

Secure Beamforming and Power Allocation for RIS-Assisted NOMA-ISAC Systems With Internal and External Eavesdroppers

Yaming Li^{ID}, Ming Jin^{ID}, Senior Member, IEEE, Qinghua Guo^{ID}, Senior Member, IEEE, Junteng Yao^{ID}, Tao Jiang^{ID}, and Juan Liu^{ID}, Member, IEEE

Abstract—This work investigates secure transmission in non-orthogonal multiple access (NOMA)-integrated sensing and communication (ISAC) systems, where legitimate users may act as internal eavesdroppers alongside external eavesdroppers. We propose a reconfigurable intelligent surface (RIS)-assisted channel selection scheme to degrade channels of internal eavesdroppers and enhance legitimate links. To counter external eavesdroppers, we minimize communication power while satisfying constraints on communication rates, security and sensing performance. Then, we formulate a secure beamforming and power allocation optimization problem, and then propose a semidefinite relaxation (SDR) and penalty-based alternating optimization (AO) algorithm to solve it. The convergence and the computational complexity of the proposed algorithm are analyzed and numerical results are provided to demonstrate the superior secure performance of the proposed scheme.

Index Terms—Integrated sensing and communication (ISAC), reconfigurable intelligent surface (RIS), non-orthogonal multiple access (NOMA), beamforming, channel selection.

I. INTRODUCTION

A. Background and Related Works

THE NEXT-GENERATION wireless networks have substantial demands for both communication and sensing to support a wide range of emerging Internet of Things (IoT) services, including smart cities and smart factories [1]. Taking smart factory applications as an example, communication and sensing involve challenges such as hardware cost, spectral efficiency, massive terminal access, and data security.

Received 20 September 2024; revised 24 March 2025; accepted 16 May 2025. Date of publication 20 May 2025; date of current version 19 December 2025. This work was supported in part by the National Natural Science Foundation of China under Grants 62471265 and 61871246, in part by the Zhejiang Provincial Natural Science Foundation of China under Grants LZ25F010008 and LR21F010001, in part by the Science and Technology Innovation 2035 Major Project of Ningbo under Grant 2024Z286 and in part by the Science and Technology Innovation 2025 Major Project of Ningbo under Grant 2022Z186. The associate editor coordinating the review of this article and approving it for publication was A. Srinivasan. (Corresponding author: Ming Jin.)

Yaming Li, Ming Jin, Junteng Yao, Tao Jiang, and Juan Liu are with the Faculty of Electrical Engineering and Computer Science, Ningbo University, Ningbo 315211, China (e-mail: 221100133@nbu.edu.cn; jinming@nbu.edu.cn; yaojunteng@nbu.edu.cn; 2301100047@nbu.edu.cn; liujuan1@nbu.edu.cn).

Qinghua Guo is with the School of Electrical, Computer and Telecommunications Engineering, University of Wollongong, Wollongong, NSW 2522, Australia (e-mail: qguo@uow.edu.au).

Digital Object Identifier 10.1109/TCCN.2025.3571935

Integrated sensing and communication (ISAC) [2], [3], [4], [5] shares the hardware and spectral resources for communication and sensing functionalities, decreasing hardware cost and increasing spectral efficiency. Non-orthogonal multiple access (NOMA) [6], [7] enables multiple terminals to access the same spectral band simultaneously, and facilitates the access of an increased number of IoT terminals (such as smart factory equipment) in ISAC systems. Reconfigurable intelligent surfaces (RISs) provide additional propagation links and a substantial spatial degrees of freedom (DoFs), and they can improve both communication and security performance [8], [9], [10], [11], [12]. Therefore, combining ISAC, NOMA and RIS can significantly improve spectral efficiency, quality of services (QoS) in communications, and security performance as well [13], [14], [15], and satisfy the requirements of communication and sensing in smart factory applications.

In communication-centric ISAC systems, communication signals carrying privacy information are often used for sensing radar targets, making them vulnerable to eavesdroppers, when the radar targets act as potential eavesdroppers [16], [17]. To achieve secure communications, a base station (BS) transmits artificial noise (AN) to sense and interfere with the radar targets/eavesdroppers [17]. While the isotropic (ISO) scheme allocates half of the transmit power to AN for simplicity [18], [19], recent studies aim to enhance efficiency by optimizing spatial resource allocation. For instance, a beamforming strategy exploiting the statistical distribution of target locations was proposed in [20], achieving dynamic AN power allocation and reducing dependence on isotropic transmission. Additionally, when some radar targets are trusted, AN can be selectively directed towards untrusted targets [21]. This approach has been extended to heterogeneous network architectures by addressing self-interference suppression and AN beamforming, thereby jointly optimizing the energy efficiency and security of full-duplex ISAC systems [22].

Integrating NOMA into the ISAC framework can further enhance system performance by leveraging the efficient resource utilization of NOMA [23]. Recent advancements in NOMA-ISAC resource allocation demonstrate significant potential in balancing spectral efficiency and functional integration. For instance, a joint beamforming and power allocation strategy was introduced in [23] that dynamically prioritizes sensing accuracy or communication rate based on channel state information (CSI), enabling dual-function

trade-offs without dedicated sensing waveforms. In [24], a joint optimization framework for user-target pairing and beamforming in ISAC networks was proposed, which leverages NOMA's superimposed signals to associate specific users with radar targets and minimizes mutual interference through spatiotemporal resource alignment. In [25], a secure precoding/beamforming scheme was proposed to maximize the sum rate of communication users under sensing and security constraints, assuming perfect successive interference cancellation (SIC) for multiple NOMA users. However, it does not take advantage of the antenna array at the BS for interference suppression, limiting its performance [26]. In [26], communication users at close angles with respect to the antenna array at the BS share the same beamforming vector for suppressing the interference from the other users, achieving significant performance improvement even with imperfect SIC in NOMA. Moreover, the aforementioned schemes consider scenarios where targets are uncooperative within the system. However, in specific scenarios, cooperative sensing targets may obtain group-oriented information from the BS in the ISAC system. To address this challenge, a NOMA-based joint radar sensing and multicast-unicast communication system was investigated in [27].

RIS can enhance ISAC security through spatial DoF exploitation [28]. In [29], a joint active/passive beamforming optimization scheme was proposed to maximize sensing performance of a secure RIS-aided ISAC. In [30], a deep reinforcement learning algorithm was proposed to find the solution to the multivariable coupling and non-convex optimization problem of RIS-assisted secure ISAC. Meanwhile, the integration of RIS in dual-functional radar-communication (DFRC) systems has been explored in [31], where physical layer security (PLS) is enhanced through directional beam nulling. In [32], a robust PLS scheme was designed, addressing the difficulty of obtaining relevant information about eavesdroppers. Active RIS has the ability of amplifying the power of the incident signals [33], [34], and it was employed in [35] to improve the security performance of NOMA communications. In [36], the active RIS is employed to sense and combat a radar target which also acts as an eavesdropper in a secure ISAC system. This capability has been further exploited in [37], where real-time adjustments of phase and amplitude are employed to simultaneously suppress interference and eavesdropping.

The aforementioned works only consider the case where a radar target acts as a potential eavesdropper or no radar target exists. When radar targets and eavesdroppers exist separately, it is difficult to achieve both high sensing and security performance. For this scenario, security performance was investigated in [38] where AN signals are focused on radar targets rather than eavesdroppers. It is demonstrated that secure communications can be achieved, because the eavesdroppers' channels are harmed by strong interference due to the NOMA decoding order condition not being met. In [39], a jamming power maximization (JPM) scheme was proposed, where the leakage of AN signals from sidelobes of the array can interfere with eavesdroppers. However, the security performance of JPM degrades quickly when the transmit power of the BS

decreases or the number of eavesdroppers increases. In [40], radar signals are used to interfere with eavesdroppers for secure ISAC, and in [41], a RIS-assisted ISAC scheme was proposed for secure communications. However, they require the knowledge of the CSI from the BS and the RIS to eavesdroppers.

The existing works in the ISAC framework consider only external eavesdroppers [19], [20], [21], [22], [23], [24], [25], [26], [27]. In practice, legitimate communication users may also wiretap other users to pursue more resources [42]. In other words, the communication users can act as internal eavesdroppers. In contrast to external eavesdroppers, internal eavesdroppers are also legitimate users and they can exploit the information of ISAC systems to intercept signals intended for other users, thereby imposing more stringent constraints on inter-user interference management. Conventional approaches face challenges in effectively suppressing such internal eavesdropping attempts while maintaining communication rates for legitimate users. For this issue, a secure NOMA scheme was proposed in [43] to address the situation where one communication user acts as an internal eavesdropper along with several external eavesdroppers, and further in [44], a RIS-assisted secure NOMA scheme was proposed to counter both internal and external eavesdroppers. In [45], an active RIS-assisted secure NOMA scheme was proposed to combat an internal eavesdropper and an external eavesdropper. However, the works in [42], [43] do not consider external eavesdropping, while the works in [42], [43], [44], [45] do not account for the issue of sensing radar targets and only address the specific scenario of a single internal eavesdropper.

B. Motivations and Contributions

Although internal eavesdroppers pose a severe security issue to legitimate communications, to the best of the authors' knowledge, this issue has not been investigated in the framework of secure ISAC in the literature. Existing secure ISAC schemes predominately focus on external eavesdroppers and mostly operate under the premise that eavesdropping channels are available through perfect or partial CSI estimation. However, acquiring CSI of external eavesdroppers is fundamentally challenging due to their inherent concealment and non-cooperative nature. It is worth noting that RIS can dynamically adjust channel phases to enhance legitimate links while simultaneously forming destructive interference to internal eavesdroppers. Meanwhile, NOMA enables legitimate users to prioritize decoding while restricting external eavesdroppers from decoding superimposed signals. Integrating RIS and NOMA into a secure ISAC system can significantly enhance the system's security performance. However, existing studies have not yet fully exploited the potential performance gains brought by these two techniques. Motivated by this, in this work, we consider the challenging security issue for secure NOMA-ISAC where all communications users are potential internal eavesdroppers along with several external eavesdroppers. Specifically, the RIS-assisted NOMA-ISAC forms destructive channels for eavesdroppers and constructive

channels for legitimate communications. The main contributions are summarized as follows:

- We address a challenging and realistic security issue for RIS-assisted NOMA-ISAC system, where all communications users are potential internal eavesdroppers, the CSI of the external eavesdroppers is unknown and the imperfect SIC is considered. Meanwhile, with the constraint on the transmit power at the BS, we minimize the power of communication signals (and maximizing the power of AN signals correspondingly) to combat external eavesdroppers. Moreover, the array beampattern at the BS is optimized to illuminate the transmitted signal on radar targets. To achieve these aims, we formulate a secure beamforming and power allocation optimization problem for RIS-assisted NOMA-ISAC systems against both internal and external eavesdroppers.
- Considering all internal eavesdropper channels could make the optimization problem unsolvable. Therefore, we propose a channel selection scheme that selectively destructs partial channels based on the NOMA decoding order. To deal with the non-convexity of the formulated problem, we propose a semidefinite relaxation (SDR)-based alternating optimization (AO) algorithm. Meanwhile, we propose a penalty iteration method to guarantee that the solutions are almost rank-one. Further, the convergence and the computational complexity of the proposed SDR and penalty terms-based AO algorithm are analyzed. Moreover, we extend the algorithm to the general case of imperfect CSI and propose a robust beamforming scheme.
- Numerical results are provided to demonstrate the effectiveness of the proposed scheme. Compared with the existing schemes, the proposed scheme delivers the best performance in secure communication and the gap in performance with the communication-only scheme is negligible.

The rest of this paper is organized as follows. Section II introduces the system model for a secure RIS-assisted NOMA-ISAC system. In Section III, the optimization problem is formulated. In Section IV, an SDR and penalty terms-based AO algorithm is proposed to solve the problem. In Section V, a robust beamforming scheme is proposed. Simulation results and discussion are provided in Section VI. Finally, conclusions are drawn in Section VII.

Notations: In this paper, boldface upper-case and lower-case letters denote matrices and vectors, respectively. The notations $|x|$, $\|\mathbf{x}\|$, \mathbf{x}^T and \mathbf{x}^H denote the absolute, Euclidean norm, transpose and Hermitian conjugate transpose operators, respectively. $\text{diag}(\mathbf{x})$ denotes a diagonal matrix whose diagonal elements are constructed from the elements of the vector \mathbf{x} . The terms $\text{Tr}(\mathbf{X})$ and $\text{rank}(\mathbf{X})$ denote the trace and rank operators, respectively. $\mathbf{X} \succeq 0$ denotes that \mathbf{X} is a positive semidefinite matrix. $\mathbb{E}\{\cdot\}$ denotes the expectation operation. $\mathbf{x} \sim \mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ denotes that vector \mathbf{x} obeys a circularly symmetric complex Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma}$. We use \otimes to denote the Kronecker product, $\text{vec}(\cdot)$ to denote the vectorization of a matrix, \mathbf{I}

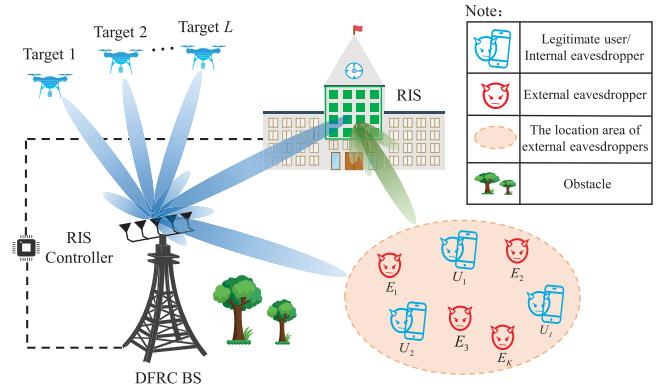


Fig. 1. Illustration of a RIS-aided NOMA-ISAC secure system, which includes a DFRC BS, a passive RIS, L sensing targets, I legitimate communication users/internal eavesdroppers, and K external eavesdroppers randomly distributed within the operational area.

to denote an identity matrix, and $\mathbf{1}$ to denote an all-ones vector.

II. SYSTEM MODEL

We examine a RIS-aided NOMA-ISAC system depicted in Fig. 1. This system comprises a DFRC BS equipped with a uniform linear array (ULA) of N antennas, a RIS with a uniform rectangular array (URA) of M reflecting elements, L radar targets, I single-antenna legitimate users served by the BS, and K single-antenna external eavesdroppers, attempting to intercept the BS's transmissions. The BS transmits superimposed signals to radar targets and legitimate users for sensing and secure communications, simultaneously. Denote the sets of legitimate users, external eavesdroppers, radar targets, and reflecting elements of the RIS by $\mathcal{I} = \{1, \dots, i, \dots, I\}$, $\mathcal{K} = \{1, \dots, k, \dots, K\}$, $\mathcal{L} = \{1, \dots, l, \dots, L\}$ and $\mathcal{M} = \{1, \dots, m, \dots, M\}$, respectively. We use \mathbf{U}_i and \mathbf{E}_k to denote the i th legitimate user and the k th external eavesdropper, and assume that the legitimate users can eavesdrop on each other as being internal eavesdroppers. Without loss of generality, the BS, RIS and legitimate users are cooperative for their communications, and the CSI among them can be obtained with channel estimation using training signals [46]. Particularly, we can utilize an anchor-assisted channel estimation method for estimating RIS-related channels [47]. In radar sensing applications, the ISAC system often has specific region-of-interests (ROIs), and it will illuminate the sensing signals on the angles in the ROIs for radar sensing [17]. Let θ_l be the angle of the l th target, and we assume that the exact θ_l is unknown but it belongs to an ROI of the ISAC system.

The transmitted signal at the BS is given by

$$\mathbf{s} = \sum_{i=1}^I \mathbf{w}_i x_i + \mathbf{s}_r \quad (1)$$

where x_i denotes the communication signal of the i th legitimate user having unit power, $\mathbf{w}_i \in \mathbb{C}^{N \times 1}$ is the beamforming vector corresponding to x_i , and \mathbf{s}_r denotes the radar signal with $\mathbf{s}_r \sim \mathcal{CN}(\mathbf{0}, \mathbf{S}_r)$ with $\mathbf{S}_r \succeq 0$ being the covariance

matrix. We assume that x_i and s_r are statistically independent of each other. It is reasonable to assume that the BS has a constraint of maximum transmitting power, denoted as p_{\max} . Since the radar signal lacks communication information, it is treated as AN to counteract eavesdropping.¹

Before introducing channel, communication and sensing models, we explain the communication and sensing parts of ISAC in Fig. 1. The sensing part of the ISAC system consists of the BS and several targets. The transmitted signal \mathbf{s} in (1) is illuminated on the targets with an optimized array beampattern, and the echoes from the targets to the BS are used for sensing. The communication part of the ISAC system consists of the BS, the RIS, legitimate users (also act as internal eavesdroppers), and external eavesdroppers. The RIS is employed to form one-hop line-of-sight (LoS) links for both legitimate users and external eavesdroppers. By optimizing the phase shifts of the RIS, it forms destructive interference to eavesdroppers while simultaneously enhancing the performance of legitimate links. This spatial control capability is crucial for suppressing internal eavesdroppers and extending the coverage of AN to external eavesdroppers. The communication signal x_i in (1) is for the legitimate users and the AN s_r is to combat both internal and external eavesdroppers. Moreover, NOMA is beneficial in countering external eavesdroppers, as it restricts the ability of external eavesdroppers in decoding superimposed signals.

A. Channel Model

We consider quasi-static flat fading channels, which remain unchanged in a channel coherence block, but vary among blocks. RIS is often used to provide one-hop LoS links from the BS to legitimate users when direct LoS links between the BS and the legitimate users are unavailable. Without loss of generality, we assume that the LoS channel from the BS to the RIS $\mathbf{H}_{B,R} \in \mathbb{C}^{M \times N}$ follows the Rician fading, and it is given by [12], [31], [32]

$$\mathbf{H}_{B,R} = \sqrt{\beta_0 d_{B,R}^{-\alpha_{B,R}}} \left(\sqrt{\frac{\kappa_{B,R}}{\kappa_{B,R} + 1}} \mathbf{G}_{B,R}^L + \sqrt{\frac{1}{\kappa_{B,R} + 1}} \mathbf{G}_{B,R}^N \right), \quad (2)$$

where β_0 denotes the path loss at one-meter reference distance, $d_{B,R}$ denotes the distance between the BS and the RIS, $\alpha_{B,R}$ denotes the path-loss exponent, $\kappa_{B,R}$ denotes the Rician factor, $\mathbf{G}_{B,R}^N$ denotes the Non-LoS (NLoS) part of the channel with its elements being independently and identically standard complex Gaussian distributed (SCGD), $\mathbf{G}_{B,R}^L = \mathbf{a}_{P,R}(\vartheta_R, \phi_R) \mathbf{a}_L^H(\theta_B)$ denotes the LoS channel component with $\mathbf{a}_{P,R}(\vartheta_R, \phi_R)$ and $\mathbf{a}_L(\theta_B)$ being the receive array response of URA at the RIS and the transmit array response of ULA at the BS, respectively. Let d_R denote the antenna spacing of the URA, ϑ_R denote the azimuth angle-of-arrival (AoA) and ϕ_R denote the elevation AoA, the receive array response $\mathbf{a}_P(\vartheta_R, \phi_R)$ is given by

$$\mathbf{a}_{P,R}(\vartheta_R, \phi_R) = \mathbf{a}_{az}(\vartheta_R, \phi_R) \otimes \mathbf{a}_{el}(\phi_R) \quad (3)$$

¹For the sake of simplicity, the radar signal will be referred to AN signal.

where

$$\begin{aligned} \mathbf{a}_{az}(\vartheta, \phi) &\triangleq \\ &[1, e^{j \frac{2\pi}{\lambda} d_R \sin \vartheta \cos \phi}, \dots, e^{j \frac{2\pi}{\lambda} (M_x - 1) d_R \sin \vartheta \cos \phi}]^T \end{aligned} \quad (4)$$

and

$$\mathbf{a}_{el}(\phi) \triangleq [1, e^{j \frac{2\pi}{\lambda} d_R \sin \phi}, \dots, e^{j \frac{2\pi}{\lambda} (M_z - 1) d_R \sin \phi}]^T \quad (5)$$

with λ denoting the carrier wavelength, M_x and M_z ($M_x \times M_z = M$) denoting the number of elements of the URA at the RIS along the x -axis and z -axis, respectively. Moreover, the transmit array response of ULA at the BS is given by

$$\mathbf{a}_L(\theta_B) = [1, e^{j \frac{2\pi}{\lambda} d_B \sin \theta_B}, \dots, e^{j \frac{2\pi}{\lambda} (N - 1) d_B \sin \theta_B}]^T \quad (6)$$

where d_B denotes the antenna spacing of the ULA at the BS,² and θ_B denotes the angle-of-departure (AoD).

For legitimate user and external eavesdroppers, let $\mathbf{h}_{B,U_i} \in \mathbb{C}^{N \times 1}$ be the channel from the BS to the i th legitimate user, $\mathbf{h}_{B,E_k} \in \mathbb{C}^{N \times 1}$ be the channel from the BS to the k th external eavesdropper, $\mathbf{h}_{R,U_i} \in \mathbb{C}^{M \times 1}$ be the channel from the RIS to the i th legitimate user, and $\mathbf{h}_{R,E_k} \in \mathbb{C}^{M \times 1}$ be the channel from the RIS to the k th external eavesdropper. It is assumed that the NLoS channels \mathbf{h}_{B,U_i} and \mathbf{h}_{B,E_k} are Rayleigh fading, and the LoS channels \mathbf{h}_{R,U_i} and \mathbf{h}_{R,E_k} are Rician fading, which are respectively given by [31], [32]

$$\mathbf{h}_{B,U_i} = \sqrt{\beta_0 d_{B,U_i}^{-\alpha_{B,U_i}}} \mathbf{g}_{B,U_i} \quad (7)$$

$$\mathbf{h}_{B,E_k} = \sqrt{\beta_0 d_{B,E_k}^{-\alpha_{B,E_k}}} \mathbf{g}_{B,E_k} \quad (8)$$

$$\mathbf{h}_{R,U_i} = \sqrt{\beta_0 d_{R,U_i}^{-\alpha_{R,U_i}}} \left(\sqrt{\frac{\kappa_{R,U_i}}{\kappa_{R,U_i} + 1}} \mathbf{g}_{R,U_i}^L + \sqrt{\frac{1}{\kappa_{R,U_i} + 1}} \mathbf{g}_{R,U_i}^N \right) \quad (9)$$

$$\mathbf{h}_{R,E_k} = \sqrt{\beta_0 d_{R,E_k}^{-\alpha_{R,E_k}}} \left(\sqrt{\frac{\kappa_{R,E_k}}{\kappa_{R,E_k} + 1}} \mathbf{g}_{R,E_k}^L + \sqrt{\frac{1}{\kappa_{R,E_k} + 1}} \mathbf{g}_{R,E_k}^N \right) \quad (10)$$

where d_{B,U_i} and d_{B,E_k} denote the distances from the BS to the i th legitimate user and the k th external eavesdropper, respectively, d_{R,U_i} and d_{R,E_k} denote the distances from the RIS to the i th legitimate user and the k th external eavesdropper, respectively, α_{B,U_i} , α_{B,E_k} , α_{R,U_i} and α_{R,E_k} denote the path-loss exponents, κ_{R,U_i} and κ_{R,E_k} denote the Rician factors, \mathbf{g}_{B,U_i} and \mathbf{g}_{B,E_k} denote the Rayleigh fading vectors with their elements being the SCGD of $\mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$, \mathbf{g}_{R,U_i}^N and \mathbf{g}_{R,E_k}^N denote the NLoS parts of the corresponding channels with their elements being independently and identically SCGD, $\mathbf{g}_{R,U_i}^L = \mathbf{a}_{P,T}(\vartheta_i, \phi_i)$ and $\mathbf{g}_{R,E_k}^L = \mathbf{a}_{P,T}(\vartheta_k, \phi_k)$ denote the LoS channel components of the corresponding channels with $\mathbf{a}_{P,T}(\vartheta_i, \phi_i)$ and $\mathbf{a}_{P,T}(\vartheta_k, \phi_k)$ being the transmit array responses of URA at the RIS. The transmit array responses $\mathbf{a}_{P,T}(\vartheta_i, \phi_i)$ and $\mathbf{a}_{P,T}(\vartheta_k, \phi_k)$ are respectively given by

$$\mathbf{a}_{P,T}(\vartheta_i, \phi_i) = \mathbf{a}_{az}(\vartheta_i, \phi_i) \otimes \mathbf{a}_{el}(\phi_i) \quad (11)$$

and

$$\mathbf{a}_{P,T}(\vartheta_k, \phi_k) = \mathbf{a}_{az}(\vartheta_k, \phi_k) \otimes \mathbf{a}_{el}(\phi_k) \quad (12)$$

²Without loss of generality, we assume that d_R and d_B are $\lambda/2$ [17], [21], [40].

where ϑ_i and ϑ_k denotes the azimuth AoD, and ϕ_i and ϕ_k denotes the elevation AoD.

B. Communication Model

Based on the aforementioned transmit signal model and channel model, the received signal at the i th legitimate user/internal eavesdropper is given by

$$y_{U_i} = \left(\mathbf{h}_{B,U_i}^H + \mathbf{h}_{R,U_i}^H \Theta \mathbf{H}_{B,R} \right) \mathbf{s} + z_{U_i} \quad (13)$$

where $z_{U_i} \sim \mathcal{CN}(0, \sigma_U^2)$ denotes the additive white Gaussian noise (AWGN) at the legitimate users or the internal eavesdroppers, $\Theta = \text{diag}(e^{j\nu_1}, e^{j\nu_2}, \dots, e^{j\nu_M})$ represents the phase-shifting matrix of the RIS with $\nu_m \in [0, 2\pi)$ being the phase of the m th element. The legitimate users employ SIC to decode their signals in an order determined based on channel gains [25], [38], [39]. We determine the order with an arbitrary initial value of Θ . Without loss of generality, it is assumed that the decoding order is U_1, U_2, \dots, U_I . To maintain the decoding order, arbitrary initial values of \mathbf{w}_i ($i = 1, \dots, I$) are selected that satisfy

$$\mathbf{g}_{U_i}^H \mathbf{S}_r \mathbf{g}_{U_i} \geq |\mathbf{g}_{U_i}^H \mathbf{w}_1|^2 \geq \dots \geq |\mathbf{g}_{U_i}^H \mathbf{w}_I|^2 \quad (14)$$

where

$$\mathbf{g}_{U_i}^H = \mathbf{h}_{B,U_i}^H + \mathbf{h}_{R,U_i}^H \Theta \mathbf{H}_{B,R}. \quad (15)$$

The signal-to-interference-plus-noise rate (SINR) at U_i for decoding the communication signal x_j can be expressed as

$$\text{SINR}_{U_i}^{U_j} = \frac{|\mathbf{g}_{U_i}^H \mathbf{w}_j|^2}{\bar{I}_i^j + \beta(\bar{I}_i^j + \mathbf{g}_{U_i}^H \mathbf{S}_r \mathbf{g}_{U_i}) + \sigma_U^2}, \forall i, j \quad (16)$$

where $\bar{I}_i^j = \sum_{m=j+1}^I |\mathbf{g}_{U_i}^H \mathbf{w}_m|^2$ with $\bar{I}_i^I = 0$, $\bar{I}_i^j = \sum_{m=1}^{j-1} |\mathbf{g}_{U_i}^H \mathbf{w}_m|^2$ with $\bar{I}_i^1 = 0$, and $\beta \in [0, 1]$ is the imperfect SIC factor. Note that the subscripts $(\cdot)_m$, $(\cdot)_i$ and $(\cdot)_j$ are just the indexes of internal eavesdropping/legitimate user. When the indexes are equal, \mathbf{w}_m , \mathbf{w}_i and \mathbf{w}_j represent the same beamforming vector. In addition, U_i and U_j represent the same user when $i = j$. Consequently, the achievable rate of x_j at U_i is given by

$$R_{U_i}^{U_j} = \log_2 \left(1 + \text{SINR}_{U_i}^{U_j} \right), \forall i, j \quad (17)$$

which represents the achievable rate of U_i itself with $i = j$, and the internal eavesdropping rate with $i \neq j$.

For the external eavesdroppers, the signal received by the k th external eavesdropper after passing through the direct and cascaded channels can be expressed as

$$y_{E_k} = \left(\mathbf{h}_{B,E_k}^H + \mathbf{h}_{R,E_k}^H \Theta \mathbf{H}_{B,R} \right) \mathbf{s} + z_{E_k} \quad (18)$$

where $z_{E_k} \sim \mathcal{CN}(0, \sigma_E^2)$ denotes the AWGN at the external eavesdroppers. Due to external eavesdroppers who have less prior knowledge of legitimate transmission, it is difficult to use the SIC to remove the interferences [25], [38], [39]. Thus,

the received SINR of x_j at the k th external eavesdropper is expressed as

$$\text{SINR}_{E_k}^{U_j} = \frac{|\mathbf{g}_{E_k}^H \mathbf{w}_j|^2}{\mathbf{g}_{E_k}^H \mathbf{S}_r \mathbf{g}_{E_k} + \sum_{i=1, i \neq j}^I |\mathbf{g}_{E_k}^H \mathbf{w}_i|^2 + \sigma_E^2}, \forall i, j \quad (19)$$

where

$$\mathbf{g}_{E_k}^H = \mathbf{h}_{B,E_k}^H + \mathbf{h}_{R,E_k}^H \Theta \mathbf{H}_{B,R}. \quad (20)$$

Thus, the eavesdropping rate towards x_j by the k th external eavesdropper is given by

$$R_{E_k}^{U_j} = \log_2 \left(1 + \text{SINR}_{E_k}^{U_j} \right), \forall j. \quad (21)$$

C. Sensing Model

Beampattern error is employed as the key performance indicator to evaluate the radar sensing performance [30], [38]. The beampattern error metric quantifies the mismatch between the designed and desired beampatterns. Minimizing this error ensures concentrated mainlobe power and reduced sidelobe interference, improving radar detection performance. More significantly, the beampattern error allows a flexible choice of the beam mainlobes width, which can account for the uncertainty of target angles.

According to (1), we can obtain the covariance matrix of the transmitted signals at the BS as

$$\mathbf{R}_s = \mathbb{E} \left\{ \mathbf{s} \mathbf{s}^H \right\} = \sum_{i=1}^I \mathbf{w}_i \mathbf{w}_i^H + \mathbf{S}_r. \quad (22)$$

Thus, the transmit beampattern can be expressed as

$$p(\theta) = \mathbb{E} \left\{ |\mathbf{a}_L^H(\theta) \mathbf{s}|^2 \right\} = \mathbf{a}_L^H(\theta) \mathbf{R}_s \mathbf{a}_L(\theta). \quad (23)$$

The desired beampattern is defined as

$$\hat{p}(\theta) = \begin{cases} 1, & \theta_l - \frac{\Delta_\theta}{2} \leq \theta \leq \theta_l + \frac{\Delta_\theta}{2}, \\ 0, & \text{otherwise,} \end{cases} \quad (24)$$

where Δ_θ denotes the beam width of an ROI of potential targets. To match a desired beampattern, the mean square error (MSE) between the desired and the designed beampatterns is given by [13], [21]

$$L(\eta, \mathbf{R}_s) = \frac{1}{S} \sum_{s=1}^S \left| \eta \hat{p}(\theta_s) - \mathbf{a}_L^H(\theta_s) \mathbf{R}_s \mathbf{a}_L(\theta_s) \right|^2 \quad (25)$$

where η denotes the scaling factor that is to be optimized,³ θ_s denotes the discrete angle in $[-\pi/2, \pi/2)$ and S is the total number of discrete angles.

³The normalized beampattern $\hat{p}(\theta)$ in (24) is defined as an ideal binary template (0 or 1). The scaling factor η scales the gain of $\hat{p}(\theta)$ to align it with the actual power budget of the BS, ensuring that the optimized beampattern $\mathbf{a}_L^H(\theta) \mathbf{R}_s \mathbf{a}_L(\theta)$ achieves the desired spatial shape while respecting power limitation [21].

III. PROBLEM FORMULATION

In this section, we establish a power minimization problem for legitimate users under the constraint of total transmit power. In PLS, maximizing secrecy capacity relies on the knowledge of the CSI of both legitimate users and eavesdroppers (including internal and external eavesdroppers). The BS, RIS and legitimate users are cooperative for their communications, and it is reasonable to assume that the channel coefficients among them are known. However, external eavesdroppers act as illegal nodes and typically conceal their identities to avoid being detected, and their CSI is hard to be acquired. BS cannot obtain the secrecy capacity of external eavesdroppers. To tackle this issue, we propose to maximize the power of radar sensing (AN) signals to counteract external eavesdroppers. Considering the maximum transmitting power of the BS, maximizing the power of radar sensing (AN) signals is equivalent to minimizing the power of communication signals. Hence, we formulate an optimization problem of minimizing the power of communication signals x_i subject to constraints on sensing beampattern error, communication rates of legitimate users, and internal eavesdropping rates as

$$\min_{\mathbf{w}_i, \mathbf{S}_r, \Theta, \eta} \sum_{i=1}^I \|\mathbf{w}_i\|^2 \quad (26a)$$

$$\text{s.t. } R_{\mathbf{U}_i}^{\mathbf{U}_j} \geq \varepsilon_i, \forall i = j, \quad (26b)$$

$$R_{\mathbf{U}_i}^{\mathbf{U}_j} \leq \varepsilon_i - \varepsilon_{th}^i, \forall i \neq j, \quad (26c)$$

$$L(\eta, \mathbf{R}_s) \leq \epsilon, \quad (26d)$$

$$\sum_{i=1}^I \|\mathbf{w}_i\|^2 + \text{Tr}(\mathbf{S}_r) \leq p_{\max}, \quad (26e)$$

$$\mathbf{g}_{\mathbf{U}_i}^H \mathbf{S}_r \mathbf{g}_{\mathbf{U}_i} \geq |\mathbf{g}_{\mathbf{U}_i}^H \mathbf{w}_1|^2 \geq \dots \geq |\mathbf{g}_{\mathbf{U}_i}^H \mathbf{w}_I|^2, \forall i \quad (26f)$$

$$\mathbf{S}_r \succeq 0, \quad (26g)$$

where ε_i denotes requirement of minimum achievable rate for \mathbf{U}_i , ε_{th}^i denotes the minimum internal secrecy rate for \mathbf{U}_i , and ϵ denotes the maximum beampattern error for radar sensing. Constraints (26b) and (26c) guarantee the internal secure communication, (26d) regulates the radar beampattern, (26e) enforces the maximum transmitting power of the BS, (26f) ensures the predefined NOMA decoding order, and (26g) guarantees the positive semidefiniteness of the covariance matrix of radar signals.

In (26c), all channels are considered to meet the secure requirements on internal eavesdropping rates. Our numerical simulations show that this can make the problem (26) difficult to solve. Hence, we propose to focus on partial channels rather than all channels. Now, we revisit $\text{SINR}_{\mathbf{U}_i}^{\mathbf{U}_j}$ for $i \neq j$ in (16). Considering that the SIC factor β is usually small, to effectively secure the information of \mathbf{U}_j from internal eavesdroppers, we focus on destructing (increasing) \bar{I}_i^j rather than $\beta(\bar{I}_i^j + \mathbf{g}_{\mathbf{U}_i}^H \mathbf{S}_r \mathbf{g}_{\mathbf{U}_i})$ in (16). Hence, we replace $\text{SINR}_{\mathbf{U}_i}^{\mathbf{U}_j}$, $i \neq j$, with

$$\overline{\text{SINR}}_{\mathbf{U}_i}^{\mathbf{U}_j} = \frac{|\mathbf{g}_{\mathbf{U}_i}^H \mathbf{w}_j|^2}{\bar{I}_i^j + \sigma_U^2}, \forall i \neq j, \quad (27)$$

where $\text{SINR}_{\mathbf{U}_i}^{\mathbf{U}_j} < \overline{\text{SINR}}_{\mathbf{U}_i}^{\mathbf{U}_j}$, then (26c) becomes

$$\log_2 \left(1 + \overline{\text{SINR}}_{\mathbf{U}_i}^{\mathbf{U}_j} \right) \leq \varepsilon_i - \varepsilon_{th}^i, \forall i \neq j. \quad (28)$$

It can be obtained that constraint (26c) always holds when (28) holds. Hence, problem (26) becomes

$$\min_{\mathbf{w}_i, \mathbf{S}_r, \Theta, \eta} \sum_{i=1}^I \|\mathbf{w}_i\|^2 \quad (29a)$$

$$\text{s.t. } (26b), (28), (26d), (26e), (26f), (26g). \quad (29b)$$

Obviously, problem (29) is non-convex because the variables are coupled in the constraint functions, and the constraint functions themselves are non-convex, which significantly increases the difficulty of solving (29). Therefore, in the following, we will focus on how to decouple problem (29) and transform it into convex optimization problems, thereby leveraging convex optimization techniques to achieve efficient solutions.

IV. JOINT SCALING FACTOR, ACTIVE AND PASSIVE BEAMFORMING OPTIMIZATION

In this section, we decompose the problem of (29) into three subproblems: 1) Optimization of scaling factor η , 2) active beamforming and power allocation at BS and 3) passive beamforming at RIS. The closed-form expression for the scaling factor η is derived, and then we propose an AO algorithm based on penalty terms and SDR to alternately solve the other subproblems.

A. Optimization of Scaling Factor η

In problem (26) or (29), the scaling factor η only exists in the constraint (26d). Hence, the variable η in the problem (26) or (29) can be eliminated by minimizing $L(\eta, \mathbf{R}_s)$. We can obtain the optimal η by letting the first-order partial derivative of $L(\eta, \mathbf{R}_s)$ with respect to η to zero, i.e.,

$$\frac{1}{S} \sum_{s=1}^S \left[2\eta \hat{p}^2(\theta_s) - 2\hat{P}(\theta_s) \mathbf{a}_L^H(\theta_s) \mathbf{R}_s \mathbf{a}_L(\theta_s) \right] = 0 \quad (30)$$

which gives

$$\eta^* = \frac{\sum_{s=1}^S \hat{p}(\theta_s) \mathbf{a}_L^H(\theta_s) \mathbf{R}_s \mathbf{a}_L(\theta_s)}{\sum_{s=1}^S \hat{p}^2(\theta_s)}. \quad (31)$$

Then, the constraint (26d) becomes

$$L(\eta^*, \mathbf{R}_s) \leq \epsilon. \quad (32)$$

B. Active Beamforming and Power Allocation at BS

In this subsection, we focus on the optimization of active beamforming and power allocation at BS, i.e., the optimization of \mathbf{w}_i and \mathbf{S}_r . As the communication signal x_i has unit power, \mathbf{w}_i and \mathbf{S}_r determine the power allocation among the

communication and radar signals. Defining the intermediate variables $\mathbf{G}_i = \mathbf{g}_{\mathbf{U}_i} \mathbf{g}_{\mathbf{U}_i}^H$, and $\mathbf{W}_i = \mathbf{w}_i \mathbf{w}_i^H$ gives⁴

$$|\mathbf{g}_{\mathbf{U}_i}^H \mathbf{w}_j|^2 = \text{Tr}(\mathbf{G}_i \mathbf{W}_j), \forall i, \forall j, \quad (33)$$

$$\mathbf{g}_{\mathbf{U}_i}^H \mathbf{S}_r \mathbf{g}_{\mathbf{U}_i} = \text{Tr}(\mathbf{G}_i \mathbf{S}_r), \forall i, \quad (34)$$

$$\text{rank}(\mathbf{W}_i) = 1, \forall i. \quad (35)$$

To facilitate subsequent processing, the optimization of \mathbf{w}_i can be transformed into an indirect optimization of \mathbf{W}_i . Omitting the rank-one constraint (35) with the SDR technique, and substituting (31) into the problem (29) give

$$\min_{\mathbf{W}_i, \mathbf{S}_r} \sum_{i=1}^I \text{Tr}(\mathbf{W}_i) \quad (36a)$$

$$\text{s.t. } \log_2 \left(1 + \text{SINR}_{\mathbf{U}_i}^{\mathbf{U}_j} \right) \geq \varepsilon_i, \forall i = j, \quad (36b)$$

$$\log_2 \left(1 + \overline{\text{SINR}}_{\mathbf{U}_i}^{\mathbf{U}_j} \right) \leq \varepsilon_i - \varepsilon_{th}^i, \forall i \neq j, \quad (36c)$$

$$L(\eta^*, \mathbf{R}_s) \leq \epsilon, \quad (36d)$$

$$\text{Tr} \left(\sum_{i=1}^I \mathbf{W}_i + \mathbf{S}_r \right) \leq p_{\max}, \quad (36e)$$

$$\text{Tr}(\mathbf{G}_i \mathbf{S}_r) \geq \text{Tr}(\mathbf{G}_i \mathbf{W}_1) \geq \dots \geq \text{Tr}(\mathbf{G}_i \mathbf{W}_I), \forall i, \quad (36f)$$

$$\mathbf{W}_i \succeq 0, \mathbf{S}_r \succeq 0, \forall i, \quad (36g)$$

where

$$\mathbf{R}_s = \sum_{i=1}^I \mathbf{W}_i + \mathbf{S}_r, \quad (37)$$

$$\text{SINR}_{\mathbf{U}_i}^{\mathbf{U}_j} = \frac{\text{Tr}(\mathbf{G}_i \mathbf{W}_j)}{\bar{I}_i^j + \beta \tilde{I}_i^j + \beta \text{Tr}(\mathbf{G}_i \mathbf{S}_r) + \sigma_{\mathbf{U}}^2}, \quad (38)$$

$$\overline{\text{SINR}}_{\mathbf{U}_i}^{\mathbf{U}_j} = \frac{\text{Tr}(\mathbf{G}_i \mathbf{W}_j)}{\bar{I}_i^j + \sigma_{\mathbf{U}}^2} \quad (39)$$

with

$$\bar{I}_i^j = \sum_{m=j+1}^I \text{Tr}(\mathbf{G}_i \mathbf{W}_m) \quad (40)$$

and

$$\tilde{I}_i^j = \sum_{m=1}^{j-1} \text{Tr}(\mathbf{G}_i \mathbf{W}_m). \quad (41)$$

The non-convex constraints (36b) and (36c) can be transformed into convex forms as

$$\begin{aligned} \text{Tr}(\mathbf{G}_i \mathbf{W}_i) &\geq (2^{\varepsilon_i} - 1) \left\{ \sum_{m=i+1}^I \text{Tr}(\mathbf{G}_i \mathbf{W}_m) \right. \\ &\quad \left. + \beta \left[\sum_{m=1}^{i-1} \text{Tr}(\mathbf{G}_i \mathbf{W}_m) + \text{Tr}(\mathbf{G}_i \mathbf{S}_r) \right] + \sigma_{\mathbf{U}}^2 \right\} \end{aligned} \quad (42)$$

⁴Note that the subscripts $(\cdot)_i$ and $(\cdot)_j$ are just the indexes of internal eavesdropping/legitimate user. When the indexes are equal, \mathbf{W}_i and \mathbf{W}_j represent the same matrix.

and

$$\begin{aligned} \text{Tr}(\mathbf{G}_i \mathbf{W}_j) &\leq \left(2^{\varepsilon_i - \varepsilon_{th}^i} - 1 \right) \left\{ \sum_{m=j+1}^I \text{Tr}(\mathbf{G}_i \mathbf{W}_m) \right. \\ &\quad \left. + \sigma_{\mathbf{U}}^2 \right\}, \forall i \neq j, \end{aligned} \quad (43)$$

respectively. Thus, problem (36) becomes

$$\min_{\mathbf{W}_i, \mathbf{S}_r} \sum_{i=1}^I \text{Tr}(\mathbf{W}_i) \quad (44a)$$

$$\text{s.t. } (36d)-(36g), (42), (43). \quad (44b)$$

The objective function and constraints in (44) are convex, which thus can be solved using convex optimization tools such as CVX. Then, the eigenvalue decomposition or Gaussian randomization technique [48] is adopted to obtain \mathbf{w}_i .

However, Gaussian randomization technique may lead to performance loss due to its probabilistic nature. Here, we employ a penalty term to tackle the rank-one constraint. Note that the inequality

$$\text{Tr}(\mathbf{W}_i) - \|\mathbf{W}_i\|_2 \geq 0 \quad (45)$$

holds for any \mathbf{W}_i , and \mathbf{W}_i becomes a rank-one matrix when $\text{Tr}(\mathbf{W}_i) - \|\mathbf{W}_i\|_2 = 0$. Therefore, we apply a penalty term to the object function in problem (44), leading to

$$\min_{\mathbf{W}_i, \mathbf{S}_r} \sum_{i=1}^I \text{Tr}(\mathbf{W}_i) + \rho_1 \sum_{i=1}^I (\text{Tr}(\mathbf{W}_i) - \|\mathbf{W}_i\|_2) \quad (46a)$$

$$\text{s.t. } (36d)-(36g), (42), (43), \quad (46b)$$

where ρ_1 is a penalty factor. However, the second part of the objective function in (46) is a difference-of-convex form. To tackle this issue, we employ the first-order Taylor expansion to obtain a lower bound of $\|\mathbf{W}_i\|_2$, and then rewrite the penalty term of problem (46) as

$$\rho_1 \sum_{i=1}^I \left(\text{Tr}(\mathbf{W}_i) - \|\widehat{\mathbf{W}}_i\|_2 - \text{Tr} \left[\widehat{v}_{\max} \widehat{v}_{\max}^H (\mathbf{W}_i - \widehat{\mathbf{W}}_i) \right] \right) \quad (47)$$

where $\widehat{\mathbf{W}}_i$ denotes the estimate of \mathbf{W}_i from the previous iteration, and \widehat{v}_{\max} is the eigenvector corresponding to the maximum eigenvalue of $\widehat{\mathbf{W}}_i$. To this extent, problem (46) can be solved using convex optimization tools, leading to an approximate rank-one solution of \mathbf{W}_i . Therefore, we can obtain the beamforming vector \mathbf{w}_i with the eigenvector of \mathbf{W}_i corresponding to its maximum eigenvalue.

C. Passive Beamforming at RIS

In this subsection, we focus on the optimization of passive beamforming at the RIS, i.e., the optimization of Θ . Similarly, to handle the non-convex constraints more succinctly, we define the intermediate variables as

$$\mathbf{G}_{i,j} = (\mathbf{H}_i \mathbf{w}_j) (\mathbf{H}_i \mathbf{w}_j)^H, \forall i, \forall j, \quad (48)$$

$$\mathbf{G}_{i,r} = \mathbf{H}_i \mathbf{S}_r \mathbf{H}_i^H, \forall i \quad (49)$$

with

$$\mathbf{H}_i = \begin{bmatrix} \text{diag}(\mathbf{h}_{\text{R},\text{U}_i}^H) \mathbf{H}_{\text{B},\text{R}} \\ \mathbf{h}_{\text{B},\text{U}_i}^H \end{bmatrix} \quad (50)$$

and an extended RIS reflecting matrix

$$\mathbf{E} = \mathbf{e}\mathbf{e}^H \quad (51)$$

with

$$\mathbf{e} = [e^{j\nu_1}, e^{j\nu_2}, \dots, e^{j\nu_M}, 1]^T. \quad (52)$$

Noting that optimizing Θ is equivalent to optimizing $\nu_m, m = 1, 2, \dots, M$, and it can be conveniently transformed into optimizing \mathbf{E} . Then, problem (29) with respect to \mathbf{E} becomes

$$\text{find } \mathbf{E} \quad (53a)$$

$$\text{s.t. } \log_2 \left(1 + \text{SINR}_{\text{U}_i}^{\text{U}_j} \right) \geq \varepsilon_i, \forall i = j, \quad (53b)$$

$$\log_2 \left(1 + \overline{\text{SINR}}_{\text{U}_i}^{\text{U}_j} \right) \leq \varepsilon_i - \varepsilon_{th}^i, \forall i \neq j, \quad (53c)$$

$$\text{Tr}(\mathbf{E}\mathbf{G}_{i,r}) \geq \text{Tr}(\mathbf{E}\mathbf{G}_{i,1}) \geq \dots \geq \text{Tr}(\mathbf{E}\mathbf{G}_{i,I}), \forall i, \quad (53d)$$

$$\text{diag}(\mathbf{E}) = \mathbf{1}_{(M+1) \times 1}, \quad (53e)$$

$$\mathbf{E} \succeq 0, \mathbf{S}_r \succeq 0, \quad (53f)$$

where

$$\text{SINR}_{\text{U}_i}^{\text{U}_j} = \frac{\text{Tr}(\mathbf{E}\mathbf{G}_{i,j})}{\bar{I}_i^j + \beta \tilde{I}_i^j + \beta \text{Tr}(\mathbf{E}\mathbf{G}_{i,r}) + \sigma_{\text{U}}^2} \quad (54)$$

$$\overline{\text{SINR}}_{\text{U}_i}^{\text{U}_j} = \frac{\text{Tr}(\mathbf{E}\mathbf{G}_{i,j})}{\bar{I}_i^j + \sigma_{\text{U}}^2}, \forall i \neq j \quad (55)$$

with

$$\bar{I}_i^j = \sum_{m=j+1}^I \text{Tr}(\mathbf{E}\mathbf{G}_{i,m}) \quad (56)$$

and

$$\tilde{I}_i^j = \sum_{m=1}^{j-1} \text{Tr}(\mathbf{E}\mathbf{G}_{i,m}). \quad (57)$$

For the details of the transformation of the squared modulus term in this process, please refer to the Appendix. Moreover, note that $\text{SINR}_{\text{U}_i}^{\text{U}_j}$ in (38) and $\overline{\text{SINR}}_{\text{U}_i}^{\text{U}_j}$ in (39) are functions of \mathbf{W}_j and \mathbf{S}_r , while in (54) and (55), they are regarded as functions of \mathbf{E} . Therefore, the non-convex constraints (53b) and (53c) can be transformed into convex forms as

$$\begin{aligned} \text{Tr}(\mathbf{E}\mathbf{G}_{i,i}) &\geq (2^{\varepsilon_i} - 1) \left\{ \sum_{m=i+1}^I \text{Tr}(\mathbf{E}\mathbf{G}_{i,m}) \right. \\ &\quad \left. + \beta \left[\sum_{m=1}^{i-1} \text{Tr}(\mathbf{E}\mathbf{G}_{i,m}) + \text{Tr}(\mathbf{E}\mathbf{G}_{i,r}) \right] + \sigma_{\text{U}}^2 \right\} \end{aligned} \quad (58)$$

and

$$\begin{aligned} \text{Tr}(\mathbf{E}\mathbf{G}_{i,j}) &\leq (2^{\varepsilon_i - \varepsilon_{th}^i} - 1) \left\{ \sum_{m=j+1}^I \text{Tr}(\mathbf{E}\mathbf{G}_{i,m}) \right. \\ &\quad \left. + \sigma_{\text{U}}^2 \right\}, \forall i \neq j. \end{aligned} \quad (59)$$

Then, problem (53) becomes

$$\text{find } \mathbf{E} \quad (60a)$$

$$\text{s.t. } (53d)-(53f), (58), (59) \quad (60b)$$

which is a convex optimization problem. However, the problem (60) is a feasible solution problem without the objective function. In order to achieve a better converged solution, we propose an explicit objective function for (60) by introducing nonnegative auxiliary variables $\{\mu_i, \psi_{i,j}, \lambda_{i,j}\}$, $i, j = 1, 2, \dots, I$. With these auxiliary variables, (60) is rewritten as

$$\begin{aligned} \max_{\mu_i, \psi_{i,j}, \lambda_{i,j}, \mathbf{E}} & \sum_{i=1}^I \mu_i + \sum_{i \neq j} \sum_{j=1}^I \psi_{i,j} + \sum_{i=1}^I \sum_{j=1}^I \lambda_{i,j} \\ & \text{s.t. } \text{Tr}(\mathbf{E}\mathbf{G}_{i,i}) \geq \mu_i + (2^{\varepsilon_i} - 1) \left\{ \sum_{m=i+1}^I \text{Tr}(\mathbf{E}\mathbf{G}_{i,m}) \right. \end{aligned} \quad (61a)$$

$$\begin{aligned} & \quad \left. + \beta \left[\sum_{m=1}^{i-1} \text{Tr}(\mathbf{E}\mathbf{G}_{i,m}) + \text{Tr}(\mathbf{E}\mathbf{G}_{i,r}) \right] + \sigma_{\text{U}}^2 \right\}, \end{aligned} \quad (61b)$$

$$\begin{aligned} \text{Tr}(\mathbf{E}\mathbf{G}_{i,j}) + \psi_{i,j} &\leq (2^{\varepsilon_i - \varepsilon_{th}^i} - 1) \cdot \left\{ \sigma_{\text{U}}^2 \right. \\ & \quad \left. + \sum_{m=j+1}^I \text{Tr}(\mathbf{E}\mathbf{G}_{i,m}) \right\}, \forall i \neq j, \end{aligned} \quad (61c)$$

$$\text{Tr}(\mathbf{E}\mathbf{G}_{i,r}) \geq \lambda_{i,1} + \text{Tr}(\mathbf{E}\mathbf{G}_{i,1}), \forall i \in \mathcal{I}, \quad (61d)$$

$$\begin{aligned} \text{Tr}(\mathbf{E}\mathbf{G}_{i,j-1}) &\geq \lambda_{i,j} + \text{Tr}(\mathbf{E}\mathbf{G}_{i,j}), \forall i, j \in \mathcal{I}, \\ & (53e), (53f). \end{aligned} \quad (61e) \quad (61f)$$

Similar to the handling of \mathbf{W}_i , we have

$$\begin{aligned} \max_{\mu_i, \psi_{i,j}, \lambda_{i,j}, \mathbf{E}} & \sum_{i=1}^I \mu_i + \sum_{i \neq j} \sum_{j=1}^I \psi_{i,j} + \sum_{i=1}^I \sum_{j=1}^I \lambda_{i,j} - \rho_2 \\ & \times \left(\text{Tr}(\mathbf{E}) - \|\tilde{\mathbf{E}}\|_2 - \text{Tr}[\tilde{v}_{\max} \tilde{v}_{\max}^H (\mathbf{E} - \tilde{\mathbf{E}})] \right) \end{aligned} \quad (62a)$$

$$\text{s.t. } (61b)-(61f), \quad (62b)$$

where ρ_2 is a penalty factor, $\tilde{\mathbf{E}}$ denotes an estimate of \mathbf{E} from the previous iteration, and \tilde{v}_{\max} is the eigenvector corresponding to the maximum eigenvalue of $\tilde{\mathbf{E}}$, respectively. Problem (62) is convex, which can be solved using convex optimization tools such as CVX, leading to an approximate rank-one solution of \mathbf{E} . Therefore, we can obtain the phase-shifting matrix Θ with the eigenvector of \mathbf{E} corresponding to its maximum eigenvalue.

Decomposing problem (26) into two subproblems leads to the SDR and penalty-based AO algorithm summarized in **Algorithm 1**.

D. Convergence and Computational Complexity

Problems (46) and (62) are convex and can be solved by a CVX solver. At the q th iteration of **Algorithm 1**, the objective function satisfies

Algorithm 1 SDR and Penalty-Based AO Algorithm for Problem (29)

```

1: Initialize BS beamforming vector  $\mathbf{w}_i$ , sensing covariance matrix  $\mathbf{S}_r$  and extended RIS reflecting vector  $\mathbf{e}$ , set initial penalty factor  $\rho_1$  and  $\rho_2$ , and  $\tau > 1$ . Let  $Q$  be the maximum number of iterations.
2: Calculate  $J^{(0)} = \sum_{i=1}^I \|\mathbf{w}_i\|^2$ ,  $\mathbf{W}_i^{(0)} = \mathbf{w}_i \mathbf{w}_i^H$ ,  $\mathbf{S}_r^{(0)} = \mathbf{S}_r$ ,  $\mathbf{E}^{(0)} = \mathbf{e} \mathbf{e}^H$ , and let  $q = 0$ .
3: Repeat
4:    $q \leftarrow q + 1$ .
5:   Repeat
6:      $t_1 \leftarrow 0$ .
7:     Repeat
8:       Obtain  $\mathbf{W}_i^{(t_1+1)}$  and  $\mathbf{S}_r^{(t_1+1)}$  by solving (46).
9:        $t_1 \leftarrow t_1 + 1$ .
10:      Until the iterative tolerance of the objective function of (46) is below the threshold  $\epsilon_1$ .
11:      Update  $\mathbf{W}_i^{(0)} \leftarrow \mathbf{W}_i^{(t_1)}$ ,  $\mathbf{S}_r^{(0)} \leftarrow \mathbf{S}_r^{(t_1)}$ ,  $\rho_1 \leftarrow \tau \rho_1$ .
12:      Until  $\sum_{i=1}^I (\text{Tr}(\mathbf{W}_i^{(t_1)}) - \|\mathbf{W}_i^{(t_1)}\|_2) \leq \bar{\epsilon}_1$ .
13:      Update  $\mathbf{W}_i^{(q)} \leftarrow \mathbf{W}_i^{(t_1)}$ ,  $\mathbf{S}_r^{(q)} \leftarrow \mathbf{S}_r^{(t_1)}$ .
14:   Repeat
15:      $t_2 \leftarrow 0$ .
16:     Repeat
17:       Obtain  $\mathbf{E}^{(t_2+1)}$  by solving (62).
18:        $t_2 \leftarrow t_2 + 1$ .
19:     Until the iterative tolerance of the objective function of (62) is below the threshold  $\epsilon_2$ .
20:     Update  $\mathbf{E}^{(0)} \leftarrow \mathbf{E}^{(t_2)}$ ,  $\rho_2 \leftarrow \tau \rho_2$ .
21:     Until  $\text{Tr}(\mathbf{E}^{(t_2)}) - \|\mathbf{E}^{(t_2)}\|_2 \leq \bar{\epsilon}_2$ .
22:     Update  $\mathbf{E}^{(q)} \leftarrow \mathbf{E}^{(t_2)}$ .
23:     Obtain  $\mathbf{w}_i$  and  $\mathbf{e}$  with  $\mathbf{W}_i^{(q)}$  and  $\mathbf{E}^{(q)}$ .
24:     Calculate  $J^{(q)}$  with  $\{\mathbf{w}_i, \forall i\}$ .
25:   Until  $|J^{(q)} - J^{(q-1)}| < \varrho$  or  $q > Q$ .

```

$$\begin{aligned}
& \text{Obj}\left(\mathbf{w}_1^{(q)}, \dots, \mathbf{w}_I^{(q)}, \mathbf{S}_r^{(q)}, \mathbf{e}^{(q-1)}\right) \\
& \leq \text{Obj}\left(\mathbf{w}_1^{(q-1)}, \dots, \mathbf{w}_I^{(q-1)}, \mathbf{S}_r^{(q-1)}, \mathbf{e}^{(q-1)}\right) \\
& = \min_{\mathbf{w}_i, \mathbf{S}_r} \text{Obj}\left(\mathbf{w}_1, \dots, \mathbf{w}_I, \mathbf{S}_r, \mathbf{e}^{(q-1)}\right)
\end{aligned} \tag{63}$$

and

$$\begin{aligned}
& \text{Obj}\left(\mathbf{w}_1^{(q)}, \dots, \mathbf{w}_I^{(q)}, \mathbf{S}_r^{(q)}, \mathbf{e}^{(q)}\right) \\
& \leq \text{Obj}\left(\mathbf{w}_1^{(q)}, \dots, \mathbf{w}_I^{(q)}, \mathbf{S}_r^{(q)}, \mathbf{e}^{(q-1)}\right) \\
& = \min_{\mathbf{e}} \text{Obj}\left(\mathbf{w}_1^{(q)}, \dots, \mathbf{w}_I^{(q)}, \mathbf{S}_r^{(q)}, \mathbf{e}\right).
\end{aligned} \tag{64}$$

As a result, we can have

$$J^{(q)} \leq J^{(q-1)} \tag{65}$$

which implies that $J^{(q)}$ in **Algorithm 1** decreases with iterations. In other words, the power allocated to sensing signals increases with iterations. Moreover, the power for sensing is bounded with the constraint of p_{\max} , thus the convergence of **Algorithm 1** is guaranteed.

The computational complexity of problem (26) primarily stems from solving subproblems (46) and (62). Subproblems (46) and (62) are semidefinite programming (SDP), and they involve $(I+1)N^2$ and $M^2 + 2I^2$ variables, respectively. Hence, according to [44], the overall complexity of **Algorithm 1** is $\mathcal{O}(q(t_1((I+1)N^2) + t_2(M^2 + 2I^2)) \log \frac{1}{\varrho})^{3.5}$, where q denotes the number of iterations.

V. ROBUST OPTIMIZATION OF ACTIVE AND PASSIVE BEAMFORMING

In this section, we consider the imperfect channels of \mathbf{h}_{B,U_i} and $\mathbf{G}_i = \text{diag}(\mathbf{h}_{R,U_i}^H) \mathbf{H}_{B,R}$. Let $\hat{\mathbf{h}}_{B,U_i}$ and $\hat{\mathbf{G}}_i$ be the estimated channel coefficients, and $\Delta\mathbf{h}_{B,U_i}$ and $\Delta\mathbf{G}_i$ be the estimation errors. Hence, \mathbf{h}_{B,U_i} and \mathbf{G}_i are respectively given by

$$\mathbf{h}_{B,U_i} = \hat{\mathbf{h}}_{B,U_i} + \Delta\mathbf{h}_{B,U_i}, \forall i \tag{66}$$

and

$$\mathbf{G}_i = \hat{\mathbf{G}}_i + \Delta\mathbf{G}_i, \forall i. \tag{67}$$

We employ the bounded CSI error model as

$$\|\Delta\mathbf{h}_{B,U_i}\| \leq \epsilon_{d,i}, \|\Delta\mathbf{G}_i\| \leq \epsilon_{r,i}, \forall i \tag{68}$$

where $\epsilon_{d,i}$ and $\epsilon_{r,i}$ denote the channel error bound. This CSI error model can effectively characterize the channel quantization error within an unknown bounded region.

Next, we re-consider the constraints (26b), (26c) and (26f) with channel errors taken into account. For the constraint (26b), we can reshape it as

$$\text{vec}^H(\mathbf{H}_i)\mathbf{B}_i \text{vec}(\mathbf{H}_i) + (2^{\varepsilon_i} - 1)\sigma_U^2 \geq 0, \forall i \tag{69}$$

where

$$\mathbf{B}_i = \left(\mathbf{A}_i^T \otimes \mathbf{E} \right), \tag{70}$$

$$\mathbf{A}_i = \mathbf{W}_i - (2^{\varepsilon_i} - 1) \left[\sum_{m=i+1}^I \mathbf{W}_m + \beta \left(\sum_{m=1}^{i-1} \mathbf{W}_m + \mathbf{S}_r \right) \right] \tag{71}$$

and

$$\begin{aligned}
\mathbf{H}_i &= \left[\begin{array}{c} \hat{\mathbf{G}}_i + \Delta\mathbf{G}_i \\ \hat{\mathbf{h}}_{B,U_i}^H + \Delta\mathbf{h}_{B,U_i}^H \end{array} \right] = \left[\begin{array}{c} \hat{\mathbf{G}}_i \\ \hat{\mathbf{h}}_{B,U_i}^H \end{array} \right] + \left[\begin{array}{c} \Delta\mathbf{G}_i \\ \Delta\mathbf{h}_{B,U_i}^H \end{array} \right] \\
&= \hat{\mathbf{H}}_i + \Delta\mathbf{H}_i
\end{aligned} \tag{72}$$

with

$$\begin{aligned}
\|\Delta\mathbf{H}_i\|_F &= \sqrt{\|\Delta\mathbf{h}_{B,U_i}\|_F^2 + \|\Delta\mathbf{G}_i\|_F^2} \\
&\leq \sqrt{(\epsilon_{d,i})^2 + (\epsilon_{r,i})^2} \triangleq \epsilon_i, \forall i.
\end{aligned} \tag{73}$$

Then, (69) can be rewritten as

$$\begin{aligned}
& (\hat{\mathbf{h}}_i + \Delta\mathbf{h}_i)^H \mathbf{B}_i (\hat{\mathbf{h}}_i + \Delta\mathbf{h}_i) + (2^{\varepsilon_i} - 1)\sigma_U^2 \\
&= \Delta\mathbf{h}_i^H \mathbf{B}_i \Delta\mathbf{h}_i + 2 \operatorname{Re} \left\{ \Delta\mathbf{h}_i^H \mathbf{B}_i \hat{\mathbf{h}}_i \right\} + \hat{\mathbf{h}}_i^H \mathbf{B}_i \hat{\mathbf{h}}_i \\
&\quad + (2^{\varepsilon_i} - 1)\sigma_U^2 \geq 0, \|\Delta\mathbf{h}_i\| \leq \epsilon_i, \forall i
\end{aligned} \tag{74}$$

where $\hat{\mathbf{h}}_i = \text{vec}(\hat{\mathbf{H}}_i)$ and $\Delta\mathbf{h}_i = \text{vec}(\Delta\mathbf{H}_i)$. However, constraint (74) is still intractable as it is a semi-infinite

inequality. Note that $\|\Delta \mathbf{h}_i\| \leq \epsilon_i$ is equivalent to $\Delta \mathbf{h}_i^H \mathbf{I} \Delta \mathbf{h}_i - \epsilon_i^2 \leq 0$. According to the S-procedure [21], constraint (74) can be rewritten as

$$\begin{bmatrix} c_i \mathbf{I} + \mathbf{B}_i & \mathbf{B}_i \hat{\mathbf{h}}_i \\ \hat{\mathbf{h}}_i^H \mathbf{B}_i & -c_i \epsilon_i + \hat{\mathbf{h}}_i^H \mathbf{B}_i \hat{\mathbf{h}}_i + (2^{\varepsilon_i} - 1) \sigma_U^2 \end{bmatrix} \succeq \mathbf{0} \quad (75)$$

where $c_i \geq 0$ is the auxiliary optimization variable.

Similarly, constraint (26c) can be rewritten as

$$\begin{bmatrix} d_i \mathbf{I} - \mathbf{C}_j & -\mathbf{C}_j \hat{\mathbf{h}}_i \\ -\hat{\mathbf{h}}_i^H \mathbf{C}_j & -d_i \epsilon_i - \hat{\mathbf{h}}_i^H \mathbf{C}_j \hat{\mathbf{h}}_i + (2^{\varepsilon_i - \varepsilon_{th}} - 1) \sigma_U^2 \end{bmatrix} \succeq \mathbf{0} \quad (76)$$

where

$$\mathbf{C}_j = \left[\mathbf{W}_j - (2^{\varepsilon_i - \varepsilon_{th}} - 1) \left(\sum_{m=j+1}^I \mathbf{W}_m \right) \right]^T \otimes \mathbf{E}, \forall i \neq j \quad (77)$$

and $d_i \geq 0$ is the auxiliary optimization variable.

Constraint (26f) can be rewritten as

$$\begin{bmatrix} e_i \mathbf{I} + \mathbf{D}_j & \mathbf{D}_j \hat{\mathbf{h}}_i \\ \hat{\mathbf{h}}_i^H \mathbf{D}_j & -e_i \epsilon_i + \hat{\mathbf{h}}_i^H \mathbf{D}_j \hat{\mathbf{h}}_i \end{bmatrix} \succeq \mathbf{0} \quad (78)$$

where

$$\mathbf{D}_j = \begin{cases} (\mathbf{S}_r - \mathbf{W}_j)^T \otimes \mathbf{E}, & j = 1, \\ (\mathbf{W}_j - \mathbf{W}_{j+1})^T \otimes \mathbf{E}, & \text{otherwise,} \end{cases} \quad (79)$$

and $e_i \geq 0$ is the auxiliary optimization variable.

Constraints (26b), (26c) and (26f) are now expressed as tractable linear matrix inequalities. Following a process similar to that in **Algorithm 1**, we alternately optimize matrices \mathbf{W}_i and \mathbf{E} while using penalty terms to enforce rank-one constraints. For brevity, detailed steps of the algorithm are omitted here.

VI. SIMULATION RESULTS

In this section, we provide numerical results to validate the secure transmission performance in the RIS-aided NOMA-ISAC system. Consider a three-dimensional coordinate as shown in Fig. 2, where a BS, two legitimate users U_1 and U_2 , and a RIS are located at $(5, 0, 10)$ m, $(8, 40, 0)$ m, $(3, 60, 0)$ m and $(0, 50, 6)$ m, respectively. The BS has $N = 8$ antennas and the RIS has $M = 30$ antennas. Assume that $K = 5$ external eavesdroppers are randomly distributed in a region centered at $(4, 40, 0)$ m with a radius of $R = 20$ meters. Three targets are at the azimuth angles of $\theta_1 = -40^\circ$, $\theta_2 = 0^\circ$ and $\theta_3 = 40^\circ$ with respect to the BS. The beam width for each target is $\Delta_\theta = 20^\circ$. We choose $S = 1801$ angles for θ_s which are uniformly sampled over $[-\pi/2, \pi/2]$ [30]. It is assumed that $\beta_0 = -30$ dB, $\alpha_{B,U_i} = \alpha_{B,E_k} = 3.6$, $\alpha_{B,R} = \alpha_{R,U_i} = \alpha_{R,E_k} = 2.2$, and $\kappa_{B,R} = \kappa_{R,U_i} = \kappa_{R,E_k} = 3$ dB [44]. The minimum communication rates of users U_1 and U_2 are $\varepsilon_1 = 4$ bps/Hz and $\varepsilon_2 = 5$ bps/Hz, respectively. The internal eavesdropping rate cannot exceed $\varepsilon_i - \varepsilon_{th}^i = 0.1$ bps/Hz. The SIC factor is $\beta = 0.1$. The beampattern error $\epsilon = 0.01$. The noise power is set to $\sigma_U^2 = \sigma_E^2 = -110$ dBm [25], [38], [44].

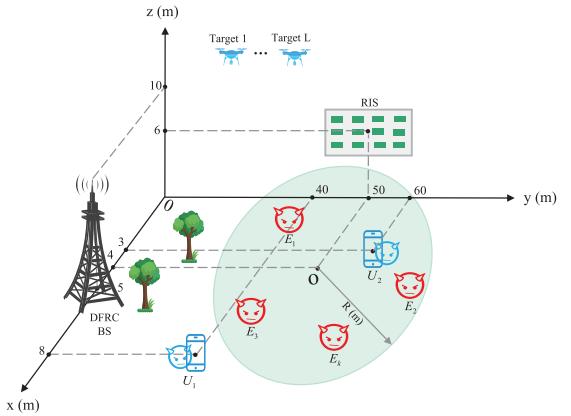


Fig. 2. Simulation setup for the proposed system.

The channel error bounds are $\epsilon_{d,i} = \alpha \|\hat{\mathbf{h}}_{B,U_i}\|$ and $\epsilon_{r,i} = \alpha \|\hat{\mathbf{G}}_i\|$.

Moreover, the initial penalty factor is set to $\rho_1 = \rho_2 = 10$ with $\tau = 1.5$.

The secrecy rate is used as the indicator of security performance [25], [26], [38], [39], [40]. With the influence of the internal and external eavesdroppers, the secrecy rate of U_j is given by

$$R_s^j = \left[R_{U_j}^{U_j} - \max_{\forall i, k, i \neq j} \{ R_{U_i}^{U_j}, R_{E_k}^{U_j} \} \right]^+ \quad (80)$$

where $[x]^+ \triangleq \max(x, 0)$.

To show the superiority of the proposed approach, we consider the following approaches for comparisons.

- **Proposed:** This is our proposed approach described in Algorithm 1 in Section IV.
- **Comm-only:** This approach only takes into account communication functionality within the system to evaluate the impact of integrating radar sensing capabilities on communication performance.
- **Radar-only:** This approach only takes into account radar sensing functionality within the system to evaluate the impact of integrating communication capabilities on radar sensing performance.
- **ARIS:** Similar to [45], this approach considers the deployment of active RIS within the system.
- **W/o RIS:** This approach considers the system without the deployment of RIS to assess the impact of RIS deployment on system performance.
- **W/o NOMA:** This approach considers the system without the implementation of NOMA technique to evaluate its impact on system performance.
- **JPM:** The scenario considered in this approach aligns with that of reference [39].
- **Collusion:** Similar to [49], this approach considers external eavesdroppers to be colluding with each other to assess the impact of different levels of eavesdropping on system performance. The secrecy rate of U_j is recalculated as

$$\widetilde{R}_s^j = \left[R_{U_j}^{U_j} - \max_{\forall i, k, i \neq j} \left\{ R_{U_i}^{U_j}, \sum_{k=1}^K R_{E_k}^{U_j} \right\} \right]^+ \quad (81)$$

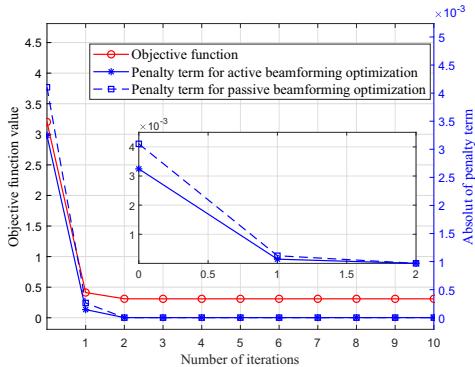


Fig. 3. Convergence of the proposed algorithm when $p_{\max} = 15\text{dBm}$, $M = 30$, $K = 5$, $R = 20$ and $\epsilon = 0.01$.

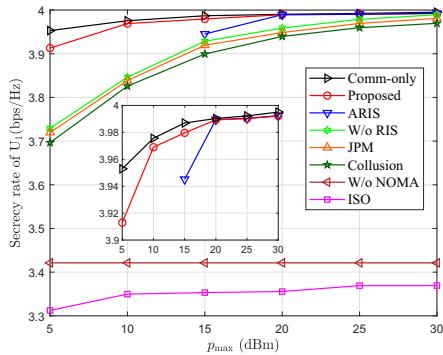


Fig. 4. Secrecy rate of legitimate communication user U_1 versus the BS maximum transmission power threshold p_{\max} when $M = 30$, $K = 5$, $R = 20$ and $\epsilon = 0.01$.

- **ISO:** Similar to [18] and [19], in this approach, we set $S_r = \frac{p_{\max}}{2} \frac{\mathcal{P}_G^\perp}{\|\mathcal{P}_G^\perp\|_F^2}$, where $\mathcal{P}_G^\perp = \mathbf{I} - \mathbf{G}(\mathbf{G}^H \mathbf{G})^{-1} \mathbf{G}^H$ and $\mathbf{G} \in \mathbb{C}^{N \times I}$ contains all the communication user effective channel vectors $\{\mathbf{g}_{U_i}\}_{i=1}^I$ stacked in the columns of \mathbf{G} . This design ensures that communication users are not disturbed by the AN signal. Then, the remaining available power for eigen-beamforming, i.e., $\mathbf{w}_i = \frac{\sqrt{p_{\max}} \mathbf{g}_{U_i}}{\sqrt{2I} \|\mathbf{g}_{U_i}\|}$. Finally, the phase-shifting matrix of the RIS is set randomly.

Fig. 3 illustrates the convergence behavior of the proposed algorithm, showing the objective function and penalty term versus the number of iterations. It can be seen that the proposed algorithm can converge within a few iterations, leading to the low complexity of the proposed algorithm. Meanwhile, we can see from Fig. 3 that the absolute values of the penalty terms for sub-problem (45) and (61) close to zero after several iterations, which implies that the proposed algorithm achieves almost rank-one solution of \mathbf{W}_i and \mathbf{E} .

Fig. 4 and Fig. 5 show the secrecy rates of U_1 and U_2 , respectively, for different transmit power p_{\max} of the BS. It can be seen from Figs. 4 and 5 that the performance gap between the proposed scheme and comm-only scheme is small, which implies that the proposed scheme integrates radar sensing functionality at the cost of a small loss in secrecy rate. As active RIS consumes additional biasing power, ARIS cannot achieve secure communications with small p_{\max} . Moreover,

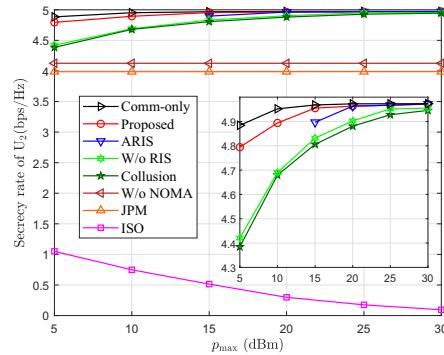


Fig. 5. Secrecy rate of legitimate communication user U_2 versus the BS maximum transmission power threshold p_{\max} when $M = 30$, $K = 5$, $R = 20$ and $\epsilon = 0.01$.

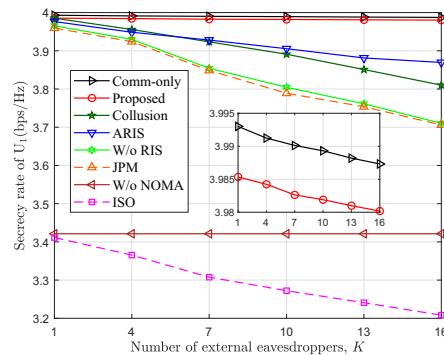


Fig. 6. Secrecy rate of legitimate communication user U_1 versus number of external eavesdroppers K when $p_{\max} = 15\text{ dBm}$, $M = 30$, $R = 30$ and $\epsilon = 0.01$.

compared to the W/o RIS scheme, the proposed scheme with a RIS delivers significant performance improvement, implying the necessity of employing a RIS in security NOMA-ISAC systems. Furthermore, we can see that the proposed scheme has a much higher secrecy rate of U_1 than JPM when p_{\max} is small, while significantly outperforms JPM for U_2 with all p_{\max} . Due to the cooperation among external eavesdroppers, the secrecy rate achieved by the collusion scheme is much lower than that of the proposed scheme when p_{\max} is small. However, when p_{\max} is large, the secrecy rate of the collusion scheme approaches the communication rate, indicating that the AN effectively counteracts the collusion eavesdropping by external eavesdroppers. Additionally, for the W/o NOMA scheme, the system's secrecy rate remains unchanged with varying p_{\max} and is significantly lower than the proposed scheme. This is mainly because the internal eavesdropping rate exceeds the external eavesdropping rate. It also highlights the necessity of introducing NOMA technique into the system. Finally, ISO focuses on only the orthogonality of the transmitted communication and radar signals, and its secrecy rate is far below the other schemes. For U_2 , the secrecy rate of ISO scheme decreases with transmit power, as the increase in eavesdropping rate outweighs the increase in communication rate.

Fig. 6 and Fig. 7 show the performance of secrecy rates of U_1 and U_2 respectively with different number of external eavesdroppers, analyzing the impact of different levels of

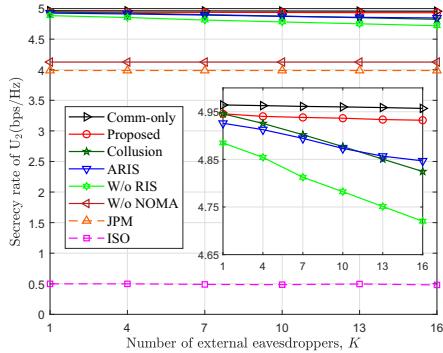


Fig. 7. Secrecy rate of legitimate communication user U_2 versus number of external eavesdroppers K when $p_{\max} = 15$ dBm, $M = 30$, $R = 30$ and $\epsilon = 0.01$.

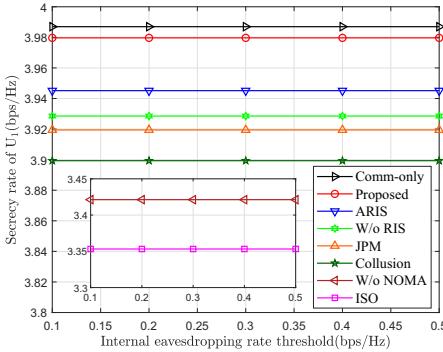


Fig. 8. Secrecy rate of legitimate communication user U_1 versus internal eavesdropping rate threshold when $p_{\max} = 15$ dBm, $M = 30$, $K = 5$, $R = 20$ and $\epsilon = 0.01$.

external eavesdropping on the system's secrecy rate. It can be observed from Fig. 6 and Fig. 7 that the proposed scheme with RIS achieves a stable secrecy rate close to the commonly scheme for U_1 and U_2 even when the number of eavesdroppers is large. This is because the power of AN is large enough to deal with external eavesdropping and the internal eavesdropping rate is limited in the proposed scheme. As for U_1 and U_2 , the secrecy rate of the W/o RIS, collusion, ARIS, JPM and ISO schemes decrease with K due to the higher external eavesdropping rate. Moreover, under the W/o NOMA scheme, the secrecy rates of U_1 and U_2 are respectively stabilized around 3.41 bps/Hz and 4.15 bps/Hz. This phenomenon is primarily due to the fact that the impact of internal eavesdropping outweighs that of external eavesdropping. As for U_2 , JPM keeps the secrecy rate at about 4.0 bps/Hz for any K , also due to the impact of internal eavesdropping plays a dominant role. The achievable secrecy rate of ISO is only 0.5 bps/Hz.

Fig. 8 and Fig. 9 show the performance of secrecy rates of U_1 and U_2 respectively with different internal eavesdropping rate thresholds. As can be seen from Fig. 8, the secrecy rate of the comm-only, proposed, ARIS, W/o RIS and collusion schemes for U_1 do not change with the variation of the internal eavesdropping rate threshold. This is because, as a weak user, U_1 can ensure the security of its internal communication by itself according to the order of SIC. The constant secrecy rate of the W/o NOMA scheme is due to the fact that once

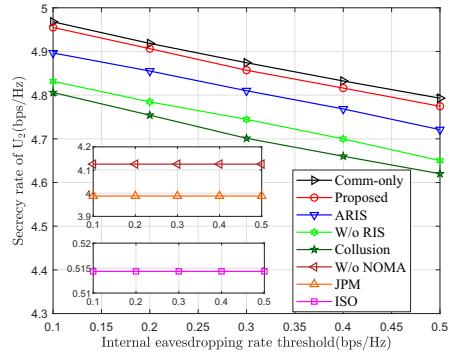


Fig. 9. Secrecy rate of legitimate communication user U_2 versus internal eavesdropping rate threshold when $p_{\max} = 15$ dBm, $M = 30$, $K = 5$, $R = 20$ and $\epsilon = 0.01$.

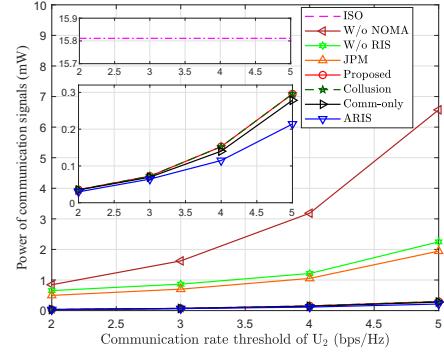


Fig. 10. The power of communication signals (i.e., the value of the objective function for problem (29)) versus U_2 's communication rate threshold ϵ_2 when $p_{\max} = 15$ dBm, $M = 30$, $K = 5$, $R = 20$ and $\epsilon = 0.01$.

the system departs from NOMA technique, U_1 is unable to ensure internal security. The secrecy rates of the JPM and ISO schemes remain unchanged because these schemes do not account for internal eavesdropping. As can be seen from Fig. 9, for U_2 , the secrecy rate of the comm-only, proposed, ARIS, W/o RIS and collusion schemes gradually decreases with the increase of the internal eavesdropping rate threshold. This is mainly due to the relaxation of the internal secure communication constraints. Additionally, the reason for the constant secrecy rate under the W/o NOMA, JPM and ISO schemes is the same as that for U_1 .

Fig. 10 investigates the total power of communication signals versus communication rate threshold of U_2 . Fig. 10 shows that, compared with the other schemes, ISO allocates the largest amount of power (half of the total power) to communication signals, leading to low power of AN and thus lower secrecy rates as shown in previous numerical results. Both the proposed scheme and the collusion scheme allocate the same lower power to communication signals, while a large amount of power is allocated to AN to counteract external eavesdropping. Without the assistance of NOMA and RIS, more power is required for communication signals to satisfy communication rate and internal eavesdropping secrecy rate constraints. This demonstrates the necessity of employing NOMA and RIS technologies in our proposed scheme. It can be seen that ARIS allocates lower power to the communication signals than that of the proposed scheme,

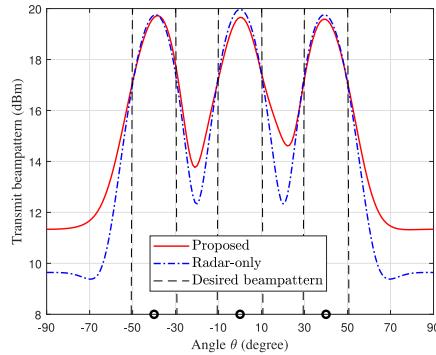


Fig. 11. Transmit beampattern at BS when $p_{\max} = 20\text{dBm}$, $M = 30$, $K = 5$, $R = 20$ and $\epsilon = 0.01$. The targets angles are -40° , 0° and 40° .

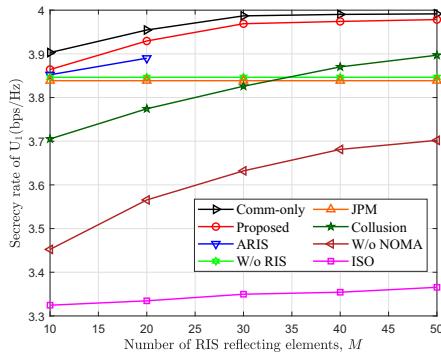


Fig. 12. Secrecy rates of legitimate communication user U_1 versus the number of RIS reflecting elements M when $p_{\max} = 10\text{ dBm}$, $K = 5$, $R = 20$ and $\epsilon = 0.01$.

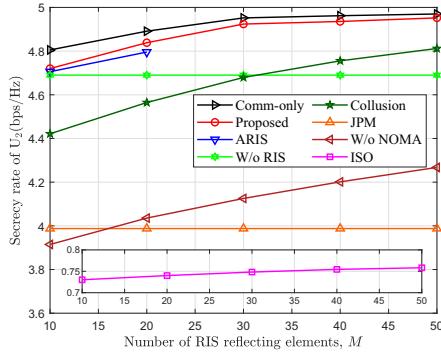


Fig. 13. Secrecy rates of legitimate communication user U_2 versus the number of RIS reflecting elements M when $p_{\max} = 10\text{ dBm}$, $K = 5$, $R = 20$ and $\epsilon = 0.01$.

however, it requires extra consumption of DC biasing power and signal amplification power, and its active RIS requires higher hardware complexity than passive RIS.

Fig. 11 shows the transmit beampattern of the DFRC BS when $p_{\max} = 20\text{dBm}$. The beampattern of the radar-only scheme is also presented as a benchmark. It can be seen from Fig. 11 that the proposed scheme achieves almost the similar beampattern as the radar-only scheme. This implies that, besides having security communications, the proposed scheme has the similar sensing performance as the radar-only scheme.

Fig. 12 and Fig. 13 show the performance of secrecy rates of U_1 and U_2 respectively with different number of RIS

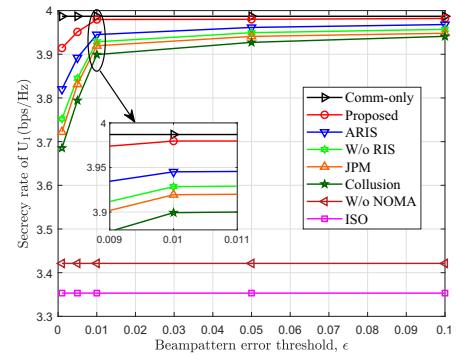


Fig. 14. Secrecy rates of legitimate communication user U_1 versus the beampattern error threshold ϵ when $p_{\max} = 15\text{ dBm}$, $M = 30$, $K = 5$ and $R = 20$.

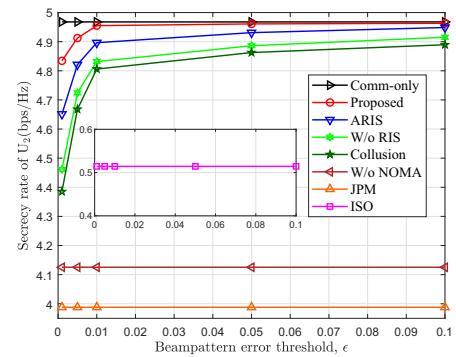


Fig. 15. Secrecy rates of legitimate communication user U versus the beampattern error threshold ϵ when $p_{\max} = 15\text{ dBm}$, $M = 30$, $K = 5$ and $R = 20$.

reflecting elements. As can be seen from the Fig. 12 and Fig. 13, with the increase in the number of RIS reflecting elements, the secrecy rates of U_1 and U_2 under the comm-only, proposed, ARIS, collusion and W/o NOMA schemes increase. It is worth mentioning that when the number of RIS reflecting elements reaches 30, the secrecy rate achieved by the proposed scheme is very close to the ideal secrecy rate, indicating that the proper selection of the number of RIS reflecting elements can maximize the gain while ensuring hardware cost. Additionally, when the number of active RIS reflecting elements exceeds 20, the total power budget of the system is insufficient to support the operation of the active RIS, resulting in the inability of the ARIS scheme to achieve secure communication. Meanwhile, the secrecy rates of the W/o RIS and JPM schemes do not change with the variation in the number of RIS reflecting elements, as these schemes do not deploy RIS. Finally, for U_1 and U_2 , the secrecy rate of the ISO scheme slightly increases with the increase in the number of RIS reflecting elements, as this scheme employs a random RIS phase strategy.

Fig. 14 and Fig. 15 show the performance of secrecy rates of U_1 and U_2 respectively with different beampattern error thresholds. It can be observed from Fig. 14 and Fig. 15 that, the secrecy rates of the proposed, ARIS, W/o RIS, and collusion schemes improve as the beampattern error threshold increases. This is because a larger beampattern error threshold implies relaxed constraints on radar sensing,

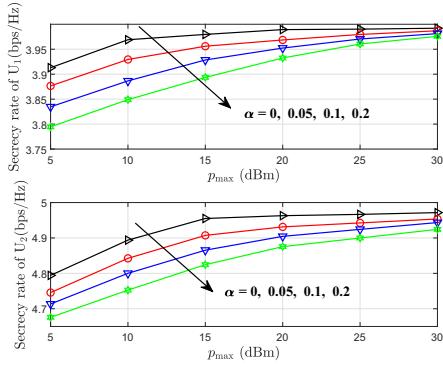


Fig. 16. The secrecy rate of the proposed scheme under different channel error bounds when $M = 30$, $K = 5$, $R = 20$ and $\epsilon = 0.01$.

allowing the system to allocate more resources to secure communication. This phenomenon indicates a performance trade-off between communication and sensing functionalities in the system. Additionally, the secrecy rate of the communication-only scheme remains unchanged, as it does not incorporate sensing functionality. Finally, the secrecy rates for U_1 under the W/o NOMA and ISO schemes, as well as for U_2 under the W/o NOMA, JPM, and ISO schemes, remain unaffected by variations in the beampattern error threshold. This is primarily due to the dominant impact of internal eavesdropping on these scenarios.

Fig. 16 shows the secrecy rate of the proposed scheme under different channel error bounds. As can be seen from Fig. 16, the secrecy rates of users U_1 and U_2 exhibit slight performance degradation as the channel error bound increases. The reason for this is that as the channel estimation error grows, the system allocates more power to legitimate communications, which correspondingly reduces the power allocated to AN signals for counteracting external eavesdropping. Notably, even with a channel error of 20% ($\alpha=0.2$), the security performance loss remains less than 3%, demonstrating that the proposed scheme exhibits excellent robustness.

VII. CONCLUSION AND FUTURE WORK

In this paper, we have investigated the secure beamforming and power allocation problem in RIS-assisted NOMA-ISAC systems. Different from existing secure ISAC, this work deals with the coexistence of both internal and external eavesdroppers in secure ISAC, where legitimate users are potential internal eavesdroppers and the channel state information of external eavesdroppers is unavailable. To handle both internal and external eavesdroppers, we employ RIS to form destructive interference for internal eavesdroppers. Additionally, we combine RIS and NOMA to counteract external eavesdroppers. In formulating the optimization problem, we have proposed a channel selection scheme to destruct partial channels of internal eavesdroppers, according to the decoding order of NOMA signals. Further, to deal with the non-convexity of the formulated problem, we have proposed a semidefinite relaxation based alternating optimization algorithm together with a penalty iteration method, and analyzed the convergence and the computational complexity of the proposed algorithm.

Moreover, we have extended the algorithm to the general case of imperfect CSI and proposed a robust beamforming scheme. Numerical results demonstrate that the proposed RIS-assisted NOMA-ISAC scheme achieves performance close to the communication-only scheme, and significantly outperforms other schemes.

In this work, both the radar and communication signals are used to illuminate the targets, and only the radar sensing beampattern has been considered. In some scenarios, the targets may act as eavesdroppers, and we can illuminate only radar signals on the targets for secure communications. In this case, both the sensing beampattern and signal-to-noise ratio of target echoes should be considered in beamforming and power allocation of radar and communication signals. This poses another challenging issue on the secure ISAC and will be addressed in our future work.

APPENDIX

DETAILS OF SQUARED MODULUS TERM TRANSFORMATION

For the sake of brevity, we illustrate with the numerator term in (16) as an example.

$$|\mathbf{g}_{\mathbf{U}_i}^H \mathbf{w}_j|^2 \stackrel{(a)}{=} \mathbf{g}_{\mathbf{U}_i}^H \mathbf{w}_j \mathbf{w}_j^H \mathbf{g}_{\mathbf{U}_i} \quad (82a)$$

$$\stackrel{(b)}{=} \mathbf{e}^H \mathbf{H}_i \mathbf{w}_j \mathbf{w}_j^H \mathbf{H}_i^H \mathbf{e} \quad (82b)$$

$$\stackrel{(c)}{=} \text{Tr}(\mathbf{e} \mathbf{e}^H \mathbf{H}_i \mathbf{w}_j \mathbf{w}_j^H \mathbf{H}_i^H) \quad (82c)$$

$$= \text{Tr}(\mathbf{E} \mathbf{G}_{i,j}) \quad (82d)$$

where equality (a) represents the modulus squared operation of a complex number, equality (b) represents the substitution of vectors, and equality (c) represents the trace operation of a matrix.

REFERENCES

- [1] F. Liu et al., "Integrated sensing and communications: Towards dual-functional wireless networks for 6G and beyond," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1728–1767, Jun. 2022.
- [2] F. Liu, C. Masouros, A. P. Petropulu, H. Griffiths, and L. Hanzo, "Joint radar and communication design: Applications, state-of-the-art, and the road ahead," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3834–3862, Jun. 2020.
- [3] Z. Wei et al., "Integrated sensing and communication signals toward 5G-A and 6G: A survey," *IEEE Internet Things J.*, vol. 10, no. 13, pp. 11068–11092, Jul. 2023.
- [4] J. Yao, L. Mai, and Q. Zhang, "Approximate capacity-distortion region of joint state sensing and communication in MIMO real gaussian channels," *IEEE Trans. Commun.*, vol. 72, no. 5, pp. 2625–2638, May 2024.
- [5] Z. Wei, R. Yao, X. Yuan, H. Wu, Q. Zhang, and Z. Feng, "Precoding optimization for MIMO-OFDM integrated sensing and communication systems," *IEEE Trans. Cogn. Commun.*, vol. 11, no. 1, pp. 288–299, Feb. 2025.
- [6] Y. Liu et al., "Evolution of NOMA toward next generation multiple access (NGMA) for 6G," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 4, pp. 1037–1071, Apr. 2022.
- [7] A. Ahmed, W. Xingfu, A. Hawbani, W. Yuan, H. Tabassum, and Y. Liu, "Unveiling the potential of NOMA: A journey to next generation multiple access," *IEEE Commun. Surveys Tuts.*, early access, Dec. 25, 2024, doi: [10.1109/COMST.2024.3521647](https://doi.org/10.1109/COMST.2024.3521647).
- [8] C. Pan et al., "An overview of signal processing techniques for RIS/IRS-aided wireless systems," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 5, pp. 883–917, Aug. 2022.

- [9] Y. Liu et al., "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1546–1577, 3rd Quart., 2021.
- [10] N. Huang, C. Dou, Y. Wu, L. Qian, S. Zhou, and R. Lu, "Image analysis oriented integrated sensing and communication via intelligent reflecting surface," *IEEE Trans. Cogn. Commun.*, vol. 11, no. 1, pp. 274–287, Feb. 2025.
- [11] T. Wu et al., "Exploit high-dimensional RIS information to localization: What is the impact of faulty element?" *IEEE J. Sel. Areas Commun.*, vol. 42, no. 10, pp. 2803–2819, Oct. 2024.
- [12] Q. Zhang et al., "Robust beamforming design for RIS-aided NOMA secure networks with transceiver hardware impairments," *IEEE Trans. Commun.*, vol. 71, no. 6, pp. 3637–3649, Jun. 2023.
- [13] Z. Wang, Y. Liu, X. Mu, Z. Ding, and O. A. Dobre, "NOMA empowered integrated sensing and communication," *IEEE Commun. Lett.*, vol. 26, no. 3, pp. 677–681, Mar. 2022.
- [14] C. Dou, N. Huang, Y. Wu, L. Qian, and T. Q. S. Quek, "Sensing-efficient NOMA-aided integrated sensing and communication: A joint sensing scheduling and beamforming optimization," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13591–13603, Oct. 2023.
- [15] J. Zuo, Y. Liu, C. Zhu, Y. Zou, D. Zhang, and N. Al-Dhahir, "Exploiting NOMA and RIS in integrated sensing and communication," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 12941–12955, Oct. 2023.
- [16] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700–6705, Jul. 2018.
- [17] 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. 2021.
- [18] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
- [19] A. Bazzi and M. Chafii, "Secure full duplex integrated sensing and communications," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 2082–2097, 2024.
- [20] K. Hou and S. Zhang, "Optimal beamforming for secure integrated sensing and communication exploiting target location distribution," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 11, pp. 3125–3139, Nov. 2024.
- [21] Z. Ren, L. Qiu, J. Xu, and D. W. K. Ng, "Robust transmit beamforming for secure integrated sensing and communication," *IEEE Trans. Commun.*, vol. 71, no. 9, pp. 5549–5564, Sep. 2023.
- [22] X. Zhang, W. Jiao, W. Liu, and C. Qi, "Energy efficiency optimization in secure full-duplex ISAC systems," *IEEE Commun. Lett.*, vol. 29, no. 1, pp. 220–224, Jan. 2025.
- [23] Z. Xie, R. Li, Y. Gu, Z. Jiang, J. Zhu, and P. Chen, "Joint beamforming and power allocation strategy for NOMA empowered ISAC systems," *IEEE Trans. Veh. Technol.*, vol. 74, no. 2, pp. 3445–3450, Feb. 2025.
- [24] A. Nasser, A. Celik, and A. M. Eltawil, "Joint user-target pairing, power control, and beamforming for NOMA-aided ISAC networks," *IEEE Trans. Cogn. Commun.*, vol. 11, no. 1, pp. 316–332, Feb. 2025.
- [25] Z. Yang, D. Li, N. Zhao, Z. Wu, Y. Li, and D. Niyato, "Secure precoding optimization for NOMA-aided integrated sensing and communication," *IEEE Trans. Commun.*, vol. 70, no. 12, pp. 8370–8382, Dec. 2022.
- [26] Y. Liu, M. Jin, Q. Guo, and J. Yao, "Secure beamforming for NOMA-ISAC with system imperfections," *IEEE Commun. Lett.*, vol. 28, no. 7, pp. 1559–1563, Jul. 2024.
- [27] H. Zhang, M. Jin, Q. Guo, and J. Yao, "Secure beamforming for NOMA-ISAC with multicast and unicast communications," *IEEE Wireless Commun. Lett.*, vol. 13, no. 10, pp. 2927–2931, Oct. 2024.
- [28] C. Jiang, C. Zhang, C. Huang, J. Ge, M. Debbah, and C. Yuen, "Exploiting RIS in secure beamforming design for NOMA-assisted integrated sensing and communication," *IEEE Internet Things J.*, vol. 11, no. 17, pp. 28123–28136, Sep. 2024.
- [29] J. Ye, J. Dai, C. Pan, K. Wang, and J. Li, "Joint active and passive beamforming design for secure RIS-aided ISAC system," *IEEE Wireless Commun. Lett.*, vol. 14, no. 3, pp. 916–920, Mar. 2025, doi: [10.1109/LWC.2025.3528080](https://doi.org/10.1109/LWC.2025.3528080).
- [30] Q. Liu, Y. Zhu, M. Li, R. Liu, Y. Liu, and Z. Lu, "DRL-based secrecy rate optimization for RIS-assisted secure ISAC systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 16871–16875, Dec. 2023.
- [31] T.-X. Zheng, X. Chen, L. Lan, Y. Ju, X. Hu, and R. Liu, "Reconfigurable intelligent surface-aided secure integrated radar and communication systems," *IEEE Trans. Wireless Commun.*, vol. 24, no. 3, pp. 1934–1948, Mar. 2025, doi: [10.1109/TWC.2024.3514663](https://doi.org/10.1109/TWC.2024.3514663).
- [32] C. Jiang, C. Zhang, C. Huang, J. Ge, D. Niyato, and C. Yuen, "RIS-assisted ISAC systems for robust secure transmission with imperfect sense estimation," *IEEE Trans. Wireless Commun.*, vol. 24, no. 5, pp. 3979–3992, May 2025, doi: [10.1109/TWC.2025.3534439](https://doi.org/10.1109/TWC.2025.3534439).
- [33] K. Zhi, C. Pan, H. Ren, K. K. Chai, and M. Elkashlan, "Active RIS versus passive RIS: Which is superior with the same power budget?" *IEEE Commun. Lett.*, vol. 26, no. 5, pp. 1150–1154, May 2022.
- [34] Z. Yu et al., "Active RIS-aided ISAC systems: Beamforming design and performance analysis," *IEEE Trans. Commun.*, vol. 72, no. 3, pp. 1578–1595, Mar. 2024.
- [35] C. Gong, H. Li, S. Hao, K. Long, and X. Dai, "Active RIS enabled secure NOMA communications with discrete phase shifting," *IEEE Trans. Wireless Commun.*, vol. 23, no. 4, pp. 3493–3506, Apr. 2024.
- [36] A. A. Salem, M. H. Ismail, and A. S. Ibrahim, "Active reconfigurable intelligent surface-assisted MISO integrated sensing and communication systems for secure operation," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 4919–4931, Apr. 2023.
- [37] R. Ma, Y. Peng, R. Ye, M. Yue, F. Al-Hazemi, and J. Lee, "Active RIS-assisted secure communications against simultaneous jamming and eavesdropping," *IEEE Wireless Commun. Lett.*, vol. 14, no. 3, pp. 686–690, Mar. 2025, doi: [10.1109/LWC.2024.3520355](https://doi.org/10.1109/LWC.2024.3520355).
- [38] D. Luo, Z. Ye, and J. Zhu, "Secure transmit beamforming for radar-communication systems using NOMA," *IEEE Commun. Lett.*, vol. 26, no. 11, pp. 2557–2561, Nov. 2022.
- [39] D. Luo, Z. Ye, B. Si, and J. Zhu, "Secure transmit beamforming for radar-communication system without eavesdropper CSI," *IEEE Trans. Veh. Technol.*, vol. 71, no. 9, pp. 9794–9804, Sep. 2022.
- [40] J. Chu, R. Liu, M. Li, Y. Liu, and Q. Liu, "Joint secure transmit beamforming designs for integrated sensing and communication systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 4778–4791, Apr. 2023.
- [41] 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, Nov. 2023.
- [42] H. Han et al., "Secure transmission for STAR-RIS aided NOMA against internal eavesdropping," *IEEE Trans. Veh. Technol.*, vol. 72, no. 11, pp. 15068–15073, Nov. 2023.
- [43] K. Cao, B. Wang, H. Ding, T. Li, J. Tian, and F. Gong, "Secure transmission designs for NOMA systems against internal and external eavesdropping," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2930–2943, 2020.
- [44] H. Han, Y. Cao, M. Sheng, N. Zhao, J. Liu, and D. Niyato, "IRS-aided secure NOMA networks against internal and external eavesdropping," *IEEE Trans. Commun.*, vol. 70, no. 11, pp. 7536–7548, Nov. 2022.
- [45] X. Li, Y. Pei, X. Yue, Y. Liu, and Z. Ding, "Secure communication of active RIS assisted NOMA networks," *IEEE Trans. Wireless Commun.*, vol. 23, no. 5, pp. 4489–4503, May 2024.
- [46] L. Wei et al., "Joint channel estimation and signal recovery for RIS-empowered multiuser communications," *IEEE Trans. Commun.*, vol. 70, no. 7, pp. 4640–4655, Jun. 2022.
- [47] X. Guan, Q. Wu, and R. Zhang, "Anchor-assisted channel estimation for intelligent reflecting surface aided multiuser communication," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 3764–3778, Jun. 2022.
- [48] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.
- [49] K. Tang, Z. Wang, B. Zheng, W. Feng, W. Che, and Q. Xue, "RSMA-enhanced secure transmission in IRS-assisted networks against internal and external eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 13, no. 12, pp. 3310–3314, Dec. 2024.



Yaming Li received the B.E. degree in optoelectronic information science and engineering from Huangshan University, Huangshan, Anhui, in 2022. He is currently pursuing the M.S. degree with the School of Information Science and Engineering, Ningbo University, Ningbo, Zhejiang. His research interests include integrated sensing and communication, physical layer security, and reconfigurable intelligent surfaces.



Ming Jin (Senior Member, IEEE) received the B.E. degree in electronic engineering and the M.E. degree in signal and information processing from Xidian University, Xi'an, China, in 2005 and 2010, respectively. From 2013 to 2014, he was an Associate Researcher with the School of Electrical, Computer and Telecommunications Engineering, University of Wollongong, Wollongong, NSW, Australia. He is currently a Professor with the Faculty of Electrical Engineering and Computer Science, Ningbo University, Ningbo, China. His research interests include cognitive radio, localization, DOA estimation, and UAV detection.



Tao Jiang received the B.E. degree in telecommunications engineering from Wenzhou University, Zhejiang, China, in 2020, and the M.S. degree in information and communication engineering from Ningbo University, Ningbo, China, where he is currently pursuing the Ph.D. degree. His research interests include Integrated communication and sensing, and power allocation.



Qinghua Guo (Senior Member, IEEE) received the B.E. degree in electronic engineering and the M.E. degree in signal and information processing from Xidian University in 2001 and 2004, respectively, and the Ph.D. degree in electronic engineering from the City University of Hong Kong in 2008. He is currently an Associate Professor with the School of Electrical, Computer and Telecommunications Engineering, University of Wollongong, Wollongong, NSW, Australia, and an Adjunct Associate Professor with the School of Engineering, The University of Western Australia, Perth, WA, Australia. His research interests include signal processing, telecommunications, radar, machine learning for signal processing, and optical sensing. He was a recipient of the Australian Research Council's Inaugural Discovery Early Career Researcher Award in 2012. He serves as an Associate Editor for IEEE TRANSACTIONS ON SIGNAL PROCESSING and IEEE WIRELESS COMMUNICATIONS LETTERS.



Junteng Yao received the B.Eng. and M.S. degrees in electronic engineering from Ningbo University, Ningbo, China, in 2016 and 2019, respectively, and the Ph.D. degree in information and communication engineering from Sun Yat-sen University, Guangzhou, China, in 2023. He is currently a Lecturer with the Faculty of Electrical Engineering and Computer Science, Ningbo University. His research interests include fluid antenna system, integrated sensing and communication, and reconfigurable intelligent surface.



Juan Liu (Member, IEEE) received the B.S. degree in information and electronic engineering from Zhejiang University, Hangzhou, China, in 2000, the M.S. degree in information engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2005, and the Ph.D. degree in electronic engineering from Tsinghua University, Beijing, in 2011.

From March 2012 to June 2014, she was with the ECE Department, NC State University, Raleigh, NC, USA. From February 2015 to February 2016, she was with the ECE Department, Hong Kong University of Science and Technology, Hong Kong. Since March 2016, she has been with the College of Information Science and Engineering, Ningbo University, Ningbo, China, where she is a Professor. She is currently focusing on a wide range of research topics, such as wireless communications and networking, UAV communications, and deep learning for wireless communications.