to the single victim case, the adversary's BER also increases. The reason behind this is that the adversary interference cancellation module is unable to compensate for the increased number of interfering streams.

VIII. Conclusions

In this paper, we have prototyped and evaluated a new attack vector (WHACK) against MU-MIMO in wireless communication networks. Through WHACK, an adversary triggers changes in the beamforming that result in maximizing the BER at victim devices. This is obtained by transmitting malicious beamforming feedback to the beamformer during the channel sounding process. Conversely from existing work that relied on the uncompressed CFR, WHACK uses the *compressed feedback*, which is the actual way the feedback is transmitted. To craft the WHACK attack, we defined an optimization problem (ACFP) to maximize the victims' BER by leveraging the compressed feedback of the devices in the network. Hence, we defined a custom-tailored nonlinear conjugate gradient solver

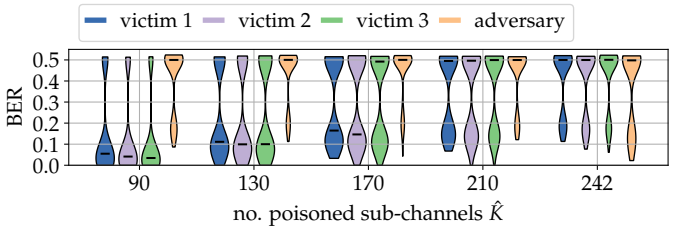

Fig. 16: BER for three victim beamformees and the adversary under WHACK varying the number of poisoned sub-channels.

to derive the malicious feedback. WHACK has been evaluated through experimental IEEE 802.11ac data. The results have shown that using WHACK the adversary is only required to change less than 60% of the compressed feedback to maximize the BER of victims (BER$=0.5$) while satisfying the transmission power constraint at the beamformer. We hope that the results in this article will inform existing standardization efforts and spur additional research on MU-MIMO security.

APPENDIX A
FORMULATION OF THE POWER CONSTRAINT

We define P as $P=\sum_{k\in\mathcal{K}}\mathbb{E}\left[||\mathbf{W}_k\mathbf{x}_k||^2\right]$ following the formulation in [18]. Hence, assuming $\mathbb{E}\left[\mathbf{x}_k\mathbf{x}_k^\dagger\right]=1$, we can rewrite the expression of P as

$$P=\sum_{k\in\mathcal{K}}||\mathbf{W}_k||_F^2=\sum_{k\in\mathcal{K}}\mathrm{Tr}\left[\mathbf{W}_k\mathbf{W}_k^\dagger\right], \tag{15}$$

where F indicates the Frobenius norm of a matrix. Using Eq. (2) and the equality $(\mathbf{A}^{-1})^\dagger=(\mathbf{A}^\dagger)^{-1}$, we have

$$P=\mathrm{Tr}\left[\tilde{\mathbf{V}}_{\gamma,k}\left(\tilde{\mathbf{V}}_{\gamma,k}^\dagger\tilde{\mathbf{V}}_{\gamma,k}\right)^{-1}\left(\tilde{\mathbf{V}}_{\gamma,k}^\dagger\tilde{\mathbf{V}}_{\gamma,k}\right)^{-1}\tilde{\mathbf{V}}_{\gamma,k}^\dagger\right]. \tag{16}$$

Applying the trace propriety $\mathrm{Tr}[\mathbf{AB}]=\mathrm{Tr}[\mathbf{BA}]$ with $\mathbf{A}=\tilde{\mathbf{V}}_{\gamma,k}\left(\tilde{\mathbf{V}}_{\gamma,k}^\dagger\tilde{\mathbf{V}}_{\gamma,k}\right)^{-1}$ and $\mathbf{B}=\left(\tilde{\mathbf{V}}_{\gamma,k}^\dagger\tilde{\mathbf{V}}_{\gamma,k}\right)^{-1}\tilde{\mathbf{V}}_{\gamma,k}^\dagger$, we can simplify the expression in Eq. (16) and obtain

$$P=\mathrm{Tr}\left[\left(\tilde{\mathbf{V}}_{\gamma,k}^\dagger\tilde{\mathbf{V}}_{\gamma,k}\right)^{-1}\right]. \tag{17}$$

Note that the Hermitian matrix $\tilde{\mathbf{V}}_{\gamma,k}^\dagger\tilde{\mathbf{V}}_{\gamma,k}$ is positive semidefinite (see Appendix C) and so is its inverse. This implies that the values on the main diagonal of $\left(\tilde{\mathbf{V}}_{\gamma,k}^\dagger\tilde{\mathbf{V}}_{\gamma,k}\right)^{-1}$ are real and non-negative. In turn, $P_k\in\mathbb{R}_{\geq 0}$.

APPENDIX B
GENERAL FORMULATION FOR DERIVING EQ. (14)

Here we provide the general analysis for obtaining Eq. (14) from the MSE defined in Eq. (8). We first note that the inverse of $\mathbf{\Omega}_k$ in Eq. (9) cannot be expressed in closed form using the block-matrix inverse formulation, as the Schur complements are zero [32]. To invert it, we rewrite Eq. (8) by using the general expression for the inverse of a matrix. The multiplication by the identity matrices on the left and right sides in Eq. (8) implies retaining only the $N_{\mathrm{ss},1}\times N_{\mathrm{ss},1}$ upper-left sub-matrix of the inverse, and the trace operation further selects only the diagonal elements of such sub-matrix. Hence, the $d\in\{0,N_{\mathrm{ss},1}-1\}$ addend of the trace operation in Eq. (8), i.e., the (d,d) element of the inverse matrix $\mathbf{\Omega}_k^{-1}$, is obtained by computing the (d,d) cofactor $C_{d,d}$ and dividing it by the determinant of the matrix $\mathbf{\Omega}_k$. Specifically, $C_{d,d}$ is obtained as

$$C_{d,d}=(-1)^{2(d+1)}\sum_{\boldsymbol{\zeta}\in S_d}(-1)^{\#\mathrm{inv}(\boldsymbol{\zeta})}\prod_{s\in\{0,\ldots,N_{\mathrm{ss}}-1\}\setminus d}\left[\mathbf{\Omega}_k\right]_{\zeta_s,s}, \tag{18}$$

where S_d is the set of permutations $\boldsymbol{\zeta}$ of set $\{0,\ldots,N_{\mathrm{ss}}-1\}\setminus d$, ζ_s is the s-th element of the permutation vector $\boldsymbol{\zeta}$, and $\#\mathrm{inv}(\boldsymbol{\zeta})$ is the number of inversions in the permutation $\boldsymbol{\zeta}$. Hence, we can rewrite Eq. (8) as

$$\mathrm{MSE}\left(\hat{\mathbf{x}}_{k,1},\mathbf{x}_{k,1}\right)=\left(\det[\mathbf{\Omega}_k]\right)^{-1}\sum_{d=0}^{N_{\mathrm{ss},1}-1}C_{d,d}. \tag{19}$$

Note that by definition $\mathbf{\Omega}_k$ in Eq. (9) is positive semidefinite and, in turn, the determinant is positive and all cofactors $C_{d,d}$ satisfy $C_{d,d}\geq 0$. Moreover, from the formulation in Eq. (18), it follows that each term in Eq. (19) is associated with inter-stream or inter-user interference as for each stream d, we only consider the terms different from d in the cofactor definition. In the ideal case, $\mathbf{\Omega}_k$ takes the values specified in Eq. (10) and the cofactors in Eq. (19) equal zero, i.e., there is no interference.

Given these considerations, to maximize Eq. (19) based on the control variable $\tilde{\mathbf{V}}_{\gamma,\mathrm{all,a}}$ we need to set $\tilde{\mathbf{V}}_{\gamma,\mathrm{all,a}}$ to make the terms in Eq. (9) containing such control variable deviate from zero. Hence, we next focus on the common product matrix $\mathbf{W}_{k,\mathrm{a}}^\dagger\mathbf{H}_{k,1}^\dagger$, or, equivalently, $\mathbf{H}_{k,1}\mathbf{W}_{k,\mathrm{a}}$, associated with the inter-user interference caused by the adversary to the victim. We rewrite the expression of $\mathbf{W}_{k,\mathrm{a}}^\dagger\mathbf{H}_{k,1}^\dagger$ by decomposing the channel matrix $\mathbf{H}_{k,1}$ via SVD, as presented in Eq. (1) for $\mathbf{H}_{\gamma,k,i}$. We have $\mathbf{H}_{k,1}=\mathbf{U}_{k,1}\mathbf{S}_{k,1}\mathbf{Z}_{k,1}^\dagger$, where $\mathbf{U}_{k,1}$ and $\mathbf{Z}_{k,1}$ are $N_{\mathrm{ss},1}\times N_{\mathrm{ss},1}$ and $M\times M$ unitary matrices, and $\mathbf{S}_{k,1}$ is a $N_{\mathrm{ss},1}\times M$ matrix collecting the singular values of $\mathbf{H}_{k,1}$. Adopting the same notation used in Section III, we refer to the first $N_{\mathrm{ss},1}$ columns of $\mathbf{Z}_{k,1}$ as $\tilde{\mathbf{V}}_{k,1}$. As the number of singular values, i.e., the rank of $\mathbf{H}_{k,1}$ is $\min\{M,N_{\mathrm{ss},1}\}=N_{\mathrm{ss},1}$, we can write $\mathbf{H}_{k,1}=\mathbf{U}_{k,1}\mathbf{S}_{k,1}\mathbb{I}_{M\times N_{\mathrm{ss},1}}\tilde{\mathbf{V}}_{k,1}^\dagger$. Hence, to maximize Eq. (19) we can further focus on making the term $\mathbf{W}_{k,\mathrm{a}}^\dagger\tilde{\mathbf{V}}_{k,1}$ deviate from zero. We remind that, as mentioned in Section III, the precoding matrix in Eq. (2) enforces $\mathbf{W}_{k,\mathrm{a}}^\dagger\tilde{\mathbf{V}}_{\gamma,k,1}=\mathbf{0}$. However, by leveraging the small differences between $\tilde{\mathbf{V}}_{\gamma,k,1}$ and $\tilde{\mathbf{V}}_{k,1}$ we can effectively make $\mathbf{W}_{k,\mathrm{a}}^\dagger\tilde{\mathbf{V}}_{k,1}\neq 0$. By definition, $\mathbf{W}_{k,\mathrm{a}}$ consists of the right $N_{\mathrm{ss,a}}$ columns of $\mathbf{W}_k=\left[\tilde{\mathbf{V}}_{\gamma,k,1}\ \tilde{\mathbf{V}}_{\gamma,k,\ell}\ \tilde{\mathbf{V}}_{\gamma,k,\mathrm{a}}\right]\left(\tilde{\mathbf{V}}_{\gamma,k}^\dagger\tilde{\mathbf{V}}_{\gamma,k}\right)^{-1}$. Using the general expression for the matrix inverse we have

$$\begin{aligned}\mathbf{W}_{k,\mathrm{a}}\tilde{\mathbf{V}}_{k,1}=\det\left[\tilde{\mathbf{V}}_{\gamma,k}^\dagger\tilde{\mathbf{V}}_{\gamma,k}\right]^{-1}\big(&\tilde{\mathbf{V}}_{\gamma,k,1}\mathbf{C}_{1,\mathrm{a}}+\tilde{\mathbf{V}}_{\gamma,k,\ell}\mathbf{C}_{\ell,\mathrm{a}}\\&+\tilde{\mathbf{V}}_{\gamma,k,\mathrm{a}}\mathbf{C}_{\mathrm{a,a}}\big)\tilde{\mathbf{V}}_{k,1},\end{aligned} \tag{20}$$

where $\mathbf{C}_{\cdot,\mathrm{a}}$ are the $N_{\mathrm{ss},\cdot}\times N_{\mathrm{ss,a}}$ dimensional matrices containing the cofactors of $\mathbf{\Pi}$ in the last $N_{\mathrm{ss,a}}$ columns. Specifically, the cofactor at index (d,f) in $\mathbf{C}_{\cdot,\mathrm{a}}$ is obtained as

$$C_{d,f}=(-1)^{(d+f+1)}\sum_{\boldsymbol{\zeta}\in S_d}(-1)^{\#\mathrm{inv}(\boldsymbol{\zeta})}\prod_{s\in\{0,\ldots,N_{\mathrm{ss}}-1\}\setminus f}\left[\tilde{\mathbf{V}}_{\gamma,k}^\dagger\tilde{\mathbf{V}}_{\gamma,k}\right]_{\zeta_s,s}. \tag{21}$$

The numerator of $\mathbf{W}_{k,\mathrm{a}}^{\dagger}\tilde{\mathbf{V}}_{k,1}$ in Eq. (20), i.e., $\left(\mathbf{C}_{1,\mathrm{a}}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k,1}^{\dagger}+\mathbf{C}_{\ell,\mathrm{a}}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k,\ell}^{\dagger}+\mathbf{C}_{\mathrm{a},\mathrm{a}}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k,\mathrm{a}}^{\dagger}\right)\tilde{\mathbf{V}}_{k,1}$, approaches zero as $\tilde{\mathbf{V}}_{\gamma,k,1}$ approaches $\tilde{\mathbf{V}}_{k,1}$ (for each stream we can write an expression similar to the one in Eq. (13)). However, as introduced before, the variability of the wireless channel prevents $\tilde{\mathbf{V}}_{\gamma,k,1}$=$\tilde{\mathbf{V}}_{k,1}$ to hold. Following the same reasoning detailed in Section IV for the simple case, we obtain that the problem in Eq. (6) can be replaced by the problem in Eq. (14), i.e., the maximization of the inverted denominator of $\mathbf{W}_{k,\mathrm{a}}^{\dagger}\tilde{\mathbf{V}}_{k,1}$ in Eq. (20).

APPENDIX C
PROOF OF POSITIVE SEMIDEFINITE MATRIX

Lemma C.1. *The matrix $\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}$ is positive semidefinite.*

Proof. $\mathbf{r}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\mathbf{r}=\left|\tilde{\mathbf{V}}_{\gamma,k}\mathbf{r}\right|^{2}\geq 0,\ \ \forall\ \mathbf{r}\in\mathbb{C}^{N_{\mathrm{ss}}}\backslash\{0\}.$ □

Lemma C.2. $\det\left[\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\right]\in\mathbb{R}_{\geq 0}$.

Proof. Based on the mathematical proprieties of the determinant, we can write:

$$\begin{aligned}\det\left[\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}\right]&=\det\left[\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\right]\det\left[\tilde{\mathbf{V}}_{\gamma,k}\right]\\&=\left(\det\left[\tilde{\mathbf{V}}_{\gamma,k}\right]\right)^{*}\det\left[\tilde{\mathbf{V}}_{\gamma,k}\right]\\&=\left|\det\left[\tilde{\mathbf{V}}_{\gamma,k}\right]\right|^{2}.\end{aligned}\tag{22}$$

Lemma C.2 can also be proved observing that $\tilde{\mathbf{V}}_{\gamma,k}^{\dagger}\tilde{\mathbf{V}}_{\gamma,k}$ is Hermitian and positive semidefinite (from Lemma C.1). □

REFERENCES

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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] P. K. Sangdeh, H. Pirayesh, A. Mobiny, and H. Zeng, "LB-SciFi: Online learning-based channel feedback for MU-MIMO in wireless LANs," in *Proc. of IEEE 28th International Conference on Network Protocols (ICNP)*, 2020.

[9] 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.

[10] J. Guo, C.-K. Wen, S. Jin, and G. Y. Li, "Overview of deep learning-based CSI feedback in massive MIMO systems," *IEEE Transactions on Communications*, vol. 70, no. 12, pp. 8017–8045, 2022.

[11] 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.

[12] Q. Liu, J. Guo, C.-K. Wen, and S. Jin, "Adversarial attack on DL-based massive MIMO CSI feedback," *Journal of Communications and Networks*, vol. 22, no. 3, pp. 230–235, 2020.

[13] 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.

[14] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2840–2852, 2013.

[15] 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.

[16] 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.

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

[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] M. A. Woodbury, *Inverting modified matrices*. Statistical Research Group, 1950.

[21] K. F. Haque, F. Meneghello, and F. Restuccia, "Wi-BFI: Extracting the IEEE 802.11 Beamforming Feedback Information from Commercial Wi-Fi Devices," in *Proceedings of the 17th ACM Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization*, pp. 104–111, 2023.

[22] J. Dattorro, *Convex optimization & Euclidean distance geometry*. Lulu. com, 2010.

[23] A. Ben-Tal and A. Nemirovski, *Lectures on modern convex optimization: analysis, algorithms, and engineering applications*. SIAM, 2001.

[24] J. Nocedal and S. J. Wright, *Numerical Optimization*. Springer, 1999.

[25] R. Fletcher and C. M. Reeves, "Function Minimization by Conjugate Gradients," *The computer journal*, vol. 7, no. 2, pp. 149–154, 1964.

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

[27] F. A. Potra and S. J. Wright, "Interior-point methods," *Journal of computational and applied mathematics*, vol. 124, no. 1-2, pp. 281–302, 2000.

[28] S.-D. Wang, H.-M. Wang, C. Feng, and V. C. Leung, "Sequential anomaly detection against demodulation reference signal spoofing in 5G NR," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 1, pp. 1291–1295, 2022.

[29] S. Rajendran, V. Lenders, W. Meert, and S. Pollin, "Crowdsourced wireless spectrum anomaly detection," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 694–703, 2019.

[30] F. Gringoli, M. Schulz, J. Link, and M. Hollick, "Free your CSI: A channel state information extraction platform for modern Wi-Fi chipsets," in *Proc. of ACM WiNTECH*, (Los Cabos, Mexico), 2019.

[31] 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.

[32] S. R. Searle and A. I. Khuri, *Matrix algebra useful for statistics*. John Wiley & Sons, 2017.