sensors

MDPI

Article

Joint Active and Passive Beamforming in RIS-Assisted Secure ISAC Systems

Jinsong Chen [1], Kai Wu [2,*], Jinping Niu [1] and Yanyan Li [1]

[1] School of Information Science and Technology, Northwest University, Xi'an 710127, China; 202121822@stumail.nwu.edu.cn (J.C.); jinpingniu@nwu.edu.cn (J.N.); liyanyan@nwu.edu.cn (Y.L.)
[2] Global Big Data Technologies Centre (GBDTC), University of Technology Sydney, Sydney, NSW 2122, Australia
* Correspondence: kai.wu@uts.edu.au

Abstract: This paper investigates joint beamforming in a secure integrated sensing and communications (ISAC) system assisted by reconfigurable intelligent surfaces (RIS). The system communicates with legitimate downlink users, detecting a potential target, which is a potential eavesdropper attempting to intercept the downlink communication information from the base station (BS) to legitimate users. To enhance the physical-layer secrecy of the system, we design and introduce interference signals at the BS to disrupt eavesdroppers' attempts to intercept legitimate communication information. The BS simultaneously transmits communication and interference signals, both utilized for communication and sensing to guarantee the sensing and communication quality. By jointly optimizing the BS active beamformer and the RIS passive beamforming matrix, we aim to maximize the achievable secrecy rate and radiation power of the system. We develop an effective scheme to find the active beamforming matrix through fractional programming (FP) and semi-definite programming (SDP) techniques and obtain the RIS phase shift matrix via a local search technique. Simulation results validate the effectiveness of the proposed methods in enhancing communication and sensing performance. Additionally, the results demonstrate the effectiveness of introducing the interference signals and RIS in enhancing the physical-layer secrecy of the ISAC system.

Keywords: reconfigurable intelligent surfaces (RIS); integrated sensing and communications (ISAC); physical-layer secrecy

Citation: Chen, J.; Wu, K.; Niu, J.; Li, Y. Joint Active and Passive Beamforming in RIS-Assisted Secure ISAC Systems. *Sensors* **2024**, *24*, 289. https://doi.org/ 10.3390/s24010289

Academic Editors: Agnese Mazzinghi and Federico Puggelli

Received: 4 December 2023
Revised: 20 December 2023
Accepted: 26 December 2023
Published: 3 January 2024

1. Introduction

With the explosive growth of wireless devices, spectrum and energy resources have become a valuable asset. The scarcity of these resources has promoted the development of more efficient technologies. Integrated sensing and communications (ISAC) is a promising technology to substantially enhance the spectral and energy efficiency of numerous next-generation wireless systems [1,2]. Due to their unique integration and coordination advantages, ISAC systems have attracted widespread interest in various fields [3], such as vehicle networks, unmanned aerial vehicle sensing, and communication and localization sensing, etc. In ISAC systems, many efforts have been devoted to designing ISAC waveforms to achieve the simultaneous support of target detection and communications through simultaneous sensing and communications [4–7]. A main focus has been on transmitting designs for enhancing the communication performances of legitimate users, with limited attention to the presence of potential eavesdroppers in the environment.

From the perspective of typical radar systems, the power of the sensing signal can be concentrated in the direction of targets of interest to ensure high detection performance. For the ISAC system, the transmitting signal encompasses not only sensing information but also communication information. Therefore, the communication information is susceptible to being intercepted by potential sensing targets, and these sensing targets are likely to be potential eavesdroppers, introducing potential security risks into the ISAC system. To tackle

the security issues in the ISAC system, potential eavesdroppers can be regarded as radar targets [8]. While preventing eavesdropping on legitimate information, it is also essential to ensure the system maintains optimal sensing performance. However, the challenge lies in achieving a balance between suppressing eavesdropping and ensuring satisfactory sensing performance. The pursuit of robust sensing performance may inadvertently lead to sub-optimal communication performance for legitimate users in the ISAC system.

Various schemes have been proposed to address the security issue and maximize the communication security rate, such as artificial noise interference and multi-antenna beamforming [9–15], etc. In [12], the security of ISAC was investigated, aiming to maximize the signal-to-interference-plus-noise ratio (SINR) of the radar while ensuring the achievement of secure rates for legitimate users. The authors in [13] proposed an auxiliary method for Artificial Noise (AN) deployment in an ISAC system. This approach involves the base station (BS) providing communication services to legitimate users while concurrently detecting radar targets. In [14], pseudo-random interference signals were introduced during the transmission of communication signals. These signals are designed to disrupt eavesdroppers' attempts to intercept useful signals and simultaneously act as signals for detecting targets. In [15], a multiple-user interference was leveraged to address security issues in the dual-functional radar and communication (DFRC) system. Constructive interference is employed to enhance the received signal at communication users, while destructive interference is utilized to degrade eavesdropping signals at radar targets. In the context of the ISAC system, it is crucial to enhance the communication secrecy rate for legitimate users while maintaining sensing performance. But, for the secure communications in the ISAC system, the performance is heavily constrained by the wireless propagation environment.

Recently, due to the introduction of RIS to beyond 5G communications, RIS-based ISAC has attracted extension attention. For instance, in [16], RIS is employed in an ISAC system to enhance downlink communications. This is achieved by maximizing SINR for radar applications and minimizing the multi-user interference (MUI) for communication purposes. In [17], RIS is employed to mitigate MUI under the Cramer–Rao bound (CRB) constraint for direction of arrival (DOA) estimation. In [18], a study on fair sensing–communication waveform design with RIS is conducted. In this study, the joint optimization of beamforming at the BS and RIS is performed. The optimization aims to maximize the sensing SINR and minimize the MUI for communication.

Given the potential of RIS in improving ISAC performances, RIS has also become popular in secure ISAC designs. In [19], the secrecy rate of legitimate users was enhanced through the introduction of RIS. In [20], RIS was used to sense and locate targets in wireless networks, where a special sensor is installed near the RIS to sense the direction of nearby targets through the RIS. In [21], RIS was used to assist the wireless communication system of a security classification to ensure the quality of service of ordinary users and the safe rate of confidential users while reducing the transmission power of the BS. In [22], RIS was employed to assist the ISAC system. This involves maximizing the output SINR of the radar while ensuring the quality of service (QoS) of communication. In [23], by jointly designing the radar's received beamformer, active RIS reflection coefficient matrix, and transmit beamforming matrix, the maximum secrecy of the system was achieved under the conditions of the total power budget and the minimum signal-to-noise-ratio (SNR) of the radar. In [24], RIS was employed to assist the communication link between the BS and legitimate users while simultaneously aiding in the detection of obstructed sensing targets. The objective is to maximize the secrecy rate for legitimate users while ensuring a specified SINR for sensing. From these works, we see that RIS can provide additional communication links to improve the performance of communication networks, while increasing the SINR of legitimate users while suppressing the SINR of eavesdroppers. At the same time, RIS has expanded the ISAC system coverage range, not only ensuring communication performance, but also improving sensing performance. Inspired by the aforementioned efforts, we intend to leverage RIS to maximize both communication secrecy rate and radar radiation power towards a target.

In this paper, we leverage the potential of RIS to modify the wireless environment and design an ISAC transmitting waveform to improve the performance of the RIS-assisted secure ISAC system. We formulate an optimization problem to maximize the secrecy rate for legitimate users and the radar radiation power towards potential eavesdroppers. The main contributions are summarized as follows:

- In order to suppress the eavesdropper from intercepting legitimate users' information, the BS is designed to simultaneously transmit communication signals and interference signals, which is to achieve both sensing and communication by introducing the designed interference signals into the system. To maximize the communication secrecy rate and radar radiation power, we jointly optimize the communication beamformer, interference signal beamformer, and the reflection coefficient matrix of the RIS. Specifically, under power and phase constraints, we maximize the secrecy rate in logarithmic form and maximize the detection power in quadratic form, rendering a highly non-convex problem that is challenging to solve.
- We reformulate the secrecy rate problem as a fractional programming (FP) problem. Together with maximizing the radiation power, we then cast the problem into a semi-definite programming (SDP) formulation. The combined use of FP and SDP addresses the challenges posed by the multi-ratio fractional and non-convex optimization aspects of the problem. This enables us to further apply the semi-definite relaxation (SDR) for solving the reformulated optimization problem. Subsequently, we employ an alternating optimization framework to optimize the active beamforming matrix and the reflection coefficient matrix to achieve the final solution.

The remainder of this paper is organized as follows. Section 2 introduces the system model of the considered RIS-assisted secure ISAC system. Section 3 introduces the problem formulation involved in the system, as well as develops the joint beamforming scheme. Section 4 presents and discusses the numerical and simulation results, and Section 5 concludes the paper.

Notations: Bold lowercase letters and bold uppercase letters denote column vectors and matrices, respectively. $\mathbb{C}$ represents the set of complex numbers. $\|\cdot\|^2$ denotes the Euclidean norm, and $\|\cdot\|_{\mathrm{F}}$ denotes the Frobenius-norm of its argument. $\mathrm{diag}(a_1, a_2, \ldots, a_N)$ denotes an N-dimensional diagonal matrix whose diagonal elements are $a_1, a_2, \ldots, a_n$. $\{\cdot\}^{\mathrm{T}}$ and $\{\cdot\}^{\mathrm{H}}$ and denote the transpose and conjugate transpose operation, respectively. $\mathbf{I}_M$ represents the $M \times M$ identity matrix. $\{\cdot\}^*$ is the conjugate operation. $\mathbb{E}\{\cdot\}$ is the expectation operation. $\Re\{\cdot\}$ is the real part of a complex number.

2. System Model

We consider a secure RIS-aided ISAC system that includes a dual-functional BS, a RIS, an eavesdropper that can be treated as a sensing target, and K single antenna users, as illustrated in Figure 1. The BS is equipped with a uniform linear array of M transmitting antennas, serving K users ($M \geq K$) while detecting the target. The RIS is with N reflecting elements, each of which has a discrete adjustable phase. Let $\boldsymbol{\Theta}$ be the diagonal reflecting phase matrix of the RIS, $\boldsymbol{\Theta} = \mathrm{diag}\{\phi_1, \cdots, \phi_n, \cdots, \phi_N\}$, and $\phi_n = e^{j\vartheta_n}$, where $\vartheta_n = \frac{2\pi i}{2^b}, i = \left\{0, 1, \ldots, 2^b - 1\right\}$ is the set of possible phase values for the n-th RIS element and b is the number of quantization bits. The users are uniformly distributed within a confined area, while the potential target is located in a different area.

This work focuses on designing the ISAC waveform for different stages of the physical-layer secrecy enhancement. First, we consider refining the target detection based on prior knowledge of the coarse direction of the target, ensuring communication quality of service for legitimate users in the meantime. In the second stage, we design ISAC waveforms to actively transmit interference signals towards eavesdroppers, enhancing the secrecy rate and further improving target detection. To achieve this goal, the BS is designed to simultaneously transmit two different signals, the communication signal $\mathbf{s}_{\mathrm{c}}$ and interference signal $\mathbf{s}_{\mathrm{r}}$, and both signals can be used to detect the potential target. Assume that both

$\mathbf{s}_c$ and $\mathbf{s}_r$ are simultaneously transmitted for communications and sensing by the shared antennas, where $\mathbf{s}_c$ contains information required by legitimate users, and $\mathbf{s}_r$ is used to interfere with the eavesdropper. We assume that the prior location information of the eavesdropper has been obtained. In the ISAC system, such information can be achieved by the sensing function and treating the eavesdropper as a sensing target [15,24]. Let $\mathbf{W}_c \in \mathbb{C}^{M\times K}$ represent the related communication beamformer and $\mathbf{W}_r \in \mathbb{C}^{M\times M}$ denote the corresponding interference beamformer. Let $\mathbf{x}$ be the dual-function signal from the BS, and $\mathbf{x}$ can be expressed as

$$\mathbf{x} = \mathbf{W}_c\mathbf{s}_c + \mathbf{W}_r\mathbf{s}_r, \tag{1}$$

where $\mathbf{s}_c \in \mathbb{C}^{K\times 1}$ and $\mathbf{s}_r \in \mathbb{C}^{M\times 1}$. To avoid mutual interference between communication and interference signals, we assume that the communication and interference signals are statistically independent and uncorrelated [23], i.e., $\mathbb{E}\{\mathbf{s}_c\mathbf{s}_r^H\} = \mathbf{0}$. This is a typical and legitimate assumption in the sense that both signals are noise-like in the time domain and generated independently. And the communication and interference signals satisfy $\mathbb{E}\{\mathbf{s}_c\mathbf{s}_c^H\} = \mathbf{I}_K$ and $\mathbb{E}\{\mathbf{s}_r\mathbf{s}_r^H\} = \mathbf{I}_M$, where $\mathbf{I}_X$ represents an X-order identity matrix. For convenience, we introduce $\mathbf{W} = [\mathbf{W}_c, \mathbf{W}_r] \in \mathbb{C}^{M\times(K+M)}$ and $\mathbf{s} = [\mathbf{s}_c^T, \mathbf{s}_r^T]^T \in \mathbb{C}^{1\times(K+M)}$.

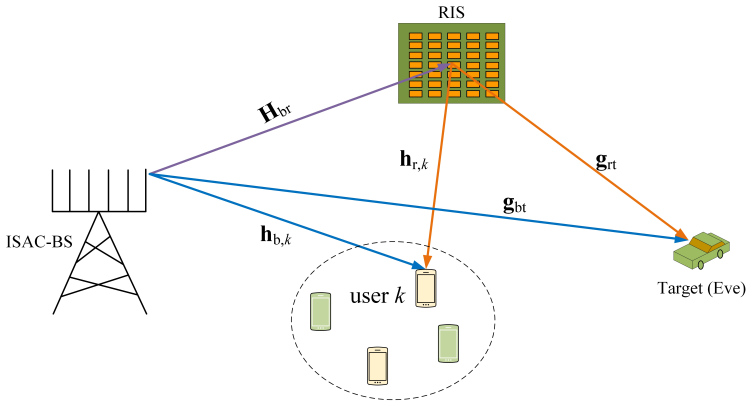


Figure 1. A RIS-aided secure ISAC system.

2.1. Communication Model

Let $\mathbf{H}_{br} \in \mathbb{C}^{N\times M}$ denote the channel information matrix from the BS to the RIS, $\mathbf{h}_{b,k}^H \in \mathbb{C}^{1\times M}$ denote the channel vector from the BS to user k, and $\mathbf{h}_{r,k}^H \in \mathbb{C}^{1\times N}$ denote the channel vector from the RIS to user k. Based on the symbols and channels modeled above, the signal received at user k can be written as

$$y_k = (\mathbf{h}_{b,k}^H + \mathbf{h}_{r,k}^H\mathbf{\Theta}\mathbf{H}_{br})\mathbf{x} + n_k, \tag{2}$$

where n_k is the additive white Gaussian noise (AWGN) with $n_k \sim \mathcal{CN}(0, \sigma_k^2)$.

Denote $\mathbf{h}_{br,k} = \mathbf{h}_{b,k}^H + \mathbf{h}_{r,k}^H\mathbf{\Theta}\mathbf{H}_{br}$ as the composite communication channel from the BS to user k. Then, the received SINR at the k-th user can be written as

$$\begin{aligned}\gamma_k &= \frac{\left\|\left(\mathbf{h}_{b,k}^H + \mathbf{h}_{r,k}^H\mathbf{\Theta}\mathbf{H}_{br}\right)\mathbf{w}_k\right\|^2}{\sum_{j=1,j\neq k}^{K+M}\left\|\left(\mathbf{h}_{b,k}^H + \mathbf{h}_{r,k}^H\mathbf{\Theta}\mathbf{H}_{br}\right)\mathbf{w}_j\right\|^2 + \sigma_k^2} \\ &= \frac{\left\|\mathbf{h}_{br,k}\mathbf{w}_k\right\|^2}{\sum_{j=1,j\neq k}^{K+M}\left\|\mathbf{h}_{br,k}\mathbf{w}_j\right\|^2 + \sigma_k^2},\end{aligned} \tag{3}$$

where $\mathbf{w}_j \in \mathbb{C}^{M\times 1}$ represents the j-th column of $\mathbf{W}$, and σ_{k}^2 denotes the noise power at the k-th user. According to (3), the achievable sum data rate of the legitimate users can be given by

$$R_{\mathrm{c}} = \sum_{k=1}^{K} \log_2 (1 + \gamma_k). \tag{4}$$

2.2. Sensing Model

Let $\mathbf{g}_{\mathrm{bt}} = \mu_{\mathrm{bt}}\mathbf{a}(\theta_{\mathrm{bt}}) \in \mathbb{C}^{M\times 1}$ denote the direct channel from the BS to the target and $\mathbf{g}_{\mathrm{rt}} = \mu_{\mathrm{rt}}\mathbf{a}(\theta_{\mathrm{rt}}) \in \mathbb{C}^{N\times 1}$ denote the channel from the RIS to the target. μ_{bt} and μ_{rt} denote the path loss from the BS to the target and from the RIS to the target, respectively. θ_{bt} and θ_{rt} denote the target direction from BS and RIS, respectively; let $\mathbf{a}(\theta_{\mathrm{bt}}) = \left[1, \mathrm{e}^{j2\pi\Delta\sin(\theta_{\mathrm{bt}})}, \ldots, \mathrm{e}^{j2\pi(M-1)\Delta\sin(\theta_{\mathrm{bt}})}\right]^{\mathrm{T}} \in \mathbb{C}^{M\times 1}$ and $\mathbf{a}(\theta_{\mathrm{rt}}) = \left[1, \mathrm{e}^{j2\pi\Delta\sin(\theta_{\mathrm{rt}})}, \ldots, \mathrm{e}^{j2\pi(N-1)\Delta\sin(\theta_{\mathrm{rt}})}\right]^{\mathrm{T}} \in \mathbb{C}^{N\times 1}$ be the steering vectors from the BS to the target and from the RIS to the target, respectively. Then, the radiation power in the direction of the target can be given by

$$\begin{aligned} P_{\mathrm{b}} =& (\mathbf{g}_{\mathrm{bt}}^{\mathrm{H}} + \mathbf{g}_{\mathrm{rt}}^{\mathrm{H}}\boldsymbol{\Theta}\mathbf{H}_{\mathrm{br}})^{\mathrm{H}}\mathbf{W}\mathbf{W}^{\mathrm{H}}(\mathbf{g}_{\mathrm{bt}}^{\mathrm{H}} + \mathbf{g}_{\mathrm{rt}}^{\mathrm{H}}\boldsymbol{\Theta}\mathbf{H}_{\mathrm{br}}) \\ =& \mathbf{h}_{\mathrm{bt}}^{\mathrm{H}}\mathbf{W}\mathbf{W}^{\mathrm{H}}\mathbf{h}_{\mathrm{bt}}, \end{aligned} \tag{5}$$

where $\mathbf{h}_{\mathrm{bt}} = \mathbf{g}_{\mathrm{bt}}^{\mathrm{H}} + \mathbf{g}_{\mathrm{rt}}^{\mathrm{H}}\boldsymbol{\Theta}\mathbf{H}_{\mathrm{br}}$ in (5).

In the considered ISAC system, the target is a potential eavesdropper, who attempts to decode the information sent to the legitimate users. The received SINR at the target in terms of the k-th user can be given by

$$\gamma_{\mathrm{t},k} = \frac{\|\mathbf{h}_{\mathrm{bt}}\mathbf{w}_k\|^2}{\sum_{j=1,j\neq k}^{K+M}\|\mathbf{h}_{\mathrm{bt}}\mathbf{w}_j\|^2 + \sigma_{\mathrm{t}}^2}, \tag{6}$$

where σ_{t}^2 denotes the noise power at the target.

Based on (6), the achievable rate of the communication information eavesdropped by the target can be given by

$$R_{\mathrm{t}} = \sum_{k=1}^{K} \log_2 (1 + \gamma_{\mathrm{t},k}). \tag{7}$$

Then, the secrecy rate of the considered system can be computed by

$$\begin{aligned} R_{\mathrm{s}} =& R_{\mathrm{c}} - R_{\mathrm{t}} \\ =& \sum_{k=1}^{K} \log_2 (1 + \gamma_k) - \sum_{k=1}^{K} \log_2 (1 + \gamma_{\mathrm{t},k}). \end{aligned} \tag{8}$$

3. Problem Formulation and Algorithm Design

In this paper, we jointly design the BS transmit beamformer $\mathbf{W}$ and RIS phase shift matrix $\boldsymbol{\Theta}$ to maximize the secrecy rate of the system and the radiation power of the target.

3.1. Problem Formulation

The problem is formulated as

$$\begin{aligned} \max_{\mathbf{W},\boldsymbol{\Theta}} \ & \rho R_{\mathrm{s}} + P_{\mathrm{b}} \\ \text{s.t.} \ \ & C1: \|\mathbf{W}\|_{\mathrm{F}}^2 \le P, \\ & C2: \vartheta_n = \frac{2\pi i}{2^b}, i = \left\{0, 1, \ldots, 2^b - 1\right\}, \end{aligned} \tag{9}$$

where ρ is the regularization parameter, P_{b} is the radiation power in the direction of the target (5), and P is the maximum transmission power of the BS. According to (3)–(6), the impact of $\mathbf{W}$ and $\boldsymbol{\Theta}$ on the secrecy rate and radiation power optimization mainly depends on γ_k, $\gamma_{\mathrm{t},k}$, and P_{b}.

Problem (9) is a non-convex optimization problem and is difficult to solve directly. Next, we will first transform the problem into two optimization problems with respect to $\mathbf{W}$ and $\boldsymbol{\Theta}$, respectively, and then employ FP [25] and SDP to develop a low complexity solution to the original problem.

3.2. Proposed Scheme

In this section, we solve Problem (9) in two steps: optimizing $\mathbf{W}$ with a given RIS phase matrix and optimizing $\boldsymbol{\Theta}$ with a fixed BS beamforming matrix. The two steps alternate and iterate until convergence.

3.2.1. Step 1: Optimizing Active Beamforming Matrix $\mathbf{W}$ at the BS

We solve the BS beamforming matrix $\mathbf{W}$ by fixing the reflection coefficients matrix of the RIS, $\boldsymbol{\Theta}$. Then, Problem (9) can be simplified as

$$\begin{aligned} \max_{\mathbf{W}} \ & \rho(R_{\mathrm{c}} - R_{\mathrm{t}}) + P_{\mathrm{b}} \\ \text{s.t.} \ \ & C1. \end{aligned} \tag{10}$$

Problem (10) is still non-convex, and we will transform it into a convex problem to find its solution. For the non-convex term involving the difference between two logarithmic functions in the first term, i.e., $\rho R_{\mathrm{s}} = \rho(R_{\mathrm{c}} - R_{\mathrm{t}})$, we apply the FP method [25] to recast it to a convex problem. For the second term P_{b}, we will reshape it to be convex, adopting a similar approach to that in [26]. By rephrasing the two terms, we rewrite the objective function with respect to the optimization variable $\mathbf{W}$ into a convex form.

We start with recasting R_{c} in the objective function of (10) as a convex form regarding $\mathbf{W}$. According to (4), R_{c} in (8) can be expressed as

$$R_{\mathrm{c}} = \sum_{k=1}^{K} \log_2 \left(1 + \frac{\left\|\mathbf{h}_{\mathrm{br},k}\mathbf{w}_k\right\|^2}{\sum_{j=1,j\neq k}^{K+M} \left\|\mathbf{h}_{\mathrm{br},k}\mathbf{w}_j\right\|^2 + \sigma_k^2} \right). \tag{11}$$

Applying the quadratic transformation [27], (11) can be expressed as a Lagrangian dual expression as

$$R_{\mathrm{c}} = \sum_{k=1}^{K} \log_2 \left(1 + \beta_k\right) - \sum_{k=1}^{K} \beta_k + \sum_{k=1}^{K} \frac{\left(1 + \beta_k\right)\left\|\mathbf{h}_{\mathrm{br},k}\mathbf{w}_k\right\|^2}{\sum_{j=1,j\neq k}^{K+M} \left\|\mathbf{h}_{\mathrm{br},k}\mathbf{w}_j\right\|^2 + \sigma_k^2}, \tag{12}$$

where $[\beta_k, \cdots, \beta_K]$ is the auxiliary variable introduced. Note that there is still a fractional part on the right side of (12); hence, we apply the quadratic transformation again, leading to

$$R_{\mathrm{c}} = \sum_{k=1}^{K} \log_2(1+\beta_k) - \sum_{k=1}^{K} \beta_k - \sum_{k=1}^{K} |\varepsilon_k|^2 \sigma_k^2 + 2\sum_{k=1}^{K} \sqrt{1+\beta_k}\Re\{\varepsilon_k^* \mathbf{h}_{\mathrm{br},k}\mathbf{w}_k\} - \sum_{k=1}^{K} |\varepsilon_k|^2 \sum_{j=1,j\neq k}^{K+M} \left|\mathbf{h}_{\mathrm{br},k}\mathbf{w}_j\right|^2, \tag{13}$$

where $[\varepsilon_k, \cdots, \varepsilon_K]$ is the auxiliary variable introduced.

Note that β_k and ε_k are auxiliary variables. With all other variables fixed, then β_k and ε_k can be obtained by solving the equations of $\frac{\partial R_{\mathrm{c}}}{\partial \beta_k}$ and $\frac{\partial R_{\mathrm{c}}}{\partial \varepsilon_k}$ equal to zero, respectively. With the details suppressed, β_k and ε_k are obtained as

$$\beta_k = \frac{\left\|\mathbf{h}_{\mathrm{br},k}\mathbf{w}_k\right\|^2}{\sum_{j=1,j\neq k}^{K+M} \left\|\mathbf{h}_{\mathrm{br},k}\mathbf{w}_j\right\|^2 + \sigma_k^2}; \tag{14}$$

$$\varepsilon_k = \frac{\sqrt{1+\beta_k}\mathbf{h}_{\mathrm{br},k}\mathbf{w}_k}{\sum_{j=1,j\neq k}^{K+M} \left\|\mathbf{h}_{\mathrm{br},k}\mathbf{w}_j\right\|^2 + \sigma_k^2}. \tag{15}$$

Define $\bar{\mathbf{w}} = \mathrm{vec}\{\mathbf{W}\}$ and $\mathbf{w}_j = \mathbf{\Gamma}_j \bar{\mathbf{w}}$, where $\mathbf{\Gamma}_j$ refers to a permutation matrix. Further define $\mathbf{v}$ and $\mathbf{U}$ as

$$\mathbf{v} = \left[2\varepsilon_k^*\sqrt{1+\beta_1}\mathbf{h}_{\mathrm{br},1}, \cdots, 2\varepsilon_k^*\sqrt{1+\beta_K}\mathbf{h}_{\mathrm{br},k}, \cdots, \mathbf{0}_{1\times M(K+M)-MK}\right]^{\mathrm{H}} \in \mathbb{C}^{M(K+M)\times 1}, \tag{16}$$

$$\mathbf{U} = \left[\mathbf{u}_{1,1}, \cdots, \mathbf{u}_{K,K+M}\right]^{\mathrm{T}} \in \mathbb{C}^{(K+M)\times M(K+M)}, \tag{17}$$

where $\mathbf{u}_{k,j} = |\varepsilon_k|\mathbf{\Gamma}_j^{\mathrm{T}}\mathbf{h}_{\mathrm{br},k}^{\mathrm{H}}$. Based on (13)–(17), R_{c} can be further written into

$$R_{\mathrm{c}} = f_1 + \Re\left\{\mathbf{v}^{\mathrm{H}}\bar{\mathbf{w}}\right\} - \|\mathbf{U}\bar{\mathbf{w}}\|^2, \tag{18}$$

where $f_1 = \sum_{k=1}^{K} \log_2(1+\beta_k) - \sum_{k=1}^{K} \beta_k - \sum_{k=1}^{K} |\varepsilon_k|^2\sigma_k^2$.

Then, we recast R_{t} in the objective function of (10) as a convex form regarding $\mathbf{W}$. Similarly, R_{t} in (8) can be expressed as

$$R_{\mathrm{t}} = \sum_{k=1}^{K} \log_2\left(1 + \frac{\left\|\mathbf{h}_{\mathrm{bt}}\mathbf{w}_k\right\|^2}{\sum_{j=1,j\neq k}^{K+M} \left\|\mathbf{h}_{\mathrm{bt}}\mathbf{w}_j\right\|^2 + \sigma_k^2}\right). \tag{19}$$

Its polynomial form can be given by

$$R_{\mathrm{t}} = \sum_{k=1}^{K} \log_2(1+\beta_{\mathrm{r},k}) - \sum_{k=1}^{K} \beta_{\mathrm{r},k} - \sum_{k=1}^{K} \left|\varepsilon_{\mathrm{r},k}\right|^2 \sigma_{\mathrm{t}}^2 + 2\sum_{k=1}^{K} \sqrt{1+\beta_{\mathrm{r},k}}\Re\left\{\varepsilon_{\mathrm{r},k}^* \mathbf{h}_{\mathrm{br},k}\mathbf{w}_k\right\} - \sum_{k=1}^{K} \left|\varepsilon_{\mathrm{r},k}\right|^2 \sum_{j=1,j\neq k}^{K+M} \left|\mathbf{h}_{\mathrm{br,\,k}}\mathbf{w}_j\right|^2, \tag{20}$$

where β_r and ε_r are auxiliary variables and are given by

$$\beta_{\mathrm{r},k} = \frac{\left\|\mathbf{h}_{\mathrm{bt}}\mathbf{w}_k\right\|^2}{\sum_{j=1,j\neq k}^{K+M} \left\|\mathbf{h}_{\mathrm{bt}}\mathbf{w}_j\right\|^2 + \sigma_{\mathrm{t}}^2}; \tag{21}$$

$$\varepsilon_{\mathrm{r},k} = \frac{\sqrt{1+\beta_{\mathrm{r},k}}\mathbf{h}_{\mathrm{bt}}\mathbf{w}_k}{\sum_{j=1,j\neq k}^{K+M}\left\|\mathbf{h}_{\mathrm{bt}}\mathbf{w}_j\right\|^2+\sigma_{\mathrm{t}}^2}. \tag{22}$$

Note that $\beta_{\mathrm{r},k}$ in (21) and $\varepsilon_{\mathrm{r},k}$ in (22) can again be obtained by solving the equations of $\frac{\partial R_{\mathrm{t}}}{\partial \beta_{\mathrm{r},k}}$ and $\frac{\partial R_{\mathrm{t}}}{\partial \varepsilon_{\mathrm{r},k}}$ equal to zero.

Define $\mathbf{v1}$ and $\mathbf{U1}$ as follows

$$\begin{aligned}\mathbf{v1} =&\left[2\varepsilon_{\mathrm{r},k}^*\sqrt{1+\beta_{\mathrm{r},1}}\mathbf{h}_{\mathrm{bt}},\cdots,2\varepsilon_{\mathrm{r},k}^*\sqrt{1+\beta_{\mathrm{r},K}}\mathbf{h}_{\mathrm{bt}},\cdots,\mathbf{0}_{1\times M(K+M)-MK}\right]^{\mathrm{H}}\\ &\in\mathbb{C}^{M(K+M)\times 1},\end{aligned} \tag{23}$$

$$\mathbf{U1} = \left[\mathbf{u1}_{1,1},\cdots,\mathbf{u1}_{K,K+M}\right]^{\mathrm{T}}\in\mathbb{C}^{(K+M)\times M(K+M)}, \tag{24}$$

where $\mathbf{u1}_{k,j} = \left|\varepsilon_{\mathrm{r},k}\right|\mathbf{\Gamma}_j^{\mathrm{T}}\mathbf{h}_{\mathrm{bt}}^{\mathrm{H}}$. Based on (20)–(24), R_{t} can be further written into

$$R_{\mathrm{t}} = f_2+\Re\left\{\mathbf{v1}^{\mathrm{H}}\bar{\mathbf{w}}\right\}-\|\mathbf{U1}\bar{\mathbf{w}}\|^2, \tag{25}$$

where $f_2=\sum_{k=1}^{K}\log_2(1+\beta_{\mathrm{r},k})-\sum_{k=1}^{K}\beta_{\mathrm{r},k}-\sum_{k=1}^{K}\left|\varepsilon_{\mathrm{r},k}\right|^2\sigma_{\mathrm{t}}^2$.

Substituting (18) and (25) into (8), R_{s} becomes

$$R_{\mathrm{s}} = f_1+\Re\left\{\mathbf{v}^{\mathrm{H}}\bar{\mathbf{w}}\right\}-\|\mathbf{U}\bar{\mathbf{w}}\|^2-f_2-\Re\left\{\mathbf{v1}^{\mathrm{H}}\bar{\mathbf{w}}\right\}+\|\mathbf{U1}\bar{\mathbf{w}}\|^2. \tag{26}$$

Finally, we recast the last term P_{b} in the objective function of (10) as a convex form regarding $\mathbf{W}$. To make the last term convex, we first reformulate (5) as follows

$$\begin{aligned}P_{\mathrm{b}} =&\mathbf{h}_{\mathrm{bt}}^{\mathrm{H}}\mathbf{W}\mathbf{W}^{\mathrm{H}}\mathbf{h}_{\mathrm{bt}}\\ =&\sum_{k=1}^{K+M}\mathbf{w}_k^{\mathrm{H}}(M\mathbf{I}_M-\mathbf{h}_{\mathrm{bt}}\mathbf{h}_{\mathrm{bt}}^{\mathrm{H}})\mathbf{w}_k-MP.\end{aligned} \tag{27}$$

Note that $\mathbf{Z}=M\mathbf{I}_M-\mathbf{h}_{\mathrm{bt}}\mathbf{h}_{\mathrm{bt}}^{\mathrm{H}}$ is a positive semi-definite matrix [26]. Therefore, (27) is a convex function.

Substituting (26) and (27) into (10), Problem (10) can be reformulated as

$$\begin{aligned}&\max_{\mathbf{W}}\ \rho\left(\Re\{\bar{\mathbf{v}}\bar{\mathbf{w}}\}-\|\mathbf{U}\bar{\mathbf{w}}\|^2+\|\mathbf{U1}\bar{\mathbf{w}}\|^2\right)+\sum_{k=1}^{K}\mathbf{w}_k^{\mathrm{H}}\mathbf{Z}\mathbf{w}_k\\ &\text{s.t.}\quad C1.\end{aligned} \tag{28}$$

Since $\mathbf{h}_{\mathrm{br},k}=\mathbf{h}_{\mathrm{b},k}^{\mathrm{H}}+\mathbf{h}_{\mathrm{r},k}^{\mathrm{H}}\mathbf{\Theta}\mathbf{H}_{\mathrm{br}}$ and $\mathbf{h}_{\mathrm{bt}}=\mathbf{g}_{\mathrm{bt}}^{\mathrm{H}}+\mathbf{g}_{\mathrm{rt}}^{\mathrm{H}}\mathbf{\Theta}\mathbf{H}_{\mathrm{br}}$, according to the expressions in (16)–(24) and (27), it can be observed that (28) is a function of $\mathbf{W}$ and $\mathbf{\Theta}$. Note that when $\mathbf{\Theta}$ is fixed, Problem (28) is an SDP convex problem and can be efficiently solved by the CVX toolbox [28].

3.2.2. Step 2: Optimizing Passive Beamforming Matrix at the RIS

For given $\mathbf{W}$, Problem (9) can be simplified to

$$\begin{aligned}&\max_{\mathbf{\Theta}}\ \rho R_{\mathrm{s}}+P_{\mathrm{b}}\\ &\text{s.t.}\quad C2.\end{aligned} \tag{29}$$

In (29), the available phase range of each reflective element depends on the bit of RIS. When $\mathbf{W}$ is fixed and power constraints are removed, the objective function in (29) regarding $\mathbf{\Theta}$ still remains non-convex. Considering the complexity of the problem, here, we adopt

a local search method [29] to solve it. For the optimization of the phase of the n-th RIS element, we first fix the phase values of the other N-1 RIS elements to their initial values (for those with already optimized phase values, these are fixed at their optimal values). We enumerate all possible values within the feasible region $\left\{\vartheta_n = \frac{2\pi i}{2^b}, i = 0, 1, \ldots, 2^b - 1\right\}$, identifying the value that maximizes the secrecy rate as the optimal phase value for the n-th element. Subsequently, we continue the search process until we obtain the optimal phase values for all RIS elements. The searching process will be executed $N \times 2^b$ times until all RIS elements obtain the optimal phase values.

3.2.3. Overall Optimization Framework

In Sections 3.2.1 and 3.2.2, we have developed solutions to the problems of BS beamforming optimization and RIS phase shift optimization. In this section, we will describe the proposed overall alternate optimization scheme. Specifically, we execute Step 1 and Step 2 sequentially, and then alternatively iterate between these two steps to facilitate a RIS-assisted secure ISAC, as shown in Algorithm 1. In the algorithm, Line 1 is to optimize the variable settings for feasible initial values. Lines 3-11 involve alternately solving for $\mathbf{W}$ and $\mathbf{\Theta}$ based on the convex problems transformed in (10) and (29). In this context, Lines 3–6 pertain to various auxiliary variables involved in the optimization process.

Algorithm 1 Proposed joint beamforming scheme in RIS-assisted secure ISAC systems

1: **Input** initial values of $\mathbf{W}^{[0]}$, $\mathbf{\Theta}^{[0]}$, β_k, ε_k, $\beta_{\mathrm{r},k}$, $\varepsilon_{\mathrm{r},k}$, and the number of quantization bits b; set the initial iteration number $i = 1$;
2: **Repeat**
3: Calculate $\beta_k^{[i]}$ by solving (14);
4: Update $\varepsilon_k^{[i]}$ by solving (15);
5: Calculate $\beta_{\mathrm{r},k}^{[i]}$ by solving (21);
6: Update $\varepsilon_{\mathrm{r},k}^{[i]}$ by solving (22);
7: Given $\mathbf{\Theta} = \mathbf{\Theta}^{[i-1]}$, update $\mathbf{W}^{[i]}$ by solving (10);
8: Given $\mathbf{W} = \mathbf{W}^{[i]}$, update $\mathbf{\Theta}^{[i]}$ by solving (29);
9: For $n = 1$ to N do
10: Assign all possible values to ϑ_n and select the value maximizing the R_{s} in (29);
11: End For
12: i=i+1
13: **Until** $\left|R_{\mathrm{s}}^{[i-1]} - R_{\mathrm{s}}^{[i]}\right| \leq \delta$ or maximum iteration reached.

The computational complexity of Algorithm 1 is analyzed next. We can observe that the complexity of the algorithm is primarily concentrated in lines 7 and 8. Line 7 involves solving an SDP problem; its computational complexity for one iteration is $\mathcal{O}\left(M^{4.5}\right)$. Line 8 is used to solve the optimization of discrete phase shift performs for Algorithm 1, with the respective computational complexity of $\mathcal{O}\left(N \times 2^b\right)$. Therefore, the overall computational complexity of Algorithm 1 is in the order of $\mathcal{O}\left(I_t\left(KM^{4.5} + N \times 2^b\right)\right)$, where I_t denotes the iteration times. The convergence of Algorithm 1 will be demonstrated in the subsequent section.

4. Simulation Results

In this section, we present simulation results to validate the performance of the RIS-assisted secure ISAC system. We consider the RIS-assisted secure ISAC system depicted in Figure 1. Assume the direct link channel follows Rayleigh fading and the RIS-aided channels follow Rician fading. In the simulation, we set the number of antennas at the BS as $M = 32$, employing a ULA with half-wavelength spacing between adjacent antennas and the total power budget as $P = 20$ dBm, $\sigma_k^2 = -90$ dBm, $\sigma_{\mathrm{t}}^2 = -90$ dBm, and $\delta = 10^{-3}$. The

Rician factor is four, and the regularization parameter is 100. K single-antenna users are uniformly and randomly distributed within a circle centered at (200 m, −50 m) with a radius of 30 m. The BS and the RIS are located at (0 m, 0 m) and (200 m, 0 m), respectively. The target is positioned at an azimuth angle of $\theta_{\mathrm{bt}} = 45^{\circ}$ and $\theta_{\mathrm{rt}} = 45^{\circ}$. The path loss models for direct and indirect links are Los $= 32.6 + 36.7 \log_{10}(di)$ dB, NLos $= 35.6 + 22 \log_{10}(di)$ dB according to [30], where di is the link distance.

Before showing the ISAC performance, we demonstrate the convergence of the proposed Algorithm 1. Figure 2 illustrates the convergence of the proposed algorithm with RIS, without RIS, and without the designed interference signal, where $N = 20$. As clearly shown, the average secrecy rate achieved by the proposed algorithm exhibits rapid growth with an increasing number of iterations, reaching convergence in less than 10 iterations. We also see that the introduction of RIS and the designed interference signals significantly enhance the security performance of the ISAC system.

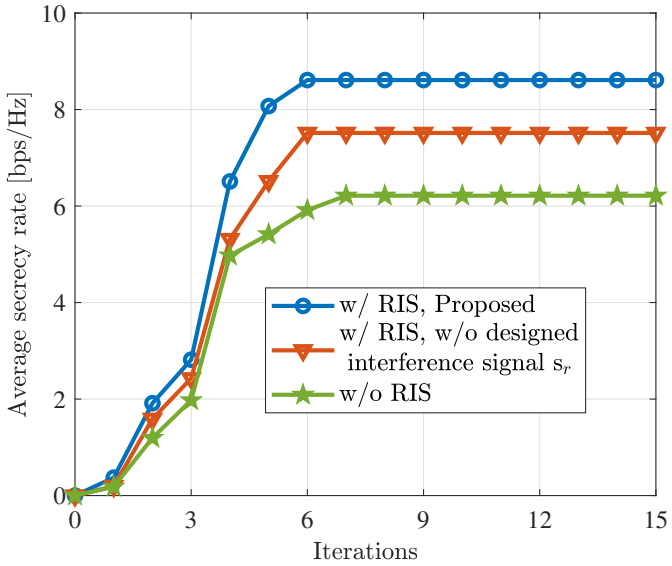
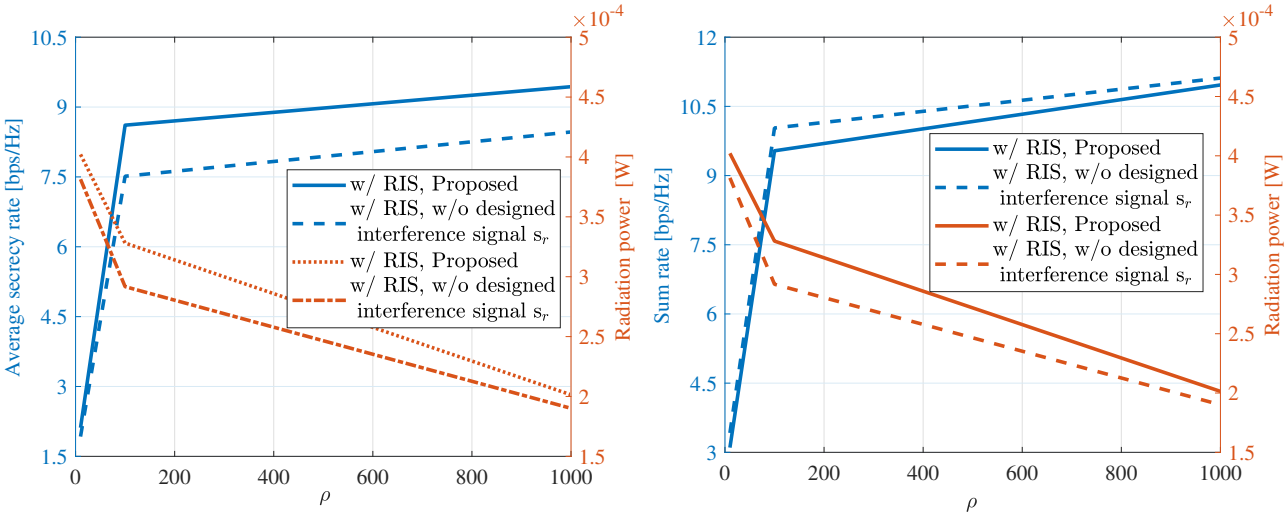


Figure 2. Convergence of the proposed algorithm for scenarios with RIS, without RIS, and without the designed interference signal. 'w/o' and 'w/ ' stand for without and with, respectively.

Figure 3 illustrates the impact of the regularization factor ρ introduced in Problem (9). It can be observed that the proposed method converges for different values of ρ. However, due to the different weighting of the two physical quantities in (9) by ρ, we can see that the performance achieved by the ISAC system varies with different regularization factors. Figure 3a and Figure 3b, respectively, depict the achieved communication secrecy rate, sum rate, and sensing radiation power under different values of ρ. Across various regularization factors, the system's achievable sum rate consistently surpasses the secrecy rate. This implies that maximizing the secrecy rate does not adversely affect the overall sum rate of the system. And from the simulation results, it can be seen that the performance achieved by the ISAC system varies with different regularization factors, which further proves the rationality of our proposed method.

In Figure 4, we evaluate the secrecy rates and radar radiation power of the considered ISAC system under different network densities, as indicated by the numbers of legitimate users in a confined region. It can be observed that as the number of users increases, the two performance metrics slightly degrade. This is reasonable due to the increasing channel coherence. However, it is worth noting that the proposed approach actively transmitting interference signals achieves non-trivial performance improvements over the considered range of Ks. Specifically, when the number of legitimate users is six, the ISAC system with interference signals exhibits approximately a 13% improvement in the secrecy rate and an 11% increase in radiation power compared to the ISAC system without interference

signals. This validates that introducing interference signals can effectively enhance the performance of the ISAC system. Moreover, our approach exhibits robust performance across different numbers of users, further confirming the robustness and applicability of the proposed method.



(**a**) Average secrecy rate and radiation power versus the ρ

(**b**) Sum rate and radiation power versus the ρ

Figure 3. Performance trade-off.

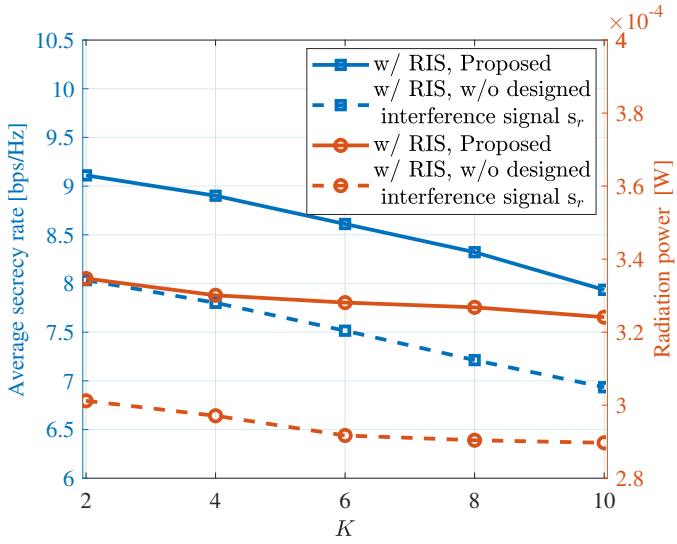
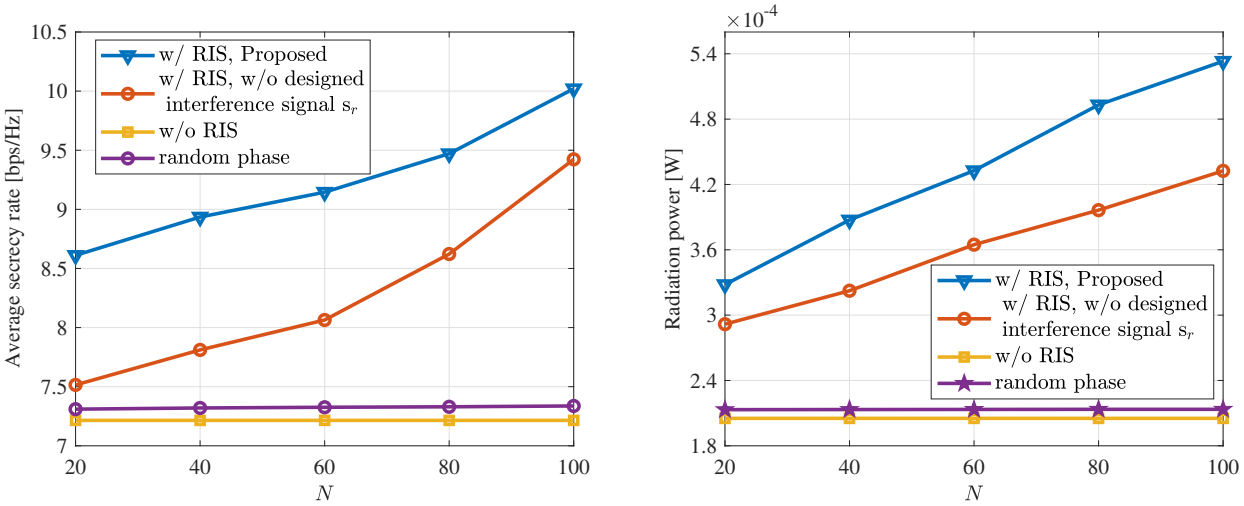


Figure 4. The communication and sensing performance under different values of K (user number), where curves with circle markers use the right y-axis.

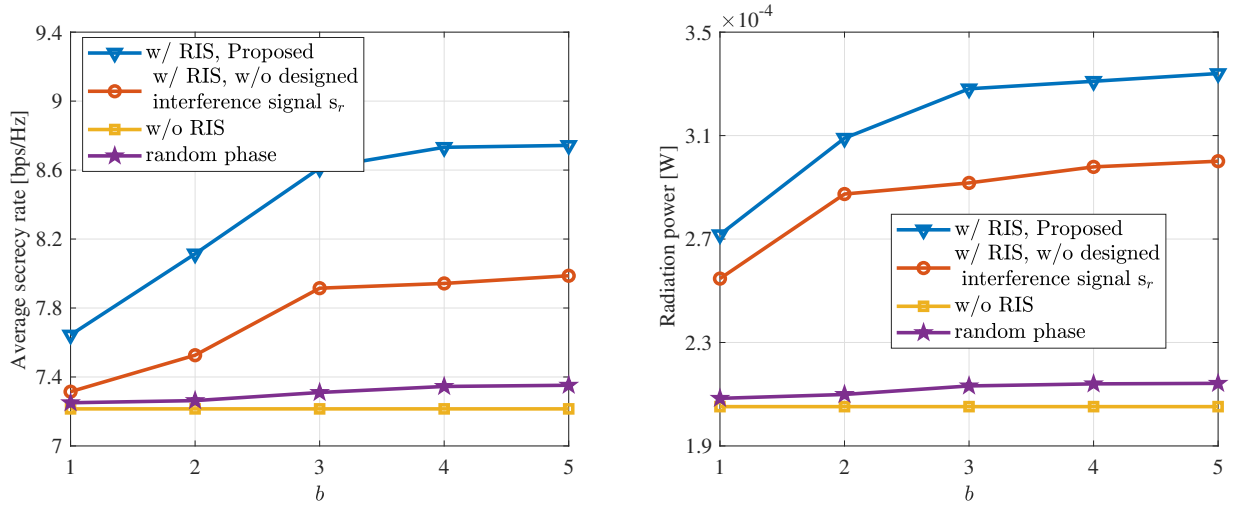
In Figure 5a, we compare the average secrecy rate with the number of RIS elements N. We can see that the performance of all schemes, except for the case without RIS, increases with the increment of N. Furthermore, compared to the method without the designed interference signals, the proposed approach achieves significant performance improvement. Specifically, when $N = 60$, the average secrecy rate of the system increases by 15%. Similarly, in Figure 5b, we compare the radiation power with the number of RIS elements N. It can be observed that the radiation power gradually increases with the increment of N. At $N = 60$, the system's radiation power increases by 18%. Additionally, we find that the proposed approach exhibits a significant improvement in sensing performance. Combining the results from Figure 5a,b, the proposed algorithm significantly enhances the performance of the ISAC system. The introduction of RIS and interference signals has significantly enhanced the ISAC system's performance.



(**a**) Average secrecy rate versus the number of RIS elements N (**b**) Radiation power versus the number of RIS elements N

Figure 5. The communication and sensing performance under different values of N.

In Figure 6, the achievable average secrecy rate and radiation power of the system are plotted against the increasing bit quantization number, ranging from 1 to 5. In Figure 6a, we can observe a clear advantage of the proposed approach in terms of secrecy rate. In the presence of interference signals, the average secrecy rate can be increased by up to 10%. Additionally, we observed that the bit quantization number increases from 1 to 4, and then from 4 to 5; the average secrecy rate remains relatively constant. This suggests that the system's performance reaches a saturation point once the quantization bit number exceeds 4. Similarly, in Figure 6b, we can also observe a significant increase in radiation power with the addition of RIS and the introduction of interference signals. Likewise, as the quantization bit number varies, a phenomenon similar to Figure 6a is evident.



(**a**) Average secrecy rate versus the number of quantization bits b (**b**) Radiation power versus the number of quantization bits b

Figure 6. The communication and sensing performance under different values of b.

Figure 7 illustrates the average secrecy rate of legitimate users when $N = 20$, while moving the RIS from (50 m, 0 m) to (250 m, 0 m). It can be observed that as the distance between RIS and BS increases, the ISAC system's secrecy rate decreases and its security performance is weaker. Additionally, we also observe that under the same power constraints, introducing interference signals can provide a better secrecy rate.

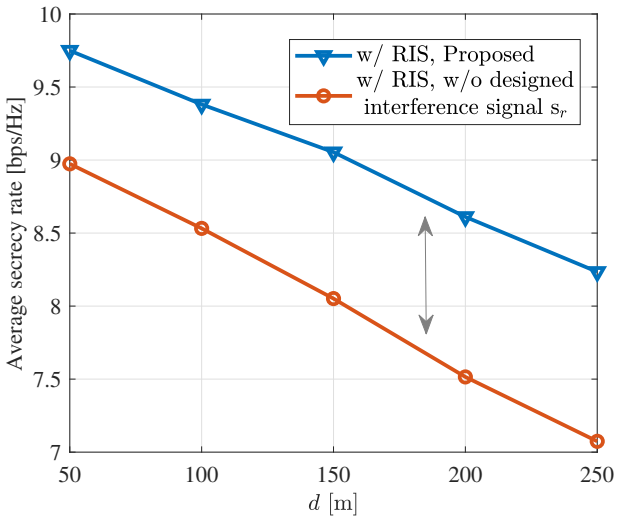


Figure 7. Average secrecy rate versus the horizontal distance of the RIS from the BS d.

5. Conclusions

In this paper, we introduced the design of a secure ISAC system, proposing a joint optimization scheme on the transmit beamforming and the RIS coefficient matrix. Specifically, leveraging the potential of the RIS, we added the designed interference signals at the BS transmitter to confuse eavesdroppers attempting to intercept information from legitimate users. To ensure both the secrecy rate for legitimate users and the sensing performance of target detection, we formulated an optimization problem aiming to maximize the secrecy rate for legitimate users and the sensing radiation power. To overcome the non-convexity of the optimization problem, techniques such as FP and SDR were applied to convert the non-convex problem into a convex one. The problem was then solved using a low-complexity alternating optimization approach. Simulation results validated the effectiveness of the proposed method, demonstrating that the inclusion of RIS and interference signals can effectively enhance the ISAC system's secrecy rate and sensing performance.

Though the optimization techniques applied in this work have achieved non-trivial performance enhancements in the considered secure ISAC system, it can be an interesting future work to further explore other optimization techniques, such as the popular majorization–minimization (MM) [24] and the manifold optimization [31]. In the future, we may consider exploring new methods to control nulls in the transmission waveform design to enhance the security rate and energy efficiency of the ISAC system [32]. And machine learning methods are showing promising results in addressing the issue of channel correlation between eavesdroppers and legitimate users [33], and in the future, we can further leverage machine learning techniques to enhance the security and efficiency of ISAC systems. Additionally, extending the proposed scheme to multi-RIS scenarios can be an interesting future work.

Author Contributions: Conceptualization, J.C. and K.W.; methodology, J.C.; software, J.C.; validation, J.C., K.W. and J.N.; formal analysis, K.W.; investigation, J.N.; resources, K.W.; data curation, J.C.; writing—original draft preparation, J.C.; writing—review and editing, J.C., K.W. and J.N.; visualization, J.C.; supervision, K.W., J.N. and Y.L.; project administration, J.C.; funding acquisition, J.N. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China (Grant No. 62072373, 61901372, 61972316), by the International Cooperation Foundation of Shaanxi Province (Grant No. 2019KW-012), by the Natural Science Research Program of Shaanxi Province (Grant No. 2020JQ-599), and by China Postdoctoral Science Foundation (Grant No. 2020M683541).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to legal restrictions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Liu, F.; Masouros, C.; Petropulu, A.P.; Griffiths, H.; Hanzo, L. Joint Radar and Communication Design: Applications, State-of-the-Art, and the Road Ahead. *IEEE Trans. Commun.* **2020**, *68*, 3834–3862. [CrossRef]
2. Wu, K.; Zhang, J.A.; Guo, Y.J. *Joint Communications and Sensing: From Fundamentals to Advanced Techniques*; John Wiley & Sons: Hoboken, NJ, USA, 2022.
3. Zhang, J.A.; Rahman, M.L.; Wu, K.; Huang, X.; Guo, Y.J.; Chen, S.; Yuan, J. Enabling Joint Communication and Radar Sensing in Mobile Networks—A Survey. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 306–345. [CrossRef]
4. Liu, F.; Zhou, L.; Masouros, C.; Li, A.; Luo, W.; Petropulu, A. Toward Dual-functional Radar-Communication Systems: Optimal Waveform Design. *IEEE Trans. Signal Process.* **2018**, *66*, 4264–4279. [CrossRef]
5. Liu, F.; Masouros, C.; Li, A.; Sun, H.; Hanzo, L. MU-MIMO Communications with MIMO Radar: From Co-Existence to Joint Transmission. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 2755–2770. [CrossRef]
6. Sturm, C.; Wiesbeck, W. Waveform Design and Signal Processing Aspects for Fusion of Wireless Communications and Radar Sensing. *Proc. IEEE* **2011**, *99*, 1236–1259. [CrossRef]
7. Liu, X.; Huang, T.; Shlezinger, N.; Liu, Y.; Zhou, J.; Eldar, Y.C. Joint Transmit Beamforming for Multiuser MIMO Communications and MIMO Radar. *IEEE Trans. Signal Process.* **2020**, *68*, 3929–3944. [CrossRef]
8. Dong, L.; Han, Z.; Petropulu, A.P.; Poor, H.V. Improving Wireless Physical Layer Security via Cooperating Relays. *IEEE Trans. Signal Process.* **2010**, *58*, 1875–1888. [CrossRef]
9. Wu, K.; Zhang, J.A.; Huang, X.; Guo, Y.J. Integrating Secure Communications Into Frequency Hopping MIMO Radar with Improved Data Rate. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 5392–5405. [CrossRef]
10. Liu, L.; Zhang, R.; Chua, K.C. Secrecy Wireless Information and Power Transfer with MISO Beamforming. *IEEE Trans. Signal Process.* **2014**, *62*, 1850–1863. [CrossRef]
11. Wu, K.; Ni, W.; Zhang, J.A.; Liu, R.P.; Guo, J. Secrecy Rate Analysis for Millimeter-Wave Lens Antenna Array Transmission. *IEEE Commun. Lett.* **2020**, *24*, 272–276. [CrossRef]
12. Chalise, B.K.; Amin, M.G. Performance tradeoff in a unified system of communications and passive radar: A secrecy capacity approach. *Digital Signal Process.* **2018**, *82*, 282–293. [CrossRef]
13. Su, N.; Liu, F.; Masouros, C. Secure Radar-Communication Systems with Malicious Targets: Integrating Radar, Communications and Jamming Functionalities. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 83–95. [CrossRef]
14. Deligiannis, A.; Daniyan, A.; Lambotharan, S.; Chambers, J.A. Secrecy Rate Optimizations for MIMO Communication Radar. *IEEE Trans. Aerosp. Electron. Syst.* **2018**, *54*, 2481–2492. [CrossRef]
15. Su, N.; Liu, F.; Wei, Z.; Liu, Y.F.; Masouros, C. Secure Dual-Functional Radar-Communication Transmission: Exploiting Interference for Resilience against Target Eavesdropping. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 7238–7252. [CrossRef]
16. Zhong, K.; Hu, J.; Pan, C.; Deng, M.; Fang, J. Joint Waveform and Beamforming Design for RIS-Aided ISAC Systems. *IEEE Signal Process. Lett.* **2023**, *30*, 165–169. [CrossRef]
17. Wang, X.; Fei, Z.; Huang, J.; Yu, H. Joint Waveform and Discrete Phase Shift Design for RIS-Assisted Integrated Sensing and Communication System Under Cramer-Rao Bound Constraint. *IEEE Trans. Veh. Technol.* **2022**, *71*, 1004–1009. [CrossRef]
18. An, D.; Hu, J.; Huang, C. Joint design of transmit waveform and passive beamforming for RIS-assisted ISAC system. *Signal Process.* **2023**, *204*, 108854. [CrossRef]
19. Cui, M.; Zhang, G.; Zhang, R. Secure Wireless Communication via Intelligent Reflecting Surface. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 1410–1414. [CrossRef]
20. Shao, X.; You, C.; Ma, W.; Chen, X.; Zhang, R. Target Sensing with Intelligent Reflecting Surface: Architecture and Performance. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 2070–2084. [CrossRef]
21. Xing, J.; Lv, T.; Cao, Y.; Zeng, J.; Huang, P. Downlink Power Minimization in Intelligent Reflecting Surface Aided Security Classification Wireless Communications System. *IEEE Syst. J.* **2023**, *17*, 407–418. [CrossRef]
22. Liu, R.; Li, M.; Liu, Y.; Wu, Q.; Liu, Q. Joint Transmit Waveform and Passive Beamforming Design for RIS-Aided DFRC Systems. *IEEE J. Sel. Top. Signal Process.* **2022**, *16*, 995–1010. [CrossRef]
23. Salem, A.A.; Ismail, M.H.; Ibrahim, A.S. Active Reconfigurable Intelligent Surface-Assisted MISO Integrated Sensing and Communication Systems for Secure Operation. *IEEE Trans. Veh. Technol.* **2023**, *72*, 4919–4931. [CrossRef]
24. Hua, M.; Wu, Q.; Chen, W.; Dobre, O.A.; Lee Swindlehurst, A. Secure Intelligent Reflecting Surface Aided Integrated Sensing and Communication. *IEEE Trans. Wirel. Commun.* **2023**, *early access*. [CrossRef]
25. Shen, K.; Yu, W. Fractional Programming for Communication Systems—Part II: Uplink Scheduling via Matching. *IEEE Trans. Signal Process.* **2018**, *66*, 2631–2644. [CrossRef]
26. Xu, C.; Clerckx, B.; Zhang, J. Multi-Antenna Joint Radar and Communications: Precoder Optimization and Weighted Sum-Rate vs Probing Power Tradeoff. *IEEE Access* **2020**, *8*, 173974–173982. [CrossRef]

27. Shen, K.; Yu, W. Fractional Programming for Communication Systems—Part I: Power Control and Beamforming. *IEEE Trans. Signal Process.* **2018**, *66*, 2616–2630. [CrossRef]
28. Grant, M.; Boyd, S. CVX: Matlab Software for Disciplined Convex Programming, Version 2.1. Available online: http://cvxr.com/cvx (accessed on 1 March 2014).
29. Chen, Y.; Ai, B.; Zhang, H.; Niu, Y.; Song, L.; Han, Z.; Vincent Poor, H. Reconfigurable Intelligent Surface Assisted Device-to-Device Communications. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 2792–2804. [CrossRef]
30. Guo, H.; Liang, Y.C.; Chen, J.; Larsson, E.G. Weighted Sum-Rate Maximization for Reconfigurable Intelligent Surface Aided Wireless Networks. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 3064–3076. [CrossRef]
31. Yu, X.; Xu, D.; Schober, R. MISO Wireless Communication Systems via Intelligent Reflecting Surfaces : (Invited Paper). In Proceedings of the IEEE/CIC International Conference on Communications in China (ICCC), Changchun, China, 11–13 August 2019; pp. 735–740. [CrossRef]
32. Madani, S.; Jog, S.; Lacruz, J.O.; Widmer, J.; Hassanieh, H. Practical null steering in millimeter wave networks. In Proceedings of the USENIX Symposium on Networked Systems Design and Implementation (NSDI), Virtual, 12–14 April 2021; pp. 903–921.
33. Rawat, D.B. Deep Transfer Learning for Physical Layer Security in Wireless Communication Systems. In Proceedings of the IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA), Virtual, 13–15 December 2021, pp. 289–296. [CrossRef]