Deceptive Jamming in WLAN Sensing

Hasan Can Yildirim*, Musa Furkan Keskin†, Henk Wymeersch†, and François Horlin*

*Wireless Communications Group, Université Libre de Bruxelles, Belgium

†Department of Electrical Engineering, Chalmers University of Technology, Sweden

Abstract—Joint Communication and Sensing (JCAS) is taking its first shape in WLAN sensing under IEEE 802.11bf, where standardized WLAN signals and protocols are exploited to enable radar-like sensing. However, an overlooked problem in JCAS, and specifically in WLAN Sensing, is the sensitivity of the system to a deceptive jammer, which introduces phantom targets to mislead the victim radar receiver. Standardized waveforms and sensing parameters make the system vulnerable to physical layer attacks. Moreover, orthogonal frequency-division multiplexing (OFDM) makes deceptive jamming even easier as it allows digitally generated artificial range/Doppler maps. This paper studies deceptive jamming in JCAS, with a special focus on WLAN Sensing. The provided mathematical models give insights into how to design jamming signals and their impact on the sensing system. Numerical analyses illustrate various distortions caused by deceptive jamming, while the experimental results validate the need for meticulous JCAS design to protect the system against physical layer attacks in the form of deceptive jamming.

Index Terms—Joint Communication and Sensing, WLAN Sensing, deceptive jamming, physical layer security, OFDM radars.

I. Introduction

In recent years, joint communication and sensing (JCAS) received attraction from both industry and academia, especially as it constitutes an enabler for 6G [1]. JCAS aims at combining communication and sensing capabilities in a single device [2]. While 6G is still several years away, lessons can be learned from one of the first communication-centric JCAS systems under the IEEE Wi-Fi 802.11 standards, namely WLAN Sensing 802.11bf [3]. WLAN Sensing aims to enable presence/intruder and fall detection, identity/gesture recognition, tracking of people, and many more [4]. To do so, orthogonal frequency-division multiplexing (OFDM) modulated WLAN signals (at 2.45, 5, 6, and 60 GHz) and the already existing communication-oriented protocols are exploited for radar-like sensing. In particular, standardized training fields, present in the preamble of any Wi-Fi frame to enable channel estimation and equalization for communication, are used in WLAN Sensing [5]. Therefore, the access points (APs) and user stations (STAs) have access to the original transmit signal, which enables radar-like processing in both monostatic and bistatic geometries [6].

Although OFDM has many benefits for JCAS [7], the general JCAS and the WLAN Sensing communities overlook one important fact about using a standardized OFDM
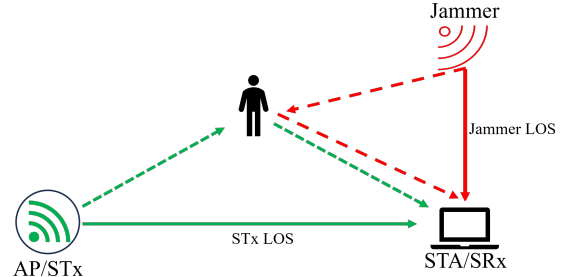
Fig. 1. A scenario with a sensing transmitter (STx), sensing receiver (SRx), a mobile target, and a Jammer that transmits pre-modulated signals that carry phantom targets.

waveform for sensing: its sensitivity to deceptive jamming, which aims at misleading a victim radar receiver by generating phantom targets, illustrated in Fig. 1. The idea of deceptive jamming is not new in the conventional radar literature [8]. Historically, the deceptive jammer device must (a) estimate the radar operation parameters such as system bandwidth, pulse repetition interval (PRI), etc., (b) reconstruct the original radar waveform with great precision, (c) artificially introduce realistic propagation delays, Doppler shifts, and attenuation to mimic real targets, and (d) transmit these signals within the time frame of the victim radar [8]. In order to accomplish these in real-time, digital radio-frequency memory (DRFM) technology is often employed where high-speed sampling and digital memory are used to store radar signals [9]. In the context of wireless sensor networks, [10] provides an extensive survey about various types of jamming attacks and countermeasures, but ignores the implications related to the use of OFDM waveforms. OFDM deceptive jamming was treated in [11]–[13]. In [11], a deceptive jamming framework for OFDM-based synthetic aperture radars (SARs) is proposed, where deceptive target images are injected into the SAR image of the victim radar. Various techniques for reconstructing the original waveform are also discussed. In [12], a new advanced model for airborne deceptive jamming is proposed using DRFM and applying the sub-Nyquist sampling theorem to reduce the sampling rate of the deceptive jammer. Finally, counter-acting deceptive jamming is considered in [13], where the robustness of randomly generated OFDM radar waveforms against deceptive jamming is analyzed.

JCAS, and more specifically WLAN Sensing, is particularly sensitive to deceptive jamming, since i) *radar parameters are selected from a pre-determined set of parameters* [14], and ii) the *OFDM waveform is standardized* [3]. These properties remove the need for previously mentioned steps (a) and (b),

and hence, the need for DRFM. Instead, the primary focus shifts to generating realistic range/Doppler maps (RDMs) and aligning the transmission time within the time frame of the victim radar receiver. The alignment of transmission time benefits from OFDM-based bistatic radar processing which requires the correlation between the transmitted and the received signals to find the timing reference [15]. Hence, the timing reference can be triggered by the jamming signal instead of the actual reference signal as long as i) the jamming signal arrives within half of the OFDM symbol duration [16] and ii) it exhibits a larger amplitude than the actual timing reference signal. Since JCAS is relatively new in the literature, deceptive jamming is not yet fully addressed. Moreover, the potential and challenges of a deceptive jammer in the JCAS context are not yet validated within a complete system such as WLAN Sensing.

In this paper, we provide insights into what makes WLAN Sensing, or more generally, OFDM-based JCAS, prone to deceptive jamming and analyze various possible scenarios. Our contributions are summarized as follows

- The shortcomings of WLAN Sensing against deceptive jamming are identified, and a mathematical framework to design deceptive jammers is provided.
- Thanks to the flexibility of the jamming framework, it is shown that the victim radar can be deceived at the output of the target detector (i.e., per radar snapshot) as well as in the target tracking layer (i.e., over multiple radar snapshots).
- Different deceptive jamming scenarios are discussed, and their impact on the victim radar performance is numerically analyzed.
- The vulnerability of WLAN Sensing against deceptive jamming in real-life application environments is experimentally validated using two USRP X310s to emulate the transmitter, the receiver, and the jammer in an indoor scenario with a walking human.

II. WLAN SENSING AND SYSTEM MODEL

In this section, we introduce the WLAN Sensing and its characteristics. Then, we provide the system model (including the OFDM waveform, the channel, and the receiver-side processing).

A. Fundamentals of WLAN Sensing

In WLAN Sensing [3], a given Wi-Fi device can be i) a sensing transmitter (STx) which only transmits; ii) a sensing receiver (SRx) which only receives, and iii) a sensing transceiver (STRx) which transmits and receives sensing signals [6]. These roles simply determine the radar geometries: i) bistatic if STx and SRx are separated devices as illustrated in Fig. 1, or ii) monostatic if a single device is acting as an STRx. In this paper, we specifically focus on the bistatic WLAN Sensing geometry since it is the most vulnerable to jamming –with AP and STA acting as STx and SRx, respectively.

In order to enable bistatic sensing, first the AP discovers the STAs equipped with 802.11ac/ax/be Wi-Fi chipsets during the
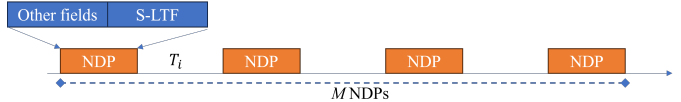

Fig. 2. An overview of sensing measurement instance (SMI), where a null data packet (NDP) is composed of a sensing-long training field (S-LTF), which refers to the only OFDM symbol used for sensing, and other fields such as Legacy-LTF, are ignored for simplicity.

sensing session setup (SSS). Then, the AP and the previously paired STAs fix their sensing parameters, such as the signal bandwidth, etc., during the sensing measurement setup (SMS). Finally, radar-like sensing takes place during the so-called sensing measurement instance (SMI). In this phase, STx and SRx exploit channel sounding protocols initially implemented to enable multi-user multi-input multi-output communication in Wi-Fi [17]. More specifically, STx transmits priorly known packets, called null data packets (NDPs), through the wireless channel, and the SRx estimates the radar channel transfer function (CTF) from the corresponding sensing-long training fields (S-LTFs) found in each NDP.[1] Hence, as illustrated in Fig. 2, one can see the entire SMI as a pulsed OFDM-modulated radar scheme where each pulse corresponds to an NDP/S-LTF with PRI T_i.

Since the SSS and SMS phases described above take place over the air in bistatic geometry, a jammer can listen to these transmissions: i) if it is acting as a legitimate Wi-Fi device such as a neighboring AP, or an STA paired with the sensing AP[2], or else ii) it can passively eavesdrop on the transmission of NDPs and estimate the WLAN Sensing parameters among a predetermined set of parameters.[3] Regardless, deceptive jamming becomes relatively straightforward.

B. System Model

Since OFDM modulation is very well-known in the literature [18], [19], only a summary of the OFDM-based bistatic radar chain is provided. The OFDM modulation parameters are defined as follows: number of subcarriers Q, number of samples in cyclic prefix (CP) Q_{cp}, system bandwidth B, sampling interval $T = 1/B$, subcarrier spacing $\Delta_f = 1/QT$, OFDM symbol duration $T_o = (Q + Q_{cp})T$ and PRI T_i which is an integer multiple of T_o. In Fig. 3, a block diagram is provided where STx and SRx pursue the following stages: i) $X[q, m]$ contains standardized BPSK symbols on its subcarriers q which are identical $\forall m$, and the inverse fast Fourier transform (IFFT) is computed over $X[q, m]$ along q for the m-th S-LTF; ii) after adding of CP of length Q_{cp}, the S-LTFs are transmitted through the time-varying multipath channel; iii) SRx samples the received signal, finds the timing reference by using a correlator; iv) reshapes all the samples into parallel

---

[1]Depending on the amendment, S-LTFs have different names: VHT, HE, and EHT for 11ac, 11ax, and 11be, respectively. For simplicity, we refer to them as Sensing LTFs.

[2]In Wi-Fi, the unicast and multicast management frames are protected so that eavesdropping and forging are avoided, hence, the need for acting as a legitimate device.

[3]In any other non-standardized radar system, the radar parameters can take any value, which raises the need for DRFM. In WLAN Sensing, the size of the set of possible radar parameters is between 4 and 8 [6].

streams and removes the CP, and v) computes the fast Fourier transform (FFT) of each S-LTF symbol.

Assuming that there is no carrier frequency offset between STx and SRx[4], and neither of the devices is mobile, the signal received on subcarrier q of S-LTF m is defined in the frequency domain as follows

$$R[q,m] = H[q,m]X[q,m] + Z[q,m], \quad (1)$$

where $Z[q,m]$ is the additive white Gaussian noise (AWGN) at SRx, and $H[q,m]$ is the channel transfer function (CTF) to be estimated. The CTF is of the form

$$H[q,m] = \sum_{p=0}^{P} \alpha_p e^{-j2\pi q \Delta_f (\tau_p - \tau_0)} e^{j2\pi m T_i f_p}, \quad (2)$$

where P denotes the number of echoes, which are characterized by their amplitude α_p, propagation delays τ_p with respect to the timing reference τ_0, and Doppler frequency shifts f_p, while $p = 0$ refers to the LOS between STx and SRx.

Assuming that the timing reference is STx line-of-sight (LOS), the estimated CTF is trivially written as

$$\hat{H}[q,m] = R[q,m]/X[q,m] \quad (3)$$

from which the RDM is obtained through a series of inverse discrete Fourier transforms (IDFT) over q and discrete Fourier transforms over m (DFT) as (for $l = 0, \ldots, Q-1$ and $v = 0, \ldots, M-1$)

$$\hat{Y}[l,v] = \sum_{q=0}^{Q-1} \sum_{m=0}^{M-1} \hat{H}[q,m] e^{j2\pi \frac{ql}{Q}} e^{-j2\pi \frac{mv}{M}}$$

$$= \sum_{p=0}^{P} \alpha_p \sum_{q=0}^{Q-1} e^{j2\pi \frac{q}{Q}(l-l_p)} \sum_{m=0}^{M-1} e^{-j2\pi \frac{m}{M}(v-v_p)} + Z[l,v]$$

$$= \sum_{p=0}^{P} \alpha_p D_Q(l, l_p) D_M(v, v_p) + Z[l,v] \quad (4)$$

where $l_p = (\tau_p - \tau_0)/T$ and $v_p = T_i f_p$ correspond to the target propagation delay relative to the STx LOS and Doppler frequency shift, each normalized with respect to sampling interval and PRI, respectively. In general, neither l_p nor v_p are integers.[5] Moreover, $D_N(y,x) = e^{j\pi \frac{N-1}{N}(y-x)} \sin(\pi(y-x))/\sin(\pi(y-x)/N)$ corresponds to the Dirichlet kernel obtained by expanding the geometric series of Fourier transforms [20]. Once an RDM is obtained, a constant false-alarm rate (CFAR) detector separates the target echo peaks from noise peaks [21].

III. DECEPTIVE JAMMER: SIGNAL AND EFFECTS

In this section, we describe the deceptive jammer, and how it can be designed to deteriorate the WLAN Sensing performance on the target detection layer, i.e., at the output of the CFAR detector applied on an RDM, and on the tracking layer which is applied on successively obtained detection

---

[4]Only residual CFO remains in S-LTF. The coarse CFO correction is already handled with Legacy-LTF which is received prior to S-LTF.

[5]In an unlikely case where l_p and v_p are integers, the Dirichlet functions reduce to a Dirac delta function. However, l_p and v_p are rarely integers in reality, yielding sidelobes on the range and Doppler profiles which can be suppressed by windowing functions.
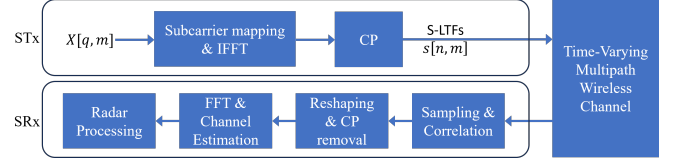

Fig. 3. The block diagram for WLAN Sensing that shows the transmitter and the receiver processing stages up until the radar processing.

maps. We assume that the jammer can either listen to the sensing-related procedures between STx and SRx by acting as a legitimate device during SSS and SMS, or it can passively eavesdrop on the NDP/S-LTF transmissions to deduce the sensing parameters. In return, the jammer can tune its analog front-end for the specific sensing parameter, such as the carrier frequency, sampling rate, etc. We also assume that the jammer can transmit with more power than the STx.

A. Transmit Signal by the Jammer

The artificial RDM generated by the jammer, which causes a single target at the SRx, is defined as follows:

$$\bar{Y}[l,v] = \bar{\alpha} D_Q(l, \bar{l}) D_M(v, \bar{v}) \quad (5)$$

with $\bar{l} = \bar{\tau}/T$ and $\bar{v} = \bar{f} T_i$. The bar symbol indicates the artificial parameters introduced by the jammer: $\bar{\alpha}$, $\bar{\tau}$ and $\bar{f}$ correspond to the amplitude, propagation delay, and Doppler frequency shift of the phantom target, respectively. Here, $\bar{\tau} > 0, \bar{\tau} \in \mathbb{R}$ to ensure that the phantom target has a positive range and $\bar{f} \in \mathbb{R}$ can take any real value depending on the desired phantom target pattern to be forced at SRx. Following the delay-frequency and Doppler-time dualities in [22], the CTF which yields the artificial RDM $\bar{Y}[l,v]$ is obtained by computing the DFT over the range/delay axis and IDFT over speed/Doppler axis of (5), yielding

$$\bar{H}[q,m] = \bar{\alpha} e^{-j2\pi q \Delta_f \bar{\tau}} e^{j2\pi m T_i \bar{f}}. \quad (6)$$

After mapping each subcarrier with $\bar{H}[q,m]$ and $X[q,m]$, the jammer signal takes the following form in the frequency domain

$$\bar{S}[q,m] = \left(1 + \bar{H}[q,m]\right) X[q,m]. \quad (7)$$

The first term in $(1 + \bar{H}[q,m])$ allows us to create an original copy of the S-LTF, i.e., untouched by the artificial RDM, to be forced as the timing reference at SRx. The second term allows us to pre-modulate the OFDM spectrum. Finally, computing the IDFT over q yields

$$\bar{s}[n,m] = \sum_{q=0}^{Q-1} \bar{S}[q,m] e^{j2\pi \frac{qn}{Q}}, n = 0, \ldots, Q-1. \quad (8)$$

The first and second dimensions of $\bar{s}[n,m]$ correspond to pre-modulated OFDM symbols and linearly increasing phase shifts for the Doppler profiles, respectively. After adding the CP to each OFDM symbol, the jammer transmits $\bar{s}[n,m]$ in the time domain.

B. Signal Received at SRx

The channel between the jammer and the SRx is

$$H'[q,m] = \sum_{\rho=0}^{P'} \alpha'_\rho e^{-j2\pi q \Delta_f \tau'_\rho} e^{j2\pi m T_i f'_\rho}, \quad (9)$$

where P', α'_ρ, τ'_ρ, and f'_ρ correspond to the number of echoes, attenuation, propagation delay, and Doppler frequency shift, respectively, while $\rho = 0$ refers to the LOS between the jammer and SRx.

The jamming signal perceived by SRx thus takes the following form in the frequency domain

$$R'[q,m] = H'[q,m]S[q,m] = H'[q,m](1 + \bar{H}[q,m])X[q,m]$$

$$= \sum_{\rho=0}^{P'} \alpha'_\rho e^{-j2\pi q \Delta_f \tau'_\rho} e^{j2\pi m T_i f'_\rho} X[q,m] \quad (10)$$

$$+ \sum_{\rho=0}^{P'} \alpha'_\rho \bar{\alpha} e^{-j2\pi q \Delta_f (\tau'_\rho + \bar{\tau})} e^{j2\pi m T_i (f'_\rho + \bar{f})} X[q,m].$$

Since the jammer transmits an original copy of the S-LTF, signals from the true targets between the jammer and SRx are also received, modeled by the first sum in (10). Note that, since the position of the jammer is generally different than the STx, the radar parameters of the targets in (10) are different than those in (3), i.e., $\alpha_p \neq \alpha'_p$, $\tau_p \neq \tau'_p$ and $f_p \neq f'_p$, $\forall p$. On the other hand, the multipath channel between SRx and the jammer generates multiple copies of the phantom target, modeled by the second sum in (10).

Putting the legitimate signal from the STx and the signal from the deceptive jammer together, the SRx observes

$$R_o[q,m] = R[q,m] + R'[q,m]$$
$$= \underbrace{H[q,m]X[q,m]}_{\text{sensing of STx-SRx channel}} + \underbrace{H'[q,m]X[q,m]}_{\text{sensing of jammer-SRx channel}}$$
$$+ \underbrace{H'[q,m]\bar{H}[q,m]X[q,m]}_{\text{artifical RDM between jammer and SRx}} + Z[q,m]. \quad (11)$$

C. Different Cases for Jammer Signal Time-of-Arrival

The time difference of arrival between the true sensing signal and the jamming signal has great consequences at SRx as illustrated in Fig. 4. Ideally, the timing reference, obtained after the correlation at SRx, will be the S-LTF that propagates through STx LOS since it exhibits the largest amplitude at SRx. However, the timing reference can potentially be triggered by another S-LTF transmitted by the jammer. The time difference of arrival between the true and jamming signals is defined as $\Delta_\tau = \tau'_0 - \tau_0 \pm \bar{\epsilon}$. Here, $\bar{\epsilon}$ can be a deterministic variable that is used by the jammer to time-align its signals with the true sensing signals depending on the desired effects. However, the jammer needs to know τ'_0 and τ_0 to have full control over Δ_τ. On the other hand, $\bar{\epsilon}$ can be a random scenario-specific variable if neither τ'_0 nor τ_0 are known. In this case, the type of jamming effects perceived by the SRx cannot be guaranteed. Assuming that the jamming LOS is stronger than STx LOS, the different consequences depending on the value of Δ_τ are summarized as follows:

- *Jammer Case I:* The jamming LOS signal arrives earlier than the STx LOS. The true RDM will be positively shifted based on Δ_τ/T, i.e., the true echoes will appear at further distances. The phantom target, and its multipath components, will appear at $\bar{\tau} + \tau'_\rho - \tau'_0$, $\rho = 1, \ldots, P'$.
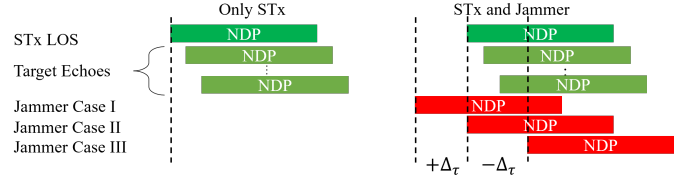

Fig. 4. An illustration of the echoes when only the STx is active vs. both the STx and the jammer are active.

- *Jammer Case II:* In an unlikely scenario where the STx LOS and the jamming signal arrive simultaneously at the SRx, both the true and phantom targets will be present near the zero range, with both of their LOS paths appearing exactly at the zero range.
- *Jammer Case III:* The jamming signal arrives later than the STx LOS. The true RDM will be negatively shifted based on Δ_τ/T, i.e., the true echoes will appear to be at closer distances. This can potentially destroy the subcarrier orthogonality on the true sensing signal if it is sampled beyond its CP. The phantom target, and its multipath components, will appear as in Jammer Case I.

The combined RDM perceived by the SRx can be written as follows

$$\hat{Y}_o[l,v] = \sum_{p=0}^{P} \alpha_p D_Q(l, l_p \pm \Delta_\tau/T) D_M(v, v_p) + Z[l,v]$$

$$+ \sum_{\rho=0}^{P'} \alpha'_\rho D_Q(l, l'_\rho) D_M(v, v'_\rho) + \sum_{\rho=0}^{P'} \alpha'_\rho \bar{\alpha} D_Q(l, \bar{l}_\rho) D_M(v, \bar{v}_\rho).$$
$$(12)$$

The first sum in (12) models the true RDM between STx and SRx, range shifted by Δ_τ/T number of range gates due to the forced timing reference. The second sum corresponds to the RDM between the jammer and SRx, also with the true target. However, its normalized range $l'_\rho = \tau'_\rho/T$ and Doppler frequency $v'_\rho = T_i f'_\rho$ differs from the true RDM since the location of the jammer is different than STx, as shown in Fig. 1. Finally, the third sum corresponds to the artificial RDM propagated through the multipath channel, with P' number of phantom targets at the normalized ranges $\bar{l}_\rho = (\tau'_\rho + \bar{\tau})/T$ and Doppler frequencies $\bar{v}_\rho = (v'_\rho + \bar{v})T_i$.

The model provided in (12) corresponds to a single snapshot, yielding a single RDM. However, modern radar systems use multiple snapshots to track the targets over time. Thanks to the flexibility of the proposed jamming method, RDMs with a target (or potentially multiple targets) that is moving according to Newtonian kinematics can digitally be designed and transmitted by the jamming signal over multiple snapshots.

IV. PERFORMANCE EVALUATION

In this section, numerical analyses illustrate the vulnerability of WLAN Sensing against deceptive jamming, and experimental results are provided for validation.

A. Scenario and Parameters

Jammer Cases I and III from Section III-C have been implemented. To ensure that all the effects described in Sections

Fig. 5. The picture and the diagram of the experimental setup. The jammer (J) antenna is behind the camera. Solid and dashed lines correspond to the LOS and reflections from the target (H), respectively.

II-B and III are taken into account, the entire simulation chain shown in Fig. 3 is simulated, and the simulation parameters are summarized as follows: $B = 80$ MHz, $Q = 1024$, $Q_{cp} = 64$, $M = 128$, $T_i = 2$ms, and the STx transmit power is 23 dBm.

For the experimental results, a real-life scenario with a moving person in a room is considered, as shown in Fig. 5. Two USRP X310s are used to emulate the devices: one for the STx and the Jammer, another for the SRx, while we maintain the parameters used in our simulations, with 30 dBm transmit power at the jammer.

B. Simulation Results

In Fig. 6, four RDMs are provided, which we now discuss in detail:

- *True RDM:* The first RDM is obtained when only the true sensing echoes are received by SRx. Peak (i) is the timing reference, while peak (ii) is the true mobile target.
- *Artificial RDM:* The second RDM is obtained when only the jamming signal is received by SRx. Peak (iii) corresponds to the jammer timing reference, while peaks (iv), (v), and (vi) correspond to the phantom target, the true target, and the phantom target signal reflected from the true target, respectively. Notice that the true target has different characteristics compared to (ii) since the jammer is positioned differently than the STx, as depicted in Fig. 1.
- *Jammed RDM Case I:* The third RDM is obtained when SRx first receives the jamming signal and then the true sensing signal, i.e., Jammer Case I with $\Delta_\tau/T = 16$. As pointed out in (12), SRx perceives a linear combination of the artificial RDM and the true RDM range shifted by about 30 meters. In case Δ_τ/T is much larger, the true target will appear even further away and potentially will be ignored by the tracking layer due to its distance.
- *Jammed RDM Case III:* The last RDM corresponds to the Jammer Case III with $\Delta_\tau/T = -70$. In this case, the RDM exhibits the phantom target, the timing reference peak from the jammer, and ridges along the range dimension. These ridges are due to the loss of subcarrier orthogonality on the true sensing symbols since they are sampled beyond their CP. Moreover, the fact that the true target is not visible at all introduces an even bigger problem than the previous one since there is nothing to detect/track at all.
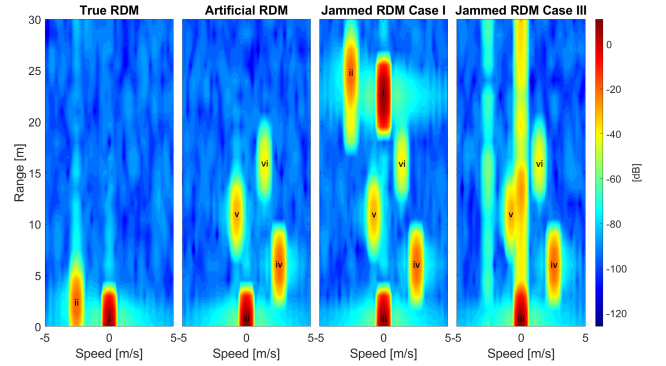

Fig. 6. Simulation: Jammer Cases I and III when the timing reference is triggered by the jammer LOS.
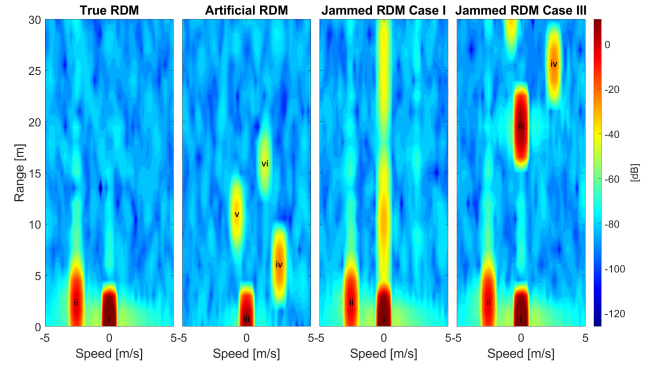

Fig. 7. Simulation: Jammer Cases I and III when the timing reference is triggered by the STx LOS.

For the sake of completeness, Fig. 7 is provided where the amplitude of STx LOS is larger than the jammer LOS, hence, the timing reference is triggered by the STx LOS. In this case, the previously mentioned effects are reversed. When the jamming signal arrives earlier than STx LOS, the phantom target that it carries is not visible on the jammed RDM. Instead, the jammer symbols yield the ridges due to the lost orthogonality among its subcarriers. On the other hand, when the jamming signal arrives later than STx LOS, the phantom target as well as the jammer LOS are visible at further distances than intended.

C. Experimental Results

In Fig. 8, three RDMs are provided, which we again discuss in detail:

- *True RDM:* The true RDM is obtained when only the STx is active in the environment. As opposed to the simulation results from Fig. 6, the RDMs possess a few differences. First, the static clutter (i) is visible at 0 m/s, extending until 40 meters range. Second, the true mobile target (ii) is also subject to multipath, therefore, there are ghost targets[6] until 20 meters. However, since the ghost targets do not move in the same direction as the true target, they yield slightly different Doppler frequency shifts.

---

[6]A phantom target refers to a target digitally generated by the jammer, whereas a ghost target refers to the multipath components of true or phantom targets.
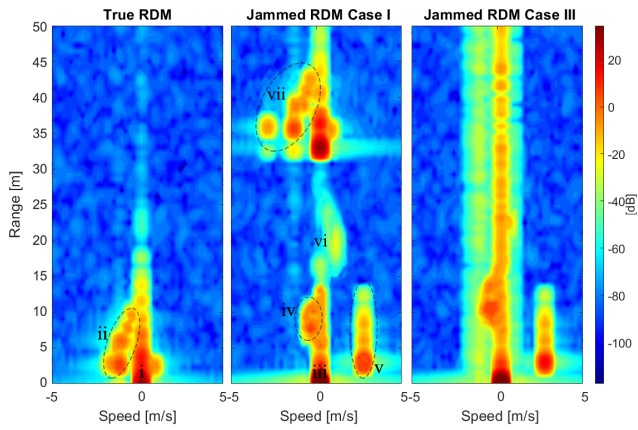
Fig. 8. Experiment: Indoor results with a human target considering Jammer Cases I and III.

- *Jammed RDM Case I:* The second RDM corresponds to the Jamming Case I, where both the STx and the jammer are active. The jammed RDM exhibits the static clutter (iii), the true target (iv), the phantom target (v), and the phantom-to-true target (vi). As predicted by the numerical results, the artificial RDM is the one that is present at short ranges. Meanwhile, the true RDM (vii) (which has slightly different Doppler characteristics compared to the first RDM since it is a new realization) is range-shifted. The most important difference is how the phantom target (v) reacts to the multipath conditions. As opposed to the true target, the artificially generated target is not an actual object moving in the environment, hence, it does not experience the same physical effects. Instead, its ghost targets appear at the same speed gate at further distances.

- *Jammed RDM Case III:* Finally, the third RDM corresponds to the Jamming Case III with a new experimental realization. In this case, two ridges along the range are visible, one for the static clutter and the other for the true mobile target. As pointed out earlier, when the true sensing symbols are sampled far beyond their CP, the orthogonality on their subcarriers is completely lost, yielding such sidelobes along the range profile [19]. Apart from the true target peaks, the sensing system is almost completely deceived since the phantom target is the only mobile peak that appears on the RDM.

Overall, there is a good match between simulation and experimental results, indicating that the models from Section III are valid.

V. CONCLUSION

In this paper, an important but overlooked fact regarding the OFDM-based JCAS systems and their proneness against deceptive jamming was studied. Since JCAS is already taking shape within WLAN Sensing, we specifically focused our analyses on the parameters, the protocols, and the waveforms used in WLAN. We have shown that OFDM makes it very easy to digitally generate realistic RDMs for deceptive jamming, and the underlying methods behind bistatic radar processing further help the deceptive jammer to either push the true targets away along the range dimension or completely eliminate them from the RDM. Our experiments demonstrated that the deceptive jammer is easy to implement, and its consequences should raise concerns regarding the safety and security applications foreseen in WLAN Sensing, and more generally, in OFDM-based JCAS. We conclude that to guarantee robust and future-proof JCAS systems, electronic-counter-countermeasure techniques must be studied, developed, and included in JCAS standardization. Two important research questions remain to be answered: how deceptive jamming can be applied in a 6G context and how 6G can be designed to be less susceptible than WLAN.

REFERENCES

[1] Z. Wei *et al.*, "Toward multi-functional 6G wireless networks: Integrating sensing, communication, and security," *IEEE Communications Magazine*, vol. 60, no. 4, pp. 65–71, 2022.

[2] J. A. Zhang *et al.*, "Enabling joint communication and radar sensing in mobile networks—a survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 306–345, 2021.

[3] R. Du *et al.*, "An overview on IEEE 802.11 bf: WLAN sensing," in *arXiv preprint arXiv:2207.04859*.

[4] IEEE 802.11bf TG, "IEEE WLAN sensing use cases, official document," https://mentor.ieee.org/802.11/dcn/20/11-20-1712-02-00bf-wifi-sensing-use-cases.xlsx, last accessed: 17/10/2023.

[5] P. Kumari *et al.*, "IEEE 802.11 ad-based radar: An approach to joint vehicular communication-radar system," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 3012–3027, 2017.

[6] T. Ropitault *et al.*, "IEEE 802.11 bf WLAN sensing procedure: Enabling the widespread adoption of Wi-Fi sensing," in *IEEE Communications Standards Magazine*, 2023.

[7] J. A. Zhang *et al.*, "An overview of signal processing techniques for joint communication and radar sensing," in *IEEE Journal of Selected Topics in Signal Processing*, vol. 15, no. 6, 2021, pp. 1295–1315.

[8] G. Tang *et al.*, *Techniques and System Design of Radar Active Jamming*. Springer Nature, 2023.

[9] S. Roome, "Digital radio frequency memory," *Electronics & communication engineering journal*, vol. 2, no. 4, pp. 147–153, 1990.

[10] A. Mpitziopoulos *et al.*, "A survey on jamming attacks and countermeasures in WSNs," *IEEE communications surveys & tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[11] J. Schuerger *et al.*, "Deception jamming modeling in radar sensor networks," in *IEEE Military Communications Conference (MILCOM)*.

[12] A. Almslmany *et al.*, "Advanced deceptive jamming model based on DRFM sub-Nyquist sampling," in *IEEE International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 2016, pp. 727–730.

[13] J. Schuerger *et al.*, "Performance of random ofdm radar signals in deception jamming scenarios," in *2009 IEEE Radar Conference*.

[14] F. Meneghello *et al.*, "Toward integrated sensing and communications in IEEE 802.11 bf Wi-Fi networks," *IEEE Communications Magazine*, vol. 61, no. 7, pp. 128–133, 2023.

[15] M. Malanowski, *Signal processing for passive bistatic radar*. Artech House, 2019.

[16] A. Van Zelst *et al.*, "Implementation of a mimo ofdm-based wireless lan system," *IEEE Transactions on signal processing*, vol. 52, no. 2, pp. 483–494, 2004.

[17] O. Bejarano *et al.*, "IEEE 802.11 ac: from channelization to multi-user MIMO," *IEEE Communications Magazine*, vol. 51, no. 10, pp. 84–90, 2013.

[18] F. Horlin *et al.*, *Digital compensation for analog front-ends: a new approach to wireless transceiver design*. John Wiley & Sons.

[19] H. C. Yildirim *et al.*, "Impact of interference on OFDM based radars," in *IEEE Vehicular Technology Conference (VTC2020-Spring)*, 2020.

[20] H. Levi, "A geometric construction of the dirichlet kernel," in *Transactions of the New York Academy of Sciences*. Wiley Online Library.

[21] M. A. Richards *et al.*, "Principles of modern radar," 2010.

[22] G. D. Durgin, "Space-time wireless channels." Prentice Hall Professional, 2003.