Physical-Layer Spoofing in WiFi 6 to Steer the Beam Toward the Attacker

Tiep M. Hoang, Alireza Vahid, Douglas C. Sicker, and Ashutosh Sabharwal

***Abstract*—Security threats of an IEEE 802.11ax (WiFi 6) system can occur throughout the layers of the protocol stack. Looking at the security aspect of the physical layer and from an attacker's perspective, we present how a spoofing attack can cause an access point to steer the beam dedicated to a legitimate user toward the attacker. More particularly, we propose the BeamSteal attack that takes advantage of the vulnerability of the beamforming feedback (BFF) mechanism. The purpose of the BeamSteal attack is to cause the access point to receive the wrong BFF-information-bearing bits and end up steering the beam toward the attacker instead of the legitimate user. To contrast the harmful effect of the proposed attack, we compare it with two benchmarks, namely the no attack case and the jamming attack case. Our numerical results show that the BeamSteal attack not only degrades the performance of the legitimate user, but also helps the attacker improve its performance significantly.**

***Index terms*—**802.11ax, WiFi 6, physical layer security.

I. Introduction

The physical layer (PHY) security has been an active research area for many years. Unlike the security at the higher layers that normally relies on cryptography, the PHY security mainly relies on the random nature of channels [1]. When it comes to the PHY security in IEEE 802.11 systems (namely, WiFi systems), it seems that there has been a paucity of work. Even broadening our interest in security at both the PHY and MAC layers for WiFi systems, little work can be found [2]–[7]. Not to mention, WiFi versions generally differ from each other; thus, there is a need to conduct research on the PHY security for each specific WiFi version. Given that IEEE 802.11ax (namely, WiFi 6) is a new generation of WiFi and is becoming more commercially popular, it is worth investigating the PHY security on IEEE 802.11ax systems.

Among the related papers [2]–[7], the work in [2] considered a detection method based on received signal strength to cope with spoofers, who can clone the MAC address of an access point (AP). The authors of [3] studied how to impersonate legitimate devices based on the fingerprints of hardware devices. The authors of [4] evaluated the performance of jamming attacks at the PHY and MAC layer in a cognitive radio network. While the aforementioned work focused on the MAC-layer attacks, [5] considered the impact of a PHY attack on IEEE 802.11p and focused on degrading the location privacy of vehicles by using a simple scrambler. In [6], the author proposed embedding a bit sequence in the short training field to make the so-called preamble modulation. This new design was supposed to support PHY functions, including the ability to deal with spoofing attacks, but the security performance was not well studied. Meanwhile, [7] looked at the PHY security aspect from an attacker's perspective and showed that an attacker can break channel state information (CSI)-based passwords of a WiFi system

Unlike [2]–[4], which focus on the MAC-layer security, we focus more on the PHY aspect in this paper. Additionally, compared to [5]–[7], we look at the vulnerability of beamforming feedback (BFF) and propose a bit-flipping attack in the attacker's favor, which we call the "BeamSteal" attack. Although [7] also considers the WiFi security aspect from an attacker's perspective, it relies on estimating the channel between a pair of legitimate transceivers. By contrast, in our attack method, the attacker steals information dedicated to the legitimate user without the need for the estimation of legitimate channel. Moreover, the work in [2]–[6] is about securing WiFi systems rather than attacking the systems. Our work seeks to exploit a security hole existing in IEEE 802.11 standards, specifically to 802.11ax, and demonstrates how an attacker can harness it for stealing information. We focus on the BFF in 802.11ax and prove that the lack of encryption for the BFF makes 802.11ax vulnerable to a spoofing attack.

Our main contributions can be listed as follows:

- We look at the security threat from an attacker's perspective and take advantage of the BFF vulnerability to initiate a spoofing attack, which we call the BeamSteal attack. To be more specific, the attacker can know the BFF-information-bearing bit sequence, which the legitimate user wants to inform the AP of. Since the attacker also knows another bit sequence that benefits the best performance for itself, the attacker can realize the differences in bits and perform bit-flipping to deceive the AP.
- We compare the proposed BeamSteal attack with conventional jamming attacks and show that the former is much more dangerous in terms of information leakage.
- We demonstrate that the package error rate (PER) of an attacker can be significantly improved and even close to

T. M. Hoang and A. Vahid are with Department of Electrical and Microelectronic Engineering, Rochester Institute of Technology, NY 14623, US (emails: tmheme@rit.edu, arveme@rit.edu). D. C. Sicker is with Department of Electrical Engineering, University of Colorado Denver, CO 80204, US (email: douglas.sicker@ucdenver.edu). A. Sabharwal is with Department of Electrical and Computer Engineering, Rice University, Houston, TX 77005, US (e-mail: ashu@rice.edu).

The work of T. M. Hoang and A. Vahid was in part supported by NSF grants ECCS-2030285, CNS-2343959, CNS-2343964, and AST-2348589.

The work of D. C. Sicker was in part supported by NSF grant AST-2232482.

A. Sabharwal was partially supported by NSF Grants 2211803 and 2148313, and a grant from Army Research Labs, W911NF-19-2-0269.

ICC 2024 - IEEE International Conference on Communications | 978-1-7281-9054-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICC51166.2024.10622744

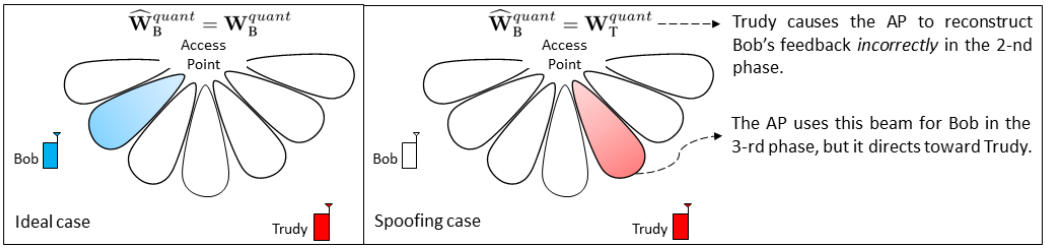

Fig. 1: The first sub-figure depicts the ideal case in Phase ③, where the AP reconstructs the beamforming matrix (i.e., $\widehat{\mathbf{W}}_{\mathrm{B}}^{quant}$) to be the same as the one that Bob desires (i.e., $\mathbf{W}_{\mathrm{B}}^{quant}$). By contrast, the second sub-figure depicts the worst case in Phase ③, where Trudy lures the AP to reconstruct $\widehat{\mathbf{W}}_{\mathrm{B}}^{quant}$ to be the same as the one that Trudy wants (i.e., $\mathbf{W}_{\mathrm{T}}^{quant}$).

the PER of the legitimate user in the case of no attack. We also demonstrate that the conventional jamming attack can only degrade the legitimate user's performance while not improving the attacker's performance.

Our BeamSteal attack illustrates an example of the capability of an adversary in remotely controlling the behavior of the AP. Beyond the example in this paper, BeamSteal-like attacks can achieve a targeted outcome behavior by forcing the AP to direct the energy towards some specific directions. Such BeamSteal-like methods could be performed for more nefarious attacks. For instance, the attacker could make the AP scan all possible directions in order for the attacker to collect reflected energy to portray the physical environment around it. In this case, the attacker is taking advantage of the AP to learn about the physical environment and extract the location of objects in the scene.

II. Attack Plan and A Brief Review of the BFF

We first present Trudy's attack plan and then describe the BFF's role in 802.11ax that Trudy will take advantage of.

A. Attack Plan

To begin with, let us recall a downlink transmission process in 802.11ax that includes the following phases:

- Phase ①, namely the NDP-phase: The AP sends a null data packet (NDP) to a legitimate user (Bob).
- Phase ②, namely the BFF-phase: Bob uses the NDP to estimate the channel state information (CSI) that will be then quantized and fed back to the AP.
- Phase ③, namely the payload-phase: Based on receiving and decoding the quantized BFF, the AP will design the beamforming vector/matrix that is best suited for Bob.

The security threat stems from the fact that in 802.11ax and its predecessors, the BFF is *not* protected by encryption and any device with a MAC-frame-capturing tool can decode the user's feedback [8]. Thus, Trudy can use a MAC-frame-capturing tool to decode Bob's BFF regardless of whether Trudy is passive as an eavesdropper or active as an attacker. When Trudy is passive, he can collect information from the AP and Bob, including Bob's BFF. Then, when Trudy becomes active, Trudy employs Bob's BFF to make an attack plan.

We define $\mathbf{W}_{\mathrm{B}}^{quant}$ as the beamforming matrix chosen by Bob, $\widehat{\mathbf{W}}_{\mathrm{B}}^{quant}$ as the beamforming matrix reconstructed by the AP, and $\mathbf{W}_{\mathrm{A}}$ as the beamforming matrix designed by the AP. We always have $\mathbf{W}_{\mathrm{A}} = \widehat{\mathbf{W}}_{\mathrm{B}}^{quant}$ because the AP designs the beam based on what it reconstructs from Bob's feedback. In the ideal scenario, the AP reconstructs $\widehat{\mathbf{W}}_{\mathrm{B}}^{quant} = \mathbf{W}_{\mathrm{B}}^{quant}$ and then uses the beamforming matrix $\mathbf{W}_{\mathrm{A}} = \mathbf{W}_{\mathrm{B}}^{quant}$ for the downlink transmission. However, if the AP cannot reconstruct the beam that Bob desires, i.e., $\widehat{\mathbf{W}}_{\mathrm{B}}^{quant} \neq \mathbf{W}_{\mathrm{B}}^{quant}$, then the AP will end up with $\mathbf{W}_{\mathrm{A}} \neq \mathbf{W}_{\mathrm{B}}^{quant}$. This means that the transmit beam does not direct its main lobe toward Bob but to another user/direction.

Based on this argument, Trudy's plan is to deceive the AP so that the AP directs the transmit beam toward Trudy's position. To be more specific, let $\mathbf{W}_{\mathrm{T}}^{quant}$ be the quantized beamforming matrix best suited for Trudy. The goal of Trudy is to make the AP choose $\mathbf{W}_{\mathrm{A}} = \mathbf{W}_{\mathrm{T}}^{quant}$ instead of $\mathbf{W}_{\mathrm{A}} = \mathbf{W}_{\mathrm{B}}^{quant}$. Herein, $\mathbf{W}_{\mathrm{A}} = \mathbf{W}_{\mathrm{T}}^{quant}$ implies that Trudy succeeds in *stealing* Bob's beam. Figure 1 illustrates a successful attack.

This paper mainly focuses on showcasing the threat in Phase ②. Upon a successful attack, if the payload is not encrypted, Trudy will have access to Bob's information. However, even if the payload is encrypted, our spoofing attack is superior to jamming attacks (from an attacker's perspective) as it will enhance other threats such as traffic analysis attacks at higher layers [9] by providing Trudy with an improved signal.

B. The role of the BFF: A Review

In order for Trudy to achieve his goal, it is important to understand the role of the BFF. Thus, we will present a *backward* analysis, from Phase ③ back to Phase ②, in order to expose the vulnerability of the BFF.

1) The payload-phase: In Phase ③, the AP transmits the downlink signal $\mathbf{x}_{\mathrm{A}} \in \mathbb{C}^{N_{\text{stream}} \times 1}$ to Bob denoted by B. The signal received at B can be given by:

$$\mathbf{y}_{\mathrm{B}} = \mathbf{H}_{\mathrm{BA}} \mathbf{W}_{\mathrm{A}} \mathbf{x}_{\mathrm{A}} + \mathbf{n}_{\mathrm{B}}, \tag{1}$$

where $\mathbf{H}_{\mathrm{BA}} \in \mathbb{C}^{N_{\mathrm{B}} \times N_{\mathrm{A}}}$ is the channel of the downlink A-B link, $\mathbf{W}_{\mathrm{A}} \in \mathbb{C}^{N_{\mathrm{A}} \times N_{\text{stream}}}$ is the beamforming matrix designed by the AP, and $\mathbf{n}_{\mathrm{B}} \in \mathbb{C}^{N_{\mathrm{B}} \times 1}$ is the additive white Gaussian noise (AWGN) at Bob. Note that $\mathbb{E}\left\{\|\mathbf{x}_{\mathrm{A}}\|^2\right\} = P_{\mathrm{A}}$ and $\mathbb{E}\left\{\|\mathbf{n}_{\mathrm{B}}\|^2\right\} = N_0$. Herein, $\mathbb{C}^{m \times n}$ denotes the complex field that includes all complex-valued matrices of size $m \times n$; while $\mathbf{z} \sim \mathcal{CN}(\mathbf{m}, \mathbf{\Sigma})$ is a complex Gaussian random vector with mean $\mathbf{m}$ and covariance matrix $\mathbf{\Sigma}$.

Upon receiving $\mathbf{y}_{\mathrm{B}}$ in Phase ③, Bob performs maximum likelihood (ML) estimation to estimate the transmitted signal, the ML estimate of $\mathbf{x}_{\mathrm{A}}$ can be calculated as follows:

$$\widehat{\mathbf{x}}_{\mathrm{A|at\ B}} = \arg\min_{\mathbf{x}} \|\mathbf{y}_{\mathrm{B}} - \mathbf{H}_{\mathrm{BA}}\widetilde{\mathbf{W}}_{\mathrm{B}}\mathbf{x}\|. \tag{2}$$

Extracting further latent messages from the payload data will be ignored since it should be addressed at the upper layers.

Since Bob wants the AP to be aware that $\widetilde{\mathbf{W}}_{\mathrm{B}}$ is the correct beamforming matrix for Bob, he will send the BFF to the AP in Phase ② with the aim that the AP will then design $\mathbf{W}_{\mathrm{A}} = \widetilde{\mathbf{W}}_{\mathrm{B}}$ in Phase ③. The calculation of $\widetilde{\mathbf{W}}_{\mathrm{B}}$ is based on $\mathbf{H}_{\mathrm{BA}}$. To be more specific, in Phase ②, Bob first performs the singular value decomposition (SVD) to factorize $\mathbf{H}_{\mathrm{BA}}$ into $\mathbf{H}_{\mathrm{BA}} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^{\dagger}$, where $\mathbf{U} \in \mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{B}}}$ and $\mathbf{V} \in \mathbb{C}^{N_{\mathrm{A}}\times N_{\mathrm{A}}}$ are unitary matrices, and $\mathbf{\Sigma} \in \mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{A}}}$ is a matrix of singular values. Bob then calculates $\widetilde{\mathbf{W}}_{\mathrm{B}}$ as follows:

$$\widetilde{\mathbf{W}}_{\mathrm{B}} = [\mathbf{v}_1, \ldots, \mathbf{v}_{N_{\mathrm{stream}}}] \in \mathbb{C}^{N_{\mathrm{A}}\times N_{\mathrm{stream}}}, \tag{3}$$

where $\mathbf{v}_i$ is the i^{th} column of $\mathbf{V}$. As a result, Bob will obtain the product $\mathbf{V}^{\dagger}\widetilde{\mathbf{W}}_{\mathrm{B}} = \begin{bmatrix} \mathbf{I}_{N_{\mathrm{stream}}\times N_{\mathrm{stream}}} \\ \mathbf{0}_{(N_{\mathrm{A}}-N_{\mathrm{stream}})\times N_{\mathrm{stream}}} \end{bmatrix} \triangleq \widetilde{\mathbf{I}}$, which simplifies (2) into the following:

$$\widehat{\mathbf{x}}_{\mathrm{A|at\ B}} = \arg\min_{\mathbf{x}} \left\| \mathbf{U}^{\dagger}\mathbf{y}_{\mathrm{B}} - \widetilde{\mathbf{\Sigma}}\mathbf{x} \right\|, \tag{4}$$

where $\widetilde{\mathbf{\Sigma}} = \mathbf{\Sigma}\widetilde{\mathbf{I}} \in \mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{stream}}}$. Herein, $\mathbf{I}_n$ denotes the identity matrix of size $n \times n$; the upperscripts $(\cdot)^{\top}$ and $(\cdot)^{\dagger}$ represent the transpose and Hermitian operators, respectively.

In short, Bob reports $\widetilde{\mathbf{W}}_{\mathrm{B}}$ to the AP in Phase ② so that the AP designs $\mathbf{W}_{\mathrm{A}} = \widetilde{\mathbf{W}}_{\mathrm{B}}$ in Phase ③. However, Bob does not report all elements of $\widetilde{\mathbf{W}}_{\mathrm{B}}$ to the AP. Instead, Bob reports the indices that will enable the AP to reconstruct $\widetilde{\mathbf{W}}_{\mathrm{B}}$.

2) The BFF-phase: Since $\mathbf{V}$ is a unitary matrix, Bob can decompose $\widetilde{\mathbf{W}}_{\mathrm{B}}$ into polar values [10]–[12]. Let $\left[\widetilde{\mathbf{W}}_{\mathrm{B}}\right]_{\ell,i}$ be the $(\ell,i)^{th}$ element of $\widetilde{\mathbf{W}}_{\mathrm{B}}$. Using the Euler's formula, it is possible to express $\left[\widetilde{\mathbf{W}}_{\mathrm{B}}\right]_{\ell,i} = \left|\left[\widetilde{\mathbf{W}}_{\mathrm{B}}\right]_{\ell,i}\right| e^{j\phi_{\ell,i}}$. Then, according to [13], $\widetilde{\mathbf{W}}_{\mathrm{B}}$ can be decomposed into the following:

$$\begin{aligned}\widetilde{\mathbf{W}}_{\mathrm{B}} &= \left[\prod_{i=1}^{\min\{N_{\mathrm{stream}}, N_{\mathrm{A}}-1\}} \left(\mathbf{D}_i \prod_{\ell=i+1}^{N_{\mathrm{A}}} \mathbf{G}_{\ell,i}^{\top}(\psi_{\ell,i})\right)\widetilde{\mathbf{I}}\right]\widetilde{\mathbf{D}} \\ &\triangleq \widetilde{\mathbf{W}}_{\mathrm{B}}(\phi_{\ell,i}, \psi_{\ell,i})\end{aligned} \tag{5}$$

where $\widetilde{\mathbf{D}}$ is defined as $\widetilde{\mathbf{D}} = \mathrm{diag}\left(e^{j\phi_{N_{\mathrm{A}},1}}, \ldots, e^{j\phi_{N_{\mathrm{A}},N_{\mathrm{stream}}}}\right)$, $\mathbf{D}_i$ is defined as $\mathbf{D}_i = \mathrm{diag}\left(\mathbf{I}_{(i-1)}, \mathrm{diag}\left(e^{j\phi_{i,i}}, \ldots, e^{j\phi_{N_{\mathrm{A}}-1,i}}\right), 1\right)$. The details of $\mathbf{G}_{\ell,i}(\psi_{\ell,i})$ and $\psi_{\ell,i}$ are given in [12] and [14].

Instead of sending all the elements $\left[\widetilde{\mathbf{W}}_{\mathrm{B}}\right]_{\ell,i}$ in $\widetilde{\mathbf{W}}_{\mathrm{B}}$, Bob reports $\phi_{\ell,i}$ and $\psi_{\ell,i}$ to the AP. In theory, for given $\phi_{\ell,i}$ and $\psi_{\ell,i}$, the AP can reconstruct $\widetilde{\mathbf{W}}_{\mathrm{B}}$ by using (5). However, the AP cannot reconstruct the exact value of $\widetilde{\mathbf{W}}_{\mathrm{B}}$, because Bob will report the quantized versions of $\phi_{\ell,i}$ and $\psi_{\ell,i}$. Both $\phi_{\ell,i}$ and $\psi_{\ell,i}$ are quantized into $\phi_{\ell,i}^{quant}$ and $\psi_{\ell,i}^{quant}$ before being sent to the AP. Replacing $\phi_{\ell,i}$ and $\psi_{\ell,i}$ by $\phi_{\ell,i}^{quant}$ and $\psi_{\ell,i}^{quant}$ in (5), we obtain a quantized version of $\widetilde{\mathbf{W}}_{\mathrm{B}}(\phi_{\ell,i}, \psi_{\ell,i})$, which is $\mathbf{W}_{\mathrm{B}}^{quant} \triangleq \widetilde{\mathbf{W}}_{\mathrm{B}}(\phi_{\ell,i}^{quant}, \psi_{\ell,i}^{quant})$. According to [12], we have

$$\phi_{\ell,i}^{quant} = \left(2\pi/2^{b_\phi}\right)\left(1/2 + i_{\ell,i}^{\phi}\right), \tag{6}$$

$$\psi_{\ell,i}^{quant} = \left(2\pi/2^{b_\psi+2}\right)\left(1/2 + i_{\ell,i}^{\psi}\right), \tag{7}$$

where $i_{\ell,i}^{\phi} \in \{0, \ldots, 2^{b_\phi} - 1\}$ and $i_{\ell,i}^{\psi} \in \{0, \ldots, 2^{\psi} - 1\}$. Note that b_ϕ is the number of bits used for quantizing the angle $\phi_{\ell,i}^{quant}$, and b_ψ is the number of bits used for quantizing the angle $\psi_{\ell,i}^{quant}$. The values of $i_{\ell,i}^{\phi}$ and $i_{\ell,i}^{\psi}$ can be computed as follows [12, Table 9-62, p. 895], [14, eq. (13.52)]:

$$i_{\ell,i}^{\phi} = \mathrm{round}\left\{\left(\phi_{\ell,i}2^{b_\phi}\right)/(2\pi) - 1/2\right\}, \tag{8}$$

$$i_{\ell,i}^{\psi} = \mathrm{round}\left\{\left(\psi_{\ell,i}2^{b_\psi+2}\right)/(2\pi) - 1/2\right\}. \tag{9}$$

Since $i_{\ell,i}^{\phi}$ and $i_{\ell,i}^{\psi}$ are *decimal* numbers, they will be converted into *binary* numbers before being sent. Hence, $i_{\ell,i}^{\phi}$ is converted into a b_ϕ-bit binary number, while $i_{\ell,i}^{\psi}$ is converted into a b_ψ-bit binary number. Denote L as the number of binary bits used for conveying the information about the quantized angles. At Bob's side, the sequence of binary bits carrying the information about the quantized angles is $\mathcal{S}_{\mathrm{B}} = \left\{s_{\mathrm{B}}^{(1)}, s_{\mathrm{B}}^{(2)}, \ldots, s_{\mathrm{B}}^{(L)}\right\}$. Suppose that Bob uses the BPSK modulation, $\mathcal{S}_{\mathrm{B}}$ will be modulated into the following symbols:

$$\mathcal{S}_{\mathrm{B}} \xrightarrow{\text{BPSK mod.}} \left\{x_{\mathrm{B}}^{(1)}, x_{\mathrm{B}}^{(2)}, \ldots, x_{\mathrm{B}}^{(L)}\right\} \triangleq \mathcal{X}_{\mathrm{B}}, \tag{10}$$

where $x_{\mathrm{B}}^{(i)} = +\sqrt{P_{\mathrm{B}}}$ if $s_{\mathrm{B}}^{(i)} = 1$ or $x_{\mathrm{B}}^{(i)} = -\sqrt{P_{\mathrm{B}}}$ if $s_{\mathrm{B}}^{(i)} = 0$. Note that $\mathcal{X}_{\mathrm{B}}$ is placed in the high-efficiency (HE) compressed beamforming report field of an HE compressed beamforming frame [15, Section 9.6.31.2]. In 802.11ax and its predecessors, the BFF is not protected by encryption.[1] Thus, the BFF can be easily obtained after a recovery procedure.

Upon receiving the waveform from Bob, the AP will extract the data field and recover $\mathcal{X}_{\mathrm{B}}$ from the received waveform. Since there are possibly errors in the data recovery, the recovered data will be $\widehat{\mathcal{X}}_{\mathrm{B}}$. We can express $\widehat{\mathcal{X}}_{\mathrm{B}}$ as a sequence of bits, i.e., $\widehat{\mathcal{X}}_{\mathrm{B}} \triangleq \left\{\widehat{x}_{\mathrm{B}}^{(1)}, \widehat{x}_{\mathrm{B}}^{(2)}, \ldots, \widehat{x}_{\mathrm{B}}^{(L)}\right\}$. Based on $\widehat{\mathcal{X}}_{\mathrm{B}}$, the AP will reconstruct $\mathbf{W}_{\mathrm{B}}^{quant}$ as follows:

$$\widehat{\mathcal{X}}_{\mathrm{B}} \xrightarrow{\text{BPSK demod.}} \widehat{\mathcal{S}}_{\mathrm{B}} \triangleq \left\{\widehat{s}_{\mathrm{B}}^{(1)}, \widehat{s}_{\mathrm{B}}^{(2)}, \ldots, \widehat{s}_{\mathrm{B}}^{(L)}\right\} \tag{11}$$

$$\widehat{s}_{\mathrm{B}}^{(l)} \rightarrow \left\{\widehat{i}_{\ell,i}^{\phi}, \widehat{i}_{\ell,i}^{\psi}\right\} \xrightarrow{(6)-(7)} \left\{\widehat{\phi}_{\ell,i}^{quant}, \widehat{\psi}_{\ell,i}^{quant}\right\} \tag{12}$$

$$\left\{\widehat{\phi}_{\ell,i}^{quant}, \widehat{\psi}_{\ell,i}^{quant}\right\} \xrightarrow{\text{reconstructing } \mathbf{W}_{\mathrm{B}}^{quant}} \widehat{\mathbf{W}}_{\mathrm{B}}^{quant}. \tag{13}$$

If the AP attains $\widehat{\mathcal{S}}_{\mathrm{B}} = \mathcal{S}_{\mathrm{B}}$, then we have $\widehat{\mathbf{W}}_{\mathrm{B}}^{quant} = \mathbf{W}_{\mathrm{B}}^{quant}$ at the end of the above process. As a result, the AP can design the beamforming matrix $\mathbf{W}_{\mathrm{A}} = \mathbf{W}_{\mathrm{B}}^{quant}$.

[1]Encryption requires keys so that only authorized devices can access the information. By contrast, encoding does not require keys to encrypt and decrypt information. In 802.11ax, there exist channel coding schemes that are specified by the *modulation and coding scheme* (MCS) index. The information about MCS is available and accessible in the HE-SIG-A field of an HE frame.

III. BeamSteal Attack

In this section, we consider that Trudy is aware of the desired beamforming matrix of Bob. If Trudy wants to overhear the DL message of Bob, Trudy can impersonate Bob by performing the BeamSteal attack to cause the AP to mistakenly decode Bob's feedback into what Trudy wants. In doing so, Trudy can make the AP direct the beam, which is meant to be designated for Bob, to Trudy's position.

Since Trudy also receives the NDP from the AP in Phase ①, he can estimate the channel $\mathbf{h}_{\mathrm{TA}}$ and then perform the SVD on $\mathbf{h}_{\mathrm{TA}}$ to find the best beamforming matrix for him. Let $\widetilde{\mathbf{W}}_{\mathrm{T}}$ be the beamforming matrix desired/found by Trudy. Obviously, Trudy wants the AP to design $\mathbf{W}_{\mathrm{A}} = \widetilde{\mathbf{W}}_{\mathrm{T}}$ so that he gets the most of it. Since $\mathbf{W}_{\mathrm{A}}$ is determined by reconstructing $\widehat{\mathbf{W}}_{\mathrm{B}}^{quant}$, Trudy may desire $\mathbf{W}_{\mathrm{A}} = \widehat{\mathbf{W}}_{\mathrm{B}}^{quant} = \mathbf{W}_{\mathrm{T}}^{quant}$. Herein, $\mathbf{W}_{\mathrm{T}}^{quant}$ is the quantized version of the matrix $\widetilde{\mathbf{W}}_{\mathrm{T}}$ for which Trudy can compute by using the NDP in Phase ①. It is obvious that at the Trudy's side, based on $\widetilde{\mathbf{W}}_{\mathrm{T}}$, Trudy can calculate the quantized angles, then the associated angle indices, and finally the binary bit sequence $\mathcal{S}_{\mathrm{T}} = \left\{s_{\mathrm{T}}^{(1)}, s_{\mathrm{T}}^{(2)}, \ldots, s_{\mathrm{T}}^{(L)}\right\}$. The process of deriving $\mathcal{S}_{\mathrm{T}}$ from $\mathbf{h}_{\mathrm{TA}}$ is similar to the process of deriving $\mathcal{S}_{\mathrm{B}}$ from $\mathbf{h}_{\mathrm{BA}}$. Hence, for simplicity and readability, we will ignore the intermediate steps in the process of deriving $\mathcal{S}_{\mathrm{T}}$ from $\mathbf{h}_{\mathrm{TA}}$ (i.e., quantizing angles, finding angle indices and decimal-to-binary conversion will not be repeatedly discussed).

Denote $x_{\mathrm{T}}^{(i)}$ as the modulated symbol that is associated with the binary bit $s_{\mathrm{T}}^{(i)}$. Using BPSK modulation scheme, Trudy can construct the set $\mathcal{X}_{\mathrm{T}} = \left\{x_{\mathrm{T}}^{(1)}, x_{\mathrm{T}}^{(2)}, \ldots, x_{\mathrm{T}}^{(L)}\right\}$ as follows:

$$\mathcal{S}_{\mathrm{T}} \xrightarrow{\text{BPSK mod.}} \mathcal{X}_{\mathrm{T}}, \tag{14}$$

where $x_{\mathrm{T}}^{(i)} = +\sqrt{P_{\mathrm{T}}}$ if $s_{\mathrm{T}}^{(i)} = 1$, and $x_{\mathrm{T}}^{(i)} = -\sqrt{P_{\mathrm{T}}}$ if $s_{\mathrm{T}}^{(i)} = 0$.

Remark 1. *The goal of the BFF-phase is to have the AP correctly recover $\widehat{\mathcal{X}}_{\mathrm{B}} = \mathcal{X}_{\mathrm{B}}$. However, Trudy wishes to have the AP to reconstruct $\widehat{\mathcal{X}}_{\mathrm{B}} = \mathcal{X}_{\mathrm{T}}$. Unlike Bob who transmits $\mathcal{X}_{\mathrm{B}}$, Trudy does* not *transmit $\mathcal{X}_{\mathrm{T}}$ to the AP. Instead, Trudy transmits $\mathcal{E}_{spoofing}$ that is added up to Bob's signal, with the goal of making the AP reconstruct $\widehat{\mathcal{X}}_{\mathrm{B}} = \mathcal{X}_{\mathrm{T}}$. As such, $\mathcal{E}_{spoofing}$ will be built on the basis of $\mathcal{X}_{\mathrm{B}}$ and $\mathcal{X}_{\mathrm{T}}$. Figure 2 depicts the employment of the HE MIMO control field and the HE compressed beamforming report field to reduce Trudy's power consumption, while the first two fields are optional.*

Denote $\mathcal{E}_{\text{spoofing}} = \{\epsilon_{\mathrm{T}}^{(1)}, \epsilon_{\mathrm{T}}^{(2)}, \ldots, \epsilon_{\mathrm{T}}^{(L)}\}$. When Trudy sends his spoofing signal to the AP in the BFF-phase, the signal received at the n^{th} antenna of the AP can be given by

$$y_{\mathrm{A}}^{(i,n)} = \mathbf{h}_{\mathrm{AB}}^{(n)}\mathbf{f}_{\mathrm{B}}^{(n)}x_{\mathrm{B}}^{(i)} + \mathbf{h}_{\mathrm{AT}}^{(n)}\mathbf{f}_{\mathrm{T}}^{(n)}\epsilon_{\mathrm{T}}^{(i)} + n_{\mathrm{A}}^{(n)}, \tag{15}$$

where $\mathbf{h}_{\mathrm{AB}}^{(n)} \in \mathbb{C}^{1\times N_{\mathrm{B}}}$ is the uplink channel from Bob to the AP and $\mathbf{f}_{\mathrm{B}}^{(n)} \in \mathbb{C}^{N_{\mathrm{B}}\times 1}$ is the BF vector. As the pair $\left(s_{\mathrm{B}}^{(i)}, s_{\mathrm{T}}^{(i)}\right)$ belongs to the set $\{(1,1),(1,0),(0,0),(0,1)\}$, there are four possibilities as follows: if $\left(s_{\mathrm{B}}^{(i)}, s_{\mathrm{T}}^{(i)}\right) = (1,1)$, then $y_{\mathrm{A}}^{(i,n)} = \sqrt{P_{\mathrm{B}}}\mathbf{h}_{\mathrm{AB}}^{(n)}\mathbf{f}_{\mathrm{B}}^{(n)} + n_{\mathrm{A}}^{(n)}$; if $\left(s_{\mathrm{B}}^{(i)}, s_{\mathrm{T}}^{(i)}\right) = (1,0)$, then $y_{\mathrm{A}}^{(i,n)} = \sqrt{P_{\mathrm{B}}}\mathbf{h}_{\mathrm{AB}}^{(n)}\mathbf{f}_{\mathrm{B}}^{(n)} - \sqrt{P_{\mathrm{T}}}e^{j\alpha^{(i)}}\mathbf{h}_{\mathrm{AT}}^{(n)}\mathbf{f}_{\mathrm{T}}^{(n)} + n_{\mathrm{A}}^{(n)}$; if $\left(s_{\mathrm{B}}^{(i)}, s_{\mathrm{T}}^{(i)}\right) = (0,0)$, then $y_{\mathrm{A}}^{(i,n)} = -\sqrt{P_{\mathrm{B}}}\mathbf{h}_{\mathrm{AB}}^{(n)}\mathbf{f}_{\mathrm{B}}^{(n)} + n_{\mathrm{A}}^{(n)}$; if $\left(s_{\mathrm{B}}^{(i)}, s_{\mathrm{T}}^{(i)}\right) = (0,1)$, then $y_{\mathrm{A}}^{(i,n)} = -\sqrt{P_{\mathrm{B}}}\mathbf{h}_{\mathrm{AB}}^{(n)}\mathbf{f}_{\mathrm{B}}^{(n)} + \sqrt{P_{\mathrm{T}}}e^{j\alpha^{(i)}}\mathbf{h}_{\mathrm{AT}}^{(n)}\mathbf{f}_{\mathrm{T}}^{(n)} + n_{\mathrm{A}}^{(n)}$. Note that $\epsilon_{\mathrm{T}}^{(i)}$ takes the following form:

$$\epsilon_{\mathrm{T}}^{(i)} = \begin{cases} 0, & \text{if } s_{\mathrm{B}}^{(i)} = s_{\mathrm{T}}^{(i)} = 1 \text{ or } 0; \\ -\sqrt{P_{\mathrm{T}}}e^{j\alpha^{(i)}}, & \text{if } \left(s_{\mathrm{B}}^{(i)}, s_{\mathrm{T}}^{(i)}\right) = (1,0); \\ +\sqrt{P_{\mathrm{T}}}e^{j\alpha^{(i)}}, & \text{if } \left(s_{\mathrm{B}}^{(i)}, s_{\mathrm{T}}^{(i)}\right) = (0,1). \end{cases} \tag{16}$$

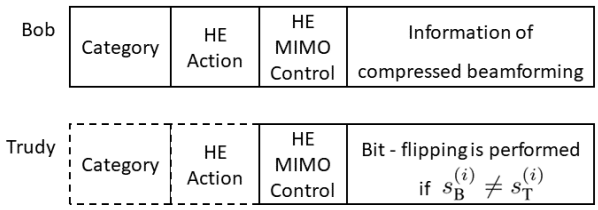

Fig. 2: An illustration of Bob's and Trudy's frames in the BFF-phase. Herein, HE stands for high efficiency. In the last field, the bits sent by Trudy are designed based on the difference between $\mathcal{S}_{\mathrm{B}}$ and $\mathcal{S}_{\mathrm{T}}$.

A. Methodology of Trudy

In the case of $\left(s_{\mathrm{B}}^{(i)}, s_{\mathrm{T}}^{(i)}\right) = (1,0)$, to deceive the AP into thinking that Bob sends bit 0, Trudy may need

$$y_{\mathrm{A}}^{(i,n)} = \underbrace{-\sqrt{P_{\mathrm{B}}}\mathbf{h}_{\mathrm{AB}}^{(n)}\mathbf{f}_{\mathrm{B}}^{(n)} + n_{\mathrm{A}}^{(n)}}_{\text{The AP can mistakenly decode } s_{\mathrm{B}}^{(i)}=0.} \tag{17}$$

Herein, the right hand side of (17) looks like $s_{\mathrm{B}}^{(i)} = 0$ is sent by Bob, but it is not the case. The idea is that Trudy sends something to make the received signal $y_{\mathrm{A}}^{(i,n)}$ at the AP look like the right hand side of (17). Using the appropriate value of $y_{\mathrm{A}}^{(i,n)}$, we can rewrite (17) as follows:

$$\sqrt{P_{\mathrm{T}}}e^{j\alpha^{(i)}} = 2\sqrt{P_{\mathrm{B}}}\mathbf{h}_{\mathrm{AB}}^{(n)}\mathbf{f}_{\mathrm{B}}^{(n)}/(\mathbf{h}_{\mathrm{AT}}^{(n)}\mathbf{f}_{\mathrm{T}}^{(n)}). \tag{18}$$

Similarly, in the case of $\left(s_{\mathrm{B}}^{(i)}, s_{\mathrm{T}}^{(i)}\right) = (0,1)$, Trudy can also find the same design as (18).

Without the knowledge of $\mathbf{h}_{\mathrm{AB}}^{(n)}$ and $\mathbf{f}_{\mathrm{B}}^{(n)}$, Trudy cannot compute the transmit power P_{T} and the angle $\alpha^{(i)}$ correctly. From a practical viewpoint, Trudy may rely on his guesswork to construct a suitable attack strategy as presented below.

Trudy's guesswork: Trudy knows that when Bob transmits, the term $|\mathbf{h}_{\mathrm{AB}}^{(n)}\mathbf{f}_{\mathrm{B}}^{(n)}|^2$ will appear in the received SNR expression at the AP. Thus, Trudy may guess that Bob will use $\mathbf{f}_{\mathrm{B}}^{(n)} = \frac{\mathbf{h}_{\mathrm{AB}}^{(n)\dagger}}{\|\mathbf{h}_{\mathrm{AB}}^{(n)}\|}$ to maximize the term $|\mathbf{h}_{\mathrm{AB}}^{(n)}\mathbf{f}_{\mathrm{B}}^{(n)}|^2$. Obviously, Trudy is aware that Bob (i.e., the legitimate sender) may want to maximize the received SNR at the AP (i.e., the receiver). Using the Cauchy-Schwarz inequality, Trudy can analyze $|\mathbf{h}_{\mathrm{AB}}^{(n)}\mathbf{f}_{\mathrm{B}}^{(n)}|^2$ as follows:

$$|\mathbf{h}_{\mathrm{AB}}^{(n)}\mathbf{f}_{\mathrm{B}}^{(n)}|^2 \leq \|\mathbf{h}_{\mathrm{AB}}^{(n)}\|^2\|\mathbf{f}_{\mathrm{B}}^{(n)}\|^2. \tag{19}$$

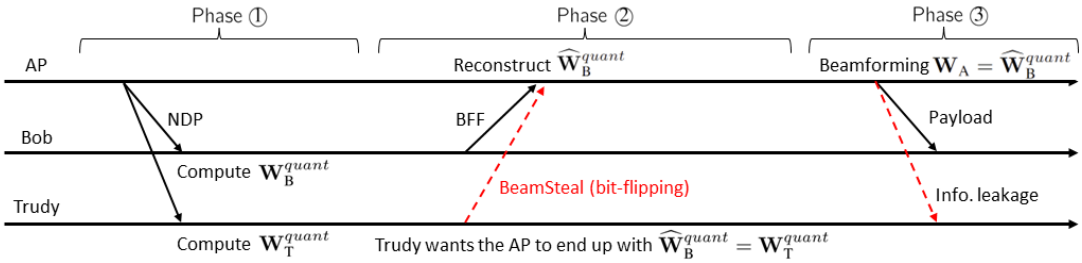

Fig. 3: An illustration of the BeamSteal attack. In the BFF-phase (i.e., in Phase ②), Trudy deceives the AP into thinking that $\mathcal{X}_{\mathrm{T}}$ is transmitted by Bob. Once the AP mistakenly demodulates $\widehat{\mathcal{X}}_{\mathrm{B}} = \mathcal{X}_{\mathrm{T}}$, it will lead to $\widehat{\mathbf{W}}_{\mathrm{B}}^{quant} = \mathbf{W}_{\mathrm{T}}^{quant}$. As a result, in the next phase (i.e., in Phase ③), the AP will design $\mathbf{W}_{\mathrm{A}} = \widehat{\mathbf{W}}_{\mathrm{B}}^{quant}$, which will steer the beam towards the Trudy's position.

Trudy supposes that Bob wants the equality to occur so that $|\mathbf{h}_{\mathrm{AB}}^{(n)}\mathbf{f}_{\mathrm{B}}^{(n)}|^2$ is maximized. As mentioned earlier, Trudy guesses $\mathbf{f}_{\mathrm{B}}^{(n)} = \frac{\mathbf{h}_{\mathrm{AB}}^{(n)\dagger}}{\|\mathbf{h}_{\mathrm{AB}}^{(n)}\|}$, thus the equality in (19) occurs, which leads to $\|\mathbf{h}_{\mathrm{AB}}^{(n)}\mathbf{f}_{\mathrm{B}}^{(n)}\|^2 = \|\mathbf{h}_{\mathrm{AB}}^{(n)}\|^2$. From Trudy's perspective, he also wants to maximize his contribution in the received SNR expression at the AP, thus he can design $\mathbf{f}_{\mathrm{T}}^{(n)} = \frac{\mathbf{h}_{\mathrm{AT}}^{(n)\dagger}}{\|\mathbf{h}_{\mathrm{AT}}^{(n)}\|}$, which leads to $\left|\mathbf{h}_{\mathrm{AT}}^{(n)}\mathbf{f}_{\mathrm{T}}^{(n)}\right|^2 = \|\mathbf{h}_{\mathrm{AT}}^{(n)}\|^2$. As a result, (18) becomes

$$\begin{cases} P_{\mathrm{T}} = 4P_{\mathrm{B}}\|\mathbf{h}_{\mathrm{AB}}^{(n)}\|^2/\|\mathbf{h}_{\mathrm{AT}}^{(n)}\|^2; \\ \alpha^{(i)} = \measuredangle\left(\|\mathbf{h}_{\mathrm{AB}}^{(n)}\|/\|\mathbf{h}_{\mathrm{AT}}^{(n)}\|\right) = 0 \text{ for } \forall i \text{ and } \forall n. \end{cases} \tag{20}$$

Noticeably, $\alpha^{(i)} = 0$ is independent of $\mathbf{h}_{\mathrm{AB}}^{(n)}$, simply because the angle of a real positive number is equal to 0. Hence, regardless of the knowledge of $\mathbf{h}_{\mathrm{AB}}^{(n)}$, Trudy can design $\alpha^{(i)} = 0$. On the other hand, the knowledge of $\mathbf{h}_{\mathrm{AB}}^{(n)}$ is still required for designing P_{T} in (20). To overcome this difficulty, Trudy simply designs $P_{\mathrm{T}} = \xi P_{\mathrm{B}}$, where ξ is a positive value. Herein, ξ can be adjusted by Trudy to attain desired performance. Substituting $P_{\mathrm{T}} = \xi P_{\mathrm{B}}$ and $\alpha^{(i)} = 0$ into (16), Trudy easily obtains the specific value of $\epsilon_{\mathrm{T}}^{(i)}$ as well as the specific value of the transmit signal $\mathcal{E}_{\text{spoofing}} = \{\epsilon_{\mathrm{T}}^{(1)}, \epsilon_{\mathrm{T}}^{(2)}, \ldots, \epsilon_{\mathrm{T}}^{(L)}\}$.

IV. Numerical Results

In this section, numerical results are presented to demonstrate the BeamSteal attack. Unless otherwise stated, the default system parameters are shown in Table I. Three different cases are compared to each other: i) no-attack; ii) BeamSteal attack; and iii) jamming attack. Note that the jamming attack is briefly summarized below.

Jamming attack: This is the benchmark scheme, where Trudy performs a jamming attack during the BFF phase in order to interfere with the reception process at the AP in Phase ②. Herein, the jamming case is similar to Figure 3 but the attack is jamming instead of BeamSteal. The main difference lies in the attack type conducted in the BFF phase, which will result in the difference in the performance in Phase ③. For comparison, we consider that the transmit power of the jamming signal is the same as that of the spoofing signal.

In Figure 4, we depict the PERs at Bob versus P_A/N_0, concerning different values of the power ratio ξ. To be more specific, in the first sub-figure, the no-attack case is compared with the BeamSteal cases ($\xi = 2$ and $\xi = 6$). The first sub-figure shows that the PER at Bob increases with ξ and thus, the decoding process at Bob is more prone to errors. Meanwhile,

TABLE I: Default system parameters.

Parameters	Values
Channel bandwidth	20 MHz
Carrier frequency	5.25 GHz
Sample rate	20×10^6
Delay profile	Model-B
Distance between the AP and Bob	$5\ m$
Distance between the AP and Trudy	$8\ m$
Number of antennas at the AP	$N_{\mathrm{A}} = 4$
Number of streams	$N_{\text{stream}} = 1$
MCS in Phase ① and Phase ③	3
MCS in Phase ②	0
Channel coding	LDPC
Number of sub-carriers	242
FFT length	256
Guard interval (cyclic prefix) duration	$3.2\ \mu s$
Number of bits used for quantizing an angle of ϕ-type	$b_\phi = 4$
Number of bits used for quantizing an angle of ψ-type	$b_\psi = 2$

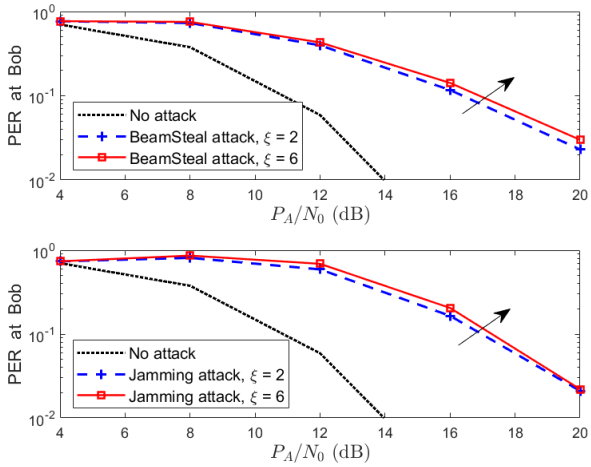

Fig. 4: PERs at Bob are depicted against P_A/N_0 for different cases. The above sub-figure compares the no-attack case with the proposed BeamSteal, while the below sub-figure compares the no-attack case with the jamming attack.

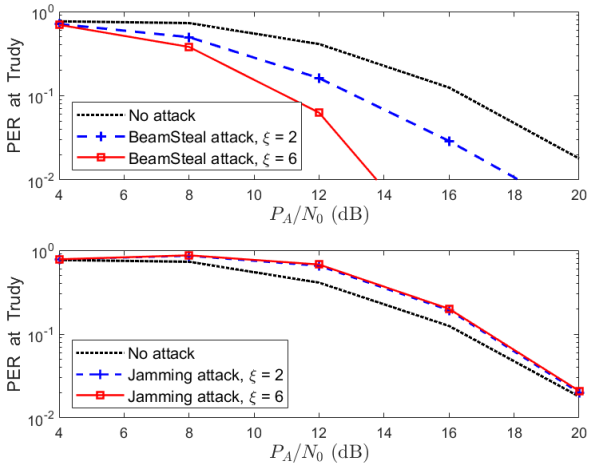

Fig. 5: PERs at Trudy are depicted against P_A/N_0 for different cases. The above sub-figure compares the no-attack case with the BeamSteal, while the below sub-figure compares the no-attack case with the jamming attack.

the second sub-figure compares the no-attack case with the jamming cases ($\xi = 2$ and $\xi = 6$). It is quite clear that when Trudy increases the jamming power, the PER at Bob also gets worse. In short, a higher value of ξ will worsen the decoding process at Bob, whether Trudy performs the jamming attack or the proposed BeamSteal attack.

In Figure 5, we illustrate the PER at Trudy versus P_A/N_0, concerning different values of ξ. Particularly, in the first sub-figure, the no-attack case is compared with the BeamSteal attack. This sub-figure shows that the PER at Trudy is substantially improved when ξ increases. This is to say, if Trudy performs the BeamSteal attack with a higher value of ξ, Trudy has a higher percentage of receiving the Bob's information in Phase ③, because Trudy has a higher chance of deceiving the AP to steer the beam towards his location. On the other hand, in the second sub-figure, we compare the no-attack case with the jamming case. It can be seen that if Trudy performs the jamming attack, the PER at Trudy may not be improved. This is because the jamming attack spoils the information processing at the AP but does not improve anything for Trudy.

V. Conclusions

In this paper, we revealed a security threat in WiFi-supported systems. Taking advantage of the vulnerability of the BFF, a potential attacker, Trudy, impersonates a legitimate user (i.e., Bob) by performing the BeamSteal attack (in Phase ② of the WiFi protocol) to make the AP steer the beams toward Trudy (in Phase ③) and thus helping Trudy to steal more information. Furthermore, we have also considered a more dangerous attack type, where Trudy respectively conducts the BeamSteal attacks and the jamming ones in Phase ② and Phase ③. While the BeamSteal attacks are aimed at the AP for steering the beams towards Trudy and helping Trudy to steal more information, the jamming attacks are aimed at Bob for confusing the reception process at Bob. Indeed, we have shown that by performing the BeamSteal attack, Trudy can reduce his PER significantly, demonstrating Trudy's success in stealing Bob's beams. On the other hand, if Trudy introduces the jamming attack, Trudy can only cause Bob to be unable to decode his information. Finally, this paper serves as a demonstration of the insecure nature of the BFF due to the lack of encryption. Thus, encryption methods should be integrated into the BFF designs in the next-generation WiFi standards. Additionally, along with the security at the upper layers, PHY security solutions should be further addressed to deal with the attacks at the PHY layer in the near future. Such a PHY security solution may rely on the randomness of channels and other physical aspects of wireless propagation.

References

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. on Sel. Areas in Commun.*, vol. 36, no. 4, pp. 679–695, 2018.

[2] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in *IEEE INFOCOM 2008 - The 27th Conf. on Computer Commun.*, 2008, pp. 1768–1776.

[3] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proc. of the third ACM conf. on Wirel. netw. sec.*, 2010, pp. 89–98.

[4] S. Prasad and D. J. Thuente, "Jamming attacks in 802.11g - a cognitive radio based approach," in *MILCOM 2011 Military Commun. Conf.*, 2011, pp. 1219–1224.

[5] B. Bloessl, C. Sommer, F. Dressler, and D. Eckhoff, "The scrambler attack: A robust physical layer attack on location privacy in vehicular networks," in *2015 Int. Conf. on Comp., Netw. and Commun. (ICNC)*, 2015, pp. 395–400.

[6] H. Rahbari and M. Krunz, "Exploiting frame preamble waveforms to support new physical-layer functions in OFDM-based 802.11 systems," *IEEE Trans. on Wirel. Commun.*, vol. 16, no. 6, pp. 3775–3786, 2017.

[7] X. Zhang and E. W. Knightly, "CSIsnoop : Inferring channel state information in multi-user MIMO WLANs," *IEEE/ACM Trans. on Networking*, vol. 27, no. 1, pp. 231–244, 2019.

[8] S. Itahara, S. Kondo, K. Yamashita, T. Nishio, K. Yamamoto, and Y. Koda, "Beamforming feedback-based model-driven angle of departure estimation toward legacy support in WiFi sensing: An experimental study," *IEEE Access*, vol. 10, pp. 59 737–59 747, 2022.

[9] A. Niakanlahiji, S. Orlowski, A. Vahid, and J. H. Jafarian, "Toward practical defense against traffic analysis attacks on encrypted DNS traffic," *Computers & Security*, vol. 124, p. 103001, 2023.

[10] E. Jeon, W. B. Lee, M. Ahn, S. Kim, and J. Kim, "Adaptive feedback of the channel information for beamforming in IEEE 802.11ax WLANs," in *2019 IEEE 90th Veh. Tech. Conf. (VTC2019-Fall)*, 2019, pp. 1–6.

[11] C. Iloki, M. Mbaye, and M. Diallo, "Feedback of the channel information for transmit beamforming in WLAN," in *2015 9th European Conf. on Antennas and Propagation (EuCAP)*, 2015, pp. 1–6.

[12] "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," *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)*, pp. 1–4379, 2021.

[13] J. Kim and C. Aldana, "Efficient feedback of the channel information for closedloop beamforming in WLAN," in *2006 IEEE 63rd Veh. Tech. Conf.*, vol. 5, 2006, pp. 2226–2230.

[14] E. Perahia and R. Stacey, *Next generation wireless LANs: 802.11 n and 802.11 ac*. Cambridge University Press, 2013.

[15] "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)*, pp. 1–767, 2021.