Secure Integrated Sensing and Communication Systems with the Assistance of Sensing Functionality

Nanchi Su[1], Fan Liu[2], Christos Masouros[1]
[1] Department of Electronic and Electrical Engineering, University College London, London, UK
[2] Department of Electrical and Electronic Engineering, Southern University of Science and Technology, Shenzhen, China

***Abstract*—With the expectation of deeper integration between sensing and communication functionalities, we investigate the sensing-assisted approach to ensure the security of confidential information in Integrated Sensing and Communication (ISAC) systems. In physical layer security (PLS) studies, the acquisition of channel state information (CSI) is considered to be the common limitation. However, in ISAC systems, the sensing functionality is able to provide the channel information towards each target, aka., potential eavesdropper (Eve), by estimating the directions. In our design, the dual-functional base station (BS) emits an omnidirectional waveform, aiming to search for targets and obtain the angle estimations by employing the combined Capon and approximate maximum likelihood (CAML) technique. Afterwards, we formulate a weighted optimization problem with the help of artificial noise (AN) to jointly optimize the secrecy rate and the Cramér-Rao Bound (CRB), while generating a wide main-beam beampattern, covering all possible angles of the detected targets. 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. Finally, the numerical results reveal the feasibility of the proposed algorithm and prove that it enables the multi-target scenario for secure ISAC systems.**

***Index Terms*—Integrated Sensing and Communication systems, physical layer security, Cramér-Rao Bound.**

I. Introduction

The evolution of integrated sensing and communication (ISAC) systems has been driven by the commonalities between sensing and communication (S&C) in hardware architecture, channel characteristics, and signal processing with recent developments of radar and communication (R&C) systems towards high-frequency bands and large-scale antennas [1], [2]. To this end, ISAC systems have emerged as a transformative technology that enables a good balance between two potentially conflicting design objectives: high-quality communication and high-timeliness sensing [3], getting increasingly prevalent in a wide range of applications such as vehicle-to-everything (V2X) communications, smart cities, and the Internet of Things (IoT). However, ISAC systems present unique security challenges due to the shared use of spectrum and the broadcast nature of wireless transmission, that is, communication data is susceptible to eavesdropping as radar probing signals include confidential information.

Existing research has shown that radar and communication systems typically work independently towards separate end-goals, instead of collaborating to enhance security. To address this, we propose a novel approach that leverages the sensing functionality to ensure physical layer security (PLS) of communication data transmission. The approach involves a dual-functional access point (AP) that emits an omnidirectional waveform to search for potential eavesdroppers (Eves). The AP receives echoes reflected from communication users (CUs) and Eves located within the sensing range. Since we assume that all CUs are cooperative, their angles are known to the AP, allowing the estimation of Eve angles by subtracting known CU angles. The estimation performance metric is measured by the Cramér-Rao Bound (CRB). Furthermore, we formulate a weighted optimization problem. The goal of this optimization is to minimize the CRB, while maximizing the secrecy rate, subject to constraints on the beampattern and transmit power budget. An important novelty of this optimization setup is that the channel information in the secrecy rate is a function of the sensing performance. To avoid false dismissal detection, the beampattern's main lobe is designed to be wide, with a width that depends on the estimation accuracy. As estimation accuracy improves, the sensing and security functionalities provide mutual benefits, resulting in improvement of the mutual performances with every iteration of the optimization, until convergence.

II. System Model

A. Communication Signal Model and Metrics

In this section, 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. We assume the BS has knowledge of the CUs and their channels, and has no knowledge of the Eves. 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. $\mathbf{H} = [\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_I]^H \in \mathbb{C}^{I \times N_t}$ 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 [4], [5], 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, $\mathbf{h}_{L,i}^{\mathrm{LoS}} = \sqrt{N_t}\mathbf{a}_t\left(\omega_{i,0}\right)$ is the LoS deterministic component. $\mathbf{a}\left(\omega_{i,0}\right)$ denotes the array steering vector, where $\omega_{i,0} \in \left[\text{-}\ \frac{\pi}{2}, \frac{\pi}{2}\right]$ is the angle of departure (AOD) of the LoS component from the BS to the user i [4], [6]. The scattering component $\mathbf{h}_{S,i}^{\mathrm{NLoS}}$ can be expressed as $\mathbf{h}_{S,i}^{\mathrm{NLoS}} = \sqrt{\frac{N_t}{L_p}}\sum_{l=1}^{L_p} c_{i,l}\mathbf{a}_t\left(\omega_{i,l}\right)$, where L_p denotes the number of propagation paths, $c_{i,l} \sim \mathcal{CN}\left(0,1\right)$ is the complex path gain and $\omega_{i,l} \in \left[\text{-}\ \frac{\pi}{2}, \frac{\pi}{2}\right]$ 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 $\mathbf{N} \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{R}_N\right)$, 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 $\mathbf{W} = \left[\mathbf{w}_1, \ldots, \mathbf{w}_I\right]$, 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

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

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

By emitting the waveform $\mathbf{X}$ to sense Eves, the reflected echo signal matrix at the BS receive array is given as

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

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

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

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

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

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

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

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

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

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

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 [7], 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 $\theta_1, \ldots, \theta_K$ and $\beta_1, \ldots, \beta_K$ was derived in [8] 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

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

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 $\dot{\mathbf{A}} = \left[\ ,\frac{\partial\mathbf{a}(\theta_1)}{\partial\theta_1}\quad \frac{\partial\mathbf{a}(\theta_2)}{\partial\theta_2}\quad \cdots\quad \frac{\partial\mathbf{a}(\theta_K)}{\partial\theta_K}\ \right]$, $\dot{\mathbf{B}} = \left[\ \frac{\partial\mathbf{b}(\theta_1)}{\partial\theta_1}\quad \frac{\partial\mathbf{b}(\theta_2)}{\partial\theta_2}\quad \cdots\quad \frac{\partial\mathbf{b}(\theta_K)}{\partial\theta_K}\ \right]$. Also, the covariance matrix $\mathbf{R}_X$ is given as

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

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

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

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

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

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

and

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

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 [9], [10]

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

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. Problem Formulation

In this section, we propose a normalized weighted optimization problem that reveals the performance tradeoff between the communication security and Eve parameters estimation. Additionally, the ISAC access point firstly emits an omnidirectional beampattern to search for potential Eves, thus imprecise angles of Eves have been obtained at the given SNR by deploying the combined Capon and approximate maximum likelihood (CAML) method, 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 desirable 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

$$\max_{\tilde{\mathbf{W}}_i, \mathbf{R}_N} \quad \rho \frac{|\mathbf{J}|}{|\mathbf{J}|_{UB}} + (1-\rho) \frac{\text{SR}}{\text{SR}_{UB}} \tag{18a}$$

$$\text{s.t. } \mathbf{a}^H\left(\vartheta_{k,0}\right) \mathbf{R}_X \mathbf{a}\left(\vartheta_{k,0}\right) - \mathbf{a}^H\left(\vartheta_{k,p}\right) \mathbf{R}_X \mathbf{a}\left(\vartheta_{k,p}\right) \geq \gamma_s, \quad \forall \vartheta_{k,p} \in \text{card}\left(\Psi_k\right), \forall\ k \tag{18b}$$

$$\mathbf{a}^H\left(\vartheta_{k,n}\right) \mathbf{R}_X \mathbf{a}\left(\vartheta_{k,n}\right) \leq (1+\alpha)\, \mathbf{a}^H\left(\vartheta_{k,0}\right) \mathbf{R}_X \mathbf{a}\left(\vartheta_{k,0}\right), \forall\ \vartheta_{k,n} \in \text{card}\left(\Omega_k\right), \forall\ k \tag{18c}$$

$$\mathbf{a}^H\left(\vartheta_{k,n}\right) \mathbf{R}_X \mathbf{a}\left(\vartheta_{k,n}\right) \geq (1-\alpha)\, \mathbf{a}^H\left(\vartheta_{k,0}\right) \mathbf{R}_X \mathbf{a}\left(\vartheta_{k,0}\right), \forall\ \vartheta_{k,n} \in \text{card}\left(\Omega_k\right), \forall\ k \tag{18d}$$

$$\mathbf{R}_N \succeq \mathbf{0}, \tilde{\mathbf{W}}_i \succeq \mathbf{0}, \forall\ i \tag{18e}$$

$$\text{tr}\left(\sum_{i=1}^{I} \tilde{\mathbf{W}}_i + \mathbf{R}_N\right) = P_0, \tag{18f}$$

where $|\mathbf{J}|_{UB}$ and SR_{UB} denote the upper bounds of the FIM matrix determinant and the secrecy rate, respectively. $0 \leq \rho \leq 1$ denotes 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 card$\left(\cdot\right)$ denotes the the cardinality of $\left(\cdot\right)$.

Remark 1. *Upper-bound of the FIM Determinant [8]*

$$\max_{\tilde{\mathbf{W}}_i, \mathbf{R}_N} \quad |\mathbf{J}| \tag{19a}$$

$$\textit{s.t.} \quad \left(18e\right), \left(18f\right), \tag{19b}$$

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 [11]. Consequently, by substituting the optimal $\tilde{\mathbf{W}}_i, \mathbf{R}_N$ in (11), the upper-bound of FIM determinant is obtained.

Remark 2. *Upper-bound of the Secrecy Rate*

Assuming that the CSI is perfectly known to the BS, the

$$\max_{\tilde{\mathbf{W}}_i,\mathbf{R}_N} \quad \min_i \left(\frac{\rho}{|\mathbf{J}|_{UB}} |\mathbf{J}| + \frac{1-\rho}{2^{SR_{UB}}} \frac{\Sigma_i + \text{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1}{b\left(\Sigma_i - \text{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_i\right) + \text{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1\right)} \right) \tag{21a}$$

$$\text{s.t.} \quad \frac{|\alpha_k|^2 \mathbf{a}^H(\vartheta_{k,n}) \sum_{i=1}^{I} \tilde{\mathbf{W}}_i \mathbf{a}(\vartheta_{k,n})}{|\alpha_k|^2 \mathbf{a}^H(\vartheta_{k,n}) \mathbf{R}_N \mathbf{a}(\vartheta_{k,n}) + 1} \leq b - 1, \forall\, \vartheta_{k,n} \in \text{card}(\Omega_k), \forall\, k \tag{21b}$$

$$(18b), (18c), (18d), (18e) \text{ and } (18f). \tag{21c}$$

secrecy rate maximization problem can be formulated as

$$SR^\star = \max_{\tilde{\mathbf{W}}_i,\mathbf{R}_N} \min_{i,k} \; SR\left(\tilde{\mathbf{W}}_i, \mathbf{R}_N\right) \tag{20a}$$

$$\textit{s.t.} \quad (18e), (18f). \tag{20b}$$

The above problem can be simply relaxed into a convex SDP problem. For brevity, we refer readers to [12] for more details.

B. Efficient Solver

To tackle problem (18), we first recast the complicated secrecy rate term in the objective function. For simplicity, we denote $\Sigma_i = \sum_{m=1}^{I} \text{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_m\right)$ and introduce the scalar b, then the weighted optimization problem can be recast as (21) [12].

It is noted that the min operator only applies to the second term of the objective function of problem (21). According to the Fractional Programming (FP) algorithm [13], the optimization problem can be further reformulated by replacing the fraction term with the coefficient z, which is given as

$$\max_{\tilde{\mathbf{W}}_i,\mathbf{R}_N,\mathbf{y},z} \quad \frac{\rho}{|\mathbf{J}|_{UB}} |\mathbf{J}| + \frac{1-\rho}{2^{SR_{UB}}} z \tag{22a}$$

$$\text{s.t.} \quad 2y_i \sqrt{\Sigma_i + \text{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1} - y_i^2 \left(b\left(\Sigma_i - \text{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_i\right) + \text{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1\right)\right) \geq z, \forall\, i \tag{22b}$$

$$(21b), (18b), (18c), (18d), (18e) \text{ and } (18f), \tag{22c}$$

where $\mathbf{y}$ denotes a collection of variables $\mathbf{y} = \{y_1, \ldots, y_I\}$. Referring to [12], let $c = \frac{1}{b}$, where $c \in \left[\left(\min\limits_i \; 1 + P_0 \|\mathbf{h}_i\|^2\right)^{-1}, 1\right]$. Thus, problem (22) can be rewritten as (24) (next page) by replacing b with c, and the optimal y_i can be found in the following closed form

$$y_i = \frac{c\sqrt{\Sigma_i + \text{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1}}{\Sigma_i - \text{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_i\right) + \text{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1}. \tag{23}$$

Note that problem (24) (at the top of next page) can be efficiently solved by the cvx toolbox [11]. 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 line search over c, such as uniform sampling or the golden search [14]. To this end, the optimal CRB* and SR* can be accordingly calculated.

IV. Numerical Results

In this section, numerical results are provided for characterizing the performance 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.

Resultant beampatterns of the proposed sensing-aided ISAC security technique are shown in Fig. 1, which demonstrates the multi-Eve scenario (located at $\vartheta_{1,0} = -25°, \vartheta_{2,0} = 15°$). Note that the Rician factor is set as $v_i = 0.1$ for generating a Rician channel with 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 verify the efficiency of the proposed approach, the receive SNR of the echo signal is set as SNR=-22 dB, which is defined as $\text{SNR} = \frac{|\beta|^2 L P_0}{\sigma_R^2}$. 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. In Fig. 2, we consider the performance tradeoff between the target/Eve estimation and communication data security with different power budget by varying the weighting factor ρ. We note that higer P_0 results in a better performance of the estimation metric, i.e., root-CRB of the amplitude and the angle. Additionally, with the increase of secrecy rate, the CRB grows as well, which demonstrates the deterioration of the Eve's angle estimation accuracy.

V. Conclusions

In this work, we have proposed a novel approach to ensure transmission data security with the assistance of sensing functionality in ISAC systems. The BS initially emits the omnidirectional beampattern for estimating the parameters of targets, then we design a weighted optimization problem to ensure the performance of the secrecy rate and the estimation accuracy. The proposed algorithm has enabled sensing and

$$\max_{\tilde{\mathbf{W}}_i, \mathbf{R}_N, \mathbf{y}, z} \quad \frac{\rho}{|\mathbf{J}|_{UB}} |\mathbf{J}| + \frac{1-\rho}{2^{SR_{UB}}} z \tag{24a}$$

$$\text{s.t.} \quad 2cy_i\sqrt{\Sigma_i + \text{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1} - y_i^2 \left(\Sigma_i - \text{tr}\left(\tilde{\mathbf{H}}_i \tilde{\mathbf{W}}_i\right) + \text{tr}\left(\tilde{\mathbf{H}}_i \mathbf{R}_N\right) + 1\right) \geq cz, \forall\, i \tag{24b}$$

$$c|\alpha_k|^2 \mathbf{a}^H\left(\vartheta_{k,n}\right) \sum_{i=1}^{I} \tilde{\mathbf{W}}_i \mathbf{a}\left(\vartheta_{k,n}\right) \leq (1-c)\left(|\alpha_k|^2 \mathbf{a}^H\left(\vartheta_{k,n}\right) \mathbf{R}_N \mathbf{a}\left(\vartheta_{k,n}\right) + 1\right), \forall\, \vartheta_{k,n} \in \text{card}\left(\Omega_k\right), \forall\, k \tag{24c}$$

$$(18b), (18c), (18d), (18e) \text{ and } (18f). \tag{24d}$$

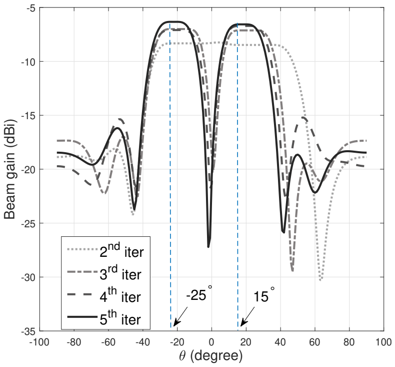
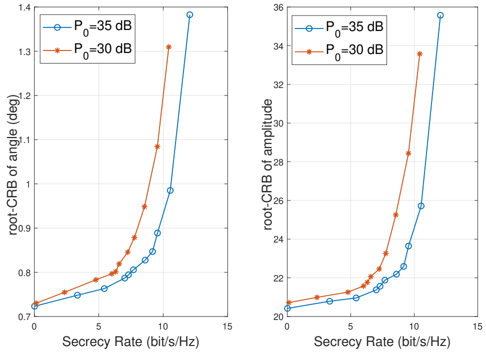


Fig. 1: Beampatterns for the scenario of two Eves to be estimated, illustrating the circumstance when the main lobes overlap at the first iteration, $\vartheta_{1,0} = -25°, \vartheta_{2,0} = 15°, I = 3, K = 2, P_0 = 35$dBm, SNR=-22dB.



(a)

(b)

Fig. 2: Tradeoff between the CRB and the secrecy rate with different power budget. $\vartheta_{1,0} = -25°, I = 3, K = 1,$ SNR=-15dB.

communication functionalities to be integrated more deeply and to gain mutual benefits from each other. In the end, the numerical results have verified the effectiveness of the proposed method and revealed the tradeoff between the sensing and secrecy performance.

Acknowledgment

This work has received funding from the Engineering and Physical Sciences Research Council (EPSRC) of the UK Grant number EP/S028455/1, in part by the National Natural Science Foundation of China under Grant 62101234 and Grant U20B2039, in part by the Young Elite Scientist Sponsorship Program by CAST under Grant No. YESS20210055.

References

[1] F. Liu, L. Zheng, Y. Cui, C. Masouros, A. P. Petropulu, H. Griffiths, and Y. C. Eldar, "Seventy years of radar and communications: The road from separation to integration," *arXiv preprint arXiv:2210.00446*, 2022.

[2] S. Lu, F. Liu, and L. Hanzo, "The degrees-of-freedom in monostatic isac channels: Nlos exploitation vs. reduction," *IEEE Transactions on Vehicular Technology*, 2022.

[3] K. Meng, Q. Wu, S. Ma, W. Chen, and T. Q. Quek, "Uav trajectory and beamforming optimization for integrated periodic sensing and communication," *IEEE Wireless Communications Letters*, vol. 11, no. 6, pp. 1211–1215, 2022.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

[12] 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.

[13] 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.

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