Orthogonality-Sabotaging Attacks against OFDMA-based Wireless Networks

Shangqing Zhao, Zhuo Lu, Zhengping Luo and Yao Liu
University of South Florida, Tampa, FL 33620
Emails: {shangqing@mail., zhuolu@, zhengpingluo@mail., yliu@cse.}usf.edu.

***Abstract*—Wireless jamming remains as one of the primary threats towards wireless security. Traditionally, jamming is able to disrupt wireless signals within, but not beyond, its covered bandwidth. In this paper, we propose a novel attack strategy, called orthogonality-sabotaging attack, against orthogonal frequency division multiple access (OFDMA) that has been widely adopted in today's wireless network standards (e.g., 4G/5G and 802.11ax). The attack intentionally introduces an unaligned narrowband jamming signal to an OFDMA network so as to destroy the orthogonality among all subcarriers in broadband signals. We theoretically formulate and optimize the attack strategies, and then use real-world experiments to show that orthogonality sabotaging is very efficient and can take down an 802.11ax network with only 1/5–1/4 of the full network bandwidth. Finally, we propose an attack identification and localization method to identify and localize orthogonality-sabotaging attacks in the full-band spectrum with 92% overall accuracy and localization errors within about 0.4 subcarrier spacing in experiments.**

I. Introduction

Today's broadband wireless networks are still susceptible to jamming attacks [1]–[3], which broadcast radio frequency (RF) interference to disrupt wireless communications among network users. Although wireless jamming attacks have been well investigated regarding attack strategies [4], [5], attack detection [6]–[9], and spread spectrum based defense [10]–[12], we notice that among most studies, a common assumption about a wireless jammer is that the jamming signal cannot affect the wireless spectrum beyond what the jammer can cover. This has served as a foundation for many defense designs. For example, frequency hopping based schemes [10], [11] chooses the frequency channels for communication, which a jammer does not cover given its limited transmission bandwidth.

However, this paper shows that the assumption is not necessarily true under orthogonal frequency-division multiplexing (OFDM) and its multi-user version orthogonal frequency-division multiple access (OFDMA). Due to their spectrum efficiency, both OFDM and OFDMA have become the primary technologies in broadband wireless standards to support high data throughput and robustness in multipath fading environments. OFDM has been adopted by existing WiFi standards (e.g., 802.11a/g/n/ac) for years, and the incoming 802.11ax standard will further use OFDMA in its uplink multi-user communications [13]. In addition, 4G/5G cellular standards also rely on OFDMA for their air-interfaces [14], [15].

We design and develop a new attack strategy, called orthogonality-sabotaging attack, against the OFDMA-based wireless networks which adopt the OFDM or OFDMA technology. Given only a limited bandwidth covering the spacing of a few subcarriers, the orthogonality-sabotaging attack can substantially disrupt the full-band communication in a wireless network. In other words, we show that in contrast to the widely-adopted assumption of the jamming capability, a carefully-designed narrowband jamming signal can indeed take down broadband wireless communications. This in turn renders an asymmetric advantage of security attacks over designers in wireless networks.

The design intuition of such an attack is, as its name indicates, to destroy the orthogonality among all subcarriers used in OFDMA networks. We do so by constructing a narrowband signal with a central frequency shift which is intentionally unaligned to all subcarriers. Although the spectrum of the narrowband attack signal only overlaps a limited number of subcarrier spectrums, the attack-induced frequency shift will break the orthogonality to all subcarriers and cause interferences to each of them during the essential fast Fourier transform (FFT) procedure for OFDM/OFDMA.

We define and formulate the orthogonality-sabotaging attack, and investigate two real-world attack strategies against OFDMA systems: 1) continuous-subcarrier attack that has a continuous, narrowband jamming signal spectrum and 2) scattered-subcarrier attack that can contain multiple narrowband attacks, yielding a scattered jamming signal spectrum. We develop the optimal attack strategy and use USRP X300s to setup an 802.11ax network to validate our analysis and show the real-world impact of orthogonality sabotaging in wireless networks. We also measure the impact of the attack strategies on commercial off-the-shelf (COTS) 802.11ac products. Our contributions can be summarized as follows.

We propose a new attack mechanism, orthogonality sabotaging, against OFDMA based wireless networks. We systematically formulate two attack strategies and investigate the impact of orthogonality sabotaging. We perform real-world experiments on USRP X300 based 802.11ax testbeds and commercial 802.11ac products. Experimental results show that orthogonality sabotaging is more effective than traditional narrowband jamming and is able to disrupt the OFDMA signal with a bandwidth 400%–500% broader than the attacker's. We propose an attack identification and localization method to identify and localize orthogonality-sabotaging attacks in the full-band spectrum with 92% accuracy and localization errors within about 0.4 subcarrier spacing in experiments.

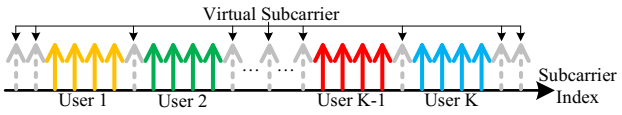

Fig. 1. OFDMA example with a typical user and subcarrier distribution in 802.11ax.

The systematic study in this paper serves as the first work to analyze the impact of narrowband orthogonality-sabotaging attacks on a broadband OFDM/OFDM-based WiFi system. The attack strategy can be easily extended to other OFDM/OFDMA based wireless networks such as 4G/5G cellular systems. Our work serves as the first work to analyze the impact of narrowband orthogonality-sabotaging attacks on a broadband OFDMA system, and points out that an attacker can manipulate its signal to have a larger effective bandwidth than traditional narrowband jamming. In addition, our attack approach is orthogonal to recent smart jamming strategies (e.g., jamming physical-layer preambles [2], [16]). Hence, orthogonality sabotaging can be integrated with these existing strategies to make jamming attacks even more efficient.

II. OFDMA Wireless Networks

In this section, we briefly introduce the OFDMA network model and communication process.

A. OFDMA Network Model

We consider an OFDMA based uplink wireless network (e.g. 802.11ax) with K active users and N subcarriers. When $K = 1$, the system becomes the traditional OFDM system. Hence, OFDM is considered as a special case of OFDMA in this paper. Among the N subcarriers, there are M data subcarriers used for data transmission and $N - M$ virtual subcarriers (i.e., the subcarriers without data) located in the guard bands used to separate different users (e.g., the dashed lines in Fig. 1). Define by $\mathcal{M}$ the set of all data subcarriers. By leveraging the trigger frame, L_k data subcarriers are assigned to user k with the index set $\mathcal{M}_k = \{m_0^{(k)}, m_1^{(k)}, \cdots, m_{L_k-1}^{(k)}\}$. The superscript $(\cdot)^{(k)}$ denotes user k. To avoid inter-user interference, OFDMA assigns subcarriers to users such that $\mathcal{M}_k \cap \mathcal{M}_j = \phi$ and $\cup_{i=1}^{K} \mathcal{M}_k = \mathcal{M}$,for any pair of k, j with $1 \leq k \neq j \leq K$ and ϕ is the empty set.

B. OFDMA Data Communication

Let $[X_0^{(k)}, X_1^{(k)}, \cdots, X_{L_k-1}^{(k)}]$ be the L_k data modulation symbols at the physical layer of user k to be transmitted within an OFDMA block. Before transmitting, user k projects the modulation symbols onto the user's own subcarriers and nulls other subcarriers; i.e., the L_k modulation symbols are interpolated into N symbols $\{S_i^{(k)}\}_{0 \leq i \leq N-1}$, where $S_i^{(k)} = X_j^{(k)}$ if there exists j such that $i = m_j^{(k)} \in \mathcal{M}_k$ and is 0 otherwise.

Then, the OFDMA block with N symbols is transformed from the frequency domain to the time domain by N-point inverse FFT (IFFT). The n-th $(0 \leq n \leq N-1)$ output sample of IFFT for user k can be written as $x_n^{(k)} = 1/\sqrt{N} \sum_{i=0}^{N-1} S_i^{(k)} e^{j2\pi ni/N}$,which will be up-converted into the RF signal. All users' RF signals will be aggregated in the wireless channel and transmitted to the receiver. Upon receiving the signal, the receiver down-converts the aggregated RF signal to the baseband signal, then the received n-th time-domain signal can be written as $y_n = 1/\sqrt{N} \sum_{k=1}^{K} \sum_{i=0}^{N-1} S_i^{(k)} H_i^{(k)} e^{j2\pi ni/N} + w_n$,where $H_i^{(k)}$ denotes the frequency-domain channel response between user k and the receiver on subcarrier i; w_n is the additive white Gaussian noise (AWGN) with zero mean and variance δ^2. Let W_i be FFT of w_n, then the receiver uses the FFT operation to convert the signal from the time domain to the frequency domain. The received frequency-domain symbols Y_i $(0 \leq i \leq N-1)$ on subcarrier i within an OFDMA block is

$$Y_i = \sum_{k=1}^{K} S_i^{(k)} H_i^{(k)} + W_i. \tag{1}$$

III. Orthogonality-Sabotaging Attacks

In this section, we first introduce the attack intuition. Then, we formulate the attack strategies.

A. Intuition behind Orthogonality Sabotaging

To disrupt wireless transmissions, conventional jamming attacks usually cover the full bandwidth of the communication signal such that the overall receiving signal-to-interference-plus-noise ratio (SINR) at the receiver is lower than the decoding threshold. A narrowband jamming is generally considered not effective to disrupt a broadband signal because the jamming power on the narrowband spectrum averaged on the full-band spectrum may not garner enough SINR to take down the broadband signal under error-correction mechanisms [17].

Our objective is to design a smart attack mechanism that leverages a narrowband jamming signal to disrupt the broadband OFDMA based WiFi signal. To this end, we first notice that the OFDMA decoding relies on the fact that the interval between any pair of subcarriers is exactly a multiple of the subcarrier bandwidth to maintain orthogonality during the FFT process at the receiver [18]. If an attacker intentionally transmits a jamming signal spanning one or more subcarriers with unaligned central frequency to all other subcarriers, the jamming signal will break the orthogonality and result in interference to all subcarriers on the full-band spectrum.

To elaborate, we evaluate and compare the impacts of the basic strategies of both exact subcarrier jamming attack and orthogonality-sabotaging attack.

1) Exact Subcarrier Jamming Attack: We first consider the exact subcarrier jamming attack that transmits a jamming signal on exactly one particular subcarrier. Suppose the attacker wishes to jam subcarrier m. Denoted by $S_m^{(a)}$ the transmitted symbol of the attacker on subcarrier m. As it only targets subcarrier m, the n-th transmitted time-domain jamming signal from the attacker can be represented as

$$x_n^{(a)} = (1/\sqrt{N}) S_m^{(a)} e^{j2\pi nm/N}. \tag{2}$$

All users' signals and the jamming signal will be transmitted to the receiver. Based on (1), the aggregated frequency-domain signal on subcarrier i at the receiver under jamming is

$$Y_i = \begin{cases} \sum_{k=1}^{K} S_i^{(k)} H_i^{(k)} + W_i, & \text{if } i \neq m \\ \sum_{k=1}^{K} S_i^{(k)} H_i^{(k)} + W_i + \underbrace{S_i^{(a)} H_i^{(a)}}_{\text{jamming interference}}, & \text{if } i = m, \end{cases} \tag{3}$$

where $H_i^{(a)}$ is the channel response from the jammer to the receiver. We can see from (3) that the jamming interference part exists only when $i = m$, which means that the attacker can only jam subcarrier m, and lead to zero impact on any other subcarrier.

2) Orthogonality-Sabotaging Attack: Then, we define a very basic orthogonality-sabotaging attack based on the exact subcarrier jamming attack. We intentionally shift the central frequency of the exact subcarrier jamming attack by $\varepsilon_m^{(a)} \in [-0.5, 0.5]$, which is called the attacker's normalized frequency shift (i.e., the actual frequency shift divided by the bandwidth of a subcarrier). Based on (2), the n-th time-domain jamming signal with the frequency shift $\varepsilon_m^{(a)}$ is

$$x_n^{(a)} = (1/\sqrt{N}) S_m^{(a)} e^{j\frac{2\pi\left(\varepsilon_m^{(a)}+m\right)n}{N}}. \tag{4}$$

At the receiver, the corresponding frequency-domain signal on subcarrier i, after FFT, can be represented as

$$Y_i = \sum_{k=1}^{K} S_i^{(k)} H_i^{(k)} + W_i + \underbrace{S_m^{(a)} H_m^{(a)} I(i, m, \varepsilon_m^{(a)})}_{\text{jamming interference}}, \tag{5}$$

for any $0 \leq i \leq N-1$, where $I(i, m, \varepsilon_m^{(a)})$ satisfies

$$I(i, m, \varepsilon_m^{(a)}) = \frac{1}{N} \sum_{n=0}^{N-1} e^{j\frac{2\pi\left((i-m)+\varepsilon_m^{(a)}\right)n}{N}}, \tag{6}$$

and reflects the jamming interference on subcarrier i.

Taking a closer look at (6), we can notice that for any $0 \leq i \leq N-1$ and $\varepsilon_m^{(a)} \neq 0$, $I(i, m, \varepsilon_m^{(a)}) \neq 0$; i.e., the attack-induced frequency shift breaks the orthogonality among all aligned subcarriers during FFT and leads to interference on all of them. Therefore, despite having the same bandwidth with exact subcarrier jamming, the interference impact of the orthogonality-sabotaging attack universally exists on all subcarriers, rather than only on subcarrier m.

In conventional OFDM communication systems, the frequency mismatch between the transmitter and the receiver can lead to inter-carrier interference (ICI) [2] similar to (6). However, the frequency mismatch can be corrected by frequency synchronization [19] such that the ICI impact becomes negligible. In contrast, the frequency shift introduced maliciously by an attacker can be significantly larger and not correctable, thereby causing damage to all subcarriers.

B. Attack Formulation and Strategies

Given the fact that jamming signals with malicious frequency shifts can sabotage the orthogonality of OFDMA signals, the goal of a narrowband attacker is to find the optimal frequency shift to maximize its impact on all subcarriers in the full-band spectrum. In the following, we formulate the orthogonality-sabotaging attack and its objective.

1) Attack Formulation: Defined by $\mathcal{M}_a$ the subcarrier set used by the attacker. The size of $\mathcal{M}_a$ is written as $L_a = |\mathcal{M}_a|$. Also denote by $S_m^{(a)}$ and $\varepsilon_m^{(a)}$ the attacker's transmitted symbol and the intentional frequency shift on subcarrier $m \in \mathcal{M}_a$, respectively. Similar to the simple case in (5), the received frequency-domain signal on subcarrier i after FFT can be represented as

$$Y_i = \underbrace{\sum_{k=1}^{N} S_i^{(k)} H_i^{(k)}}_{\text{signal}} + \underbrace{\sum_{m \in \mathcal{M}_a} S_m^{(a)} H_m^{(a)} I(i, m, \varepsilon_m^{(a)})}_{\text{jamming interference}} + W_i, \tag{7}$$

where the first term is the users' signals through the wireless channel; the second represents the overall jamming interference from the attacker; and the last term denotes noise.

Because the decoding performance relies dominantly on the SINR on each subcarrier at the receiver. It follows from (7) that under a random wireless fading channel with normalized channel responses [20], the SINR on subcarrier i satisfies

$$\text{SINR}_i = \Big(\sum_{k=1}^{N} P_i^{(k)}\Big) / (\Psi_i + \delta^2), \tag{8}$$

where $P_i^{(k)} = \mathbb{E}|S_i^{(k)}|^2$ is the transmit power of user k on subcarrier i, δ^2 is the noise power, and Ψ_i denotes the total jamming interference on subcarrier i and is written as

$$\Psi_i = \sum_{m \in \mathcal{M}_a} P_m^{(a)} |I(i, m, \varepsilon_m^{(a)})|^2, \tag{9}$$

with $P_m^{(a)} = \mathbb{E}|S_m^{(a)}|^2$ being the attacker's transmit power on subcarrier m and $I(i, m, \varepsilon_m^{(a)})$ satisfying (6).

By nature, a user's signal on a subcarrier cannot be correctly decoded if the SINR on the subcarrier is less than a decoding threshold β, which is usually around 10 dB (depending on a practical network system), such as 10-15 dB for WiFi networks [21]. As a result, we formulate the attacker's objective as manipulating the frequency shift $\varepsilon_m^{(a)}$ on each subcarrier $m \in \mathcal{M}_a$ to maximize the number of subcarriers with SINR below the threshold β, i.e.,

$$\text{Objective: } \max_{\{\varepsilon_m^{(a)}\}_{m \in \mathcal{M}_a}} \sum_{i=1}^{N} \mathbf{1}_{\{\text{SINR}_i < \beta\}}, \tag{10}$$

where $\mathbf{1}_{\{\text{SINR}_i < \beta\}}$ is the indicator function defined as

$$\mathbf{1}_{\{\text{SINR}_i < \beta\}} = \begin{cases} 1, & \text{if SINR}_i < \beta \\ 0, & \text{otherwise.} \end{cases} \tag{11}$$

In addition, the attacker can also target a particular user k to maximize the total number of corrupted subcarriers assigned to user k, i.e.,

$$\text{Objective (target user } k\text{): } \max_{\{\varepsilon_m^{(a)}\}_{m \in \mathcal{M}_a}} \sum_{i \in \mathcal{M}_k} \mathbf{1}_{\{\text{SINR}_i < \beta\}}, \tag{12}$$

where M_k is the set of user k's subcarriers and $L_k = |\mathcal{M}_k|$.

2) Optimizing Orthogonality-Sabotaging Attacks: Given $\mathcal{M}_a$, the attacker must find the corresponding set of frequency shifts $\{\varepsilon_m^{(a)}\}_{m\in\mathcal{M}_a}$ in (10) to maximize the attack impact. We state the main result as follows.

Theorem 1 (Optimal Frequency Shifts): When N goes to infinity (i.e., $N \to \infty$), the objective function (10) is maximized when $\varepsilon_m^{(a)}$ is 0.5 or -0.5 for all $m \in \mathcal{M}_a$.

Proof: Let $L = \sum_{i=1}^{N} \mathbf{1}_{\{\text{SINR}_i<\beta\}}$. First, notice that L is a monotonically decreasing function of SINR_i. According to (8) and (9), SINR_i is a monotonically decreasing function of the total jamming interference $|I(i,m,\varepsilon_m^{(a)})|^2$ on subcarrier i. Overall, L is a monotonically increasing function of $|I(i,m,\varepsilon_m^{(a)})|^2$. If $N \to \infty$, it holds for $|I(i,m,\varepsilon_m^{(a)})|^2$ that

$$\lim_{N\to\infty} |I(i,m,\varepsilon_m^{(a)})|^2 = \text{sinc}(\pi(m-i+\varepsilon_m^{(a)})^2, \tag{13}$$

where $\text{sinc}(x)$ is the sinc function defined as

$$\text{sinc}(x) = \sin(x)/x. \tag{14}$$

When $\varepsilon_m^{(a)} = 0$, it is clear that $L = |\mathcal{M}_a|$ because the attack becomes exact subcarrier jamming.

When $\varepsilon_m^{(a)} \neq 0$, we first show that $L \geq |\mathcal{M}_a|$. In this case, for $m \in \mathcal{M}_a$, the majority of the jamming signal spectrum still occupies subcarrier m and the total jamming interference level on subcarrier m is denoted as $\text{sinc}(\pi\varepsilon_m^{(a)})^2$ based on (13).

Based on the property of the sinc function, the minimum of $\text{sinc}(\pi\varepsilon_m^{(a)})^2$ is 0.4053 when $\varepsilon_m^{(a)} = \pm 0.5$. According to (8), we can show that the maximum SINR on subcarrier m is at most 3.9 dB (if the jamming power is no less than the users' transmit power), which is below the decoding SINR threshold β in real-world wireless networks (e.g., β=10-15 dB in WiFi networks [21]). As a result, despite the fact that $\varepsilon_m^{(a)} = \pm 0.5$ maximizes the SINR on subcarrier m, the decoding on subcarrier m still cannot succeed. Therefore, we obtain $L \geq |\mathcal{M}_a|$ when $\varepsilon_m^{(a)} = \pm 0.5$.

As L is a monotonically increasing function of (13), it then suffices to show that $\varepsilon_m^{(a)} = \pm 0.5$ maximizes (13) for all $m \neq i$. According to the property of function $\text{sinc}(x)$, it has local maximum values when x is $\pm 1.5\pi$, $\pm 2.5\pi$, $\pm 3.5\pi$, $\pm 4.5\pi$, $\cdots$. Hence, $\pi(m-i+\varepsilon_m^{(a)})$ in (13) achieves the maximum when $\varepsilon_m^{(a)} = \pm 0.5$ for any pair of m and i with $m \neq i$. This completes the proof. □

The result in Theorem 1 shows that an attacker should always choose the half-subcarrier frequency shift to maximize its damage to the wireless network performance.

3) Real-World Attack Strategies: In practice, an attacker can choose different strategies to transmit the jamming signal. Based on $\mathcal{M}_a$, we consider two attack strategies to sabotage the orthogonality in real-world OFDMA scenarios.

1) Continuous-subcarrier attack if $\mathcal{M}_a$ contains only a sequence of continuous subcarrier indices. It means that a narrowband attacker can only cover a continuous subcarrier subset of the full OFDMA spectrum.
2) Scattered-subcarrier attack if $\mathcal{M}_a$ is not continuous. This type of attack can consist of multiple narrowband attacks, each of which transmits the jamming signal to target a different group of subcarriers (thereby targeting particular users). Such an attack leads to a scattered jamming signal spectrum in the full-band spectrum. In practice, since each user is only assigned to a specific subset of subcarriers, an attacker can learn the subcarrier indices used by users by sensing their transmissions.

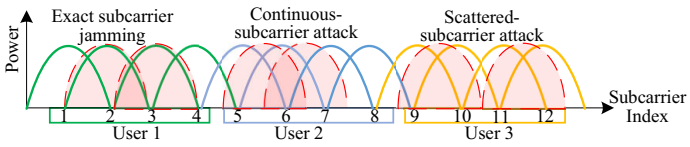

Fig. 2. Illustrative examples of three attack strategies.

Fig. 2 shows examples of the exact subcarrier jamming attack and the two orthogonality-sabotaging strategies: the continuous-subcarrier attack uses subcarriers 5 and 6 with frequency shift 0.5 to attack the system; the scattered-subcarrier attack uses subcarriers 9 and 11 with frequency shift 0.5 and has a non-continuous spectrum; the exact subcarrier jamming attack exactly jams subcarriers 2 and 3 with no frequency shift.

IV. Experimental Study

In this section, we evaluate the practical impact of orthogonality-sabotaging attacks in WiFi networks [13], [22]. Our experiments are conducted on USRP-based and COTS-based platforms, representing the incoming 802.11ax and the state-of-the-art 802.11ac WiFi networks, respectively.

A. Experimental Setups for 802.11ax

1) Implementation and Configurations: We use USRP X300 as the implementation platform for the incoming 802.11ax standard (currently, there is no COTS product available for 802.11ax). Another advantage of USRP-based implementation is that we are able to measure any physical-layer performance for WiFi because today's 802.11ac firmware is still proprietary without providing fine-grained physical layer control to users. A basic functionality set of 802.11ax is implemented, including three physical-layer modulation schemes (BPSK, QPSK, and 16QAM), the OFDMA specification, and the Alamouti code based MIMO transmission scheme. Note that because the full version of 802.11ax has not yet been officially released, all the modulation/coding setups are in accordance with 802.11ac as 802.11ax is backward-compatible, except for the OFDMA configurations that are based on the current draft version of 802.11ax [13].

2) Experimental Setups: We conduct experiments in a realistic indoor environment, as shown in Fig. 3. There are 10 USRPs, where one USRP with two antennas acts as the AP, one USRP with two antennas acts as the orthogonality-sabotaging attacker with intent to use narrowband jamming signals to cause damage to the network, and the remaining 8 USRPs with signal antenna synchronized by OctoClock-G [23] are users. In the network, we adopt the 20MHz subcarrier allocation mechanism in 802.11ax: there are in total 245 subcarriers including 208 data subcarriers assigned to 8

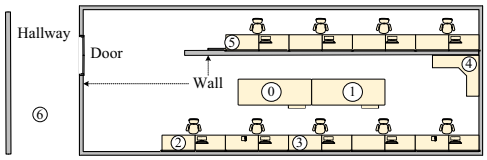

Fig. 3. Office environment (the circled numbers indicate location indices).

timing-synchronized users and each user has a sub-band of 26 subcarriers. All others are virtual subcarriers.

Let $L_a = |\mathcal{M}_a|$ be the attacker's bandwidth (measured as a multiplier of a single subcarrier's bandwidth). Unless otherwise specified in our experiments, the orthogonality-sabotaging attacker uses the continuous-subcarrier attack strategy with a narrow bandwidth $L_a = 18$ placed at location 1. The AP is placed at location 0 in Fig. 3. The objective of our experiments is to evaluate the impact of orthogonality-sabotaging attacks, we place all users at location 3 which is very close to the AP such that all users have very good channels to the AP and the performance degradation of a user is dominantly due to the attacker rather than poor channel condition. The default modulation scheme for each user is QPSK. The attacker and users have the same transmit power.

During the experiments, the attacker can use the continuous-subcarrier or scattered-subcarrier attack strategy. The continuous-subcarrier attack has a jamming signal spectrum within one user's sub-band. In contrast, the scattered-subcarrier attack consists of 18 scattered narrowband jamming signals with a bandwidth of 9 subcarriers to attack two of the eight users in the network.

3) Evaluation Metric: To assess the impact of orthogonality sabotaging in the network, we use the bit error rate (BER), which is the ratio of the number of incorrectly decoded bits to the total number of received bits.

B. Experimental Results in 802.11ax

In the following, we measure the real-world impact of orthogonality-sabotaging attacks on the performance of the 802.11ax network under different situations.

1) Varying Attacker's Intentional Frequency Shift: We first measure the impact of the orthogonality-sabotaging attack for different frequency shifts in $[-0.5, 0.5]$ to validate Theorem 1. Fig. 4 plots the relationship between the frequency shift of the narrowband attacker and the average BER from all users to the AP. We can see that the BER reaches the maximum when the normalized frequency shift is ± 0.5, which verifies the result in Theorem 1. Furthermore, we see that the impact of the scattered-subcarrier attack is more significant than that of the continuous-subcarrier attack. In addition, when the frequency shift becomes 0, the attack becomes the exact subcarrier jamming attack. We also observe that both strategies of orthogonality-sabotaging attacks cause more damage than the exact subcarrier jamming attack, which in fact leads to the minimum damage to the network.

2) Varying Attacker's Bandwidth: In the remaining experiments, the frequency shifts are all set to 0.5 to maximize the attacker's impact on the network performance. We next evaluate the efficiency of the orthogonality-sabotaging attack; i.e., evaluate how many subcarriers can be damaged by the attacker with different narrow bandwidth. Fig. 5 shows the BER performance of the received signal on each of the 208 subcarriers under different attack bandwidth L_a. When the attacker uses $L_a = 6$ subcarriers to launch the attack, it can affect at least 25 adjacent subcarriers. As L_a increases to 18, we observe that it affects at least 63 surrounding subcarriers. Consequently, it is noted from Fig. 5 that the orthogonality-sabotaging attack can go beyond its own bandwidth and substantially disrupt the signal spectrum with a bandwidth 400% broader than its own bandwidth.

3) Varying Modulation Scheme: We evaluate the sensitivity of the modulation scheme to the orthogonality-sabotaging attack. It is obvious that higher-order modulation schemes, such as 16QAM, can tolerate less interference. Fig. 6 shows the BER performance on different subcarriers of the received signals from all users. It is observed from Fig. 6 that under 16QAM, the attack can disrupt the signal spectrum with a bandwidth 500% broader than its own bandwidth. We can expect that when the data rate further increases (e.g., when 256QAM is used), the impact of the orthogonality-sabotaging attack becomes even more significant in the network.

4) Varying Attacker's Location: We also evaluate the impact of the orthogonality-sabotaging attack at different locations. The AP is fixed at location 0, and 8 users' devices are all placed at location 1 as shown in Fig. 3. We place the attacker's device from location 1 to location 6, representing different channel and power conditions from the attacker to the AP. Fig. 7 shows the BER performance at the AP for different attacker's locations under BPSK, QPSK, and 16QAM. We can see that when the attacker is closer to the AP, orthogonality sabotaging causes a larger impact. At location 6, the attack results in a slight impact because the signal strength of the jamming signal is weak when it reaches the AP.

5) Impact on Different Users: Figs. 8 and 9 show the attack impact for different users in the OFDMA-based 802.11ax network. We measure from a user to the AP both the BER and the packet drop rate (PDR) (defined as the ratio of the number of successfully decoded packets at the AP to the total number of packets transmitted to the AP by a user). The packet length is set to 200 bytes. Note that a longer packet is usually more susceptible to channel noise or fading as more information is transmitted. Thus, we choose 200 bytes as the packet size to make sure that packet disruption in the network is mainly due to jamming instead of channel fading or noise. The attacker is placed at location 1 and launches both continuous-subcarrier and scattered-subcarrier attacks. The continuous-subcarrier attack with a bandwidth $L_a = 18$ is within user 5's sub-band. The scattered-subcarrier attack consists of two narrowband continuous-subcarrier attacks with bandwidth spanning 9 subcarriers each (thus the total bandwidth L_a is still 18) to attack users 4's and 6's sub-bands, respectively.

For the BER performance, Fig. 8 shows that under the

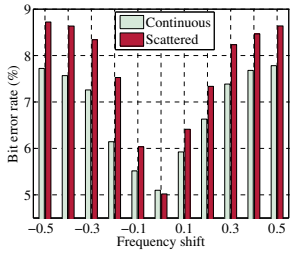

Fig. 4. BER performance under different frequency offsets.

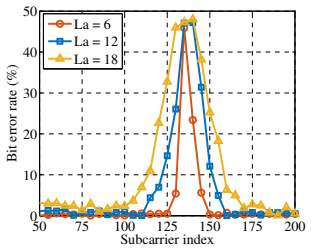

Fig. 5. BER performance for different bandwidths of the attacker.

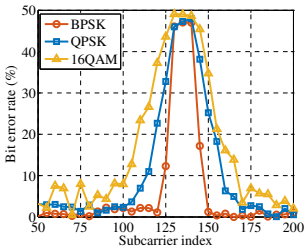

Fig. 6. BER performance under different modulation schemes.

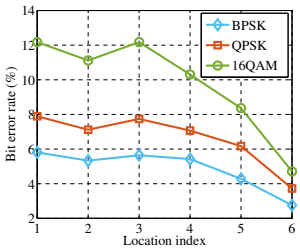

Fig. 7. BER performance under different locations.

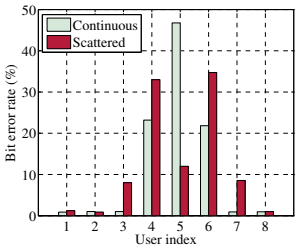

Fig. 8. BER performance of different users.

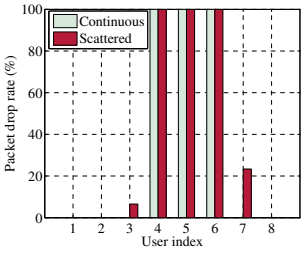

Fig. 9. PDR performance of different users.

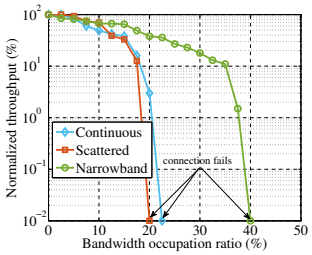

Fig. 10. Normalized network throughput for different attack strategies.

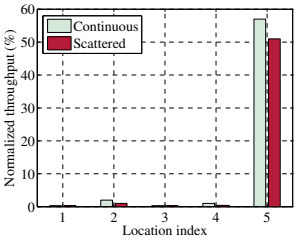

Fig. 11. Normalized network throughput at different locations.

continuous-subcarrier attack, users 4 to 6 are largely affected, especially for user 5 with the BER near 50%. Under the scattered-subcarrier attack, users from 3 to 7 are all affected, revealing that the scattered-subcarrier attack causes damage to more users than the continuous-subcarrier attack in practical networks.

For the PDR performance, we note in Fig. 9 that both attack strategies severely damage the performance of users 4-6. In addition, the scattered-subcarrier attack also substantially affects users 3 and 7. To summarize, orthogonality-sabotaging attacks are very bandwidth-efficient to take down broadband OFDMA communications.

C. Experiments in 802.11ac

To study the impact of orthogonality-sabotaging attacks on COTS products, we use Linksys EA8500 [24] as the WiFi AP, running in 802.11ac mode at 5GHz with 20MHz bandwidth, to setup an 802.11ac network. Note that the source code in today's 802.11ac firmware is always proprietary. We have no fine-grained control on an 802.11ac WiFi chipset, such as modulation/code rate and frame aggregation, which makes it not possible to directly measure the physical layer performance (e.g., bit error rates in Fig 4). Thus, we aim to measure the network-layer throughput between two communicating nodes in the network.

We use two laptops, equipped with the Wireless-AC 7265 WiFi chipset [25], as the two ends of the throughput measurement. We use iPerf to generate UDP traffic between the two laptops. The default UDP packet payload is 1470 bytes. Our evaluation metric, the normalized throughput is defined as the ratio between the received bytes and the total transmitted bytes. In the network, the AP is placed at location 0 and two laptops are placed at locations 1 and 3. The attacker is placed at location 3 and launches jamming attacks with the same transmit power, combining with reactive jamming strategies (i.e., the jammer sends jamming signals only when it detects any WiFi transmission on-going).

We consider three attack strategies: 1) continuous-subcarrier attack, 2) scattered-subcarrier attack, and 3) traditional narrowband jamming, which randomly jams a part of the WiFi frequency spectrum.

1) Results: We first measure the throughput by varying the bandwidth occupation ratio of the jammer, which is the ratio of the total bandwidth of the jamming signal to that used by the AP. Fig. 10 shows the throughput performance under continuous-subcarrier attack, scattered-subcarrier attack, and traditional narrowband jamming attack. From Fig. 10, we notice that the normalized throughput decreases as the jammer increases his own bandwidth. During this process, the AP and WiFi nodes adaptively decrease their data rates for reliable transmissions under their rate-adaptive algorithms. When the bandwidth of the attacker exceeds a threshold, the SINR becomes too low to decode any received signal (e.g., the acceptable SINR of WiFi signals is around 10dB [21]), resulting in network connection failures observed on our laptops. Fig. 10 shows that orthogonality sabotaging is more effective than traditional narrowband jamming, and requires about 20% of the full bandwidth to completely disrupt the network connection.

We also evaluate the impact of orthogonal sabotaging on the throughput performance by placing the jammer at different locations in Fig. 11. The bandwidth of the attacker is set to be 5MHz against the full WiFi bandwidth of 20MHz. It is observed from Fig. 11 that when the jammer is placed at

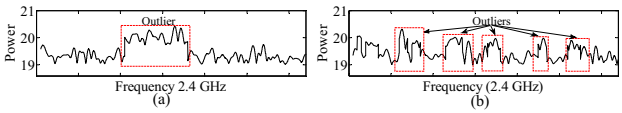

Fig. 12. A wireless signal under jamming through (a) frequency-flat fading, (b) frequency-selective fading.

locations 1-4, the throughput is almost 0, indicating that the network is almost down due to the orthogonality-sabotaging attacks. In addition, we also observe that the scattered and continuous strategies lead to similar performance degradations.

V. Attack Identification and Localization

We have used theoretical analysis and real-world experiments to measure the impact of the narrowband orthogonality-sabotaging attacks against a broadband OFDMA network. In this section, we propose an attack identification and localization algorithm and evaluate its effectiveness.

A. Algorithm Design

As jamming detection is a well-known topic in the literature [7]–[9], our goal is not to design yet another jamming detection algorithm, which confines to yield a binary result to show whether a potential jamming exists or not. Rather, we aim to create an algorithm to identify whether an orthogonality-sabotaging attack exists as well as to localize it in the full-band spectrum if it exists. As a result, the proposed algorithm can work with existing jamming detection methods to provide fine-grained information about an attack in addition to the coarse information about whether jamming exists or not.

1) Motivation: Intuitively, spectrum analysis is a straightforward method to identify and localize orthogonality-sabotaging attacks. The method should work well in the frequency-flat fading channel since an orthogonality-sabotaging attack can lead to a narrowband outlier in the full-band spectrum. However, it can face difficulties in the frequency-selective fading channel because a signal at a distinct frequency can experience substantially different fading in the frequency-selective channel [26], resulting in a number of outliers in the spectrum. For example, Fig. 12 shows the spectrums of jammed 2.4GHz OFDMA signals in (a) frequency-flat and (b) frequency-selective fading channels. From Fig. 12(b), it is hard to identify which one of the outliers is resulted from random fading or attacks in frequency-selective fading. Thus, the spectrum analysis based identification methods cannot be effective in all channel conditions.

To propose our algorithm, we need to address two challenges: 1) it should be a channel condition insensitive method that works well in both flat-fading and frequency-selective channels; 2) the method should be non-invasive and does not change any wireless standard.

After carefully going through many OFDMA standards (e.g., 4G, 5G and 802.11ax), we find that our method can be built upon the virtual subcarriers, which are inserted as the guard zones to protect users from multi-access interference [13]–[15]. As the example shown in Fig. 1, one virtual subcarrier is inserted between two adjacent users. By nature, all virtual subcarriers carry no information with zero power. Therefore, the measured power on such subcarriers at the receiver should be zero (in the ideal case) and is insensitive to the wireless fading condition. Any positive measurement can be only due to noise or jamming interference. Measuring the interference level at each virtual subcarrier opens a door to attack identification and localization.

In particular, we first notice that according to (6) and (13), an orthogonality-sabotaging attack with a single subcarrier bandwidth leads to interference levels on all subcarriers following a squared sinc function pattern, where the sinc function is defined in (14), indicating that a subcarrier closer to the attack suffers more damage from the attack. Then, the interference levels on virtual subcarriers should also satisfy this pattern. Furthermore, for either continuous-subcarrier or scattered-subcarrier attack that spans more than one subcarrier bandwidth, the interference levels on virtual subcarriers should be the aggregation of different sinc function patterns. Thus, our idea is to try different combinations of sinc function patterns to best fit the measured interference levels, thereby finding out where narrowband attacks are.

Note that virtual subcarriers exist in OFDMA systems. For single-user OFDM networks (e.g., 802.11a/g/n/ac), we can use the pilot subcarriers as the alternatives. They carry known symbols for channel estimation purposes; therefore, we can still measure the interference levels on them after removing these known symbols.

2) Formulation: We mathematically formulate our attack identification and localization method. Given the attack with sets $\mathcal{M}_a$, $\{\varepsilon_m^{(a)}\}_{m\in\mathcal{M}_a}$, and $\{P_m^{(a)}\}_{m\in\mathcal{M}_a}$ unknown to the receiver, we aim to find the combination $\hat{\mathcal{M}}_a$, $\{\hat{\varepsilon}_m^{(a)}\}$, and $\{\hat{P}_m^{(a)}\}$ such that they have exact or close values to $\mathcal{M}_a$, $\{\varepsilon_m^{(a)}\}$, and $\{P_m^{(a)}\}$, respectively.

To proceed, given one potential combination of $\hat{\mathcal{M}}_a$, $\{\hat{\varepsilon}_m^{(a)}\}$, and $\{\hat{P}_m^{(a)}\}$, according to (9), the power level of interference on virtual subcarrier $x \in \mathcal{V}$, where $\mathcal{V}$ is the set of all subcarrier indices, can be defined as

$$\Phi_x(\hat{\mathcal{M}}_a, \{\hat{\varepsilon}_m^{(a)}\}, \{\hat{P}_m^{(a)}\}) = \sum_{m\in\hat{\mathcal{M}}_a} \hat{P}_m^{(a)} |I(m, x, \hat{\varepsilon}_m^{(a)})|^2. \tag{15}$$

Denote the measured interference level by y_x on subcarrier $x \in \mathcal{V}$ at the receiver. Then, our objective is to find the combination of $\hat{\mathcal{M}}_a$, $\{\hat{\varepsilon}_m^{(a)}\}$, and $\{\hat{P}_m^{(a)}\}$ by minimizing the mean squared error during fitting

$$E_{\text{fitting}} = \min_{\hat{\mathcal{M}}_a, \{\hat{\varepsilon}_m^{(a)}\}, \{\hat{P}_m^{(a)}\}} \sum_{x\in V} \|y_x - \Phi_x(\hat{\mathcal{M}}_a, \{\hat{\varepsilon}_m^{(a)}\}, \{\hat{P}_m^{(a)}\})\|^2. \tag{16}$$

The minimization in (16) will output the minimized fitting error E_{fitting} with the corresponding $\hat{\mathcal{M}}_a$, $\{\hat{\varepsilon}_m^{(a)}\}$ and $\{\hat{P}_m^{(a)}\}$.

3) Solving the Optimization: Given measured interference levels, the optimization problem in (16) is non-convex. To solve the problem, we notice that its formulation is similar to the form of the optimization problem in Eq. (15) of [27]. Hence, we adopt the interior-point method used in [27] to

solve the problem. The basic idea is to iteratively approach the optimal point from the interior of the feasible subcarrier, frequency offset, and transmit power sets. As pointed out in [27], good initial values are important to find the global optimum. Therefore, we choose the following initial values for $\hat{\mathcal{M}}_a$, $\{\hat{\varepsilon}_m^{(a)}\}$, and $\{\hat{P}_m^{(a)}\}$.

- To determine the initial values for $\hat{\mathcal{M}}_a$, we see that the interference level is mainly due to jamming attacks. Therefore, there will be a number of peaks if we look at the interference levels on all virtual subcarriers. Then, the positions of the attacks should be around the peaks because orthogonality-sabotaging attacks cause more impacts on subcarriers that are closer to them. We choose the initial values of $\hat{\mathcal{M}}_a$ to be the set of those peaks. We say an interference level is a peak if it exceeds a threshold η, which can be set above the noise level during normal wireless communication.
- The initial values of $\{\varepsilon_m^{(a)}\}$ are set to be 0.5 because Theorem 1 shows that the 0.5 frequency shift is able to maximize the attack impact. If a narrowband attacker wants to attack the network to the maximum extent, it should choose the 0.5 frequency shift.
- The initial values for attack powers $\{P_m^{(a)}\}$ are set to be the users' transmit power. This is because the attack should have a power no less than the users', i.e., $P_m^{(a)} \geq P_m^{(k)}$, which is also used as a constraint in the interior-point method to solve the optimization.

4) Decision Rules: Based on the outputs from the optimization in (16), we can identify and localize the orthogonality-sabotaging attack. However, orthogonality sabotaging is not the only way to attack. What if the attack is the exact subcarrier jamming or broadband jamming? Hence, we identify the type of an attack as follows.

- Because the exact subcarrier jamming cannot lead to interference on virtual subcarriers, the attack is identified as the exact subcarrier jamming attack if there is no peak among all interference levels and the data packets are not correctly decoded.
- A broadband jamming attack (or multiple narrowband jamming attacks cooperating to jam most parts of the full bandwidth) can cause strong interference to all or most virtual subcarriers. Therefore, when the number of elements in the output $\hat{\mathcal{M}}_a$ is larger than a threshold L_{th}, i.e., $|\hat{\mathcal{M}}_a| > L_{\text{th}}$, we consider the attack broadband-like jamming attack.
- Otherwise (i.e., when there exists at least one peak and $|\hat{\mathcal{M}}_a| \leq L_{\text{th}}$), we identify the attack as orthogonality sabotaging. Then, we use the outputs $\hat{\mathcal{M}}_a$ and $\{\varepsilon_m^{(a)}\}$ to localize every narrowband part of the attack in the full-band spectrum.

B. Experimental Evaluation

We then use the experimental platform and system configurations described in Section IV to evaluate the performance of our identification and localization method. During the experiments, we use the peak threshold β=13 dB, which is chosen to be above the noise threshold level in experiments. The broadband-like jamming threshold is set as $L_{\text{th}} = 52$. That is, we consider an attacker as broadband-like jamming if $|\hat{\mathcal{M}}_a| > 52$. This value is chosen based on the total number of data subcarriers and the impact of orthogonality sabotaging. As previous experimental results demonstrate, orthogonality sabotaging can disrupt the signal spectrum with a bandwidth 400% broader than the attacker's bandwidth. There are totally 208 data subcarriers in the network; then an attack with bandwidth $L_a = 52 = 208/400\%$ is sufficient to take down the entire network, leading to the same effect of broadband jamming. As a result, L_{th} is set to 52.

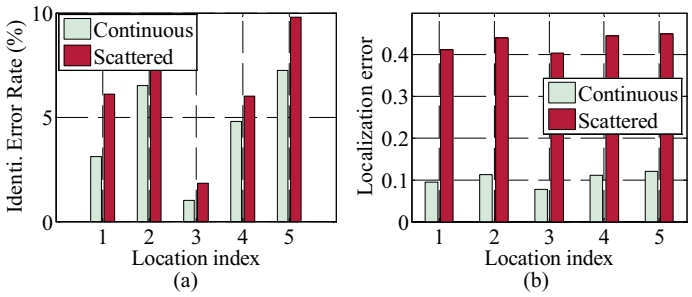

Fig. 13. The performance of the algorithm at different locations: (a) identification error probability, (b) localization error.

TABLE I
PERFORMANCE OF ATTACK IDENTIFICATION.

	Orth.-Sab.	Broad.-like	Exact-sub.
iden. as Orth.-Sab.	92.99%	2.4%	0.2%
iden. as Broad.-like	2.62%	98.6%	0.0%
iden. as Exact-sub.	4.39%	0.0%	99.8%

1) Identification Error: The proposed algorithm can identify a jamming attack as one of the three types: orthogonality sabotaging, broadband-like jamming, and exact subcarrier jamming. Therefore, we need to evaluate the attack identification performance of the algorithm.

Table I shows the probabilities that given the type of an attack, how the attack is identified by our algorithm run at the AP. The AP and the jammer are placed at locations 0 and 1, respectively; and the users are at location 3, as shown in Fig. 3. It is noted from Table I that when the attack is orthogonality-sabotaging, it can be identified with over 92% accuracy. In addition, the algorithm also yields 98.6% and 99.8% accuracies for identifying broadband jamming and exact subcarrier jamming, respectively.

Fig. 13(a) also shows the identification error probabilities for different attack locations under two attack strategies. We can see that the identification error probability for the continuous-subcarrier attack is lower than the scattered-subcarrier attack. This is because the interference pattern is more evident for the continuous-subcarrier attack, which makes it easy to identify. From Fig. 13, we also notice that the identification error probability when the attacker is at location 5 is larger than that in any other location. This is because

the attacker's signal from location 5 is the weakest at the AP, making it hard to be identified (at the same time causing less impact on the network). Overall, the proposed algorithm achieves around 92% identification accuracy.

2) Localization Error: Our algorithm also localizes an attack in the full-band spectrum, if the attack is identified as orthogonality sabotaging. We then measure the localization error of our algorithm. The localization error is defined as follows. First, for each $m \in \hat{\mathcal{M}}_a \cap \mathcal{M}_a$ we compute the error $e_m = |\hat{\varepsilon}_m^{(a)} - \varepsilon_m^{(a)}|$, for each $m \notin \hat{\mathcal{M}}_a \cap \mathcal{M}_a$, we compute $e_m = |\hat{\varepsilon}_m^{(a)} + m|$ if $m \in \hat{\mathcal{M}}_a$ and $e_m = |\varepsilon_m^{(a)} + m|$ if $m \in \mathcal{M}_a$. The localization error is then the mean value of $\{e_m\}$.

Fig. 13(b) shows the localization error for different attack locations. We can see that the localization performance for the continuous-subcarrier attack is significantly better than that of the scattered-subcarrier attack. For example, if the attacker is at location 2, the localization errors are 0.12 and 0.44 for the continuous-subcarrier and scattered-subcarrier attacks, respectively. As aforementioned, this is because the interference pattern caused by the continuous-subcarrier attack is easier to be identified and thus localized. Overall, we can conclude from Fig. 13(b) that the localization error of the algorithm is as low as 0.1–0.45 subcarrier spacing.

VI. Related Work

Recent studies on OFDMA systems mainly focus on estimating and compensating carrier frequency offsets in users' signals [28], [29]. In this paper, the frequency shifts are introduced intentionally by attacks and cannot be compensated because they are embedded in outside jamming signals unknown to the receiver. To the best of knowledge, our work is the first to investigate the impact of narrowband jamming with maliciously frequency shifts on OFDMA wireless networks.

For jamming attacks, smart or intelligent jamming strategies have been developed to target various communication and network systems [1], [4]–[7], [10], [11], [16], [30], [31]. In this paper, we revisit the orthogonality of the OFDMA system and show that such a common assumption for jamming is not necessary. We create a new orthogonality-sabotaging attack mechanism which is very efficient to destroy the orthogonality in all subcarriers. Furthermore, our work is orthogonal to recent smart jamming strategies [2], [16], and can be combined with them to form more efficient attack strategies.

We also propose a fine-grained method that not only identifies the type of a jamming attacker [6], [7], [30], but also localizes an attacker in the full-band spectrum, which provides more detailed attack information to a network defender.

VII. Conclusions

In this paper, we proposed orthogonality-sabotaging attack, against wireless OFDMA networks. We provided both theoretical and experimental results to demonstrate the damage of the attack under various conditions. Our results showed that narrowband orthogonality-sabotaging attacks are able to significantly damage broadband OFDMA systems. Finally, we developed an algorithm to identify and localize such attacks.

Acknowledgement: The work was supported in part by NSF CNS-1553304, CNS-1717969 and ARO W911NF-17-1-0180.

References

[1] T. C. Clancy, "Efficient OFDM denial: Pilot jamming and pilot nulling," in *IEEE ICC*, 2011.
[2] H. Rahbari, M. Krunz, and L. Lazos, "Swift jamming attack on frequency offset estimation: The Achilles' heel of OFDM systems," *IEEE Trans. Mobile Comput.*, vol. 15, 2016.
[3] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "MIMO-based jamming resilient communication in wireless networks," in *IEEE INFOCOM*, 2014.
[4] Z. Liu, J. Liu, N. Kato, J. Ma, and Q. Huang, "Divide-and-conquer based cooperative jamming: Addressing multiple eavesdroppers in close proximity," in *IEEE INFOCOM*, 2016.
[5] S. Fang, Y. Liu, and P. Ning, "Wireless communications under broadband reactive jamming attacks," *IEEE TDSC*, vol. 13, 2016.
[6] J. T. Chiang and Y.-C. Hu, "Cross-layer jamming detection and mitigation in wireless broadcast networks," *IEEE Trans. Netw.*, vol. 19, 2011.
[7] M. K. Hanawal, D. N. Nguyen, and M. Krunz, "Jamming attack on in-band full-duplex communications: Detection and countermeasures," in *IEEE INFOCOM*, 2016.
[8] L. Zhang, Z. Guan, and T. Melodia, "Cooperative anti-jamming for infrastructure-less wireless networks with stochastic relaying," in *IEEE INFOCOM*, 2014.
[9] J. Dams, M. Hoefer, and T. Kesselheim, "Jamming-resistant learning in wireless networks," *IEEE Trans. Netw.*, vol. 24, 2016.
[10] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *IEEE INFOCOM*, 2007.
[11] Y. Wu, B. Wang, K. R. Liu, and T. C. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *IEEE JSAC*, vol. 30, 2012.
[12] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in *IEEE INFOCOM*, 2010.
[13] "IEEE P802. 11 Wireless LANs," *IEEE 802.11-15/0132rI6*, 2016.
[14] 3GPP, "3GPP TS 36.413 V10.3.0 (release 10)," 2011.
[15] ——, "3GPP TS 23.501 V1.0.0 (release 15)," 2017.
[16] H. Rahbari and M. Krunz, "Rolling preambles: Mitigating stealthy FO estimation attacks in OFDM-based 802.11 systems," in *IEEE CNS*, 2016.
[17] J. Huang, G. Xing, J. Niu, and S. Lin, "CodeRepair: PHY-layer partial packet recovery without the pain," in *IEEE INFOCOM*, 2015.
[18] Z. Cao, U. Tureli, Y.-D. Yao, and P. Honan, "Frequency synchronization for generalized OFDMA uplink," in *IEEE GLOBECOM*, 2004.
[19] P. Cheng, Z. Chen, F. de Hoog, and C. K. Sung, "Sparse blind carrier-frequency offset estimation for OFDMA uplink," *IEEE Trans. Commun.*, vol. 64, 2016.
[20] C. Joo and M. Shin, "Queue-affectance-based scheduling in multi-hop wireless networks under SINR interference constraints," in *IEEE INFOCOM*, 2016.
[21] J. Geier, "Wi-Fi: Define minimum SNR values for signal coverage," *Enterprise Networking Planet: Standards & Protocols*, 2008.
[22] "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Std 802.11*, 2013.
[23] Ettus, "Synchronization and MIMO capability with USRP devices."
[24] I. Linksys, "Linksys Mu-Mimo gigabit router EA8500 user guide."
[25] Intel, "Intel dual band wireless-ac 7260 specifications."
[26] N. Liang and W. Zhang, "Mixed-ADC massive MIMO uplink in frequency-selective channels," *IEEE Trans. Commun.*, vol. 64, 2016.
[27] D. Vasisht, S. Kumar, H. Rahul, and D. Katabi, "Eliminating channel feedback in next-generation cellular networks," in *SIGCOMM*, 2016.
[28] M. Huang, L. Huang, C. Guo, P. Zhang, J. Zhang, and L.-L. Yang, "Carrier frequency offset estimation in uplink OFDMA systems: An approach relying on sparse recovery," *IEEE Trans. Veh. Technol.*, 2017.
[29] W. Zhang and F. Gao, "Blind frequency synchronization for multiuser OFDM uplink with large number of receive antennas," *IEEE Trans. Signal Process.*, vol. 64, 2016.
[30] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *IEEE INFOCOM*, 2011.
[31] C. Shahriar, S. Sodagari, R. McGwier, and T. C. Clancy, "Performance impact of asynchronous off-tone jamming attacks against OFDM," in *IEEE ICC*, 2013.