CHALMERS
UNIVERSITY OF TECHNOLOGY

OFDM-based JCAS under Attack: The Dual Threat of Spoofing and Jamming in WLAN Sensing

Citation for the original published paper (version of record):
Yildirim, H., Keskin, M., Wymeersch, H. et al (2025). OFDM-based JCAS under Attack: The Dual Threat of Spoofing and Jamming in WLAN Sensing. IEEE Internet of Things Journal, 12(10): 14511-14525. http://dx.doi.org/10.1109/JIOT.2025.3527062

(article starts on next page)

OFDM-based JCAS under Attack: The Dual Threat of Spoofing and Jamming in WLAN Sensing

Hasan Can Yildirim, *Member, IEEE*, Musa Furkan Keskin, *Member, IEEE*,
Henk Wymeersch, *Fellow, IEEE*, François Horlin, *Member, IEEE*

***Abstract*—This study reveals the vulnerabilities of Wireless Local Area Networks (WLAN) sensing, under the scope of joint communication and sensing (JCAS), focusing on target spoofing and deceptive jamming techniques. We use orthogonal frequency-division multiplexing (OFDM) to explore how adversaries can exploit WLAN's sensing capabilities to inject false targets and disrupt normal operations. Unlike traditional methods that require sophisticated digital radio-frequency memory hardware, we demonstrate that much simpler software-defined radios can effectively serve as deceptive jammers in WLAN settings. Through comprehensive modeling and practical experiments, we show how deceptive jammers can manipulate the range-Doppler map (RDM) by altering signal integrity, thereby posing significant security threats to OFDM-based JCAS systems. Our findings comprehensively evaluate jammer impact on RDMs and propose several jamming strategies that vary in complexity and detectability.**

***Index Terms*—JCAS, ISAC, WLAN sensing, target spoofing, deceptive jammer.**

I. Introduction

Wireless local area network (WLAN) sensing [1] is a pioneering technology within joint communication and sensing (JCAS) [2]. It enables WLAN devices to detect, track, and interpret their environment through radio signals. By leveraging orthogonal frequency-division multiplexing (OFDM), WLAN sensing provides channel measurements that are highly applicable to use cases like indoor localization [3], where two devices, Alice and Bob, alternately function as the transmitter and receiver in a half-duplex mode. In this configuration, as illustrated in Fig. 1, the line-of-sight (LOS) between Alice and Bob serves as a critical timing reference, while echoes from surrounding targets, called surveillance signals, are received and processed by Bob for sensing purposes.

However, WLAN sensing, initially designed as a communication-centric technology, was not built with sensing as its primary focus. Sensing features were integrated later, leading to certain vulnerabilities in the system due to its communication-centric design approach. These vulnerabilities present potential entry points for attackers, making WLAN sensing systems increasingly susceptible to security threats. Attackers could exploit these weaknesses to compromise the system, leading to false readings, data manipulation, or disruption of the sensing function altogether. An attacker, Eve, with sophisticated capabilities could eavesdrop on the sensing-related information and transmit jamming signals, severely distorting the received signals at Bob. These attacks are divided into two categories based on their outcome.

Target spoofing, also known as the preamble or fake-path injection [4], is the first category where artificial targets are injected at Bob. The literature is focused on exploiting the vulnerabilities of Wi-Fi frame detection, synchronization, and channel estimation *to reduce the communication throughput*. In [4], the authors show that joint time and frequency synchronization (JTFS) makes OFDM-based systems vulnerable to attacks. In [5], [6], the frequency and time acquisition algorithms are independently shown to be vulnerable to attacks, and the receiver can be deceived by pilot injection. In [7], [8], vulnerabilities in the channel state information feedback mechanism are exploited. In [9], the orthogonality of OFDM subcarriers is sabotaged by forcing frequency shifts to the subcarriers. Authors in [10] focus on various spoofing attacks, their success rates, and their classifications based on deployment architectures. In [11], how Wi-Fi geolocation spoofing can link devices to their identities is demonstrated. Attacks on public WLAN positioning systems have been explored in [12], showing how precise models can be used to spoof location information. Methods to identify location spoofing devices in wireless networks are investigated in [13], especially when LOS is absent. From a broader view, surveys on OFDM-based network vulnerability can be found in [14], [15], as well as a survey on the physical layer security aspects of OFDM signals in [16].

Deceptive jamming is the second category where the perception of real targets is altered. However, the literature on OFDM-based deceptive jamming is quite sparse. Authors in [17] designed a deceptive jammer against OFDM-based imaging radars which altered the radar image obtained by the receiver. Meanwhile, [18] has shown that randomly generated OFDM signals can be further exploited in deceptive jamming. Authors in [19] designed a novel method to jam frequency diverse arrays under the narrow band assumption. In [20], [21], authors investigate deceptive jamming methods for both static and dynamic objects under the imaging radar framework. In [22], an algorithm for the fast generation of deceptive signals is designed. Traditionally, deceptive jamming relied on advanced digital radio-frequency memory (DRFM) hardware to estimate system parameters and mimic targets,

Hasan Can Yildirim (hasan.can.yildirim@ulb.be) and François Horlin are with the Wireless Communications Group, Université Libre de Bruxelles, Belgium. Musa Furkan Keskin and Henk Wymeersch are with the Department of Electrical Engineering, Chalmers University of Technology, Sweden.

This work was supported, in part, by the European Commission through the Horizon Europe/JU SNS project Hexa-X-II (Grant Agreement no. 101095759), in part by the Swedish Research Council (VR grant 2023-03821), and part by the Chalmers Transport Area of Advance project Towards a Multi-Layer Security Vision for Transportation Systems in the 6G Era.

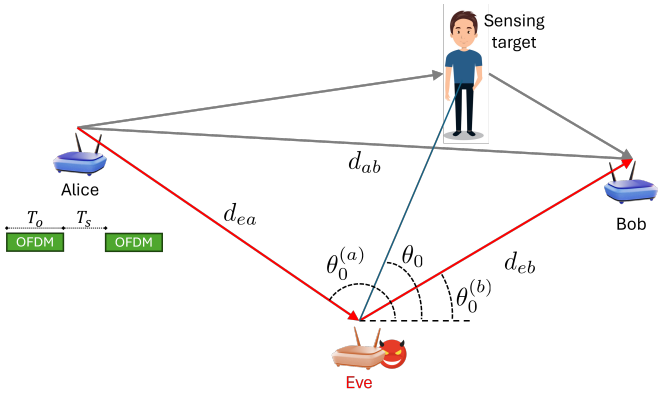

Fig. 1: Jammer scenario topology with relevant line-of-sight (LOS) distances d_{ab}, d_{ea}, and d_{eb}, and LOS angles $\theta_0^{(a)}$, θ_0^b, and θ_0. Alice operates as a pulsed radar by continuously transmitting the same OFDM symbol of duration T_o, with a PRI of $T_s \gg T_o$.

which is costly and complex for civil use [23]. However, WLAN sensing's standardized OFDM symbols enable simpler software-defined radios (SDRs) to perform target spoofing and deceptive jamming without DRFM.

Several countermeasures have been proposed to address these vulnerabilities in OFDM-based JCAS systems. One approach to combating jammers mimicking authorized signals is secure OFDM precoding, as explored in [24]. Other studies, such as [25], propose novel designs like time-frequency modulation using metasurfaces to create deceptive targets in radar profiles. Angle-of-arrival (AoA) based physical-layer authentication, developed in [26], can filter out jammers, while machine and deep learning techniques have been applied to detect 5G signal jammers in [27]–[29]. These approaches show promise, but no single method has emerged as universally effective against all types of jamming signals under every scenario. On the other hand, authors in [30], [31] have shown that fake path injection can be used to increase location privacy in wireless networks. While authors in [32] focus on preventing passive emitter tracking in OFDM-based systems, and in [18] on the effectiveness of randomly generated OFDM waveforms against deceptive jamming.

In this paper, we explore SDRs in WLAN sensing and the security risks they pose on future OFDM-based JCAS systems. While this study focuses on the sensing aspect, it is crucial to point out that this is within the broader context of communication-centric JCAS systems. We believe that our study provides valuable insights into how the reuse of communication systems for sensing opens up new threat vectors, which future JCAS designs must consider, ensuring both secure communication and accurate sensing. We build upon and significantly extend the research originally introduced in our previous conference paper [33], by providing a comprehensive analysis of both target spoofing and deceptive jamming strategies, offering greater control and predictability. By incorporating carrier frequency offset (CFO) into our models, we demonstrate that once Bob synchronizes with Eve's signal, Alice's signal is fully invalidated, ensuring a more deterministic impact on the attacking process for deceptive jamming. By combining various methods that exploit Wi-Fi standardization, advanced jamming strategies are introduced for i) artificial target injection such as overcrowding, selective target injection, and advanced target mimicry, and ii) invalidating the surveillance signal with the preceding jamming signal or the forced synchronization. We also provide an in-depth numerical evaluation of their complexity and effectiveness. Furthermore, the experimental validation is enhanced by implementing these more sophisticated jamming strategies. While giving the jammer extensive capabilities, we maintain the WLAN sensing framework in its current form and focus on RDM-based sensing. This methodology is intended to reveal the vulnerabilities inherent in WLAN sensing systems, and more broadly, in all OFDM-based JCAS systems, when subjected to target spoofing and deceptive jamming.

A. Contributions

Our primary contributions are summarized as follows:

- **Spoofing and Jamming Framework:** We introduce a detailed mathematical framework for target spoofing and deceptive jamming in WLAN sensing systems. We begin with a basic single-antenna, single-target jamming model that highlights the intricacies of signal generation and the interaction between the jamming and legitimate sensing signals. This foundational model is expanded to include more sophisticated scenarios involving multiple antennas and advanced target mimicry techniques. We show that these enhancements allow the jammer to more effectively disrupt the sensing process, significantly increasing the impact of the attack and the jammer's complexity.
- **Evaluation of Strategies and Their Implications:** We systematically evaluate various jamming strategies, considering their complexity, effectiveness, and detectability. Our analysis covers both simple jamming techniques and more advanced methods that exploit vulnerabilities in Wi-Fi standardization. We demonstrate how these strategies can distort RDMs and affect the target detection probabilities, compromising the integrity of the sensing process and posing significant security threats.
- **Experimental Validation with SDR Platforms:** We implement the proposed jamming strategies using SDR platforms to validate our theoretical findings. Our experiments confirm the feasibility of executing sophisticated jamming attacks with relatively simple and accessible hardware, highlighting the real-world applicability of our approach and the pressing need for enhanced security measures in WLAN sensing systems.

B. Related Work

In Table I, the comparison between the relevant works and this study is provided. Authors in [4]–[9] explored jamming strategies that target the communication throughput. To do so, they exploited the JTFS, independent frequency/time synchronization, and known signal structures. Since the focus was on communication throughput, the key performance indicator (KPI) for jamming was mainly the bit-error rate (BER). In [18], authors targeted an imaging radar by exploiting the channel estimation process, and they showed a reduction in target probability of detection (PD). As mentioned earlier, our

Ref.	Target	Exploit	KPI
[4]	Throughput	JTFS	BER
[5]	Throughput	FS	FER
[6]	Throughput	TS	TER
[7]	Throughput	Known signals	BER
[8]	Throughput	Known signals	BER
[9]	Throughput	JTFS	BER
[18]	Imaging	Channel estimation	Target PD
[33]	Sensing	TS	RDM
This study	Sensing	JTFS Known signals Channel estimation	RDM Target PD

TABLE I: The acronyms are FS: frequency synchronization, TS: time synchronization, FER: Frequency synchronization error rate, TER: time synchronization error rate, RDM: range-Doppler map, PD: probability of detection.

previous work [33] targeted WLAN sensing by exploiting only the time synchronization (TS) and the only KPI was RDM. In [33], we discovered the fundamental vulnerabilities of WLAN sensing. The target spoofing was achieved by transmitting OFDM symbols modulated with artificial channel transfer functions. Meanwhile, the deceptive jamming performance was dependent on the time alignment between the cyclic prefix of the legitimate and jamming signals. Eve could either range-shift the true RDM observed by Bob or destroy the subcarrier orthogonality of Alice's signals, effectively turning them into noise. However, these effects were uncontrolled by Eve and occurred randomly. In this study, we continue to target WLAN sensing by exploiting JTFS, known signal structures, and channel estimation procedures. We show RDMs for illustrative purposes, and the main KPI is the target PD.

The remainder of this paper is organized as follows. WLAN sensing framework, the scenario, system model, and radar processing are described in Section II. The basic jammer functionalities, such as signal generation, jammer channel, and the jammed RDM are modeled in Section III. Based on these analyses, various advanced jamming strategies and their complexity and effectiveness are discussed in Section IV. Numerical analyses are provided in Section V, which are experimentally validated in Section VI. Finally, the conclusion is drawn in Section VII.

Notation: Matrices and vectors are given by bold characters, $\mathbf{X}$ and $\mathbf{x}$, respectively. The Hadamard product $\odot$ and division $\oslash$ correspond to the element-wise multiplication and division between matrices or vectors of the same size, respectively. The forward and inverse Fourier transform matrices of size N are defined as $\mathbf{F}_N$ and $\mathbf{F}_N^{\mathsf{H}}$, respectively, where $\mathbf{F}_N^{\mathsf{H}}$ is the Hermitian transpose of $\mathbf{F}_N$. Finally, the phase of a cisoid is obtained as $\angle(e^{-jX}) = -X$.

II. System Model

In this section, we describe the high-level jammer scenario. Then, we detail the sensing framework and signal processing chain under nominal operating conditions (i.e., without a jammer) where we assume that Bob employs RDM-based processing. Finally, we identify the main vulnerabilities in WLAN sensing.

A. Scenario Description

The scenario consists of three stationary devices, Alice, Bob, and Eve, and a mobile target, as shown in Fig. 1. Alice and Bob are involved in the legitimate WLAN Sensing, while Eve acts as the jammer. Table II details the operating modes of the devices during different stages of the process.

TABLE II: Each device's role during a given stage.

WLAN Sensing	Negotiation		Measurement
Alice	Tx	Rx	Tx
Bob	Rx	Tx	Rx
Sensing Attack	Eavesdropping		Jamming
Eve	Rx	Rx	Tx

1) WLAN Sensing: Alice and Bob operate in half-duplex mode, alternating as transmitter (Tx) and receiver (Rx) using OFDM for channel measurements in a bistatic setup. They first exchange sensing parameters during the *negotiation* phase and localize each other while exchanging their roles. Then, Alice sends sensing signals during the *measurement* phase, which Bob receives and processes the surveillance signal for sensing. Bob uses RDM-based processing for sensing, the most common approach.

2) Jamming: While WLAN sensing is taking place, an adversarial device, Eve, intervenes with the WLAN sensing procedure. It transmits signals that can introduce artificial targets to Bob, and potentially invalidate the surveillance signal perceived by Bob. To achieve these, Eve has to operate in a dual capacity: i) as an Rx during sensing negotiation between Alice and Bob to *eavesdrop* on the sensing parameters, and to potentially deduce other metrics related to the topology, and ii) as a Tx during a sensing measurement to emit *spoofing and jamming* signals targeting Bob.

B. WLAN Sensing – Detailed Operation

In this section, we detail the WLAN sensing framework, based on [1] [34]. For the envisioned use cases, we refer to [3]. We describe the sensing stages, the frame structure, the transmitted sensing signal, the surveillance channel, and finally the received-side signal processing chain.

1) Stages of WLAN Sensing: The WLAN sensing uses the protocols initially implemented for multi-user multi-input multi-output in the 802.11ac amendment [35]. In essence, this protocol allows a Tx to trigger channel sounding with explicit feedback from an Rx. To do so, the Tx (Alice) emits two packets called null data packet announcement (NDPA) and null data packet (NDP). Then, Rx (Bob) estimates the channel transfer function (CTF) from the NDP. Depending on the configuration, Bob can either send the estimated CTF back to Alice, or it can compute the RDM itself. The WLAN sensing framework is composed of five stages, summarized as follows:

1) *Sensing session setup* is when Alice discovers potential responders like Bob. Alice and Bob estimate the distance between each other through round-trip time as explained in Appendix B, where we assume that LOS is present and resolvable.
2) *Sensing measurement setup* is when Alice and Bob agree on sensing parameters (such as bandwidth, number of antennas, carrier frequency, pulse repetition interval, and subcarrier grouping) with unprotected over-the-air transmission. Hence, any device can eavesdrop to deduce the sensing parameters.

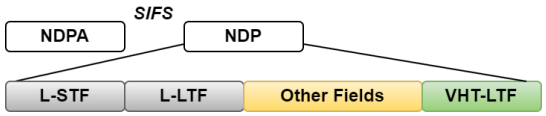

Fig. 2: During a sensing measurement instance, Alice transmits an NDPA and an NDP, separated by SIFS seconds. Only the last field of the NDP, VHT-LTF, is used in channel estimation for sensing.

3) *Sensing measurement instance* is when the sensing takes place, i.e., Alice emits NDPA/NDP, and Bob estimates the CTFs. *WLAN sensing resembles a pulsed-OFDM radar scheme*, where successive NDPA/NDP transmissions are separated by a fixed pulse repetition interval. Since the standard defines the number of samples in NDPA/NDP, Bob knows exactly how many to collect before waiting for the next pulse. This will play a crucial role when the jammer framework is introduced.
4) *Sensing measurement and session termination* are the two stages where Alice and Bob release their resources dedicated to sensing.

For ease of reference, we refer to the combination of the sensing session setup and sensing measurement setup as sensing *negotiation*.

2) Frame Structure during Sensing Measurement: Following the negotiation stages, Alice transmits two frames per sensing measurement instance. These frames are the NDPA and NDP as shown in Fig. 2. The NDPA is a management frame, and its transmission announces that an NDP will follow. It contains information about which devices are involved in the sensing process and typically lasts around 40 to 80 μs. The NDPA triggers the Rx to prepare for receiving an NDP. The NDP is a control frame, transmitted after the NDPA following a short inter-frame space (SISF), typically lasting 10 μs. It contains only the preamble and is used by Bob to perform channel estimation. Bob obtains a range profile with each NDP, and the Doppler profiles are computed over multiple NDPs. The NDP consists of different fields as shown in Fig. 2. The legacy short training field (L-STF) and legacy long training field (L-LTF) are used for joint time-frequency synchronization [36], [37]. The other fields contain higher-level information. Finally, the very high throughput long training field (VHT-LTF) is used in channel estimation for sensing[1]. Without losing any generality, and for clarity, we assume that each sensing measurement instance is composed of only the VHT-LTF, serving for both synchronization and channel estimation. This simplification allows us to model the synchronization and channel estimation more easily.

3) Transmitted Signal: The OFDM parameters are defined as follows: B is the signal bandwidth, f_c is the carrier frequency, Q is the number of subcarriers, Q_{cp} is the cyclic prefix (CP) length, M is the number of OFDM symbols, q and m represent the subcarrier and slow-time indices, respectively, $T = 1/B$, T_o and T_s correspond to the sampling interval, the duration of an OFDM symbol including the CP, and the pulse repetition interval (PRI) which is an integer multiple of T_o, respectively and $T_s \gg T_o$, and $\Delta_f = 1/(QT)$ is the subcarrier spacing. What follows in this section takes place during the sensing measurements instance, hence, we assume that the sensing negotiation already took place. The signal transmitted by Alice is then defined as $\mathbf{S} \in \mathbb{R}^{Q\times M}$ in the frequency domain whose M columns are identical. Here, $\mathbf{S}$ contains standardized BPSK symbols making channel estimation quite straightforward with element-wise divisions [38]. In the time domain, the signal structure resembles a pulsed radar where the OFDM symbols are separated by T_s seconds as shown on Fig. 1.

4) Surveillance Channel: Let us define the steering vectors for the propagation delay as follows

$$\mathbf{d}(\tau) = [1\ e^{-j2\pi\tau\Delta_f}\ \ldots\ e^{-j2\pi\tau(Q-1)\Delta_f}]^T \in \mathbb{C}^{Q\times 1}, \quad (1)$$

where τ_p is the bi-static propagation delay. Similarly, the steering vector for the Doppler frequency shift is defined as

$$\mathbf{b}(f) = [1\ e^{-j2\pi f T_s}\ \ldots\ e^{-j2\pi f(M-1)T_s}]^T \in \mathbb{C}^{M\times 1}, \quad (2)$$

where f is the Doppler frequency. The surveillance channel is modeled under the following assumptions: i) each object is a point in space with diffuse scattering characterized by its radar cross-section, and ii) each path can refer to any reflection, e.g., walls, furniture, mobile objects, etc. These generic assumptions are sufficient for this study [39], [40] since we focus on exposing the vulnerabilities at the signal processing level. The channel model in the frequency domain is defined as

$$\mathbf{H} = \sum_{p=0}^{P} \alpha_p \mathbf{d}(\tau_p)\mathbf{b}^{\mathsf{H}}(f_p), \in \mathbb{C}^{Q\times M}. \quad (3)$$

The path index $p = 0$ models the LOS with complex amplitude $\alpha_0 = a_0 e^{-j2\pi\tau_0 f_c}$, where a_0 represents path gain. The remaining indices model the different paths, each with a complex amplitude α_p, a bi-static propagation delay τ_p, and a bi-static Doppler frequency shift f_p. The propagation delays are assumed to be sorted in increasing order, i.e., $\tau_0 < \tau_1 < \ldots < \tau_P$. Hence $\Delta_\tau = \tau_P - \tau_0$ represents the delay spread of the channel.

5) Receiver Signal Processing Stage 1 – Time-Frequency Synchronization: In a bistatic geometry, the receiver, Bob, needs time and frequency synchronization [1], [41]. To do so, Bob uses an auto-correlation algorithm to estimate the time of arrival based on the detection of amplitude peaks. Hence, assuming that LOS is present and dominant, the signal propagated through it will be used for joint time-frequency synchronization. We define the strongest peak at the output of the lag-1 auto-correlation [42], [43] without losing any generality as follows

$$\Xi[n_0] = |\alpha_0|^2 e^{-j2\pi\eta T_s} + z_0, \quad (4)$$

where z_0 is the noise sample obtained after correlation, and $n_0 = (\tau_0 + \delta_t)/T$ is the sample index of the LOS signal at the correlator's output with δ_t modeling the clock offset (see Appendix A for derivations)[2]. Since the phase of the peak is associated with the CFO, η, between Bob and Alice, Bob can

[1]We focus only on the 802.11ac amendment, which has the VHT acronym. Newer versions of the standard, such as 802.11ax, have different acronyms.

[2]Since we have simplified the frame structure used for sensing, the phase in Equation 4 evolves with T_s which should be replaced by T_o to be fully standard compliant in a real-life setting.

detect the peak at $k = n_0$ for time synchronization[3] and use its phase for frequency synchronization, correcting the CFO via $\hat{\eta} = \angle\Xi[n_0]/(2\pi T_s)$. *This synchronization step will be crucial when the jamming framework is introduced.*

Following the joint time and frequency synchronization, Bob performs the standard OFDM demodulation (removal of CP and FFT over each symbol), leading to the following received signal in the frequency domain:

$$\mathbf{R} = \mathbf{H}_0 \odot \mathbf{S} + \mathbf{Z}, \tag{5}$$

where the entries in $\mathbf{Z} \in \mathbb{C}^{Q\times M}$ correspond to the noise samples in the frequency domain with zero mean and σ^2 variance. Here, the CTF perceived by Bob $\mathbf{H}_0$ is defined as

$$\mathbf{H}_0 = \sum_{p=0}^{P} \alpha_p \mathbf{d}(\tau_p - \tau_0)\mathbf{b}^{\mathsf{H}}(f_p). \tag{6}$$

Here, we assume no time and frequency synchronization errors. Due to prior time synchronization, the propagation delays τ_p are now *relative* to the direct path τ_0 propagation delay. This is indicated by the zero-index on $\mathbf{H}_0$. Meanwhile, the CFO is compensated without errors; hence, the corresponding term does not appear on the estimated CTF. If LOS is missing in the Alice-Bob channel, Bob would synchronize with the first non-LOS (NLOS) path, i.e., $l = 1$, and the delay/Doppler terms in (6) would be relative to that path.

6) Receiver Signal Processing Stage 2 – Radar Processing: The CTF estimated by Bob is defined as follows

$$\hat{\mathbf{H}}_0 = \mathbf{R} \oslash \mathbf{S} = \mathbf{H}_0 + \mathbf{Z} \oslash \mathbf{S}.$$

Since the training fields, $\mathbf{S}$, are composed of BPSK symbols, the CTF estimation does not affect the noise variance, hence, no enhancement in the noise energy. The RDM, $\hat{\mathbf{Y}} \in \mathbb{C}^{Q\times M}$, is obtained through inverse discrete Fourier transforms (IDFT) over q and discrete Fourier transforms over m (DFT) as follows

$$\hat{\mathbf{Y}} = \mathbf{F}_Q \hat{\mathbf{H}}_0 \mathbf{F}_M^{\mathsf{H}}, \in \mathbb{C}^{Q\times M}. \tag{7}$$

where matrix $\hat{\mathbf{Y}}$ contains $P + 1$ peaks. The peak at zero-range/zero-Doppler corresponds to the direct path used as the reference, while the remaining P peaks correspond to the target echoes. Once an RDM is obtained, a constant false-alarm rate (CFAR) detector separates the target echo peaks from noise peaks [41]. Finally, we define the RDM processing operator $\hat{\mathbf{Y}} = \mathbf{\Sigma}(\hat{\mathbf{H}})$ which encapsulates the range IDFT and Doppler DFTs as described in (7).

C. Vulnerabilities

For future reference, we underline the following facts since they will play a crucial role in jamming. First, the transmitted signals, $\mathbf{S}$, are standardized and known. This makes the target spoofing and deceptive jamming with SDRs much easier since signal reconstruction can be bypassed. Secondly, Bob synchronizes to the peak with the largest amplitude at the output of its correlator. This allows Eve to deceive Bob in different ways.

[3]This approach allows the receiver to synchronize with the time-of-arrival, but neither δ_t nor τ_0 can directly be estimated from n_0.

III. Target Spoofing and Deceptive Jamming Framework

The framework focuses on generating artificial channel transfer functions (CTFs) to modulate the OFDM symbols. When these symbols are transmitted, they will alter Bob's perception of the true CTFs. Furthermore, we assume that Eve knows the type of signal processing employed by Bob, i.e., RDM-based. If Bob uses other methods for sensing, the attack may be less effective. However, Eve can adapt its jamming method for a variety of methods, which should be considered in future work.

The jammer, Eve, has two main goals. The first one is to *inject artificial targets* into Bob's RDM as in target spoofing. The second goal is to *invalidate the surveillance signal* and the true target echoes that it contains as in deceptive jamming. If Bob employs other sensing methods, e.g., channel state information-based sensing, Eve's attacking method should be updated accordingly. To achieve its goals, we assume that Eve knows the sensing parameters[4] $(Q, Q_{cp}, M, T, f_c, T_s)$ established between Alice and Bob during the sensing negotiation. Moreover, the channel parameters for each bistatic geometry (Alice-Bob, Alice-Eve, and Eve-Bob) are assumed to be different.

A. Time Alignment between the Surveillance and Jamming Signals at Bob

Jamming takes place during a sensing measurement where Alice is transmitting sensing signals. Timing the signal transmission is crucial for Eve to ensure a successful attack. Although the distances, and the propagation delays, between the devices can be quite low in many scenarios, the frame structure shown in Fig. 2 helps Eve in timing its signal transmission. Since an NDPA lasts at least $40\mu s$ [1], Eve has enough time to detect the transmissions on air and time its transmission [7]. Moreover, Bob has a time frame to receive these sensing signals. Hence, Eve's transmission should fall within this time frame. Since the duration of this time frame is not standardized, we consider various time alignment cases between Alice's and Eve's signals. Due to the nature of the OFDM waveform, these time alignment cases have different consequences. The corresponding cases are shown in Fig. 3 and summarized as follows.

- *Case 1: Eve's signal arrives earlier than Alice's:* There is no alignment between the two signals[5]. Hence, Bob synchronizes with Eve's signal, collects a predetermined amount of samples, and waits for the next OFDM symbol while completely omitting Alice's signal.
- *Case 2: Alice's and Eve's signals are partially aligned:* Bob will detect two peaks at the correlator output and synchronize with the one having the largest amplitude [42]. Whether Eve's signal arrives earlier (2a) or later

[4]Either by eavesdropping during sensing negotiation or sensing measurement. The former is more straightforward since it only involves demodulating the appropriate fields in the preamble. The latter is more complicated since it requires the estimation of all the parameters directly from samples.

[5]The tail of Eve's signal may align with the CP of Alice's signal. In this case, the surveillance channel may be observed at very large distances, e.g., hundreds of meters, and the peaks will be ignored by Bob.

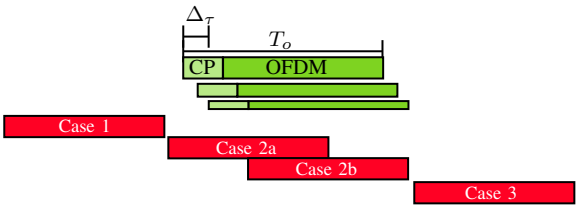

Fig. 3: Different signal alignment cases during jamming. Green and red boxes correspond to Alice and Eve signals, respectively, while Δ_τ and T_o are the delay spread and OFDM symbol duration, respectively.

Parameter\Channel	A-B	B-E	E
Number of targets	P	L	1
Path index	p	l	-
Path gain	α_p	$\alpha_l^{(b)}$	$\bar{\alpha}$
Path delay	τ_p	$\tau_l^{(b)}$	$\bar{\tau}$
Path Doppler frequency	f_p	$f_l^{(b)}$	$\bar{f}$
Path angles	θ_p	$\theta_l^{(b)}$	-
CFO	η	$\eta^{(b)}$	$\bar{\eta}$

TABLE III: From left to right, the columns correspond to the Alice-Bob (A-B) and Bob-Eve (B-E) pairs, while the last column corresponds to the parameters of the artificial target generated by Eve (E).

(2b) has different consequences which are detailed in Section III-B3.

- *Case 3: Eve's signal arrives later than Alice's:* Bob will only sample Alice's signals, causing jamming to fail.

Since the 802.11 standard does not dictate specific receiver design, hardware vendors have the flexibility to determine Bob's timing window for signal reception. If Bob has a reliable RTT-based distance estimation and is configured to operate with a very narrow timing window, then the scenario described in Case 1 would likely be invalid. In such a configuration, Bob would only be vulnerable against Case 2.

B. Jammer Operation

The mathematical models are only derived for Case 2, which is the most general one. Due to the introduction of the jamming signal, there will be four different sets of channel parameters and CFOs, i.e., path gains, delays, Doppler shifts, and angles per channel. These are summarized in Table III for easy reference. Even though the number of targets can potentially be equal (i.e., $P = L$), their channel parameters will not be, i.e., amplitudes $\alpha_p \neq \alpha_l^{(b)}$, propagation delays $\tau_p \neq \tau_l^{(b)}$, and Doppler frequencies $f_p \neq f_l^{(b)}$ for $\forall p, l$.

1) Jamming Transmitter: Eve generates the deceptive signal by reversing the radar processing stages and exploiting the delay-frequency and time-Doppler dualities in [39]. Let us define the artificial RDM as $\bar{\mathbf{Y}}_j$ that contains two peaks: i) at zero-range/zero-Doppler with unit amplitude, corresponding to the reference peak, and ii) at $\bar{\tau}$ delay and $\bar{f}$ Doppler frequency with $\bar{\alpha}$ amplitude, corresponding to the artificial target. For the sake of simplicity, we include only one artificial target, but in more advanced scenarios, many artificial targets can be included. We also focus on generating an artificial RDM for a single radar snapshot. However, Eve can alter the artificial path parameters $(\bar{\alpha}, \bar{\tau}, \bar{f})$ over multiple snapshots, and generate multiple RDMs $\bar{\mathbf{Y}}_j$ successively. For a single snapshot, applying the radar processing in reverse order yields

$$\bar{\mathbf{H}} = \mathbf{F}_Q^{\mathsf{H}} \bar{\mathbf{Y}}_j \mathbf{F}_M = \mathbf{1} + \bar{a}\mathbf{d}(\bar{\tau})\mathbf{b}^{\mathsf{H}}(\bar{f}), \in \mathbb{C}^{Q\times M}. \quad (8)$$

Here, $\mathbf{1} \in \mathbb{R}^{Q\times M}$ is a matrix of ones which allows us to generate a reference peak at zero-range/zero-Doppler. With the second term, a single artificial and mobile target is generated with amplitude $\bar{\alpha}$, propagation delay $\bar{\tau} > 0, \bar{\tau} \in \mathbb{R}$, and Doppler frequency $\bar{f} \in \mathbb{R}$. Then, after modulating each subcarrier with $\bar{\mathbf{H}}$ and $\mathbf{S}$, the symbols that will be transmitted are defined as $\bar{\mathbf{H}} \odot \mathbf{S}, \in \mathbb{C}^{Q\times M}$. Finally, these modulated OFDM symbols can now be transmitted in the time domain by computing the IDFT over q and adding the CP.

2) Jamming Channel: During the sensing measurement instance, Eve transmits the jamming signals through the channel between itself and Bob. We denote the corresponding frequency-domain channel by

$$\mathbf{B} = \sum_{l=0}^{L} \alpha_l^{(b)} \mathbf{d}(\tau_l^{(b)}) \mathbf{b}^{\mathsf{H}}(f_l^{(b)}) \in \mathbb{C}^{Q\times M}. \quad (9)$$

Here, $\alpha_l^{(b)}$, $\tau_l^{(b)}$, and $f_l^{(b)}$ correspond to the amplitude, propagation delay, and Doppler frequency of the lth path between Eve and Bob. Meanwhile, $l = 0$ refers to the LOS, and since the device is assumed to be stationary, $f_0^{(b)} = 0$.

3) Receiver Signal Processing Stage 1 – Time-Frequency Synchronization: If a jammer is present, Bob can be forced to synchronize with the jammer signal. The only requirement is that the signal transmitted by Eve, and propagated through the LOS with Bob (Eve-LOS), should have 3 dB or more power at Bob than the one transmitted by Alice, and propagated through the corresponding LOS (Alice-LOS) [42].

As described in Section II-B5, Bob computes the lag-1 auto-correlation over the received samples. In this case, there are two strict peaks at the following indices: $k = n_0$ and $k = n_0^{(b)}$ where $n_0^{(b)} = (\tau_0^{(b)} + \bar{\delta}_t)/T$ represents the time of arrival of Eve-LOS, with $\bar{\delta}_t$ being the clock offset. Similar to the definition of $\Xi[n_0]$ in (4), $\Xi[n_0^{(b)}]$ can be defined as

$$\Xi[n_0^{(b)}] = |\alpha_0^{(b)}|^2 e^{-j2\pi\eta^{(b)}T_s} + z_0, \quad (10)$$

where $\eta^{(b)}$ refers to the CFO between Eve and Bob. Since Bob synchronizes to the peak with the largest magnitude at the output of the correlator, and if we assume that $20\log_{10}(|\alpha_0^{(b)}|) - 20\log_{10}(|\alpha_0|) > 3$dB (whether because $d_{eb} < d_{ab}$ or because Eve's transmit power is adjusted accordingly), Bob will time and frequency synchronize to Eve's jamming signal. This forced synchronization comes with different consequences.

- *Time synchronization implication:* If $n_0^{(b)} < n_0$, i.e., the jamming signal arrives *earlier* than the surveillance signal, Bob will be time synchronized with an earlier clock corresponding to the Case 2a. Hence, the targets on the surveillance RDM will be range-shifted[6]. On the other hand, if $n_0^{(b)} > n_0$ the jammer signal arrives *later* than the legitimate signal. If in addition $n_0^{(b)} - n_0 > Q_{cp}$ and $T_o = T_s$, the surveillance signal will be sampled beyond its CP, destroying its subcarrier orthogonality. These two cases have been studied in our earlier publication [33] and also in [6], [9].

[6]In case target echoes arrive later than $n_0^{(b)}$, there will be also intersymbol interference. However, considering the minimum duration of the CP (which is $0.8\mu s$), the targets should be beyond 120 meters to satisfy the given condition. Hence, we omit this interference term.

- *Frequency synchronization implication:* Bob will synchronize to the CFO of Eve, i.e., $\eta^{(b)}$. Hence, assuming the CFO is estimated without any errors, and if $\eta - \eta^{(b)}$ is significantly large[7], the subcarrier orthogonality of the surveillance signal will be completely lost, turning it into interference regardless of the time alignment between the two signals as studied in [5]. Hence, Bob will not be able to observe the surveillance channel at all.

In summary, if Bob can be forced to synchronize with Eve, Alice's surveillance signal will experience inter-carrier interference (ICI), mainly due to the CFO, but potentially due to sampling beyond the CP. Regardless, the surveillance RDM will be corrupted. Moreover, the CFO will shift the surveillance RDM along the speed dimension since it has the same effect as the Doppler frequency shift.

Following the time-frequency synchronization, Bob perceives the channel between Eve and itself as follows

$$\mathbf{B}_0 = \sum_{l=0}^{L} \alpha_l^{(b)} \mathbf{d}(\tau_l^{(b)} - \tau_0^{(b)}) \mathbf{b}^{\mathsf{H}}(f_l^{(b)}), \in \mathbb{C}^{Q \times M} \tag{11}$$

where the delays are modeled relative to the direct path.

If LOS is missing in the Eve-Bob channel, the forced synchronization would still work as long as the first Non-LOS (NLOS) path, i.e., $l = 1$, is stronger than the LOS (or NLOS) in the Alice-Bob channel. However, the drawback is that the delays and Dopplers in (11) would become relative to the NLOS path. Hence, the artificial target will not appear on the intended RDM cell.

4) Receiver Signal Processing Stage 2 – Radar Processing: Assuming that Bob is force-synchronized with Eve, and demodulates the OFDM symbols, the estimated CTF takes the following form

$$\hat{\mathbf{H}}_j = \underbrace{\mathbf{B}_0 \odot \bar{\mathbf{H}}}_{=\mathbf{G}_1} + \underbrace{\mathbf{H}' \odot \mathbf{C}}_{=\mathbf{G}_2} + \mathbf{Z}. \tag{12}$$

Here, $\bar{\mathbf{H}}$ is the artificial CTF, introduced in (8), $\mathbf{B}_0$ corresponds to the physical channel between Eve and Bob, $\mathbf{H}'$ is the desynchronized surveillance channel, and $\mathbf{C}$ is the ICI. They are now described in detail. Hence, the first Hadamard product yields

$$\mathbf{G}_1 = \mathbf{B}_0 \odot \bar{\mathbf{H}} = \mathbf{B}_0 + \sum_{l=0}^{L} \alpha_l^{(b)} \bar{\alpha} \mathbf{d}(\tau_l^{(b)} - \tau_0^{(b)} + \bar{\tau}) \mathbf{b}^{\mathsf{H}}(f_l^{(b)} + \bar{f}). \tag{13}$$

Compared to the channel $\mathbf{H}_0$ observed in (6), there are different types of targets observed in $\mathbf{G}_1$. The first term corresponds to the channel between Eve and Bob $\mathbf{B}_0$ and is present due to the reference peak in the artificial RDM. The second term with $l = 0$ corresponds to the artificial target injected on delay/Doppler cell $(\bar{\tau}, \bar{f})$ when $l = 0$. The remaining L terms on delay/Doppler cells $(\tau_l^{(b)} + \bar{\tau}, f_l^{(b)} + \bar{f})$ are the real targets affected by the presence of the artificial target.

The desynchronized surveillance channel is

$$\mathbf{H}' = \sum_{p=0}^{P} \alpha_p \mathbf{d}(\tau_p - \tau') \mathbf{b}^{\mathsf{H}}(f_k^{(a)} + \eta_w), \tag{14}$$

[7]Usually above $B/(2Q)$ is sufficient.

where the delays are now relative to $\tau' = \tau_0^{(b)} + \bar{\delta}_t$ due to the time synchronization and $\eta_w = \eta - \eta^{(b)}$ is the combined CFO. Consequently, the desynchronized surveillance channel $\mathbf{H}'$ contains the same $P + 1$ peaks as $\mathbf{H}_0$ but these peaks are shifted in delay by τ' and in Doppler by η_w.

Finally, the ICI, present due to the forced time and frequency synchronization, is modeled with $\mathbf{C} = \mathbf{P}\mathbf{S}\mathbf{\Lambda}$, [38] where the entries in $\mathbf{P} \in \mathbb{C}^{Q \times Q}$ are defined as

$$P[q, i] = \frac{1 - e^{j2\pi(\frac{q-i}{Q} - \eta_w T)Q}}{1 - e^{j2\pi(\frac{q-i}{Q} - \eta_w T)}} \tag{15}$$

and the entries of the diagonal matrix $\mathbf{\Lambda} \in \mathbb{C}^{M \times M}$ are given as $\Lambda[m, m] = e^{-j2\pi\eta_w m T_s}$. For later reference, we define the second Hadamard product as $\mathbf{G}_2 = \mathbf{H}' \odot \mathbf{C}$. Here, $\mathbf{C}$ mixes the subcarriers and greatly affects the detectability of real target peaks.

The jammed and corrupted RDM is obtained by range/Doppler processing $\hat{\mathbf{H}}_j$ as follows

$$\begin{aligned} \hat{\mathbf{Y}}_j &= \mathbf{F}_Q \hat{\mathbf{H}}_j \mathbf{F}_M^{\mathsf{H}} \\ &= \underbrace{\mathbf{F}_Q \mathbf{G}_1 \mathbf{F}_M^{\mathsf{H}}}_{=\mathbf{Y}_{\mathbf{G}_1}} + \underbrace{\mathbf{F}_Q \mathbf{G}_2 \mathbf{F}_M^{\mathsf{H}}}_{=\mathbf{Y}_{\mathbf{G}_2}} + \underbrace{\mathbf{F}_Q \mathbf{Z} \mathbf{F}_M^{\mathsf{H}}}_{=\mathbf{Y}_{\mathbf{Z}}} \end{aligned} \tag{16}$$

Remark 1. *The model in* (16) *can be generalized for the different time alignment cases from Fig. 3:*

$$\hat{\mathbf{Y}}_j = \begin{cases} \mathbf{Y}_{\mathbf{G}_1} + \mathbf{Y}_{\mathbf{Z}} & \textit{Case 1} \\ \mathbf{Y}_{\mathbf{G}_1} + \mathbf{Y}_{\mathbf{G}_2} + \mathbf{Y}_{\mathbf{Z}} & \textit{Case 2} \\ \hat{\mathbf{Y}} + \mathbf{Z} & \textit{Case 3.} \end{cases} \tag{17}$$

If the time alignment corresponds to the first case, then only the first Hadamard product remains in (16) *since Alice's signal falls completely outside of the sampling window. The second case corresponds to the model provided in* (16)*. Finally, the third case corresponds to the model provided in* (7) *where the surveillance channel is estimated as it is. Since Eve's jamming signals are not present at all, the jamming fails.*

C. Achieving the Jammer Goals

From (16), the RDM comprises two terms, given by the two Hadamard products, and they correspond to Eve's goals.

1) Injecting artificial targets: This goal is achieved by the first Hadamard product, $\mathbf{Y}_{\mathbf{G}_1}$, which combines the RDM between Eve and Bob ($\mathbf{Y}_{\mathbf{B}_0} = \mathbf{F}_Q \mathbf{B}_0 \mathbf{F}_M^{\mathsf{H}}$) with the artificially generated RDM ($\mathbf{Y}_{\bar{\mathbf{H}}} = \mathbf{F}_Q \bar{\mathbf{H}} \mathbf{F}_M^{\mathsf{H}}$). Here, $\mathbf{Y}_{\mathbf{B}_0}$ includes a reference peak at zero-range/zero-Doppler and physical targets at various range-Doppler cells, while $\mathbf{Y}_{\bar{\mathbf{H}}}$ includes an artificial mobile target and a reference peak. This product results in weighted, and range/Doppler-shifted copies of $\mathbf{Y}_{\bar{\mathbf{H}}}$ according to the peaks in $\mathbf{Y}_{\mathbf{B}_0}$, with its reference peak serving as the baseline.

Limitations: The main drawback of injecting artificial targets is that each peak in $\mathbf{Y}_{\mathbf{B}_0}$ adds an extra copy of $\mathbf{Y}_{\bar{\mathbf{H}}}$, potentially overcrowding the RDM. Although beneficial for Eve, this could alert Bob to an anomaly.

2) Invalidating the surveillance RDM: The second goal uses the Hadamard product $\mathbf{Y}_{\mathbf{G}_2}$, which reflects the interaction between the desynchronized surveillance channel $\mathbf{H}'$ and the ICI effects, $\mathbf{C}$. Without CFO and ICI, the surveillance channel remains observable as $\mathbf{Y}_{\mathbf{H}'} = \mathbf{F}_Q \mathbf{H}' \mathbf{F}_M^{\mathsf{H}}$. However, the ICI

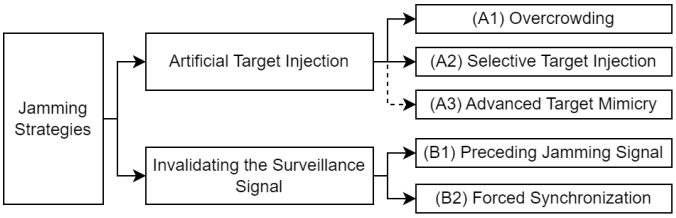

Fig. 4: Different jamming strategies to achieve Eve's goals.

matrix $\mathbf{C}$ spreads the energy across the range dimension after the range IDFT. Then, the Doppler DFT focuses this energy along a single Doppler cell relative to CFO, causing a so-called ridge [44]. Hence, each real target peak in $\mathbf{Y}_{\mathbf{H}'}$ will be replaced by range/Doppler shifted copies of this ridge.

Limitations: The first limitation is that Bob can detect the ridges, which are known indicators of OFDM-based radar interference and can respond effectively when detected. The second limitation is that Eve may unintentionally sabotage its artificial targets if they are aligned with the ridges.

IV. Advanced Jamming Strategies: A Qualitative Analysis

More advanced jamming strategies and their combinations are provided and discussed in this section, as visualized in Fig. 4. First, artificial target injection strategies will be discussed, where the options are either overcrowding (A1) or selective target injection (A2). Both of these strategies can be further enhanced with advanced target mimicry (A3). Second, we will discuss methods to invalidate the surveillance signal by preceding jamming signal (B1) or by forced synchronization (B2). Finally, we will qualitatively rate these strategies based on their simplicity/complexity and various effects on Bob.

A. Injecting Artificial Targets

1) Overcrowding: This type of target spoofing introduces *many* targets to Bob, including artificial ones from Eve, real targets between Eve and Bob, and combinations of both. Hence, Eve cannot fully control where the real targets will appear in the range/Doppler cells. To overcrowd Bob's CFAR output, Eve keeps the first Hadamard product in (16) unchanged, introducing $2(L+1)$ targets. The artificial target appears at the intended RDM cell, while real targets are range/Doppler shifted based on the artificial target's parameters.

2) Selective Target Injection: This type of target spoofing gives Eve full control over the targets introduced to Bob. To ensure only the artificial target appears in Bob's CFAR output, Eve should exploit only the LOS path, which can be achieved by using multiple antennas. During the sensing negotiation, Eve estimates angles using subspace-based methods like MUSIC [45] or ESPRIT [46], then constructs a precoder to focus a beam towards Bob while nulling other real target paths. Once the radiation pattern is optimized, only the LOS term will remain in (11), and Bob will receive a single target at zero-range/zero-Doppler.

3) Advanced Target Mimicry: Bob may use technologies for target tracking and micro-Doppler analysis, and Eve can enhance deception by exploiting these. To force Bob to track the artificial target, Eve can update (8) over multiple snapshots following Newtonian kinematics, aligning with the tracking filters' equations. Simultaneously, Eve can mimic micro-Doppler signatures using empirical data or simulated patterns, such as simulating human walking motion with the Boulic model [47] via Matlab's radar toolbox.

B. Invalidating the Surveillance Signal

As pointed out in (17), Eve has two options to invalidate the surveillance signal. Eve can benefit from estimating the distances shown in Fig. 1[8]. This can be done using the round-trip time when Alice and Bob alternate as Tx and Rx during the sensing negotiation stage, as outlined in Appendix B. Although topology parameters, such as LOS distances, might be known beforehand, our analysis will focus on estimating them through signal processing.

1) Preceding Jamming Signal: If Eve can ensure the Case 1 signal alignment, then Bob will not perceive the surveillance signal. This corresponds to the best strategy for invalidating the surveillance signal. To successfully implement this strategy, Eve must accurately estimate the round-trip times (see in Appendix B) and the transmission schedule of Alice. By doing so, Eve can time its transmissions so that Bob receives only the jamming signal, and collects the predetermined amount of samples, thereby rendering the legitimate signal invisible.

2) Forced Synchronization: If signals are aligned as in Case 2, Eve must force Bob to synchronize with itself rather than Alice. This leads to ICI on the surveillance signal, where ridges replace target peaks. Two conditions are necessary. First, Eve's jamming signal power must exceed the surveillance signal power at Bob. To achieve this, Eve must know the distances between Alice and Bob (d_{ab}) and between itself and Bob (d_{eb}), and adjust its transmit power accordingly without overdoing it to remain stealthy. Second, Eve needs to estimate the CFO between itself and Alice ($\eta^{(a)}$) and Bob ($\eta^{(b)}$), then compute $\hat{\eta} = \eta^{(b)} - \eta^{(a)}$. Eve can introduce a much larger CFO, $\bar{\eta}$, ensuring a corrupted surveillance signal.

C. Qualitative Analysis

Now that various jamming strategies and different options to achieve them are discussed, they are qualitatively analyzed in Table IV. (A1) Overcrowding Bob is the simplest approach since it has no additional requirements other than a single antenna. However, it introduces the real targets along with the artificial ones. (A2) If only the artificial targets are desired at Bob, then multiple antennas are needed for beamforming. Then Eve can exploit the LOS with Bob, and avoid illuminating the real targets, greatly increasing the jamming

[8]The topology parameters, e.g., the LOS distances, can be known before jamming without signal processing. The attacker may access the network topology, e.g., networks in public areas, or perform other measurements, e.g., distance measurement with laser meters. Having access to such information makes the attacker more effective for jamming. However, for the sake of brevity, our analysis will only focus on estimating these parameters with signal processing.

TABLE IV: Different jamming strategies. Requirements are defined as $\mathcal{S}$: single antenna, $\mathcal{M}$: multiple antennas, $\mathcal{P}$: additional processing unit for tracking/micro-Doppler signatures, $\mathbf{\Theta}$: LOS AoAs, $\mathcal{D}$: LOS distances, $\mathcal{T}$: timed transmission algorithm, $\mathcal{F}$: CFO estimation.

Strategy	Requirement tags	Complexity	Effectiveness	Detectability by Bob	Target presence
Overcrowding (A1)	$\mathcal{S}$	Very low	Low	High	Artificial+True+Combined
Selective Target Injection (A2)	$\mathcal{M}, \mathbf{\Theta}$	Moderate	High	Moderate	Artificial+True
Advanced Target Mimicry (A3)	$\mathcal{P}$	High	Very High	Low	Artificial+True+Combined
Preceding Jamming Signal (B1)	$\mathcal{S}/\mathcal{M}, \mathcal{D}, \mathcal{T}$	High	Very High	Very Low	Artificial+Combined
Forced Synchronization (B2)	$\mathcal{S}/\mathcal{M}, \mathcal{D}, \mathcal{F}$	Moderate	High	Moderate	Artificial+Ridges

TABLE V: System and topology parameters for numerical analysis, where p_A, p_B, p_E, and p_T correspond to the 2D coordinates of Alice, Bob, Eve and the Target, respectively. The velocity vector and radar cross-section of the target are indicated by v_T and σ_T, respectively.

Parameter	Value	Parameter	Value
Q	1024	p_A	$(10\text{m}, 0\text{m})$
Q_{cp}	64	p_B	$(0\text{m}, 0\text{m})$
B	80 MHz	p_E	$(5\text{m}, 10\text{m})$
M	128	p_T	$(5\text{m}, 10\text{m})$
M_o	100	v_T	$(-3\text{m/s}, -3\text{m/s})$
f_c	5 GHz	σ_T	0.1m^2

effectiveness. However, it comes with increased complexity due to the AoA estimations and beamforming. (A3) Mimicking realistic target signatures is the most effective but complicated way to deceive Bob, especially when this is combined with A2. (B1) Preceding jamming signal provides the best method to invalidate the surveillance signal since it will not be observed at all. However, it requires the estimation of the device distances, transmission schedules, and a timed transmission algorithm which will greatly increase the complexity. (B2) Forced synchronization is a reliable option if B1 is not available, since ridges replace the true target peaks. However, the presence of the ridges can alert Bob, making it react accordingly. Moreover, Eve has to estimate the device distances to adjust its transmit power, and the relative CFO to create ICI.

V. Numerical Analyses

A. Simulation Parameters

The radar parameters and topology information can be found in Table V. We use the Blackman window for sidelobe suppression along the range and speed dimensions. It is important to note that the RDMs shown here are not derived from the numerical solution of (7) or (16). Instead, they result from a full radar chain simulation, including channel propagation with convolution, time-frequency synchronization with correlation, and subsequent radar processing.

B. Results and Discussion

In this section, we provide results for the target spoofing and deceptive jamming performance of Eve. Initially, we analyze Bob's RDMs on a realization basis. In Fig. 5, target spoofing strategies, and in Fig. 6 combined strategies are evaluated. Then, we evaluate the overall spoofing and jamming performance of Eve where the main key performance indicator is the probability of detection (PD) of targets. In Fig. 7, the PD is analyzed as a function of the artificial CFO. In Fig. 8, the PD is analyzed as a function of jammer-to-signal-ratio (JSR). In Fig. 9, overall jamming performance is studied where we compare the missed detection rate of real targets with the PD of artificial targets. Finally, in Fig. 10, the detection rate is evaluated for the different probability of false alarms (PFa)

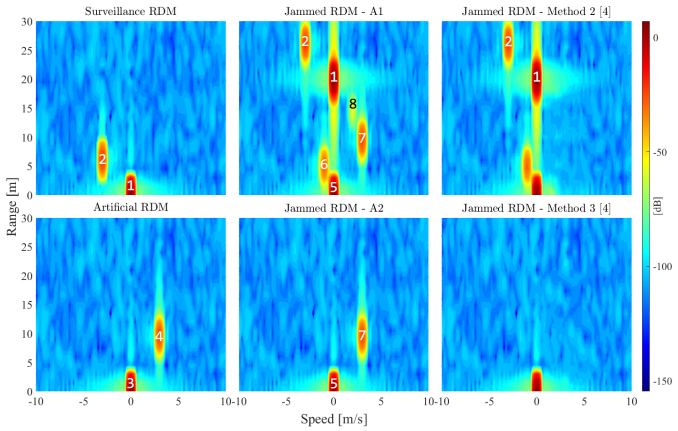

Fig. 5: Six RDMs are provided. The first column shows the surveillance and artificial RDMs in isolation. The second column corresponds to jammed RDMs with A1 and A2 strategies. The third column corresponds to the methods in [4], adapted and implemented for sensing. As a comparison, surveillance RDM and artificial RDM correspond to case 3 and case 1 types of time alignments, respectively.

and number of real targets. In all the detection-related studies, the OS-CFAR [48] algorithm is used.

1) Injecting Artificial Targets: In Fig. 5, the RDMs illustrate WLAN sensing and artificial target injection. The surveillance RDM shows the physical channel between Alice and Bob with synchronization peak $\langle 1 \rangle$ and the target $\langle 2 \rangle$. Eve's artificial RDM contains synchronization peak $\langle 3 \rangle$ and artificial target $\langle 4 \rangle$. The upper-middle RDM, A1 jamming, shows Bob synchronizing with Eve's signal, where peak $\langle 5 \rangle$ corresponds to $\langle 3 \rangle$, and the real target between Eve and Bob appears as peak $\langle 6 \rangle$. Though at a different range/speed than $\langle 2 \rangle$, it is still detectable. The artificial target peak $\langle 7 \rangle$ appears at its intended spot and the combination of artificial and real targets forms peak $\langle 8 \rangle$. Here, Eve's LOS arrives earlier than Alice's, shifting Bob's time synchronization, and causing the surveillance RDM to appear beyond 20 meters. In other cases, peaks may be beyond CFAR detection limits, causing Bob to discard them. The bottom-middle RDM, A2 jamming, shows beamforming's effect—nulling the real target makes it undetectable, leaving only the artificial target visible. Here, Alice's LOS arrival time is intentionally forced to arrive much later during simulations, making the surveillance RDM disappear. These findings align with those in [32]. For comparison, the throughput jamming methods from [4] are adapted to disrupt the sensing session. In method 2, an injected preamble arrives before Alice's signal, which Bob uses to synchronize, causing a range shift on the surveillance RDM. However, the true target still appears. In method 3, the injected preamble arrives significantly later than Alice's signal, and due to the beamforming, no additional paths are illuminated. As a result, only the reference peak appears on the RDM. In both cases, Eve does not introduce

artificial targets. These findings indicate that the methods in [4] provide some effectiveness for deceptive jamming, but they are inadequate for target spoofing.

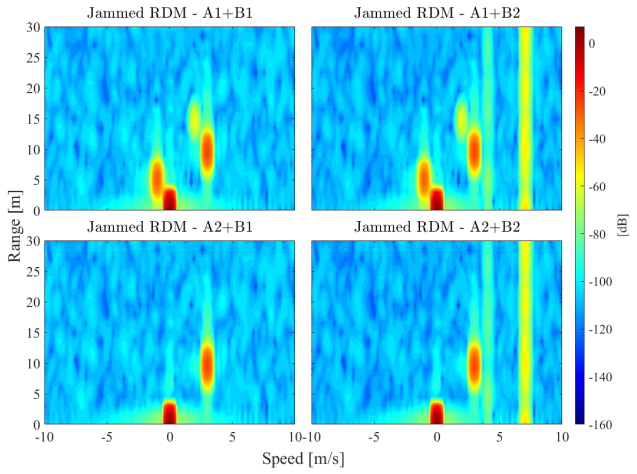

Fig. 6: Four RDMs for different strategy combinations. The best jamming performance is the combination of A2 and B1 where only the artificial target peak is present.

2) Combined Strategies: In Fig. 6, four RDMs display the effects of combining different jamming strategies. The top-left RDM shows overcrowding and preceding jamming, the true surveillance channel is obscured, but true and combined targets remain visible. In the top-right RDM overcrowding and forced synchronization are combined. Alice's and Eve's signals are somewhat aligned, and the surveillance RDM is present. However, ICI caused by CFO spreads the energy along the range dimension, forming ridges $\langle 1 \rangle$ and $\langle 2 \rangle$. The speed dimension remains unaffected since symbol-to-symbol phase shifts remain unaffected, though Doppler shifts occur due to CFO. The bottom-left RDM combines selective injection and preceding jamming. It is the most effective strategy since only the artificial RDM is visible without extra targets or ridges. Lastly, the bottom-right RDM combines selective injection and forced synchronization, where surveillance peaks are replaced with ridges, though additional targets are absent due to beamforming.

3) Target Detection Probability vs. CFO: In Fig. 7, the effect of CFO on the PD of real and artificial targets in the forced synchronization strategy is examined for 10 dB JSR. With wider subcarrier spacing (312 kHz, as in 802.11ac), when the CFO is below 3 ppm, the range IDFT focuses energy on a range cell, allowing the real target to be detected. However, above 3 ppm, *the PD of the real target drops significantly* as energy spreads along the range, creating ridges. For narrower subcarrier spacing (78 kHz, as in 802.11ax), the system is more sensitive to CFO, with a critical threshold of around 1 ppm, beyond which PD rapidly declines. In contrast, *the PD of detecting the artificial target remains unaffected by subcarrier spacing or CFO*, as the CFO impacts only the surveillance signal, not the jamming signal. However, if the ridges caused by the CFO and the artificial target are aligned along the speed dimension, the artificial target may not be detected. Thus, Eve could unintentionally undermine its target

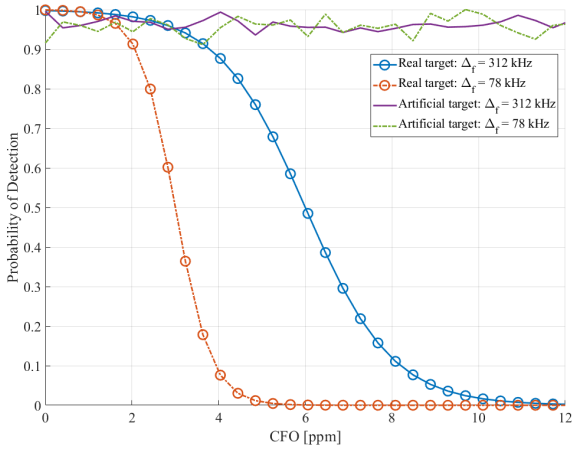

Fig. 7: Probability of detecting real and artificial targets as a function of CFO for two different subcarrier spacings: 312kHz for 802.11ac and earlier, 78kHz for 802.11ax and later. The OS-CFAR [48] algorithm is used for target detection, with 10^{-6} as the probability of false alarm. The real target speed is randomized over 5k realizations for each CFO value.

spoofing. This explains why the PD of the artificial target is not 100% and varies with different CFO values–sometimes the ridges conceal the artificial target. This is unavoidable since Eve does not know the real target's speed relative to the Alice-Bob channel.

4) Target Detection Probability vs. Jammer-to-Signal-Ratio: In Fig. 8, the effect of varying Eve's signal power relative to Alice's is analyzed by plotting the PD of both artificial and real targets as a function of the JSR across three CFO regions. The noise floor remains constant, ensuring that at 0 dB JSR, the jammer-to-noise ratio and SNR are both 30 dB. The PD values are derived from 10k realizations for each JSR and CFO combination, with the CFO randomly chosen within the defined regions. The time alignment between Alice's and Eve's signals also varies randomly between -24 and +24 samples, ensuring that CFO is the only source of orthogonality loss. At low JSR values, the jamming does not work since Bob synchronizes to Alice's signal. This leads to a loss of orthogonality in Eve's signal, which the CFO influences. As a result, artificial target peaks in the RDM either i) stretch into ridges, reducing PD for high CFO values or ii) remain detectable for lower CFO values. During this phase, the PD of real targets is high as expected. As JSR increases, there is a transition in PD between real and artificial targets. When JSR exceeds 10 dB, the PD of artificial targets becomes high enough to ensure effective jamming. Meanwhile, real targets are increasingly missed due to the CFO. *This region highlights strong target spoofing and deceptive jamming performances–indicated by the high PD of artificial targets and low PD of real targets, respectively.*

5) Missed Detection Rate vs. Detection Rate: Fig. 9 further shows the effectiveness of the jammer by plotting the miss detection rate of real targets (MDRrt, obtained from the corresponding PD) and the detection rate of artificial targets (DRat) as a function of JSR. Based on the plot, three JSR regions can be identified: low (below 0 dB), medium (between 0 and 10 dB), and high (above 10 dB). When JSR is low, the MDRrt is also very low. Meanwhile, for relatively lower CFO

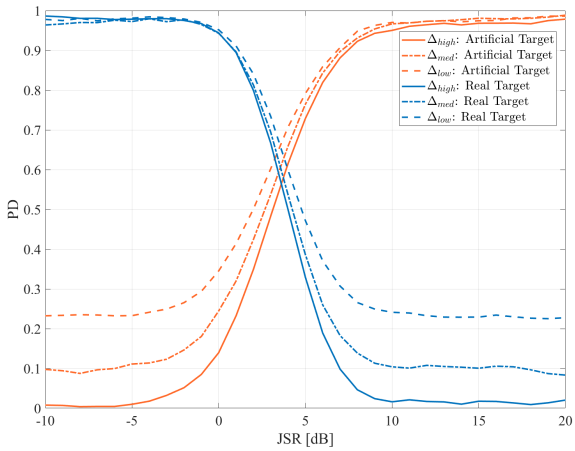

Fig. 8: The PD of artificial and real targets are shown as a function of JSR for three different CFO regions. The CFO difference between Eve and Alice is given as $\Delta = |\eta - \bar{\eta}|$ and the corresponding regions are defined as $\Delta_{high} > 4$ ppm, 4 ppm $\geq \Delta_{med} > 1$ ppm, and 1 ppm $\geq \Delta_{low}$. Above 8-10 dB JSR, the jamming works since Bob synchronizes to Eve, and Alice's signal turns into noise. Below this threshold, jamming does not work.

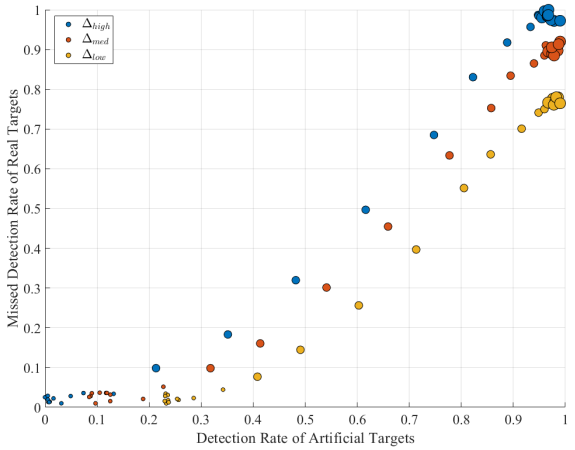

Fig. 9: The MDRrt and DRat are plotted for three different CFO regions. Based on Fig. 8, three JSR regions can be identified: low (below 0 dB), medium (between 0 and 10 dB), and high (above 10 dB). The size of the scatter plots are linked with these regions, e.g., high JSR points have the largest scatter points. The CFO difference between Eve and Alice is given as $\Delta = |\eta - \bar{\eta}|$, and the regions defined for Fig. 8 apply here.

differences, the DRat reaches roughly 20%. The medium JSR levels serve as a transition region where minimal differences in JSR significantly increase the MDRrt and DRat. As the system reaches high JSR levels, MDRrt and DRat reach their maximal values. Similar to the low JSR region, the real targets may be detected in some realizations when the CFO difference is low. *Hence, Eve should operate above 10-12 dB JSR and with a high CFO difference for the best jamming performance.*

6) Overcrowding Detection Performance: Fig. 10 illustrates the number of detected targets as a function of the total number of targets in the environment, across three different false alarm rates (PFa) For each PFa and number of real targets, 10k realizations were simulated. In these simulations, Eve transmits an RDM with two peaks: one representing the artificial target and the other as a reference, accounting only for first-order reflections between these peaks and the

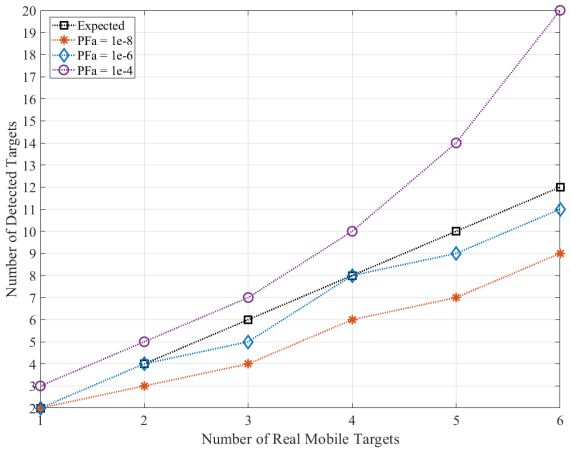

Fig. 10: The impact of the number of real scatterers in the environment is studied as a function of Bob's PFa. The JSR is fixed to 10 dB, and the SNR is 30 dB.

targets. The expected number of detected targets is calculated using the analytical expression in (13). When PFa is 10^{-4}, the detection algorithm is more permissive, leading Bob to detect more peaks than expected, i.e., some noise peaks are mistakenly identified as targets. At PFa $= 10^{-6}$, the detection accuracy aligns closely with the expected values, though slight deviations still occur. Finally, at PFa $= 10^{-8}$, the detection algorithm becomes overly strict, causing Bob to miss many real targets, which decreases the reliability of the sensing system. *In essence, the overcrowding strategy works.* However, assuming that Eve does not have access to PFa used by Bob, the outcome is not entirely under the control of Eve.

VI. Experimental Validation

In this section, we explore the design and implementation of an SDR-based jammer by utilizing the USRP X310 platform.

A. Experimental Setup

Our experimental setup is indoors and it is similar to the topology provided in Fig. 1, as shown in Fig. 11. A metallic fan emulates a mobile target due to the consistent speed pattern obtained from its rotating blades, which helps diagnose RDMs. In our models, we simplified the sensing frame structure by transmitting a single OFDM symbol used both for synchronization and channel estimation purposes. However, as described in Section II-B2, NDPA/NDP frames consist of multiple fields, such as L-STF and L-LTF for synchronization, and VHT-LTF for channel estimation [1]. In a real WLAN sensing setting, Eve must mimic L-STF and L-LTF to ensure that Bob synchronizes with Eve. However, we omit these fields in our experiments since i) they are straightforward to implement; and ii) they are unnecessary for our purposes, as VHT-LTF is the primary field for sensing processing.

The transmitted signals follow the structure shown in Fig. 12. Alice continuously transmits legitimate sensing signals, separated by $T_s = 1.32$ ms. Simultaneously, Eve transmits clusters of modulated OFDM symbols, with each cluster containing three identical symbols for the time instant m. This

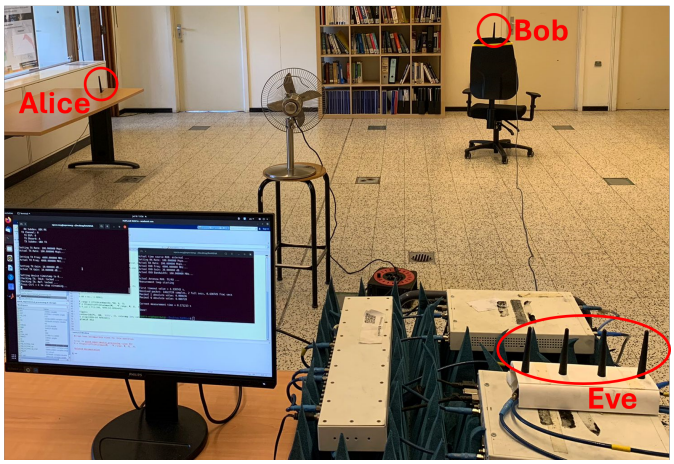

Fig. 11: The picture of the experimental setup, consisting of a metallic fan as the mobile target and three USRP X310s: one to emulate Alice and Bob, and the remaining two to emulate Eve's array. For Eve's single antenna transmission: i) only the antenna at the far left is kept, and ii) the remaining antennas are removed to avoid coupling effects. For Eve's multiple antenna transmission: i) the AoA estimation stage is bypassed, instead, the angles are computed manually, and ii) the precoder matrix is designed to steer a null towards the target and a beam towards Bob

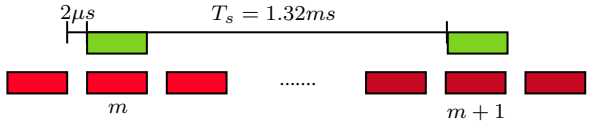

Fig. 12: Signal structure for jamming. Alice transmits the same OFDM symbol with PRI $T_s = 1.32ms$, indicated with green. Meanwhile, Eve transmits in batches, each consisting of three identical OFDM symbols for time instant m, indicated with red.

clustered transmission serves two purposes: (i) ensuring coverage for each time alignment case in (17), and (ii) increasing the probability of at least one jamming signal aligning with Alice's legitimate signal. The jamming signal clusters are also separated by $T_s = 1.32$ ms, using the middle symbol of each cluster as a reference.

B. Results and Discussion

We show the experimental surveillance channels between Alice and Bob and Eve and Bob. Then we show the impact of the different combined strategies (A1-B1, A1-B2, A2-B1, and A2-B2), to relate to the simulation results in Section V.

1) Surveillance Channel: We present the RDMs for both the Alice-Bob and Eve-Bob channels, as shown in Fig. 13. In real-world wireless channels, static environmental features like walls and furniture generate multipath components (MPCs), appearing as clutter peaks around zero-Doppler in both RDMs. Four distinct peaks appear at approximately 3 and 6 meters in the bistatic ranges for the Alice-Bob and Eve-Bob channels, respectively. These peaks result from Doppler shifts caused by the fan's blades. Additionally, ghost targets appear at farther ranges due to multipath effects. The clutter and fan blade peaks differ in each RDM due to the distinct bistatic geometries.

2) Combined Strategies: We present four RDMs in Fig. 14, each reflecting different combined jamming strategies. These RDMs include an artificial target at a 10-meter range and a speed of 5 m/s, marked with a red cross. The top-left RDM shows the first strategy, where the fan's signatures appear as peaks $\langle 1 \rangle$, similar to those in Fig. 13. The target peaks $\langle 2 \rangle$ result from the interaction between the fan's signatures and the artificial target peak $\langle \times \rangle$. Additionally, Eve's transmission of range/Doppler shifted signals for the artificial target creates a range/Doppler shifted clutter $\langle 3 \rangle$, scaled by $\bar{\alpha}$, enhancing the realism of the deception. The top-right RDM displays the effect of forced synchronization, where target peaks and clutter are replaced by ridges $\langle 4 \rangle$ that shift along the speed dimension due to CFO, potentially folding over multiple times. The bottom-left RDM shows the most effective strategy, where Eve utilizes the directivity of a linear array. However, despite this, the mobile target's signatures $\langle 5 \rangle$ remain due to calibration errors and array sidelobes. The clutter pattern also differs from the top two RDMs because the scene is not isotropically illuminated. The bottom-right RDM, representing the last strategy, is characterized by ridges caused by the CFO.

3) Comparison of Numerical and Experimental Results: We begin by discussing the similarities between the numerical analyses (Section V) and experimental validation (Section VI). In all cases, the artificial target is successfully introduced to Bob. The effects of different combined strategies align well with the numerical analysis. The simplest combination, A1+B1, shows numerous target peaks. Both A1+B2 and A2+B2 produce similar RDMs, dominated by ridges. The third strategy, A2+B1, generates the cleanest RDM, showing mainly the artificial target.

However, significant differences emerge between numerical and experimental results due to real-world environments and hardware limitations. First, static objects introduce clutter centered at zero-Doppler, along with ghost targets of moving entities. Since the clutter patterns differ between Alice-Bob and Eve-Bob, Bob may detect these discrepancies and react accordingly. Second, Eve's range/Doppler-shifted signals for the artificial target cause clutter peaks to shift according to the artificial target's parameters. Third, the experimental noise floor is higher than in simulations, which consider only thermal noise. Fourth, if the number of ridges–determined by mobile target peaks in the Alice-Bob channel–is high, the artificial target is more likely to be hidden by them. Lastly, when Eve uses A2 to form a beam towards Bob and null towards the target, calibration errors create imperfections in the radiation pattern, making mobile target peaks slightly visible.

VII. Conclusion

This paper examines the design and application of target-spoofing deceptive jammers in WLAN sensing, highlighting vulnerabilities in communication-centric OFDM-based JCAS systems that rely on RDM processing. Through qualitative and quantitative analysis, we demonstrate how techniques like overcrowding, selective target injection, and forced synchronization disrupt target detection. Experiments confirm that low-cost SDR platforms can effectively carry out these jamming techniques without sophisticated hardware.

We identify key vulnerabilities in RDM-based WLAN sensing: i) standardized OFDM symbols, ii) joint time and frequency synchronization, and iii) unprotected over-the-air negotiation. These are exploitable when i) JSR is above 8-12

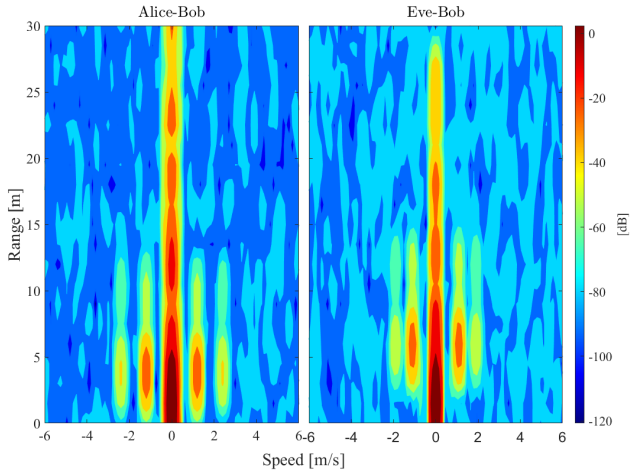

Fig. 13: The RDMs obtained for Alice-Bob and Eve-Bob channels while the mobile target is active. Black stars mark the peaks in Alice-Bob RDM for comparison. The environment appears as a set of static targets centered at 0m/s, and the fan's blades appear as four distinct peaks.

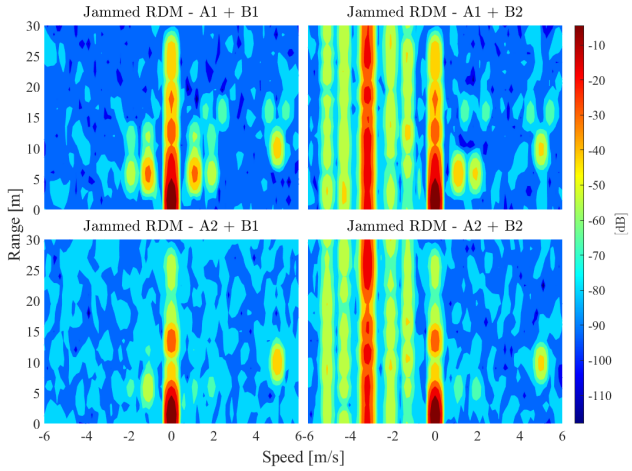

Fig. 14: The jammed RDMs with combined strategies, with $\eta_w = 5$ppm. The black stars correspond to the range/Doppler cells of the true target, while the red cross corresponds to the (10m,5m/s) cell for the artificial target. The ridges are caused by the loss of orthogonality on Alice's signals.

dB, and ii) the CFO difference Δ is at least 3 ppm (or 6 ppm with wider subcarrier spacing). Under these conditions, target spoofing and deceptive jamming are highly effective. These results underscore the need to address such weaknesses in future WLAN sensing and JCAS systems as they enter critical applications.

In summary, this study reveals substantial risks posed by target-spoofing and deceptive jamming, encouraging future work on securing physical-layer waveforms, enhancing synchronization, and developing adaptive methods to mitigate these vulnerabilities in OFDM-based JCAS systems.

Appendix A
Joint Time and Frequency Synchronization

Bob exploits a dominant LOS for JTFS, meaning $\alpha_0 \gg \alpha_p, \forall p$ and $\tau_0 < \tau_p, \forall p$. The received LOS signal sampled at time $t = nT + mT_s$ (where n and m denote the fast and slow time indices, respectively) is expressed as [36], [37]

$$r[n,m] = \alpha_0 s[n - n_0, m] e^{j2\pi\eta(nT+mT_s)}$$

where the noise is omitted, η represents the CFO between Alice and Bob, and $s[n,m]$ is the transmitted signal. For coarse synchronization, Bob computes the lag-1 auto-correlation over a sliding window of the received samples, expressed as

$$\Xi[k] = \sum_{n=-Q_{cp}}^{Q} r[n+k,m] r^*[n+k,m+1].$$

Substituting the received signal into the equation yields the strongest peak at $k = n_0$ corresponding to the arrival time of the LOS path since $\alpha_0 \gg \alpha_p, \forall p$. Assuming that the transmitted signal is normalized to $\sum_{n=-Q_{cp}}^{Q} s[n,m] = 1$, the complex amplitude of this peak is defined as

$$\Xi[n_0] = |\alpha_0|^2 e^{-j2\pi\eta T_s}.$$

Here, the phase of $\Xi[n_0]$ is directly linked to the CFO between Alice and Bob. Hence, Bob can synchronize to the timing of the LOS based on the peak at $k = n_0$, and estimate and compensate the CFO using the phase of the peak $\hat{\eta} = \angle\Xi[n_0]/2\pi T_s$. This process ensures that Bob is correctly synchronized in both time and frequency domains.

Appendix B
Round-trip-time for distance estimation

The devices in the legitimate WLAN sensing network, Alice and Bob, estimate $\tau_{ab} = d_{ab}/c$ for themselves where c is the speed of light. The process is visualized in Fig. 15 and summarized as follows [49]. I) Alice transmits and starts its reference clock. II) Bob receives the signal and starts its reference clock. III) Bob waits for the standardized duration of τ_x, then transmits. IV) Alice receives the signal after $2\tau_{ab} + \tau_x$ seconds, then estimates τ_{ab}. V) Alice waits τ_x seconds, then transmits. VI) Bob receives the signal after $3\tau_{ab} + 2\tau_x$ seconds, and estimates τ_{ab}. VII) Both devices now have τ_{ab}.

Meanwhile, Eve can estimate $\tau_{be} = d_{be}/c$, $\tau_{ae} = d_{ae}/c$ and $\tau_{ab} = d_{ab}/c$ as follows [50]. I) Alice transmits. II) Eve receives the signal and knows that Alice has transmitted it. Eve does not start its reference clock yet and waits for the next transmission. III) Bob waits τ_x seconds, then transmits. IV) Eve receives Bob's signal and starts its reference clock since it knows that $\tau_{ab} + \tau_x + \tau_{be}$ seconds have passed. V) Eve listens for the next transmissions and keeps measurement times as C_1 to C_4. Once all the reception times are collected, the propagation delays are calculated as

$\tau_{abx} = (C_3 - C_1)/2, \tau_{be} = (3C_1 - C_3)/2, \tau_{ae} = C_2 – C_3 + C_1$

where $\tau_{abx} = \tau_{ab} + \tau_x$.

References

[1] R. Du *et al.*, "An overview on IEEE 802.11 bf: WLAN sensing," *arXiv preprint arXiv:2207.04859*, 2021.

[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] 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.

[4] Z. Zhang *et al.*, "Preamble injection and spoofing attacks in Wi-Fi networks," in *2021 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2021, pp. 1–6.

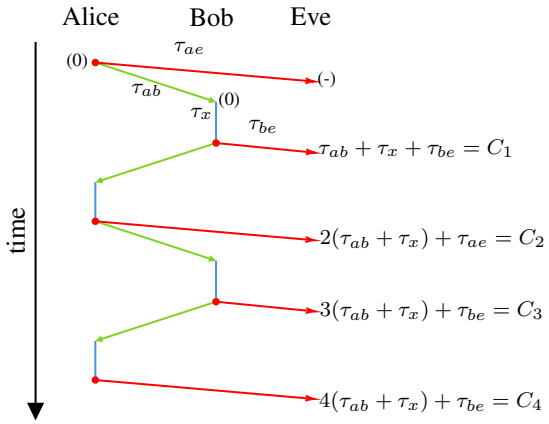

Fig. 15: RTT-based distance estimation procedure. The green and red arrows correspond to the propagation delays over the related distances. Blue lines correspond to the standardized idle time τ_x.

[5] M. J. La Pan *et al.*, "Phase warping and differential scrambling attacks against ofdm frequency synchronization," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013, pp. 2886–2890.

[6] M. J. L. Pan *et al.*, "Jamming attacks against ofdm timing synchronization and signal acquisition," in *MILCOM 2012 - 2012 IEEE Military Communications Conference*, 2012, pp. 1–7.

[7] T. C. Clancy, "Efficient ofdm denial: Pilot jamming and pilot nulling," in *2011 IEEE International Conference on Communications (ICC)*, 2011, pp. 1–5.

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

[9] S. Zhao *et al.*, "Orthogonality-sabotaging attacks against ofdma-based wireless networks," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019, pp. 1603–1611.

[10] J. R. v. d. Merwe *et al.*, "Classification of spoofing attack types," in *2018 European Navigation Conference (ENC)*. IEEE, 2018, pp. 91–99.

[11] C. Matte *et al.*, "Device-to-identity linking attack using targeted Wi-Fi geolocation spoofing," *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pp. 1–6, 2015.

[12] N. O. Tippenhauer *et al.*, "Attacks on public WLAN-based positioning systems," *Proceedings of the 7th international conference on Mobile systems, applications, and services*, pp. 29–40, 2009.

[13] D. Liu *et al.*, "Identification of location spoofing in wireless sensor networks in non-line-of-sight conditions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2375–2384, 2017.

[14] H. Pirayesh *et al.*, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE communications surveys & tutorials*, vol. 24, no. 2, pp. 767–809, 2022.

[15] C. Günther, "A survey of spoofing and counter-measures," *NAVIGATION: Journal of the Institute of Navigation*, vol. 61, no. 3, pp. 159–177, 2014.

[16] R. Melki *et al.*, "A survey on OFDM physical layer security," *Physical Communication*, vol. 32, pp. 1–30, 2019.

[17] J. Schuerger *et al.*, "Deception jamming modeling in radar sensor networks," *IEEE Military Communications Conference*, pp. 1–7, 2008.

[18] ——, "Performance of random OFDM radar signals in deception jamming scenarios," *IEEE Radar Conference*, pp. 1–6, 2009.

[19] M. Tan *et al.*, "A novel deceptive jamming approach against frequency diverse array radar," *IEEE Sensors Journal*, vol. 21, no. 6, pp. 8323–8332, 2021.

[20] Q. Sun *et al.*, "Efficient deceptive jamming method of static and moving targets against sar," *IEEE Sensors Journal*, vol. 18, no. 9, pp. 3610–3618, 2018.

[21] P. Ji *et al.*, "A smart multitransmitter cooperative false images generation method against multichannel sar-gmti," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 62, pp. 1–17, 2024.

[22] K. Yang *et al.*, "Fast generation of deceptive jamming signal against spaceborne sar based on spatial frequency domain interpolation," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 60, pp. 1–15, 2022.

[23] S. Roome, "Digital radio frequency memory," *Electronics & communication engineering journal*, 1990.

[24] Y. Liang *et al.*, "Secure OFDM system design and capacity analysis under disguised jamming," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 738–752, 2020.

[25] X. Fang *et al.*, "Diverse frequency time modulation for passive false target spoofing: Design and experiment," *IEEE Transactions on Microwave Theory and Techniques*, vol. 72, no. 3, pp. 1932–1942, 2024.

[26] M. Srinivasan *et al.*, "AoA-based physical layer authentication in analog arrays under impersonation attacks," *arXiv preprint arXiv:2407.08282*, 2024.

[27] M. Varotto *et al.*, "Detecting 5G signal jammers using spectrograms with supervised and unsupervised learning," *arXiv preprint arXiv:2405.10331*, 2024.

[28] ——, "Detecting 5G signal jammers with autoencoders based on loose observations," in *2023 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2023, pp. 160–165.

[29] ——, "Detecting 5G narrowband jammers with CNN, k-nearest neighbors, and support vector machines," *arXiv preprint arXiv:2405.09564*, 2024.

[30] J. Li *et al.*, "Channel state information-free location-privacy enhancement: Delay-angle information spoofing," in *ICC 2024 - IEEE International Conference on Communications*, 2024, pp. 3767–3772.

[31] ——, "Channel state information-free location-privacy enhancement: Fake path injection," *IEEE Transactions on Signal Processing*, vol. 72, pp. 3745–3760, 2024.

[32] A. Argyriou, "Range-doppler spoofing in OFDM signals for preventing wireless passive emitter tracking," in *2023 IEEE Radar Conference (RadarConf23)*. IEEE, 2023, pp. 1–6.

[33] H. C. Yildirim *et al.*, "Deceptive jamming in WLAN sensing," *2024 IEEE Radar Conference (RadarConf24)*, 2024.

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

[35] O. Bejarano *et al.*, "IEEE 802.11 ac: from channelization to multi-user MIMO," *IEEE Communications Magazine*, 2013.

[36] J.-J. van de Beek *et al.*, "A time and frequency synchronization scheme for multiuser OFDM," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 11, pp. 1900–1914, 1999.

[37] T. Schmidl *et al.*, "Robust frequency and timing synchronization for ofdm," *IEEE Transactions on Communications*, vol. 45, no. 12, pp. 1613–1621, 1997.

[38] F. Horlin *et al.*, *Digital compensation for analog front-ends: a new approach to wireless transceiver design*. John Wiley & Sons, 2008.

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

[40] Z. Wei *et al.*, "Integrated sensing and communication channel modeling: A survey," *IEEE Internet of Things Journal*, pp. 1–1, 2024.

[41] M. A. Richards *et al.*, *Principles of Modern Radar: Basic principles*. The Institution of Engineering and Technology, 2010.

[42] T.-D. Chiueh *et al.*, *Baseband receiver design for wireless MIMO-OFDM communications*. John Wiley & Sons, 2012.

[43] A. Mahmood *et al.*, "Clock synchronization over IEEE 802.11—a survey of methodologies and protocols," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 907–922, 2016.

[44] H. C. Yildirim *et al.*, "Impact of interference on OFDM based radars," *IEEE Vehicular Technology Conference*, 2020.

[45] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Transactions on Antennas and Propagation*, vol. 34, no. 3, pp. 276–280, 1986.

[46] R. Roy *et al.*, "ESPRIT-estimation of signal parameters via rotational invariance techniques," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 37, no. 7, pp. 984–995, 1989.

[47] R. Boulic *et al.*, "A global human walking model with real-time kinematic personification," *The visual computer*, 1990.

[48] S. Blake, "OS-CFAR theory for multiple targets and nonuniform clutter," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 24, no. 6, pp. 785–790, 1988.

[49] D. Mirkovic *et al.*, "A survey of round trip time prediction systems," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1758–1776, 2018.

[50] H. Jiang *et al.*, "Passive estimation of TCP round-trip times," *ACM SIGCOMM Computer Communication Review*, vol. 32, no. 3, pp. 75–88, 2002.