Securing the Sensing Functionality in ISAC Networks: An Artificial Noise Design

Jiaqi Zou, *Graduate Student Member, IEEE*, Christos Masouros, *Fellow, IEEE*, Fan Liu, *Senior Member, IEEE*
Songlin Sun, *Senior Member, IEEE*

***Abstract*—Integrated sensing and communications (ISAC) systems employ dual-functional signals to simultaneously accomplish radar sensing and wireless communication tasks. However, ISAC systems open up new *sensing security* vulnerabilities to malicious illegitimate eavesdroppers (Eves) that can also exploit the transmitted waveform to extract sensing information from the environment. In this paper, we investigate the beamforming design to enhance the sensing security of an ISAC system, where the communication user (CU) serves as a sensing Eve. Our objective is to maximize the mutual information (MI) for the legitimate radar sensing receiver while considering the constraint of the MI for the Eve and the quality of service to the CUs. Then, we consider the artificial noise (AN)-aided beamforming to further enhance the sensing security. Simulation results demonstrate that our proposed methods achieve MI improvement of the legitimate receiver while limiting the sensing MI of the Eve, compared with the baseline scheme, and that the utilization of AN further contributes to sensing security.**

***Index Terms*—Integrated sensing and communications, sensing security, mutual information, artificial noise.**

I. INTRODUCTION

Integrated sensing and communications (ISAC) is identified as a key 6G technology that will support various futuristic applications through the co-design of sensing and communication functionalities. In particular, supported by the implementation of the dual-functional waveform and the base stations (BSs), ISAC provides a step change from the spectral coexistence of radar and communication systems to the shared utilization of costly hardware platforms. Inspired by these favorable characteristics, various designs have been proposed for the dual-functional waveforms to promote sensing and communication performance. For example, recent works in [1] considered the Cramér-Rao bound (CRB) minimization subject to the minimum signal-to-interference-plus-noise ratio (SINR) constraints for each communication user (CU), and intelligent reflecting surface assisted sensing is studied in [2]. However, the aforementioned works have overlooked the consideration of security issues, which avail unique vulnerabilities in ISAC systems.

Due to the inherent broadcast nature of wireless signals, it is inevitable that wireless communication/sensing systems are susceptible to potential security threats. Compared with the communication-only systems, ISAC systems encounter more intricate security issues which can be generally categorized into the information security for communication and the sensing security for radar. The former arises from the fact that the probing ISAC waveform is modulated with information, which could potentially be leaked to the sensed targets that can act as eavesdroppers (Eves). To deal with this, physical layer security schemes have been proposed, such as [3] that maximized the secrecy rate by jointly optimizing the beamforming vector, the duration of snapshots, and the covariance matrix of the artificial noise (AN). Besides, the work in [4] optimized the beamforming and AN design to minimize the signal-to-noise ratio (SNR) at the Eve. The work in [5] designed the ISAC systems for securing confidential information from wiretapping from the viewpoint of information theory and studied the inner and outer bounds on its secrecy-distortion region. Additionally, a few works have highlighted the issue of radar privacy in the radar-communication spectrum sharing scenarios. In such cases, the radar information embedded within a precoder could be utilized by an adversary to infer the radar's location [6].

In contrast, the sensing security issue in ISAC systems has not been well investigated. In future ISAC deployments, there will be users subscribing to a communication service, others to a sensing service and others to both. In this case, we consider a very realistic scenario where a CU subscribing to a communication service, should not be able to exploit ISAC signals for its own sensing. Security solutions for this scenario will be of paramount importance. In particular, the transmitted waveform could be exploited by a CU, which acts as a malicious passive sensing Eve to extract sensing information about targets or their surroundings. In comparison with networks dedicated solely to communication, such a possibility introduces a unique and significant risk: the potential for privacy breaches concerning environmental and target information, as any CU within the network can illegally use the waveform for sensing. This risk poses significant challenges and the urgent need to secure the sensing functionality of ISAC

The work has been supported in part by the National Natural Science Foundation of China Grant 62331023, in part by project 6GMUSICAL part of the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme with Grant Agreement No. 101139176, and in part by Shenzhen Fundamental Research Program Grant 20220815100308002.

Jiaqi Zou is with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications (BUPT), Beijing, 100876, China, and also with the Department of Electrical and Electronic Engineering, University College London, London, WC1E 7JE, UK (e-mail: jqzou@bupt.edu.cn).

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

Fan Liu is with the School of System Design and Intelligent Manufacturing, Southern University of Science and Technology, Shenzhen 518055, China. (e-mail: liuf6@sustech.edu.cn).

Songlin Sun is with Beijing University of Posts and Telecommunications (BUPT), Beijing, 100876, China (e-mail: slsun@bupt.edu.cn).

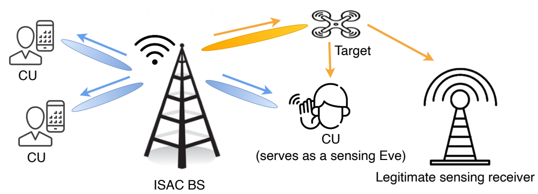

Fig. 1. System model. The BS transmits ISAC waveform for a dual purpose: simultaneously sensing the target and serving multiple CUs.

networks.

Against this background, our work proposes to address the sensing security issue for ISAC systems. In particular, we consider a bi-static ISAC scenario, simultaneously achieving multiple user communication and bi-static target estimation with a legitimate radar receiver. In this scenario, one of the CUs, granted access only to communication services, seeks unauthorized access to illegitimate sensing, therefore taking the role of a sensing Eve. To prevent sensing information leakage from the sensing Eve in ISAC networks, we formulate the sensing security problem to maximize the radar mutual information (MI) of the legitimate receiver, subject to the limitation of the radar MI of the Eve, the minimum SINR constraints of each CU and the maximum transmit power budget. Since the formulated problem is nonconvex, we propose a successive convex approximation (SCA) method combined with semidefinite relaxation (SDR) to deal with the non-convexity.

Furthermore, we propose an AN-aided secure sensing method to provide spatial degrees of freedom to degrade the radar MI of the Eve. Different from the AN in communication-only scheme which need to be carefully designed to avoid interfering with legitimate CU, we show that in sensing, the AN can act as a useful signal for the legitimate radar receiver but is harmful to the sensing Eve. Different from the AN used in communication-only schemes, which requires careful design to avoid interference with legitimate CUs, we demonstrate that in sensing functionalities, AN can serve a dual role. It acts as a useful signal for the legitimate radar receiver while simultaneously impeding sensing capabilities of the Eve. We give the derivation of radar MI with AN for the first time, and then jointly optimize the beamforming and the covariance of AN. Simulation results demonstrate significant improvement in the sensing MI of our proposed methods compared with the baseline and also reveal that through adding AN to the transmit signals of the BS, the secure sensing performance can be effectively improved.

II. System Model

We consider a bistatic multiple-input multiple-output (MIMO) ISAC system, which consists of a central BS transmitting dual-functional signals to a legitimate radar receiver and K single-antenna CUs. Simultaneously, a CU serves as an unauthorized sensing Eve who perfectly knows/intercepts the transmitted signals and also wishes to sense the targets/environment. We assume that the transmitter is equipped with a uniform linear array (ULA) of N_t antennas and that the legitimate receiver and the Eve are equipped with N_r and N_e antennas, respectively.

A. Communication Signal Model and Metrics

Let $\mathbf{h}_k \in \mathbb{C}^{N_t\times 1}$ represent the communication channel vector for the k-th use. We assume that the channel follows a slow-fading block Rician fading channel, given as

$$\mathbf{h}_k = \sqrt{\frac{K_k}{K_k+1}}\mathbf{h}_{LoS,k} + \sqrt{\frac{1}{K_k+1}}\mathbf{h}_{NLoS,k}, \tag{1}$$

where K_k denotes the Rician factor of the channel between the k-th CU and the BS. $\mathbf{h}_{LoS,k}$ denotes the deterministic LoS channel component with $\mathbf{h}_{LoS,k} = \left[1, \cdots, e^{-j\pi(N_t-1)cos\theta_k}\right]$, where $\theta_k \in [0,\pi]$ is the angle-of-arrival (AoA) of the line-of-sight (LoS) link from the k-th CU to the BS and we assume half-wavelength antenna spacing. $\mathbf{h}_{NLoS,k}$ represents the random scattered components whose elements follows $\mathcal{CN}(0,1)$.

Let us denote the beamforming matrix as $\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_k] \in \mathcal{C}^{N_t\times K}$, where $\mathbf{w}_k \in \mathbb{C}^{N_t\times 1}$ stands for the beamforming vector of the k-th user. Then, the transmitted signal at the l-th time slot can be expressed as

$$\mathbf{x}[l] = \mathbf{W}\mathbf{s}[l], \tag{2}$$

where $\mathbf{s}[l] \in \mathcal{C}^{K\times 1}$ includes K parallel communication symbol streams to be communicated to K users. Without loss of generality, we assume the communication symbols have unit power, i.e., $\mathbb{E}[\mathbf{s}[l]\mathbf{s}[l]^H] = \mathbf{I}$, and the communication channel matrix is perfectly estimated and known at the BS side. Then, we have the SINR at the k-th CU as

$$\text{SINR}_k = \frac{\left|\mathbf{h}_k^H\mathbf{w}_k\right|^2}{\sigma_c^2 + \sum_{j=1,j\neq k}^{K}\left|\mathbf{h}_k^H\mathbf{w}_j\right|^2}, \tag{3}$$

where σ_c^2 is the variance of additive white Gaussian noise.

B. Radar Signal Model

We consider a bistatic radar sensing scenario where the transmitted signals are shared between the transmitter and receiver through a control center. Denoting $\mathbf{X} = [\mathbf{x}[1], \mathbf{x}[2], \cdots, \mathbf{x}[L]] \in \mathcal{C}^{N_t\times L}$ as the transmitted waveform during L time slots, the received signal matrix at the legitimate receiver and the Eve can be expressed, respectively, as

$$\mathbf{Y}_r = \mathbf{H}_r(\boldsymbol{\theta}_r)\mathbf{X} + \mathbf{Z}_r, \mathbf{Y}_e = \mathbf{H}_e(\boldsymbol{\theta}_e)\mathbf{X} + \mathbf{Z}_e, \tag{4}$$

where $\mathbf{Z}_r$ and $\mathbf{Z}_e$ are the noise matrices at the legitimate receiver and the Eve, respectively and each columns of $\mathbf{Z}_r$ and $\mathbf{Z}_e$ follow $\mathcal{CN}(\mathbf{0}, \sigma_r^2\mathbf{I})$ and $\mathcal{CN}(\mathbf{0}, \sigma_e^2\mathbf{I})$, respectively. $\mathbf{H}_r$ and $\mathbf{H}_e$ are the target response matrices from the transmitter to the legitimate receiver and the Eve, respectively, which are determined by the target parameters of interests $\boldsymbol{\theta}_r$ and $\boldsymbol{\theta}_e$[1]. Note that $\boldsymbol{\theta}_r \neq \boldsymbol{\theta}_e$ since the legitimate receiver and the Eve may have different sensing interests to estimate different angles and ranges, etc. As Eve is a legitimate CU, we note that $\mathbf{H}_e$ can also be known at the BS, which is achievable by leveraging the knowledge of Eve's location [9].

[1]At the transmitter side, the beam direction from the transmitter to the target and the target response matrices are generally predefined, which is determined based on the location of target identified in previous observations or the central angle of the sector of interest [1], [3], [7], [8].

For radar sensing, it is essential to estimate the target response matrix, i.e., $\mathbf{H}_r$ or $\mathbf{H}_e$, as it contains the sensing information. With estimated $\mathbf{H}_r$ or $\mathbf{H}_e$ at hand, one can extract the sensing parameters in real time, such as the range, radial velocity, angular direction [10], [11]. To measure the sensing performance at the receivers, we adopt the MI between the received radar signal and target response matrix, as MI characterizes the amount of sensing information of the radar to estimate the parameters describing the target. It is also implied in [12], [13] that maximing the sensing MI enables improved performance in target parameter estimation, classification, and identification. Following [14], the sensing MI of the legitimate receiver can be given as

$$I_r(\mathbf{Y}_r;\boldsymbol{\theta}_r|\mathbf{X}) = I_r(\mathbf{Y}_r;\mathbf{H}_r|\mathbf{X}). \tag{5}$$

Vectorizing $\mathbf{Y}$, we have

$$\mathrm{vec}(\mathbf{Y}_r) = \tilde{\mathbf{X}}\mathbf{h}_r + \mathbf{z}_r, \tag{6}$$

where $\tilde{\mathbf{X}} = \mathbf{X}^T \otimes \mathbf{I}_{N_r}$, $\mathbf{h}_r = \mathrm{vec}(\mathbf{H}_r)$, and $\mathbf{z}_r = \mathrm{vec}(\mathbf{Z}_r)$ [15, Eq. 1.11.20]. Following the assumptions are also used in [11], we assume the target response vector $\mathbf{h}_r$ is zero-mean circular-symmetric Gaussian distributed with covariance $\mathbf{R}_h$. As the transmitted waveform is perfectly known, the MI between $\mathbf{Y}_r$ and $\mathbf{H}_r$ at the legitimate receiver can be expressed as

$$\begin{aligned} I_r(\mathbf{Y}_r;\mathbf{H}_r|\mathbf{X}) &= h(\mathbf{Y}_r|\mathbf{X}) - h(\mathbf{Y}_r|\mathbf{H}_r,\mathbf{X}) && \text{(7a)}\\ &= \log\det(\mathbf{I} + \sigma_r^{-2}\tilde{\mathbf{X}}\mathbf{R}_{h_r}\tilde{\mathbf{X}}^H) && \text{(7b)}\\ &= \log\det(\mathbf{I}+\sigma_r^{-2}\mathbf{R}_{h_r}(\mathbf{X}^*\mathbf{X}^T \otimes \mathbf{I}_{N_r})), && \text{(7c)} \end{aligned}$$

where we used the property of matrix determinant that $\det(\mathbf{I}+\mathbf{AB}) = \det(\mathbf{I}+\mathbf{BA})$. Let $\mathbf{R}_{h_r} = \mathbf{U}_r\boldsymbol{\Lambda}_r\mathbf{U}_r^H$ be the eigenvalue decomposition of $\mathbf{R}_{h_r}$, and $\mathbf{K}$ be a real commutation matrix satisfying $\mathbf{K}\mathbf{K}^T = \mathbf{I}$. We then have

$$\begin{aligned} I_r &= \log\det(\mathbf{I} + \sigma_r^{-2}\boldsymbol{\Lambda}_r\mathbf{U}_r^H\mathbf{K}(\mathbf{I}_{N_r} \otimes \mathbf{X}^*\mathbf{X}^T)\mathbf{K}^T\mathbf{U}_r)\\ &= \log\det(\mathbf{I} + \sigma_r^{-2}L\boldsymbol{\Lambda}_r\sum_{i=1}^{N_r}\mathbf{P}_i\mathbf{R}_{\mathbf{X}}^*\mathbf{P}_i^H), \end{aligned} \tag{8}$$

where $\mathbf{P} = \mathbf{U}_r^H\mathbf{K} = [\mathbf{P}_1, \mathbf{P}_2, \cdots, \mathbf{P}_{N_r}]$ and $\mathbf{R}_{\mathbf{X}}$ denotes the covariance matrix of the transmit signal, given as [1]

$$\mathbf{R}_{\mathbf{X}} = \frac{1}{L}\mathbf{X}\mathbf{X}^H \approx \mathbf{W}\mathbf{W}^H = \sum_{k=1}^{K}\mathbf{w}_k\mathbf{w}_k^H, \tag{9}$$

where the approximation holds when L is large enough. Similarly, the MI between $\mathbf{Y}_r$ and $\mathbf{H}_r$ at the Eve can be expressed as

$$\begin{aligned} I_e(\mathbf{Y}_e;\mathbf{H}_e|\mathbf{X}) &= \log\det(\mathbf{I} + \sigma_e^{-2}\mathbf{R}_{h_e}(\mathbf{X}^*\mathbf{X}^T \otimes \mathbf{I}_{N_e}))\\ &= \log\det(\mathbf{I} + \sigma_e^{-2}L\boldsymbol{\Lambda}_e\sum_{i=1}^{N_e}\mathbf{Q}_i\mathbf{R}_{\mathbf{X}}^*\mathbf{Q}_i^H), \end{aligned} \tag{10}$$

where $\mathbf{R}_{h_e}$ denotes the covariance of zero-mean circular-symmetric Gaussian distributed $\mathbf{h}_e = \mathrm{vec}(\mathbf{H}_e)$, whose eigenvalue decomposition is given as $\mathbf{R}_{h_e} = \mathbf{U}_e\boldsymbol{\Lambda}_e\mathbf{U}_e^H$. $\mathbf{Q} = \mathbf{U}_e^H\mathbf{K} = [\mathbf{Q}_1, \mathbf{Q}_2, \cdots, \mathbf{Q}_{N_e}]$.

III. Beamforming Design for Sensing Security without AN

In this section, we first investigate the beamforming design without the aid of AN to guarantee secure sensing. Our objective is to maximize the MI of the legitimate receiver while keeping the MI of the Eve lower than the preset threshold, and satisfying multiple users' required SINR and the power budget. The optimization problem can be formulated as follows

$$\begin{aligned} \max_{\{\mathbf{W}_k\}_{k=1}^K}\ & I_r = \log\det\left(\mathbf{I} + \sigma_r^{-2}L\boldsymbol{\Lambda}_r\sum_{i=1}^{N_r}\mathbf{P}_i\mathbf{R}_{\mathbf{X}}^*\mathbf{P}_i^H\right) && \text{(11a)}\\ \text{s.t. } & I_e{=}\log\det\left(\mathbf{I}{+}\sigma_e^{-2}L\boldsymbol{\Lambda}_e\sum_{i=1}^{N_e}\mathbf{Q}_i\mathbf{R}_{\mathbf{X}}^*\mathbf{Q}_i^H\right){\le}\epsilon, && \text{(11b)}\\ & \mathrm{tr}(\mathbf{R}_{\mathbf{X}}) \le P_0, && \text{(11c)}\\ & \frac{\mathrm{tr}\left(\mathbf{h}_k\mathbf{W}_k\mathbf{h}_k^H\right)}{\sum_{k=1,k\neq i}^{K}\mathrm{tr}\left(\mathbf{h}_k\mathbf{W}_i\mathbf{h}_k^H\right) + \sigma_c^2} \ge \gamma_k, \forall k, && \text{(11d)}\\ & \mathbf{R}_{\mathbf{X}} = \sum_{k=1}^{K}\mathbf{W}_k, \mathbf{W}_k \succeq 0, \mathrm{rank}(\mathbf{W}_k) = 1, \forall k, && \text{(11e)} \end{aligned}$$

where $\mathbf{W}_k = \mathbf{w}_k\mathbf{w}_k^H$. In general, it is challenging to solve problem (11) directly, due to the nonconvexity of the constraint (11b), (11d), and the rank-1 constraint in (11e). For addressing the nonconvex constraint (11b), we notice that I_e is a concave function in $\mathbf{R}_{\mathbf{X}}$. Thus, we give the upper-bound of (11b) based on first-order Taylor expansion at a given transmit covariance matrix $\tilde{\mathbf{R}}_{\mathbf{X}} = \sum_{k=1}^{K}\tilde{\mathbf{W}}_k$ as

$$\begin{aligned} \tilde{I}_e \triangleq\, & f(\tilde{\mathbf{R}}_{\mathbf{X}}) + \mathrm{tr}\left(\mathrm{Re}\left(2\sigma_e^{-2}L\sum_{i=1}^{N_e}\mathbf{Q}_i^T(\mathbf{M}^{-1})^*\boldsymbol{\Lambda}_e\mathbf{Q}_i^*\mathbf{R}_{\mathbf{X}}\right)\right)\\ & - \mathrm{tr}\left(\mathrm{Re}\left(2\sigma_e^{-2}L\sum_{i=1}^{N_e}\mathbf{Q}_i^T(\mathbf{M}^{-1})^*\boldsymbol{\Lambda}_e\mathbf{Q}_i^*\tilde{\mathbf{R}}_{\mathbf{X}}\right)\right). \end{aligned} \tag{12}$$

where $\mathbf{M} = \mathbf{I} + \sigma_e^{-2}L\boldsymbol{\Lambda}_e\sum_{i=1}^{N_e}\mathbf{Q}_i\tilde{\mathbf{R}}_X^*\mathbf{Q}_i^H$. The details are given in Appendix A. As such, it can be easily observed that the approximated function is convex on $\mathbf{R}_{\mathbf{X}}$. Thus, $\mathbf{R}_{\mathbf{X}}$ can be iteratively obtained by updating $\tilde{\mathbf{R}}_{\mathbf{X}}$.

Then, we focus on dealing with the rank-1 constraint in (11e), which can be equivalently transformed into an equivalent linear matrix inequality (LMI) as

$$\begin{aligned} & \begin{bmatrix}\mathbf{W}_k & \mathbf{w}_k\\ \mathbf{w}_k^H & 1\end{bmatrix} \succeq 0, && \text{(13a)}\\ & \mathrm{tr}(\mathbf{W}_k) - \mathbf{w}_k^H\mathbf{w}_k \le 0, \forall k. && \text{(13b)} \end{aligned}$$

Additionally, the non-convexity in (13b) can be handled by the first-order Taylor expansions at $\tilde{\mathbf{w}}_k$ as

$$\mathrm{tr}(\mathbf{W}_k) - \tilde{\mathbf{w}}_k^H\tilde{\mathbf{w}}_k - 2\,\mathrm{Re}\left(\tilde{\mathbf{w}}_k^H\mathbf{w}_k\right) \le 0, \tag{14}$$

where $\mathrm{Re}(\cdot)$ denotes the real part of the argument and $\tilde{\mathbf{w}}_k$ can be updated at each iteration. Therefore, a convex approximation of problem (11) is reformulated as

$$\begin{aligned} \max_{\{\mathbf{w}_k,\mathbf{W}_k\}_{k=1}^K}\ & I_r && \text{(15a)}\\ s.t.\ & \tilde{I}_e \le \epsilon, && \text{(15b)} \end{aligned}$$

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. 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/TVT.2024.3422036

$$\mathrm{tr}(\mathbf{R}_{\mathbf{X}}) \le P_0, \tag{15c}$$

$$\mathbf{W}_k \succeq 0, \mathbf{R}_{\mathbf{X}} = \sum_{k=1}^{K} \mathbf{W}_k, \tag{15d}$$

$$\mathrm{tr}\left(\mathbf{h}_k \mathbf{W}_k \mathbf{h}_k^H\right) - \gamma_k \sum_{k \neq i, k=1}^{K} \mathrm{tr}\left(\mathbf{h}_k \mathbf{W}_k \mathbf{h}_k^H\right) \ge \gamma_k \sigma_c^2, \forall k, \tag{15e}$$

$$(13a), (14), \tag{15f}$$

which is easily shown to be convex, and hence, $\mathbf{W}_k$ can be iteratively obtained by solving problem (15) based on updating $\tilde{\mathbf{w}}_k$ and $\tilde{\mathbf{W}}_k$ in an iterative manner. However, due to the stringent requirement introduced by (15b) and (13b), it is generally non-trivial to directly obtain a feasible solution as an initial point. Alternatively, we can adopt the penalty SCA [16] and introduce auxiliary variables $\bar{p}, \rho_k, \kappa$ to transform problem (15) into

$$\max_{\{\mathbf{w}_k, \mathbf{W}_k, \rho_k\}_{k=1}^K, \kappa} I_r - \bar{p}\kappa - \bar{p} \sum_{k=1}^{K} \rho_k \tag{16a}$$

$$s.t. \quad \tilde{I}_e \le \epsilon + \kappa, \tag{16b}$$

$$\mathrm{tr}(\mathbf{W}_k) - \tilde{\mathbf{w}}_k^H \tilde{\mathbf{w}}_k - 2\,\mathrm{Re}\left(\tilde{\mathbf{w}}_k^H \mathbf{w}_k\right) \le \rho_k, \tag{16c}$$

$$(13a), (15c), (15d), (15e), \tag{16d}$$

where $\bar{p}$ and ρ_k, κ denote the weight coefficient and the penalty terms, respectively. We present the proposed iterative algorithm in Algorithm 1.

Algorithm 1 : *Proposed Iterative Algorithm for Handling* (16)

Randomly set $\{\mathbf{w}_k^{(0)}, \mathbf{W}_k^{(0)}\}$, $\bar{p}^{(0)} = 10^{-3}$, $\lambda > 1$, $i = 0$;
repeat
  $i \leftarrow i + 1$;
  $\tilde{\mathbf{w}}_k^{(i)}, \tilde{\mathbf{W}}_k^{(i)} \leftarrow \mathbf{w}_k^{(i-1)}, \mathbf{W}_k^{(i-1)}$;
  Solve problem (15) to obtain the optimal $\mathbf{w}_k^{(i)}, \mathbf{W}_k^{(i)}$;
  $\bar{p}^{(i)} \leftarrow \lambda \bar{p}^{(i-1)}$
until both $I_r^{(i)} - I_r^{(i-1)}$ and the penalty terms ρ_k, κ are significantly small.

IV. Secure Sensing with AN

In this section, we consider utilizing AN to assist secure sensing. Note that the instantaneous AN matrix, $\mathbf{N}$, can be known to the legitimate receiver but remains unknown to the Eve[2].

Firstly, we give the received signal at the legitimate receiver as

$$\mathbf{Y}_r = \mathbf{H}_r(\boldsymbol{\theta}_r)\mathbf{X} + \mathbf{H}_r(\boldsymbol{\theta}_r)\mathbf{N} + \mathbf{Z}_r. \tag{17}$$

Then, the MI of the legitimate receiver can be expressed as

$$I_r(\mathbf{Y}_r; \boldsymbol{\theta}_r | \mathbf{X}, \mathbf{N}) = I_r(\mathbf{Y}_r; \mathbf{H}_r | \mathbf{X}, \mathbf{N}) \tag{18a}$$

$$= h(\mathbf{Y}_r | \mathbf{X}, \mathbf{N}) - h(\mathbf{Y}_r | \mathbf{H}_r, \mathbf{X}, \mathbf{N}) \tag{18b}$$

$$= \log\det(\mathbf{I} + \sigma_r^{-2}(\tilde{\mathbf{X}} + \tilde{\mathbf{N}})\mathbf{R}_{h_r}(\tilde{\mathbf{X}} + \tilde{\mathbf{N}})^H) \tag{18c}$$

$$= \log\det(\mathbf{I} + \sigma_r^{-2}(\tilde{\mathbf{X}} + \tilde{\mathbf{N}})^H(\tilde{\mathbf{X}} + \tilde{\mathbf{N}})\mathbf{R}_{h_r}) \tag{18d}$$

$$\overset{(a)}{\approx} \log\det\left(\mathbf{I} + \sigma_r^{-2} L \mathbf{K}(\mathbf{I}_{N_r} \otimes (\mathbf{R}_{\mathbf{X}}^* + \mathbf{R}_{\mathbf{N}}^*))\mathbf{K}^T \mathbf{R}_{h_r}\right) \tag{18e}$$

$$= \log\det\left(\mathbf{I} + \sigma_r^{-2} L \boldsymbol{\Lambda}_r \sum_{i=1}^{N_r} \mathbf{P}_i (\mathbf{R}_{\mathbf{X}}^* + \mathbf{R}_{\mathbf{N}}^*)\mathbf{P}_i^H\right), \tag{18f}$$

where $\tilde{\mathbf{N}} = \mathbf{N}^T \otimes \mathbf{I}_{N_r}$ and $\mathbf{R}_{\mathbf{N}} = \frac{1}{L}\mathbf{N}\mathbf{N}^H$.

On the other hand, as the Eve has no prior knowledge of AN, the received signal and the MI at the Eve can be given as

$$\mathbf{Y}_e = \mathbf{H}_e(\boldsymbol{\theta}_e)\mathbf{X} + \mathbf{H}_e(\boldsymbol{\theta}_e)\mathbf{N} + \mathbf{Z}_e, \tag{19}$$

and

$$I_e(\mathbf{Y}_e; \boldsymbol{\theta}_e | \mathbf{X}) = I_e(\mathbf{Y}_r; \mathbf{H}_e | \mathbf{X}) = h(\mathbf{Y}_e | \mathbf{X}) - h(\mathbf{Y}_e | \mathbf{H}_e, \mathbf{X}), \tag{20}$$

respectively. Then, we have

$$\begin{aligned} & h(\mathbf{Y}_e | \mathbf{H}_e, \mathbf{X}) \\ &= -\int_{\mathcal{X},\mathcal{Y},\mathcal{H}} f(\mathbf{X}, \mathbf{Y}, \mathbf{H}) \log f(\mathbf{Y}|\mathbf{X}, \mathbf{H}) d\mathbf{X} d\mathbf{Y} d\mathbf{H} \\ &= -\int_{\mathcal{X},\mathcal{H}} f(\mathbf{X}, \mathbf{H}) \int_{\mathcal{Y}} f(\mathbf{Y}|\mathbf{X}, \mathbf{H}) \log f(\mathbf{Y}|\mathbf{X}, \mathbf{H}) d\mathbf{Y} d\mathbf{X} d\mathbf{H} \\ &= \int_{\mathcal{X},\mathcal{H}} f(\mathbf{X}, \mathbf{H}) \log\left((2\pi e)^n \det\left(L(\mathbf{R}_{\mathbf{N}}^* \otimes \mathbf{I}_{N_e})\mathbf{h}_e \mathbf{h}_e^H + \sigma_e^2 \mathbf{I}\right)\right) d\mathbf{X} d\mathbf{H} \\ &\approx \frac{1}{J} \sum_{j=1}^{J} \log\det\left(2\pi e L(\mathbf{R}_{\mathbf{N}}^* \otimes \mathbf{I}_{N_e})\mathbf{h}_{e,j}\mathbf{h}_{e,j}^H + \sigma_e^2 \mathbf{I}\right), \\ &= \frac{1}{J} \sum_{j=1}^{J} \log\det\left(2\pi e L \mathbf{K}(\mathbf{I}_{N_e} \otimes \mathbf{R}_{\mathbf{N}}^*)\mathbf{K}^T \mathbf{h}_{e,j}\mathbf{h}_{e,j}^H + \sigma_e^2 \mathbf{I}\right) \end{aligned} \tag{21a}$$

where $\mathbf{h}_{e,j}(\boldsymbol{\theta})$ is the j-th sample of the random variable $\mathbf{h}_e(\boldsymbol{\theta})$. However, it's still difficult to derive the exact expression of $h(\mathbf{Y}_e|\mathbf{X})$ due to the additive non-Gaussian noise of $\mathbf{H}_e(\boldsymbol{\theta}_e)\mathbf{N}$. To deal with this, we can give the upper bound of $h(\mathbf{Y}_e|\mathbf{X})$ as

$$\bar{h}(\mathbf{Y}_e | \mathbf{X}) = \log\det\left(2\pi e\left(\sigma_e^2 \mathbf{I} + \mathbf{R}_{HN}\right)\right), \tag{22}$$

where $\mathbf{R}_{HN}$ denotes the covariance of $\mathrm{vec}(\mathbf{HN})$, given as

$$\begin{aligned} \mathbf{R}_{HN} &= \mathbb{E}_{\mathbf{H},\mathbf{N}}\left[(\mathbf{I}_L \otimes \mathbf{H}_e)\,\mathrm{vec}(\mathbf{N})\,(\mathrm{vec}(\mathbf{N}))^H\,(\mathbf{I}_L \otimes \mathbf{H}_e)^H\right] \\ &= \mathbb{E}_{\mathbf{H}}\left[(\mathbf{I}_L \otimes \mathbf{H}_e)\,\mathbb{E}_{\mathbf{H}}\left[\mathrm{vec}(\mathbf{N})\,(\mathrm{vec}(\mathbf{N}))^H\right](\mathbf{I}_L \otimes \mathbf{H}_e)^H\right] \\ &= \mathbb{E}_{\mathbf{H}}\left[(\mathbf{I}_L \otimes \mathbf{H}_e)\,(\mathbf{I}_L \otimes \mathbf{R}_{\mathbf{N}})\,(\mathbf{I}_L \otimes \mathbf{H}_e)^H\right] \\ &\approx \frac{1}{J} \sum_{j=1}^{J} (\mathbf{I}_L \otimes \mathbf{H}_{e,j})\,(\mathbf{I}_L \otimes \mathbf{R}_{\mathbf{N}})\,(\mathbf{I}_L \otimes \mathbf{H}_{e,j})^H \end{aligned} \tag{23a}$$

Combining with (22), we derive the approximate upper bound of I_e as

[2]As indicated in the literature of physical layer secuirity [17]–[19], a large set of seeds for a Gaussian pseudorandom generator can be prestored at both transmitter and legitimate sensing receiver. Then, the transmitter regularly picks up one seed and securely delivers its index to the legitimate sensing receiver through the control center.

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. 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/TVT.2024.3422036

$$I_e = h(\mathbf{Y}_e|\mathbf{X}) - h(\mathbf{Y}_e|\mathbf{H}_e, \mathbf{X}) < \bar{I}_e = \bar{h}(\mathbf{Y}_e|\mathbf{X}) - h(\mathbf{Y}_e|\mathbf{H}_e, \mathbf{X}), \tag{24}$$

where

$$\bar{I}_e \approx \log\det\left(\sigma_e^2\mathbf{I} + \frac{1}{J}\sum_{j=1}^{J}\left(\mathbf{I}_L \otimes \mathbf{H}_{e,j}\right)\left(\mathbf{I}_L \otimes \mathbf{R_N}\right)\left(\mathbf{I}_L \otimes \mathbf{H}_{e,j}\right)^H\right) - \frac{1}{J}\sum_{j=1}^{J}\log\det\left(L\mathbf{K}(\mathbf{I}_{N_e} \otimes \mathbf{R}_\mathbf{N}^*)\mathbf{K}^T\mathbf{h}_{e,j}\mathbf{h}_{e,j}^H + \sigma_e^2\mathbf{I}\right).$$

Then, the problem of sensing security with AN can be formulated as

$$\max_{\{\mathbf{W}_k\}_{k=1}^K, \mathbf{R_N}} \quad I_r(\mathbf{Y}_r; \boldsymbol{\theta}_r|\mathbf{X}, \mathbf{N}) \tag{25a}$$

$$\text{s.t.} \quad \bar{I}_e \le \epsilon, \tag{25b}$$

$$\frac{\mathrm{tr}\left(\mathbf{h}_k\mathbf{W}_k\mathbf{h}_k^H\right)}{\sum_{k=1,k\neq i}^{K}\mathrm{tr}\left(\mathbf{h}_k\mathbf{W}_i\mathbf{h}_k^H\right) + \mathbf{h}_k\mathbf{R_N}\mathbf{h}_k^H + \sigma_c^2} \ge \gamma_k, \forall k, \tag{25c}$$

$$\mathrm{tr}\left(\sum_{k=1}^{K}\mathbf{W}_k + \mathbf{R_N}\right) \le P_0, \tag{25d}$$

(11e).

As previously discussed, the formulated problem is not convex due to the nonconvexity of (25b). Hence, we introduce an auxiliary matrix $\mathbf{Q}$ and reformulate (25b) based on the Taylor expansion at $\tilde{\mathbf{Q}}$ as

$$\log\det(\tilde{\mathbf{Q}}) + \mathrm{tr}(\tilde{\mathbf{Q}}(\mathbf{Q} - \tilde{\mathbf{Q}})) - \frac{1}{J}\sum_{j=1}^{J}\log\det\left(L\mathbf{K}(\mathbf{I}_{N_e} \otimes \mathbf{R}_\mathbf{N}^*)\mathbf{K}^T\mathbf{h}_{e,j}\mathbf{h}_{e,j}^H + \sigma_e^2\mathbf{I}\right) \le \epsilon, \tag{26a}$$

$$\mathbf{Q} - \left(\sigma_e^2\mathbf{I} + \frac{1}{J}\sum_{j=1}^{J}\left(\mathbf{I}_L \otimes \mathbf{H}_{e,j}\right)\left(\mathbf{I}_L \otimes \mathbf{R_N}\right)\left(\mathbf{I}_L \otimes \mathbf{H}_{e,j}\right)^H\right) \succeq 0. \tag{26b}$$

Therefore, a convex approximation of problem (25) is reformulated as

$$\max_{\{\mathbf{w}_k, \mathbf{W}_k\}_{k=1}^K, \mathbf{R_N}} \quad I_r \tag{27a}$$

$$\text{s.t.} \quad (13a), (14), (15d), (25c), (25d), (26a), (26b), \tag{27b}$$

which can be solved in a similar iterative manner as in Algorithm 1.

Convergence and complexity analysis: We can note that in the iterative procedure of the algorithm, (27) can be optimally solved and the optimal value of its objective function serves as a lower bound on that of (25). Therefore, it can be guaranteed that the optimal value at n-th iteration n, denoted as $p_*^{(n)}$, always satisfies $p_*^{(n)} \ge p_*^{(n-1)}$. Therefore, the algorithm produces a non-decreasing objective function of problem (25). As there exists K LMI constraints of size $N_t + 1$, and K LMI constraints of size N_t in (27), the worst-case computational complexity is $\mathcal{O}(M^{6.5}K^{3.5}\ I_{\text{iter}}\ln(1/\epsilon_0))$ given the required accuracy $\epsilon_0 > 0$, where I_{iter} denotes the number of iterations [20].

V. Simulation Results

In this section, we provide numerical analysis to evaluate the performance of the proposed algorithms, including secure sensing de without AN and MI gap maximization with AN. We consider a dual-functional BS transceiver equipped with N_t = 6 transmit antennas for MIMO radar sensing and multi-user communication, serving $K = 3$ CUs where one of the CU serves as the sensing Eve. The legitimate radar receiver is equipped with $N_r = 2$ receive antennas. Unless stated otherwise, the available power budget $P_{\text{max}} = 30$ dBm and the frame length $L = 30$.

Fig. 2 firstly demonstrates the convergence behavior of the proposed method without the aid of AN, under different power budgets and numbers of users. It can be seen that all three cases converge after 3 iterations, which verifies the fast convergence rate and the efficiency of our proposed alternating algorithm. With increasing P_0, the MI increases, since more power budget can be utilized to sense the target and satisfy the SINR constraints of multiple users. Moreover, increasing the number of CUs leads to a slight reduction in the sensing performance.

Fig. 3 compares the MI performance with different transmitted power budgets. We compare our proposed methods with two baseline schemes: the widely-used zero-forcing beamforming (ZF) and multi-user broadcasting beamforming design [21, Sec. 7.6.1] (MU-BC). It can be seen that I_r of the proposed method is higher than that of the baseline schemes, with constrained I_e that guarantees sensing security. With the increase of transmit power budget, the gap between I_r and I_e of the proposed algorithms achieves over 2 times higher than that of the baseline schemes. Moreover, it can be observed that the use of AN further improves the sensing MI of the legitimate receiver and while simultaneously increasing the MI performance gap. This observation indicates that the incorporation of AN can assisted sensing security with guaranteed communication SINR performance. This effectiveness arises because AN serves a dual role: it provides beneficial power for the legitimate receiver while acting as interference for the Eve. Plus, the designed AN simultaneously aligns closely with the null space of the communication channel to avoid degrading communication performance.

VI. Conclusion and Future Works

This paper addressed the sensing security issue for ISAC systems by beamforming design. The MI of radar sensing between the legitimate receiver was maximized while taking into account the MI of the potential Eve, power budget, and SINR constraints. Additionally, we adopted AN to further guarantee secure sensing. Simulation results demonstrated the effectiveness of the proposed methods in achieving a superior MI compared to the baseline scheme, with the AN further contributing to sensing security. The theoretical analysis and simulation results show that to secure sensing, network designers have the option to employ beamforming only, which can meet the basic sensing security requirements. However, for the tasks requiring higher sensitivity and enhanced sensing

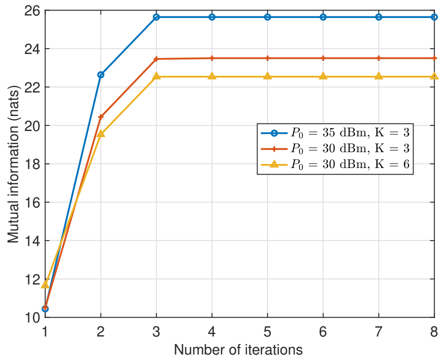

Fig. 2. MI of the legitimate receiver versus the number of iterations. The limitation of Eve's MI is $\epsilon = 5$ nats and SINR threshold is $\gamma_k = 20$ dB.

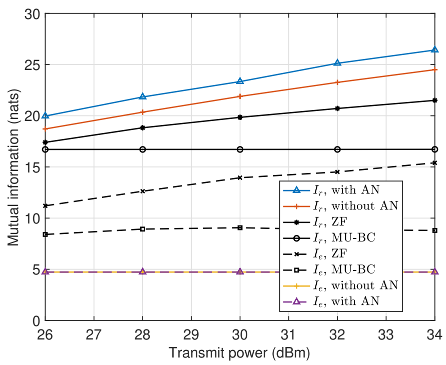

Fig. 3. MI versus the transmit power budget, in both with and without AN-aided case, compared with the baselines. The limitation of the MI of the Eve is set as $\epsilon = 5$ nats and the SINR threshold is $\gamma_k = 28$ dB.

security, the joint design of transmit beamforming and AN should be considered. This approach, while offering superior security, necessitates more intricate derivations and analysis. Future works can consider the sensing security in ISAC networks that incorporate multi-antenna CUs, including the investigation of the joint transmitter-receiver design.

Appendix A

Here, we provide the proof for the MI approximation for the Eve in (10) based on a Taylor series expansion. First, defining $f(\mathbf{R_X}) = \log\det(\mathbf{I} + \sigma_e^{-2}T\mathbf{\Lambda}_e \sum_{i=1}^{N_r} \mathbf{Q}_i\mathbf{R}_\mathbf{X}^*\mathbf{Q}_i^H)$,we have the Jacobian matrix of $f(\mathbf{R_X})$ expressed as

$$\mathrm{D}_{\mathbf{R}_\mathbf{X}^*} f(\mathbf{R_X}) = \sigma_e^{-2}T\sum_{i=1}^{N_e}\mathbf{Q}_i^H\mathbf{M}^{-1}\mathbf{\Lambda}_e\mathbf{Q}_i. \tag{28}$$

Following [21, Sec. 1.1.11] and [15, Sec. 3.1], the gradient of $f(\mathbf{R_X})$ can be given as

$$\nabla_{\mathbf{R_X}} f(\mathbf{R_X}) = 2\nabla_{\mathbf{R}_\mathbf{X}^*} f(\mathbf{R_X}) = 2\sigma_e^{-2}T\sum_{i=1}^{N_e}\mathbf{Q}_i^T\mathbf{\Lambda}_e(\mathbf{M}^{-1})^T\mathbf{Q}_i^*,$$

Then, an affine Taylor series approximation of $f(\mathbf{R_X})$ at $\mathbf{R_X} = \tilde{\mathbf{R}}_\mathbf{X}$ can be written as

$$\begin{aligned} f(\mathbf{R_X}) &\simeq f(\tilde{\mathbf{R}}_\mathbf{X}) + \mathrm{tr}\left(\mathrm{Re}\left(\nabla f(\tilde{\mathbf{R}}_\mathbf{X})^H\left(\mathbf{R_X} - \tilde{\mathbf{R}}_\mathbf{X}\right)\right)\right) \\ &= f(\tilde{\mathbf{R}}_\mathbf{X}) + \mathrm{tr}\left(\mathrm{Re}\left(2\sigma_e^{-2}T\sum_{i=1}^{N_e}\mathbf{Q}_i^T(\mathbf{M}^{-1})^*\mathbf{\Lambda}_e\mathbf{Q}_i^*\mathbf{R_X}\right)\right) \\ &\quad - \mathrm{tr}\left(\mathrm{Re}\left(2\sigma_e^{-2}T\sum_{i=1}^{N_e}\mathbf{Q}_i^T(\mathbf{M}^{-1})^*\mathbf{\Lambda}_e\mathbf{Q}_i^*\tilde{\mathbf{R}}_\mathbf{X}\right)\right) \end{aligned} \tag{29}$$

References

[1] F. Liu, Y.-F. Liu, A. Li, C. Masouros, and Y. C. Eldar, "Cramér-Rao bound optimization for joint radar-communication beamforming," *IEEE Trans. Signal Process.*, vol. 70, pp. 240–253, Dec. 2021.

[2] M. Hua, Q. Wu, W. Chen, Z. Fei, H. C. So, and C. Yuen, "Intelligent reflecting surface assisted localization: Performance analysis and algorithm design," *IEEE Wireless Communications Letters*, Jan. 2024.

[3] D. Xu, X. Yu, D. W. K. Ng, A. Schmeink, and R. Schober, "Robust and secure resource allocation for ISAC systems: A novel optimization framework for variable-length snapshots," *IEEE Trans. Commun.*, vol. 70, no. 12, pp. 8196–8214, Dec. 2022.

[4] N. Su, F. Liu, and C. Masouros, "Secure radar-communication systems with malicious targets: Integrating radar, communications and jamming functionalities," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 83–95, Jan. 2020.

[5] O. Günlü, M. R. Bloch, R. F. Schaefer, and A. Yener, "Secure integrated sensing and communication," *IEEE J. Sel. Areas Commun.*, vol. 4, pp. 40–53, May 2023.

[6] A. Dimas, M. A. Clark, B. Li, K. Psounis, and A. P. Petropulu, "On radar privacy in shared spectrum scenarios," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Brighton, UK, May 2019, pp. 7790–7794.

[7] J. Li and P. Stoica, "Mimo radar with colocated antennas," *IEEE Signal Process. Mag.*, vol. 24, no. 5, pp. 106–114, 2007.

[8] H. Hua, J. Xu, and T. X. Han, "Optimal transmit beamforming for integrated sensing and communication," *IEEE Trans. Veh. Technol.*, Mar. 2023.

[9] O. Kanhere and T. S. Rappaport, "Position location for futuristic cellular communications: 5g and beyond," *IEEE Commun. Mag.*, vol. 59, no. 1, pp. 70–75, Jan. 2021.

[10] C. Ouyang, Y. Liu, H. Yang, and N. Al-Dhahir, "Integrated sensing and communications: A mutual information-based framework," *IEEE Commun. Mag.*, vol. 61, no. 5, pp. 26–32, 2023.

[11] Y. Yang and R. S. Blum, "MIMO radar waveform design based on mutual information and minimum mean-square error estimation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 43, no. 1, pp. 330–343, Jan. 2007.

[12] B. Tang and J. Li, "Spectrally constrained mimo radar waveform design based on mutual information," *IEEE Trans. Signal Process.*, vol. 67, no. 3, pp. 821–834, 2018.

[13] M. R. Bell, "Information theory and radar waveform design," *IEEE Trans. Inf. Theory*, vol. 39, no. 5, pp. 1578–1597, Sep. 1993.

[14] F. Liu, Y. Xiong, K. Wan, T. X. Han, and G. Caire, "Deterministic-random tradeoff of integrated sensing and communications in gaussian channels: A rate-distortion perspective," in *Proc. IEEE Int. Symp. Inf. (ISIT)*. Taipei, Taiwan, 2023.

[15] X. Zhang, *Matrix analysis and applications*. 2nd ed. Beijing, China: Tsinghua Univ. Press, 2013.

[16] C. Wang, Z. Li, T.-X. Zheng, D. W. K. Ng, and N. Al-Dhahir, "Intelligent reflecting surface-aided secure broadcasting in millimeter wave symbiotic radio networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 11 050–11 055, Oct. 2021.

[17] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[18] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, and R.-F. Liao, "Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2108–2117, Aug. 2017.

[19] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Jun. 2011.

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

[21] C.-Y. Chi, W.-C. Li, and C.-H. Lin, *Convex optimization for signal processing and communications: from fundamentals to applications*. CRC press, 2017.