Secure Beamforming with IRS-Enhanced Phase Shifting for ISAC Systems

Zhiyi Wang, *Graduate Student Member, IEEE*, Yaoqiang Xiao, Jun Wang, *Graduate Student Member, IEEE*, Yuqing Li, Yonghong Zeng, *Fellow, IEEE*, Sumei Sun, *Fellow, IEEE*

***Abstract*—This paper explores physical layer security in integrated sensing and communication (ISAC) systems enhanced by an intelligent reflecting surface (IRS), where a base station (BS) operates in a multi-user multi-eavesdropper multi-input single-output (MU-ME-MISO) scenario to deliver information to multiple legitimate users (LUs) while simultaneously detecting multiple unauthorized eavesdroppers. A key challenge in designing secure ISAC systems arises from balancing effective communication, precise target sensing, and robust security measures simultaneously under practical resource constraints. To address these issues, the IRS is leveraged not only to enhance communication performance but also to prevent confidential information from being intercepted by malicious targets. Furthermore, the BS emits a specialized sensing waveform alongside the communication signal, aiming to improve sensing accuracy while safeguarding against information leakage. A joint optimization problem of IRS phase configuration as well as the design of both communication and radar beamformers is formulated to maximize the minimum beampattern gain of all target directions, incorporating constraints to guarantee the required signal-to-interference-plus-noise ratio (SINR) levels for LUs and to limit the information leakage to adversarial entities. To address the inherent non-convexity of the problem, an alternating optimization (AO) approach leveraging semi-definite relaxation (SDR) and Gaussian randomization is proposed. Numerical results verify that the proposed scheme can effectively enhance quality of service for LUs and simultaneously suppress the SINR of eavesdroppers.**

***Index Terms*—Physical layer security, integrated sensing and communication (ISAC), beamforming, intelligent reflecting surface (IRS).**

This research is supported in part by the China Scholarship Council under Grant no. 202306130099, in part by the National Natural Science Foundation of China (61975054), in part by the Natural Science Foundation of Hunan Province (2022JJ30170), in part by the Natural Science Foundation of Changsha (kq2502089) and in part by the National Research Foundation, Singapore and Infocomm Media Development Authority under its Future Communications Research & Development Programmee (~~FCP-ASTAR-TG-2022-003, FCP-NUS-RG-2022-018~~). (*Corresponding author: Yaoqiang Xiao*)

Zhiyi Wang is with the College of Computer Science and Electronic Engineering, Hunan University, Changsha, 410082, China, and also with the Institute for Infocomm Research, Agency for Science, Technology and Research, Singapore (e-mail: wangzhiyi1@hnu.edu.cn).

Yaoqiang Xiao and Yuqing Li are with the College of Computer Science and Electronic Engineering, Hunan University, Changsha, 410082, China (e-mail: {yaoqiangxiao, yuqing}@hnu.edu.cn).

Jun Wang is with the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China (e-mail: junwang@std.uestc.edu.cn).

Yonghong Zeng and Sumei Sun are with the Institute for Infocomm Research, Agency for Science, Technology and Research, Singapore (e-mail: {yhzeng, sunsm}@i2r.a-star.edu.sg).

I. Introduction

As 6G wireless communication networks evolve, there is a constant rise in the requirements for higher spectrum efficiency and data transmission rates [1]. The operating frequencies for both communication and radar systems are constantly expanding and overlapping, and high-frequency bands and large bandwidths can enable radar sensing capabilities to support higher resolution and speed [2]–[5]. To enhance band utilization, conserve limited spectral resources, and meet the demands of emerging technologies such as unmanned aerial vehicles and autonomous driving, both high-quality wireless communication capabilities and robust, precise sensing abilities are essential [6]–[9]. Consequently, the integration of communication and sensing has become a core enabling technology in upcoming network architectures.

However, unlike wired networks, wireless signals propagate through open air, making them susceptible to eavesdropping, interception, and other forms of unauthorized access [10], [11]. In the integrated sensing and communication (ISAC) scenario, radar targets may act as potential eavesdroppers, capable of intercepting detection waveforms that embed communication data, which can lead to unintended disclosure of confidential information. [12]. The intricate structure of communication networks, combined with the inherent openness of wireless channels, makes it challenging to deploy complex upper-layer encryption algorithms in wireless systems. Traditional cryptographic techniques are often computationally intensive and may not adequately address new security challenges or meet the increasing need for rapid, low-latency data transmission [13]. Therefore, the unique physical layer security challenges in ISAC system become increasingly complex and critical.

Various schemes have been investigated in recent decades to safeguard wireless transmissions at the physical layer [14]–[16]. While currently, the exploration of physical layer security for integrated system remain at an early stage [17]. Recent efforts have concentrated on mitigating the susceptibility of ISAC by developing the protected ISAC transmission techniques [18], [19]. In addition, deploying intelligent reflecting surfaces (IRS) has emerged as a promising solution for strengthening physical layer security in wireless networks [20]. An IRS consists of a planar array of elements capable of dynamically tuning the phase of incoming electromagnetic signals to create favorable propagation conditions [21]–[24]. By intelligently controlling these elements, an IRS can enhance signal strength toward intended users and attenuate the signal received by unauthorized parties, thereby improving

the overall security and performance of wireless transmissions [25]. The physical layer security for IRS-assisted networks is investigated in [26], which utilizes block coordinate descent and the minorization-maximization framework to tackle the optimization of secrecy rates. However, this approach does not focus on ISAC systems. Secure beamforming strategies for IRS-aided ISAC setups are discussed in [27], [28], where the analysis is limited to cases with one legitimate user and one sensing target. Moreover, the authors in [29] presents a framework that leverages artificial noise to jointly optimize both active and passive beamforming, aiming to enhance the aggregate secrecy rate in a multi-user single-eavesdropper (MU-SE) multi-input single-output (MISO) ISAC configuration. In [30], strong radar signals are intentionally employed as jamming sources, combined with optimized beamforming, to suppress the maximum signal-to-interference-plus-noise ratio (SINR) at potential eavesdroppers in MU-SE scenario. Meanwhile, a secure IRS-enabled ISAC system has been investigated where the direct path for radar sensing is obstructed, highlighting that the inclusion of dedicated sensing waveforms can further boost overall system performance [31]. Although many optimization algorithms have delivered impressive simulation and theoretical results, their practical implementation is challenged by high computational complexity. Recent advances in IRS-enhanced ISAC systems have inspired a range of learning-based beamforming designs [32]. Deep learning techniques can reduce the costs, but their reliance on large training datasets limit adaptability. In contrast, deep reinforcement learning (DRL) eliminates the need for labeled data and enables efficient online learning offering a distinct advantage in large-scale optimization [33]. Such approaches optimize performance metrics like power allocation [34], energy efficiency [35], interference coordination [36], and downlink SNR [37]. On the security front, learning-based solutions have been applied to enhance system resilience. A physical-layer security scheme is designed to prevent unauthorized interception in visible light communication (VLC) channels [38]. An intelligent DRL-based beamforming frameworks have demonstrated that optimal base station (BS) and IRS reflecting beamforming designs can be maintained even under rapidly changing channel conditions [39]. Additionally, simultaneously transmitting and reflecting RIS (STAR-RIS) have been incorporated into secure ISAC systems to serve dual roles in communication and sensing across opposite sides of the surface. This method employ off-policy actor-critic algorithm to dynamically tune the transmission strategy at the BS as well as the configuration of the STAR-RIS, thereby reinforcing physical layer security [40]. However, most above studies assume that targets are passive and do not attempt to access the transmitted information. In practice, both sensing and communication signals are transmitted in ISAC, which malicious targets may exploit to intercept sensitive information. Therefore, achieving both high communication quality of service and accurate sensing performance while preventing information leakage has largely been overlooked. Moreover, only a few works have considered scenarios involving multiple eavesdroppers in IRS-aided ISAC systems. It remains challenging for IRS to assist in both communication and radar sensing to enhance transmission performance and physical layer security in ISAC systems.

Inspired by these prior researches and problems, this paper explores an IRS-enhanced secure scheme for ISAC systems. Specifically, a multi-user multi-eavesdropper MISO (MU-ME-MISO) configuration is considered, where a BS with multiple antennas concurrently transmits to several legitimate users and senses multiple malicious eavesdroppers. The scenario includes both direct and reflective links between the BS and targets, with the IRS introduced to establish reflective sensing links and enhance overall system performance. This paper makes the following primary contributions:

- We explore a secure IRS-aided ISAC system using a MU-ME-MISO configuration, aiming at simultaneously ensuring physical layer security and improving transmission performance. An integrated sensing waveform is introduced and transmitted alongside the communication signal to enhance sensing accuracy and mitigate the risk of information leakage.
- A joint optimization problem of IRS phase shifts and transmit beamformers vectors is established, targeting both communication and radar signal requirements. The goal is to maximize the minimum beampattern gain across all sensing eavesdroppers, with explicit constraints imposed on minimum required SINR for legitimate users and maximum information leakage allowed for malicious eavesdroppers.
- To effectively tackle inherent non-convexity challenge, an alternating optimization (AO) approach leveraging semi-definite relaxation (SDR) and Gaussian randomization is proposed. The proposed algorithm exhibits practical computational complexity and robust convergence characteristics.
- Extensive Numerical results verify the proposed scheme achieves a favorable trade-off between communication security and sensing performance. Specifically, the IRS significantly enhances beampattern gains and effectively suppresses SINR at malicious eavesdroppers, preventing unauthorized access to sensitive information while maintaining satisfactory quality of service (QoS) for legitimate users. Furthermore, our algorithm achieves superior convergence performance and higher beampattern gains compared to existing benchmark schemes.

The remainder of this paper is structured as follows: Section II introduces the system model, and section III formulates the optimization problem. Section IV provides a comprehensive description of the proposed solution. Section V presents the simulation results and discussions. The conclusions are presented in Section VI.

Notations: Italic letters denote scalar quantities, whereas boldface letters are used for vectors and matrices. The notation $|x|$ indicates the absolute value of a scalar x, while $\|\mathbf{x}\|$ denotes the Euclidean norm of a complex vector $\mathbf{x}$. $\mathrm{diag}(\mathbf{x})$ constructs a diagonal matrix with the elements of vector $\mathbf{x}$ on its main diagonal. $\mathbb{C}^{m\times n}$ designates the set of all $m \times n$ complex matrices. A random variable x that follows a circularly symmetric complex Gaussian distribution with mean μ and variance σ^2 is denoted as $x \sim \mathcal{CN}(\mu, \sigma^2)$.

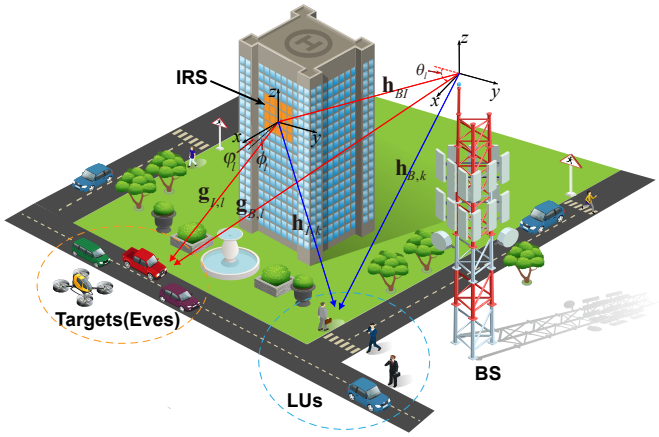


Fig. 1: System model.

The Kronecker product is represented by the operator $\otimes$, and $\mathcal{O}(\cdot)$ stands for big-O computational complexity. For a square matrix $\mathbf{S}$, $\mathrm{Tr}(\mathbf{S})$ gives the trace, and $\mathbf{S} \succeq 0$ means that $\mathbf{S}$ is positive semi-definite. For a general matrix $\mathbf{X}$, $\mathbf{X}^H$ refers to its Hermitian (conjugate transpose), $\mathrm{rank}(\mathbf{X})$ indicates its rank, and $\mathbf{X}_{i,j,k}$ specifies the (i,j,k)-th entry. The expectation operator is denoted by $\mathbb{E}\{\cdot\}$.

II. System Model

As illustrated in Fig. 1, this paper considers a dual-functional ISAC setup where the BS is equipped with M uniform linear array (ULA) antennas serving both communication and radar sensing.The system includes K legitimate users (LUs) and L targets as eavesdroppers (Eves). The orange part of the building features an IRS comprising N reflecting elements, which is deployed to improve the QoS for LUs and safeguard confidential transmissions from being intercepted by unauthorized targets. In practical scenarios such as military applications, these sensing targets may represent adversarial units, e.g., enemy drones or surveillance vehicles, which not only are sensed by radar but also actively attempt to intercept sensitive communication signals. Similarly, in civilian contexts involving critical infrastructure, radar targets could be unauthorized drones or malicious devices aiming to intercept confidential communications between the control center and security units. Thus, it is practical and essential to model these radar-sensed targets as potential eavesdroppers. For simplicity, let $\mathcal{M}$, $\mathcal{K}$, $\mathcal{L}$ and $\mathcal{N}$ represent the collections of BS transmit antennas, LUs, Eves and IRS elements, respectively.

We consider scenarios where the BS has knowledge of all LUs and sensing targets and their channel state information (CSI). We assume perfect CSI to facilitate clear analysis and to evaluate an upper bound on system performance [1]. Pilot signals are transmitted by the LUs to assist the BS in estimating the channel state information. Consequently, the BS can obtain accurate instantaneous CSI for LUs. Eve's CSI is obtained by analyzing the radar echoes observed by the BS in prior sensing intervals. The ISAC signal at the BS is represented as

$$\mathbf{s} = \sum_{k=1}^{K} \mathbf{w_{c,k}} s_{c,k} + \sum_{m=1}^{M} \mathbf{w_{r,m}} s_{r,m}, \tag{1}$$

where $s_{c,k} \in \mathbb{C}^K$ represents the communication signal associated with k_{th} LU and $s_{r,m} \in \mathbb{C}^M$ denotes the m-th radar signal, both satisfying $s_{c,k}, s_{r,m} \sim \mathcal{CN}(0,1)$. Communication and radar signals are assumed mutually independent, ensuring $\mathbb{E}\{s_{r,m} s_{c,k}^H\} = 0$, $k \in \mathcal{K}$, $m \in \mathcal{M}$. $\mathbf{w}_{c,k} \in \mathbb{C}^{M\times 1}$ and $\mathbf{w}_{r,m} \in \mathbb{C}^{M\times 1}$ represent the beamforming vectors for communication and radar.

A. Communication Signal Model

Let $\mathbf{\Theta} = \mathrm{diag}(\upsilon_1, \upsilon_2, \ldots, \upsilon_N)$ be the IRS reflection phase shifts, where $\upsilon_n = e^{j\vartheta_n}, \forall n \in \mathcal{N}$. The quasi-static block fading channels are considered in this paper. Denote $\mathbf{h}_{B,k}^H \in \mathbb{C}^{1\times M}$, $\mathbf{h}_{I,k}^H \in \mathbb{C}^{1\times N}$, $\mathbf{h}_{BI} \in \mathbb{C}^{N\times M}$ as the channels matrices corresponding to the BS-k_{th} LU, IRS-k_{th} LU and BS-IRS links, respectively. Therefore, for the k_{th} LU, the received signal is

$$y_{c,k} = \left(\mathbf{h}_{B,k}^H + \mathbf{h}_{I,k}^H \mathbf{\Theta} \mathbf{h}_{BI}\right) \mathbf{s} + u_{c,k}, \tag{2}$$

where $u_{c,k}$ represents the Gaussian noise that follows the distribution of $\mathcal{CN}(0, \sigma_{c,k}^2)$. The received SINR for k_{th} LU is calculated as

$$\gamma_{c,k} = \frac{|\mathbf{h}_{c,k}^H \mathbf{w}_{c,k}|^2}{\sum_{i\neq k} |\mathbf{h}_{c,k}^H \mathbf{w}_{c,i}|^2 + \sum_{m=1}^{M} |\mathbf{h}_{c,k}^H \mathbf{w}_{r,m}|^2 + \sigma_{c,k}^2}, \tag{3}$$

where $\mathbf{h}_{c,k}^H = \mathbf{h}_{B,k}^H + \mathbf{h}_{I,k}^H \mathbf{\Theta} \mathbf{h}_{BI}$.

B. Radar Sensing Model

For target l, the transmit array steering vector in the direction of θ_l is

$$\mathbf{a}(\theta_l) = \left[1, e^{-j\frac{2\pi d}{\lambda}\sin\theta_l}, \ldots, e^{-j\frac{2\pi d}{\lambda}(M-1)\sin\theta_l}\right]^T. \tag{4}$$

Denote $\mathbf{g}_{B,l}^H \in \mathbb{C}^{1\times M}$ as the CSI of the line-of-sight (LoS) path between BS and l_{th} target, specified as

$$\mathbf{g}_{B,l}^H = \alpha \left[1, e^{-j\frac{2\pi d}{\lambda}\sin\theta_l}, \ldots, e^{-j\frac{2\pi d}{\lambda}(M-1)\sin\theta_l}\right], \tag{5}$$

where α represents the path loss; λ denotes the wavelength; d denotes the interval separating adjacent elements in the transmit array which generally sets as half-wavelength. Accordingly, denote $\mathbf{g}_{I,l}^H \in \mathbb{C}^{1\times N}$ as the CSI of the non-LoS (NLoS) path from IRS to l_{th} target. Then, for the IRS-target link, the steering vector in the direction (ϕ_l, φ_l) is represented as

$$\mathbf{g}_{I,l}^H = \beta \left[1, e^{-j\frac{2\pi d}{\lambda}\sin\phi_l\cos\varphi_l}, \ldots, e^{-j\frac{2\pi d}{\lambda}(N_x-1)\sin\phi_l\cos\varphi_l}\right] \otimes \left[1, e^{-j\frac{2\pi d}{\lambda}\sin\phi_l\cos\varphi_l}, \ldots, e^{-j\frac{2\pi d}{\lambda}(N_z-1)\sin\phi_l\cos\varphi_l}\right], \tag{6}$$

where β is the channel coefficient; N_x and N_z represents the quantities of IRS elements arranged along the horizontal and

[1] As for the idealized assumption that acquiring perfect CSI is challenging in practical scenarios due to estimation errors and feedback latency. Addressing resource allocation under imperfect CSI scenarios is crucial and involves additional robust optimization methods, which we consider as an important extension for future research.

vertical axes. ϕ_l and φ_l are the azimuth and elevation angle-of-departure (AoD) from the IRS towards the l_{th} target. Thus, the received signal at l_{th} target can be given by

$$y_{r,l} = \left(\mathbf{g}_{B,l}^H + \mathbf{g}_{I,l}^H \mathbf{\Theta} \mathbf{h}_{BI}\right) \mathbf{s} + u_{r,l}, \tag{7}$$

where $u_{r,l}$ denotes the noise that follows the distribution of $\mathcal{CN}(0, \sigma_{r,l}^2)$. In this system, we assume the targets are potential eavesdroppers aiming to intercept communication information. As an eavesdropper, such a target will try to intercept and decode the information sent for communication users. Thus, it is important to minimize the communication signal received by the Eve targets. To quantify the quality of the received signal at an Eve target, we use the SINR defined as follows. The received SINR at l_{th} target for k_{th} LU is

$$\gamma_{r,l,k} = \frac{|\mathbf{G}_l^H \mathbf{w}_{c,k}|^2}{\sum_{i \neq k} |\mathbf{G}_l^H \mathbf{w}_{c,i}|^2 + \sum_{m=1}^{M} |\mathbf{G}_l^H \mathbf{w}_{r,m}|^2 + \sigma_{r,l}^2}, \tag{8}$$

where $\mathbf{G}_l^H = \mathbf{g}_{B,l}^H + \mathbf{g}_{I,l}^H \mathbf{\Theta} \mathbf{h}_{BI}$.

III. Problem Formulation

Beampattern gain is introduced in our proposed scheme to evaluate directional amplification or sensitivity of antenna arrays [31]. It characterizes the directional distribution of transmitted or received signal power. According to (7), for target l, the corresponding beampattern gain is defined as

$$\begin{aligned} P_l &= \mathbb{E}\left\{ \left| \mathbf{G}_l^H \Big(\sum_{k=1}^{K} \mathbf{w}_{c,k} s_{c,k} + \sum_{m=1}^{M} \mathbf{w}_{r,m} s_{r,m} \Big) \right|^2 \right\} \\ &= \mathbf{G}_l^H \Big(\sum_{k=1}^{K} \mathbf{w}_{c,k} \mathbf{w}_{c,k}^H + \sum_{m=1}^{M} \mathbf{w}_{r,m} \mathbf{w}_{r,m}^H \Big) \mathbf{G}_l. \end{aligned} \tag{9}$$

The transmit beamformers and IRS phase shifts are jointly optimized to maximize the minimum beampattern gain of all Eves. Higher beampattern gain indicates the system's ability to more effectively focus energy in the desired direction, thus enhancing signal strength in corresponding direction. This is crucial for both communication and radar systems, as it improves signal detection capability and communication quality. This optimization is carried out subject to user SINR thresholds and information leakage constraints imposed on the Eves. The problem is formulated as problem $(P1)$

$$P1: \max_{\{\mathbf{w}_{c,k}, \mathbf{w}_{r,m}, \mathbf{\Theta}\}} \min_l \mathbf{G}_l^H \Big(\sum_{k=1}^{K} \mathbf{w}_{c,k} \mathbf{w}_{c,k}^H + \sum_{m=1}^{M} \mathbf{w}_{r,m} \mathbf{w}_{r,m}^H \Big) \mathbf{G}_l \tag{10}$$

$$\text{s.t.} \quad \gamma_{c,k} \geq \xi_{c,k}, \quad \forall k \in \mathcal{K}, \tag{11}$$

$$\gamma_{r,l,k} \leq \xi_{r,l}, \quad \forall l \in \mathcal{L}, k \in \mathcal{K}, \tag{12}$$

$$\sum_{k=1}^{K} \|\mathbf{w}_{c,k}\|^2 + \sum_{m=1}^{M} \|\mathbf{w}_{r,m}\|^2 \leq Q, \tag{13}$$

$$|\upsilon_n| = 1, \quad \forall n \in \mathcal{N}, \tag{14}$$

where $\xi_{c,k} > 0$ denotes the SINR requirement of the k_{th} LU and $\xi_{r,l}$ denotes the l_{th} Eve SINR threshold below which the eavesdropper cannot successfully eavesdrop on valid information. Q represents the transmit power budget. The SINR constraints (11) and (12) ensure secure transmission within the proposed IRS-aided ISAC system.

IV. Proposed Solution

The original problem $(P1)$ is inherently non-convex, owing to its non-convex objective and constraints. Specifically, the IRS phase shifts are subject to unit-modulus restrictions, and the quadratic term objective function and constraints, along with coupled variables, makes problem $(P1)$ challenging to solve. To tackle this complex problem, we propose an AO algorithm combined with SDR and Gaussian randomization approach.

First of all, the original max-min optimization problem can be reformulated to be a more favorable form by introducing an auxiliary variable t:

$$P2: \max_{\{\mathbf{w}_{c,k}, \mathbf{w}_{r,m}, \mathbf{\Theta}, t\}} t \tag{15}$$

$$\text{s.t.} \quad \mathbf{G}_l^H \Big(\sum_{k=1}^{K} \mathbf{w}_{c,k} \mathbf{w}_{c,k}^H + \sum_{m=1}^{M} \mathbf{w}_{r,m} \mathbf{w}_{r,m}^H \Big) \mathbf{G}_l \geq t, \forall l \in \mathcal{L}, \tag{16}$$

$$(11) - (14). \tag{17}$$

Then, AO algorithm is performed to decompose it into two sub-problems that can be solved iteratively: 1) transmit beamforming optimization: given IRS phase shifts υ_n, optimize the transmit beamformers; 2) υ_n optimization: with the optimized transmit beamformers, adjust υ_n. We convert each subproblem into a semidefinite programming (SDP) formulation [41]. The Gaussian randomization method is employed to generate a suitable rank-one solution. By iteratively solving these subproblems, the AO algorithm converges to a solution that approximately maximizes the beampattern gain at the targets while satisfying the constraints of the problem.

A. Optimizing $\mathbf{w}_{c,k}$ and $\mathbf{w}_{r,m}$ for given υ_n

With fixed υ_n, the subproblem is expressed as

$$P3: \max_{\{\mathbf{w}_{c,k}, \mathbf{w}_{r,m}, t\}} t \tag{18}$$

$$\text{s.t.} \quad \mathbf{G}_l^H \Big(\sum_{k=1}^{K} \mathbf{w}_{c,k} \mathbf{w}_{c,k}^H + \sum_{m=1}^{M} \mathbf{w}_{r,m} \mathbf{w}_{r,m}^H \Big) \mathbf{G}_l \geq t, \forall l \in \mathcal{L}, \tag{19}$$

$$\frac{|\mathbf{h}_{c,k}^H \mathbf{w}_{c,k}|^2}{\sum_{i \neq k} |\mathbf{h}_{c,k}^H \mathbf{w}_{c,i}|^2 + \sum_{m=1}^{M} |\mathbf{h}_{c,k}^H \mathbf{w}_{r,m}|^2 + \sigma_{c,k}^2} \geq \xi_{c,k}, \forall k \in \mathcal{K}, \tag{20}$$

$$\frac{|\mathbf{G}_l^H \mathbf{w}_{c,k}|^2}{\sum_{i \neq k} |\mathbf{G}_l^H \mathbf{w}_{c,i}|^2 + \sum_{m=1}^{M} |\mathbf{G}_l^H \mathbf{w}_{r,m}|^2 + \sigma_{r,l}^2} \leq \xi_{r,l}, \forall l \in \mathcal{L}, k \in \mathcal{K}, \tag{21}$$

$$\sum_{k=1}^{K} \|\mathbf{w}_{c,k}\|^2 + \sum_{m=1}^{M} \|\mathbf{w}_{r,m}\|^2 \leq Q. \tag{22}$$

The main difficulty to solve $(P3)$ is quadratic terms with respect to optimized variables for all constraints. Furthermore, (20) and (21) are fractional, non-convex constraints. SDR is applied to solve these difficulties [42]. Denote $\mathbf{W}_{c,k} = \mathbf{w}_{c,k}\mathbf{w}_{c,k}^H$ and $\mathbf{W}_{r,m} = \mathbf{w}_{r,m}\mathbf{w}_{r,m}^H$, which are equivalent to $\mathbf{W}_{c,k} \succeq 0$, $\text{rank}(\mathbf{W}_{c,k}) = 1$ and $\mathbf{W}_{r,m} \succeq 0$, $\text{rank}(\mathbf{W}_{r,m}) = 1$. Moreover,

$$\mathbf{G}_l^H \mathbf{w}_{c,k}\mathbf{w}_{c,k}^H \mathbf{G}_l = \text{Tr}(\mathbf{G}_l^H \mathbf{W}_{c,k}\mathbf{G}_l), \tag{23}$$

$$|\mathbf{h}_{c,k}^H \mathbf{w}_{c,k}|^2 = \text{Tr}(\mathbf{h}_{c,k}^H \mathbf{W}_{c,k}\mathbf{h}_{c,k}). \tag{24}$$

Then, the subproblem can be rewritten as

$$P4: \max_{\{\mathbf{W}_{c,k}, \mathbf{W}_{r,m}, t\}} t \tag{25}$$

$$\text{s.t.} \quad \text{Tr}\Big(\mathbf{G}_l^H \Big(\sum_{k=1}^{K} \mathbf{W}_{c,k} + \sum_{m=1}^{M} \mathbf{W}_{r,m}\Big)\mathbf{G}_l\Big) \geq t, \forall l \in \mathcal{L}, \tag{26}$$

$$\text{Tr}(\mathbf{h}_{c,k}^H \mathbf{W}_{c,k}\mathbf{h}_{c,k}) \geq \xi_{c,k}\Big(\sum_{i\neq k} \text{Tr}(\mathbf{h}_{c,k}^H \mathbf{W}_{c,i}\mathbf{h}_{c,k}) \tag{27}$$

$$+ \sum_{m=1}^{M} \text{Tr}(\mathbf{h}_{c,k}^H \mathbf{W}_{r,m}\mathbf{h}_{c,k}) + \sigma_{c,k}^2\Big), \forall k \in \mathcal{K},$$

$$\text{Tr}(\mathbf{G}_l^H \mathbf{W}_{c,k}\mathbf{G}_l) \leq \xi_{r,l}\Big(\sum_{i\neq k} \text{Tr}(\mathbf{G}_l^H \mathbf{W}_{c,i}\mathbf{G}_l) \tag{28}$$

$$+ \sum_{m=1}^{M} \text{Tr}(\mathbf{G}_l^H \mathbf{W}_{r,m}\mathbf{G}_l) + \sigma_{r,l}^2\Big), \forall l \in \mathcal{L}, k \in \mathcal{K},$$

$$\sum_{k=1}^{K} \text{Tr}(\mathbf{W}_{c,k}) + \sum_{m=1}^{M} \text{Tr}(\mathbf{W}_{r,m}) \leq Q, \tag{29}$$

$$\text{rank}(\mathbf{W}_{c,k}) = 1, \quad \mathbf{W}_{c,k} \succeq 0, \quad \forall k \in \mathcal{K}, \tag{30}$$

$$\text{rank}(\mathbf{W}_{r,m}) = 1, \quad \mathbf{W}_{r,m} \succeq 0, \quad \forall m \in \mathcal{M}. \tag{31}$$

The semi-definite constraint can be straightforwardly tackled, but the rank-one condition introduces non-convexity. To address this, we remove the rank-one requirement and reformed the subproblem to maximize a linear objective under linear matrix inequality constraints, thus resulting in a convex SDP problem. Standard convex optimization tools employing interior-point methods can efficiently obtain the optimal solution [43], [44]. However, the relaxed solution generally does not guarantee a rank-one solution, so the optimal value derived from this relaxation only provides an upper bound for the original problem. Therefore, if the optimal results fails to meet the rank-one condition, Gaussian randomization is then employed to generate rank-one solution.

B. Optimizing υ_n for given $\mathbf{w}_{c,k}$ and $\mathbf{w}_{r,m}$

In this subsection, with given optimal $\mathbf{w}_{c,k}$ and $\mathbf{w}_{r,m}$, the IRS phase shift υ_n is optimized. We rewrite the formulation $(P2)$ in the form of following subproblem

$$P5: \max_{\{\boldsymbol{\Theta}, t\}} t \tag{32}$$

$$\text{s.t.} \quad \mathbf{G}_l^H \Big(\sum_{k=1}^{K} \mathbf{w}_{c,k}\mathbf{w}_{c,k}^H + \sum_{m=1}^{M} \mathbf{w}_{r,m}\mathbf{w}_{r,m}^H\Big)\mathbf{G}_l \geq t, \forall l \in \mathcal{L}, \tag{33}$$

$$\frac{|\mathbf{h}_{c,k}^H \mathbf{w}_{c,k}|^2}{\sum_{i\neq k} |\mathbf{h}_{c,k}^H \mathbf{w}_{c,i}|^2 + \sum_{m=1}^{M} |\mathbf{h}_{c,k}^H \mathbf{w}_{r,m}|^2 + \sigma_{c,k}^2} \geq \xi_{c,k}, \forall k \in \mathcal{K}, \tag{34}$$

$$\frac{|\mathbf{G}_l^H \mathbf{w}_{c,k}|^2}{\sum_{i\neq k} |\mathbf{G}_l^H \mathbf{w}_{c,i}|^2 + \sum_{m=1}^{M} |\mathbf{G}_l^H \mathbf{w}_{r,m}|^2 + \sigma_{r,l}^2} \leq \xi_{r,l}, \forall l \in \mathcal{L}, k \in \mathcal{K}, \tag{35}$$

$$|\upsilon_n| = 1, \quad \forall n \in \mathcal{N}. \tag{36}$$

It can be seen that, the non-convex constraints (34) and (35) along with unit modulus IRS phase shifts constraint, make the problem difficult to solve. Let $\boldsymbol{\nu}^H = [\upsilon_1, \upsilon_2, \ldots, \upsilon_N]$. Then, define $\boldsymbol{\Phi}_k = \text{diag}(\mathbf{h}_{I,k}^H)\mathbf{h}_{BI} \in \mathbb{C}^{N\times M}$ and $\boldsymbol{\Psi}_l = \text{diag}(\mathbf{g}_{I,l}^H)\mathbf{h}_{BI} \in \mathbb{C}^{N\times M}$. The reflective channel matrix can be rewritten as

$$\mathbf{h}_{I,k}^H \boldsymbol{\Theta} \mathbf{h}_{BI} = \boldsymbol{\nu}^H \boldsymbol{\Phi}_k, \tag{37}$$

$$\mathbf{g}_{I,l}^H \boldsymbol{\Theta} \mathbf{h}_{BI} = \boldsymbol{\nu}^H \boldsymbol{\Psi}_l. \tag{38}$$

Furthermore, denote

$$\bar{\boldsymbol{\nu}} = \begin{bmatrix} \boldsymbol{\nu} \\ 1 \end{bmatrix}, \qquad \bar{\boldsymbol{\Phi}}_k = \begin{bmatrix} \boldsymbol{\Phi}_k \\ \mathbf{h}_{B,k}^H \end{bmatrix}, \qquad \bar{\boldsymbol{\Psi}}_l = \begin{bmatrix} \boldsymbol{\Psi}_l \\ \mathbf{g}_{B,l}^H \end{bmatrix}. \tag{39}$$

As a result, this subproblem is equivalent to

$$P6: \max_{\{\bar{\boldsymbol{\nu}}, t\}} \quad t \tag{40}$$

$$\text{s.t.} \quad \bar{\boldsymbol{\nu}}^H \bar{\boldsymbol{\Psi}}_l \Big(\sum_{k=1}^{K} \mathbf{W}_{c,k} + \sum_{m=1}^{M} \mathbf{W}_{r,m}\Big)\bar{\boldsymbol{\Psi}}_l^H \bar{\boldsymbol{\nu}} \geq t, \forall l \in \mathcal{L}, \tag{41}$$

$$\bar{\boldsymbol{\nu}}^H \bar{\boldsymbol{\Phi}}_k \mathbf{W}_{c,k} \bar{\boldsymbol{\Phi}}_k^H \bar{\boldsymbol{\nu}} \geq \xi_{c,k}\Big(\sum_{i\neq k} \bar{\boldsymbol{\nu}}^H \bar{\boldsymbol{\Phi}}_k \mathbf{W}_{c,i} \bar{\boldsymbol{\Phi}}_k^H \bar{\boldsymbol{\nu}} \tag{42}$$

$$+ \sum_{m=1}^{M} \bar{\boldsymbol{\nu}}^H \bar{\boldsymbol{\Phi}}_k \mathbf{W}_{r,m} \bar{\boldsymbol{\Phi}}_k^H \bar{\boldsymbol{\nu}} + \sigma_{c,k}^2\Big), \forall k \in \mathcal{K},$$

$$\bar{\boldsymbol{\nu}}^H \bar{\boldsymbol{\Psi}}_l \mathbf{W}_{c,k} \bar{\boldsymbol{\Psi}}_l^H \bar{\boldsymbol{\nu}} \leq \xi_{r,l}\Big(\sum_{i\neq k} \bar{\boldsymbol{\nu}}^H \bar{\boldsymbol{\Psi}}_l \mathbf{W}_{c,i} \bar{\boldsymbol{\Psi}}_l^H \bar{\boldsymbol{\nu}} \tag{43}$$

$$+ \sum_{m=1}^{M} \bar{\boldsymbol{\nu}}^H \bar{\boldsymbol{\Psi}}_l \mathbf{W}_{r,m} \bar{\boldsymbol{\Psi}}_l^H \bar{\boldsymbol{\nu}} + \sigma_{r,l}^2\Big), \forall l \in \mathcal{L}, k \in \mathcal{K},$$

$$|\bar{\nu}_i| = 1, \quad i = 1, \ldots, N+1. \tag{44}$$

However, this subproblem $(P6)$ is still non-convex. Denote $\mathbf{V} = \bar{\boldsymbol{\nu}}\bar{\boldsymbol{\nu}}^H$ that satisfying $\mathbf{V} \succeq 0$ and $\text{rank}(\mathbf{V}) = 1$. After relaxing this rank constraint according to SDR, the subproblem is reduced to

$$P7: \max_{\{\mathbf{V}, t\}} \quad t \tag{45}$$

$$\text{s.t.} \quad \text{Tr}(\mathbf{V}\mathbf{R}_{1,l}) \geq t, \forall l \in \mathcal{L}, \tag{46}$$

$$\text{Tr}(\mathbf{V}\mathbf{T}_{1,k,k}) \geq \xi_{c,k}\Big(\sum_{i\neq k} \text{Tr}(\mathbf{V}\mathbf{T}_{2,k,i}) \tag{47}$$

$$+ \sum_{m=1}^{M} \text{Tr}(\mathbf{V}\mathbf{T}_{3,k,m}) + \sigma_{c,k}^2\Big), \forall k \in \mathcal{K},$$

$$\mathrm{Tr}(\mathbf{V}\mathbf{R}_{2,l,k}) \le \xi_{r,l}\Big(\sum_{i\neq k}\mathrm{Tr}(\mathbf{V}\mathbf{R}_{3,l,i}) + \sum_{m=1}^{M}\mathrm{Tr}(\mathbf{V}\mathbf{R}_{4,l,m}) + \sigma_{r,l}^2\Big), \forall l \in \mathcal{L}, k \in \mathcal{K}, \tag{48}$$

$$\mathbf{V}_{i,i} = 1, \quad i = 1, \ldots, N+1, \tag{49}$$

$$\mathbf{V} \succeq 0. \tag{50}$$

where

$$\mathbf{R}_{1,l} = \bar{\mathbf{\Psi}}_l\Big(\sum_{k=1}^{K}\mathbf{W}_{c,k} + \sum_{m=1}^{M}\mathbf{W}_{r,m}\Big)\bar{\mathbf{\Psi}}_l^H, \tag{51}$$

$$\mathbf{R}_{2,l,k} = \bar{\mathbf{\Psi}}_l\mathbf{W}_{c,k}\bar{\mathbf{\Psi}}_l^H, \tag{52}$$

$$\mathbf{R}_{3,l,i} = \bar{\mathbf{\Psi}}_l\mathbf{W}_{c,i}\bar{\mathbf{\Psi}}_l^H, \tag{53}$$

$$\mathbf{R}_{4,l,m} = \bar{\mathbf{\Psi}}_l\mathbf{W}_{r,m}\bar{\mathbf{\Psi}}_l^H, \tag{54}$$

$$\mathbf{T}_{1,k,k} = \bar{\mathbf{\Phi}}_k\mathbf{W}_{c,k}\bar{\mathbf{\Phi}}_k^H, \tag{55}$$

$$\mathbf{T}_{2,k,i} = \bar{\mathbf{\Phi}}_k\mathbf{W}_{c,i}\bar{\mathbf{\Phi}}_k^H, \tag{56}$$

$$\mathbf{T}_{3,k,m} = \bar{\mathbf{\Phi}}_k\mathbf{W}_{r,m}\bar{\mathbf{\Phi}}_k^H. \tag{57}$$

In this step, problem $(P7)$ has been converted into a convex SDP, which is solvable using the interior point algorithms by convex optimization tools. Similarly, if the optimal results do not satisfy rank-one constraint, additional Gaussian randomization step are needed according to the higher rank solution.

C. Gaussian randomization procedure

Since the rank constraints make the problem non-convex and are typically handled by SDR, we employ Gaussian randomization to retrieve a feasible rank-one candidate [42].

During the t_{th} AO iteration, the optimal solution $\mathbf{W}_{c,k}^* = \mathbf{W}_{c,k}^{(t)}$, $\mathbf{W}_{r,m}^* = \mathbf{W}_{r,m}^{(t)}$, $\mathbf{V}^* = \mathbf{V}^{(t)}$ can be obtained. First of all, according to eigenvalue decomposition, for beamformers matrices, decompose $\mathbf{W}_{c,k}^*$ and $\mathbf{W}_{r,m}^*$ as

$$\mathbf{W}_{c,k}^* = \mathbf{U}_{c,k}\mathbf{\Sigma}_{c,k}\mathbf{U}_{c,k}^H, \tag{58}$$

$$\mathbf{W}_{r,m}^* = \mathbf{U}_{r,m}\mathbf{\Sigma}_{r,m}\mathbf{U}_{r,m}^H, \tag{59}$$

where $\mathbf{U}$ and $\mathbf{\Sigma}$ refer to unitary and diagonal matrices, respectively. Then, extract the square root matrix and generate a random vector satisfying

$$\boldsymbol{\omega}_{c,k} = \mathbf{U}_{c,k}\mathbf{\Sigma}_{c,k}^{1/2}\boldsymbol{\zeta}_{c,\ell}, \tag{60}$$

$$\boldsymbol{\omega}_{r,m} = \mathbf{U}_{r,m}\mathbf{\Sigma}_{r,m}^{1/2}\boldsymbol{\zeta}_{r,\ell}, \tag{61}$$

where $\boldsymbol{\zeta}_{c,\ell}, \boldsymbol{\zeta}_{r,\ell} \sim \mathcal{CN}(0, \mathbf{I}_N)$. Next, randomly generate vectors $\boldsymbol{\zeta}_{c,\ell}, \boldsymbol{\zeta}_{r,\ell}$, and then evaluate them based on the objective and constraints. The process concludes by selecting the optimal approximate solutions $\boldsymbol{\omega}_{c,k}^*$ and $\boldsymbol{\omega}_{r,m}^*$. Similarly, for IRS phase shifts, decompose $\mathbf{V}^*$ as $\mathbf{V}^* = \mathbf{U}_\nu\mathbf{\Sigma}_\nu\mathbf{U}_\nu^H$ and generate a vector satisfying $\mathbf{v}_r = \mathbf{U}_\nu\mathbf{\Sigma}_\nu^{1/2}\boldsymbol{\zeta}_{\nu,\ell}$, where $\boldsymbol{\zeta}_{\nu,\ell} \sim \mathcal{CN}(0, \mathbf{I}_N)$. Then normalize each element of $\mathbf{v}_r$ to recover the original phase vector and eventually obtain $\mathbf{v}^*$.

Therefore, the overall algorithm details are presented in **Algorithm 1**. The computational complexity arises from solving SDP subproblems in the proposed algorithm. The complexity is estimated based on the number of arithmetic operations required by interior-point method [45]. For problem $(P3)$, the complexity is $\mathcal{O}\left(\max\{M, LK+K+L\}^4 M^{1/2}\log\left(\frac{1}{\varepsilon}\right)\right)$, where $\varepsilon > 0$ is convergence threshold. The computational complexity for problem $(P5)$ is $\mathcal{O}\left(\max\{N, LK+K+L\}^4 N^{1/2}\log\left(\frac{1}{\varepsilon}\right)\right)$. The complexity for the Gaussian randomization step at each AO iteration is $\mathcal{O}\left(T_{rand}(M^2+N^2)\right)$, where T_{rand} represents the number of Gaussian random samples. Thus, when M and N are large, the total complexity of Algorithm 1 is given by

$$\mathcal{O}(I_{iter}(\max\{M, LK+K+L\}^4 M^{1/2}\log(\frac{1}{\varepsilon}) + \max\{N, LK+K+L\}^4 N^{1/2}\log(\frac{1}{\varepsilon}))), \tag{62}$$

where I_{iter} denotes the the iteration count for achieving AO convergence.

Algorithm 1 Joint beamforming and IRS phase shifts design for problem $(P1)$

1: Initialize $\{\mathbf{w}_{c,k}, \mathbf{w}_{r,m}, \forall k, m\}$, $\boldsymbol{\nu}$. Compute $\mathbf{W}_{c,k}^{(0)} = \mathbf{w}_{c,k}\mathbf{w}_{c,k}^H$, $\mathbf{W}_{r,m}^{(0)} = \mathbf{w}_{r,m}\mathbf{w}_{r,m}^H$ and $\mathbf{V}^{(0)} = \bar{\boldsymbol{\nu}}\bar{\boldsymbol{\nu}}^H$.
2: Set convergence threshold ε and iteration $\rho = 0$.
3: **repeat**
4: Obtain the transmit beamformers $\mathbf{W}_{c,k}^{(\rho+1)}$ and $\mathbf{W}_{r,m}^{(\rho+1)}$ for given $\mathbf{V}^{(\rho)}$ by solving problem $(P4)$.
5: Obtain $\{\boldsymbol{\omega}_{c,k}^{*(\rho+1)}, \boldsymbol{\omega}_{r,m}^{*(\rho+1)}\}$ based on $\mathbf{W}_{c,k}^{(\rho+1)}$, $\mathbf{W}_{r,m}^{(\rho+1)}$ via Gaussian randomization.
6: Obtain the IRS phase shifts $\mathbf{V}^{(\rho+1)}$ based on $\mathbf{W}_{c,k}^{(\rho+1)}$ and $\mathbf{W}_{r,m}^{(\rho+1)}$ by solving problem $(P7)$.
7: Obtain $\mathbf{v}^{*(\rho+1)}$ based on $\mathbf{V}^{(\rho+1)}$ via Gaussian randomization.
8: Update iteration index $\rho = \rho + 1$.
9: **until** convergence.
10: Return the optimal solution $\{\boldsymbol{\omega}_{c,k}^{*(\rho)}, \boldsymbol{\omega}_{r,m}^{*(\rho)}\}$ and $\mathbf{v}^{*(\rho)}$.

D. Convergence and optimality analysis

Convergence and algorithmic optimality are analyzed in the following subsection.

Theorem 1. *The proposed AO algorithm monotonically increases the objective value across iterations, and the solution converges to a Karush–Kuhn–Tucker (KKT) point of the non-convex optimization problem (P1).*

Proof. First, the monotonicity of the AO algorithm is verified. Define the objective function of (P1) as $P(\mathbf{W}, \mathbf{v})$. In the AO iteration $\rho+1$, solving problem $(P4)$ for given $\mathbf{v}^{(\rho)}$, we obtain:

$$P(\mathbf{W}^{(\rho)}, \mathbf{v}^{(\rho)}) \le P(\mathbf{W}^{(\rho+1)}, \mathbf{v}^{(\rho)}), \tag{63}$$

since $\mathbf{W}^{(\rho+1)}$ is the optimal solution of subproblem $(P4)$ with fixed $\mathbf{v}^{(\rho)}$. Similarly, solving $(P7)$ for given $\mathbf{W}^{(\rho+1)}$, we have:

$$P(\mathbf{W}^{(\rho+1)}, \mathbf{v}^{(\rho)}) \le P(\mathbf{W}^{(\rho+1)}, \mathbf{v}^{(\rho+1)}). \tag{64}$$

Therefore, the objective function satisfies:

$$P(\mathbf{W}^{(\rho)}, \mathbf{v}^{(\rho)}) \le P(\mathbf{W}^{(\rho+1)}, \mathbf{v}^{(\rho+1)}), \tag{65}$$

indicating the monotonic improvement at each AO iteration. Then, as for algorithm convergence, due to the finite power constraint (13), the objective function is upper bounded. Given the monotonic improvement established, the solution $\{P(\mathbf{W}^{(\rho)}, \mathbf{v}^{(\rho)})\}$ generated by AO is monotonically non-decreasing and bounded above. Thus, according to standard convergence theory [46], there exists a convergent solution $\{(\mathbf{W}^{(\rho_\nu)}, \mathbf{v}^{(\rho_\nu)})\}$ converging to some point $(\mathbf{W}^*, \mathbf{v}^*)$. The limit of the entire sequence of objective values therefore converges:

$$\lim_{t\to\infty} P(\mathbf{W}^{(\rho)}, \mathbf{v}^{(\rho)}) = P(\mathbf{W}^*, \mathbf{v}^*). \tag{66}$$

Finally, since the subproblems $(P4)$ and $(P7)$ solved at each iteration are convex (after SDR relaxation), their optimal solutions necessarily satisfy the corresponding convex KKT conditions [47]. At the limit point $(\mathbf{W}^*, \mathbf{v}^*)$, both sets of KKT conditions (for beamforming subproblem and IRS phase shift subproblem) simultaneously hold due to convergence. Thus, the limit point $(\mathbf{W}^*, \mathbf{v}^*)$ satisfies the KKT point of the non-convex problem (P1). □

V. Numerical Results

Performance analysis of the proposed secure system is carried out via numerical simulations. A 3-D coordinate system in meters (m) is adopted [22], [31]: the BS is positioned at $(0, 0, 5)$ m and the IRS is deployed at $(30, 0, 5)$ m. The LUs are uniformly arranged on a circle of radius 2.5 m, centered at $(30, 10, 0)$ m in the $x-y$ axis. Three Eves are placed at fixed distances from the BS and IRS (specifically 30m, 35m and 30m from the BS; 10m, 15m and 15m from the IRS). They are located at the azimuth angle and elevation angle of $\phi_1 = -30°$, $\varphi_1 = 40°$, $\phi_2 = -30°$, $\varphi_2 = 45°$ and $\phi_3 = -30°$, $\varphi_3 = 35°$, respectively. This arrangement reflects realistic adversarial scenarios in which malicious devices, such as unauthorized drones or surveillance equipment, are positioned strategically near critical communication infrastructure, increasing their capability of intercepting sensitive signals. The distance-dependent path loss function can be defined by $c_0 \left(d/d_0\right)^{-\mu}$, where $c_0 = -30$ dB as the reference loss at $d_0 = 1$ m. Here, d indicates the transmission distance, and the path loss exponents μ are set as 2.2, 2.2, 3.6, 3, 2 for the links between BS-IRS, IRS-LUs, BS-LUs, BS-Eves, IRS-Eves, respectively. Thus, the distance-dependent Rician fading channel can be given by

$$\boldsymbol{h}_i = \sqrt{\frac{c_0}{(d_i/d_0)^{\mu}}}\left(\sqrt{\frac{\kappa_i}{\kappa_i+1}}\boldsymbol{h}_i^{LoS} + \sqrt{\frac{1}{\kappa_i+1}}\boldsymbol{h}_i^{NLoS}\right). \tag{67}$$

The BS-IRS and IRS-LUs links are modeled as Rician fading channels with a Rician factor $\kappa = 3$ dB, while the BS-LUs links are assumed to experience Rayleigh fading. Unless otherwise stated, we set $K = 2$, $L = 2$, $M = 8$, $N = 60$, $\sigma_{c,k}^2 = -80$ dBm, $\sigma_{r,l}^2 = -80$ dBm, $\forall k, l$, $\varepsilon = 10^{-3}$.

The simulation parameters are based on typical configurations reported in recent IRS-aided ISAC literature. The coordinates of the BS, IRS, and LU deployment area represent realistic indoor-outdoor hybrid or small-cell environments, ensuring clear LoS propagation. Path-loss exponents adopt lower values for LoS-dominant links and higher values typical of NLoS urban microcell scenarios. Rician factors ($\kappa = 3$ dB for BS-IRS and IRS-LU) reflect strong LoS components, whereas the Rayleigh fading model ($\kappa = 0$) captures multipath-dominated BS-LU links. Additionally, selected antenna counts, IRS elements, noise variances, and convergence tolerance balance realism with computational feasibility, ensuring credible and reproducible simulation results.

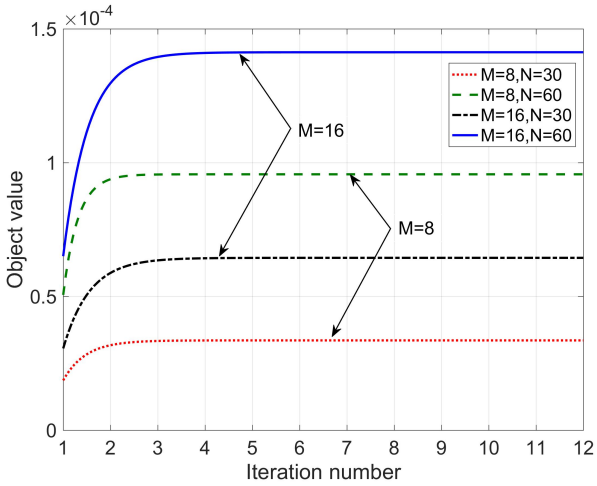


Fig. 2: Convergence behaviour with varying transmit antennas and IRS reflecting elements, $K = 2$, $L = 2$, $P = 25$ dBm.

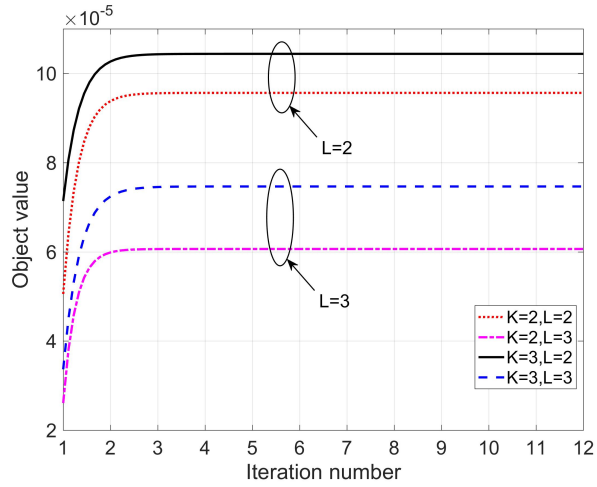


Fig. 3: Convergence behaviour with varying number of LUs and targets, $M = 8$, $N = 60$, $P = 25$ dBm.

First of all, we analyze the convergence of the proposed algorithm. The convergence behavior for different transmit antennas and IRS elements are compared in Fig. 2. The results show that the objective function rapidly stabilizes across different values of M and N, confirming the effectiveness of the proposed method. Configurations with higher values of M and N achieve higher object values. This is because more antennas and IRS elements provides additional degrees of freedom (DoFs) for resource allocation, thereby enabling higher beamforming gains. In addition, the convergence behavior for

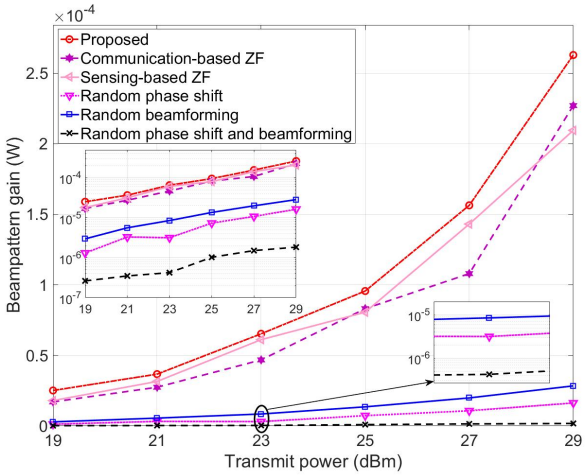


Fig. 4: Beampattern gain vs transmit power, $M = 8$, $N = 60$, $K = 2$, $L = 2$.

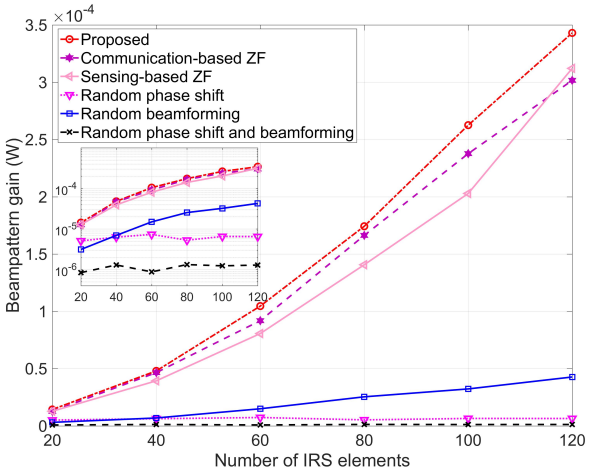


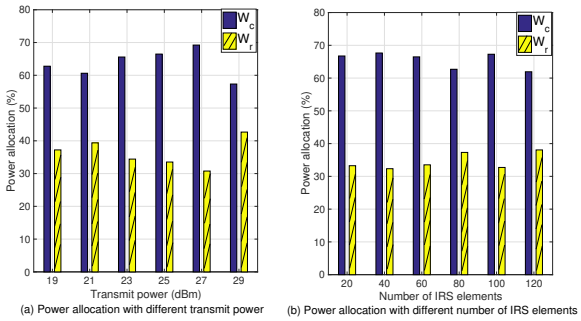
Fig. 5: Beampattern gain vs IRS elements, $M = 8$, $K = 2$, $L = 2$, $P = 25$ dBm.

different number of LUs and targets are analyzed in Fig. 3. For fixed transmit power, adding more targets results in a lower beampattern gains, since system must handle more complex resource allocation and interference management, resulting in lower beampattern gains. However, the optimization process shows rapid improvement in the initial iterations before stabilizing, demonstrating effective convergence of the algorithm across different scenarios.

Next, Fig. 4 presents the beampattern gain for different schemes versus transmit power. "Proposed" means the proposed scheme in Algorithm 1; "Random phase shifts" means that only beamformers are optimized while IRS phase shifts are randomly generated; "Random beamforming" means that only IRS phase shifts are optimized while beamforming vectors are randomly generated; "Random phase shifts and beamforming" means that both beamforming vectors and IRS phase shifts are randomly generated. "Communication-based zero-forcing (ZF)" means that communication beamforming vectors are designed to be orthogonal to target channel to eliminate information leakage. "Sensing-based ZF" means that radar beamforming vectors are lie in the null space of user channels, minimizing interference to communication users [31]. As transmit power rises, all schemes exhibit an increase in beampattern gains. Furthermore, the proposed scheme achieves the highest beampattern gain across all levels of transmit power, which indicates jointly optimizing transmit beamformers and IRS phase can most effectively utilize the transmit power to focus more energy in the target direction, achieving optimal performance. The random beamforming scheme achieves higher beampattern gain than random phase shift but lower than the proposed. This emphasizes the importance of precise IRS phase adjustment. "Random phase shifts and beamforming" exhibits lowest beampattern gain among all considered methods, showing that without proper optimization, the beamforming strategy is less effective. The inset provides a detailed view of the beampattern gains at different power levels, which indicates the random schemes fail to make efficient use of the available power, resulting in significantly lower beampattern gains. The "Communication-based ZF" and "Sensing-based ZF" schemes perform closely to the proposed scheme indicating that, within the considered system model, even if the communication or radar beamformers are constrained to the null space, the optimization of transmit beamformming and IRS phase still effectively leverages available DoFs. In general, for a given transmit power, the proposed scheme provides higher beampattern gain, indicating greater power efficiency. In practical applications, this can contribute to longer detection ranges, higher communication quality, or lower required transmit power, thereby enhancing overall system performance and energy efficiency.

Then, Fig. 5 illustrates the beampattern gain of various schemes versus the number of IRS element. As expected, the proposed scheme consistently delivers superior performance compared to all benchmarks, including the "Communication-based ZF" and "Sensing-based ZF" schemes, highlighting the advantage of jointly optimizing IRS phase and transmit beamforming. Notably, the proposed scheme achieves significantly higher beampattern gains than the random approaches. With more IRS elements, the system can more effectively focus the transmitted energy towards the target, resulting in higher signal strength and better detection capabilities. In addition, it is worth to note that "Random Phase Shift" scheme shows a constant beampattern gain that does not improve with an increasing number of IRS elements, demonstrating that without optimization, increasing IRS elements does not enhance performance. While the random beamforming scheme performs better than the random phase shift scheme with a upward trend, indicating some improvement with the optimization of IRS phase shift when IRS elements become larger. The both random scheme still shows the lowest beamforming gains, regardless of how many IRS elements are deployed.

The allocation of power between W_c (communication) and W_r (radar) is shown in Fig. 6. With the IRS reflecting elements fixed at 60, increasing the total transmit power results in a stable power allocation between communication and radar functions. The proportion of power allocation to radar remains



(a) Power allocation with different transmit power (b) Power allocation with different number of IRS elements

Fig. 6: Impact of transmit power and IRS elements on power allocation, $M = 8$, $K = 2$, $L = 2$.

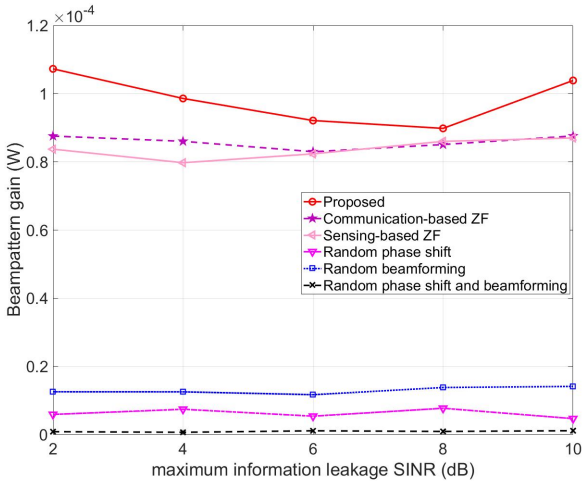


Fig. 7: Beampattern gain vs maximum information leakage SINR, $M = 8$, $N = 60$, $K = 2$, $L = 2$, $P = 25$ dBm.

nearly unchanged as the power budget grows, indicating that the optimization consistently balances the requirements of both communication and radar, regardless of higher power budgets. With a constant transmit power of 25 dBm, increasing the IRS configuration from 20 to 120 leads to only minor changes in the power allocation between W_c and W_r. This behavior is mainly due to the fixed constraints and objectives of the optimization problem and the symmetric gain improvement provided by the IRS for both communication and radar channels.

Finally, the beampattern gain for different schemes versus the maximum information leakage SINR tolerance is analyzed in Fig. 7, where the proposed scheme consistently outperforms others across different maximum information leakage SINR. This indicates that simultaneously optimizing IRS phase shifts and BS beamforming is highly effective in enhancing the beampattern gain while managing information leakage. The close performance observed between the proposed method and both ZF schemes in this scenario is primarily because the presence of direct BS-Eves link and tight SINR requirements for information leakage inherently restricts feasible solutions, thus limiting the potential advantage of additional DoFs in the proposed joint optimization. It is worth to note that all simulation results obtained through the proposed algorithm meet the constraints of the original problem. Thus, according to these constraints, the minimum SINR requirements guarantee the communication quality for LUs, while the maximum allowable information leakage constraints effectively prevent unauthorized targets from accessing valuable information, thereby ensuring the security of the system. Furthermore, the proposed scheme maintains high and relatively stable beampattern gains as the maximum information leakage SINR increases. By optimizing the beamformers and IRS phase shifts, the proposed scheme not only increases the signal strength in the target direction but also better suppresses interference and leakage signals in non-target directions, which is crucial for enhancing physical layer security, preventing information leakage, and improving system reliability in interference-prone environments. The proposed scheme effectively leverages the available degrees of freedom provided by the IRS and the BS beamformers to maintain high beampattern gains across varying SINR levels. This demonstrates its robustness and adaptability in different scenarios, particularly when balancing system performance with security considerations.

VI. Conclusions

In conclusion, we have proposed a secure IRS-aided scheme for ISAC systems. By leveraging the capabilities of an IRS, we jointly optimized the IRS phase configuration along with the BS beamforming vectors, aiming to maximize the sensing beampattern gains across Eves while maintaining secure communication by preventing information leakage to them. To solve this challenging non-convex problem, AO algorithm is applied leveraging SDR and Gaussian randomization techniques. Numerical simulations are carried out to verify the theoretical analysis and compare the performance of the proposed scheme. The performance gap shows the effectiveness of coordinated beamforming and IRS phase design. Overall, our study highlights that incorporating IRS technology can significantly strengthen both physical layer security and sensing capabilities in ISAC systems.

References

[1] X. You, C. 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," *Sci. China Inf. Sci.*, vol. 64, 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 Commun.*, vol. 17, no. 1, pp. 1–27, 2020.

[3] C. Wang, J. Huang, H. Wang, X. Gao, X. You, and Y. Hao, "6G wireless channel measurements and models: Trends and challenges," *IEEE Veh. Technol. Mag.*, vol. 15, no. 4, pp. 22–32, 2020.

[4] J. Yu, Y. Wang, J. Ding, J. Zhang, W. Li, F. Wang, C. Wang, K. Wang, Y. Tan, M. Zhu *et al.*, "Broadband photon-assisted terahertz communication and sensing," *J. Lightw. Technol.*, vol. 41, no. 11, pp. 3332–3349, 2023.

[5] A. Li, S. Wu, S. Meng, R. Lu, S. Sun, and Q. Zhang, "Toward goal-oriented semantic communications: New metrics, framework, and open challenges," *IEEE Wireless Commun.*, pp. 1–8, 2024.

[6] A. Hassanien, M. G. Amin, E. Aboutanios, and B. Himed, "Dual-function radar communication systems: A solution to the spectrum congestion problem," *IEEE Signal Process. Mag.*, vol. 36, no. 5, pp. 115–126, 2019.

[7] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: Vision and potential techniques," *IEEE Netw.*, vol. 33, no. 4, pp. 70–75, 2019.

[8] Y. Zeng, Y. Ma, and S. Sun, "Joint radar-communication with cyclic prefixed single carrier waveforms," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4069–4079, 2020.

[9] Y. Long, S. Zhao, S. Gong, B. Gu, D. Niyato, and X. Shen, "Aoi-aware sensing scheduling and trajectory optimization for multi-uav-assisted wireless backscatter networks," *IEEE Trans. Veh. Technol.*, pp. 1–16, 2024.

[10] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," *Proc. IEEE*, vol. 108, no. 2, pp. 292–307, 2019.

[11] F. Liu, C. Masouros, A. Li, H. Sun, and L. Hanzo, "MU-MIMO communications with MIMO radar: From co-existence to joint transmission," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2755–2770, 2018.

[12] 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)*, 2019, pp. 7790–7794.

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

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

[15] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, 2016.

[16] D. Hu, W. Zhang, L. He, and J. Wu, "Secure transmission in multi-cell multi-user massive MIMO systems with an active eavesdropper," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 85–88, 2018.

[17] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci.*, vol. 114, no. 1, pp. 19–26, 2017.

[18] 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 Trans. Wireless Commun.*, vol. 21, no. 9, pp. 7238–7252, 2022.

[19] N. Su, F. Liu, and C. Masouros, "Sensing-assisted eavesdropper estimation: An ISAC breakthrough in physical layer security," *IEEE Trans. Wireless Commun.*, vol. 23, no. 4, pp. 3162–3174, 2024.

[20] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, 2019.

[21] J. Wang, Y. Liang, Y. Pei, and X. Shen, "Reconfigurable intelligent surface as a micro base station: A novel paradigm for small cell networks," *IEEE Trans. Wireless Commun.*, vol. 22, no. 4, pp. 2338–2351, 2022.

[22] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, 2019.

[23] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, M. Di Renzo, and N. Al-Dhahir, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Commun. Surv. Tut.*, vol. 23, no. 3, pp. 1546–1577, 2021.

[24] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, 2019.

[25] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, 2020.

[26] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[27] X. Chen, T. Zheng, X. Wang, U. Zeb, X. Hu, C. Liu, and Y. He, "Intelligent reflecting surface aided robust secure integrated sensing and communication systems," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*. IEEE, 2023, pp. 1–6.

[28] S. Fang, G. Chen, P. Xu, J. Tang, and J. A. Chambers, "Sinr maximization for RIS-assisted secure dual-function radar communication systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*. IEEE, 2021, pp. 01–06.

[29] C. Jiang, C. Zhang, C. Huang, J. Ge, J. He, and C. Yuen, "Secure beamforming design for RIS-assisted integrated sensing and communication systems," *IEEE Wireless Commun. Lett.*, vol. 13, no. 2, pp. 520–524, 2024.

[30] H. Zhao, F. Wu, W. Xia, Y. Zhang, Y. Ni, and H. Zhu, "Joint beamforming design for RIS-aided secure integrated sensing and communication systems," *IEEE Commun. Lett.*, vol. 27, no. 11, pp. 2943–2947, 2023.

[31] M. Hua, Q. Wu, W. Chen, O. A. Dobre, and A. L. Swindlehurst, "Secure intelligent reflecting surface aided integrated sensing and communication," *IEEE Trans. Wireless Commun.*, 2023.

[32] X. Liu, H. Zhang, K. Long, M. Zhou, Y. Li, and H. V. Poor, "Proximal policy optimization-based transmit beamforming and phase-shift design in an irs-aided isac system for the thz band," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 7, pp. 2056–2069, 2022.

[33] C. Huang, R. Mo, and C. Yuen, "Reconfigurable intelligent surface assisted multiuser miso systems exploiting deep reinforcement learning," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1839–1850, 2020.

[34] Y. Eghbali, S. Faramarzi, S. K. Taskou, M. R. Mili, M. Rasti, and E. Hossain, "Beamforming for star-ris-aided integrated sensing and communication using meta drl," *IEEE Wireless Commun. Lett.*, vol. 13, no. 4, pp. 919–923, 2024.

[35] Z. Ma, R. Zhang, B. Ai, Z. Lian, L. Zeng, and D. Niyato, "Deep reinforcement learning for energy efficiency maximization in rsma-irs-assisted isac system," *arXiv preprint arXiv:2501.15091*, 2025.

[36] F. B. Mismar, B. L. Evans, and A. Alkhateeb, "Deep reinforcement learning for 5g networks: Joint beamforming, power control, and interference coordination," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1581–1592, 2019.

[37] K. Feng, Q. Wang, X. Li, and C.-K. Wen, "Deep reinforcement learning based intelligent reflecting surface optimization for miso communication systems," *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 745–749, 2020.

[38] L. Xiao, G. Sheng, S. Liu, H. Dai, M. Peng, and J. Song, "Deep reinforcement learning-enabled secure visible light communication against eavesdropping," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 6994–7005, 2019.

[39] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, and Q. Wu, "Deep reinforcement learning-based intelligent reflecting surface for secure wireless communications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 375–388, 2020.

[40] Z. Zhu, M. Gong, G. Sun, P. Liu, and D. Mi, "Ai-enabled star-ris aided miso isac secure communications," *Tsinghua Sci. Technol.*, vol. 30, no. 3, pp. 998–1011, 2024.

[41] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM Rev.*, vol. 38, no. 1, pp. 49–95, 1996.

[42] Z. Luo, W. Ma, A. M. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, 2010.

[43] S. J. Wright, *Primal-Dual Interior-Point Methods*. SIAM, 1997. [Online]. Available: https://doi.org/10.1137/1.9781611971453

[44] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.2," Jan. 2020. [Online]. Available: https://cvxr.com/cvx

[45] S. P. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[46] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secrecy rate beamforming for multicell networks with information and energy harvesting," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 677–689, 2016.

[47] H. W. Kuhn and A. W. Tucker, "Nonlinear programming," in *Traces and emergence of nonlinear programming*. Springer, 2013, pp. 247–258.