Practical Blind Full-Frame Replay Attacks on OFDM-Based ISAC Systems

Stefania Bartoletti, Giulia Focarelli, Ivan Palamà, Samuele Zanini, Nicola Blefari Melazzi, Giuseppe Bianchi

***Abstract*—Integrated Sensing and Communication (ISAC) systems promise unprecedented capabilities by merging connectivity and situational awareness, but also expose new attack surfaces at the physical layer. In this work, we demonstrate a blind full-frame OFDM replay attack that manipulates sensing outputs by injecting false targets and concealing real ones, without disrupting communication. The blind nature of our attack lies in the fact that it requires neither synchronization nor any knowledge of the signal structure, reference signals, or sensing parameters, making it not only practically viable, but even (somewhat) straightforward to execute. By replaying entire OFDM frames with a controlled delay and a frequency shift, the attacker can distort range estimations and induce Doppler shifts, mimicking the presence of moving targets. We present a general analytical framework to characterize the attack's impact on range-Doppler processing and validate it through both system-level simulations with 5G NR parameters and real-world experiments. Experimental results build directly on a working 5G testbed with software-defined radios and commercial off-the-shelf hardware, which we extend with sensing capabilities, thereby demonstrating the attack's feasibility and impact in a realistic ISAC scenario.**

***Index Terms*—Integrated sensing and communication, security, threat models, replay attack, integrity.**

I. Introduction

Cellular networks are progressively incorporating localization and sensing as native capabilities, laying the foundation for integrated sensing and communication (ISAC). These developments include the introduction of dedicated reference signals, new network functions, and architectural support for joint communication and sensing [1]–[6]. This integration leverages capabilities like multi-antenna systems and operation in high-frequency bands, enabling precise target localization and environmental awareness [7]–[10].

Most applications enabled by ISAC, such as autonomous driving and industrial automation, depend on accurate and tamper-resistant sensing for reliable decision-making [11]–[13]. Although protocol-level mechanisms such as authentication and encryption can be extended to ISAC [14]–[16], they might not fully address emerging physical-layer threats. Indeed, armed with increasingly powerful software-defined radios (SDRs), attackers can now intercept, manipulate, and replay wireless signals over the air, gaining the ability to compromise both the integrity of sensing data and the reliability of communication. In 5G-based localization, for instance, overshadowing and selective spoofing attacks have shown how adversaries can tamper with position estimates [17]–[19], highlighting the urgent need for robust integrity mechanisms [20].

Among physical-layer threats, replay attacks stand out as a prominent example, where a malicious actor intercepts and retransmits legitimate signals to deceive the receiver or bypass security mechanisms. They are a well-established threat in systems such as global navigation satellite system (GNSS) or monostatic radar,[1] where signals are often predictable and unencrypted, and where the sole function is localization and sensing, with no concern for data integrity or communication continuity. In these contexts, replay can be used to manipulate position estimates, disrupt target tracking, or inject false targets [21].

In ISAC systems, however, the presence of a communication component fundamentally alters the threat landscape. Since the same waveform carries both sensing and data traffic, any over-the-air modification risks disrupting the communication link. As a result, replay attacks in ISAC are often considered either inherently impractical or feasible only by highly capable adversaries. As discussed in [22], [23], to avoid impairing communication, an attacker would seemingly need to demodulate the signal, apply minimally invasive modifications, re-encode it, and ensure precise timing, all of which demand advanced signal processing capabilities.

The goal of this work is to challenge the above belief and demonstrate, through both system-level simulations and real-world experiments, that *blind full-frame replay attacks* can be both feasible and effective against ISAC systems. Here, *blind* refers to the scenario illustrated in Fig. 1, where an attacker does not parse or decode the frame, but simply (and *continuously*) retransmits a filtered and delayed version of the received OFDM signal, without any knowledge of the signal structure, reference signals, or sensing parameters, and without requiring synchronization with the transmitter. Crucially, we show that such attacks can be implemented in practice using off-the-shelf hardware, and are capable of injecting false targets and induce Doppler shifts, all while preserving communication performance within tolerable limits. This reveals a fundamental concern in ISAC: attackers do not need sophisticated signal manipulation to pose a serious threat: even naïve replay strategies can stealthily compromise sensing integrity. Summarizing, the key contributions of this work are:

S. Bartoletti, G. Focarelli, S. Zanini, N. Blefari Melazzi, and G. Bianchi are with CNIT and University of Rome Tor Vergata, Italy. I. Palamà is with CNIT. S. Zanini is also with IMT School for Advanced Studies, Lucca, Italy.

This work was partially supported by the European Research Council (ERC) under the European Union's Horizon Europe (Grant agreement No. 101078411), and by the projects SERICS (PE00000014) and RESTART (PE00000001) under the Italian National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.3.

[1]Monostatic radar uses co-located transmitter and receiver; bistatic radar uses spatially separated ones. We refer to these respectively as monostatic or bistatic configurations throughout the paper.

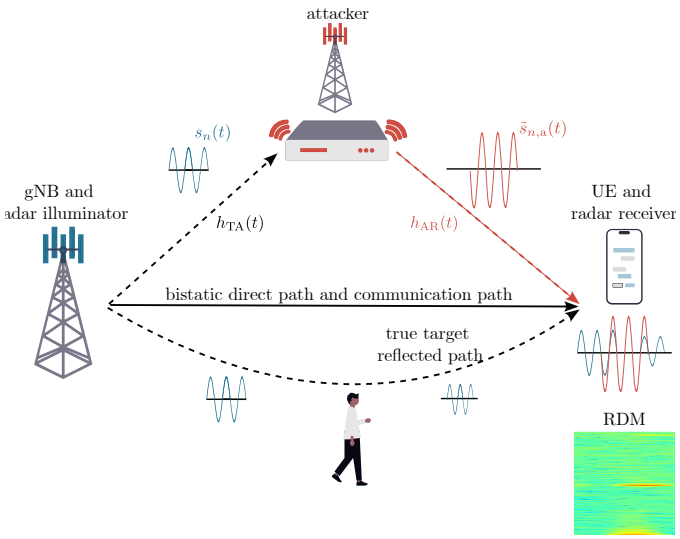


Fig. 1: Illustration of the considered replay attack in a bistatic ISAC system. The gNB transmits the signal $s_n(t)$, which is captured by the attacker through the channel $h_{\mathrm{TA}}(t)$ and replayed toward the victim UE via $h_{\mathrm{AR}}(t)$, generating forged or interfering echoes in the resulting range-Doppler map.

- We expose a previously overlooked threat model based on blind full-frame OFDM replay, which requires no frame parsing, synchronization, or signal knowledge. This simple (and highly practical) strategy has been largely dismissed in recent ISAC literature, likely due to the implicit assumption that such a naïve replay would inherently disrupt communication. Our findings challenge this notion.
- We provide a detailed, simulation-based assessment of the attack's impact on sensing performance, showing that depending on how the replay is configured, it can manipulate the apparent position of a real target, obscure it entirely, or inject false targets, achieving both deception and concealment effects.
- We experimentally demonstrate the practical viability of the attack using commodity SDR hardware and a real 5G gNB–UE system in a bistatic configuration, showing that blind replay can tamper with the sensing output in the range-Doppler domain, including false target injection and genuine target distortion.
- We assess the attack's effect on the communication layer, showing that despite its impact on sensing, the replay can preserve acceptable communication performance, enabling stealthy operation even with commercial off-the-shelf (COTS) 5G devices. Importantly, we experimentally demonstrate that the attacker can gradually increase power to induce controlled performance degradation, mimicking natural channel dynamics and thus reducing detectability via communication metrics.

Finally, while this work focuses on replay threats to ISAC systems, the same principles can also support privacy protection and defensive strategies. Controlled signal manipulation and false target injection may enable anti-surveillance, obfuscation, and deception-based defenses, motivating research into privacy-preserving ISAC architectures.

The remainder of the paper is organized as follows. Section II reviews related work. Section III introduces the baseline system model, and Section IV describes the attack scenario. Section V details threat models and attacker strategies. Sections VI and VII present simulation and experimental results, respectively. Section VIII discusses potential countermeasures and concludes the paper.

II. Related Works

Classical localization and radar systems are vulnerable to a wide range of attacks at both the physical and logical layers. For instance, GNSS systems are well known to be susceptible to spoofing and jamming due to the public nature of their reference signal codes [24]–[27]. In such attacks, adversaries can disrupt the legitimate links between users and satellites, impersonating them to corrupt localization information [17]–[19], [28]–[31]. Similar threats also affect radar systems, including those leveraging communication waveforms, where attackers can jam the radar signal or inject false targets at the receiver side [32]–[34].

In the context of ISAC, security and privacy issues have recently attracted significant attention. A broader overview of open research challenges is provided in [35]–[37], with particular emphasis on vulnerabilities at the physical layer, which are rapidly evolving. Along this line, replay-based threat models for ISAC have been proposed in [22], [23]. In [22], the attacker is assumed to synchronize with the legitimate transmitter in order to replay the signal with controlled delays and Doppler shifts, enabling the injection of crafted sensing echoes. In [23], the authors demonstrate that SDRs can act as effective deceptive jammers in WLAN-based ISAC systems, assuming that the attacker can sniff the sensing parameters exchanged between the transmitter and the receiver acting as a bistatic radar.

While effective, such attacks typically rely on strong adversarial capabilities and may disrupt communication in addition to localization or sensing. This highlights how the integration of sensing and communication can, in some cases, offer inherent advantages in detecting and mitigating certain error sources [9]. Beyond replay attacks, adversarial effects in distributed ISAC networks have also been investigated in [38], where a theoretical framework quantifies the impact of spoofing on cooperative localization accuracy.

Against this background, this paper considers a fundamentally different and more constrained adversarial model. We study an OFDM-based ISAC system in which radio resources are jointly allocated for sensing and data transmission. The adversary is external to the network and has no knowledge of the system structure or sensing parameters, nor the capability to sniff their exchange. Its only available action is to blindly manipulate and delay the over-the-air signal. Moreover, to remain stealthy, the attack must leave the communication performance unaffected.

Despite these stringent constraints, we demonstrate that a blind adversary can still successfully deceive the sensing functionality. By performing full-frame manipulation and

replay of the OFDM signal, the attacker can inject false targets or conceal real ones, while communication remains uninterrupted.

Unlike the replay strategy in [22], which assumes that the attacker can synchronize with the transmitter to craft echoes with specific delays and Doppler shifts, the adversary considered here performs no synchronization at all. It simply records the received signal as a continuous stream of IQ samples and retransmits it after a chosen delay. The legitimate receiver then synchronizes to the replayed waveform exactly as it would for a genuine echo, since the replayed signal naturally preserves the structure required by the receiver's own synchronization algorithms.

Full-frame replay has previously been studied in [39] only in the context of active UE localization, with the limited objective of biasing time-of-arrival estimates in downlink transmissions. ISAC sensing, however, differs fundamentally from active localization. Radar-like ISAC systems must detect and interpret weak reflections embedded within communication signals, which opens a much richer attack surface: adversaries can not only bias estimates but also mimic or obscure physical targets, directly altering the sensing outcome. These differences necessitate a distinct threat model and analytical treatment, motivating the dedicated investigation presented in this work.

To the best of our knowledge, no prior work has jointly analyzed sensing and communication performance under blind replay attacks in ISAC systems. Existing threat models typically assume that the attacker has knowledge of the signal structure or can emulate legitimate transmissions. In contrast, our adversary is fully blind and limited to delaying and retransmitting received signals while remaining stealthy on the communication side. We show that even under these conditions, sensing performance can be severely degraded.

Finally, while [40] provides a preliminary feasibility study showing that full-frame replay can perturb sensing outputs in an NR-compliant system, the present manuscript goes significantly further. We develop a general and systematic attack framework for ISAC sensing by (i) introducing an analytical model that characterizes how replay-induced delay and frequency shifts affect range–Doppler processing, (ii) considering a broader set of ISAC scenarios and stealthier adversarial strategies, and (iii) jointly evaluating sensing and communication performance.

III. System Model without Attack

We consider an ISAC system in a monostatic or bistatic configuration. In particular, the system is composed of a multi-antenna transmitter with a transmitting antenna of N_{T} elements and a multi-antenna receiver with a receiving antenna of N_{R} elements; alternatively, the transmitter and receiver can be co-located in a monostatic configuration (e.g., a single gNodeB (gNB) or user equipment (UE) acting as monostatic radar while communicating). The transmitter and receiver can be in different locations according to a bistatic configuration (e.g., a gNB or UE acting as bistatic radar while communicating with the receiving gNB or UE).[2] The signal transmitted by the n-th antenna element, denoted by $s_n(t)$ with $n \in \{1, \ldots, N_{\mathrm{T}}\}$, is composed of M orthogonal frequency division multiplexing (OFDM) symbols and K active subcarriers

$$s_n(t) = \sum_{m=0}^{M-1} \sum_{k=0}^{K-1} x_{n,k}^{(m)} e^{j2\pi \frac{k}{T} t} g(t - mT_{\mathrm{s}}) \tag{1}$$

where $x_{n,k}^{(m)}$ is the complex modulation symbol transmitted by antenna n on subcarrier k during OFDM symbol m. The OFDM symbol duration is defined as the sum of the useful symbol duration and the Cyclic Prefix (CP), i.e., $T_{\mathrm{s}} = T + T_{\mathrm{cp}}$. The function $g(\cdot)$ denotes the transmit window or pulse shape applied to each OFDM symbol (e.g., a rectangular window of duration T_{s}). The transmitted symbol at each antenna after beamforming is given by

$$\mathbf{x}_k^{(m)} = \mathbf{w}_{\mathrm{T}} x_k^{(m)} \tag{2}$$

where $\mathbf{w}_{\mathrm{T}} \in \mathbb{C}^{N_{\mathrm{t}} \times 1}$ is the beamforming or precoder vector.

The signal is received after propagation in the operating environment and backscattering from surrounding target objects. The OFDM receiver performs time synchronization by looking at the correlation between the transmitted and received signal and then proceeds with an FFT block, according to the classical OFDM radar receiver [5], [44], [45]. The received modulation symbols at each antenna after time synchronization and the FFT block in the OFDM receiver are

$$\mathbf{y}_k^{(m)} = \mathbf{H}_k^{(m)} \mathbf{x}_k^{(m)} + \boldsymbol{\nu}_k^{(m)} + \mathbf{n}_k \tag{3}$$

where $\mathbf{H}_k^{(m)} \in \mathbb{C}^{N_{\mathrm{r}} \times N_{\mathrm{t}}}$ is the channel matrix of the mth symbol and the kth subcarrier, $\boldsymbol{\nu}_k^{(m)} \in \mathbb{C}^{N_{\mathrm{r}} \times N_{\mathrm{t}}}$ is the self-interference term, which is present only in the monostatic configuration, and $\mathbf{n}_k \in \mathbb{C}^{N_{\mathrm{r}} \times 1}$ is the additive white Gaussian noise (AWGN) with variance σ_{n}^2.[3] If we consider L point target reflections, the channel matrix can be written as

$$\mathbf{H}_k^{(m)} = \sum_{l=1}^{L} \beta_{l,m,k}\, \mathbf{a}_{\mathrm{r}}(\theta_{\mathrm{r},l})\, \mathbf{a}_{\mathrm{t}}^{\mathsf{T}}(\theta_{\mathrm{t},l}) \tag{4}$$

where $\mathbf{a}_{\mathrm{t}}(\theta_{\mathrm{t},l})$ and $\mathbf{a}_{\mathrm{r}}(\theta_{\mathrm{r},l})$ denote the transmit and receive steering vectors for the l-th target, and $\theta_{\mathrm{t},l}$, $\theta_{\mathrm{r},l}$ are the corresponding angles of departure and arrival. The complex reflection coefficient β_l is defined as

$$\beta_{l,m,k} = \alpha_l e^{j2\pi m T_{\mathrm{s}} f_{\mathrm{D},l}} e^{-j2\pi \frac{k}{T} \tau_l} \tag{5}$$

where τ_l, $f_{\mathrm{D},l}$, are the delay and Doppler shift of the l-th target, respectively, and $\alpha_l = |\alpha_l| e^{j\phi_l}$ the complex amplitude.

These parameters vary based on the target's position and speed and differ between the monostatic and bistatic cases. The term $\alpha_l = |\alpha_l| e^{j\phi_l}$ is the complex amplitude, which includes phase shift and attenuation along the lth propagation path.

[2] In this work, we focus on single radars in bistatic or monostatic configuration. Models for multistatic and cooperative cases can be found in [41]–[43]. At the end, we will discuss how spatial diversity can help mitigate such attacks.

[3] We will no longer consider the effect of the self-interference term, as it falls outside the scope of this paper. However, readers may refer to [44] for further details on this topic.

In line-of-sight (LOS) propagation conditions, the power received at a given array element from the lth path $P_{\mathrm{R},l}$, illuminated by the sensing beam, is proportional to $|\alpha_l|^2$ and is defined as

$$P_{\mathrm{R},l} = \frac{\rho P_{\mathrm{t}} G_{\mathrm{t}} G_{\mathrm{r}} c^2 \sigma_{\mathrm{RCS},l}}{(4\pi)^3 f_c^2 (r_{\mathrm{t},l} r_{\mathrm{r},l})^2} \gamma_l \tag{6}$$

ì where ρ is the amount of transmitting power allocated for the sensing operation, G_{t} and G_{r} are the single-element antenna gains at the transmitter and receiver, γ_l accounts for the non-perfect alignment between the target direction of arrival (DOA) and the sensing direction (with $\gamma_l = 1$ indicating perfect alignment), c is the speed of light in vacuum, f_{c} is the carrier frequency of the transmitted signal, $\sigma_{\mathrm{RCS},l}$ is the radar cross section (RCS) of the lth target, $r_{\mathrm{t},l}$ and $r_{\mathrm{r},l}$ are the distances from the target to the transmitter and receiver, respectively, [44].

The range-Doppler matrix is obtained starting from $\mathbf{y}[k,m]$ and removing the unwanted data symbol as [5], [44], [45]

$$g_k^{(m)} = \tilde{y}_k^{(m)} / x_k^{(m)} = \left(\sum_{l=1}^{L} \tilde{\beta}_l \Upsilon(\theta_{\mathrm{t},l}, \theta_{\mathrm{r},l}) \right) + \tilde{n}_k \tag{7}$$

where $\tilde{y}_k^{(m)} = \mathbf{w}_{\mathrm{R}}^T \mathbf{y}_k^{(m)}$ with $\mathbf{w}_{\mathrm{R}}$ being the receiving beamforming vector; $\Upsilon(\theta_{\mathrm{t},l}, \theta_{\mathrm{r},l}) \in \mathbb{C}$ is a factor which accounts for the gain due to the array response vector at transmitter and receiver.

We collect the sensing snapshots into the matrix $\mathbf{G} \in \mathbb{C}^{K_{\mathrm{p}} \times M_{\mathrm{p}}}$ with entries $g_k^{(m)}$, where rows correspond to frequency (range) bins $k \in \{0, \ldots, K_{\mathrm{p}} - 1\}$ and columns to slow-time OFDM symbol indices $m \in \{0, \ldots, M_{\mathrm{p}} - 1\}$. The range–Doppler periodogram $\mathbf{P} \in \mathbb{C}^{K_{\mathrm{p}} \times M_{\mathrm{p}}}$ can be obtained as

$$\mathbf{P} = \mathbf{F}_{K_{\mathrm{p}}} \mathbf{G} \mathbf{F}_{M_{\mathrm{p}}}^{-1} \tag{8}$$

where $\mathbf{F}_N$ represents the FFT matrix with N taps, and $\mathbf{F}_N^{-1}$ represents the IFFT matrix with N taps.

Starting from the RDM matrix, target detection requires mitigating noise and clutter while preserving the correct association between range and Doppler bins. Although several algorithms can be used for range–Doppler target detection, the choice of detector is not the focus of this work. Instead, we aim to evaluate system performance under a widely adopted and representative detection framework. For this purpose, we consider the Cell-Averaging constant false alarm rate (CFAR) (CA-CFAR) technique [46]–[48], to adaptively set a detection threshold $T_{n,m}$ based on the noise statistics of the Range-Doppler Map (RDM), denoted as $P_{n,m}$. In such a case, the target is declared present at cell (n,m) if the related test exceeds the threshold, i.e., $|P_{n,m}|^2 > T_{n,m}$. This adaptive thresholding ensures robust detection performance under varying noise conditions in the RDM [49].

Our numerical evaluation focuses exclusively on target detection. However, in scenarios requiring further parameter estimation (e.g., angle-of-arrival or position refinement), additional high-resolution processing stages may be included. In such cases, algorithms such as MUSIC can serve as optional super-resolution components beyond the detection stage [5], [7], [44], [45], [50].

IV. System Model with Attack

In a classical replay attack, a malicious actor intercepts legitimate data transmissions and retransmits them later to deceive the recipient or circumvent security measures. This tactic is commonly employed in communication systems to gain unauthorized access or impersonate a legitimate user. In radar systems, an attacker may capture radar signals and retransmit them to confuse or mislead the radar receiver, potentially disrupting target tracking, identification, and even triggering false alarms. In this context, we now present a replay attack on a full-frame OFDM system and analyze its impact on sensing processing steps.

a) Signal Reception: The signal transmitted by each antenna is received by the attacker after propagation through the direct channel between the transmitter and the attacker as

$$r_{n,\mathrm{a}}(t) = s_n(t) * h_{\mathrm{TA}}(t) + w(t) \tag{9}$$

where $h_{\mathrm{TA}}(t)$ is the channel impulse response for the direct link between the transmitter and the attacker. The attacker applies to $r_{n,\mathrm{a}}(t)$ a manipulation filter with impulse response $h_{\mathrm{MF}}(t)$. Then, the signal is transmitted by the attacker towards the legitimate receiver, e.g. through a directive antenna, as $\tilde{s}_{n,\mathrm{a}}(t)$, where

$$\tilde{s}_{n,\mathrm{a}}(t) = r_{n,\mathrm{a}}(t) * h_{\mathrm{MF}}(t)\,. \tag{10}$$

b) Synchronization and Timing Considerations: The OFDM receiver at the legitimate node will synchronize with either the legitimate signal or the replayed one, by identifying the first correlation peak between the transmitted and received signals.

In a bistatic scenario, the first correlation peak typically corresponds to the direct path between the transmitter and receiver, and this peak is used to establish the receiver's timing reference. Any replayed or delayed signal therefore arrives strictly after the legitimate direct-path component. If the attacker amplifies and retransmits the replayed signal such that it becomes the dominant correlation peak, the receiver may lock onto this manipulated component and interpret it as the direct path. This shift in the timing reference alters the resulting delay-Doppler geometry and makes bistatic ISAC systems particularly sensitive to replay-based manipulation.

In a monostatic scenario, the transmitter and receiver share the same signal, and no direct-path component is observed at the receiver. The earliest detectable peak instead corresponds to the closest reflecting object, while the timing reference is fixed by the transmission itself. Although the direct-path timing cannot be spoofed in the same manner as in the bistatic case, synchronization to the received reflections remains necessary for both sensing and demodulation. As a result, replayed or manipulated reflections can still modify the delay-Doppler structure or mask weak targets, even though the attack mechanism differs from the bistatic case.

The aggregate delay (including signal reception at the attacker, manipulation, replay, and reception at the legitimate node) is ideally expected to fall within the cyclic prefix. When the total replay delay satisfies this condition, the replayed signal remains entirely within the guard interval, the circular

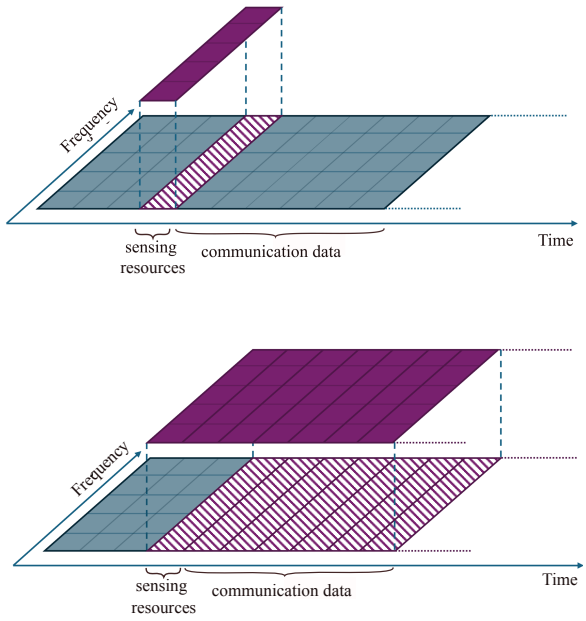


Fig. 2: Attack configurations in the time-frequency domain. Blue denotes the legitimate signal, solid violet indicates the attacker's transmitted signal, and hatched violet marks the time-frequency resources at the victim where the attacker's signal overlaps with the legitimate signal (i.e., the corrupted/overlaid portion received by the victim). The top panel illustrates a selective-spoofing scenario, in which the attacker overshadows only a subset of the legitimate resources. The bottom panel shows the full-frame meaconing configuration, which is the primary model considered in this work, where the attacker replays the entire received frame.

convolution property of OFDM holds, and no inter-symbol interference (ISI) is introduced. In this regime, orthogonality across subcarriers is preserved, and the spoofed signal is functionally equivalent to an additional multipath component.

In practice, however, the attack may result in delays that exceed the cyclic prefix. When the delay exceeds the cyclic prefix but not the symbol time, the circular convolution assumption breaks down: the replayed symbol partially overlaps with the next useful symbol interval, resulting in ISI and loss of perfect subcarrier orthogonality. The presence of ISI does not imply that sensing or synchronization must necessarily fail; rather, it means that the received signal contains an additional interference term whose magnitude depends on the amount of overlap.

These effects manifest differently depending on the spoofing strategy. In selective spoofing scenarios (top of Fig. 2, taken from case 2 in [23]) only part of the frame is replayed. Here, any delay beyond the CP produces partial overlap with an ongoing legitimate symbol, increasing sensitivity to ISI and making precise delay control more critical. Even a small excess delay can distort the demodulated samples, potentially degrading sensing performance. In contrast, full-frame meaconing (see bottom of Fig. 2) is less timing-critical. Because the entire frame (including pilots, data symbols, and synchronization fields) is replayed coherently, the delayed spoofed frame may be interpreted by the receiver as a self-consistent replica of the legitimate signal. Even when the cyclic prefix is exceeded, the receiver may lock onto the spoofed frame if it appears stronger or better correlated than the legitimate one, treating the delay-induced misalignment similarly to a long multipath component. In this regime ISI is still present, but it does not necessarily prevent synchronization or sensing: the receiver's estimator can still converge onto the spoofed replica as long as the delay remains within the useful symbol duration.

Experiments conducted with our testbed support this interpretation: by considering multiple cyclic prefix configurations and varying the attacker-induced delay beyond the CP duration, we observe that link disruption occurs only when the spoofing signal power is sufficiently increased, rather than as a direct consequence of delay misalignment. We observe that synchronization can still succeed with delays slightly exceeding the CP, not because ISI is absent, but because practical OFDM receivers are designed to maintain synchronization in the presence of multipath components with delays up to the useful symbol duration. Thus, the replayed signal can dominate the correlation metrics and act as the effective reference, even in the presence of the ISI term predicted by theory.

c) Demodulation: The receiver proceeds with OFDM demodulation following this synchronization. The signal at the receiver after the FFT block is the result of the superposition of the legitimate signal and the replayed signal

$$\begin{aligned}\mathbf{y}_k^{(m)} &= \mathbf{H}_k^{(m)}\mathbf{x}_k^{(m)} + \mathbf{n}_k \\ &\quad + \breve{\mathbf{H}}_k^{(m)}\mathbf{x}_k^{(m)} + \tilde{\mathbf{H}}_k^{(m)}\mathbf{w}_k \end{aligned} \tag{11}$$

where the first two terms are the same as (3) as they are due to the reflection from legitimate targets and the receiver noise; The term $\breve{\mathbf{H}}_k^{(m)}$ given by

$$\breve{\mathbf{H}}_k^{(m)} = \mathbf{H}_{\mathrm{TA},k}^{(m)}\mathbf{H}_{\mathrm{MF},k}^{(m)}\mathbf{H}_{\mathrm{AR},k}^{(m)} \tag{12}$$

represents the effective channel from the transmitter through the attacker to the receiver, and $\tilde{\mathbf{H}}_k^{(m)} = \mathbf{H}_{\mathrm{MF},k}^{(m)}\mathbf{H}_{\mathrm{AR},k}^{(m)}$ accounts for the noise component introduced by the attacker, where $\mathbf{H}_{\mathrm{MF},k}^{(m)}$ and $\mathbf{w}_k$ being the corresponding frequency-domain responses of the manipulation filter and noise at the attacker side, respectively.

If we consider an attacker with directive transmitting and receiving antennas (i.e., the position of the transmitter and receiver is known on the attacker side), we can consider a single path for the direct and reflected channel between the transmitter and the attacker and the attacker and the receiver. Then, after performing spatial combining through the receiving beamforming vector and removing the unwanted data symbol

$$g_k^{(m)} \simeq \Big(\sum_{l=1}^{L}\tilde{\beta}_l\Upsilon(\theta_{\mathrm{t},l},\theta_{\mathrm{r},l})\Big) + \tilde{n}_k + \xi\mathbf{H}_{\mathrm{MF},k}^{(m)} + \tilde{\tilde{w}}_k\,. \tag{13}$$

where the first two terms are equivalent to (7); the term $\tilde{\tilde{w}}_k$ is the residual received component of $\mathbf{w}_k$ after propagation

through the attacker-to-receiver path and after data symbol removal; ξ is a complex coefficient that takes into account the direct and reflected channel from the transmitter and from the attacker to the receiver; in particular

$$\xi = \alpha_{\mathrm{TA}}\alpha_{\mathrm{AR}}\Upsilon(\theta_{\mathrm{TA}},\theta_{\mathrm{AR}})e^{j\pi m T_{\mathrm{s}} f_{\mathrm{D,ar}}}e^{-j2\pi\frac{k}{T}(\tau_{\mathrm{TA}}+\tau_{\mathrm{AR}})} \quad (14)$$

where τ_{TA} is the delay from the transmitter to the attacker; τ_{AR} is the delay from the attacker to the receiver; $f_{\mathrm{D,AR}}$ is the Doppler shift due to the attacker; θ_{TA} is the relative angle between the attacker and the transmitter; θ_{AR} is the relative angle between the attacker and the receiver. We can now rewrite the matrix $\mathbf{G}$ with elements $g_k^{(m)}$ as

$$\mathbf{G} = \mathbf{G}_0 + \xi\mathbf{H}_{\mathrm{MF}} + \mathbf{W}_0 \quad (15)$$

where each element of $\mathbf{G}_0$ contains the effect of the legitimate channel (i.e., the first term of equation (13)); $\mathbf{W}_0$ depends on the residual noise replayed by the attacker after manipulation and contained in $\tilde{\tilde{w}}_k$; $\mathbf{H}_{\mathrm{MF}}$ is the channel response to the manipulation filter. Equivalently, one may view $\mathbf{H}_{\mathrm{MF}}$ as the block-diagonal (or block-stacked) matrix obtained by arranging the individual matrices $\mathbf{H}_{\mathrm{MF},k}^{(m)}$ across frequency and time. This notation emphasizes that the same manipulation filter operates across the entire OFDM frame, while still preserving the multi-antenna structure of each subcarrier response.

d) Range-doppler periodogram: The new range-Doppler periodogram matrix can then be rewritten as

$$\mathbf{P} = \mathbf{P}_0 + \mathbf{\Psi} + \mathbf{Z}_0 \quad (16)$$

where $\mathbf{P}_0 = \mathbf{F}_{K_{\mathrm{p}}}\mathbf{G}_0\mathbf{F}_{M_{\mathrm{p}}}^{-1}$ is the useful term containing the true target information; $\mathbf{\Psi} = \mathbf{F}_{K_{\mathrm{p}}}\xi\mathbf{H}_m\mathbf{F}_{M_{\mathrm{p}}}^{-1}$ is the intentional periodogram component introduced by the attacker and depending on the manipulation filter; $\mathbf{Z}_0 = \mathbf{F}_{K_{\mathrm{p}}}\mathbf{W}_0\mathbf{F}_{M_{\mathrm{p}}}^{-1}$ is the component due to the legitimate receiver noise and including an unintentional component due to the residual noise replayed by the attacker as $\mathbf{w}_k$.

V. Threat Model and Design of the Attacker Response

Previous works on replay attacks against ISAC systems [22], [23] have adopted a threat model akin to the one illustrated in Fig. 3 (left). In this scenario, the attacker captures the legitimate OFDM signal, demodulates and decodes it, manipulates its contents in the time-frequency domain (e.g., injecting range or Doppler shifts), re-encodes it, and finally re-transmits the modified signal. To be effective, all of this processing must occur within extremely tight latency constraints (e.g., order of a fraction of the OFDM symbol duration).

Executing such a complete processing chain within this limited time window is highly non-trivial: it demands advanced hardware capabilities, precise synchronization with the transmitter, and often prior knowledge of the signal structure, including reference signals and sensing parameters, which are typically concealed from adversaries in real-world ISAC deployments. As a matter of fact, while the theoretical implications of this threat model have been rigorously analyzed in [22], [23], neither of them has experimentally demonstrated its feasibility in realistic scenarios.

In contrast, our work introduces a much simpler and more practical threat model, illustrated in Fig. 3 (right). This model, based on a basic filter-and-retransmit strategy, entirely avoids demodulation, decoding, or signal parsing. The attacker simply captures the incoming OFDM signal, applies a basic filter (e.g., a small delay and frequency shift), and retransmits the result. As demonstrated in Section VII, this filter-and-retransmit approach is *practically viable and compatible with complex real-world frame structures such as 5G New Radio*: it can be deployed in a (somewhat) straightforward manner using commercial-off-the-shelf (COTS) SDRs and requires no knowledge of the underlying signal structure.

In the remainder of this section, we elaborate on three example threat models and explore strategies for designing the manipulation filter to effectively alter the system's response, without requiring any prior knowledge of the sensing parameters.

a) Target Injection via FIR filter: As a first simple threat model, we consider the injection of a single fake target into the sensing system. This threat applies to both monostatic and bistatic configurations. A single target injection can be performed by employing a finite impulse response (FIR) filter to introduce a delay of D samples with a single tap of amplitude α. To mimic a delay of τ_{d} we use the sampling rate T_{samp} and $D = \lfloor \tau_{\mathrm{d}}/T_{\mathrm{samp}} \rfloor$. The filter coefficients are

$$h_{\mathrm{MF}}[k] = \begin{cases} \alpha & \text{if } k = \lfloor \tau_{\mathrm{d}}/T_{\mathrm{samp}} \rfloor, \\ 0 & \text{otherwise.} \end{cases} \quad (17)$$

We then extend this model to the injection of N targets by using a FIR filter with N taps after sampling the received signal with sampling time T_{samp}. To introduce N targets with specific delays $D_1, D_2, \ldots, D_N$ and corresponding amplitudes $\alpha_1, \alpha_2, \ldots, \alpha_N$, the FIR filter coefficients $h_{\mathrm{MF}}[j]$ are defined as

$$h_{\mathrm{MF}}[j] = \begin{cases} \alpha_i & \text{if } j = D_i \text{ for } i \in \{1, 2, \ldots, N\}, \\ 0 & \text{otherwise.} \end{cases} \quad (18)$$

The output of the FIR filter is the sampled version of the signal $\tilde{s}_{n,\mathrm{a}}(t)$ in (20), i.e.,

$$\tilde{s}_{n,\mathrm{a}}[q] = \sum_{i=1}^{N} \alpha_i \cdot \tilde{r}_{n,\mathrm{a}}[q - D_i]. \quad (19)$$

As a time-invariant filter, the FIR does not introduce a Doppler shift. The Doppler shift of the injected targets would depend on the attacker speed through ξ in (13). Time-variant filters can be used instead of FIR filters to introduce a Doppler shift. A simpler approach would be to insert a fake Doppler shift equal to all the injected targets before the FIR filter to the received signal, i.e.

$$\tilde{s}_{n,\mathrm{a}}[q] = (r_{n,\mathrm{a}}[q] \cdot d[q]) * h_{\mathrm{MF}}[q]\,. \quad (20)$$

where $d[q] = e^{j2\pi\delta_{\mathrm{f}} q T_{\mathrm{samp}}}$. Then, all the injected targets are considered with the same speed.

An alternative approach is to use a bank of FIR filters after introducing a Doppler shift. Specifically, different delayed copies of the received signal can be generated, each associated with a different Doppler frequency shift, before being

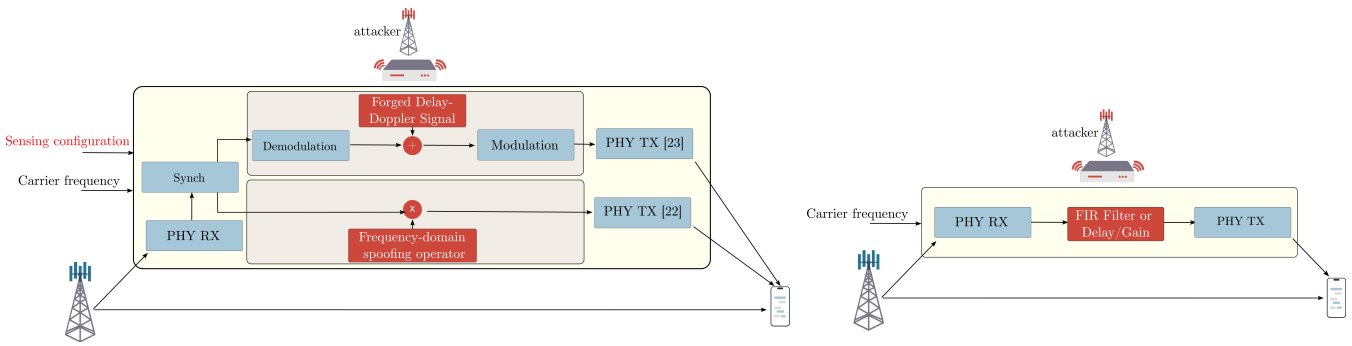


Fig. 3: Threat models comparison. Replay pipeline involving demodulation, manipulation in the time-frequency domain, and re-encoding, as done in [22], [23] (left). Our elementary filter-and-retransmit replay pipeline (right).

processed by separate FIR filters. This allows the attacker to simulate multiple injected targets, each with a different frequency shift $\delta_{\mathrm{f},i}$ with $i = 1, 2, \ldots, N$. Mathematically, the received signal can be modified as follows

$$\tilde{s}_{n,\mathrm{a}}[q] = \sum_{i=1}^{N} \alpha_i \cdot e^{j2\pi\delta_{\mathrm{f},i} q T_{\mathrm{samp}}} \tilde{r}_{n,\mathrm{a}}[q - D_i]. \tag{21}$$

This approach naturally increases the complexity of the operation, making it more challenging to be implemented within the 5G OFDM time constraints.

b) Direct Path Shift in Bistatic Configuration: In a bistatic configuration, the transmitter-receiver direct path range r_{dp} might be unknown. Therefore, the receiver first estimates the direct path range and subsequently calculates the target-receiver distance [45]. When the injected target has a higher amplitude than the signal received through the direct path, it can dominate the overall received signal, effectively shifting the perceived direct path. Considering the power ratio between the replayed signal and the legitimate one, the attacker component is higher than the legitimate one when

$$\frac{\gamma_{\mathrm{a}} \max_i\{\alpha_i\}}{4\pi\left(\frac{r_{\mathrm{ta}} r_{\mathrm{ra}}}{r_{\mathrm{dp}}}\right)^2} \geq 1\,. \tag{22}$$

In such a case, the receiver may interpret the injected signal as the direct path and estimate the direct path range as

$$\hat{r}_{\mathrm{dp}} = r_{\mathrm{ta}} + r_{\mathrm{ra}} + (T_{\mathrm{proc}} + D_{i_{\max}} T_{\mathrm{samp}})c \tag{23}$$

where T_{proc} is the processing time at the attacker before retransmission and $i_{\max} = \arg\max \alpha_i$. This results in a direct path shift, altering the reference timing for range estimation. Consequently, all true targets' measured ranges will be shifted, potentially causing errors in localization and tracking. Indeed, the estimated target would be [45]

$$\hat{r}_l = \frac{(r_{\mathrm{t},l} + r_{\mathrm{r},l})^2 - \hat{r}_{\mathrm{dp}}^2}{2[(r_{\mathrm{t},l} + r_{\mathrm{r},l}) + \hat{r}_{\mathrm{dp}} \sin(\theta_{\mathrm{r},l} - \pi/2)]}\,. \tag{24}$$

c) Target Masking and Interference Effects: When a target is injected with significantly high reflection power, it can obscure weaker targets due to interference effects, and in particular: (i) the Doppler shift associated with the injected path causes energy to leak across adjacent subcarriers, generating inter-carrier interference (ICI); (ii) when the replayed signal extends beyond the cyclic prefix creates inter-symbol interference (ISI) due to the overlap between the replayed portion of the previous OFDM symbol and the current symbol. Under these conditions, the received symbol on subcarrier k of OFDM symbol m can be expressed as [51], [52]

$$\mathbf{y}_k^{(m)} = \sum_{n=0}^{N-1} \tilde{\mathbf{H}}_{k,n}^{(m,m)} \mathbf{x}_n^{(m)} + \sum_{n=0}^{N-1} \tilde{\mathbf{H}}_{k,n}^{(m,m-1)} \mathbf{x}_n^{(m-1)} \tag{25}$$

where the first term represents the ICI-induced spectral leakage within symbol m, and the second term captures the ISI contribution arising from the previous symbol $m-1$. As expected, this ISI term becomes non-zero only when the replay delay exceeds the CP, consistent with standard OFDM results [53].

Beyond these linear interference mechanisms, nonlinearities such as receiver saturation, quantization artifacts, and phase noise can further distort the received signal, thereby exacerbating both ICI and ISI.

As a result, the effect of the attack on the RDM is twofold:

- First, it introduces the contribution of the injected targets, not only within the specific Doppler and range bins but also in adjacent bins due to the replayed residual noise as well as ISI and ICI effects. This results in an overall distortion of the RDM, which can be quantified as an error with respect to the attack-free RDM, characterized by $\mathbf{\Psi} + \mathbf{Z}_0$ in (16).
- The attack impacts detection as the noise power estimation incorporates the injected targets. Consequently, the higher the received power of the injected targets, the higher the CFAR threshold, potentially leading to the obfuscation of real targets. The extent of this obfuscation depends on the design of the manipulation filter.

Nevertheless, the interference caused by ICI and ISI not only degrades radar detection but also significantly impacts the communication system. The increased interference power can lead to a deterioration of signal-to-noise ratio (SNR), causing reduced data rates, higher bit error rates (BER), and even communication link failure. When the interference level becomes excessively high, similar to deceptive jamming, it can completely interrupt communication. This threat applies to both monostatic and bistatic configurations.

VI. Simulation Results

In this section, we analyze the impact of the proposed blind replay attack on the ISAC system through system-level simulations in a bistatic configuration. Our investigation focuses on how varying the attacker's gain and distance, via single-tap and two-tap FIR filtering, affects the sensing performance. In particular, our threat model suggests that the attacker can both inject false targets and mask genuine targets by adjusting the manipulation filter. The simulation metrics include the number of estimated targets, the probability mass function (PMF) of target detection, and the root mean square error (RMSE) of the RDM. The RMSE for the RDM is obtained by considering as RDM error, the difference between the RDM without attack and the one obtained with the attack.

A. Simulation Settings

For our simulations, we employed the 5G-based Link-level ISAC open-access simulator available on GitHub [54]. We adapted the simulator from a monostatic to a bistatic configuration and modified it to incorporate an attacker designed to disrupt the system. The simulated scenario illustrated in Fig. 4 features a gNB establishing a 5G connection with a UE. In the simulations, the PDSCH is configured with a 16 QAM modulation scheme and a target code rate of 490/1024. The number of transmission layers is set to 2, while the number of codewords is 1. HARQ is enabled, with 16 parallel HARQ processes and a redundancy version sequence of [0 2 3 1]. The LDPC decoder uses the normalized min-sum algorithm, with a maximum of 6 decoding iterations per codeword. During communication, the UE simultaneously performs target estimation under the ISAC paradigm. In this setup, the estimated ranges are the sum of the gNB–target and target–UE paths (i.e. the bistatic range), with two targets at $r_1 = 244.26\,\text{m}$ and $r_2 = 335.94\,\text{m}$, both moving at 5 m/s and with $\sigma_{\text{RCS},1} = \sigma_{\text{RCS},2} = 1\,\text{m}^2$. The attacker is positioned at a distance $r_{\text{A}} = 20\,\text{m}$, 40 m, and 80 m from the UE along a line forming a 135 degree angle with the x-axis, and moves at 5 m/s.

The transmitted signal is a full-frame OFDM waveform operating at a carrier frequency of 3.5 GHz, with a system bandwidth of 100 MHz and a subcarrier spacing of 60 kHz. The gNB is equipped with an 8×8 array for both transmission and reception (with a single antenna element in the vertical direction), while the attacker uses a single-element directional antenna. The transmit antenna gain at the gNB and the receive antenna gain at the UE are $G_{\text{t}} = G_{\text{r}} = 25.5\,\text{dB}$. Target detection is performed using a CFAR-CA algorithm to estimate range and velocity, with a selected per-cell false alarm probability $P_{\text{fa}} = 10^{-9}$. A very low false alarm probability is adopted because the statistical test is applied independently to all range-Doppler resolution cells, causing the global false alarm rate to scale linearly with the number of cells under test. Given the size of the processed range-Doppler map, which in our configuration contains 7030 cells, choosing $P_{\text{fa}} = 10^{-9}$ ensures that the resulting global false alarm probability is $P_{\text{FA,global}} \approx 7.0 \times 10^{-6}$.

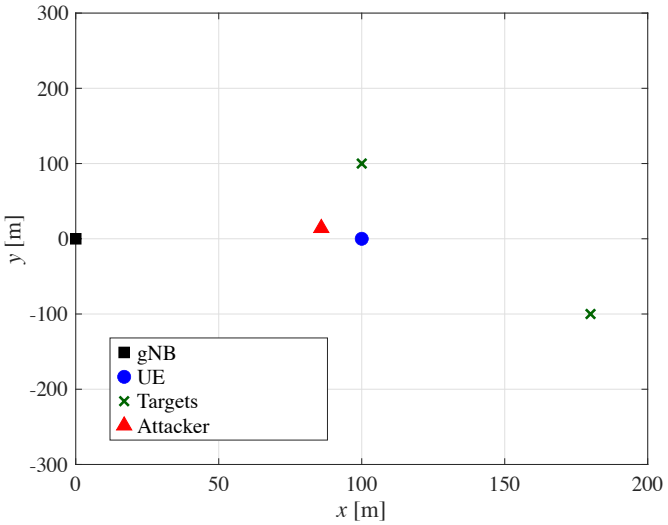


Fig. 4: Simulated scenario including the spatial layout of the gNB, UE, targets, and the attacker. In this illustrated configuration, the attacker is positioned 20 m from the UE.

The CA-CFAR algorithm estimates the noise power at a given range-Doppler cell (n, m) by averaging the power measurements from a set of neighboring training cells, denoted by $\mathcal{T}$. These training cells are selected from the surrounding area while excluding guard cells that are close to the test cell, in order to avoid contamination from target signals. For the ith detected target, the estimated range $\hat{r}_i$ and speed $\hat{v}_i$ are computed as

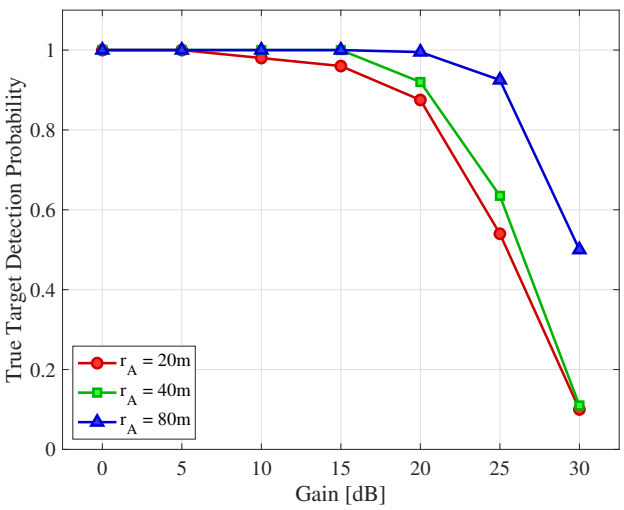
$$\hat{r}_i = \frac{\hat{q}_i\, c}{2\,\Delta_f\, K_p}, \quad \hat{v}_i = \frac{\hat{p}_i\, c}{2\, f_c\, T_s\, M_p}. \tag{26}$$

In this scenario, the attacker disrupts the sensing process by manipulating the received signal with a FIR filter with $N = 1$ (one tap) or $N = 2$ (two taps). The FIR filter is designed with randomly selected taps, i.e., D_i are random sample indices ($i = 1, 2$) that vary at each simulation. The filter gain is constant $\alpha_i = \alpha_0$ varies as 0 dB, 5 dB, 10 dB, 15 dB, 20 dB, 25 dB, and 30 dB. This allows the attacker to generate one or two fake targets at different ranges. The attacker introduces an additional frequency shift, which varies at every simulation, on top of the Doppler shift naturally caused by its motion. As a result, the system estimates velocities for the fake targets that differ from the attacker's actual velocity. By varying the attacker's gain and distance, we investigate how the attacker can inject false targets or obscure genuine ones, thereby degrading the system's sensing accuracy.

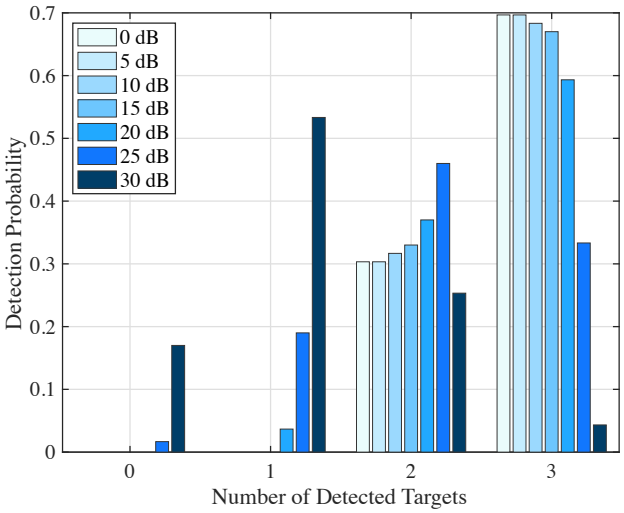
B. Performance Evaluation

1) Single-Tap Attack: The attacker injects one fake target in the first set of simulations using a single-tap FIR filter. We study the effect of varying the attacker's gain on the target detection performance.

Fig. 5a shows the probability of true target detection as a function of the attacker's gain for different attacker distances, while Fig. 5b presents the PMF for the total number of detected targets (both true and false). As the attacker's gain

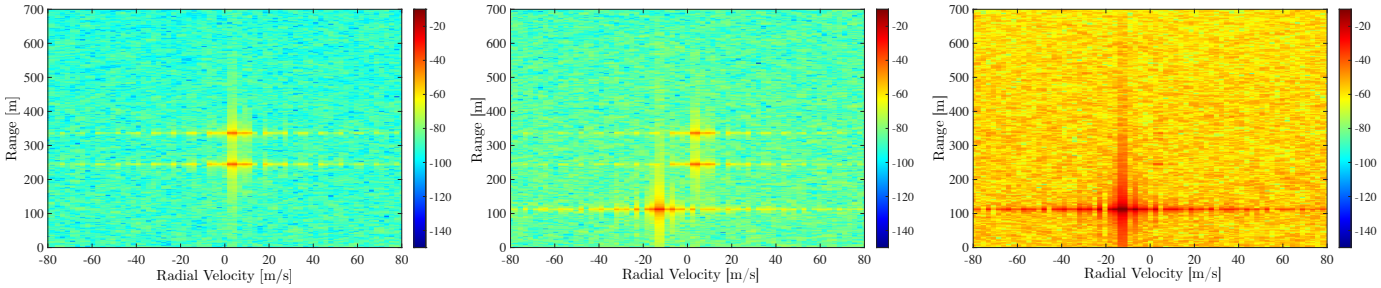


(a) Probability of detecting the genuine target.



(b) Overall PMF of total detected targets.

Fig. 5: Performance metrics for the single-tap FIR attack scenario. (a) Probability of genuine target detection falls steeply with increasing attacker gain; and (b) Probability mass function for the total detected targets (genuine and injected ones); higher attack gains may completely mask the genuine target.



(a) Without the presence of attack. (b) With an attacker gain below 20 dB. (c) With an attacker gain of 25/30 dB.

Fig. 6: RDMs for the single-tap attack: without an attack (a), two true targets are clearly visible. Below 20 dB (b), one additional false target appears, while at 25/30 dB (c), the genuine targets are completely concealed, leaving only the false detection.

increases, the probability of detecting the genuine target drops sharply because the strong replayed peak, and its sidelobes, progressively masks the true reflections. For a range of 20 m, the detection probability of true targets falls from 98% at 10 dB to 54% at 25 dB, and further down to 10% at 30 dB. A similar trend is observed for greater attacker-to-UE distances; however, as the distance increases, the attacker becomes less able to suppress genuine targets, leading to higher detection probabilities. For instance, at a gain of 30 dB and a range of 80 m, the true target detection rate remains around 50%. Fig 5b reflects this behavior: at higher attacker gains ($\sim$ 30 dB) the system often detects either no target or only the injected false one, as the strong replay peak inflates the CA-CFAR threshold and conceals the genuine target. Occasional cases with multiple detected targets still appear but are significantly less frequent.

The RDMs in Fig. 6 visually represents these effects. The genuine targets are clearly observed without an attack (Fig. 6a). At attacker gains below 20 dB (Fig. 6b), the injected false target begins to appear while the genuine targets remain detectable, though increasingly perturbed. At higher gains

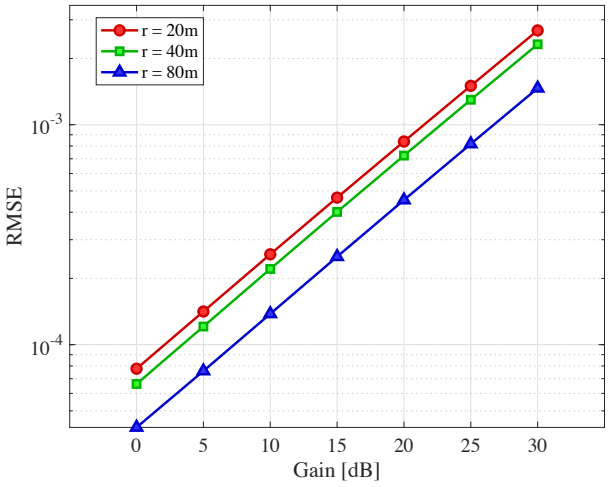


Fig. 7: RMSE of the RDM versus attacker gain for the single-tap attack. The rising RMSE indicates that increased false target injection and masking of the genuine target at high gains deteriorate sensing accuracy.

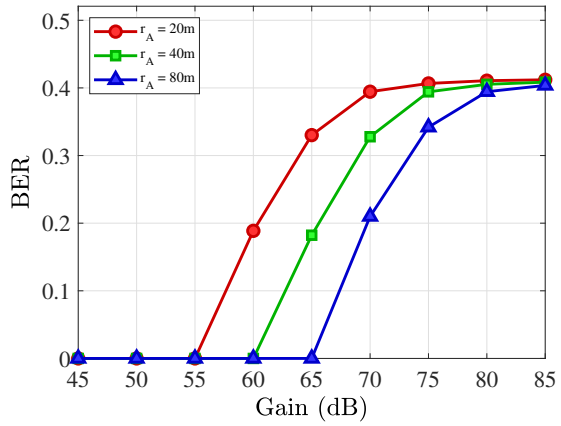


Fig. 8: BER as a function of the attacker's gain for the FIR configuration with one tap. The BER remains zero for gains below 55 dB and increases as the gain increases, reaching excessively high values above 70 dB, leading to a denial of the communication service.

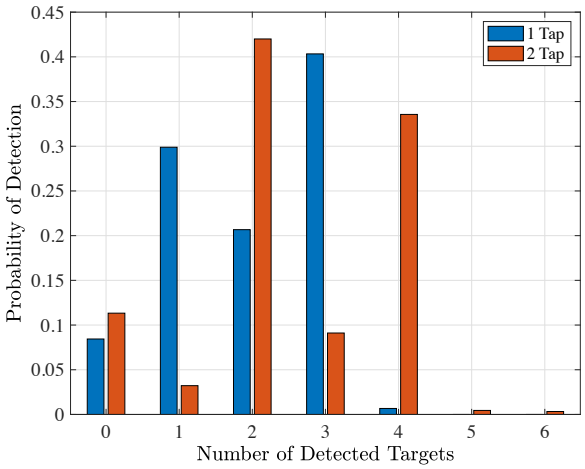


Fig. 9: Comparison of the PMF for the total number of detected targets (both true and fake) in single-tap (blue) and two-tap (red) attack configurations. The number of genuine targets is 2.

(Fig. 6c), the sidelobes of the strong replayed peak dominate the delay-Doppler plane, and the genuine targets become fully concealed. This visual progression is consistent with the trend observed in Fig. 5 and is quantified in Fig. 7, where the RMSE increases as attacker gain grows and attacker–UE distance decreases, reflecting the resulting degradation in sensing accuracy.

To analyse the impact on the communication layer, the simulations were used to evaluate how the bit error rate (BER) evolves as a function of the attacker's gain. Fig. 8 shows the BER trend for the one-tap attack scenario. It can be observed that, for attacker power levels below 55 dB, the communication remains fully operational, with a BER equal to zero. In this condition, the attacker is able to mask the true targets by using gains higher than 25 dB (Fig. 6c and 10c) without interrupting or degrading the performance of the communication service. As the attacker's gain increases, the BER gradually rises, reaching excessively high values around 70-80 dB, at which point the communication link collapses. This trend confirms that the replayed waveform, even without an explicit jamming attempt, acts as an interference component whose impact grows with both gain and attacker proximity. Therefore, the replay-induced Doppler and multipath distortions can effectively create fast-fading conditions and degrade link reliability.

2) Two-Tap Attack: In the next set of simulations, the attacker employs a two-tap FIR filter to inject two fake targets simultaneously. Fig. 9 compares the PMF for the total number of detections between single-tap (blue) and two-tap (red) configurations. The two-tap attack typically results in a higher number of detections at moderate gains, occasionally introducing up to four false targets and bringing the total number of detections to six, although such occurrences are rare; however, at high gains, the outcome is similar, only false targets are detected, in full agreement with our threat model, with a high probability of observing exactly two detections corresponding to the injected targets.

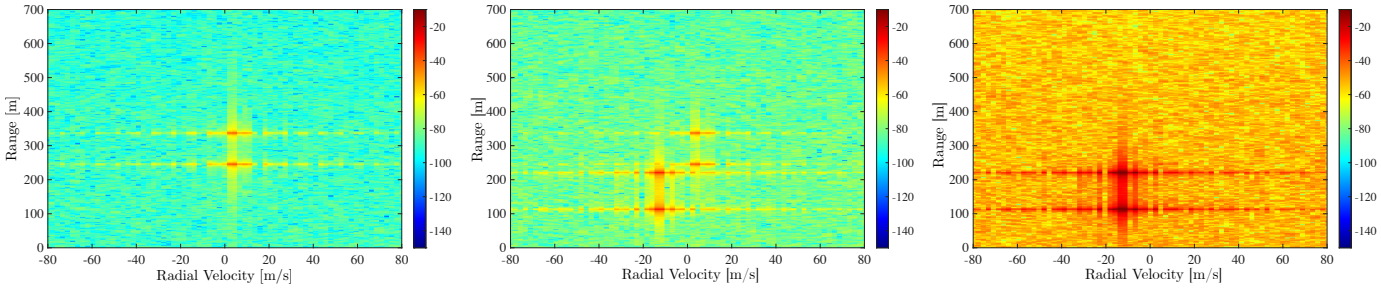
The RDMs in Fig. 10 visually confirms these observed trends. As in the previous single-tap attack configuration, the genuine targets are clearly seen in the absence of an attack (Fig. 10a). Below 20 dB (Fig. 10b), additional false targets are introduced, while at 25 dB and 30 dB gain the genuine targets are completely masked (Fig. 10c), leaving only the injected false targets.

C. Discussion of Simulation Results

The simulation results consistently confirm our threat model. They demonstrate that by carefully tuning the gain and FIR filter parameters, the attacker can both inject additional false targets and completely conceal genuine targets. In the single-tap scenario, moderate gains add one false target, while at high gain (30 dB), the genuine target is fully masked. In the two-tap configuration, a similar pattern is observed. These findings are evident in the PMF curves and the visual appearance of the RDMs, as well as in the rising RMSE values. These results demonstrate the possibility of manipulating the sensing outcome, underscoring the importance of evaluating the feasibility of such attacks and their impact on communication performance, both of which will be experimentally examined in Sec. VII.

VII. Experimental Results

This section presents the experimental evaluation of the proposed replay-based attack on our ISAC testbed, focusing on both 5G communication and sensing services. We first briefly reference the results of instantaneous attacks on downlink PRS, as detailed in our previous work [39], and then introduce and analyze the incremental attack strategy, designed to maximize stealth by minimizing visible communication degradation. We report and discuss the outcomes of incremental attacks on both downlink positioning reference signal (PRS) and uplink Sounding Reference Signal (SRS), with



(a) Without the presence of attack. (b) With an attacker gain below 20 dB. (c) With an attacker gain of 25/30 dB.

Fig. 10: RDMs for the two-tap attack scenario: without an attack (a), the true targets are distinctly visible. With an attacker gain below 20 dB (b), additional false targets are injected, and at 25/30 dB (c), the real targets are completely concealed, resulting in the detection of only false targets.

particular attention to the joint communication and sensing impact observable in the uplink case.

A. Testbed Setup

Our ISAC testbed integrates robust communication and high-resolution sensing within a unified, compact framework. All experimental evaluations were conducted in a controlled indoor laboratory environment to avoid any interference with legitimate networks or other devices.

Our testbed, depicted in Fig. 11, features a commercial Athonet 5G core network [55] connected to an Amarisoft Call Box Mini gNB [56]. The gNB operates in the N78 band using Time Division Duplex (TDD), with a bandwidth of 40 MHz allocated for communication and 100 MHz for positioning and sensing. As dedicated sensing reference signals are not yet standardized [1], [57], our evaluation leverages the PRS for downlink sensing and the SRS for uplink sensing.

1) Downlink: We assess communication and sensing performance separately.

- Communication: A COTS Samsung A54 5G smartphone is used to monitor downlink quality metrics (reference signal received power (RSRP) and signal-to-interference-plus-noise ratio (SINR)). The UE is positioned at a distance of ~ 2 m from the gNB.
- Sensing: A NI Ettus USRP X310 [58], acting as a sensing-specific UE and placed alongside the smartphone at roughly 2 m from the gNB, captures the PRS using an omnidirectional antenna (2 dBi gain) [59]. The X310 operates at a sampling rate of 122.88 Msps, and the resulting ranging data is then processed in MATLAB.

2) Uplink: We jointly evaluate both services from the gNB's perspective, using a single COTS UE.

- Communication & Sensing: The Amarisoft platform analyzes the uplink transmissions from the Samsung A54 smartphone. It measures the uplink bitrate to determine communication performance while simultaneously processing the Channel Impulse Response (CIR) of the transmitted SRS to assess sensing performance.

The replay-based attack is implemented using a NI Ettus USRP X410 [60] with onboard Xilinx Zynq-Ultrascale+ ZU28DR RFSoC FPGA processing operating at a sampling rate of 245.76 Msps to minimize latency down to ~ 3.9 μs, and is equipped with a directional HyperLOG 6080 antenna (receive gain 6 dBi) [61] for reception and an omnidirectional antenna for retransmission. The attacker is positioned at a distance of ~ 1.5 m from the gNB and ~ 0.5 m from the victim UE. A Keysight mxa9021b spectrum analyzer [62] continuously monitors the power distribution across OFDM resource elements, validating the attack's spectral impact.

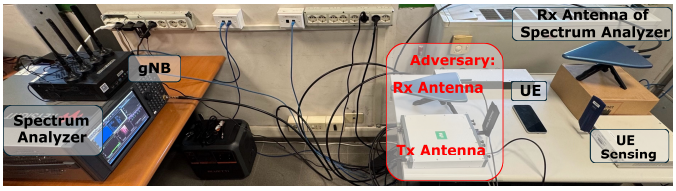
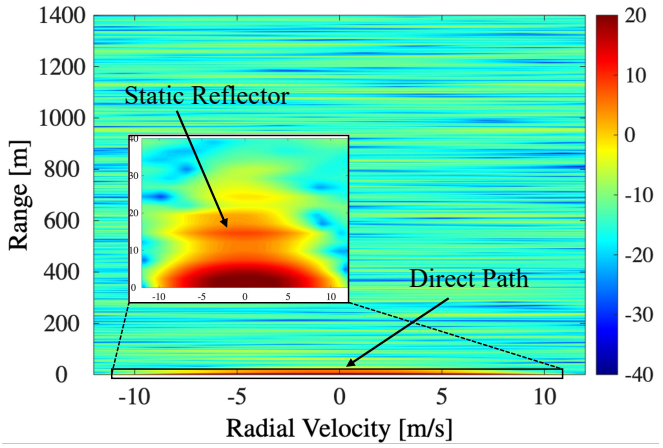


Fig. 11: Experimental testbed for the replay-based attack: an Amarisoft Call Box Mini gNB, two UEs (a COTS smartphone for communications and a USRP X310 for positioning), a USRP X410 acting as the attacker, and a Keysight mxa9021b spectrum analyzer monitoring the signal's power distribution.

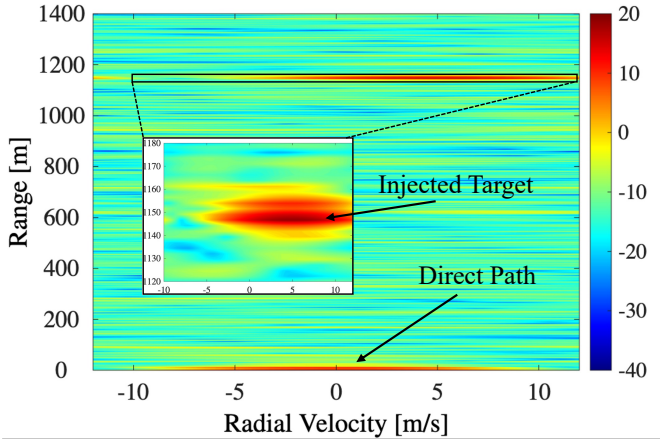
B. Attack Implementation and Configuration

As in [39], the replay-based attack is implemented using a radio loopback mechanism on our SDR platform. The attacker captures the legitimate OFDM signal, applies a programmable delay, and retransmits it with increased power, functionally equivalent to a single-tap FIR filter. The delay is precisely controlled through the samples per packet (SPP) parameter in the FPGA-based RFSoC architecture, which we set to 100, corresponding to about 3.9 μs delay. This short delay in the uplink scenario ensures that the injected path's peak remains within the limited CIR window of the Amarisoft gNB. By boosting the retransmitted signal's power, the attacker can inject false targets or mask genuine ones, while maintaining operational communication.

Since the attacker does not know the attacker to receiver channel and cannot observe the true target echo power, the replay transmit power cannot be set analytically. Instead, the attacker relies on an incremental power strategy. For target injection, the attacker selects the desired apparent radar cross section at the receiver and increases the replay amplitude



(a) Experimental RDM with no attack.



(b) Experimental RDM with attack of gain 48 dB and frequency shift 100 Hz.

Fig. 12: RDMs at the receiver: without an attack (a), the legitimate direct path appears centered at zero range and zero Doppler, as highlighted in the plot zoom. In (b), the attacker introduces a fake target at a bistatic range of approximately 1150 m, and induces an apparent radial velocity of 5 m/s by applying a 100 Hz frequency offset to the retransmitted signal.

gradually until the forged peak becomes detectable with the intended power level in the range Doppler map. This approach implicitly compensates for the unknown channel. For target concealment, the attacker does not aim at a specific received power but simply increases the replay power, subject to the constraint of not disrupting the communication link. Thus, power selection is driven by the observable effect on the sensing output rather than by channel knowledge.

Considering a downlink scenario, the resulting RDM at the receiver, with and without the attack, is shown in Fig. 12. In the absence of the attack (Fig. 12a), the strongest correlation peak corresponding to the direct path is aligned to zero range, and due to the static nature of the setup, it also appears at zero Doppler. To be more specifically, as shown in the zoomed-in views around the zero-range region, in addition to the direct path we can clearly distinguish also another peak, with lower power, around 7 meters and zero Doppler caused by the static reflection of the legitimate signal. When the attacker is active, an additional target appears in the RDM. The bistatic range of the fake target is determined by the delay introduced by the attacker, a delay of approximately 3.9μs results in a range of about 1150 m. Moreover, by retransmitting the delayed signal with a frequency offset, the attacker successfully induces an apparent Doppler shift. This creates the illusion of motion in the forged target. In the Fig. 12b, retransmits the signal with a 100 Hz offset, which the receiver interprets as a radial velocity of about 5 m/s as clearly illustrated in the zoomed-in region around the injected target.

As detailed in [39], a straightforward instantaneous relay attack, where the attacker immediately transmits with high power, can severely disrupt both sensing and communication. While highly effective at injecting false peaks and biasing localization, this approach causes a sharp drop in SINR and a sudden, visible reduction in communication bitrate, making it easily detectable by standard network monitoring. Such abrupt anomalies limit the stealth and practical impact of the attack in real-world scenarios.

To address these limitations, we designed a smarter incremental relay attack. In this approach, the attacker gradually increases its transmit power in small, controlled steps, mimicking natural channel variations and minimizing abrupt changes in communication metrics. This strategy preserves the attack's effectiveness against sensing while significantly reducing the risk of detection due to communication anomalies.

C. Incremental Attack on Downlink PRS

1) Communication Impact: In the incremental attack scenario, the attacker ramps up its TX gain from 30 dB to 60 dB in steps of 3 dB every 15 seconds. As shown in Table I and Fig. 13, the SINR at the UE gradually degrades from 21 dB to -5 dB, while the RSRP remains relatively stable. The downlink bitrate decreases smoothly, allowing the link adaptation mechanism to progressively lower the modulation order (from 16-quadrature amplitude modulation (QAM) to quadrature phase shift keying (QPSK)) without triggering abrupt alarms. This demonstrates that the incremental attack can stealthily degrade communication performance, avoiding the sudden drops that would likely trigger detection.

2) Sensing Impact: On the sensing side, the impact follows the same trend shown in [39]. Indeed, the incremental attack translates to a progressively stronger malicious correlation peak in the PRS correlator output. This can result in false target injection and, at higher attacker gains, even mask the legitimate path, compromising the accuracy and reliability of the sensing function. Initially, the injected path (IP) appears as a minor peak, but as the attacker's power increases, its amplitude grows and can eventually dominate the legitimate direct path (DP). In such a case, the spatio-temporal reference of the system might be compromised.

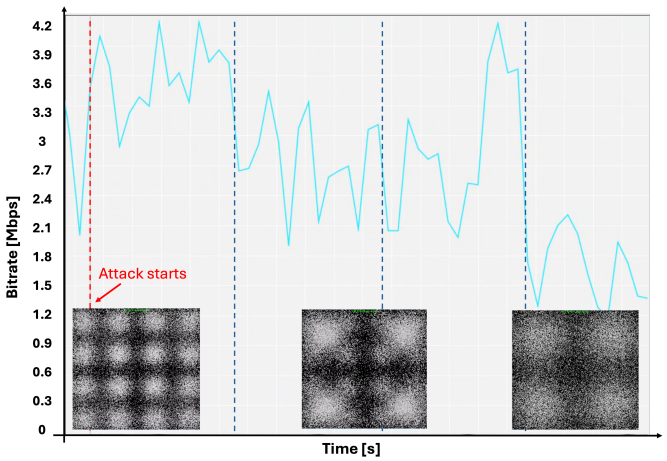


Fig. 13: Downlink bitrate and modulation constellations during the incremental PRS attack. Bitrate declines stepwise with each 3 dB increase in attacker TX power (dashed lines mark each increment).

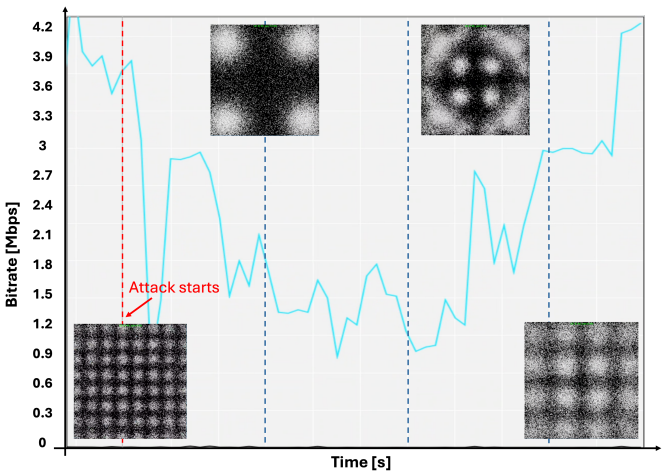


Fig. 14: Uplink bitrate and modulation constellations during the incremental SRS attack. The bitrate initially drops, then increases stepwise with each 3 dB increment in attacker TX power (dashed lines).

TABLE I: RSRP and SINR at the UE during the DL PRS incremental attack. Attacker RX gain fixed at 43 dB; TX gain is increased.

	No Attack	**Attacker TX Gain (dB)**									
Metric	(TX Gain 0)	30	33	37	40	43	47	50	53	57	60
RSRP	-93	-94	-93	-95	-93	-92	-97	-95	-96	-95	-95
SINR	21	20	18	14	13	12	5	4	1	-2	-5

D. Incremental Attack on Uplink SRS

1) Communication Impact: We further extend the incremental attack to the uplink, targeting the SRS in a TDD configuration. The attacker captures the legitimate SRS with a directional antenna and retransmits a delayed version using an omnidirectional antenna, incrementally raising the TX gain. In this scenario, the uplink bitrate exhibits a non-monotonic trend: it initially drops sharply due to destructive interference, then gradually recovers as the attacker's signal becomes dominant and the network's link adaptation logic mistakenly interprets the malicious signal as an improvement in channel quality. This is reflected in the modulation order, which is first reduced to QPSK and then increased back to 16QAM as the attacker's power rises (Fig. 14), exposing a critical vulnerability in the link adaptation mechanism.

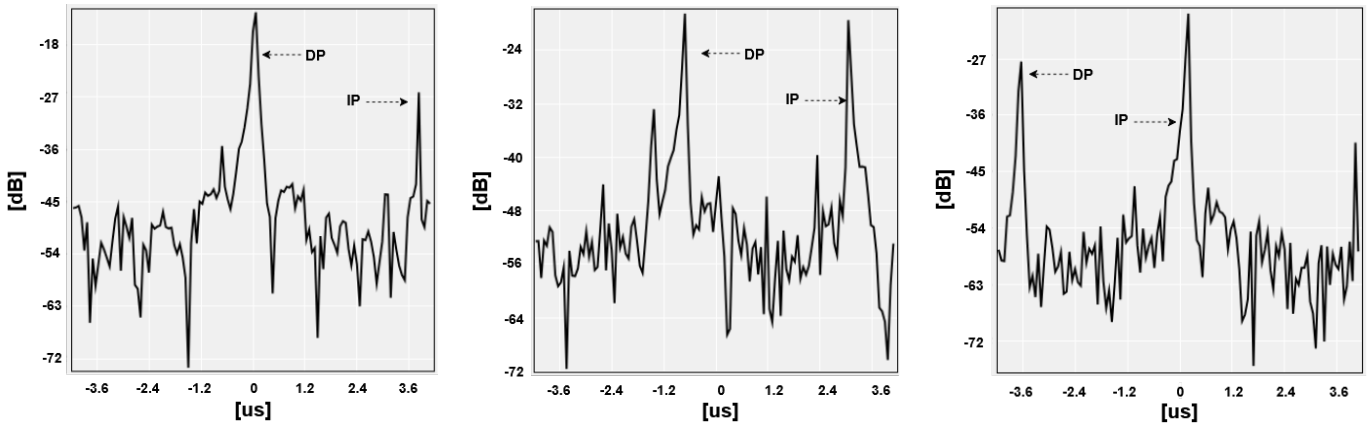
2) Sensing Impact: The attack's impact on uplink sensing is evaluated by analyzing the CIR and SNR of the SRS at the gNB. As shown in Fig. 15a, the legitimate direct path appears as the central peak, while the attacker successfully injects a delayed peak corresponding to the malicious path with a gain of 44 dB. At this point, the SNR of the SRS is 10.9 dB. As the attacker's gain increases to 48 dB (Fig. 15b), the SNR drops significantly to -7.1 dB, and the legitimate peak is no longer centered. Finally, in Fig. 15c, with a gain of 52 dB, the attacker's peak becomes dominant, and the gNB resynchronizes on it. The SNR in this case slightly recovers to 0.4 dB. The time offset between the peaks matches the configured delay, i.e. approx. 4 μs delay, confirming the attack's precision and its potential to compromise both communication and sensing integrity in integrated systems.

VIII. Countermeasures and Defensive Strategies

To effectively mitigate blind replay attacks, ISAC systems must adopt defensive strategies that operate across multiple layers of the sensing and communication stack. A first line of defense is multistatic cooperation, where geographically distributed sensing nodes share measurements to introduce redundancy and cross-validation. Because replayed echoes originate from a single adversarial transmitter rather than from spatially distributed scatterers, multistatic fusion can reveal inconsistencies in angle, delay, or Doppler signatures observed across nodes. At the signal-processing level, replay attacks can be detected by examining temporal coherence features that are inherently difficult for an attacker to reproduce. For example, analyzing temporal correlations in the range–Doppler domain can reveal unnatural persistence, abrupt discontinuities, or repeated target trajectories created by replayed frames. Similarly, monitoring inter-frame channel phase continuity enables the receiver to detect phase patterns that are inconsistent with genuine radar propagation.

Another complementary indicator is the impact of the attack on the communication SINR, which may subtly deviate from expected values due to the injected echo structure. Although these deviations may be small, they provide a practical anomaly cue that can be monitored continuously with minimal overhead. Importantly, gradual or incremental manipulation of SINR is more challenging to detect, as it can remain within the natural variability of wireless channels; characterizing the limits of such detection and developing robustness against incremental perturbations constitute promising directions for future work.

More broadly, physical-layer consistency checks, such as verifying range–Doppler coupling, assessing the spatial diver-



(a) CIR when the attacker gain is 44 dB. The attacker injects a delayed peak.

(b) CIR when the attacker gain is 48 dB. The legitimate peak is no longer centered.

(c) CIR when the attacker gain is 52 dB. The gNB resynchronizes on the injected peak.

Fig. 15: SRS CIR at the gNB during the incremental attack. The CIR window shows both the legitimate direct path (DP) peak and the delayed malicious injected path (IP) peak. As the attacker's gain increases, the receiver resynchronizes on the injected peak.

sity of echoes, or incorporating anomaly detectors trained on clean radar returns, can improve resilience. Combining these techniques can substantially enhance the robustness of ISAC systems, hindering adversarial attempts to manipulate sensing results.

IX. Final Remarks

We presented a scenario in which an external adversary, operating outside the network and without prior system knowledge or access to sensing parameters, can compromise an OFDM-based ISAC system. The attacker is unable to sniff control information and must remain stealthy with respect to the communication link, restricting them to blind manipulation and delay of the over-the-air signal. Despite these stringent constraints, we show that the adversary can deceive the sensing functionality by performing full-frame manipulation and replay of the OFDM signal, achieving range shifts, Doppler distortions, or complete target concealment while leaving data transmission uninterrupted.

The practicality of the proposed attack is particularly noteworthy. It requires no synchronization, no system knowledge, and only commodity hardware, yet results in sophisticated manipulation of radar observables. These findings highlight a significant vulnerability in ISAC architectures that must be addressed as such systems become integral to next-generation wireless networks.

It is also important to consider that current hardware limitations, while restrictive today, are temporary. The rapid evolution of SDR technology continues to expand the capabilities available to both legitimate users and adversaries, enabling increasingly advanced forms of signal manipulation. As ISAC technology matures, ongoing research will be essential to ensure that these systems remain secure against emerging threats.

Finally, although this work focuses on vulnerabilities, the same principles of controlled signal manipulation can support privacy protection and defensive deception. Techniques such as false-target injection, obfuscation, or controlled replay can be used for anti-surveillance and privacy-preserving ISAC designs, opening new possibilities for secure and resilient ISAC architectures.

References

[1] 3rd Generation Partnership Project (3GPP), "Feasibility Study on Integrated Sensing and Communication," 3GPP, Technical Report TR 22.837, 2024, release 19.

[2] L. G. De Oliveira, B. Nuss, M. B. Alabd, A. Diewald, M. Pauli, and T. Zwick, "Joint Radar-Communication Systems: Modulation Schemes and System Design," *IEEE Trans. Microw. Theory Tech.*, vol. 70, no. 3, pp. 1521–1551, Mar. 2022.

[3] J. A. Zhang, M. L. Rahman, K. Wu, X. Huang, Y. J. Guo, S. Chen, and J. Yuan, "Enabling Joint Communication and Radar Sensing in Mobile Networks—A Survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 306–345, 1st Quart. 2022.

[4] C. R. Berger, B. Demissie, J. Heckenbach, P. Willett, and S. Zhou, "Signal processing for passive radar using OFDM waveforms," *IEEE J. Sel. Topics Signal Process.*, vol. 4, no. 1, pp. 226–238, Feb. 2010.

[5] M. Braun, "OFDM radar algorithms in mobile communication networks," Ph.D. dissertation, Karlsruher Institut für Technologie, 2014.

[6] S. Bartoletti, Z. Liu, M. Z. Win, and A. Conti, "Device-Free Localization of Multiple Targets in Cluttered Environments," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 5, pp. 3906–3923, 2022.

[7] R. Zhang, X. Wu, Y. Lou, F.-G. Yan, Z. Zhou, W. Wu, and C. Yuen, "Channel-Training-Aided Target Sensing for Terahertz Integrated Sensing and Massive MIMO Communications," *IEEE Internet of Things Journal*, vol. 12, no. 4, pp. 3755–3770, 2025.

[8] F. Liu, P. Zhao, and Z. Wang, "EKF-Based Beam Tracking for mmWave MIMO Systems," *IEEE Commun. Lett.*, vol. 23, no. 12, pp. 2390–2393, December 2019.

[9] J. Johnston, L. Venturino, E. Grossi, M. Lops, and X. Wang, "MIMO OFDM Dual-Function Radar-Communication Under Error Rate and Beampattern Constraints," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1951–1964, June 2022.

[10] C. Giovannetti, N. Decarli, S. Bartoletti, R. A. Stirling-Gallacher, and B. M. Masini, "Target Positioning Accuracy of V2X Sidelink Joint Communication and Sensing," *IEEE Wireless Communications Letters*, vol. 13, no. 3, pp. 849–853, 2024.

[11] S. Bartoletti, N. Decarli, B. M. Masini, C. Giovannetti, A. Zanella, A. Bazzi, and R. A. Stirling-Gallacher, "Integration of Sensing and Localization in V2X Sidelink Communications," *IEEE Commun. Mag.*, vol. 62, no. 8, pp. 185–191, 2024.

[12] N. Decarli, S. Bartoletti, A. Bazzi, R. A. Stirling-Gallacher, and B. M. Masini, "Performance Characterization of Joint Communication and Sensing With Beyond 5G NR-V2X Sidelink," *IEEE Trans. Veh. Technol.*, vol. 73, no. 7, pp. 10 044–10 059, 2024.

[13] Y. Cui, F. Liu, X. Jing, and J. Mu, "Integrating Sensing and Communications for Ubiquitous IoT: Applications, Trends, and Challenges," *IEEE Network*, vol. 35, pp. 158–167, November 2021.

[14] T. Guo and H. Li, "Secure integrated sensing and communications (S-ISAC) network," in *2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall)*. IEEE, 2024, pp. 1–6.

[15] O. Günlü, M. R. Bloch, R. F. Schaefer, and A. Yener, "Secure integrated sensing and communication," *IEEE Journal on Selected Areas in Information Theory*, vol. 4, pp. 40–53, 2023.

[16] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1728–1767, 2022.

[17] M. Singh, M. Roeschlin, A. Ranganathan, and S. Capkun, "V-Range: Enabling Secure Ranging in 5G Wireless Networks," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2022.

[18] K. Gao, H. Wang, and H. Lv, "Surgical Strike on 5G Positioning: Selective-PRS-Spoofing Attacks and Its Defence," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 10, pp. 2922–2937, 2024.

[19] H. Yang, S. Bae, M. Son, H. Kim, S. Kim, and Y. Kim, "Hiding in plain signal: Physical signal overshadowing attack on LTE," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 55–72.

[20] S. Bartoletti, I. Palamà, L. Chiaraviglio, S. M. Razavi, Y. Zhao, G. Bianchi, and N. Blefari-Melazzi, "Positioning integrity via uncertainty quantification," *IEEE Trans. Veh. Technol.*, 2024.

[21] H. Calatrava, S. Tang, and P. Closas, "Advances in Anti-Deception Jamming Strategies for Radar Systems: A Survey," *IEEE Aerosp. Electron. Syst. Mag.*, pp. 1–22, 2025.

[22] G. Chrysanidis, Y. Liu, and A. Argyriou, "A Replay Attack Against ISAC Based on OFDM," *IEEE Access*, vol. 12, pp. 20 998–21 003, 2024.

[23] H. C. Yildirim, M. F. Keskin, H. Wymeersch, and F. Horlin, "OFDM-based JCAS under attack: The dual threat of spoofing and jamming in WLAN sensing," *IEEE Internet of Things Journal*, pp. 1–1, 2025.

[24] Z. Feng, C. K. Seow, and Q. Cao, "GNSS Anti-spoofing Detection based on Gaussian Mixture Model Machine Learning," in *2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC)*. IEEE, 2022, pp. 3334–3339.

[25] B. Chettri and B. L. Sturm, "A deeper look at Gaussian mixture model based anti-spoofing systems," in *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2018, pp. 5159–5163.

[26] X. Qiu, T. Jiang, S. Wu, and M. Hayes, "Physical layer authentication enhancement using a Gaussian mixture model," *IEEE Access*, vol. 6, pp. 53 583–53 592, 2018.

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

[28] V. Hamici-Aubert, J. Saint-Martin, R. E. Navas, G. Z. Papadopoulos, G. Doyen, and X. Lagrange, "Leveraging Overshadowing for Time-Delay Attacks in 4G/5G Cellular Networks: An Empirical Assessment," in *Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES 2024)*, 2024.

[29] K. Whitehouse, A. Woo, F. Jiang, J. Polastre, and D. Culler, "Exploiting the capture effect for collision detection and recovery," in *IEEE Workshop on Embedded Networked Sensors (EmNetS-II)*. Sydney, NSW, Australia: IEEE, May 2005, pp. 45–52.

[30] M. Meghdadi, S. Ozdemir, and I. Güler, "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks," *IETE Technical Review*, vol. 28, no. 2, pp. 89–102, 2011.

[31] G. Focarelli, S. Zanini, I. Palamà, G. Bianchi, and S. Bartoletti, "Positioning Security in 5G and Beyond: Model and Detection of Physical Layer Threats," *IEEE Trans. on Wireless Commun.*, vol. 25, pp. 1048–1061, 2026.

[32] V. Krishnamurthy, K. Pattanayak, S. Gogineni, B. Kang, and M. Rangaswamy, "Adversarial Radar Inference: Inverse Tracking, Identifying Cognition, and Designing Smart Interference," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 57, no. 4, pp. 2067–2081, 2021.

[33] S. Zhang, Y. Zhou, L. Zhang, Q. Zhang, and L. Du, "Target Detection for Multistatic Radar in the Presence of Deception Jamming," *IEEE Sensors J.*, vol. 21, no. 6, pp. 8130–8141, 2021.

[34] S. Zhao, L. Zhang, Y. Zhou, N. Liu, and J. Liu, "Discrimination of active false targets in multistatic radar using spatial scattering properties," *IET Radar, Sonar & Navigation*, vol. 10, no. 5, pp. 817–826, 2016.

[35] Martins, Óscar G. and Åkesson, Henrik and Gomes, Marco and Osorio, Diana P. M. and Sen, Padmanava and Vilela, João P., "Delving Into Security and Privacy of Joint Communication and Sensing: A Survey," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 4978–5004, 2025.

[36] T. Matsumine, H. Ochiai, and J. Shikata, "Physical Layer Security for Integrated Sensing and Communication: A Survey," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 6690–6743, 2025.

[37] W. Aman, E.-M. Illi, M. Qaraqe, and S. Al-Kuwari, "Integrating Communication, Sensing, and Security: Progress and Prospects of PLS in ISAC Systems," *arXiv preprint arXiv:2505.05090*, 2025.

[38] U. Ali, N. B. Melazzi, and S. Bartoletti, "Cooperative ISAC under spoofing attacks," *IEEE Wireless Commun. Lett.*, vol. 14, no. 9, pp. 2683–2687, 2025.

[39] G. Focarelli, S. Zanini, I. Palamà, A. Rivitti, S. Bartoletti, and G. Bianchi, "WIP: Parrots in the Air: Experimental Validation of Full-Frame Meaconing in 5G Systems," in *2025 IEEE 26th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2025, pp. 118–121.

[40] I. Palamà, G. Focarelli, S. Zanini, G. Bianchi, and S. Bartoletti, "Blind deception in ISAC via Full-Frame OFDM replay," in *Proc. of the ACM Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*, ser. WiNTECH '25, 2025, p. 25–32.

[41] S. K. Dehkordi, L. Pucci, P. Jung, A. Giorgetti, E. Paolini, and G. Caire, "Multistatic Parameter Estimation in the Near/Far Field for Integrated Sensing and Communication," *IEEE Trans. Wireless Commun.*, vol. 23, no. 12, pp. 17 929–17 944, 2024.

[42] M. Manzoni, D. Tagliaferri, S. Tebaldini, M. Mizmizi, A. V. Monti-Guarnieri, C. M. Prati, and U. Spagnolini, "Wavefield Networked Sensing: Principles, Algorithms, and Applications," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 181–197, 2025.

[43] E. Favarelli, E. Matricardi, L. Pucci, W. Xu, E. Paolini, and A. Giorgetti, "Sensor fusion and resource management in MIMO-OFDM joint sensing and communication," *IEEE Trans. Veh. Technol.*, pp. 1–16, 2025.

[44] L. Pucci, E. Paolini, and A. Giorgetti, "System-Level Analysis of Joint Sensing and Communication Based on 5G New Radio," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 7, pp. 2043–2055, 2022.

[45] L. Pucci, E. Matricardi, E. Paolini, W. Xu, and A. Giorgetti, "Performance Analysis of a Bistatic Joint Sensing and Communication System," in *2022 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2022, pp. 73–78.

[46] B. Carlson, E. Evans, and S. Wilson, "Search radar detection and track with the Hough transform. I. system concept," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 30, no. 1, pp. 102–108, 1994.

[47] ——, "Search radar detection and track with the Hough transform. II. Detection statistics," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 30, no. 1, pp. 109–115, 1994.

[48] B. D. Carlson, E. D. Evans, and S. L. Wilson, "Search radar detection and track with the Hough transform. III. Detection performance with binary integration," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 30, no. 1, pp. 116–125, 1994.

[49] S. Bartoletti, A. Conti, W. Dai, and M. Z. Win, "Threshold Profiling for Wideband Ranging," *IEEE Signal Process. Lett.*, vol. 25, no. 6, pp. 873–877, 2018.

[50] R. Zhang, L. Cheng, S. Wang, Y. Lou, Y. Gao, W. Wu, and D. W. K. Ng, "Integrated Sensing and Communication with Massive MIMO: A Unified Tensor Approach for Channel and Target Parameter Estimation," *IEEE Trans. Wireless Commun.*, vol. 23, no. 8, pp. 8571–8587, January 2024.

[51] J.-H. Park, Y.-J. Yoon, W. Cho, D. Ham, and S.-C. Kim, "Intercarrier interference mitigation for communication compatible OFDM radar," *IEEE Trans. Veh. Technol.*, vol. 73, no. 4, pp. 5930–5934, 2024.

[52] M. Aaron and D. Tufts, "Intersymbol interference and error probability," *IEEE Trans. Inf. Theory*, vol. 12, no. 1, pp. 26–34, 2003.

[53] A. F. Molisch, M. Toeltsch, and S. Vermani, "Iterative Methods for Cancellation of Intercarrier Interference in OFDM Systems," *IEEE Trans. Veh. Technol.*, vol. 56, no. 4, pp. 2158–2167, 2007.

[54] D. Xue, J. Wei, Y. Li, T. Zeng, "5G-based Link-level Integrated Sensing and Communication Simulator," 2025. [Online]. Available: https://github.com/xds0112/5G_based_Link_level_Integrated_Sensing_and_Communication_Simulator?tab=readme-ov-file

[55] Hewlett Packard Enterprise, "Athonet Mobile Core," 2025. [Online]. Available: https://www.hpe.com/psnow/doc/PSN1014769364ITIT.pdf

[56] Amarisoft, "LTE Software eNodeB and NR Software gNB," https://tech-academy.amarisoft.com/lteenb.doc.
[57] 3rd Generation Partnership Project, "Service requirements for integrated sensing and communication," 3GPP, Tech. Rep. 3GPP TS 22.137 V19.1.0, March 2024.
[58] Ettus Research, National Instruments, "USRP X310," https://www.ettus.com/all-products/x310-kit/.
[59] Aaronia AG, "OmniLOG® 70600," 2025. [Online]. Available: https://aaronia.com/en/omnidirectional-antenna-6ghz
[60] Ettus Research, National Instruments, "USRP X410," https://www.ettus.com/all-products/usrp-x410/.
[61] Aaronia AG, "HyperLOG® 6080," 2025. [Online]. Available: https://aaronia.com/en/log-per-antenne-hyperlog6080
[62] Keysight, "N9021B MXA Signal Analyzer, 10 Hz to 50 GHz," 2025. [Online]. Available: https://www.keysight.com/us/en/product/N9021B/n9021b-mxa-signal-analyzer-multi-touch-10-hz-50-ghz.html