Sensing-Secure ISAC: Ambiguity Function Engineering for Impairing Unauthorized Sensing

Kawon Han, *Member, IEEE,* Kaitao Meng, *Member, IEEE,* and Christos Masouros, *Fellow, IEEE*

***Abstract*—The deployment of integrated sensing and communication (ISAC) in wireless networks brings along unprecedented vulnerabilities to authorized passive sensing, necessitating the development of secure sensing solutions. Unlike traditional wireless communication, where data security can be enhanced through data encryption, sensing security is more challenging to achieve. This is because sensing parameters are embedded within the target-reflected signal leaked to unauthorized passive radar sensing eavesdroppers (Eve), implying that they can silently extract sensory information without prior knowledge of the information data. To overcome this limitation, we propose a novel sensing-secure ISAC framework that ensures secure target detection and estimation for the legitimate system, while obfuscating unauthorized sensing without requiring any prior knowledge of Eve. Specifically, by introducing artificial imperfections into the ambiguity function (AF) of ISAC signals, we introduce artificial ghost targets into Eve's range profile which increase its range estimation ambiguity. In contrast, the legitimate sensing receiver (Alice) can suppress these AF artifacts using mismatched filtering, albeit at the expense of signal-to-noise ratio (SNR) loss. Specifically, employing an OFDM signal, a structured subcarrier power allocation scheme is designed to shape the secure autocorrelation function (ACF), inserting periodic peaks to mislead Eve's range estimation and degrade target detection performance. To quantify the sensing security level, we introduce peak sidelobe level (PSL) and integrated sidelobe level (ISL) as key performance metrics. Additionally, we analyze the three-way trade-offs between communication, legitimate sensing, and sensing security, highlighting the impact of the proposed sensing-secure ISAC signaling on system performance. Furthermore, we formulate a convex optimization problem to maximize ISAC performance while guaranteeing a certain sensing security level. Numerical results validate the effectiveness of the proposed sensing-secure ISAC signaling, demonstrating its ability to degrade Eve's target estimation while preserving Alice's performance.**

***Index Terms*—Ambiguity function (AF), integrated sensing and communication (ISAC), passive radar, physical layer security (PLS), sensing eavesdropper**

I. Introduction

Integrated Sensing and Communication (ISAC) has emerged as a promising paradigm for next-generation wireless networks, enabling dual-functional wireless communication and radar sensing within a unified system. By sharing spectrum and hardware resources, ISAC enhances spectral efficiency and reduces system costs, making it a key enabler for applications such as autonomous driving, smart cities, and industrial automation [1]–[3]. The ultimate goal of deploying ISAC in cellular networks is to provide coordinated sensing services at an unprecedented scale, offering opportunities to make future wireless networks more connected and sustainable [4]–[7].

However, integrating sensing into communication networks introduces new vulnerabilities, particularly in *sensing security*, where third parties may exploit the sensing functionality to gain knowledge of targets and environments, potentially exposing private information. Such unauthorized access could result in unauthorized tracking or identification [8], potentially leading to misuse by an adversary. Specifically, ISAC systems deployed for human sensing may leak personal information to a sensing eavesdropper (Eve), such as vital signs [9], speech [10], and hand gestures [11], posing a significant risk of privacy disclosure.

In previous generations of wireless networks, such threats were rarely considered, as these networks primarily focused on providing data communication services [12], with sensing functionality not being a point of concern. Consequently, physical layer security (PLS) techniques for wireless networks have primarily focused on protecting data security from eavesdropping [13]. Additionally, communication security can be ensured through data encryption at the upper layers [14]. Following this direction, PLS techniques in ISAC have also primarily focused on communication security, designing ISAC systems to balance the performance trade-offs between sensing, communication, and communication secrecy rate [15], [16]. Moreover, the radar sensing functionality in ISAC is utilized to assist communication PLS by providing information about potential Eve [17], [18].

Unlike conventional communication security, securing the sensing functionality in ISAC is more challenging, as unauthorized passive eavesdroppers can exploit transmitted ISAC signals to infer target information without actively engaging in the system. Furthermore, there is no data link to encrypt for sensing security, as passive radar Eve can utilize ISAC signals of opportunity as both reference and surveillance signals. Thus, achieving sensing security inevitably requires physical layer techniques that deceive Eve through obfuscating the target sensing channel [19].

A. Related Works

Sensing security in ISAC remains an underexplored research area, despite its critical importance in safeguarding privacy and preventing unauthorized surveillance. In response to these demands, a few studies on secure wireless sensing based on channel state information (CSI) have been presented recently. The works in [20]–[23] utilize additional hardware to modify

Manuscript received xx, 2025. K. Han, K. Meng, and C. Masouros are with the Department of Electronic and Electrical Engineering, University College London, London, UK (emails: kawon.han, kaitao.meng, c.masouros@ucl.ac.uk).

the physical environment, thereby imposing artificial channels on Eve. In [20], rotating fans and antennas are employed to alter the physical wireless propagation channel. Meanwhile, the studies in [21], [22] introduce reconfigurable intelligent surfaces (RIS) to generate artificial signal reflections in Eve's received signals. Similarly, RF-Protect in [23] creates ghost targets to Eve by deploying reflectors near targets. However, these approaches may be overly complex due to additional hardware requirements and may significantly impact legitimate sensing performance.

Instead of physical channel control, randomized transmission techniques have recently been considered in [24], [25] to protect WiFi-based sensing. The work in [24] proposed a randomly scheduled transmission scheme using multiple antennas, which is highly resilient to Eve while still enabling legitimate sensing. However, this method requires multiple independent streams to be transmitted from different antennas, which can significantly degrade both legitimate sensing and communication performance. Similarly, the randomized beamforming approach in [25] aims to confuse Eve in estimating the target channel. However, it has an inherent limitation, as it does not take legitimate sensing performance into account.

Alternatively, pilot modifications to obfuscate Eve's channel estimation have been proposed in [26]–[28]. They apply secret scrambled functions to pilot symbols, allowing only the legitimate sensing receiver, which possesses the secret code, to extract the true CSI related to targets. Similar approaches have been extended to multi-antenna systems, including controlling the phase difference between transmitting antennas [29] and spatial-temporal source-defined channel encryption [30], [31]. The objective of this CSI obfuscation is to prevent Eve from estimating target-related CSI variations, as Eve typically leverages long training sequences (LTS) to estimate CSI in WiFi-based sensing. However, it is important to note that these pilot modification techniques may be circumvented by an unauthorized passive radar eavesdropper, which performs radar sensing based on a reference signal received directly from the transmitter [32]. This implies that Eve can still estimate target channels using the modified pilots as a reference signal, without relying on prior known LTS, thereby bypassing the CSI obfuscation intentionally designed by the transmitter.

Unlike CSI-based sensing, a major focus in ISAC research is to facilitate radar sensing using communication data signals [33], [34], which is highly vulnerable to attacks from passive sensing Eve. In this regard, secure-sensing ISAC designs have been explored in [35]–[37]. These studies address sensing security by optimizing the detection probability in a cell-free ISAC system [35] or minimizing the Cramér-Rao bound (CRB) of legitimate sensing [36], while simultaneously keeping Eve's detection probability low. Additionally, by incorporating radar mutual information, ISAC signaling designs that maximize legitimate sensing performance have been proposed in [37], subject to constraints on Eve's performance and communication quality-of-service (QoS). However, these initial works have a fundamental limitation: they require Eve's CSI at the legitimate ISAC transmitter. This assumption may not be entirely realistic, as a passive radar eavesdropper remains silent and does not reveal its location.

B. Motivations and Contributions

In summary of related works, securing the sensing functionality in ISAC from attacks by passive sensing Eve remains largely underexplored in three key aspects of a passive radar system: 1) There is no data link to encrypt for sensing security. 2) Eve exploits the ISAC transmitter (TX) signal as both the reference and surveillance signals to detect and estimate targets. 3) It is challenging to utilize Eve's CSI for designing secure-sensing ISAC signaling. Motivated by these fundamental challenges, we aim to develop a comprehensive Eve-agnostic sensing-secure ISAC framework that not only addresses these issues but also provides a theoretical analysis of the three-way trade-offs among communication, legitimate sensing, and sensing security.

In this paper, we present a novel sensing-secure ISAC framework that leverages *ambiguity function (AF) shaping* to enhance sensing security against sensing Eve. The main idea stems from the fact that radar sensing performance is fundamentally characterized by the AF of the transmitted signal, which provides a means to control the performance of an unknown Eve. Furthermore, the knowledge gap of the ISAC TX signal between the legitimate sensing receiver (Alice) and Eve introduces a degree of freedom (DoF) in Alice's receiver design, allowing it to employ mismatched filtering to mitigate the AF sidelobes. Consequently, judiciously shaping the AF enables the protection of sensing functionality in ISAC while inherently compromising sensing and communication (S&C) performance, leading to the three-way trade-offs among communication, legitimate sensing, and sensing security. The main contributions of this paper are summarized as follows:

- We propose an AF engineering framework for ISAC signals to achieve sensing security. By introducing artificial targets into Eve's range profile, we mislead its sensing while allowing the legitimate sensing receiver to eliminate them using mismatched filtering, albeit at the cost of SNR loss. To achieve this, we design a structured subcarrier power allocation scheme in OFDM that shapes the autocorrelation function (ACF), introducing periodic peaks to degrade Eve's range estimation and target detection performance.
- We establish key performance metrics for sensing security and legitimate sensing. Specifically, we quantify sensing security using peak sidelobe level (PSL) and integrated sidelobe level (ISL), while measuring legitimate sensing performance using SNR loss caused by reciprocal filtering (RF). Under these metrics, we theoretically derive the impact of AF shaping on each performance aspect and provide comprehensive insights into the performance gap between Alice and Eve.
- Building on the theoretical foundation of AF shaping, we investigate the three-way trade-offs among communication, legitimate sensing, and sensing security, revealing how AF shaping influences ISAC system performance. Additionally, we formulate and solve an optimization problem to achieve a flexible balance between S&C performance while ensuring a guaranteed sensing security level, thereby enabling sensing-secure ISAC signaling.

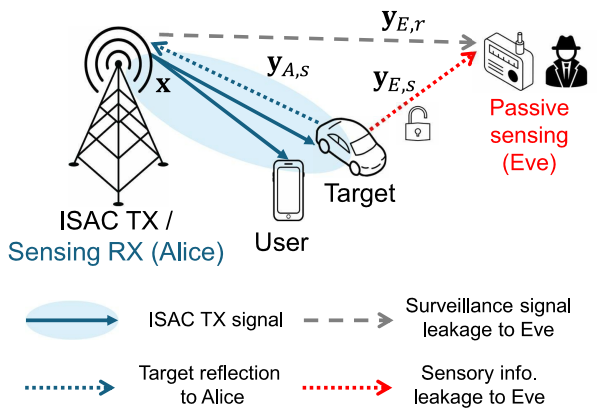


Fig. 1. Sensing-secure ISAC system to an unauthorized passive sensing eavesdropper. The leakage and target reflection to Eve cannot be controlled by the ISAC TX.

Notations: Boldface variables with lower- and upper-case symbols represent vectors and matrices, respectively. $\mathbf{A} \in \mathbb{C}^{N\times M}$ and $\mathbf{B} \in \mathbb{R}^{N\times M}$ denotes a complex-valued $N \times M$ matrix $\mathbf{A}$ and a real-valued $N \times M$ matrix $\mathbf{B}$, respectively. Also, $\mathbf{0}_N$, $\mathbf{1}_N$ and $\mathbf{I}_N$ denote an $N \times 1$ column vector of zeros, an $N \times 1$ column vector of ones, and a $N \times N$ identity matrix, respectively. $(\cdot)^T$, $(\cdot)^H$, and $(\cdot)^*$ represent the transpose, Hermitian transpose, and conjugate operators, respectively. diag($\mathbf{a}$) denotes a diagonal matrix with diagonal entries of a vector $\mathbf{a}$. The operators $\odot$ and $\oslash$ represent the Hadamard (element-wise) product and the element-wise division, respectively. $\mathbb{E}[\cdot]$ is the statistical expectation operator.

II. System Model

The proposed framework aims to develop a secure sensing ISAC system that prevents an unknown sensing eavesdropper (Eve) from detecting and estimating true targets by exploiting ISAC signals as signals of opportunity, as illustrated in Fig. 1. We consider a single-antenna ISAC transmitter (TX) that transmits an orthogonal frequency division multiplexing (OFDM) signal. The legitimate sensing receiver (RX) (Alice) can either be collocated with the ISAC TX for monostatic sensing, as depicted in Fig. 1, or be spatially separated from the TX for bistatic sensing. For both monostatic and bistatic sensing configuration, the legitimate sensing RX is assumed to have prior knowledge of the ISAC TX signal to demodulate the sensing channel. Throughout this paper, we impose the following assumptions on the sensing Eve:

- **(A.1)** The sensing Eve operates as a passive radar system equipped with a large number of receiving antennas or separately deployed directional antennas [38], enabling perfect separation of a reference surveillance signal from the target echo signal.
- **(A.2)** The sensing Eve is aware of the location of the ISAC TX, including its range and angle with respect to Eve's position.
- **(A.3)** The sensing Eve does not have prior knowledge of the ISAC TX signal, as it is randomized by communication data.
- **(A.4)** The sensing Eve has no prior range-Doppler information of the targets.
- **(A.5)** The ISAC TX has no information regarding the sensing Eve, including Eve's location.

The assumptions **(A.1)**-**(A.5)** are realistic in practical scenarios where the sensing Eve remains silent and unknown to the ISAC TX, posing a potential threat to ISAC sensing security. Notably, it should be emphasized that prior knowledge of Eve's channel is not required in the proposed framework to ensure ISAC sensing security. This aligns with the worst-case security assumption, where the legitimate ISAC system operates without any prior information on Eve's location.

A. Transmit Signal Model

The ISAC TX signal, utilizing N OFDM subcarriers, is modulated with random communication symbols drawn from the constellation set $\mathbb{S}$, which is expressed as $\mathbf{s} = [s_1, s_2, \ldots, s_N]^T$, where $s_n \in \mathcal{S}, \forall n = 1, 2, \ldots, N$. Without loss of generality, we assume that the constellations have zero-mean and unit-variance as $\mathbb{E}\left[|s_n|^2\right] = 1, \forall s_n \in \mathcal{S}$, of which statistical properties are defined as follows:

$$\mathbb{E}\left[|s_n|^4\right] = \mu_4, \quad \mathbb{E}\left[|s_n|^{-2}\right] = \nu_{-2}, \quad \forall s_n \in \mathcal{S}, \tag{1}$$

where μ_4 is the fourth moment of the constellation known as the kurtosis [33], and ν_{-2} is the inverse second moment of the constellation [38]. For a general M-QAM constellation, they can be obtained by $\mu_4 = \frac{1}{M}\sum_{m=1}^{M}|s_m|^4$ and $\nu_{-2} = \frac{1}{M}\sum_{m=1}^{M}|s_m|^{-2}$, respectively.

Furthermore, the power allocation of each individual subcarrier is embedded in the matrix $\mathbf{W}$, given by $\mathbf{W} = \text{diag}(\mathbf{w})$, where $\mathbf{w} = [w_1, w_2, \ldots, w_N]^T$ and w_n denotes the power coefficient assigned to subcarrier n. Accordingly, the frequency-domain representation of the ISAC TX signal is given by

$$\mathbf{x} = \mathbf{W}\mathbf{s}. \tag{2}$$

The total transmit signal power per OFDM symbol encapsulated in $\mathbf{W}$ is normalized to the unit-power, such that

$$\text{Tr}\left(\mathbf{W}\mathbf{W}^H\right) = N. \tag{3}$$

Taking the cyclic prefix (CP) into account, the CP-OFDM signal with a CP length of N_{cp} can be expressed in the frequency domain as $\mathbf{x}_{\text{cp}} = [\mathbf{x}^T, \mathbf{0}_{N_{\text{cp}}}^T]^T \in \mathbb{C}^{(N+N_{\text{cp}})\times 1}$. Since the CP is removed during receiver processing to mitigate inter-symbol interference (ISI) [39], it is omitted hereafter for clarity in the formulation. In cases where the target delay exceeds the CP length, the useful signal power is reduced and ISI-induced interference arises, thereby degrading the sensing performance of CP-OFDM systems [40]. Hence, in this work we assume that the delays of all targets-of-interest lie within the ISI-free region determined by the CP length, expressed as $R_{\text{max,cp}} = \frac{cN_{\text{cp}}}{2B}$, where B denotes the OFDM signal bandwidth.

This unified ISAC signal is utilized for both communication and sensing. It is received by a communication user and is also reflected by targets, returning to both the legitimate sensing receiver and the sensing eavesdropper. Notably, the formulated ISAC signal in (2) introduces a trade-off between

S&C performance. Specifically, the communication rate of the typical user and the range sidelobe level for sensing are influenced by the allocated subcarrier power $w_1, w_2, \ldots, w_N$. In the proposed framework for sensing security, our objective is to design ISAC signaling that optimally balances the three-way trade-offs between communication, sensing, and sensing security by carefully controlling the radar ambiguity through the power allocation across subcarriers.

B. Communication System Model

Let $\mathbf{y}_c$ denote the received signal at the typical communication user. After removing the CP, the frequency-domain representation of the received signal is given by

$$\mathbf{y}_c = \mathbf{H}_c\mathbf{W}\mathbf{s} + \mathbf{z}_c, \tag{4}$$

where $\mathbf{H}_c$ is a diagonal matrix representing the communication channel, given by $\mathbf{H}_c = \text{diag}(h_1, h_2, \ldots, h_N)$ with each entry h_i representing the channel gain of the i^{th} subcarrier. The term $\mathbf{z}_c$ represents additive white Gaussian noise (AWGN), modeled as $\mathbf{z}_c \sim \mathcal{CN}(0, \sigma_c^2\mathbf{I}_N)$. Here, we consider a frequency-selective fading channel. However, each subband is assumed to be sufficiently narrow, such that the subband signals modulated on each subcarrier experience flat fading. Additionally, the fading characteristics of the channel remain constant over the duration of single transmission frame. Based on this model, the achievable communication rate at the typical user is given by

$$R_c = \frac{B}{N}\sum_{i=1}^{N}\log_2\left(1 + \frac{|h_i|^2|w_i|^2}{\sigma_c^2}\right), \tag{5}$$

where B is the total bandwidth of the OFDM signal. We adopt the achievable rate as the communication performance metric for ISAC signaling design, which is determined by the SNR of each subcarrier and, in turn, depends on the subcarrier power allocation.

C. Sensing System Model: Legitimate Sensing Receiver (Alice)

Given that $U = U_t + U_c$ radar reflections from U_t targets and U_c clutter sources are located at different ranges, the received signal at the legitimate sensing receiver can be generally modeled as

$$\begin{aligned}\mathbf{y}_{A,s} &= \left(\sum_{i=1}^{U_t}\beta_{A,i}^{(t)}\mathbf{r}\left(\tau_{A,i}^{(t)}\right) + \sum_{j=1}^{U_c}\beta_{A,j}^{(c)}\mathbf{r}\left(\tau_{A,j}^{(c)}\right)\right)\odot\mathbf{x} + \mathbf{z}_{A,s},\\ &= \mathbf{h}_{A,s}\odot\mathbf{W}\mathbf{s} + \mathbf{z}_{A,s}.\end{aligned} \tag{6}$$

Here, $\beta_{A,i}^{(t)}$ denotes the complex amplitude that accounts for both the path loss and the radar cross-section (RCS) of target i, while $\tau_{A,i}^{(t)}$ represents the time-of-flight (TOF) from the ISAC transmitter to target i and back to Alice. Similarly, $\beta_{A,j}^{(c)}$ and $\tau_{A,j}^{(c)}$ denote the complex amplitude and TOF associated with clutter sources, respectively. The range steering vector is given as $\mathbf{r}(\tau) = \left[1, e^{-j2\pi\Delta f\tau}, \cdots, e^{-j2\pi(N-1)\Delta f\tau}\right]^T \in \mathbb{C}^{N\times 1}$ with the subcarrier spacing $\Delta f = B/N$. Thus, the radar channel vector of Alice $\mathbf{h}_{A,s}$ is given by $\mathbf{h}_{A,s} = \left(\sum_{i=1}^{U_t}\beta_{A,i}^{(t)}\mathbf{r}\left(\tau_{A,i}^{(t)}\right) + \sum_{j=1}^{U_c}\beta_{A,j}^{(c)}\mathbf{r}\left(\tau_{A,j}^{(c)}\right)\right)$. The term $\mathbf{z}_{A,s}$ represents the AWGN of the sensing receiver, following $\mathbf{z}_{A,s} \sim \mathcal{CN}(0, \sigma_A^2\mathbf{I}_N)$. We assume static or slowly moving targets, such that range migration and inter-carrier interference (ICI) effects are negligible. These effects, if present, would otherwise increase the overall sidelobe levels [41], [42].

As a preliminary step to target detection and parameter estimation, we consider two types of radar receiver processing: matched filtering (MF) and reciprocal filtering (RF). The MF is well known as the optimal linear receiver filter in terms of maximizing the signal-to-noise ratio (SNR) at the target coordinates, without considering sidelobe effects. In contrast, RF is a form of mismatched filtering (MMF) that can be designed to reduce sidelobe levels at the expense of decreased SNR for the targets [43].

1) Matched filtering at Alice: Let $\mathbf{g}_{A,MF}$ denote the frequency-domain MF of Alice, which is expressed as $\mathbf{g}_{A,MF} = \mathbf{x}^*$. Then, the output of the MF in the frequency-domain is given by

$$\begin{aligned}\mathbf{h}_{A,MF} &= \mathbf{y}_{A,s}\odot\mathbf{g}_{A,MF}\\ &= \mathbf{W}^2\mathbf{S}^2\mathbf{h}_{A,s} + \mathbf{z}_{A,s}\odot\mathbf{x}^*,\end{aligned} \tag{7}$$

where $\mathbf{S} = \text{diag}(\mathbf{s})$. From the MF output, the range profile is obtained by performing inverse discrete Fourier transform (IDFT) over (7). Let us define $\mathbf{F}_N$ as the normalized DFT matrix of size N. Then, the range profile $\mathbf{\Gamma}_{A,MF}$ is expressed as

$$\mathbf{\Gamma}_{A,MF} = \mathbf{F}_N^H\mathbf{W}^2\mathbf{S}^2\mathbf{h}_{A,s} + \tilde{\mathbf{z}}_{A,MF,s}, \tag{8}$$

where $\tilde{\mathbf{z}}_{A,MF,s}$ follows the noise statistics as $\tilde{\mathbf{z}}_{A,MF,s} \sim \mathcal{CN}(0, \sigma_A^2\mathbf{I}_N)$.

2) Reciprocal filtering at Alice: Let $\mathbf{g}_{A,RF}$ denote the frequency-domain RF of Alice, which is expressed as $\mathbf{g}_{A,RF} = \mathbf{1}_N \oslash \mathbf{x}$. The output of the RF in the frequency-domain is given by

$$\begin{aligned}\mathbf{h}_{A,RF} &= \mathbf{y}_{A,s}\odot\mathbf{g}_{A,RF}\\ &= \mathbf{h}_{A,s} + \mathbf{z}_{A,s}\oslash\mathbf{x}.\end{aligned} \tag{9}$$

Performing IDFT over the RF output, the range profile with the RF can be obtained as

$$\mathbf{\Gamma}_{A,RF} = \mathbf{F}_N^H\mathbf{h}_{A,s} + \tilde{\mathbf{z}}_{A,RF,s}, \tag{10}$$

where $\tilde{\mathbf{z}}_{A,RF,s} \sim \mathcal{CN}(0, \frac{1}{N}\sum_{n=1}^{N}|w_n|^{-2}\nu_{-2}\sigma_A^2\mathbf{I}_N)$.

Remark 1: Inspired by the characteristics of these receivers, we aim to design the ISAC signaling to enhance sensing security while ensuring favorable sensing performance at the legitimate sensing receiver. The key idea for the legitimate sensing receiver is to exploit the RF for mitigating the undesired sidelobes caused by the design of the secure ISAC signal. However, the use of the RF in lieu of MF at Alice inherently causes the degradation on the output SNR. Importantly, this introduces the trade-off between the legitimate sensing performance and the sensing security, of which metrics are detailed in Section III-B and III-C.

D. Sensing System Model: Sensing Eavesdropper (Eve)

The sensing eavesdropper, which is a passive bistatic sensing receiver without prior knowledge of the ISAC TX signals, requires a reference signal to demodulate the surveillance signal from targets. Based on assumption (**A.1**), we model the surveillance signal and the reference signal separately. Similar to (6), the received signal at Eve, reflected from $U = U_t + U_c$ sources including multiple targets and clutter, is given by

$$\begin{aligned}\mathbf{y}_{E,s} &= \left(\sum_{i=1}^{U_t}\beta_{E,i}^{(t)}\mathbf{r}\left(\tau_{E,i}^{(t)}\right) + \sum_{j=1}^{U_c}\beta_{E,j}^{(c)}\mathbf{r}\left(\tau_{E,j}^{(c)}\right)\right)\odot\mathbf{x} + \mathbf{z}_{E,s} \\ &= \mathbf{h}_{E,s}\odot\mathbf{W}\mathbf{s} + \mathbf{z}_{E,s},\end{aligned} \tag{11}$$

where $\beta_{E,i}^{(t)}$ and $\beta_{E,j}^{(c)}$ are the complex amplitudes of targets and clutter sources, respectively, and $\tau_{E,i}^{(t)}$ and $\tau_{E,j}^{(c)}$ are the TOFs from the ISAC TX to reflection source and then to Eve. The term $\mathbf{z}_{E,s}$ represents the AWGN at Eve's receiver, following $\mathbf{z}_{E,s} \sim \mathcal{CN}(0, \sigma_E^2\mathbf{I}_N)$.

The reference signal at Eve, which is leaked from the ISAC TX through the surveillance link in Fig. 1, is modeled as

$$\mathbf{y}_{E,r} = \mathbf{h}_{E,r}\odot\mathbf{x} + \mathbf{z}_{E,r}. \tag{12}$$

Here, we assume that Eve's channel $\mathbf{h}_{E,r}$ follows the Rician channel model, given by [44]

$$\mathbf{h}_{E,r} = \sqrt{\frac{g_{E,r}K}{K+1}}\mathbf{h}_{E,LoS} + \sqrt{\frac{g_{E,r}}{K+1}}\mathbf{h}_{E,NLoS}, \tag{13}$$

where $\mathbf{h}_{E,LoS}$ represents the line-of-sight (LoS) component with a normalized channel gain, and $\mathbf{h}_{E,NLoS}$ represents the non-line-of-sight (NLoS) component, which follows a complex Gaussian distribution with zero mean and unit variance. The term $g_{E,r}$ denotes Eve's channel gain, while K determines the relative power between the LoS and NLoS components. Additionally, assumption (**A.2**) allows Eve to have prior knowledge of $\mathbf{h}_{E,LoS}$. By substituting (13) into (12) and removing $\mathbf{h}_{E,LoS}$, the reference signal at Eve can be rewritten as

$$\tilde{\mathbf{y}}_{E,r} = \sqrt{\frac{g_{E,r}K}{K+1}}\mathbf{x} + \sqrt{\frac{g_{E,r}}{K+1}}\tilde{\mathbf{h}}_{E,NLoS}\odot\mathbf{x} + \tilde{\mathbf{z}}_{E,r}, \tag{14}$$

where $\tilde{\mathbf{h}}_{E,NLoS} = \mathbf{h}_{E,NLoS}\odot\mathbf{h}_{E,LoS}^*$ and $\tilde{\mathbf{z}}_{E,r}$ share the same statistical properties as $\mathbf{h}_{E,NLoS}$ and $\mathbf{z}_{E,r}$, respectively.

Remark 2: Importantly, unlike the legitimate sensing receiver, Eve must exploit the reference signal (14) to estimate the sensing channel [45]. However, this reference signal is affected by receiver noise as well as multi-path reflection components, which degrade the signal-to-interference-plus-noise ratio (SINR) [46]. Accordingly, performing RF at Eve is unfavorable, as it further degrades the target SNR, leading to poor target detection and estimation performance. Fig. 2 emphasizes the output SNR gap between MF and RF at Eve along the reference signal SINR. Thus, to avoid severe SNR degradation, Eve leverages MF to extract the sensing channel from the surveillance signal. Additionally, performing mismatched filtering at the sensing receiver requires full knowledge of the transmitted signal, which prevents Eve from employing advanced receiver processing without access to this information in practice. In summary, Table I outlines the operational differences between Alice and Eve that are leveraged in the design of sensing-secure ISAC signaling.

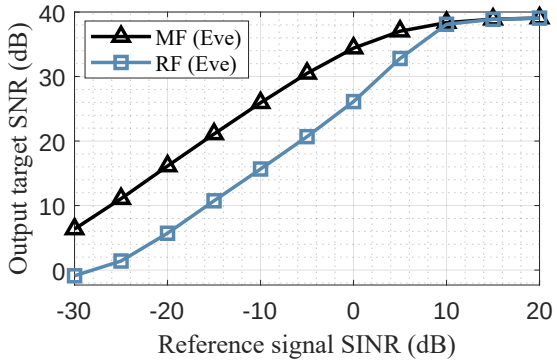


Fig. 2. The target SNR at the filter output vs. Eve's reference signal SINR with QPSK constellation and equally-allocated subcarrier power. The input target SNR is 0 dB, and 32 OFDM symbols with $N = 256$ are coherently processed, yielding 39 dB of the processing gain for a static target.

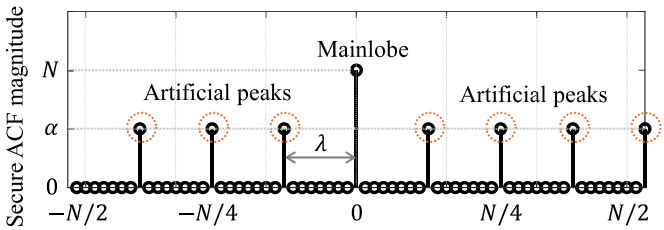
Table I
OPERATIONAL DIFFERENCES BETWEEN ALICE AND EVE UTILIZED FOR ISAC SENSING SECURITY

	Sensing mode	TX signal knowledge	Receiver processing	Resulting effects
Legitimate Sensing (Alice)	Monostatic or bistatic (Active)	Fully-known	Reciprocal filtering	SNR loss
Eavesdropper (Eve)	Bistatic (Passive)	Unknown	Matched filtering	Sidelobes

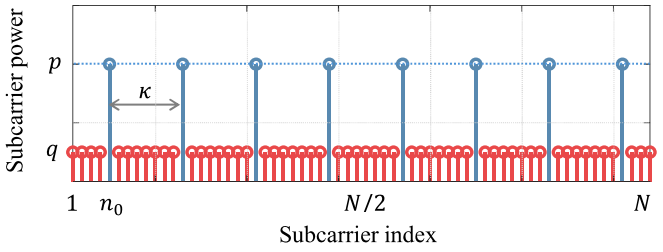
For the MF at Eve, let us denote $\mathbf{g}_{E,MF} = \tilde{\mathbf{y}}_{E,r}^*$ as the frequency-domain MF of Eve. The MF output is given by

$$\begin{aligned}\mathbf{h}_{E,MF} =& \sqrt{\frac{g_{E,r}K}{K+1}}\mathbf{W}^2\mathbf{S}^2\mathbf{h}_{E,s} + \sqrt{\frac{g_{E,r}}{K+1}}\mathbf{W}^2\mathbf{S}^2\mathbf{h}_{E,s}\odot\tilde{\mathbf{h}}_{E,NLoS}^* \\ &+ \mathbf{y}_{E,s}\odot\tilde{\mathbf{z}}_{E,r}^* + \mathbf{z}_{E,s}\odot\mathbf{y}_{E,r}^*.\end{aligned} \tag{15}$$

In (15), it is readily observed that the MF output at Eve consists of the radar channel and additive noise terms, which are determined by the SINR of the reference signal and the noise characteristics of Eve's receiver. Since these additive noise components cannot be controlled by the ISAC TX, securing the sensing functionality must instead rely on the ambiguity function (AF) of the ISAC signal, which directly impacts Eve's MF output. For the MF receiver, a high peak sidelobe level (PSL) and integrated sidelobe level (ISL) in the AF increase the risk of false detections, requiring the radar system to use higher detection thresholds to maintain acceptable false alarm rates. Moreover, elevated ISL degrades the accuracy of parameter estimation in multi-target scenarios [47], [48]. In the context of sensing security, where Eve is constrained to matched filtering due to limited knowledge of the transmitted signal, high PSL and ISL values significantly hinder both detection and estimation performance. Based on this observation, we develop a framework for sensing-secure



(a)



(b)

Fig. 3. (a) The secure ACF with artificial peaks to achieve secure sensing in ISAC, and (b) the subcarrier power allocation scheme corresponding to the secure ACF.

ISAC signaling by controlling the radar sensing ambiguity, as detailed in the following sections.

III. Ambiguity Function Engineering for Sensing Security in ISAC: Artificial Target Generation

Our key idea for achieving secure sensing in ISAC is to generate artificial targets for the unknown sensing eavesdropper while allowing the legitimate sensing receiver to eliminate them using the RF based on the known ISAC signal. This is accomplished by designing the AF of the ISAC signal to exhibit multiple ambiguous peaks with magnitudes comparable to that of the AF's mainlobe. Here, we focus on the artificial targets in the range profile of Eve. Therefore, we primarily investigate the auto-correlation function (ACF) of the ISAC signal, which corresponds to the zero-Doppler cut of the AF. It is important to note that the proposed framework emphasizes the AF characteristics of ISAC signaling, which can lead to false detections and large-scale estimation errors at Eve, rather than relying on estimation-theoretic approaches that primarily address small-scale, unbiased estimation performance.

A. Ambiguity Function Shaping for Artificial Targets

As Eve's range profile with the MF is only controllable through the ACF of the ISAC signal, we define the frequency-domain ACF as

$$\mathbf{\Lambda} = \sqrt{N}\mathbf{F}_N^H \mathbf{W}^2 \mathbf{S}^2 \mathbf{1}_N, \tag{16}$$

where the kth element is expanded in scalar form as

$$\Lambda[k] = \sum_{n=1}^{N} |w_n|^2 |s_n|^2 e^{j\frac{2\pi}{N}k(n-1)}, \quad \forall k. \tag{17}$$

It is noteworthy that the ACF exhibits an impulse function if equal power allocation is applied, i.e., $w_1 = w_2 = \cdots = w_N$, and the unit-amplitude constellation with $|s_n| = 1, \forall n$ is employed. This is in line with the understanding that PSK is optimal for OFDM sensing as proven in [33]. The proposed approach for securing sensing functionality is to generate deterministic periodic peaks in the ACF. Since Eve lacks prior information about the actual targets, these periodic peaks act as artificial targets, misleading Eve's target estimation.

Let us define $\tilde{\Lambda}[k]$ as the ideal ACF for the artificial target generation. Then, the desired ACF for secure sensing (denoted as the *"secure ACF"*) can be represented as a Dirac comb function, with its initial formulation given by

$$\tilde{\Lambda}[k] = \underbrace{N\delta[k]}_{\text{Mainlobe}} + \underbrace{\sum_{l=1}^{L} \alpha\delta[k - l\lambda]}_{\text{Artificial peaks}}, \quad \forall k. \tag{18}$$

Here, λ represents the periodicity of the peaks, L denotes the number of artificial peaks in the ACF, given by $L = N/\lambda - 1$, and α represents the artificial peak magnitude. This secure ACF is illustrated in Fig. 3(a). More explicitly, it is well known that the maximum unambiguous range of OFDM radar is given by $R_{\max} = \frac{cN}{2B}$, where c is the speed of light. The artificial peaks, relative to the zero-delay position, are equivalently located at ranges $\left[\frac{cN}{2B(L+1)}, \frac{2cN}{2B(L+1)}, \ldots, \frac{cNL}{2B(L+1)}\right]$, which limits the unambiguous range to $\frac{cN}{2B(L+1)}$. Notably, sensing security improves when the secure ACF contains a greater number of artificial peaks and higher artificial peak magnitudes, as these are perceived as potential artificial targets by Eve.

Remark 3: While our primary focus is on shaping the AF in the range domain through subcarrier power allocation in OFDM, the proposed approach can be naturally extended to enhance velocity-domain sensing security via symbol-by-symbol power allocation across the slow-time domain. This extension effectively shapes the zero-delay cut of the AF. Specifically, the maximum unambiguous Doppler frequency in OFDM radar with a symbol repetition interval of T_{sym} is given by $f_{d,\max} = \frac{1}{2T_{\text{sym}}}$. By applying OFDM symbol power allocation, L number of artificial peaks can be introduced in the Doppler domain at frequency bins $\left[\frac{1}{2T_{\text{sym}}(L+1)}, \frac{2}{2T_{\text{sym}}(L+1)}, \ldots, \frac{L}{2T_{\text{sym}}(L+1)}\right]$, thereby reducing the effective unambiguous Doppler to $\frac{1}{2T_{\text{sym}}(L+1)}$. For clarity of exposition, this paper remains focused on range-domain analysis.

The secure ACF with deterministic artificial peaks can be realized through the design of subcarrier power allocation $\mathbf{W}$. Provided that the modulated symbol comes from a unit-amplitude constellation, such as PSK, the allocated subcarrier power for achieving the secure ACF is given by the following theorem.

Theorem 1. *The power allocation of subcarriers for the secure ACF in (18) is given by*

$$|w_n|^2 = \begin{cases} p, & \text{if } n \in \mathcal{P}_{1,\kappa} = \{1, 1+\kappa, 1+2\kappa, \ldots\} \\ q, & \text{if } n \in \mathcal{P}_{1,\kappa}^c \end{cases}, \tag{19}$$

where $p > q > 0$, κ is a divisor of N, $p + (\kappa - 1)q = \kappa$, and

$$(p, q, \kappa) = \left(1 + \frac{\alpha L}{N}, 1 - \frac{\alpha}{N}, L + 1\right). \tag{20}$$

The set $\mathcal{P}_{1,\kappa}$ represents the uniformly spaced subcarriers, starting from the first subcarrier and spaced by κ, which have the dominant power p.

Proof. Please refer to Appendix A. ∎

The above theorem establishes the foundation for structured subcarrier power allocation to achieve a secure ACF. However, it only provides a fixed subcarrier power allocation for sensing-secure ISAC signaling, which lacks sufficient degrees of freedom (DoFs) to further optimize the balance between S&C performance. To address this limitation, we verify the following corollaries for advanced secure-sensing ISAC signaling, incorporating deterministic artificial peaks in the ACF to enable greater flexibility in signaling design.

Corollary 1. *(Shifted-Invariant Property) The circularly shifted subcarrier power allocation of (19), expressed as*

$$|w_n|^2 = \begin{cases} p, & \text{if } n \in \mathcal{P}_{n_0,\kappa} = \{n_0, n_0 + \kappa, n_0 + 2\kappa, \dots\} \\ q, & \text{if } n \in \mathcal{P}^c_{n_0,\kappa} \end{cases}, \tag{21}$$

where $n_0 \leq \kappa$, results in a squared ACF identical to the squared secure ACF of (18), i.e., $\left|\tilde{\Lambda}[k]\right|^2$.

Proof. Please refer to Appendix B. ∎

Corollary 2. *The subcarrier power allocation following the distribution*

$$\mathbb{E}\left[|w_n|^2\right] = \begin{cases} p, & \text{if } n \in \mathcal{P}_{n_0,\kappa} = \{n_0, n_0 + \kappa, \dots\} \\ q, & \text{if } n \in \mathcal{P}^c_{n_0,\kappa} \end{cases}, \tag{22}$$

approximately results in an expected squared ACF identical to the squared secure ACF of (18), i.e., $\left|\tilde{\Lambda}[k]\right|^2$, provided that $Var\left[|w_n|^2\right]$ is sufficiently small.

Proof. Please refer to Appendix C. ∎

The structured power allocation scheme for the secure ACF is graphically illustrated in Fig. 3(b). Consequently, the power allocation of subcarriers enables the intentional generation of deterministic artificial peaks in the ACF, where the number and magnitude of these peaks are determined by the allocation parameters (p, q, κ) given in (20).

Now, we consider the random ISAC signals based on the general constellation set, which indeed have the same artificial peaks in the ACF under the uniformly sparse subcarrier power allocation. In this regard, we evaluate the expectation of the squared ACF based on (19). This is given by a closed form as follows:

Proposition 1. *The expectation of the squared secure ACF under the subcarrier power allocation (19) and the constellation set with the kurtosis μ_4 is expressed as*

$$\mathbb{E}\left[|\Lambda[k]|^2\right] = \underbrace{N^2\delta[k]}_{\text{Mainlobe}} + \underbrace{\alpha^2 \sum_{l=1}^{L} \delta[k - l\lambda]}_{\text{Artificial peaks}} + \underbrace{(\mu_4 - 1)\left(\frac{N}{\kappa}p^2 + N\left(1 - \frac{1}{\kappa}\right)q^2\right)}_{\text{Sidelobe caused by random signaling}}. \tag{23}$$

Proof. Please refer to Appendix D. ∎

Remark 4: Notably, the ACF presented in (18) can be achieved only under unit-amplitude constellations with the kurtosis $\mu_4 = 1$. This is because other constellations with kurtosis $u_4 > 1$ inherently introduce additional sidelobes across all range bins in the ACF, as observed in (23) and corroborated by [33], [34]. Nevertheless, the proposed secure ACF with deterministic artificial peaks under the general constellation as QAM can still be achieved using the subcarrier power allocation scheme (19) as presented in Proposition 1, while including additional sidelobes induced by the constellation. Indeed, these additional sidelobes are useful to enhance the sensing security.

B. Performance of Legitimate Sensing Receiver (Alice)

In the proposed framework for secure sensing ISAC, the legitimate receiver exploits RF to cancel out the artificial peaks generated through ambiguity shaping as provided in (9). This is because the RF operation equalizes the effect of transmitted signals on the radar sensing channels [43]. Although the output of RF is free from the effects of range sidelobes caused by the secure ACF, RF suffers from noise enhancement, leading to a decrease in SNR when the noise is divided by a subcarrier element with very small power allocation. Accordingly, we introduce the SNR loss of RF relative to the SNR of MF as the performance metric of Alice, which is defined as follows [49]:

$$\mathcal{L}_A = \frac{\gamma_{MF}}{\gamma_{RF}}, \tag{24}$$

where γ_{MF} and γ_{RF} denote the SNRs of a typical target at the MF and RF outputs, respectively. This SNR loss indicates the amount of the noise amplification by RF compared to that of MF, which is the optimal receiver in terms of the SNR.

Given a scalar form of a range profile $\Gamma[n]$ and a target at the range bin of n_t, the output SNR is explicitly written as

$$\gamma = \frac{|\mathbb{E}\left[\Gamma[n_t]\right]|^2}{\mathbb{E}\left[|\Gamma[n]|^2\right]}. \tag{25}$$

With (8), (10), and (25) at hand, we derive the output SNR of the respective receiver at Alice, which are given by the following lemma.

Lemma 1. *The output SNRs of the MF and RF at Alice's receiver are respectively given by*

$$\gamma_{MF} = N\beta_A^2\sigma_A^{-2}, \tag{26}$$

$$\gamma_{RF} = N\beta_A^2\sigma_A^{-2}\left(\frac{N}{\nu_{-2}\sum_{n=1}^{N}|w_n|^{-2}}\right). \tag{27}$$

Proof. Please refer to Appendix E. ∎

Now, we are ready to explicitly express the SNR loss at Alice as a function of the ISAC TX signal.

Theorem 2. *The SNR loss of the RF output relative to the SNR of the MF output is given by*

$$\mathcal{L}_A = \frac{\nu_{-2}}{N}\sum_{n=1}^{N}|w_n|^{-2}. \tag{28}$$

Proof. Substituting (26) and (27) into (24) directly yields the result. ∎

Corollary 3. *The SNR loss with the subcarrier power allocation (19) for the secure ACF is given by*

$$\mathcal{L}_A = \frac{\nu_{-2}}{\kappa}\left(\frac{1}{p} + \frac{\kappa-1}{q}\right). \tag{29}$$

Proof. Substituting (19) into (28) yields (29). ∎

Remark 5: Clearly, the defined SNR loss depends solely on the ISAC TX signal, specifically its constellation and subcarrier power allocation. The minimum SNR loss is 0 dB, which is achieved under a unit-amplitude constellation and an equal power allocation scheme. From (29), it is intuitively observed that higher artificial peaks in the secure ACF result in greater SNR loss, implying that more secure signaling degrades legitimate sensing performance. This reveals an inherent performance trade-off between legitimate sensing and sensing security in the proposed framework.

C. Performance of Sensing Eavesdropper (Eve)

To assess the sensing security of ISAC signaling, we leverage PSL and ISL as sensing security metrics. Since Eve's receiver performance cannot be directly evaluated, PSL and ISL of the ACF serve as proxies for measuring the sensing security level. Moreover, the PSL and ISL of the AF determine the sensing performance of the MF, which is directly linked to Eve's sensing performance. A high PSL increases the likelihood of false target detection by Eve, as it corresponds to the magnitude of artificial targets generated through ambiguity shaping. Additionally, a high ISL leads to erroneous range estimation by Eve and may prevent the detection of weak targets when multiple targets exist. In our framework, ISL is influenced by the number of artificial targets and sidelobe levels caused by random signaling. Notably, these metrics represent the worst-case security level, as Eve's receiver output is further degraded due to errors in the estimation of the reference probing signal.

1) Peak Sidelobe Level: Let us define PSL as the magnitude of the highest sidelobe level relative to that of the mainlobe. This is expressed as

$$\Delta_{\mathrm{PSL,E}} = \frac{\max_{k\neq 0}\mathbb{E}\left[|\Lambda[k]|^2\right]}{\mathbb{E}\left[|\Lambda[0]|^2\right]}. \tag{30}$$

Under signaling with the secure ACF, it is immediately expressed in the following theorem.

Theorem 3. *Under the subcarrier power allocation with (p, q, κ) in (19), the PSL of the squared secure ACF is approximately given by*

$$\Delta_{PSL,E} = (1-q)^2. \tag{31}$$

Proof. From (23), the magnitude of the mainlobe level approximates N^2 for sufficiently large N. Additionally, the highest sidelobe level equals the magnitude of artificial peaks, denoted as α^2. Based on $\alpha = N(1-q)$ from (20), the ratio α^2/N^2 simplifies to $(1-q)^2$, completing the proof. ∎

Here, sparse power allocation with $q = 0$ generates artificial targets with a magnitude equal to that of the mainlobe. This implies that such a subcarrier power allocation results in a PSL of 0 dB, causing the artificial targets to have the same magnitude as the true targets in Eve's receiver. However, it is important to note that the case of $q = 0$ is not considered, as Alice would be unable to perform RF due to division by zero. Additionally, this condition ensures that communication data is always transmitted across all subcarriers.

2) Integrated Sidelobe Level: The ISL is defined as the total power contained in all sidelobes relative to the power in the mainlobe, which is given by

$$\Delta_{\mathrm{ISL,E}} = \frac{\sum_{k\neq 0}^{N}\mathbb{E}\left[|\Lambda[k]|^2\right]}{\mathbb{E}\left[|\Lambda[0]|^2\right]}. \tag{32}$$

Then, the following theorem gives the ISL under the secure sensing signaling.

Theorem 4. *Under the subcarrier power allocation with (p, q, κ) in (19), the ISL of the squared secure ACF is approximately given by*

$$\Delta_{ISL,E} = (\kappa-1)(1-q)^2 + (\mu_4-1)\left(\frac{p^2}{\kappa} + \left(1-\frac{1}{\kappa}\right)q^2\right). \tag{33}$$

Proof. From (23), the total power in sidelobes is computed as

$$\sum_{k\neq 0}^{N}\mathbb{E}\left[|\Lambda[k]|^2\right] = L\alpha^2 + N(N-1)(\mu_4-1)\left(\frac{p^2}{\kappa} + \left(1-\frac{1}{\kappa}\right)q^2\right)$$
$$\approx N^2\left((\kappa-1)(1-q)^2 + (\mu_4-1)\left(\frac{p^2}{\kappa} + \left(1-\frac{1}{\kappa}\right)q^2\right)\right). \tag{34}$$

For sufficiently large N, the mainlobe magnitude is given as N^2. Thus, this completes the proof. ∎

Corollary 4. *The ISL of the secure ACF has a linear relationship with the PSL, expressed as*

$$\Delta_{ISL,E} = \mu_4(\kappa-1)\Delta_{PSL,E} + (\mu_4-1). \tag{35}$$

Proof. From (31), we have $q = 1 - \sqrt{\Delta_{\text{PSL,E}}}$. Combining this with $p+(\kappa-1)\,q = \kappa$ gives $p = (\kappa-1)\sqrt{\Delta_{\text{PSL,E}}}+1$. Substituting p and q into (33) yields (35), completing the proof. ∎

From (35), we observe that the ISL is influenced by three factors: the constellation, the number of artificial peaks, and their magnitude relative to the mainlobe. In this framework, we primarily focus on subcarrier power allocation to design sensing-secure ISAC signaling with deterministic artificial peaks, without delving deeply into the constellation set.

IV. Signaling Design for Sensing-Secure ISAC Based on AF Shaping

Building on the above AF analysis, in this section, we present a sensing-secure ISAC signaling design with artificial targets, offering three-way trade-offs between communication, legitimate sensing, and sensing security. Notably, the subcarrier power allocation presented for the secure ACF in Theorem 1 appears to provide a trade-off only between ISAC performance and sensing security. This is because it fixes the power of subcarriers in $\mathcal{P}_{n_0,\kappa}$ and $\mathcal{P}^c_{n_0,\kappa}$ to the exact values p and q, respectively, without any degree of freedom (DoF) for ISAC signaling design under a given sensing security level. Nevertheless, Corollary 2 introduces a certain level of DoF, enabling a more flexible trade-off between S&C performance. Accordingly, we first investigate the trade-off between ISAC performance and sensing security with artificial targets and then explore a sensing-secure ISAC signaling design under a given level of sensing security.

A. Trade-off between ISAC Performance and Sensing Security

Firstly, we analyze the trade-off between ISAC performance and sensing security in the proposed framework. To this end, we determine a feasible performance region for secure-sensing ISAC based on Theorem 1, where communication, sensing, and sensing security performance are directly influenced by the selection of parameters (p, q, κ) for the secure ACF with artificial peaks. Recalling that N subcarriers in OFDM signal are modulated by the constellation set $\mathcal{S}$, let us define $\mathcal{C}(N, \mathcal{S})$ as the set of feasible performance points, given by

$$\mathcal{C}(N,\mathcal{S}) = \left\{(R_c, \mathcal{L}_A, \Delta_{\text{PSL,E}}, \Delta_{\text{ISL,E}}) \mid (5), (29), (31), \text{and } (33), \forall p, q, \kappa\right\}, \tag{36}$$

where p, q, and κ are constrained as per Theorem 1. All operating points of $\mathcal{C}(N, \mathcal{S})$ can be determined by evaluating all possible combinations of (p, q, κ). Assuming a flat-fading communication channel, there is no clear trade-off between S&C performance under the fixed power allocation scheme in Theorem 1. This is because the power allocation parameters (p, q, κ) that reduce the SNR loss of the legitimate sensing receiver also increase the communication rate in (5). However, a flexible power allocation scheme based on Corollary 2 enables a trade-off design between S&C performance under a frequency-selective fading channel, which will be detailed in Section IV-B.

Instead, the performance trade-off can be observed between ISAC and sensing security by varying the parameters (p, q, κ) in (36). It is straightforward to verify from (31) and (35) that higher values of $\Delta_{\text{PSL,E}}$ and $\Delta_{\text{ISL,E}}$ require a smaller q and a larger κ. However, this increases the SNR loss, as shown in (29), thereby degrading both the legitimate sensing performance and the communication performance. The legitimate sensing optimal point in (36) is achieved with equal subcarrier power allocation, i.e., $\kappa = 1$, resulting in the following metrics:

$$\mathcal{L}_A^{\text{sen-opt}} = \nu_{-2}, \tag{37}$$

$$\Delta_{\text{PSL,E}}^{\text{sen-opt}} = 0, \quad \Delta_{\text{ISL,E}}^{\text{sen-opt}} = \mu_4 - 1. \tag{38}$$

On the other hand, the sensing security optimal point in (36) is obtained when $\kappa = N/2$ and $q \to 0$, yielding

$$\mathcal{L}_A^{\text{sec-opt}} = \infty, \tag{39}$$

$$\Delta_{\text{PSL,E}}^{\text{sec-opt}} = 1, \quad \Delta_{\text{ISL,E}}^{\text{sec-opt}} = \frac{\mu_4 N}{2} - 1. \tag{40}$$

Accordingly, one may coarsely determine an appropriate sensing security level to ensure a desired level of ISAC performance, or vice versa, based on (36).

B. Sensing-Secure ISAC Signaling Design

We further investigate the optimization of sensing-secure ISAC signaling design with artificial targets, which provides a flexible balance between S&C performance under a given level of sensing security. Based on Corollary 2, we can finely tune the subcarrier power allocation to optimize the S&C performance bound while ensuring the desired level of sensing secrecy. Clearly, given that channel state information (CSI) is available at the ISAC TX, we can finely adjust $\{w_n\}, \forall n$, to balance the SNR loss at Alice and the communication rate.

To this end, we formulate the following sensing-secure ISAC signaling design problem:

$$(\mathbf{P.1}) \underset{\{w_n\}}{\text{maximize}} \quad -(1-\rho)\frac{\mathcal{L}_A}{\mathcal{L}_{A,\rho=0}} + \rho\frac{R_c}{R_{c,\rho=1}} \tag{41a}$$

$$\text{subject to} \quad \Delta_{\text{ISL,E}} \geq \epsilon_{\text{ISL}}, \tag{41b}$$

$$\Delta_{\text{PSL,E}} \geq \epsilon_{\text{PSL}}, \tag{41c}$$

$$\sum_{n=1}^{N} |w_n|^2 = N, \tag{41d}$$

where $\rho \in [0, 1]$ is a weighting factor that determines the priority between sensing and communication functionalities. The S&C performance metrics in the objective function (41a) are normalized by their respective values obtained when $\rho = 0$ and $\rho = 1$. The parameters ϵ_{ISL} and ϵ_{PSL} in (41b) and (41c) represent the desired worst-case sensing security levels. Since the ISL and PSL constraints cannot be expressed in closed form with respect to $\{w_n\}$, we first determine the parameters (p, q, κ) to shape the secure ACF such that the sensing security constraints are satisfied.

Under the given constellation set for data symbol modulation, the constraints (41b) and (41c) on sensing security are reformulated as constraints on $\{w_n\}$ for the secure ACF. Firstly, it is straightforward to determine the sparse subcarrier

This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2025.3618121

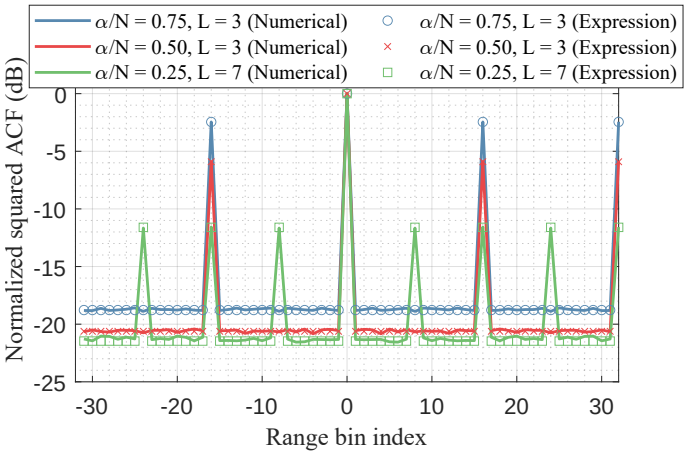


Fig. 4. Various secure ACFs with a 16QAM constellation and $N = 64$.

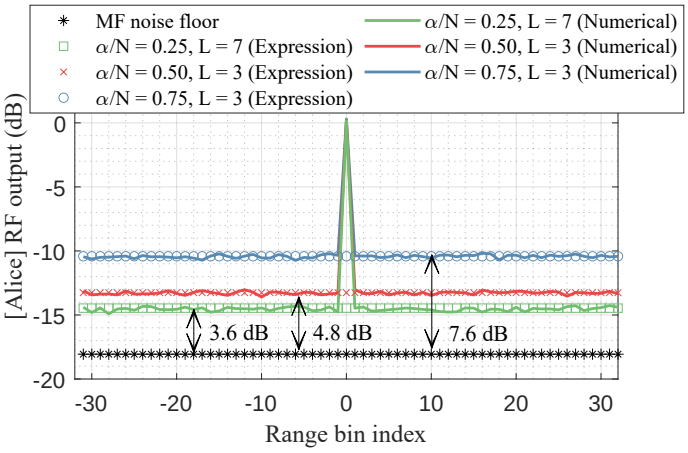


Fig. 5. Alice's range profiles with RF under the ISAC signals with the secure ACFs in Fig. 4. A target is assumed to be located at zero delay with an SNR of 0 dB. The SNR of the MF output is 18 dB.

spacing κ in relation to ϵ_{ISL} and ϵ_{PSL}. By setting $\Delta_{\text{PSL,E}} = \epsilon_{\text{PSL}}$ and substituting (35) into (41b), we obtain

$$\kappa \geq \frac{\epsilon_{\text{ISL}} - \mu_4 + 1}{\epsilon_{\text{PSL}}\mu_4} + 1. \tag{42}$$

Suppose that the number of subcarriers N is a power of 2. Then, the smallest κ satisfying (42) can be determined as

$$\kappa = 2^{\left\lceil \log_2\left(\frac{\epsilon_{\text{ISL}} - \mu_4 + 1}{\epsilon_{\text{PSL}}\mu_4} + 1\right)\right\rceil + 1}. \tag{43}$$

Furthermore, we replace (41c) using (22) and (31) with

$$\sum_{n \in \mathcal{P}^c_{n_0,\kappa}} |w_n|^2 \leq \frac{N(\kappa - 1)}{\kappa}(1 - \sqrt{\epsilon_{\text{PSL}}}). \tag{44}$$

Substituting (43) and (44) into (41b) and (41c), we reformulate problem (**P.1**) as

$$(\mathbf{P.2}) \underset{\{w_n\}}{\text{maximize}} \quad -(1-\rho)\frac{\mathcal{L}_A}{\mathcal{L}_{A,\rho=0}} + \rho\frac{R_c}{R_{c,\rho=1}} \tag{45}$$
$$\text{subject to} \quad (43), (44), \text{and } (41d).$$

Referring to (5) and Theorem 2, the formulated problem is a convex quadratic program, which can be efficiently solved using numerical convex optimization tools.

V. Numerical Results

In this section, we present numerical simulation results to validate the proposed sensing-secure ISAC framework. Unless stated otherwise, the ISAC TX transmits an OFDM signal with $B = 50$ MHz, $N = 256$, and $N_{\text{cp}} = 64$, where $R_{\max} = 768$ m and $R_{\max,\text{cp}} = 192$ m. The random communication data is modulated from a 16QAM constellation, where $\mu_4 = 1.32$ and $\nu_{-2} = 1.89$. We integrate over 32 OFDM symbols to evaluate the sensing performance at both Alice and Eve. For clarity in graphical illustration, the target range observed by Alice is assumed to be identical to that observed by Eve. Each simulation result is obtained from 1000 Monte Carlo runs.

A. Design of Secure ACF for Artificial Target Generation

Firstly, we present various secure ACFs utilized for sensing-secure ISAC transmission and analyze their corresponding impacts on Alice's RF receiver. Fig. 4 illustrates the secure ACFs with different numbers and magnitudes of artificial peaks, designed based on Theorem 1. For graphical clarity, we set $N = 64$. Recalling that α is the magnitude of the artificial peaks and L denotes the number of artificial peaks, the secure ACF with $\alpha/N = 0.75$ and $L = 3$ is obtained using $p = 3.25$, $q = 0.25$, and $\kappa = 4$, resulting in $\Delta_{\text{PSL,E}} = -2.5$ dB and $\Delta_{\text{ISL,E}} = 4$ dB. In contrast, for $\alpha/N = 0.5$ and $L = 3$, the lower PSL and ISL values of $\Delta_{\text{PSL,E}} = -6$ dB and $\Delta_{\text{ISL,E}} = 1.17$ dB indicate weaker sensing security compared to the case with $\alpha/N = 0.75$. On the other hand, the secure ACF with $\alpha/N = 0.25$ and $L = 7$ is designed using $p = 2.75$, $q = 0.75$, and $\kappa = 8$, yielding PSL and ISL values of $\Delta_{\text{PSL,E}} = -12$ dB and $\Delta_{\text{ISL,E}} = -0.5$ dB, representing the lowest security level among the three ACFs.

Notably, the squared secure ACFs in Fig. 4 exhibit sidelobes across all range bins. This is due to the random signaling with the 16QAM constellation, which introduces additional sidelobes compared to the unit-amplitude constellation, as stated in Proposition 1. The theoretical expression of the secure ACF in (23) closely matches the numerical simulation results, confirming that the secure ACF exhibits deterministic artificial peaks from subcarrier power allocation while maintaining a sidelobe floor due to the constellation.

Furthermore, we validate the SNR loss at Alice under various secure ACFs. The use of RF to cancel artificial sidelobes in the secure ACF inherently causes SNR loss compared to MF, and this loss is further influenced by the ISAC signaling design, as described in Theorem 2. Fig. 5 illustrates the range profiles of Alice's RF output under ISAC signaling with secure ACFs, assuming a single target is located at zero delay. Here, we observe that the resulting range profiles with RF exhibit no artificial peaks. Instead, each signaling scheme with a different secure ACF results in a different level of SNR loss compared to the MF noise floor, 3.6 dB, 4.8 dB, and 7.6 dB, respectively.

This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2025.3618121

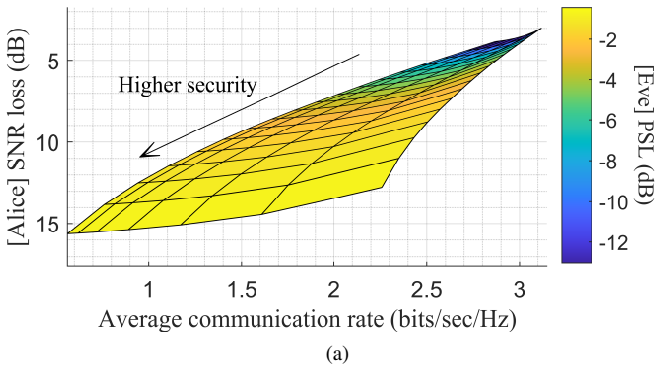


Fig. 6. Three-way trade-offs between communication, sensing, and sensing security: (a) ISAC vs. PSL of the secure ACF, and (b) ISAC vs. ISL of the secure ACF.

Interestingly, the SNR loss increases as the security level of the ACF improves, revealing a trade-off between sensing security and legitimate sensing performance.

From Corollary 3, the theoretical SNR loss is determined by both the subcarrier power allocation and the inverse second moment of the constellation. The numerical simulations confirm this theoretical proof, showing a close match between the theoretical and simulated results. In conclusion, these findings provide valuable insight into the signaling design for sensing-secure ISAC, highlighting the inherent trade-off between introducing strong artificial targets at Eve and incurring SNR loss at Alice.

B. Three-way Trade-offs in Sensing-Secure ISAC Signaling

In this section, we investigate the three-way trade-offs between communication, sensing, and sensing security in the proposed sensing-secure ISAC framework. As discussed in Section IV, the proposed AF shaping approach introduces a new trade-off between ISAC performance and sensing security, with feasible performance points determined by (36). Without considering S&C performance optimization, we explore this trade-off by sweeping the secure ACF design parameters (p, q, κ), as shown in Fig. 6, where the average communication SNR per subcarrier $|h_i|^2/\sigma_c^2$ is set to 10 dB. The minimum SNR loss and maximum communication rate are achieved simultaneously when the PSL and ISL of the ACF are minimized. Conversely, the highest SNR loss and lowest communication rate occur when sensing security is maximized,

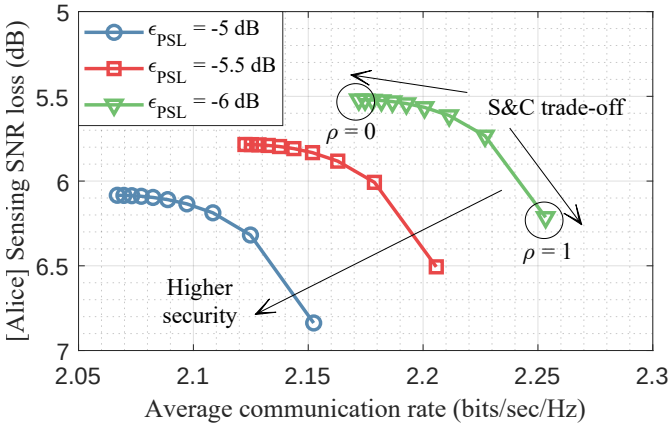


Fig. 7. S&C trade-offs under given levels of sensing security based on the sensing-secure ISAC signaling design. ϵ_{ISL} is set to 7 dB, resulting in $\kappa = 16$.

confirming the inherent trade-off between ISAC performance and sensing security. Here, it is worth noting that the minimum SNR loss at Alice is bounded due to the random signaling nature of 16QAM, as discussed in Section V-A.

On the other hand, the sensitivities of S&C performance variations with respect to PSL and ISL differ between sensing and communication. As shown in Fig. 6(a), the SNR loss is highly influenced by the PSL of the secure ACF, while its variation remains smaller than that of communication performance for a fixed PSL value. This insight suggests that legitimate sensing performance is primarily affected by the magnitude of artificial peaks, whereas the communication rate is more sensitive to the number of artificial peaks, as illustrated in Fig. 6(b). Nevertheless, both sensing security metrics negatively impact legitimate sensing and communication performance, reinforcing the inherent trade-off between ISAC and sensing security.

Next, we further optimize the sensing-secure ISAC signaling under given PSL and ISL constraints, providing a flexible trade-off between S&C performance. The key idea behind this optimization is that the optimal subcarrier power allocation for communication can be determined based on CSI, while an increased variation in subcarrier power allocation leads to a higher SNR loss. Fig. 7 illustrates the S&C trade-offs under given levels of sensing security, where each secure-sensing ISAC signaling scheme is designed using the proposed framework in Section IV-B. The results demonstrate that the proposed design enables a flexible trade-off between SNR loss at Alice and the achievable communication rate, controlled by the weighting factor ρ. Once again, these findings validate the inherent trade-off between ISAC performance and sensing security, showing that higher security levels degrade the ISAC performance region, thereby reinforcing the three-way trade-off between communication, sensing, and sensing security.

C. Security Performance Analysis: Detection and Estimation

Now, we comprehensively analyze the sensing security performance in terms of target detection and range estimation. Here, we assume that the SINR of the reference signal leaked to Eve is 0 dB. First, we present range-Doppler (RD) maps

This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2025.3618121

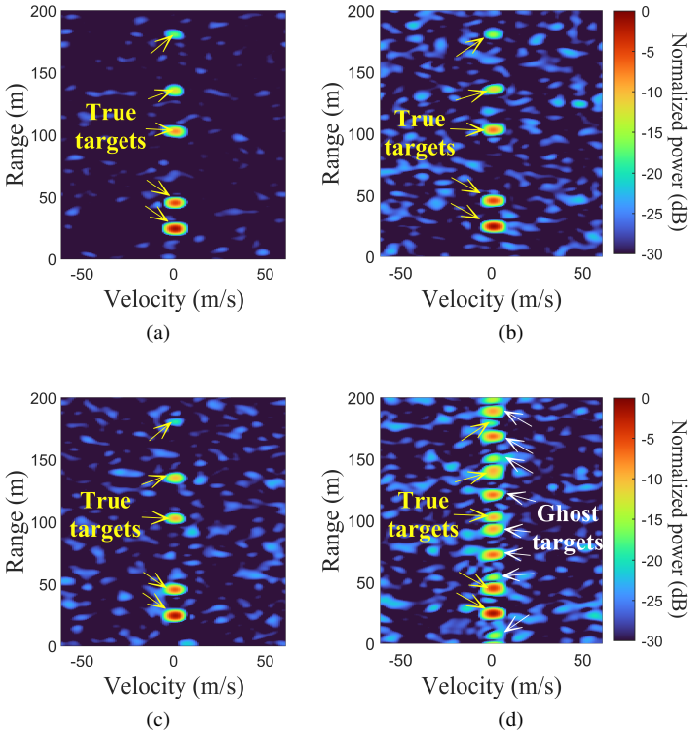


Fig. 8. Range-Doppler (RD) maps with five static targets located at different ranges. (a), (b): Alice's RD maps without and with sensing security, respectively. (c), (d): Eve's RD maps without and with sensing security, respectively. The sensing-secure ISAC signaling is designed with $\epsilon_{\text{PSL}} = -5$ dB, $\epsilon_{\text{ISL}} = 7$ dB, and $\rho = 0$.

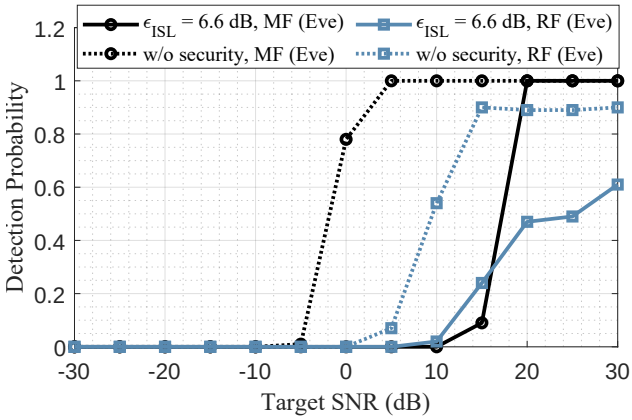


Fig. 9. Target detection performance of Eve with reciprocal filtering when clutter with an SNR of 10 dB is located at 30 m, and the target is located at a distance of 100 m. The sensing-secure ISAC signaling is designed with $\epsilon_{\text{PSL}} = -5$ dB and $\rho = 0$. The SINR of the reference signal leaked to Eve is 0 dB.

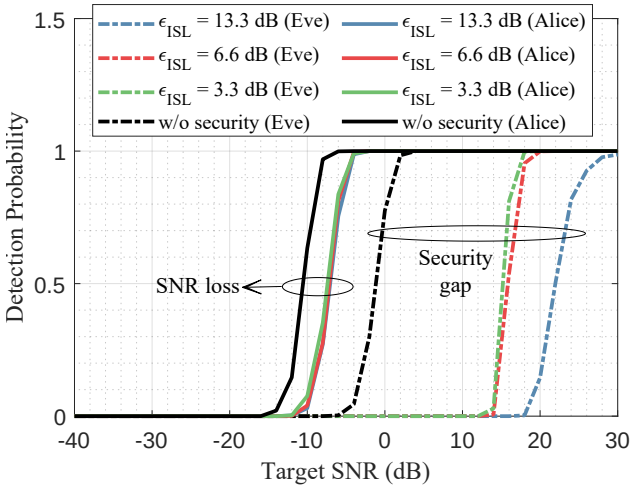


Fig. 10. Target detection performance of Alice and Eve when clutter with an SNR of 10 dB is located at 30 m, and the target is located at a distance of 100 m. The sensing-secure ISAC signaling is designed with $\epsilon_{\text{PSL}} = -5$ dB and $\rho = 0$.

for both Alice and Eve in the scenario where five static targets $U = U_t = 5$ are located at 24 m, 45 m, 100 m, 135 m, and 180 m, respectively. The targets have SNRs that gradually decrease from 0 dB to -15 dB in steps of -3 dB. Without the secure-sensing ISAC signaling design, both Alice and Eve can clearly detect all targets at zero velocity, as shown in Fig. 8(a) and Fig. 8(c), respectively. This indicates that Eve can exploit the ISAC signals of opportunity to maliciously detect and estimate targets. On the other hand, the proposed secure ISAC signaling deceives Eve, preventing it from accurately detecting and estimating true targets by introducing artificial peaks in Eve's RD map, as shown in Fig. 8(d). Meanwhile, Alice, as shown in Fig. 8(b), can still successfully locate the true targets due to the use of RF, albeit at the expense of an SNR loss compared to Fig. 8(a).

We further quantitatively compare the target detection performance between Alice and Eve in the presence of clutter, $U = 2, U_t = 1, U_c = 1$. Supposing a clutter with an SNR of 10 dB is located at 30 m, we evaluate the target detection performance for a target positioned at a distance of 100 m. A conventional cell-averaging constant false alarm rate (CA-CFAR) detector is employed with a false alarm rate of 10^{-5}. First, we evaluate the target detection performance at Eve to support the assumption that Eve employs the MF receiver rather than the RF. As illustrated in Fig. 9, the detection performance of Eve with the RF receiver is significantly degraded compared to that with the MF receiver, primarily due to the use of an imperfect reference signal. Furthermore, when the proposed secure-sensing ISAC signaling is transmitted, Eve's detection performance under the RF receiver deteriorates even further, as the associated SNR loss in the RF receiver becomes more pronounced.

Fig. 10 presents the target detection performance of Alice and Eve under various levels of sensing security. The performance of Eve deteriorates significantly as the ISL of the secure ACF increases, as it raises the average power level near the target location, making target detection more challenging by requiring 10 to 100 times higher target power. For the signaling design, the PSL is fixed at -5 dB, meaning that a higher ISL directly corresponds to more artificial peaks in the secure ACF. Compared to Eve, Alice exhibits superior target detection performance. However, the SNR loss results in minor degradation about 2 dB of the required target SNR compared to the case without sensing-secure signaling. Consequently, AF shaping with artificial targets effectively prevents unauthorized

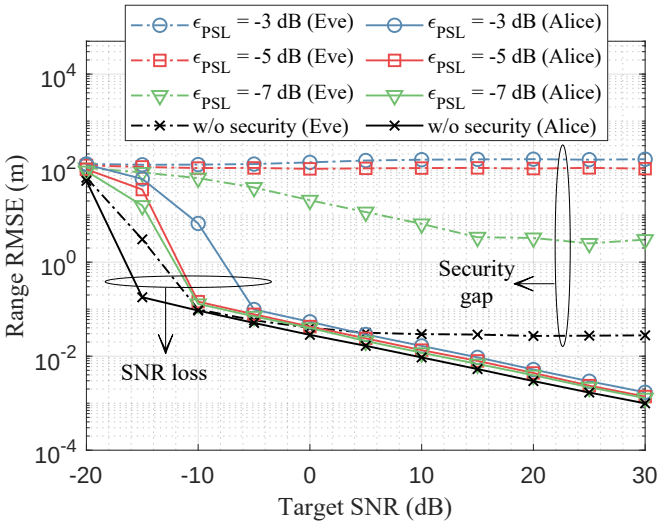


Fig. 11. Range estimation performance of Alice and Eve when two targets have a random SNR difference of 4-6 dB. The sensing-secure ISAC signaling is designed with $\epsilon_{\text{ISL}} = 7$ dB, resulting in $\kappa = 16$ and $\rho = 0$.

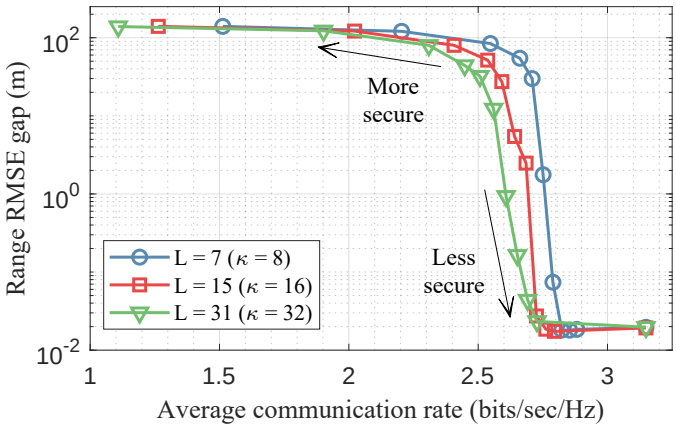


Fig. 12. Range estimation RMSE gap (Eve's RMSE − Alice's RMSE) vs. communication rate when two targets have a random SNR difference of 4-6 dB. The sensing-secure ISAC signaling is designed with varying ϵ_{PSL} and $\kappa = 8, 16$, and 32, respectively.

Eve from detecting the target while ensuring that legitimate sensing performance remains largely unaffected.

Finally, we explore the multi-target range estimation performance of Alice and Eve. Fig. 11 illustrates the range estimation performance for two targets, $U = U_t = 2$, with a random SNR gap of 4–6 dB. The target ranges are estimated using the root MUSIC estimator with a given source number. Compared to the case without sensing security, Eve's range estimation performance is severely degraded when the sensing-secure ISAC signal is applied, leading to a noticeable security gap more than 100 m estimation errors. This degradation occurs because larger artificial peaks cause Eve to falsely estimate target ranges, resulting in large-scale range estimation errors. Moreover, we define the range RMSE gap between Alice and Eve as a sensing secrecy metric, which characterizes the ultimate trade-off between sensing security performance and communication rate, as illustrated in Fig. 12. The results confirm that secure sensing functionality can be flexibly achieved at the expense of communication performance. It is worth noting that introducing more artificial peaks further degrades communication performance to maintain a desired RMSE gap. Nevertheless, the increase of the number of artificial peaks enhances sensing security in terms of target detection performance, as demonstrated in Fig. 10. It should be noted that the range RMSE gap narrows when the PSL becomes extremely high, i.e., as $\alpha/N \to 1$ or equivalently $q \to 0$ in (29), because the SNR loss at the RF output, denoted by $\mathcal{L}_A$, increases sharply, thereby degrading legitimate sensing performance. Therefore, it is recommended to avoid selecting a large value of α/N for secure ISAC signaling to preserve legitimate sensing functionality.

Building on the sensing security performance analysis of detection and estimation, we observe that the bottom-line performance, such as target detection probability and range estimation RMSE gap between Alice and Eve, is significantly improved by the proposed secure ISAC signaling design, which leverages intermediate metrics: the PSL and ISL of the AF. In conclusion, the target detection and estimation performances of Alice and Eve align with our theoretical and numerical results, confirming the effectiveness of the proposed secure-sensing ISAC signaling with artificial targets.

VI. Conclusion

In this paper, we proposed a sensing-secure ISAC framework that enhances sensing security against Eve, establishing a fundamental basis for sensing-secure ISAC signaling. By leveraging AF shaping, we introduced artificial targets into Eve's range profile while ensuring that the legitimate sensing receiver, Alice, retains target detection capabilities using reciprocal filtering. A structured subcarrier power allocation scheme was designed to shape the secure ACF, enabling periodic peak insertion to degrade Eve's range estimation performance. Furthermore, we formulated and optimized the ISAC signaling design to balance ISAC performance and sensing security under given constraints. Simulation results demonstrated the effectiveness of the proposed secure ISAC framework in degrading Eve's target detection and estimation performance while maintaining reliable sensing at Alice. The findings highlight the three-way trade-offs in sensing-secure ISAC and provide valuable insights into secure ISAC system design. The proposed fundamental framework can be broadly extended to various research areas in ISAC, including secure-sensing ISAC in high-mobility scenario, estimation- and information-theory based secure ISAC signaling design, multi-input multi-output ISAC beamforming, constellation optimization, pulse-shaping with spectral compliance, multi-path exploitation, offering additional degrees of freedom to further enhance sensing security through AF shaping.

Appendix A
Proof of Theorem 1

The subcarrier power allocation for the secure ACF can be directly obtained by taking DFT over (18), which is given by

$$|w_n|^2 = \frac{1}{N}\sum_{k=1}^{N} \tilde{\Lambda}[k] e^{-j\frac{2\pi}{N}k(n-1)}$$

$$= 1 + \frac{\alpha}{N} \sum_{l=1}^{L} e^{-j\frac{2\pi}{N} l\lambda(n-1)}, \forall n = 1, 2, \ldots, N. \quad (46)$$

With $L + 1 = N/\lambda$ in hand, it is further simplified as

$$|w_n|^2 = \left(1 - \frac{\alpha}{N}\right) + \frac{\alpha}{N} \sum_{l=1}^{L+1} e^{-j\frac{2\pi l}{(L+1)}(n-1)}$$
$$= \left(1 - \frac{\alpha}{N}\right) + \frac{\alpha(L+1)}{N} \sum_{d=0}^{\lambda-1} \delta[n - 1 - \kappa d], \quad \forall n, \quad (47)$$

where $\kappa = L + 1$. Thus, the power allocation of subcarriers for the secure ACF is equivalently written as a form of (19) with the dominant power allocation set $\mathcal{P} = \{1, 1 + \kappa, \ldots\}$.

Appendix B
Proof of Corollary 1

The circular shift of (47) by n_0 samples is expressed as

$$|w_n|^2 = \left(1 - \frac{\alpha}{N}\right) + \frac{\alpha(L+1)}{N} \sum_{d=0}^{\lambda-1} \delta[n - n_0 - 1 - \kappa d]. \quad (48)$$

Then, its ACF is given by a linear phase-shifted form of the secure ACF in (18), which is written as

$$\Lambda_{n_0}[k] = \left(N\delta[k] + \alpha \sum_{l=1}^{L} \delta[k - l\lambda]\right) e^{-j\frac{2\pi}{N} k n_0}, \quad \forall k. \quad (49)$$

Thus, the squared ACF $\left|\Lambda_{n_0}[k]\right|^2$ remains same to the squared secure ACF $\left|\tilde{\Lambda}[k]\right|^2$ of (18), completing the proof.

Appendix C
Proof of Corollary 2

From (17), the expected squared ACF is given as

$$\mathbb{E}\left[|\Lambda[k]|^2\right] = \mathbb{E}\left[\sum_{n=1}^{N}\sum_{m=1}^{N} |w_n|^2|w_m|^2 e^{j\frac{2\pi}{N}k(n-m)}\right]$$
$$= \sum_{n=1}^{N} \mathbb{E}\left[|w_n|^4\right] + \mathbb{E}\left[\sum_{n=1}^{N}\sum_{m\neq n}^{N} |w_n|^2|w_m|^2 e^{j\frac{2\pi}{N}k(n-m)}\right]$$
$$= \sum_{n=1}^{N}\left[\mathbb{E}\left[|w_n|^4\right] - \left(\mathbb{E}\left[|w_n|^2\right]\right)^2\right]$$
$$+ \sum_{n=1}^{N}\sum_{m=1}^{N} \mathbb{E}\left[|w_n|^2\right]\mathbb{E}\left[|w_m|^2\right] e^{j\frac{2\pi}{N}k(n-m)}. \quad (50)$$

Based on (22) and Theorem 1, we have

$$\mathbb{E}\left[|\Lambda[k]|^2\right] = \sum_{n=1}^{N} \mathrm{Var}\left[|w_n|^2\right] + \left|\tilde{\Lambda}[k]\right|^2 \approx \left|\tilde{\Lambda}[k]\right|^2, \quad (51)$$

where $\mathrm{Var}\left[|w_n|^2\right]$ is sufficiently small. Thus, this completes the proof.

Appendix D
Proof of Proposition 1

From (17), we derive the expected squared ACF as

$$\mathbb{E}\left[|\Lambda[k]|^2\right]$$
$$= \mu_4 \sum_{n=1}^{N} |w_n|^4 + \mathbb{E}\left[\sum_{n=1}^{N}\sum_{m\neq n}^{N} |w_n|^2|w_m|^2|s_n|^2|s_m|^2 e^{j\frac{2\pi}{N}k(n-m)}\right]$$
$$= (\mu_4 - 1)\sum_{n=1}^{N} |w_n|^4 + \sum_{n=1}^{N}\sum_{m=1}^{N} |w_n|^2|w_m|^2 e^{j\frac{2\pi}{N}k(n-m)}. \quad (52)$$

By substituting (19) into (52), the first term is written as

$$(\mu_4 - 1)\sum_{n=1}^{N} |w_n|^4 = (\mu_4 - 1)\left(\frac{N}{\kappa}p^2 + N\left(1 - \frac{1}{\kappa}\right)q^2\right). \quad (53)$$

With Theorem 1 at hand and plugging (53) into (52) leads to (23), completing the proof.

Appendix E
Proof of Lemma 1

By the definition of the SNR in (25), the output SNR of the MF from (8) is given as

$$\gamma_{MF} = \frac{\mathbb{E}\left[\beta_A \sum_{n=1}^{N} |w_n|^2|s_n|^2/\sqrt{N}\right]^2}{\sigma_A^2} = N\beta_A^2\sigma_A^{-2}. \quad (54)$$

Similarly, the output SNR of the RF from (10) is written by

$$\gamma_{RF} = \frac{N\beta_A^2}{\mathbb{E}[|\tilde{z}_{A,RF,s}[n]|^2]}, \quad (55)$$

where the denominator can be further expanded as

$$\mathbb{E}[|\tilde{z}_{A,RF,s}[n]|^2] = \frac{1}{N}\sum_{n=1}^{N} \mathbb{E}\left[\frac{|z_{A,s}[n]|^2}{|w_n|^2|s_n|^2}\right]$$
$$= \frac{\sigma_A^2}{N}\sum_{n=1}^{N} |w_n|^{-2}\mathbb{E}\left[|s_n|^{-2}\right]. \quad (56)$$

By the definition of the inverse second moment in (1), the SNR of RF is provided as (27).

References

[1] 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 Journal on Selected Areas in Communications*, vol. 40, no. 6, pp. 1728–1767, 2022.

[2] F. Dong, F. Liu, Y. Cui, W. Wang, K. Han, and Z. Wang, "Sensing as a service in 6G perceptive networks: A unified framework for ISAC resource allocation," *IEEE Transactions on Wireless Communications*, vol. 22, no. 5, pp. 3522–3536, 2022.

[3] I. Valiulahi, C. Masouros, and A. Salem, "Net-zero energy dual-functional radar-communication systems," *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 1, pp. 356–369, 2023.

[4] K. Meng, C. Masouros, A. P. Petropulu, and L. Hanzo, "Cooperative ISAC Networks: Opportunities and Challenges," *IEEE Wireless Communications*, pp. 1–8, 2024.

[5] ——, "Cooperative isac networks: Performance analysis, scaling laws and optimization," *IEEE Transactions on Wireless Communications*, vol. 24, no. 2, pp. 877–892, 2025.

[6] E. C. Strinati, G. C. Alexandropoulos, N. Amani, M. Crozzoli, G. Madhusudan, S. Mekki, F. Rivet, V. Sciancalepore, P. Sehier, M. Stark *et al.*, "Toward Distributed and Intelligent Integrated Sensing and Communications for 6G Networks," *IEEE Wireless Communications*, vol. 32, no. 1, pp. 60–67, 2025.

[7] T. Wild, V. Braun, and H. Viswanathan, "Joint Design of Communication and Sensing for Beyond 5G and 6G Systems," *IEEE Access*, vol. 9, pp. 30 845–30 857, 2021.

[8] K. Qu, J. Ye, X. Li, and S. Guo, "Privacy and security in ubiquitous integrated sensing and communication: Threats, challenges and future directions," *IEEE Internet of Things Magazine*, vol. 7, no. 4, pp. 52–58, 2024.

[9] S. A. Shah and F. Fioranelli, "Rf sensing technologies for assisted daily living in healthcare: A comprehensive review," *IEEE Aerospace and Electronic Systems Magazine*, vol. 34, no. 11, pp. 26–44, 2019.

[10] K. Han and S. Hong, "Vocal signal detection and speaking-human localization with MIMO FMCW radar," *IEEE Transactions on Microwave Theory and Techniques*, vol. 69, no. 11, pp. 4791–4802, 2021.

[11] Q. Wan, Y. Li, C. Li, and R. Pal, "Gesture recognition for smart home applications using portable radar sensors," in *2014 36th annual international conference of the IEEE engineering in medicine and biology society*. IEEE, 2014, pp. 6414–6417.

[12] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, "What will 5g be?" *IEEE Journal on selected areas in communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[13] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2018.

[14] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[15] A. Bazzi and M. Chafii, "Secure full duplex integrated sensing and communications," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2082–2097, 2023.

[16] A. Boljević, A. Bazzi, and M. Chafii, "Sum Secrecy Rate Maximization for Full Duplex ISAC Systems," *arXiv preprint arXiv:2410.13102*, 2024.

[17] N. Su, F. Liu, and C. Masouros, "Sensing-assisted eavesdropper estimation: An ISAC breakthrough in physical layer security," *IEEE Transactions on Wireless Communications*, vol. 23, no. 4, pp. 3162–3174, 2023.

[18] X. Wang, Z. Fei, P. Liu, J. A. Zhang, Q. Wu, and N. Wu, "Sensing-aided covert communications: Turning interference into allies," *IEEE Transactions on Wireless Communications*, vol. 23, no. 9, pp. 10 726–10 739, 2024.

[19] R. L. Cigno, F. Gringoli, M. Cominelli, and L. Ghiro, "Integrating CSI sensing in wireless networks: Challenges to privacy and countermeasures," *IEEE Network*, vol. 36, no. 4, pp. 174–180, 2022.

[20] Y. Yao, Y. Li, and T. Zhu, "Interference-negligible privacy-preserved shield for rf sensing," *IEEE Transactions on Mobile Computing*, vol. 23, no. 5, pp. 3576–3588, 2023.

[21] L. Ruan and H. Zhu, "Leveraging RIS to assist communication and against CSI-based passive sensing," *IEEE Wireless Communications Letters*, 2024.

[22] P. Staat, S. Mulzer, S. Roth, V. Moonsamy, M. Heinrichs, R. Kronberger, A. Sezgin, and C. Paar, "IRShield: A countermeasure against adversarial physical-layer wireless sensing," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 1705–1721.

[23] J. Shenoy, Z. Liu, B. Tao, Z. Kabelac, and D. Vasisht, "Rf-protect: privacy against device-free human tracking," in *Proceedings of the ACM SIGCOMM 2022 Conference*, 2022, pp. 588–600.

[24] S. M. Hernandez and E. Bulut, "Scheduled Spatial Sensing against Adversarial WiFi Sensing," in *2023 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, 2023, pp. 91–100.

[25] M. Cominelli, S. Shahcheraghi, J. Link, M. Hollick, F. Cerutti, F. Gringoli, and A. Asadi, "Physical-Layer Privacy via Randomized Beamforming Against Adversarial Wi-Fi Sensing: Analysis, Implementation, and Evaluation," *IEEE Transactions on Wireless Communications*, 2024.

[26] L. Ghiro, M. Cominelli, F. Gringoli, and R. L. Cigno, "On the implementation of location obfuscation in openwifi and its performance," in *2022 20th Mediterranean Communication and Computer Networking Conference (MedComNet)*. IEEE, 2022, pp. 64–73.

[27] L. F. Abanto-Leon, A. Bäuml, G. H. Sim, M. Hollick, and A. Asadi, "Stay connected, leave no trace: Enhancing security and privacy in wifi via obfuscating radiometric fingerprints," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 4, no. 3, pp. 1–31, 2020.

[28] Y. Zhu, Z. Xiao, Y. Chen, Z. Li, M. Liu, B. Y. Zhao, and H. Zheng, "Et tu alexa? when commodity wifi devices turn into adversarial motion sensors," *arXiv preprint arXiv:1810.10109*, 2018.

[29] Y. Wang, L. Sun, and Q. Du, "Multi-Antenna Signal Masking and Round-Trip Transmission for Privacy-Preserving Wireless Sensing," *IEEE Transactions on Information Forensics and Security*, 2024.

[30] J. Luo, H. Cao, H. Jiang, Y. Yang, and Z. Chen, "MIMOCrypt: Multi-user privacy-preserving Wi-Fi sensing via MIMO encryption," in *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2024, pp. 2812–2830.

[31] J. Hu, H. Jiang, S. Chen, Q. Zhang, Z. Xiao, D. Liu, J. Liu, and B. Li, "Wishield: Privacy against wi-fi human tracking," *IEEE Journal on Selected Areas in Communications*, 2024.

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

[33] F. Liu, Y. Zhang, Y. Xiong, S. Li, W. Yuan, F. Gao, S. Jin, and G. Caire, "OFDM achieves the lowest ranging sidelobe under random ISAC signaling," *arXiv preprint arXiv:2407.06691*, 2024.

[34] F. Liu, Y. Xiong, S. Lu, S. Li, W. Yuan, C. Masouros, S. Jin, and G. Caire, "Uncovering the Iceberg in the Sea: Fundamentals of Pulse Shaping and Modulation Design for Random ISAC Signals," *arXiv preprint arXiv:2501.01721*, 2025.

[35] Z. Ren, J. Xu, L. Qiu, and D. W. K. Ng, "Secure cell-free integrated sensing and communication in the presence of information and sensing eavesdroppers," *IEEE Journal on Selected Areas in Communications*, 2024.

[36] H. Jia, R. Zhu, A. Sciarrone, and L. Ma, "Illegal Sensing Suppression for Integrated Sensing and Communication System," *IEEE Internet of Things Journal*, 2024.

[37] J. Zou, C. Masouros, F. Liu, and S. Sun, "Securing the sensing functionality in ISAC networks: An artificial noise design," *IEEE Transactions on Vehicular Technology*, 2024.

[38] P. Wojaczek, F. Colone, D. Cristallini, and P. Lombardo, "Reciprocal-filter-based STAP for passive radar on moving platforms," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 2, pp. 967–988, 2018.

[39] K. Han, S. Kang, and S. Hong, "Sub-Nyquist Sampling OFDM Radar," *IEEE Transactions on Radar Systems*, vol. 1, pp. 669–680, 2023.

[40] L. Wang, Z. Wei, L. Su, Z. Feng, H. Wu, and D. Xue, "Coherent compensation based ISAC signal processing for long-range sensing," in *2023 21st International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*. IEEE, 2023, pp. 689–695.

[41] G. Hakobyan and B. Yang, "A novel intercarrier-interference free signal processing scheme for OFDM radar," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5158–5167, 2017.

[42] R. F. Tigrek and P. Van Genderen, "Compensation of range migration for cyclically repetitive Doppler-sensitive waveform (OFDM)," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 46, no. 4, pp. 2118–2123, 2010.

[43] S. Mercier, S. Bidon, D. Roque, and C. Enderli, "Comparison of correlation-based OFDM radar receivers," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 6, pp. 4796–4813, 2020.

[44] E. Panayirci, M. T. Altabbaa, M. Uysal, and H. V. Poor, "Sparse channel estimation for OFDM-based underwater acoustic systems in Rician fading with a new OMP-MAP algorithm," *IEEE Transactions on Signal Processing*, vol. 67, no. 6, pp. 1550–1565, 2019.

[45] G. Cui, J. Liu, H. Li, and B. Himed, "Target detection for passive radar with noisy reference channel," in *2014 IEEE Radar Conference*. IEEE, 2014, pp. 0144–0148.

[46] M. K. Bączyk, K. Kulpa, P. Samczyński, and M. Malanowski, "The impact of reference channel SNR on targets detection by passive radars using DVB-T signals," in *2015 IEEE Radar Conference (RadarCon)*. IEEE, 2015, pp. 0708–0712.

[47] R. A. Altes, "Target position estimation in radar and sonar, and generalized ambiguity analysis for maximum likelihood parameter estimation," *Proceedings of the IEEE*, vol. 67, no. 6, pp. 920–930, 1979.

[48] L. De Martín, W. Van Rossum, D. Ribeiro, and L. Anitori, "Sidelobe mitigation in noise radar using sparse signal processing," *IEEE Aerospace and Electronic Systems Magazine*, vol. 35, no. 9, pp. 32–40, 2020.

[49] J. T. Rodriguez, F. Colone, and P. Lombardo, "Supervised reciprocal filter for OFDM radar signal processing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, no. 4, pp. 3871–3889, 2023.