Sensing-Assisted Eavesdropper Estimation: An ISAC Breakthrough in Physical Layer Security

Nanchi Su, *Graduate Student Member, IEEE*, Fan Liu, *Member, IEEE*, Christos Masouros, *Senior Member, IEEE*

Abstract—In this paper, we investigate the sensing-aided physical layer security (PLS) towards Integrated Sensing and Communication (ISAC) systems. A well-known limitation of PLS is the need to have information about potential eavesdroppers (Eves). The sensing functionality of ISAC offers an enabling role here, by estimating the directions of potential Eves to inform PLS. In our approach, the ISAC base station (BS) firstly emits an omnidirectional waveform to search for potential Eves' directions by employing the combined Capon and approximate maximum likelihood (CAML) technique. Using the resulting information about potential Eves, we formulate secrecy rate expressions, which is a function of the Eves' estimation accuracy. We then formulate a weighted optimization problem to simultaneously maximize the secrecy rate with the aid of the artificial noise (AN), and minimize the Cramér-Rao Bound (CRB) of targets'/Eves' estimation. By taking the possible estimation errors into account, we enforce a beampattern constraint with a wide main beam covering all possible directions of Eves. This implicates that security needs to be enforced in all these directions. By improving estimation accuracy, the sensing and security functionalities provide mutual benefits, resulting in improvement of the mutual performances with every iteration of the optimization, until convergence. Our results avail of these mutual benefits and reveal the usefulness of sensing as an enabler for practical PLS.

Index Terms—Integrated Sensing and Communication system, sensing aided physical layer security, Cramér-Rao Bound, secrecy rate, artificial noise.

I. INTRODUCTION

A. Background and Motivation

AS the 5G wireless networks are being rolled-out worldwide, emerging applications, such as connected cars, smart factories, and digital twins, highlight the limitations of existing network infrastructures [1]. These applications demand both increasingly high-quality communication as well as

N. Su is with Guangdong Provincial Key Laboratory of Aerospace Communication and Networking Technology, Harbin Institute of Technology (Shenzhen), Shenzhen 518055, China; with the Department of Electronic and Electrical Engineering, Southern University of Science and Technology, Shenzhen 518055, China; and also with the Department of Electronic and Electrical Engineering, University College London, London WC1E 7JE, U.K. (e-mail: nanchi.su.18@ucl.ac.uk)

C. Masouros is with the Department of Electronic and Electrical Engineering, University College London, London WC1E 7JE, U.K. (e-mail: chris.masouros@ieee.org).

F. Liu is with the Department of Electrical and Electronic Engineering, Southern University of Science and Technology, Shenzhen 518055, China (e-mail: liuf6@sustech.edu.cn).

high accuracy and robustness of sensing, it is well-recognized that the cooperation and co-design between communication and radar systems will play a significant role in the upcoming beyond 5G (B5G) and 6G eras.

At the early stage of the radar-communication (RadCom) system studies, the two systems were conceived to spectrally coexist with each other, thus easing the severe competition over the scarce spectrum resources [2], [3]. In the forthcoming B5G/6G eras, radio sensing and communications (S&C) are both evolving towards higher frequency bands and large-scale antenna arrays, which leads to striking similarities between S&C systems in terms of hardware architecture, channel characteristics, and information processing pipeline [4]. In light of this, the research on the coexistence of radar and communication systems has involved into dual-functional radar communication (DFRC) systems. The joint design of the S&C operations, in the form of Integrated Sensing and Communications (ISAC), have been initially proposed in [5]. ISAC systems are expected to achieve higher spectral and energy efficiencies, but most importantly, promote a new paradigm of integration for attaining mutual benefits from a co-design perspective, wherein the S&C functionalities can mutually assist each other. Benefiting from these two advantages, applications of ISAC have been extended to numerous emerging areas, including smart manufacturing, environmental monitoring, vehicular networks, as well as indoor services such as human activity recognition.

With the evolution of cellular networks, the security in mmWave ISAC systems is facing with great challenges because of the shared use of the spectrum and the broadcasting nature of wireless transmission [6]. On one hand, the Rician channels are widely employed in mmWave frequencies, containing the line of sight (LoS) component, which results in an inescapable correlation with the sensing channel. This is different from conventional physical layer security (PLS) studies in communication systems with the independent and identically distributed assumption between legitimate user channels and intercept channels [7]–[9]. On the other hand, in dual-functional waveform design, the confidential information intended for communication users (CUs) is embedded in radar probing signals. This makes it susceptible to being eavesdropped by the target of interest. In this case, a unique and interesting conflict arises from the radar functionality side. To be specific, the power is expected to be focused towards targets of interest to improve detectability, while the useful signal information has to be protected from being intercepted by the targets, which are acknowledged as Eves, as each of them is reckoned as a potential eavesdropper (Eve).

To secure confidential information in ISAC systems, exist-

ing approaches can be generally divided into the following categories, i.e., 1) Cryptography and 2) PLS. Conventionally, the security of communication systems is regarded as an independent feature and addressed at the upper layers of the protocol stack by deploying cryptographic technologies. The studies of cryptography commonly assume that the physical layer provides an error-free link [10], while the wireless links are vulnerable to attacks in practice, which would result in a high risk of information leakage. It is worth pointing out that 5G has already been a large-scale heterogeneous network with multiple levels and weakly-structured architectures, which makes it difficult to distribute and manage secret keys [11]. Also, complicated encryption/decryption algorithms cannot be straightforwardly applied considering the power consumption in 5G networks. Furthermore, even if the data is encrypted, the detection of a wireless link from a potential eavesdropper can reveal critical information. In contrast to complex cryptographic approaches, signal processing operations of PLS are usually simple with little additional overheads. A major limitation of PLS is the need to obtain some information for the potential Eves. This ranges from full CSI, to an SNR estimate of Eve's link, or Eve's direction as a minimum. This difficult-to-obtain information often renders PLS impractical.

To our best knowledge of existing literature, ISAC security has been studied in more complex scenarios in recent years. To be specific, the PLS was concerned with the non-orthogonal multiple access (NOMA)-ISAC system by maximizing the sum secrecy rate for multiple users via artificial jamming, where the superimposed signal for NOMA users can be concurrently employed for target detection [12]. Moreover, Reconfigurable Intelligent Surfaces (RIS) have been applied to enhance ISAC security [13]–[15]. In [14], the authors deployed an active RIS and designed the optimization problem to maximize the achievable secrecy rate of the system by jointly designing the radar receive beamformers, the active RIS reflection coefficients matrix, and the transmit beamformers. This work proved that the deployment of active RIS improves the secrecy performance compared with the passive RIS or no-RIS case. Also, the aerial eavesdroppers (AE) were considered in [16], where the ISAC BS emitted waveforms to track and jam the AE, which achieved a higher secrecy rate and better fairness performance. The optimization problem was formulated to jointly design radar signal and receiver beamformer for improving the secrecy performance based on the tracking information.

More relevant to this work, security in ISAC systems was initially studied in [17], where MIMO radar transmits two different signals, carrying desired information and false information, respectively, both of which are employed for sensing. Optimization problems were designed to maximize the secrecy rate for safeguarding communication data. As studied in [18], [19], the dual-functional base station (BS) detects targets and transmits information to CUs simultaneously, where each of the targets is regarded as a potential eavesdropper. In this scenario, the artificial noise (AN)-aided secure beamforming design enables the secure information transmission from the BS to CUs in ISAC systems. Specifically, AN is generated at the transmitter side to deteriorate the received signal at

each target/Eve, thus the decoding capability of which is destructed. To avoid the redundant power consumption caused by the added AN, the research in [20] proposed a symbol-level precoding algorithm to exploit constructive interference (CI) to aid detection from the legitimate users, and destructive interference (DI) to inhibit detection from the target/Eve. More recently, the encryption keys mechanism has been applied in PLS, where the filter band-based PLS algorithm was proposed to enable key generation by decomposing the received signal in parallel sub-bands, namely chirp modulation [21]. This method secured ISAC systems by improving the secret key generation rate efficiently, which however depends on the radio channel characteristics. Additionally, the information-theoretic study in [22] considered mitigating information leakage between sensing and communication operations in the ISAC system, where the inner and outer bounds for the secrecy-distortion region were derived under the assumption of perfect and partial output feedback.

B. Contributions

We note that in the above works on secure ISAC transmission, the radar and communication systems work individually over separate end-goals rather than cooperating with each other. To further promote the integration of S&C functionalities to improve the security of the ISAC systems, we propose a novel approach to ensure the PLS for communication data transmission, which is assisted by the sensing functionality. At the first stage, the dual-functional access point (AP) emits an omnidirectional waveform for Eve detection, which then receives echoes reflected from both CUs and Eves located within the sensing range. Suppose that all CUs are cooperative users. That is, the location information of each is acknowledged to the AP. Thus, it is possible to obtain angle estimates of Eves contained in the reflected echo by removing known CUs' angles. The estimation performance is measured by the Cramér-Rao Bound (CRB) [23].

In the next stage, we formulate a weighted optimization problem to minimize the CRB of targets/Eves and maximize the secrecy rate, subject to beampattern constraints as well as a transmit power budget. A key novelty in this setup is that the channel information in the secrecy rates, is a function of the sensing performance. Specifically, to avoid any false dismissal detection, the main lobe of the beampattern is designed to be wide, with a width depending on the estimation accuracy. Afterwards, by improving estimation accuracy, the sensing and security functionalities provide mutual benefits, resulting in improvement of the mutual performances with every iteration of the optimization, until convergence.

Within this scope, the contributions of our work are summarized as follows:

- We present a sensing-assisted PLS algorithm for the ISAC systems, where the sensing and secrecy performance are measured by the CRB and the secrecy rate, respectively. In particular, we first perform target detection via emitting an omnidirectional waveform. Then, we formulate a beamforming design problem that jointly improves the sensing accuracy and communication secrecy rate.

- We analyze the lower bound of CRB and the upper bound of the secrecy rate in our proposed ISAC system.
- We propose an alternative optimization algorithm that iteratively maximizes the determinant of the Fisher Information Matrix (FIM) and the secrecy rate with the aid of the AN. Specifically, the secrecy rate is updated with improved accuracy of the Eves' angle estimation.
- To improve the robustness of the proposed method, we further take into account the uncertainty of Eve's location. In such cases, the main beam of the sensing beampattern is designed to be sufficiently wide to cover the possible angular region where an Eve may appear with high probability. This region is indicated by the CRB value obtained from the previous iteration.
- We design a fractional programming (FP) algorithm to solve the proposed weighted optimization problem and verify the efficiency of the solver for both single-Eve and multi-Eve detection.

C. Organization

This paper is organized as follows. Section II gives the system model. Benchmark schemes including AN design techniques with unknown and statistically known Eve channel information are given in Section III. Section IV presents the approach to estimating Eves' parameters. Bounds for the metrics CRB and secrecy rate are given in Section V and the weighted optimization problem is accordingly designed for Eves' parameters estimation and communication data security in Section VI. Section VII provides numerical results, and Section VIII concludes the paper.

Notations: Unless otherwise specified, matrices are denoted by bold uppercase letters (i.e., $\mathbf{X}$), vectors are represented by bold lowercase letters (i.e., $\mathbf{x}$), and scalars are denoted by normal font (i.e., α). Subscripts indicate the location of the entry in the matrices or vectors (i.e., $s_{i,j}$ and l_n are the (i, j)-th and the n-th element in $\mathbf{S}$ and $\mathbf{l}$, respectively). $\mathrm{tr}\,(\cdot)$ and $\mathrm{vec}\,(\cdot)$ denote the trace and the vectorization operations. $(\cdot)^T$, $(\cdot)^H$ and $(\cdot)^*$ stand for transpose, Hermitian transpose and the complex conjugate of the matrices, respectively. $\mathrm{diag}\,(\cdot)$ represents the vector formed by the diagonal elements of the matrices and $\mathrm{rank}\,(\cdot)$ is rank operation. $\|\cdot\|$, $\|\cdot\|_\infty$ and $\|\cdot\|_F$ denote the l_2 norm, infinite norm and the Frobenius norm respectively. $\mathbb{E}\,\{\cdot\}$ denotes the statistical expectation.

II. SYSTEM MODEL

We consider a mmWave ISAC system equipped with co-located antennas and let N_t and N_r denote the number of transmit antennas and receive antennas, where the base station communicates with I communication users (CUs) and detects K targets/Eves simultaneously as depicted in Fig. 1. Note that the targets of interest are considered to be malicious, which intend to intercept the confidential information from the AP to the CUs. We assume the BS has knowledge of the CUs and their channels, and has no knowledge of the Eves.
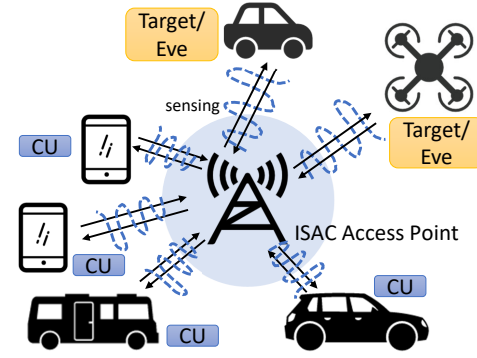
(a) Stage 1–The ISAC AP emits omnibeampattern for Eve estimations
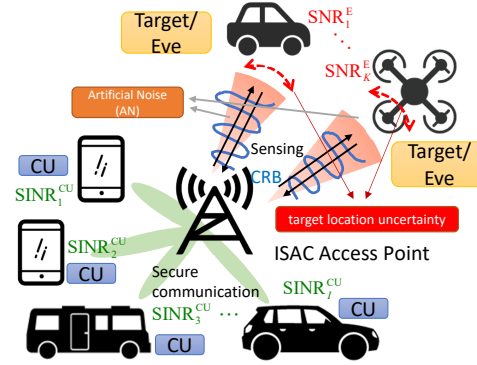
(b) Stage 2–Sensing-aided secure ISAC system

Fig. 1. Architecture of the proposed secure ISAC system assisted by the sensing functionality.

A. Communication Signal Model and Metrics

Let the rows of $\mathbf{X} \in \mathbb{C}^{N_t \times L}$ denote the transmit waveforms, where L is the number of time-domain snapshots. By transmitting the dual-functional waveforms to I CUs, the received signal matrix at the receivers can be expressed as

$$\mathbf{Y}_C = \mathbf{H}\mathbf{X} + \mathbf{Z}_C, \tag{1}$$

where $\mathbf{Z}_C \in \mathbb{C}^{I \times L}$ is the additive white Gaussian noise (AWGN) matrix and with the variance of each entry being σ_C^2. $\mathbf{H} = [\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_I]^H \in \mathbb{C}^{I \times N_t}$ represents the communication channel matrix, which is assumed to be known to the BS, with each entry being independently distributed. Following the typical mmWave channel model in [20], [24], we assume that $\mathbf{h}_i$ is a slow-fading block Rician fading channel. The channel vector of the i-th user can be expressed as

$$\mathbf{h}_i = \sqrt{\frac{v_i}{1 + v_i}}\mathbf{h}_{L,i}^{\mathrm{LoS}} + \sqrt{\frac{1}{1 + v_i}}\mathbf{h}_{S,i}^{\mathrm{NLoS}}, \tag{2}$$

where $v_i > 0$ is the Rician K-factor of the i-th user, $\mathbf{h}_{L,i}^{\mathrm{LoS}} = \sqrt{N_t}\mathbf{a}_t\,(\omega_{i,0})$ is the LoS deterministic component. $\mathbf{a}\,(\omega_{i,0})$ denotes the array steering vector, where $\omega_{i,0} \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ is the angle of departure (AOD) of the LoS component from the BS to the user i [24], [25]. The scattering component $\mathbf{h}_{S,i}^{\mathrm{NLoS}}$ can be expressed as $\mathbf{h}_{S,i}^{\mathrm{NLoS}} = \sqrt{\frac{N_t}{L_p}}\sum_{l=1}^{L_p} c_{i,l}\mathbf{a}_t\,(\omega_{i,l})$, where L_p denotes the number of propagation paths, $c_{i,l} \sim \mathcal{CN}\,(0, 1)$ is the complex path gain and $\omega_{i,l} \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ is the AOD

associated to the (i, l)-th propagation path.

The waveform $\mathbf{X}$ in (1) can be expressed as

$$\mathbf{X} = \mathbf{W}\mathbf{S} + \mathbf{N}, \tag{3}$$

where $\mathbf{W} \in \mathbb{C}^{N_t \times I}$ is the dual-functional beamforming matrix to be designed, each row of $\mathbf{S} \in \mathbb{C}^{I \times L}$ denotes the i-th unit-power data stream intended to CUs, and $\mathbf{N} \in \mathbb{C}^{N_t \times L}$ is the AN matrix generated by the transmitter to interfere potential eavesdroppers. We assume that $\mathbf{N} \sim \mathcal{CN}(\mathbf{0}, \mathbf{R}_N)$, where $\mathbf{R}_N \succeq \mathbf{0}$ denotes the covariance matrix of the AN that is to be designed. We further assume that the data streams are approximately orthogonal to each other, yielding

$$\frac{1}{L}\mathbf{S}_C\mathbf{S}_C^H \approx \mathbf{I}_{I \times I}. \tag{4}$$

Note that (4) is asymptotically achievable when L is sufficiently large. Then, we denote the beamforming matrix as $\mathbf{W} = [\mathbf{w}_1, \dots, \mathbf{w}_I]$, where each column $\mathbf{w}_i$ is the beamformer for the i-th CU. Accordingly, the SINR of the i-th user is given as

$$
\begin{aligned}
\mathrm{SINR}_i^{\mathrm{CU}} &= \frac{\left|\mathbf{h}_i^H \mathbf{w}_i\right|^2}{\sum\limits_{m=1, m\neq i}^{I} \left|\mathbf{h}_i^H \mathbf{w}_m\right|^2 + \left|\mathbf{h}_i^H \mathbf{R}_N \mathbf{h}_i\right| + \sigma_C^2} \\
&= \frac{\mathrm{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_i\right)}{\sum\limits_{m=1, m\neq i}^{I} \mathrm{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_m\right) + \mathrm{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + \sigma_C^2},
\end{aligned} \tag{5}
$$

where we denote $\tilde{\mathbf{H}}_i = \mathbf{h}_i \mathbf{h}_i^H$ and $\tilde{\mathbf{W}}_i = \mathbf{w}_i \mathbf{w}_i^H$.

B. Radar Signal Model

We here consider targets of interest associated with a particular range bin. Targets in adjacent range bins contribute as interference to the range bin of interest [26]. By emitting the waveform $\mathbf{X}$ to sense Eves, the reflected echo signal matrix at the BS receive array is given as

$$\mathbf{Y}_R = \sum_{k=1}^{K} \mathbf{a}(\theta_k) \beta_k \mathbf{b}^H(\theta_k) \mathbf{X} + \mathbf{Z}_R, \tag{6}$$

where $\mathbf{a}(\theta) \in \mathbb{C}^{N_r \times 1}$ and $\mathbf{b}(\theta) \in \mathbb{C}^{N_t \times 1}$ represent the steering vectors for the receive and transmit arrays, which are assumed to be a uniform linear array (ULA) with half-wavelength antenna spacing. β_k is the complex amplitude of the k-th Eve. We assume the number of antennas is even and define the receive steering vector as

$$\mathbf{a}(\theta) = \left[e^{-j\frac{N_r-1}{2}\pi\sin\theta}, e^{-j\frac{N_r-3}{2}\pi\sin\theta}, \cdots, e^{j\frac{N_r-1}{2}\pi\sin\theta}\right]^T. \tag{7}$$

It is noted that we choose the center of the ULA antennas as the reference point. To this end, it is easy to verify that

$$\mathbf{a}^H(\theta)\dot{\mathbf{a}}(\theta) = 0. \tag{8}$$

Finally, $\mathbf{Z}_R$ denotes the interference and the AWGN term. We assume that the columns of $\mathbf{Z}_R$ are independent and identically distributed circularly symmetric complex Gaussian random vectors with mean zero and a covariance matrix $\mathbf{Q} = \sigma_R^2 \mathbf{I}$.

Similar to the expression in (5), the eavesdropping SINR received at the k-th Eve regarding the i-th CU is written as

$$\mathrm{SINR}_{k,i}^{\mathrm{E}} = \frac{|\alpha_k|^2 \mathbf{b}^H(\theta_k) \tilde{\mathbf{W}}_i \mathbf{b}(\theta_k)}{|\alpha_k|^2 \mathbf{b}^H(\theta_k)\left(\sum\limits_{\substack{\bar{m}=1, \\ \bar{m}\neq i}}^{I} \tilde{\mathbf{W}}_{\bar{m}} + \mathbf{R}_N\right)\mathbf{b}(\theta_k) + \sigma_0^2}, \tag{9}$$

where α_k denotes the complex path-loss coefficient of the k-th target and σ_0^2 denotes the covariance of AWGN received by each Eve.

For simplicity, the reflected echo signal given in (6) can be recast as

$$\mathbf{Y} = \mathbf{A}(\boldsymbol{\theta}) \boldsymbol{\Lambda} \mathbf{B}^H(\boldsymbol{\theta}) \mathbf{X} + \mathbf{Z}_R, \tag{10}$$

where we denote $\mathbf{A}(\boldsymbol{\theta}) = [\mathbf{a}(\theta_1), \dots, \mathbf{a}(\theta_K)]$, $\mathbf{B}(\boldsymbol{\theta}) = [\mathbf{b}(\theta_1), \dots, \mathbf{b}(\theta_K)]$, and $\boldsymbol{\Lambda} = \mathrm{diag}(\beta_k)$.

C. CRB and Secrecy Rate

In this subsection, we elaborate on the radar detection and communication security metrics. Particularly, the target/Eve estimation is measured by the CRB, which is a lower bound on the variance of unbiased estimators [27], and the security performance is evaluated by the secrecy rate.

In the multi-Eve detection scenario, the CRB with respect to the unknown Eve parameters $\theta_1, \dots, \theta_K$ and $\beta_1, \dots, \beta_K$ was derived in [28] in detail, and the FIM for $\theta_k, \forall k$ as well as real and imaginary parts of $\beta_k, \forall k$ is given as

$$\mathbf{J} = 2L \begin{bmatrix} \mathrm{Re}(\mathbf{J}_{11}) & \mathrm{Re}(\mathbf{J}_{12}) & -\mathrm{Im}(\mathbf{J}_{12}) \\ \mathrm{Re}^T(\mathbf{J}_{12}) & \mathrm{Re}(\mathbf{J}_{22}) & -\mathrm{Im}(\mathbf{J}_{22}) \\ -\mathrm{Im}^T(\mathbf{J}_{12}) & -\mathrm{Im}^T(\mathbf{J}_{22}) & \mathrm{Re}(\mathbf{J}_{22}) \end{bmatrix}, \tag{11}$$

where the elements of the matrix in (11) are given in (12) at the top of next page with $\odot$ denoting the Hadamard (element-wise) matrix product, and $\dot{\mathbf{A}} = \left[\begin{array}{cccc} \frac{\partial \mathbf{a}(\theta_1)}{\partial \theta_1} & \frac{\partial \mathbf{a}(\theta_2)}{\partial \theta_2} & \cdots & \frac{\partial \mathbf{a}(\theta_K)}{\partial \theta_K} \end{array}\right]$, $\dot{\mathbf{B}} = \left[\begin{array}{cccc} \frac{\partial \mathbf{b}(\theta_1)}{\partial \theta_1} & \frac{\partial \mathbf{b}(\theta_2)}{\partial \theta_2} & \cdots & \frac{\partial \mathbf{b}(\theta_K)}{\partial \theta_K} \end{array}\right]$. Also, the covariance matrix $\mathbf{R}_X$ is given as

$$
\begin{aligned}
\mathbf{R}_X &= \frac{1}{L}\mathbf{X}\mathbf{X}^H = \mathbf{W}\mathbf{W}^H + \mathbf{R}_N \\
&= \sum_{i=1}^{I} \tilde{\mathbf{W}}_i + \mathbf{R}_N.
\end{aligned} \tag{13}
$$

As per the above, the corresponding CRB matrix is expressed as

$$\mathrm{CRB}(\boldsymbol{\theta}, \boldsymbol{\beta}) = \mathbf{J}^{-1} \tag{14}$$

and

$$
\begin{aligned}
\mathrm{CRB}(\boldsymbol{\theta}) &= \left[\mathbf{J}^{-1}\right]_{11} \\
\mathrm{CRB}(\boldsymbol{\beta}) &= \left[\mathbf{J}^{-1}\right]_{22} + \left[\mathbf{J}^{-1}\right]_{33}.
\end{aligned} \tag{15}
$$

Moreover, the achievable secrecy rate at the legitimate user is defined as the difference between the achievable rates at the legitimate receivers and the eavesdroppers. Thus, we give the expression of the worst-case secrecy rate as [19], [29]

$$\mathrm{SR}\left(\tilde{\mathbf{W}}_i, \mathbf{R}_N\right) = \min_{i,k}\left[R_i^{\mathrm{CU}} - R_{k,i}^{\mathrm{E}}\right]^+, \tag{16}$$

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.2023.3306029

5

$$\mathbf{J}_{11} = \left(\dot{\mathbf{A}}^H \mathbf{Q}^{-1} \dot{\mathbf{A}}\right) \odot \left(\mathbf{\Lambda}^* \mathbf{B}^H \mathbf{R}_X^* \mathbf{B}\mathbf{\Lambda}\right) + \left(\dot{\mathbf{A}}^H \mathbf{Q}^{-1} \mathbf{A}\right) \odot \left(\mathbf{\Lambda}^* \mathbf{B}^H \mathbf{R}_X^* \dot{\mathbf{B}}\mathbf{\Lambda}\right) + \left(\mathbf{A}^H \mathbf{Q}^{-1} \dot{\mathbf{A}}\right) \odot \left(\mathbf{\Lambda}^* \dot{\mathbf{B}}^H \mathbf{R}_X^* \mathbf{B}\mathbf{\Lambda}\right) +$$
$$\left(\mathbf{A}^H \mathbf{Q}^{-1} \mathbf{A}\right) \odot \left(\mathbf{\Lambda}^* \dot{\mathbf{B}}^H \mathbf{R}_X^* \dot{\mathbf{B}}\mathbf{\Lambda}\right) \tag{12a}$$

$$\mathbf{J}_{12} = \left(\dot{\mathbf{A}}^H \mathbf{Q}^{-1} \mathbf{A}\right) \odot \left(\mathbf{\Lambda}^* \mathbf{B}^H \mathbf{R}_X^* \mathbf{B}\right) + \left(\mathbf{A}^H \mathbf{Q}^{-1} \mathbf{A}\right) \odot \left(\mathbf{\Lambda}^* \dot{\mathbf{B}}^H \mathbf{R}_X^* \mathbf{B}\right) \tag{12b}$$

$$\mathbf{J}_{22} = \left(\mathbf{A}^H \mathbf{Q}^{-1} \mathbf{A}\right) \odot \left(\mathbf{B}^H \mathbf{R}_X^* \mathbf{B}\right) \tag{12c}$$

---

where $R_i^{\text{CU}}, \forall\, i$ and $R_k^{\text{E}}, \forall\, k$ represent the achievable transmission rate of the i-th CU and the k-th Eve, which can be expressed as (17a) and (17b), respectively.

$$R_i^{\text{CU}}\left(\tilde{\mathbf{W}}_i, \mathbf{R}_N\right) = \log\left(1 + \text{SINR}_i^{\text{CU}}\right) \tag{17a}$$

$$R_{k,i}^{\text{E}}\left(\tilde{\mathbf{W}}_i, \mathbf{R}_N\right) = \log\left(1 + \text{SINR}_{k,i}^{\text{E}}\right). \tag{17b}$$

III. BENCHMARK SCHEMES: ISOTROPIC AN-AIDED SECURE BEAMFORMING AND EVE-AWARD AN DESIGN

In the scenario considered with no knowledge of the Eves, a typical method to avoid the information inception is to transmit AN. To be specific, partial transmit power is allocated to emit the AN to interfere with the Eves, where the AN is isotropically distributed on the orthogonal complement subspace of CUs' channels [30]. To elaborate on this, we firstly take the l-th snapshot as a reference, i.e., (1) is simplified as

$$\mathbf{y}_C[l] = \mathbf{H}\mathbf{x}[l] + \mathbf{z}_C[l]. \tag{18}$$

where $\mathbf{x}[l] = \mathbf{W}\mathbf{s}[l] + \mathbf{n}[l]$. For simplicity, the snapshot index l will be omitted in the following descriptions. We further rewrite the AN vector $\mathbf{n}$ as

$$\mathbf{n} = \mathbf{V}\bar{\mathbf{n}}, \tag{19}$$

where $\mathbf{V} = \mathbf{P}_{\mathbf{H}}^\perp = \mathbf{I}_{N_t} - \mathbf{H}^H\left[\mathbf{H}\mathbf{H}^H\right]^{-1}\mathbf{H}$ denotes the orthogonal complement projector of the $\mathbf{H}$, and $\bar{\mathbf{n}}$ is the zero-mean colored noise vector with a covariance matrix $\mathbf{R}_{\bar{\mathbf{n}}} = \mathbb{E}\left\{\bar{\mathbf{n}}\bar{\mathbf{n}}^H\right\}$ [31], [32]. Accordingly, the covariance matrix is given as

$$\bar{\mathbf{R}}_x = \sum_{i=1}^{I} \tilde{\mathbf{W}}_i + \mathbf{V}\mathbf{R}_{\bar{\mathbf{n}}}\mathbf{V}^H. \tag{20}$$

Then, the received signal vector of legitimate CUs is written as

$$\mathbf{y}_C = \mathbf{H}\mathbf{W}\mathbf{s} + \mathbf{z}_C. \tag{21}$$

It is noted that the AN does not interfere with the CUs' channels and the SINR of the i-th user is given as

$$\overline{\text{SINR}}_i^{\text{CU}} = \frac{\text{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_i\right)}{\sum\limits_{m=1, m\neq i}^{I} \text{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_m\right) + \sigma_C^2}. \tag{22}$$

Likewise, the eavesdropping SINR of the k-th Eve on the i-th CU is given as

$$\overline{\text{SINR}}_{k,i}^{\text{E}} = \frac{\mathbb{E}\left\{\mathbf{g}_k^H \mathbf{w}_i \mathbf{s}\right\}}{\mathbb{E}\left\{\mathbf{g}_k^H \sum\limits_{\substack{\tilde{m}=1,\\ \tilde{m}\neq i}}^{I} \mathbf{w}_{\tilde{m}}\mathbf{s}\right\} + \mathbb{E}\left\{\mathbf{g}_k^H \mathbf{n}\right\} + \sigma_0^2}$$

$$= \frac{\mathbf{g}_k^H \tilde{\mathbf{W}}_i \mathbf{g}_k}{\mathbf{g}_k^H \sum\limits_{\substack{\tilde{m}=1,\\ \tilde{m}\neq i}}^{I} \tilde{\mathbf{W}}_{\tilde{m}} \mathbf{g}_k + \mathbf{g}_k^H \mathbf{V}\mathbf{R}_{\bar{n}}\mathbf{V}^H \mathbf{g}_k + \sigma_0^2}$$

$$= \frac{\text{tr}\left(\mathbf{G}_k \tilde{\mathbf{W}}_i\right)}{\text{tr}\left(\mathbf{G}_k \sum\limits_{\substack{\tilde{m}=1,\\ \tilde{m}\neq i}}^{I} \tilde{\mathbf{W}}_{\tilde{m}}\right) + \text{tr}\left(\mathbf{G}_k \mathbf{V}\mathbf{R}_{\bar{n}}\mathbf{V}^H\right) + \sigma_0^2}, \tag{23}$$

where $\mathbf{g}_k$ denotes the channel from the transmitter to the k-th Eve. Note that the covariance matrix of the colored noise vector, i.e., $\mathbf{R}_{\bar{n}}$, is set as the identity matrix when Eves' channels are unknown to the ISAC BS.

A. AN Refinement Based on Eves' Information

The AN design could be further refined if more information about Eve's channels $\mathbf{g}_k$ is known to the BS. In this case, we assume that the instantaneous channel realizations of Eves are known to the transmitter, which is defined as $\mathbf{G}_k = \mathbb{E}\left\{\mathbf{g}_k\mathbf{g}_k^H\right\} = \bar{\mathbf{g}}_k\bar{\mathbf{g}}_k^H + \sigma_{G,k}^2\mathbf{I}_{N_t}$, where $\bar{\mathbf{g}}_k$ and $\sigma_{G,k}^2\mathbf{I}_{N_t}$ denote the mean and covariance matrix of $\mathbf{g}_k$, respectively. In particular, to obtain a fair comparison with our approach that assumes no Eves' information, we consider the extreme setting that $\mathbf{G}_k = \sigma_{g,k}^2\mathbf{I}_{N_t}, \sigma_{g,k}^2 > 0$. Besides, we assume that $\mathbf{g}_k$ and $\mathbf{s}$ are independent and identically distributed (i.i.d.) [33]. To this end, the expression of the secrecy rate can be accordingly obtained as given in Section II-C, which is written as

$$\text{SR}_{\text{IST}} = \min_{i,k}\left[\log\left(1 + \overline{\text{SINR}}_i^{\text{CU}}\right) - \log\left(1 + \overline{\text{SINR}}_{k,i}^{\text{E}}\right)\right]^+. \tag{24}$$

In light of the above assumptions, the secrecy rate maximization problem with the omnidirectional beampattern design is given as

$$\max_{\tilde{\mathbf{W}}_i, \mathbf{R}_{\bar{n}}} \quad \text{SR}_{\text{IST}}$$
$$\text{s.t.} \quad \bar{\mathbf{R}}_X = \frac{P_0}{N_t}\mathbf{I}_{N_t} \tag{25}$$
$$\tilde{\mathbf{W}}_i \succeq \mathbf{0}, \mathbf{R}_{\bar{n}} \succeq \mathbf{0}, \forall i.$$

Note that the non-convexity of the problem above only lies in the objection function, while it can be regarded as a typical secrecy rate maximization problem, which has been solved efficiently as studied in [34], [35]. We further apply the eigenvalue decomposition or Gaussian randomization procedure to make sure the resulting beamforming matrix $\tilde{\mathbf{W}}_i$ is rank-1. The simulation results will be given in Section VII as benchmarks.

IV. EVES' PARAMETERS ESTIMATION

To avoid redundancy, we briefly present the method to estimate amplitudes and angles of Eves based on our signal models proposed in Section II, namely the combined Capon and approximate maximum likelihood (CAML) approach [36], [37]. Specifically, Capon is initially applied to estimate the peak directions, and then approximate maximum likelihood (AML) is used to estimate the amplitudes of all Eves.

We firstly give the expression of signal model $\mathbf{Y}$ [38], where we let $\hat{\theta}_k, k = 1, \ldots, K$ denote the estimated Eves' directions. Similar to the receive signal model in (6), we here have

$$\mathbf{Y} = \mathbf{A}^* \left(\hat{\boldsymbol{\theta}} \right) \hat{\boldsymbol{\Lambda}} \mathbf{B}^T \left(\hat{\boldsymbol{\theta}} \right) \mathbf{X} + \tilde{\mathbf{Z}}, \tag{26}$$

where $\hat{\boldsymbol{\Lambda}} = \operatorname{diag} \left[\beta \left(\hat{\theta}_1 \right), \ldots, \beta \left(\hat{\theta}_K \right) \right]$ and $\tilde{\mathbf{Z}}$ denotes the residual term. By employing the AML algorithm, the estimate of amplitudes can be written in a closed form given as [37]

$$\boldsymbol{\beta} = \frac{1}{L} \left[\left(\mathbf{A}^H \mathbf{T}^{-1} \mathbf{A} \right) \odot \left(\mathbf{B}^H \hat{\mathbf{R}}_X^* \mathbf{B} \right) \right]^{-1} \cdot \operatorname{vecd} \left(\mathbf{A}^H \mathbf{T}^{-1} \mathbf{Y} \mathbf{X}^H \mathbf{B}^* \right), \tag{27}$$

where $\operatorname{vecd}(\cdot)$ denotes a column vector with the elements being the diagonal of a matrix and

$$\mathbf{T} = L \hat{\mathbf{R}} - \frac{1}{L} \mathbf{Y} \mathbf{X}^H \mathbf{B}^* \left(\mathbf{B}^T \hat{\mathbf{R}}_X \mathbf{B}^* \right)^{-1} \mathbf{B}^T \mathbf{X} \mathbf{Y}^H, \tag{28}$$

where $\hat{\mathbf{R}}$ is the sample covariance of the observed data samples and $\hat{\mathbf{R}} = \frac{1}{L} \mathbf{Y} \mathbf{Y}^H$.

At the first step of the Eve parameter estimation, we design our transmission so that the AP emits an omnidirectional waveform, which is usually employed by the MIMO radar for initial probing. Thus, the covariance matrix is given as $\hat{\mathbf{R}}_X = \frac{P_0}{N_t} \mathbf{I}_{N_t}$. The CRBs for angles and amplitudes of targets can be accordingly calculated by substituting $\tilde{\mathbf{R}}_X$ into (12) and (15), where we denote them as $\operatorname{CRB}_0 \left(\hat{\boldsymbol{\theta}} \right)$ and $\operatorname{CRB}_0 \left(\hat{\boldsymbol{\beta}} \right)$. Assume that the probability density function (PDF) of the angle estimated error is modeled as Gaussian distribution, zero mean and a variance of $\operatorname{CRB}_0 \left(\hat{\boldsymbol{\theta}} \right)$. That is, $\mathrm{E}_{est,k} \sim \mathcal{CN} \left(0, \operatorname{CRB}_0 \left(\hat{\theta}_k \right) \right)$, where $\mathrm{E}_{est,k}$ denotes the angle estimation error of the k-th Eve. As a consequence, the probability that the real direction of the k-th Eve falls in the range $\Xi_k^{(0)} = \left[\hat{\theta}_k - 3 \sqrt{\operatorname{CRB}_0 \left(\hat{\theta}_k \right)}, \hat{\theta}_k + 3 \sqrt{\operatorname{CRB}_0 \left(\hat{\theta}_k \right)} \right]$ is approximately 0.9973 [39]. Thus, the main lobe width of the radar beampattern will be initially designed as $\Xi^{(0)}$, and then it will be iteratively updated based on the optimized CRB.

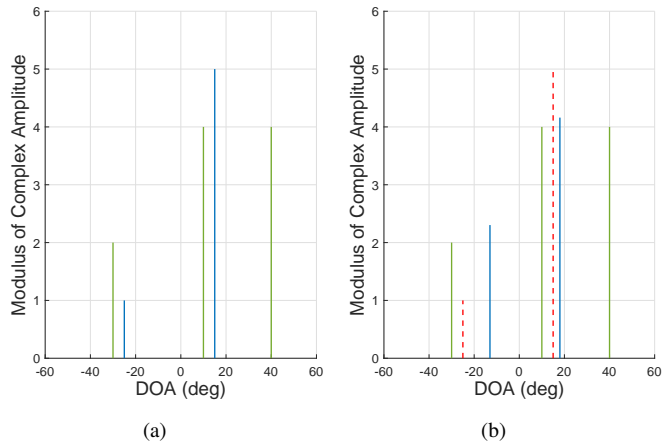For clarity, we present the spatial spectrum of the direction

Fig. 2. Spatial spectral estimates with CAML approach, when Eves locate at $\theta_1 = -25°, \theta_2 = 15°$ (blue lines), and CUs locate at $\theta_3 = 40°, \theta_4 = 10°$ and $\theta_5 = -30°$ (green lines). (a) SNR=20 dB. (b) SNR=-15 dB, where the red dashed lines denote Eves' real directions and amplitudes. Note that the CUs' information is known to the BS as they are assumed to be cooperative receivers.
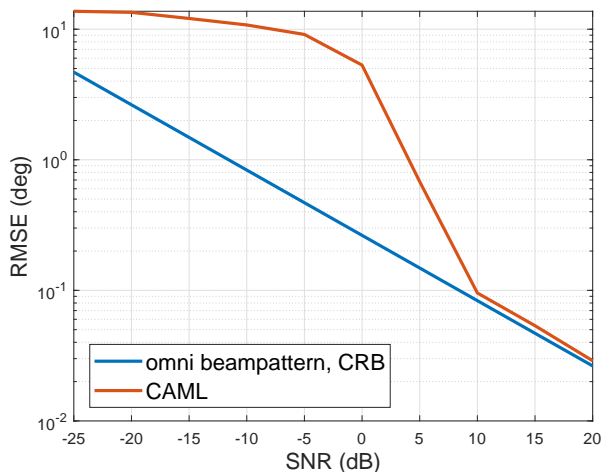

Fig. 3. Target/Eve estimation performance by applying CAML method, with the CRB obtained by omnidirectional beampattern design as a benchmark.

of angle (DOA) estimation by deploying the CAML technique in Fig. 2. It is assumed that two Eves are located at $\theta_1 = -25°, \theta_2 = 15°$ (denoted by blue lines) and three CUs locate at $\theta_3 = 40°, \theta_4 = 10°, \theta_5 = -30°$ (denoted by green lines), with the modulus of complex amplitudes $\beta_1 = 1, \beta_2 = 5, \beta_3 = 4, \beta_4 = 5$ and $\beta_5 = 2$, where directions of CUs are known to the transmitter. Fig. 2(a) and Fig. 2(b) demonstrate the CAML performance when SNR=20dB and SNR=-15dB, respectively. It is noted that the CAML approach estimates the DOA precisely when SNR is 20dB, while errors of the angle estimation happen when the SNR decreases to -15 dB. To further illustrate the performance of the CAML estimation method, the root mean square error (RMSE) versus the SNR of the echo signal is shown in Fig. 3 with the CRB as a baseline. As expected, the CRB is shown as the lower bound of the RMSE obtained by CAML estimation, in particular, the CRB gets tight in the high-SNR regime.

V. BOUNDS FOR CRB AND SECRECY RATE

The design of a weighted optimization between the radar CRB and the communication secrecy rate presents the challenge that the two performance metrics have different units and potentially different magnitudes. To overcome this challenge we need to normalize them each with their respective upper/lower bound. To obtain these bounds, in this section we present the CRB minimization problem and the secrecy rate maximization problem with the system power budget constraint. Considering the further design of the weighted objective function in the following section, the CRB minimization problem can be approximated as the FIM determinant maximization problem. To this end, the optimal solutions generate the upper bounds of the FIM determinant and the secrecy rate, both of which will be employed to normalize the metrics in Section VI.

A. Upper-bound of the FIM Determinant

We denote $\boldsymbol{\eta}$ as the sensing parameters, thus the MSE can be expressed as $\mathbf{M}\left(\boldsymbol{\eta}\right) \triangleq \mathbb{E}\left\{\left(\boldsymbol{\eta} - \hat{\boldsymbol{\eta}}\right)\left(\boldsymbol{\eta} - \hat{\boldsymbol{\eta}}\right)^T\right\} \succeq \mathbf{J}^{-1}$. For the m-th parameter η_m to be estimated, it has $\mathbb{E}\left\{\left\|\eta_m - \hat{\eta}_m\right\|^2\right\} \geq \left[\mathbf{J}^{-1}\right]_{mm}$ [40]. Thus, it is common to minimize the trace or the determinant of the CRB matrix, i.e., $\operatorname{tr}\left(\mathbf{J}^{-1}\right)$ or $\left|\mathbf{J}^{-1}\right|$. Since the CRB matrix is the inverse of the FIM matrix, the problem of minimizing $\left|\mathbf{J}^{-1}\right|$ is equivalent to maximizing $|\mathbf{J}|$, which is given as [28]

$$\max_{\tilde{\mathbf{W}}_i, \mathbf{R}_N} \quad |\mathbf{J}| \tag{29a}$$

$$\text{s.t.} \quad \mathbf{R}_N \succeq \mathbf{0}, \tilde{\mathbf{W}}_i \succeq \mathbf{0}, \forall i \tag{29b}$$

$$\operatorname{tr}\left(\sum_{i=1}^{I} \tilde{\mathbf{W}}_i + \mathbf{R}_N\right) = P_0, \tag{29c}$$

where P_0 denotes the power budget of the proposed system. It is noted that the optimization above is convex and can be efficiently solved by CVX toolbox [41], [42]. Consequently, by substituting the optimal $\tilde{\mathbf{W}}_i, \mathbf{R}_N$ in (11), the upper-bound of FIM determinant is obtained.

B. Secrecy Rate Bound

To derive the upper bound of the secrecy rate, we only consider the communication security metric in this subsection. Assuming that the CSI is perfectly known to the BS, the secrecy rate maximization problem can be formulated as

$$\text{SR}^\star = \max_{\tilde{\mathbf{W}}_i, \mathbf{R}_N} \min_{i,k} \text{SR}\left(\tilde{\mathbf{W}}_i, \mathbf{R}_N\right) \tag{30a}$$

$$\text{s.t.} \quad (29b), (29c). \tag{30b}$$

It is noted that the non-convexity lies in the objective function of (30), which makes the optimization problem above difficult to solve. To resolve this issue, we introduce an auxiliary

variable b, where (30) has the same optimal solutions as the reformulation below

$$\text{SR}^\star = \max_{\tilde{\mathbf{W}}_i, \mathbf{R}_N, b} \min_{i,k} \left[R_i^{\text{CU}}\left(\tilde{\mathbf{W}}_i, \mathbf{R}_N\right) - \log b\right]$$

s.t.

$$\log\left(1 + \frac{|\alpha_k|^2 \mathbf{b}^H\left(\theta_k\right) \tilde{\mathbf{W}}_i \mathbf{b}\left(\theta_k\right)}{|\alpha_k|^2 \mathbf{b}^H\left(\theta_k\right)\left(\sum_{\substack{\bar{m}=1, \\ \bar{m} \neq i}}^{I} \tilde{\mathbf{W}}_{\bar{m}} + \mathbf{R}_N\right) \mathbf{b}\left(\theta_k\right) + 1}\right) \leq \log b, \forall k, i$$

$$(29b), (29c). \tag{31}$$

The above problem can be simply relaxed into a convex SDP problem. For brevity, we refer readers to [35] for more details.

VI. WEIGHTED OPTIMIZATION FOR EVES' ESTIMATION AND SECURE COMMUNICATION

In this section, we propose a normalized weighted optimization problem that reveals the performance tradeoff between the communication security and Eve parameters estimation. Additionally, recall that the ISAC access point firstly emits an omnidirectional beampattern as given in Section IV, where imprecise angles of Eves have been obtained at the given SNR, with the angular uncertainty interval of the k-th Eve is denoted as $\Xi_k^{(0)}$. To reduce angle estimation errors, we also take the wide main beam design into account, which covers all possible directions of Eves.

A. Problem Formulation

To achieve the desired tradeoff between the communication data security and the radar estimation CRB, while taking the estimation errors of Eves' angles and the system power budget into account, we formulate the weighted optimization problem as follows

$$\max_{\tilde{\mathbf{W}}_i, \mathbf{R}_N} \quad \rho \frac{|\mathbf{J}|}{|\mathbf{J}|_{UB}} + (1-\rho)\frac{\text{SR}}{\text{SR}_{UB}} \tag{32a}$$

$$\text{s.t.} \quad \mathbf{b}^H\left(\vartheta_{k,0}\right)\mathbf{R}_X \mathbf{b}\left(\vartheta_{k,0}\right) - \mathbf{b}^H\left(\vartheta_{k,p}\right)\mathbf{R}_X \mathbf{b}\left(\vartheta_{k,p}\right) \geq \gamma_s,$$
$$\forall \vartheta_{k,p} \in \operatorname{card}\left(\Psi_k\right), \forall k \tag{32b}$$

$$\mathbf{b}^H\left(\vartheta_{k,n}\right)\mathbf{R}_X \mathbf{b}\left(\vartheta_{k,n}\right) \leq$$
$$(1+\alpha)\mathbf{b}^H\left(\vartheta_{k,0}\right)\mathbf{R}_X \mathbf{b}\left(\vartheta_{k,0}\right), \forall \vartheta_{k,n} \in \operatorname{card}\left(\Omega_k\right), \forall k \tag{32c}$$

$$\mathbf{b}^H\left(\vartheta_{k,n}\right)\mathbf{R}_X \mathbf{b}\left(\vartheta_{k,n}\right) \geq$$
$$(1-\alpha)\mathbf{b}^H\left(\vartheta_{k,0}\right)\mathbf{R}_X \mathbf{b}\left(\vartheta_{k,0}\right), \forall \vartheta_{k,n} \in \operatorname{card}\left(\Omega_k\right), \forall k \tag{32d}$$

$$(29b), (29c), \tag{32e}$$

where $|\mathbf{J}|_{UB}$ and SR_{UB} denote the upper bounds of the FIM matrix determinant and the secrecy rate which were obtained in Section V, respectively. γ_s denotes the given threshold to constrain the power of the sidelobe. $0 \leq \rho \leq 1$ denotes

$$\max_{\tilde{\mathbf{W}}_i, \mathbf{R}_N} \frac{\rho}{|\mathbf{J}|_{UB}} |\mathbf{J}| + \frac{1-\rho}{\mathrm{SR}_{UB}} \min_{i,k,n} \left[R_i^{\mathrm{CU}}\left(\tilde{\mathbf{W}}_i, \mathbf{R}_N\right) - \log\left(1 + \frac{|\alpha_k|^2 \mathbf{b}^H\left(\vartheta_{k,n}\right) \tilde{\mathbf{W}}_i \mathbf{b}\left(\vartheta_{k,n}\right)}{|\alpha_k|^2 \mathbf{b}^H\left(\vartheta_{k,n}\right) \left(\sum_{\substack{\bar{m}=1,\\ \bar{m}\neq i}}^{I} \tilde{\mathbf{W}}_{\bar{m}} + \mathbf{R}_N \right) \mathbf{b}\left(\vartheta_{k,n}\right) + 1}\right) \right]^+ ,$$

$$\vartheta_{k,n} \in \mathrm{card}\left(\Omega_k\right), \forall\, k,i \quad \text{(33a)}$$

s.t. $(32b),(32c),(32d)$ and $(32e)$. (33b)

Algorithm 1 Iterative optimization of the CRB and the secrecy rate

Initialization: $\Xi_k^{(0)}$ obtained from initial target/Eve estimation and CRB in Section IV; $r = 1$
1: **repeat**
2:    $\Omega_k^{(r)} = \Xi_k^{(r-1)}$, $\Psi_k^{(r)}$ is accordingly obtained;
3:    substitute $\Omega_k^{(r)}$ and $\Psi_k^{(r)}$ into problem (32);
4:    **repeat**
5:      solve problem (32) by FP algorithm;
6:    **until** find the optimal $c \in \left[\left(\min_i\ 1 + P_0\|\mathbf{h}_i\|^2\right)^{-1}, 1 \right]$ which generates the maximum value of the objective function deploying the golden search;
7:    the optimal variables $\tilde{\mathbf{W}}_i^\star, \mathbf{R}_N^\star$ are obtained;
8:    calculate the $\mathrm{CRB}_r\left(\hat{\theta}\right)$ and the secrecy rate in the r-th iteration;
9:    $\Xi_k^{(r)}$ can be accordingly obtained;
10:    update $r = r + 1$,
11: **until** Convergence.

---

the weighting factor that determines the weights for the Eve estimation performance and the secrecy rate. α denotes a given scalar associated with the wide main beam fluctuation. $\vartheta_{k,n}$ is the n-th possible direction of the k-th Eve, $\vartheta_{k,0}$ is the angle which was estimated by the algorithm proposed in Section IV. Ω_k and Φ_k denote the main beam region and sidelobe region, respectively. Note that $\mathrm{card}\left(\cdot\right)$ denotes the the cardinality of $(\cdot)$.

Remark 1. *It is important to highlight that the secrecy rate given by (16) is a function of the estimation accuracy of Eve's parameters, including θ_k and α_k. Accordingly, beyond the tradeoff in the weighted optimization in this section, the improvement in the sensing performance directly results in an improvement in the secrecy performance.*

B. Efficient Solver

To tackle problem (32), we firstly recast the complicated secrecy rate term in the objective function. For simplicity, we denote $\Sigma_i = \sum_{m=1}^I \mathrm{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_m\right)$ and rewrite the optimization problem as (33). According to [35], the weighted optimization

problem can be recast as (34) by introducing the scalar b. Problem (34) is shown at the top of the next page.

It is noted that the min operator only applies to the second term of the objective function of problem (34). According to the Fractional Programming (FP) algorithm [43], the optimization problem can be further reformulated by replacing the fraction term with the coefficient z, which is given as

$$\max_{\tilde{\mathbf{W}}_i, \mathbf{R}_N, \mathbf{y}, z} \frac{\rho}{|\mathbf{J}|_{UB}} |\mathbf{J}| + \frac{1-\rho}{2^{SR_{UB}}} z \quad \text{(35a)}$$

$$\text{s.t.}\quad 2y_i\sqrt{\Sigma_i + \mathrm{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1} -$$
$$y_i^2 \left(b\left(\Sigma_i - \mathrm{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_i\right) + \mathrm{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1\right)\right) \geq z,$$
$$\forall\, i \quad \text{(35b)}$$

$$(34b),(32b),(32c),(32d)\ \text{and}\ (32e), \quad \text{(35c)}$$

where $\mathbf{y}$ denotes a collection of variables $\mathbf{y} = \{y_1, \ldots, y_I\}$. Referring to [35], let $c = \frac{1}{b}$, where $c \in \left[\left(\min_i\ 1 + P_0\|\mathbf{h}_i\|^2\right)^{-1}, 1 \right]$. Thus, problem (35) can be rewritten as (37) (next page) by replacing b with c, and the optimal y_i can be found in the following closed form

$$y_i = \frac{c\sqrt{\Sigma_i + \mathrm{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1}}{\Sigma_i - \mathrm{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_i\right) + \mathrm{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1}. \quad \text{(36)}$$

Note that problem (37) (at the top of the next page) can be efficiently solved by the CVX toolbox [41], [42]. Given the interval of c, the optimal variables. $\tilde{\mathbf{W}}_i^\star, \mathbf{R}_N^\star, z^\star$ can be consequently obtained by performing a one-dimensional search over c, such as uniform sampling or the golden search [44]. To this end, the optimal $\mathrm{CRB}^\star$ and $\mathrm{SR}^\star$ can be accordingly calculated. The computational complexity of solving problem (37) at each iteration is $\mathcal{O}\left(N_t^{6.5}\right)$ according to [45].

To further generalize the problem above and simplify the objective function, we equivalently consider the determinant minimization problem of $\mathbf{P}^H \mathbf{J}^{-1} \mathbf{P}$ by introducing the matrix $\mathbf{P}$, where $\mathbf{P}$ associates with activated Eves with the dimension of $\mathbf{P}$ is $3K \times 3$. For example, when the CRB minimization is only associated with the first Eve, the first, the $(K+1)$-th, and the $(2K+1)$-th rows are the first, second, and third rows of the identity matrix $\mathbf{I}_{3\times 3}$, respectively [28]. Then, by

$$\max_{\tilde{\mathbf{W}}_i, \mathbf{R}_N} \quad \min_i \left(\frac{\rho}{|\mathbf{J}|_{UB}} |\mathbf{J}| + \frac{1-\rho}{2^{SR_{UB}}} \frac{\Sigma_i + \mathrm{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1}{b\left(\Sigma_i - \mathrm{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_i\right) + \mathrm{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1\right)} \right) \tag{34a}$$

$$\text{s.t.} \quad \frac{|\alpha_k|^2 \mathbf{b}^H\left(\vartheta_{k,n}\right) \tilde{\mathbf{W}}_i \mathbf{b}\left(\vartheta_{k,n}\right)}{|\alpha_k|^2 \mathbf{b}^H\left(\vartheta_{k,n}\right) \left(\sum_{\substack{\bar{m}=1, \\ \bar{m} \neq i}}^{I} \tilde{\mathbf{W}}_{\bar{m}} + \mathbf{R}_N \right) \mathbf{b}\left(\vartheta_{k,n}\right) + 1} \leq b - 1, \forall\, \vartheta_{k,n} \in \mathrm{card}\left(\Omega_k\right), \forall\, k, i \tag{34b}$$

$$(32b), (32c), (32d) \text{ and } (32e). \tag{34c}$$

$$\max_{\tilde{\mathbf{W}}_i, \mathbf{R}_N, \mathbf{y}, z} \quad \frac{\rho}{|\mathbf{J}|_{UB}} |\mathbf{J}| + \frac{1-\rho}{2^{SR_{UB}}} z \tag{37a}$$

$$\text{s.t.} \quad 2c y_i \sqrt{\Sigma_i + \mathrm{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1} - y_i^2 \left(\Sigma_i - \mathrm{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_i\right) + \mathrm{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1\right) \geq cz, \forall\, i \tag{37b}$$

$$c|\alpha_k|^2 \mathbf{b}^H\left(\vartheta_{k,n}\right) \tilde{\mathbf{W}}_i \mathbf{b}\left(\vartheta_{k,n}\right) \leq (1-c) \left(|\alpha_k|^2 \mathbf{b}^H\left(\vartheta_{k,n}\right) \left(\sum_{\substack{\bar{m}=1, \\ \bar{m} \neq i}}^{I} \tilde{\mathbf{W}}_{\bar{m}} + \mathbf{R}_N \right) \mathbf{b}\left(\vartheta_{k,n}\right) + 1 \right), \forall\, \vartheta_{k,n} \in \mathrm{card}\left(\Omega_k\right),$$
$$\forall\, k, i \tag{37c}$$

$$(32b), (32c), (32d) \text{ and } (32e). \tag{37d}$$

noting that the inequality $\mathbf{\Upsilon}^{-1} \geq \mathbf{P}^H \mathbf{J}^{-1} \mathbf{P}$ is equivalent to $\mathbf{\Upsilon} \geq \mathbf{\Upsilon} \mathbf{P}^H \mathbf{J}^{-1} \mathbf{P} \mathbf{\Upsilon}$, and based on the Schur-complement condition, problem (32) can be recast as

$$\max_{\tilde{\mathbf{W}}_i, \mathbf{R}_N, z, \mathbf{\Upsilon}} \quad \frac{\rho}{|\mathbf{J}|_{UB}} |\mathbf{\Upsilon}| + \frac{1-\rho}{2^{SR_{UB}}} z$$
$$\text{s.t.} \quad \begin{bmatrix} \mathbf{\Upsilon} & \mathbf{\Upsilon} \mathbf{P}^H \\ \mathbf{P} \mathbf{\Upsilon} & \mathbf{J} \end{bmatrix} \succeq \mathbf{0} \tag{38}$$
$$(36b), (36c) \text{ and } (36d).$$

Similarly, the determinant maximization problem above is convex and readily solvable. For clarity, the above procedure has been summarized in Algorithm 1.

VII. NUMERICAL RESULTS

In this section, we provide the numerical results to evaluate the effectiveness of the proposed sensing-aided secure ISAC system design. We assume that both the ISAC BS and the radar receiver are equipped with uniform linear arrays (ULAs) with the same number of elements with half-wavelength spacing between adjacent antennas. In the following simulations, the number of transmit antennas and receive antennas are set as $N_t = N_r = 10$ serving $I = 3$ CUs, the frame length is set as $L = 64$, the noise variance of the communication system is $\sigma_C^2 = 0$ dBm. We assume that the complex path-loss coefficient is constant over the observation interval and modeled as a complex Gaussian distributed with mean zero and variance of $\bar{\sigma}_{\alpha_k}^2 \propto \frac{1}{d_k^2}$, where d_k is the distance between the BS and the k-th target [46].
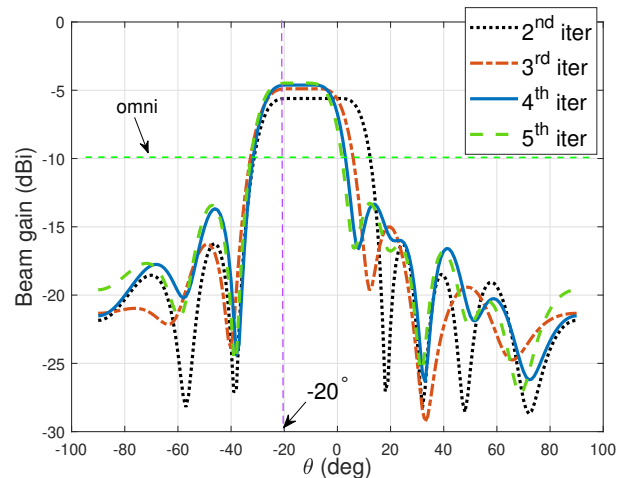

Fig. 4. Beampatterns for the scenario of single Eve angle estimation, where the main beam width narrows over each iteration, $\vartheta_{1,0} = -25°, I = 3, K = 1, P_0 = 35$ dBm, SNR=-22 dB.

Resultant beampatterns of the proposed sensing-aided ISAC security technique are shown in Fig. 4 and Fig. 5, which demonstrate the single-Eve (located at $\vartheta_{1,0} = -20°$) scenario and multi-Eve scenario (located at $\vartheta_{1,0} = -25°, \vartheta_{2,0} = 15°$), respectively. Note that the Rician factor is set as $v_i = 0.1$ for generating a Rician channel with a weak LoS component, aiming to alleviate the impact on the radar beampattern caused by the channel correlation, and α is set as $\alpha = 0.05$. To

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.2023.3306029
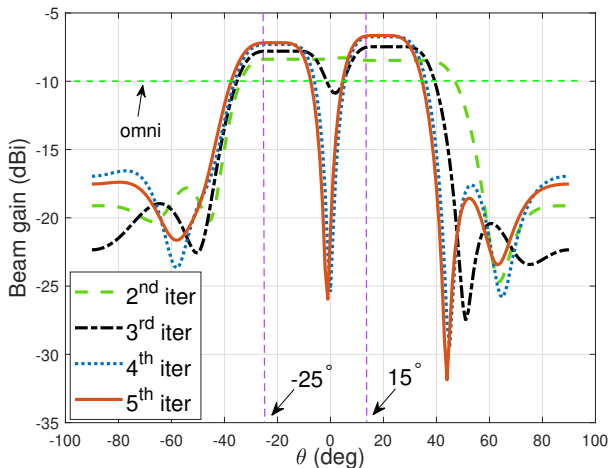
10

Fig. 5. Beampatterns for the scenario of two Eves to be estimated, illustrating the circumstance when the main lobes overlap at the first iteration, $\vartheta_{1,0} = -25°, \vartheta_{2,0} = 15°, I = 3, K = 2, P_0 = 35$ dBm, SNR=-22 dB.
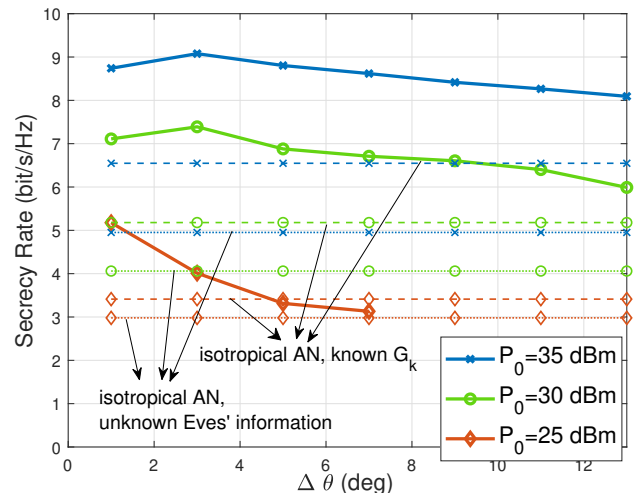

Fig. 6. The secrecy rate analysis versus Eve's location uncertainty with various power budgets, where the AN design techniques with no information of Eves' channels and with known $\mathbf{G}_k$ are denoted by dotted lines and dashed lines, respectively. $\vartheta_{1,0} = -25°, I = 3, K = 1$, SNR=-15 dB.

verify the efficiency of the proposed approach, the received SNR of the echo signal is set as SNR=-22 dB, which is defined as SNR $= \frac{|\beta|^2 L P_0}{\sigma_R^2}$. The ISAC BS first transmits an omnidirectional beampattern for Eve estimation, with the aid of the CAML technique, which is denoted by green dashed lines in Fig. 4 and Fig. 5. It is referred to as the first iteration and the CRB can be accordingly calculated. Then, to ensure that Eves stay within the angle range of main lobes, we design a beampattern with a wide main beam with a beamwidth determined by the CRB obtained from the last iteration, which has been elaborated in Section VI. By updating the CRB iteratively, the main lobes get narrow and point to the directions of Eves, as illustrated by the rest of the lines in Fig. 4 and Fig. 5. In the simulations, we repeat the weighted optimization problem until the CRB and the secrecy rate both convergence to a local optimum. The beampatterns also indicate that the main beam gain grows with the main lobe width getting narrow. Besides, Fig. 5 shows that the power towards Eves of interest gets lower compared with the single-Eve scenario, while it still outperforms the omnidirectional beampattern design.

In Fig. 6, we investigate the secrecy rate versus the main beam width with different power budget P_0, and the benchmarks are given in dashed lines and dotted lines which are obtained by the AN design techniques with knowledge of $\mathbf{G}_k$ and with no information of Eves' channels as given in Sec III, respectively. Generally, the secrecy rate gets higher with the increase of the power budget and it is obvious that the proposed algorithm outperforms benchmark methods. It is worthwhile to stress that the proposed weighted optimization (32) is implemented with no information on Eves. Note that the secrecy rate increases first and then decreases with the expansion of Eve's location uncertainty. The initial increase is because the gain of the beam towards the target/Eve of interest decreases with the growth of the main beam width, resulting in the deterioration of the eavesdropping $\text{SINR}_{k,i}^{\text{E}}$. With respect to the expression in (16), the secrecy rate improves when $\text{SINR}_{k,i}^{\text{E}}$

reduces. However, the power budget constraint becomes tight when the main beam keeps being expanded. This indicates that more power is allocated to the Eve estimation, thus, the secrecy rate decreases. Additionally, when the main beam is wider, the transmission needs to secure the data over a wider range of angles, which is reflected in an SR expression with high channel uncertainty. Particularly, when the power budget is low, for example, $P_0 = 25$ dBm, we note that the secrecy rate monotonically decreases with the growth of $\Delta\theta$, while the weighted optimization problem is infeasible due to the power budget limit when the $\Delta\theta$ is larger than 5 degree.

Fig. 7 illustrates the convergence of the CRB and the secrecy rate of the proposed algorithm. The benchmark in Fig. 7 (c) is generated following the AN design techniques in Section III, where the covariance of AWGN received by Eves is set as $\sigma_0^2 = 0$ dBm. [1] It is noted that the performance of metrics converges after five iterations when SNR=-22 dB, while the convergence requires fewer iterations at higher SNR. Additionally, the secrecy rate obtained by the proposed algorithm converges to 8.9 bit/s/Hz and 9.1 bit/s/Hz when SNR=-22 dB and SNR=-15 dB, which outperforms the isotropical AN methods.

Moreover, it is illustrated in Fig. 8 that the secrecy rate decreases with the growth of the CUs' number, given different power budgets P_0. Note that a higher power budget achieves better security performance. Particularly, the secrecy rate cannot be ensured if the ISAC system serves more than 5 CUs when $P_0 = 25$ dBm. In Fig. 9, we consider the performance tradeoff between the target/Eve estimation and communication data security with different power budgets by varying the weighting factor ρ. We note that higher P_0 results

---

[1]In the isotropical AN designs, i.e., the benchmark schemes, we deploy the omnidirectional waveform to ensure the sensing performance, where we have $\bar{\mathbf{R}}_X = \frac{P_0}{N_t}\mathbf{I}_{N_t}$ according to problem (25). As the CRB matrix is a function of the covariance matrix, the resultant root-CRB of the benchmark schemes is equal to the value at the first iteration as shown in Fig. 6.
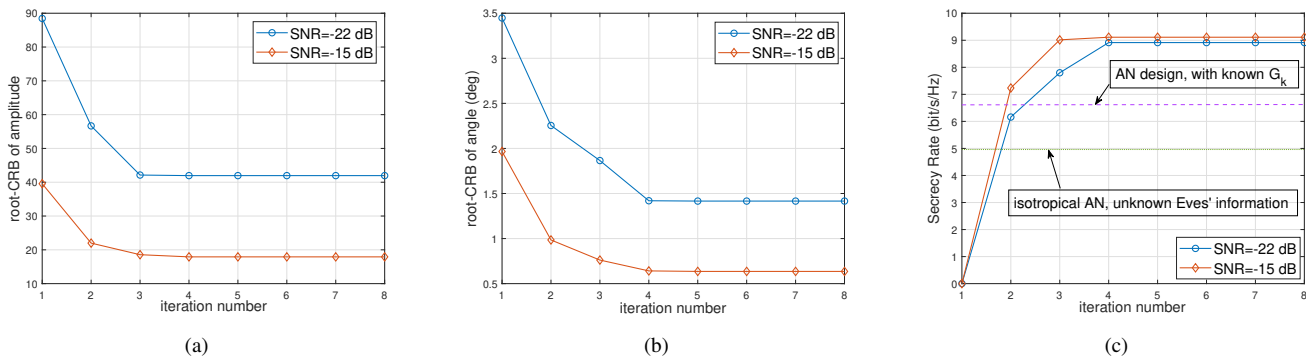
Fig. 7. Convergence with iterations when SNR=-15 dB and SNR= -22 dB. $I = 3, K = 1, P_0 = 35$ dBm. (a) Convergence of root-CRB of amplitude estimation; (b) Convergence of root-CRB of angle estimation; (c) Convergence of the secrecy rate.

in a better performance of the estimation metric, i.e., root-CRB of the amplitude and the angle. Additionally, with the increase in secrecy rate, the CRB grows as well, which demonstrates the deterioration of Eve's angle estimation accuracy.
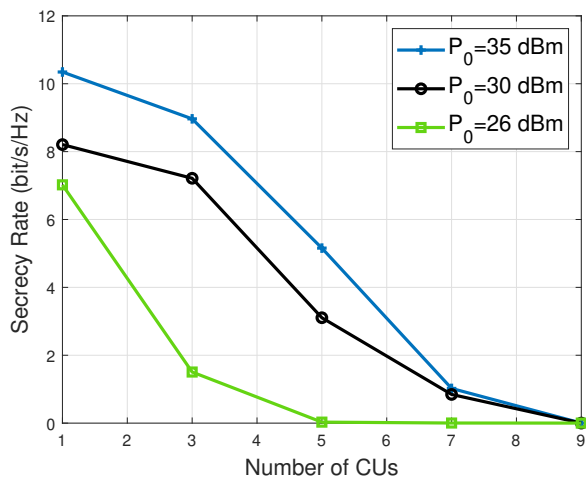

Fig. 8. The secrecy rate analysis versus the number of CUs, with various power budgets. $K = 1$, SNR=-15 dB.

Furthermore, we consider a scenario including one CU and one Eve for exploiting impacts on security and sensing metrics resulting from the angle difference between the CU and the Eve. In this case, the Rician channel model with a strong LoS component is deployed, i.e., $v_i = 7$ in (2), and the CU is assumed to locate at $-20°$. Resultant beampatterns are shown in Fig. 10 when the Eve is at $-20°$ as well. It is demonstrated that the main beam width converges after four iterations and the generated angle root-CRB at the second iteration is lower than the case of a weak Rician channel, which is validated in Fig. 11. Fig.11 illustrates the analysis of the secrecy rate and the root-CRB of angle with various angle difference. Generally speaking, with the expansion of the uncertain angular interval $\Delta\theta$, both of the metrics deteriorated. The secrecy rate decreases when the Eve and the CU directions get closer, while the performance of the CRB improves since the tradeoff is revealed in Fig. 9.
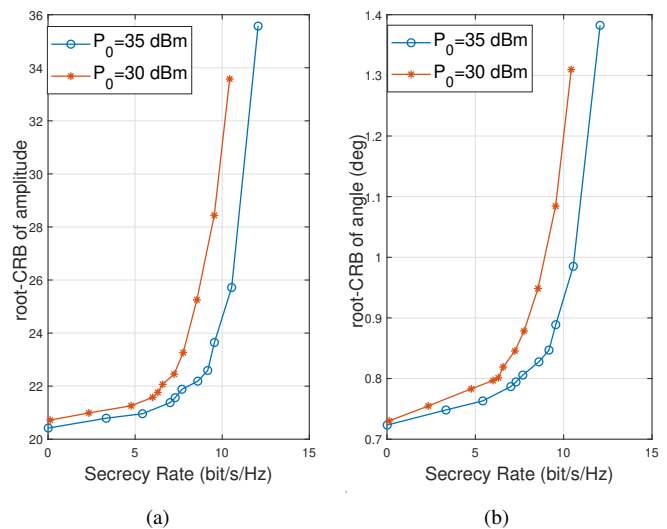

Fig. 9. Tradeoff between the CRB and the secrecy rate with different power budgets. $\vartheta_{1,0} = -25°, I = 3, K = 1$, SNR=-15 dB.
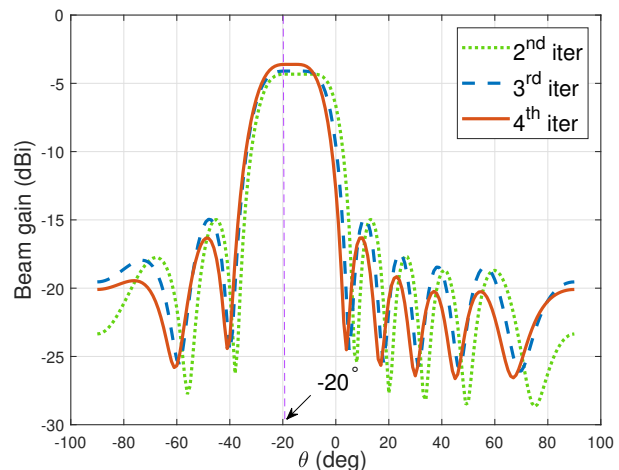

Fig. 10. Beampatterns for the scenario when the CU and the Eve both locate at $-20°$, narrowing with each iteration until convergence. $I = 1, K = 1$, SNR=-22 dB, $P_0 = 35$ dBm.

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.2023.3306029
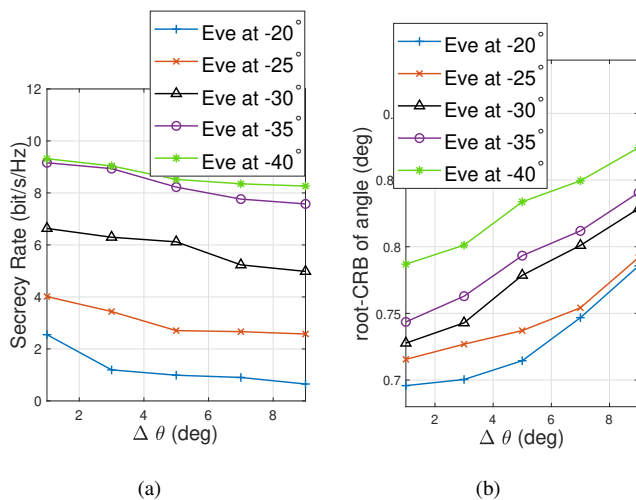
12

Fig. 11. Secrecy rate and root-CRB of angle performances versus uncertain angular interval of the target/Eve, with various angle differences between the Eve and the CU, where the CU locates at $-20°$. $I = 1, K = 1$, SNR=-15 dB, $P_0 = 35$ dBm.

VIII. CONCLUSION

In this paper, we have considered the sensing-aided secure ISAC systems, where the dual-functional BS emitted waveforms to estimate the amplitudes and the directions of potential eavesdroppers and send confidential communication data to CUs simultaneously. The proposed design has promoted the cooperation between sensing and communication rather than conventionally individual functionalities. The weighted optimization problem has been designed to optimize the normalized CRB and secrecy rate while constraining the system power budget. Our numerical results have demonstrated that the secrecy rate was enhanced with the decreasing CRB in both single and multi-Eve scenarios.

REFERENCES

[1] X. You, C.-X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang, C. Zhang, Y. Jiang, J. Wang *et al.*, "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Science China Information Sciences*, vol. 64, no. 1, pp. 1–74, 2021.

[2] Z. Feng, Z. Fang, Z. Wei, X. Chen, Z. Quan, and D. Ji, "Joint radar and communication: A survey," *China Communications*, vol. 17, no. 1, pp. 1–27, 2020.

[3] L. Zheng, M. Lops, Y. C. Eldar, and X. Wang, "Radar and communication coexistence: An overview: A review of recent methods," *IEEE Signal Processing Magazine*, vol. 36, no. 5, pp. 85–99, 2019.

[4] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated sensing and communications: Towards dual-functional wireless networks for 6G and beyond," *IEEE Journal on Selected Areas in Communications*, 2022.

[5] Y. Cui, F. Liu, X. Jing, and J. Mu, "Integrating sensing and communications for ubiquitous IoT: Applications, trends, and challenges," *IEEE Network*, vol. 35, no. 5, pp. 158–167, 2021.

[6] Z. Wei, F. Liu, C. Masouros, N. Su, and A. P. Petropulu, "Toward multifunctional 6G wireless networks: Integrating sensing, communication, and security," *IEEE Communications Magazine*, vol. 60, no. 4, pp. 65–71, 2022.

[7] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, 2017.

[8] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, "Physical layer security for 5G non-orthogonal multiple access in large-scale networks," in *2016 IEEE International Conference on Communications (ICC)*. IEEE, 2016, pp. 1–6.

[9] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2018.

[10] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, "A survey on OFDM physical layer security," *Physical Communication*, vol. 32, pp. 1–30, 2019.

[11] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China communications*, vol. 14, no. 12, pp. 1–14, 2017.

[12] D. Li, Z. Yang, N. Zhao, Z. Wu, Y. Li, and D. Niyato, "Joint precoding and jamming design for secure transmission in NOMA-ISAC networks," in *2022 14th International Conference on Wireless Communications and Signal Processing (WCSP)*. IEEE, 2022, pp. 764–769.

[13] B. Yang, X. Cao, J. Xu, C. Huang, G. C. Alexandropoulos, L. Dai, H. V. Poor, C. Yuen *et al.*, "Reconfigurable intelligent computational surfaces: When wave propagation control meets computing," *arXiv preprint arXiv:2208.04509*, 2022.

[14] A. A. Salem, M. H. Ismail, and A. S. Ibrahim, "Active reconfigurable intelligent surface-assisted miso integrated sensing and communication systems for secure operation," *IEEE Transactions on Vehicular Technology*, 2022.

[15] A. M. Elbir, K. V. Mishra, M. B. Shankar, and S. Chatzinotas, "The rise of intelligent reflecting surfaces in integrated sensing and communications paradigms," *IEEE Network*, 2022.

[16] P. Liu, Z. Fei, X. Wang, J. A. Zhang, Z. Zheng, and Q. Zhang, "Securing multi-user uplink communications against mobile aerial eavesdropper via sensing," *IEEE Transactions on Vehicular Technology*, 2023.

[17] A. Deligiannis, A. Daniyan, S. Lambotharan, and J. A. Chambers, "Secrecy rate optimizations for MIMO communication radar," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 5, pp. 2481–2492, 2018.

[18] J. Chu, R. Liu, Y. Liu, M. Li, and Q. Liu, "AN-aided secure beamforming design for dual-functional radar-communication systems," in *2021 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*. IEEE, 2021, pp. 54–59.

[19] N. Su, F. Liu, and C. Masouros, "Secure Radar-Communication systems with malicious targets: Integrating radar, communications and jamming functionalities," *IEEE Transactions on Wireless Communications*, 2020.

[20] N. Su, F. Liu, Z. Wei, Y.-F. Liu, and C. Masouros, "Secure dualfunctional radar-communication transmission: Exploiting interference for resilience against target eavesdropping," *IEEE Transactions on Wireless Communications*, 2022.

[21] S. Dwivedi, M. Zoli, A. N. Barreto, P. Sen, and G. Fettweis, "Secure joint communications and sensing using chirp modulation," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[22] O. Günlü, M. Bloch, R. F. Schaefer, and A. Yener, "Secure joint communication and sensing," *arXiv preprint arXiv:2202.10790*, 2022.

[23] S. M. Kay, *Fundamentals of statistical signal processing: estimation theory*. Prentice-Hall, Inc., 1993.

[24] L. Zhao, G. Geraci, T. Yang, D. W. K. Ng, and J. Yuan, "A tone-based AoA estimation and multiuser precoding for millimeter wave massive MIMO," *IEEE Transactions on Communications*, vol. 65, no. 12, pp. 5209–5225, 2017.

[25] X. Hu, C. Zhong, X. Chen, W. Xu, and Z. Zhang, "Cluster grouping and power control for angle-domain MmWave MIMO NOMA systems," *IEEE Journal of Selected Topics in Signal Processing*, vol. 13, no. 5, pp. 1167–1180, 2019.

[26] J. Li and P. Stoica, "MIMO radar with colocated antennas," *IEEE Signal Processing Magazine*, vol. 24, no. 5, pp. 106–114, 2007.

[27] F. Liu, Y.-F. Liu, A. Li, C. Masouros, and Y. C. Eldar, "Cramér-Rao bound optimization for joint Radar-Communication beamforming," *IEEE Transactions on Signal Processing*, pp. 1–1, 2021.

[28] J. Li, L. Xu, P. Stoica, K. W. Forsythe, and D. W. Bliss, "Range compression and waveform optimization for MIMO radar: a Cramér-Rao bound based study," *IEEE Transactions on Signal Processing*, vol. 56, no. 1, pp. 218–232, 2007.

[29] M. F. Hanif, L.-N. Tran, M. Juntti, and S. Glisic, "On linear precoding strategies for secrecy rate maximization in multiuser multiantenna wireless networks," *IEEE Transactions on Signal Processing*, vol. 62, no. 14, pp. 3536–3551, 2014.

[30] B. Hassibi and T. L. Marzetta, "Multiple-antennas and isotropically random unitary inputs: The received signal density in closed form,"

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.2023.3306029

13

IEEE Transactions on Information Theory, vol. 48, no. 6, pp. 1473–1484, 2002.

[31] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202–1216, 2010.

[32] B. Fang, Z. Qian, W. Shao, and W. Zhong, "Precoding and artificial noise design for cognitive MIMOME wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6753–6758, 2015.

[33] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in af multi-antenna multi-relay networks," *IEEE Transactions on Signal Processing*, vol. 63, no. 1, pp. 206–220, 2014.

[34] Z. Chu, H. Xing, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 283–297, 2015.

[35] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2704–2717, 2013.

[36] A. Jakobsson and P. Stoica, "Combining capon and apes for estimation of spectral lines," *Circuits, Systems and Signal Processing*, vol. 19, no. 2, pp. 159–169, 2000.

[37] L. Xu, J. Li, and P. Stoica, "Target detection and parameter estimation for MIMO radar systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 44, no. 3, pp. 927–939, 2008.

[38] J. Li, P. Stoica, and Z. Wang, "On robust capon beamforming and diagonal loading," *IEEE Transactions on Signal Processing*, vol. 51, no. 7, pp. 1702–1715, 2003.

[39] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys (CSUR)*, vol. 41, no. 3, pp. 1–58, 2009.

[40] P. Tichavsky, "Posterior Cramér-Rao bound for adaptive harmonic retrieval," *IEEE Transactions on Signal Processing*, vol. 43, no. 5, pp. 1299–1302, 1995.

[41] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," 2014.

[42] S.-P. Wu, L. Vandenberghe, and S. Boyd, "Software for determinant maximization problems—user's guild," 1996.

[43] K. Shen and W. Yu, "Fractional programming for communication systems part I: Power control and beamforming," *IEEE Transactions on Signal Processing*, vol. 66, no. 10, pp. 2616–2630, 2018.

[44] D. P. Bertsekas, "Nonlinear programming," *Journal of the Operational Research Society*, vol. 48, no. 3, pp. 334–334, 1997.

[45] A. Ben-Tal and A. Nemirovski, *Lectures on modern convex optimization: analysis, algorithms, and engineering applications*. SIAM, 2001.

[46] Z. Yu, J. Li, Q. Guo, and J. Ding, "Efficient direct target localization for distributed mimo radar with expectation propagation and belief propagation," *IEEE Transactions on Signal Processing*, vol. 69, pp. 4055–4068, 2021.

Fan Liu (Member, IEEE) received the B.Eng. and the Ph.D. degrees from Beijing Institute of Technology (BIT), Beijing, China, in 2013 and 2018, respectively. He is currently an Assistant Professor of the Department of Electronic and Electrical Engineering, Southern University of Science and Technology (SUSTech). He has previously held academic positions with the University College London, London, U.K., first as a Visiting Researcher from 2016 to 2018, and then as a Marie Curie Research Fellow from 2018 to 2020. His research interests include the general area of signal processing and wireless communications, and in particular in the area of Integrated Sensing and Communications (ISAC). He has 10 publications selected as IEEE ComSoc Besting Readings in ISAC. He is the Founding Academic Chair of the IEEE ComSoc ISAC Emerging Technology Initiative (ISAC-ETI), an Associate Editor for the IEEE Communications Letters and the IEEE Open Journal of Signal Processing, and the Guest Editor of the IEEE Journal on Selected Areas in Communications, IEEE Wireless Communications, IEEE Vehicular Technology Magazine, and China Communications. He was also an organizer and the Co-Chair of numerous workshops, special sessions and tutorials in flagship IEEE/ACM conferences, including ICC, GLOBECOM, ICASSP, and MobiCom. He is the TPC Co-Chair of the 2nd-4th IEEE Joint Communication and Sensing Symposium (JC&S), the Track Chair of the ISAC Track of the IEEE GLOBECOM 2023 Selected Areas in Communications Symposium, and a Track Co-Chair for the IEEE WCNC 2024. He is a Member of the IMT-2030 (6G) ISAC Task Group. He was the recipient of the 2023 IEEE ComSoc Stephan O. Rice Prize, 2023 IEEE ICC Best Paper Award, 2021 IEEE Signal Processing Society Young Author Best Paper Award, the 2019 Best Ph.D. Thesis Award of Chinese Institute of Electronics, and the 2018 EU Marie Curie Individual Fellowship. Dr. Fan Liu was listed in the World's Top 2% Scientists by Stanford University for citation impact in 2021 and 2022.

Nanchi Su (Graduate Student Member, IEEE) received the Ph.D. degree from University College London, London, U.K. in 2023, and received the B.E. and M.E. degrees from Harbin Institute of Technology, Heilongjiang, China, in 2015 and 2018, respectively. She is currently a visiting scholar with Guangdong Provincial Key Laboratory of Aerospace Communication and Networking Technology, Harbin Institute of Technology (Shenzhen), Shenzhen 518055, China, and with the Department of Electronic and Electrical Engineering, Southern University of Science and Technology, Shenzhen 518055, China. She is a TPC member of various flagship IEEE/ACM conferences, such as IEEE ICC, IEEE Globecom, etc. Her research interests include integrated sensing and communication systems (ISAC), constructive interference design, physical-layer security, radar signal processing, convex optimization, and situational awareness.

Christos Masouros (Senior Member, IEEE) received the Diploma degree in Electrical and Computer Engineering from the University of Patras, Greece, in 2004, and MSc by research and PhD in Electrical and Electronic Engineering from the University of Manchester, UK in 2006 and 2009 respectively. In 2008 he was a research intern at Philips Research Labs, UK. Between 2009-2010 he was a Research Associate in the University of Manchester and between 2010-2012 a Research Fellow in Queen's University Belfast. In 2012 he joined University College London as a Lecturer. He has held a Royal Academy of Engineering Research Fellowship between 2011-2016.

Since 2019 he is a Full Professor of Signal Processing and Wireless Communications in the Information and Communication Engineering research group, Dept. Electrical and Electronic Engineering, and affiliated with the Institute for Communications and Connected Systems, University College London. His research interests lie in the field of wireless communications and signal processing with particular focus on Green Communications, Large Scale Antenna Systems, Integrated Sensing and Communications, interference mitigation techniques for MIMO and multicarrier communications. Between 2018-22 he was the Project Coordinator of the €4.2m EU H2020 ITN project PAINLESS, involving 12 EU partner universities and industries, towards energy-autonomous networks. Between 2024-28 he will be the Scientific Coordinator of the €2.7m EU H2020 DN project ISLANDS, involving 19 EU partner universities and industries, towards next-generation vehicular networks. He was the recipient of the 2023 IEEE ComSoc Stephen O. Rice Prize, co-recipient of the 2021 IEEE SPS Young Author Best Paper Award and the recipient of the Best Paper Awards in the IEEE GlobeCom 2015 and IEEE WCNC 2019 conferences. He has been recognised as an Exemplary Editor for the IEEE Communications Letters, and as an Exemplary Reviewer for the IEEE Transactions on Communications. He is an Editor for IEEE Transactions on Wireless Communications, the IEEE Open Journal of Signal Processing, and Editor-at-Large for IEEE Open Journal of the Communications Society. He has been an Editor for IEEE Transactions on Communications, IEEE Communications Letters, and a Guest Editor for a number of IEEE Journal on Selected Topics in Signal Processing and IEEE Journal on Selected Areas in Communications issues. He is a founding member and Vice-Chair of the IEEE Emerging Technology Initiative on Integrated Sensing and Communications (SAC), Vice Chair of the IEEE Wireless Communications Technical Committee Special Interest Group on ISAC, and Chair of the IEEE Green Communications & Computing Technical Committee, Special Interest Group on Green ISAC. He is the TPC chair for the IEEE ICC 2024 Selected Areas in Communications (SAC) Track on ISAC.