Spatial Secrecy Spectral Efficiency Optimization Enabled by Reconfigurable Intelligent Surfaces

Konstantinos D. Katsanos and George C. Alexandropoulos
Department of Informatics and Telecommunications, School of Sciences,
National and Kapodistrian University of Athens, Panepistimiopolis Ilissia, 15784 Athens, Greece
emails: {kkatsan, alexandg}@di.uoa.gr

Abstract—Reconfigurable Intelligent Surfaces (RISs) constitute a strong candidate physical-layer technology for the 6-th Generation (6G) of wireless networks, offering new design degrees of freedom for efficiently addressing demanding performance objectives. In this paper, we consider a Multiple-Input Single-Output (MISO) physical-layer security system incorporating a reflective RIS to safeguard wireless communications between a legitimate transmitter and receiver under the presence of an eavesdropper. In contrast to current studies optimizing RISs for given positions of the legitimate and eavesdropping nodes, in this paper, we focus on devising RIS-enabled secrecy for given geographical areas of potential nodes' placement. We propose a novel secrecy metric, capturing the spatially averaged secrecy spectral efficiency, and present a joint design of the transmit digital beamforming and the RIS analog phase profile, which is realized via a combination of alternating optimization and minorization-maximization. The proposed framework bypasses the need for instantaneous knowledge of the eavesdropper's channel or position, and targets providing an RIS-boosted secure area of legitimate communications with a single configuration of the free parameters. Our simulation results showcase significant performance gains with the proposed secrecy scheme, even for cases where the eavesdropper shares similar pathloss attenuation with the legitimate receiver.

Index Terms—Reconfigurable intelligent surface, optimization, secrecy spectral efficiency, secure area of influence.

I. INTRODUCTION

The definition of the key capabilities and performance indicators of the sixth Generation (6G) of wireless networks is under the way, including demanding improvements in energy and cost efficiency, network capacity and reliability, as well localization, sensing, and trustworthiness [1]. Reconfigurable Intelligent Surfaces (RISs) are recently attracting remarkable research attention as a candidate physical-layer technology, through which a vast majority of diverse communication objectives can be offered, due to the beneficial feature of metasurfaces to dynamically control over-the-air signal propagation [2]. An RIS is an artificial planar structure with integrated electronic circuits [3], capable to manipulate, by efficient optimization, an incoming electromagnetic field in a wide variety of functionalities [4]. Physical-Layer Security (PLS), which can provide further secure guarantees especially when combined with cryptographic methods in the upper communication layers, constitutes one of the emerging wireless paradigms among the various considered RIS-enabled objectives that emerge for 6G networks [5].

According to numerous recent PLS studies, RISs are capable to provide significant performance gains with respect to secrecy performance metrics, such as secrecy rate [6]–[8] and secrecy outage probability [9], or the combination of them [10], [11]. However, all existing works rely on the assumption that the far-field locations of the receiving nodes are fixed, while it is evident that an RIS affects an area around it, as it was demonstrated in [8, Sec. IV.C] through exhaustive numerical evaluations. As an exception, the recent work [12] considers a secrecy rate maximization problem, under the assumption that Eve belongs to a suspicious area. Nevertheless, the problem of determining the secure area of influence of an RIS remains still an open challenge [13].

Motivated by the above, in this paper, we focus on investigating RIS-enabled secrecy performance under the consideration that all receivers belong to given geographical areas. Inspired by [14], we propose a novel secrecy metric, termed as spatial secrecy spectral efficiency, according to which the need for instantaneous knowledge of the receivers' exact positions is bypassed. Then, we formulate a challenging optimization problem aiming at maximizing the proposed metric, which targets the joint design of the transmit digital beamforming and the RIS phase configuration profile. Our simulation results demonstrate that, even for cases where the eavesdropper shares comparable pathloss with the legitimate receiver, the gains with the proposed design are significant.

Notations: Vectors and matrices are denoted by boldface lowercase and boldface capital letters, respectively. The transpose, conjugate, Hermitian transpose and inverse of $\mathbf{A}$ are denoted by $\mathbf{A}^T$, $\mathbf{A}^*$, $\mathbf{A}^H$, and $\mathbf{A}^{-1}$, respectively, while $\mathbf{I}_n$ and $\mathbf{0}_n$ ($n \geq 2$) are the $n \times n$ identity and zeros' matrices, respectively. $\mathrm{Tr}(\mathbf{A})$ and $\|\mathbf{a}\|_2$ represent $\mathbf{A}$'s trace and $\mathbf{a}$'s Euclidean norm, respectively, while notation $\mathbf{A} \succ \mathbf{0}$ ($\mathbf{A} \succeq \mathbf{0}$) means that the square matrix $\mathbf{A}$ is Hermitian positive definite (semi-definite). $[\mathbf{A}]_{i,j}$ is the (i,j)-th element of $\mathbf{A}$, $[\mathbf{a}]_i$ is $\mathbf{a}$'s i-th element, $\mathrm{diag}\{\mathbf{a}\}$ denotes a square diagonal matrix with $\mathbf{a}$'s elements in its main diagonal, and $\otimes$ stands for the Kronecker product. $\mathbb{C}$ represents the complex number set, $\jmath$ is the imaginary unit, $|a|$ and $\angle a$ denote the amplitude and the phase of the complex scalar a, respectively, and $\Re\{a\}$ its real part. $\mathbb{E}\{\cdot\}$ is the expectation operator and $\mathbf{x} \sim \mathcal{CN}(\mathbf{a}, \mathbf{A})$ indicates a complex Gaussian random vector with mean $\mathbf{a}$ and covariance matrix $\mathbf{A}$.

II. SYSTEM MODEL AND PROBLEM FORMULATION

The considered system model consists of a Base Station (BS) equipped with N antenna elements wishing to communicate in the downlink direction with a legitimate single-antenna Receiver (RX). In the latter's vicinity, there exists a single-antenna Eavesdropper (Eve). We assume that the direct links between the BS and the two receiving nodes are blocked. To overcome this situation, an RIS with L unit cells is deployed near the receivers' area. We assume throughout

this paper that partial Channel State Information (CSI) for both wireless links is available at the BS side [8]: the statistics of the channels $\mathbf{h}$, $\mathbf{g} \in \mathbb{C}^{L \times 1}$ (for RX and Eve, respectively) are known up to their second order. On the other hand, perfect CSI is available for the BS-RIS channel $\mathbf{H} \in \mathbb{C}^{L \times N}$.

A. Received Signal and Channel Models

To secure the confidentiality of the legitimate link, the BS applies the linear precoding vector $\mathbf{v} \in \mathbb{C}^{N \times 1}$ and jointly designs the RIS reflection vector (passive beamforming) $\boldsymbol{\phi} \triangleq [e^{j\theta_1} \ e^{j\theta_2} \ \cdots \ e^{j\theta_L}]^T \in \mathbb{C}^{L \times 1}$, where θ_ℓ ($\ell = 1, 2, \ldots, L$) denotes the effective phase shifting value at each ℓ-th RIS unit element. The baseband received signals y_{RX} and y_{E} at the RX and Eve can be mathematically expressed as follows:

$$y_i \triangleq \tilde{\mathbf{f}}^H \mathbf{v} s + n_i, \tag{1}$$

where $s \sim \mathcal{CN}(0,1)$ denotes the legitimate information symbol (in practice, it is chozen from a discrete modulation set) and $\tilde{\mathbf{f}}^H \triangleq \mathbf{f}_i^H \boldsymbol{\Phi} \mathbf{H}$ ($i = \mathrm{RX}$ and E) represents the end-to-end channel between the RX/Eve and BS via the RIS with $\boldsymbol{\Phi} \triangleq \mathrm{diag}\{\boldsymbol{\phi}\} \in \mathbb{C}^{L \times L}$. When $i = \mathrm{RX}$, $\mathbf{f}_i = \mathbf{h}$ implying the RIS-parametrized RX-BS channel, while $i = \mathrm{E}$ indicates the respective Eve-BS channel $\mathbf{f}_i = \mathbf{g}$. Finally, $n_i \sim \mathcal{CN}(0, \sigma^2)$ $\forall i$ stands for the Additive White Gaussian Noise (AWGN). It follows from (1) that the rate for each link is given by:

$$\mathcal{R}_i(\mathbf{v}, \boldsymbol{\phi}) \triangleq \log_2 \left(1 + \frac{|\tilde{\mathbf{f}}^H \mathbf{v}|^2}{\sigma^2} \right). \tag{2}$$

We further assume that the channels $\mathbf{h}$ and $\mathbf{g}$ undergo Rician fading with Rician factor K_r; we study the difficult secrecy case where RX and Eve are placed such that they share similar pathloss properties. Considering a 3D coordinate system for the nodes' placement (i.e., BS, RIS, RX, and Eve), and taking into account that both the BS and RIS possess Uniform Planar Arrays (UPAs), the channel between the RX/Eve and RIS can be expressed as follows:

$$\mathbf{f} = \sqrt{\kappa_i} \left(\sqrt{\frac{K_r}{K_r + 1}} \mathbf{f}^{\mathrm{LOS}} + \sqrt{\frac{1}{K_r + 1}} \mathbf{f}^{\mathrm{NLOS}} \right), \tag{3}$$

where $\kappa_i \triangleq \mathrm{PL}_0 \left(\frac{D_{\mathrm{RIS},i}}{d_0} \right)^{-\alpha_{\mathrm{RIS},i}}$ with $\alpha_{\mathrm{RIS},i}$ denoting the pathloss exponent of the ith link, PL_0 is the pathloss at the reference distance $d_0 = 1\mathrm{m}$, and $D_{\mathrm{RIS},i} = \|\mathbf{p}_{\mathrm{RIS}} - \mathbf{p}_i\|$ is the distance between the RIS and the reception node i with $\mathbf{p}_{\mathrm{RIS}} \triangleq [x_{\mathrm{RIS}}, y_{\mathrm{RIS}}, z_{\mathrm{RIS}}]^T$, $\mathbf{p}_{\mathrm{RX}} \triangleq [x_{\mathrm{RX}}, y_{\mathrm{RX}}, z_{\mathrm{RX}}]^T$ ($i = \mathrm{RX}$), and $\mathbf{p}_{\mathrm{E}} \triangleq [x_{\mathrm{E}}, y_{\mathrm{E}}, z_{\mathrm{E}}]^T$ ($i = \mathrm{E}$) indicating the corresponding position vectors. The Line-Of-Sight (LOS) vector $\mathbf{f}^{\mathrm{LOS}}$ in (3) is the steering vector at the RIS, which is obtained as $\mathbf{f}^{\mathrm{LOS}} \triangleq \mathbf{a}_{L_v}(\theta_{\mathbf{f}}, \varphi_{\mathbf{f}}) \otimes \mathbf{a}_{L_h}(\theta_{\mathbf{f}}, \varphi_{\mathbf{f}})$ for the case of an RIS with L_v vertical and L_h horizontal elements, such that $L = L_v \times L_h$, where $\theta_{\mathbf{f}}$ and $\varphi_{\mathbf{f}}$ denote the elevation and azimuth angles of departure (AoD) with respect to the RIS, respectively. Assuming that the RIS is deployed parallel to the yz plane, $\theta_{\mathbf{f}} = \arccos(\frac{x_{\mathrm{RIS}} - x_i}{D_{\mathrm{RIS},i}})$ and $\varphi_{\mathbf{f}} = \arctan(\frac{y_{\mathrm{RIS}} - y_i}{z_{\mathrm{RIS}} - z_i})$.

For this case, the ℓ-th entry of the vector $\mathbf{f}^{\mathrm{LOS}}$ can be obtained as $[\mathbf{f}^{\mathrm{LOS}}]_\ell = \frac{1}{\sqrt{L}} e^{j2\pi \frac{d}{\lambda_c} \xi_\ell}$ with ξ_ℓ given by:

$$\xi_\ell \triangleq \left(\left\lfloor \frac{\ell - 1}{L_h} \right\rfloor \sin \theta_{\mathbf{f}} \cos \varphi_{\mathbf{f}} \right.$$
$$\left. + \left(\ell - \left\lfloor \frac{\ell - 1}{L_h} \right\rfloor L_h - 1 \right) \sin \theta_{\mathbf{f}} \sin \varphi_{\mathbf{f}} \right), \tag{4}$$

with d and λ_c being the RIS's element spacing and the wavelength, respectively. Finally, in (3), the Non-LOS (NLOS) channel component is modeled as $[\mathbf{f}^{\mathrm{NLOS}}]_\ell \sim \mathcal{CN}(0,1)$.

B. Problem Formulation

Consider that RX and Eve are both located within a given geographical area $\mathcal{S} \triangleq \mathcal{S}_{\mathrm{RX}} \cup \mathcal{S}_{\mathrm{E}}$ with $\mathcal{S}_{\mathrm{RX}} \cap \mathcal{S}_{\mathrm{E}} = \emptyset$, where $\mathcal{S}_{\mathrm{RX}}$ denotes the area where the RX can be located and $\mathcal{S}_{\mathrm{E}}$ indicates the respective area for Eve. One example where this assumption of disjoint adjacent areas can be realized is the placement of the RX and Eve in two adjacent rooms in indoor environments, with the latter node targeting to eavesdrop legitimate communications. The extension to overlapping areas $\mathcal{S}_{\mathrm{RX}}$ and $\mathcal{S}_{\mathrm{E}}$ will be considered in future work. We further assume that each point of the area $\mathcal{S}$ is associated with a Probability Density Function (PDF) $u(\mathcal{S})$, which equals the joint probability of presence for RX and Eve in locations within $\mathcal{S}_{\mathrm{RX}}$ and $\mathcal{S}_{\mathrm{E}}$, respectively. Aiming at securing communications for each placement of RX within $\mathcal{S}_{\mathrm{RX}}$ and Eve inside $\mathcal{S}_{\mathrm{E}}$, we define the spatial secrecy spectral efficiency as the following spatially averaged metric:

$$\mathcal{R}_{\mathcal{S}} \triangleq \mathbb{E}_{\mathbf{h}, \mathbf{g}} \left\{ \int_{\mathcal{S}_{\mathrm{RX}}} \int_{\mathcal{S}_{\mathrm{E}}} u(\mathcal{X}, \mathcal{Y}) \left[\mathcal{R}_{\mathrm{RX}} - \mathcal{R}_{\mathrm{E}} \right]^+ d\mathcal{X} d\mathcal{Y} \right\}. \tag{5}$$

We next capitalize on the assumption of disjoint $\mathcal{S}_{\mathrm{RX}}$ and $\mathcal{S}_{\mathrm{E}}$ (which are assumed as 2D geographical areas for simplicity) to simplify $\mathcal{R}_{\mathcal{S}}$'s expression for its upcoming optimization.

Proposition 1. *For disjoint sets $\mathcal{S}_{\mathrm{RX}}$ and $\mathcal{S}_{\mathrm{E}}$ and independent events $\mathbf{p}_{\mathrm{RX}} \in \mathcal{S}_{\mathrm{RX}}$ and $\mathbf{p}_{\mathrm{E}} \in \mathcal{S}_{\mathrm{E}}$, where for each $\mathbf{p}_{\mathrm{RX}}$ and $\mathbf{p}_{\mathrm{E}}$ holds $z_{\mathrm{RX}} = z_{\mathrm{E}} = z$, (5) is re-written as:*

$$\mathcal{R}_{\mathcal{S}} = \mathcal{R}_{\mathcal{S}_{\mathrm{RX}}} - \mathcal{R}_{\mathcal{S}_{\mathrm{E}}}, \tag{6}$$

where $\mathcal{R}_{\mathcal{S}_{\mathrm{RX}}} \triangleq \mathbb{E}_{\mathbf{h}} \left\{ \int_{\mathcal{S}_{\mathrm{RX}}} u_{\mathrm{RX}}(x_{\mathrm{RX}}, y_{\mathrm{RX}}) \mathcal{R}_{\mathrm{RX}} dx_{\mathrm{RX}} dy_{\mathrm{RX}} \right\}$ and $\mathcal{R}_{\mathcal{S}_{\mathrm{E}}} \triangleq \mathbb{E}_{\mathbf{g}} \left\{ \int_{\mathcal{S}_{\mathrm{E}}} u_{\mathrm{E}}(x_{\mathrm{E}}, y_{\mathrm{E}}) \mathcal{R}_{\mathrm{E}} dx_{\mathrm{E}} dy_{\mathrm{E}} \right\}$ with notations $u_{\mathrm{RX}}(\cdot, \cdot)$ and $u_{\mathrm{E}}(\cdot, \cdot)$ representing the 2D spatial PDFs of RX and Eve, respectively.

Proof: From the previous assumptions, it can be deduced $u(\mathcal{S}) = u_{\mathrm{RX}}(\mathcal{S}_{\mathrm{RX}}) u_{\mathrm{E}}(\mathcal{S}_{\mathrm{E}})$. It also holds that $\int_{\mathcal{S}_{\mathrm{RX}}} u_{\mathrm{RX}}(\mathcal{X}) d\mathcal{X} = 1$ and $\int_{\mathcal{S}_{\mathrm{E}}} u_{\mathrm{RX}}(\mathcal{Y}) d\mathcal{Y} = 0$. Since the integrand function is non-negative, Tonelli's theorem [15] can be applied, which completes the proof. ∎

It can be seen from (6) that $\mathcal{R}_{\mathcal{S}}$ depends on $\mathbf{v}$ and $\boldsymbol{\phi}$. We now focus on the following design optimization problem:

$$\mathcal{OP} : \max_{\mathbf{v}, \boldsymbol{\phi}} \quad \mathcal{R}_{\mathcal{S}}(\mathbf{v}, \boldsymbol{\phi})$$
$$\text{s.t.} \quad \|\mathbf{v}\|_2^2 \leq P_T,$$
$$|\phi_\ell| = 1 \ \forall \ell = 1, 2, \ldots, L,$$

where P_T in the first constraint is the BS's transmit power whose value should not be exceeded during any transmission

slot, and the second constraint guarantees the unit-modulus property of each RIS's element. $\mathcal{OP}$ is a challenging non-convex optimization problem due to the coupling variables $\mathbf{v}$ and $\boldsymbol{\phi}$ and the double integration operations over the considered geographical areas $\mathcal{S}_{\mathrm{RX}}$ and $\mathcal{S}_{\mathrm{E}}$.

III. SPATIAL SECRECY EFFICIENCY OPTIMIZATION

We first approximate the objective function $\mathcal{R}_{\mathcal{S}}$, as follows. We assume, without loss of generality, that the presence of both RX's and Eve's in $\mathcal{S}_{\mathrm{RX}}$ and $\mathcal{S}_{\mathrm{E}}$, respectively, follows a uniform distribution in their respective areas. Based on this assumption, the resulting 2D spatial PDFs become $u_{\mathrm{RX}}(x_{\mathrm{RX}}, y_{\mathrm{RX}}) = \frac{1}{\mathcal{S}_{\mathrm{RX}}}$ and $u_{\mathrm{E}}(x_{\mathrm{E}}, y_{\mathrm{E}}) = \frac{1}{\mathcal{S}_{\mathrm{E}}}$. Hence, $\mathcal{OP}$'s objective function can be simplified to[1]:

$$
\mathcal{R}_{\mathcal{S}}(\mathbf{v}, \boldsymbol{\phi}) = \frac{1}{\mathcal{S}_{\mathrm{RX}}} \int_{\mathcal{S}_{\mathrm{RX}}} \mathbb{E}_{\mathbf{h}}\left\{\mathcal{R}_{\mathrm{RX}}\right\} dx_{\mathrm{RX}} dy_{\mathrm{RX}} \\
- \frac{1}{\mathcal{S}_{\mathrm{E}}} \int_{\mathcal{S}_{\mathrm{E}}} \mathbb{E}_{\mathbf{g}}\left\{\mathcal{R}_{\mathrm{E}}\right\} dx_{\mathrm{E}} dy_{\mathrm{E}}, \tag{7}
$$

where the linearity of the integration and expectation operations was used. The considered spatial secrecy spectral efficiency can be further simplified via the following corollary.

Corollary 1. *First, consider the following definitions:*

$$
\bar{\mathbf{f}} \triangleq \sqrt{\kappa_i} \sqrt{\frac{K_r}{1+K_r}} \mathbf{f}^{\mathrm{LOS}}, \quad \mathbf{M}_{\mathbf{f}} \triangleq \frac{\kappa_i}{1+K_r} \mathbf{I}_L. \tag{8}
$$

Moreover, $\bar{\mathbf{f}}$ is the mean of channel $\mathbf{f}$, according to the adopted Rician channel model (based on (3)), and $\mathbf{M}_{\mathbf{f}}$ is its covariance matrix (with $\mathbf{M}_{\mathbf{f}} \succ \mathbf{0}$), i.e., $\mathbf{f} \sim \mathcal{CN}(\bar{\mathbf{f}}, \mathbf{M}_{\mathbf{f}})$. Let, also, the matrix $\mathbf{J}_i \in \mathbb{C}^{L,L}$ be defined as follows:

$$
\mathbf{J}_i \triangleq \int_{\mathcal{S}_i} \left(\mathbf{M}_{\mathbf{f}} + \bar{\mathbf{f}}\bar{\mathbf{f}}^H\right) dx_i dy_i. \tag{9}
$$

Then, the average spatial secrecy spectral efficiency, can be approximated (having the same lower and upper bounds) as:

$$
\mathcal{R}_{\mathcal{S}} \approx \tilde{\mathcal{R}}_{\mathcal{S}}(\mathbf{v}, \boldsymbol{\phi}) \triangleq \log_2 \left(\frac{1 + \frac{\mathbf{v}^H \mathbf{H}^H \boldsymbol{\Phi}^H \mathbf{J}_{\mathrm{RX}} \boldsymbol{\Phi} \mathbf{H} \mathbf{v}}{\sigma^2 \mathcal{S}_{\mathrm{RX}}}}{1 + \frac{\mathbf{v}^H \mathbf{H}^H \boldsymbol{\Phi}^H \mathbf{J}_{\mathrm{E}} \boldsymbol{\Phi} \mathbf{H} \mathbf{v}}{\sigma^2 \mathcal{S}_{\mathrm{E}}}}\right). \tag{10}
$$

Proof: Expression (10) can be derived using straightforward algebraic manipulations and [16, Lemma 1]. The detailed steps are omitted for brevity. ∎

The maximization of (10) with respect to $\mathbf{v}$ and $\boldsymbol{\phi}$ remains a non-convex optimization problem due to the coupling of the optimization variables and the non-convex unit-modulus constraints. However, it can be efficiently solved by adopting Alternating Optimization (AO), i.e.: iterative optimizations keeping one variable fixed to obtain an expression for the other one, until a convergence criterion is satisfied, as described in the following subsections.

A. Optimization over the Active BS Beamformer $\mathbf{v}$

The maximization problem with respect to $\mathbf{v}$ is a fractional QCQP problem with a convex constraint, which can be optimally solved according to the following lemma.

---

[1]It is noted that the operation $[\cdot]^+$ is henceforth omitted since it does not affect the derivation of $\mathbf{v}$ and $\boldsymbol{\phi}$. This deduces from the fact that our design target is to provide positive secrecy rates.

Lemma 1. *The optimal expression for the linear precoding vector $\mathbf{v}$ is given by:*

$$
\mathbf{v}^{\mathrm{opt}} = \sqrt{P_T} \mathbf{u}_{\max}\left(\mathbf{P}_{\mathrm{E}}^{-1} \mathbf{P}_{\mathrm{RX}}\right), \tag{11}
$$

where $\mathbf{P}_i \triangleq \mathbf{I}_N + \frac{P_T}{\sigma^2 \mathcal{S}_i} \mathbf{H}^H \boldsymbol{\Phi}^H \mathbf{J}_i \boldsymbol{\Phi} \mathbf{H}$, with $i \in \{\mathrm{RX}, \mathrm{E}\}$, and $\mathbf{u}_{\max}(\mathbf{A})$ denotes the eigenvector corresponding to the largest eigenvalue of matrix $\mathbf{A}$.

Proof: We first note that the logarithmic operation can be omitted because $\log_2(\cdot)$ is a non-decreasing function. Then, it can be readily verified that the optimal $\mathbf{v}$ satisfies the constraint $\|\mathbf{v}\|^2 \leq P_T$ with equality. Based on these two key properties, the optimization problem reduces to a generalized eigenvalue problem whose optimal solution is given by (11). ∎

B. Optimization over the Passive RIS Beamformer $\boldsymbol{\phi}$

Under the assumption that $\mathbf{v}$ is fixed, it can be shown after some algebraic manipulations that $\tilde{\mathcal{R}}_{\mathcal{S}}(\cdot)$ reduces to:

$$
\tilde{\mathcal{R}}_{\mathcal{S}}(\boldsymbol{\phi}) = \frac{\boldsymbol{\phi}^H \mathbf{Q}_{\mathrm{RX}} \boldsymbol{\phi}}{\boldsymbol{\phi}^H \mathbf{Q}_{\mathrm{E}} \boldsymbol{\phi}}, \tag{12}
$$

with $\mathbf{Q}_i \triangleq \frac{1}{L} \mathbf{I}_L + \frac{1}{\sigma^2 \mathcal{S}_i} \mathrm{diag}\{\tilde{\mathbf{v}}\}^H \mathbf{J}_i \, \mathrm{diag}\{\tilde{\mathbf{v}}\}$, for $i \in \{\mathrm{RX}, \mathrm{E}\}$, where $\tilde{\mathbf{v}} \triangleq \mathbf{H}\mathbf{v}$ and the property $\boldsymbol{\phi}^H \boldsymbol{\phi} = L$ has been invoked. Then, based on the Majorization-Minimization (MM) technique [17], it can be shown that the objective function can be minorized around a feasible point $\boldsymbol{\phi}_t$ by:

$$
g(\boldsymbol{\phi}|\boldsymbol{\phi}_t) = 2 \frac{\Re\{\boldsymbol{\phi}_t^H \mathbf{Q}_{\mathrm{RX}} \boldsymbol{\phi}_t\}}{\boldsymbol{\phi}_t^H \mathbf{Q}_{\mathrm{E}} \boldsymbol{\phi}_t} - \frac{\boldsymbol{\phi}_t^H \mathbf{Q}_{\mathrm{RX}} \boldsymbol{\phi}_t}{(\boldsymbol{\phi}_t^H \mathbf{Q}_{\mathrm{E}} \boldsymbol{\phi}_t)^2} \Big\{ \boldsymbol{\phi}^H \mathrm{Tr}(\mathbf{Q}_{\mathrm{E}}) \boldsymbol{\phi} \\
+ 2 \Re\{\boldsymbol{\phi}_t^H \left[\mathbf{Q}_{\mathrm{E}} - \mathrm{Tr}(\mathbf{Q}_{\mathrm{E}}) \mathbf{I}_L\right] \boldsymbol{\phi}\} \Big\}, \tag{13}
$$

where $\mathrm{Tr}(\mathbf{Q}_{\mathrm{E}}) > 0$ since $\mathbf{Q}_{\mathrm{E}} \succ \mathbf{0}$. Then, at the inner iteration $(t+1)$ of the MM-based algorithm, it can be shown that $\boldsymbol{\phi}_{t+1} = \exp\left\{\jmath \angle \tilde{\boldsymbol{\phi}}\right\}$, where $\tilde{\boldsymbol{\phi}}$ is given by:

$$
\tilde{\boldsymbol{\phi}} = \frac{\mathbf{Q}_{\mathrm{RX}} \boldsymbol{\phi}_t}{\boldsymbol{\phi}_t^H \mathbf{Q}_{\mathrm{E}} \boldsymbol{\phi}_t} - \frac{\boldsymbol{\phi}_t^H \mathbf{Q}_{\mathrm{RX}} \boldsymbol{\phi}_t}{(\boldsymbol{\phi}_t^H \mathbf{Q}_{\mathrm{E}} \boldsymbol{\phi}_t)^2} \left(\mathbf{Q}_{\mathrm{E}} - \mathrm{Tr}(\mathbf{Q}_{\mathrm{E}}) \mathbf{I}_L\right) \boldsymbol{\phi}_t. \tag{14}
$$

IV. NUMERICAL RESULTS AND DISCUSSION

In this section, we present our performance evaluation results for the spatial secrecy spectral efficiency metric for the considered RIS-enabled MISO communication system.

A. Simulation Setup

We have evaluated the achievable rates of the legitimate and eavesdropping links using expression (2) for RX and Eve. We have used the proposed scheme in Section III for the design of the linear precoding vector and the passive beamforming vector for the RIS configuration. In our simulations, all nodes were considered placed on a 3D coordinate system, whose exact locations are represented by the triad (x, y, z) according to the orthogonal Cartesian coordinate system. We have assumed that the BS is located at the point $(0, 0, 7.5)\,m$, while the RIS at the position $(0, 50, 3)\,m$. As studied throughout the paper, both receivers are not restricted to fixed positions, but they can be uniformly located inside their respective $\mathcal{S}_i$ areas. Specifically, we have considered that $\mathcal{S}_{\mathrm{RX}}$ is centered around the point $(-15, 30)\,m$ on the
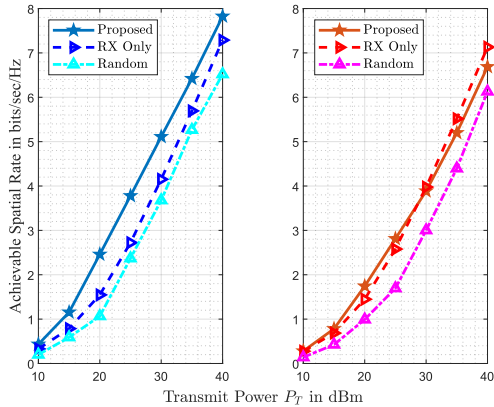
Fig. 1: Maximum achievable spatial rates in bits/sec/Hz at the legitimate RX (left) and the eavesdropper Eve (right) versus the transmit power P_T in dBm, considering a BS with $N = 16$ antenna elements and an RIS with $L = 150$ unit elements.

xy plane, having a width of $24\,m$ and length $15\,m$. Similarly, the center of Eve's area was fixed at the position $(15, 27.5)\,m$ sharing the same width and length as $\mathcal{S}_{\mathrm{RX}}$. This consideration results in areas sharing similar pathloss attenuation properties, serving as a worst-case scenario. It was also assumed that $z = 1.5\,m$. The channels **h** and **g** were modeled according to (3) with $\mathrm{PL}_0 = -30$ dB, and the pathloss exponents were set as $\alpha_{\mathrm{RIS,i}} = 2.2$. For the channel matrix **H** between the BS and RIS, we used the Rician fading model with the same pathloss properties. In addition, we have used the following setting for the system parameters: $N = 16$, $L = 150$, $K_r = 13.2$, $\sigma^2 = -105$ dBm, and the optimization algorithmic threshold ϵ for the convergence criterion was considered equal to 10^{-5}. For all performance evaluation results, we have used 100 independent Monte Carlo realizations. Moreover, the matrices $\mathbf{J}_i$'a defined in (9) were computed via numerical integration over the $\mathcal{S}_i$ areas. For comparison purposes, we have implemented two baseline schemes: *i)* the "Random" scheme including random linear precoding and passive beamforming vectors; and *ii)* the "RX Only" scheme according to which we maximize the spatial spectral efficiency only for RX (defined analogously to $\mathcal{R}_{\mathcal{S}}$).

B. Rate Performance vs. the Transmit Power

We first investigate the achievable spatial secrecy spectral efficiency as a function of the transmit power P_T. In particular, we have evaluated the achievable rates for RX and Eve for every position in the considered $\mathcal{S}_i$ areas, and illustrate their maximum values for all schemes in Fig. 1. It can be observed that, as expected, the rate exhibits a non-decreasing trend as the transmit power increases for both links, while the values achieved for the legitimate link are higher than those for the eavesdropping link. Moreover, it is shown that the gains in the legitimate RX's rate, with respect to Eve's achievable values, are larger for the case where the proposed metric and optimized design are adopted, in contrast to the other benchmark schemes. For instance, in the low SNR regime, this difference is small, whereas for higher SNR values (specifically, $P_T \geq 35$ dBm), it reaches its

maximum difference of about 1.5 bps/Hz. This behavior can be justified by the fact that the proposed metric is dedicated on maximizing the difference between RX's and Eve's rate, while the other two schemes do not emphasize on improving their deviation. It needs to be commented, though, that the aforementioned difference between RX's and Eve's rate is quite small. However, for the considered simulation setup, the areas $\mathcal{S}_{\mathrm{RX}}$ and $\mathcal{S}_{\mathrm{E}}$ yield comparable pathloss-based properties between the two receivers, which are encapsulated into the $\mathbf{J}_i$ matrices, where all distance-dependent characteristics are integrated on average. Nevertheless, even for such cases where there do not exist direct links from the BS to both receiving nodes, the optimized RIS becomes capable to provide larger rates for the legitimate RX.

C. Spatial Rate Performance Gain

In Fig. 2, we study the impact of the RIS at the entire $\mathcal{S}_i$ regions, by evaluating the gain of the two optimized schemes with respect to the random setting scheme, as described in Section IV-A. Specifically, by considering $P_T = 35$ dBm, the gains between the "Random" and the "RX Only" schemes in the achievable rates at the legitimate RX and Eve are illustrated in Figs. 2a and 2b, respectively, while Figs. 2c and 2d depict the respective rate gains between the "Random" and proposed schemes. It can be observed from all subfigures that there exist regions where the RIS enhances or degrades the rate at both receiving nodes. In addition, it is shown that the rate gains via both optimized schemes are more pronounced at the RX rather than at Eve; this is evident from the more yellow-colored areas indicating larger gains with the optimized schemes. Especially for the case of optimizing the proposed objective, the achievable gains are larger, yielding about 10% larger gains between RX and Eve, as observed from Figs. 2c and 2d. On the other hand, the corresponding gains when optimizing the RIS with respect to "RX only," span the same range of improvement, exhibiting a minimum gain below 14% and maximum gain slightly above 26%. Finally, it is inferred from Fig. 2d that the largest part of S_{E} is degraded, apart from the sub-region where there exists a strong reflective beam. This behavior is justified by the fact that this sub-region is the most distant sub-area from the RIS, according to the described placement. It, hence, yields smaller performance gains in terms of degrading Eve's performance.

V. CONCLUSION

In this paper, we studied RIS-enabled MISO communication systems, where a passive reflective RIS was deployed to extend the coverage of a legitimate link. We proposed a novel physical-layer security metric, which characterizes the spatially averaged secrecy spectral efficiency over a targeted geographical area where both the legitimate receiver and a potential eavesdropper can be located. Focusing on maximizing this metric, we investigated the joint optimization of the BS's linear precoder and the RIS's reflective beamformer. It was demonstrated that the proposed solution yields a fixed joint beamforming design for the entire area under investigation, which is capable of safeguarding MISO communications even for cases where the eavesdropper experiences similar pathloss attenuation with the legitimate receiver.
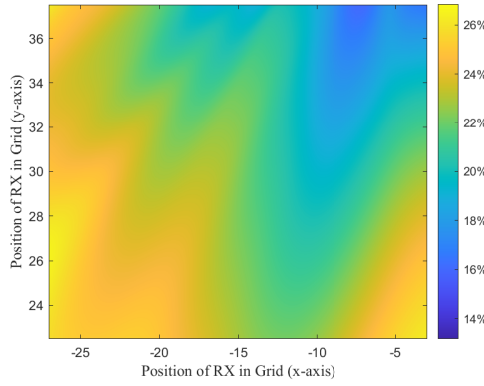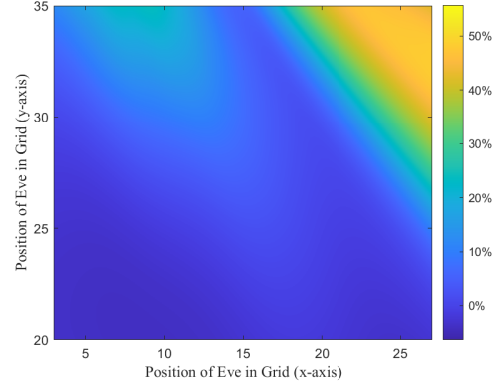
(a) Spatial rate gain at RX between the random configuration and the "RX Only" scheme.
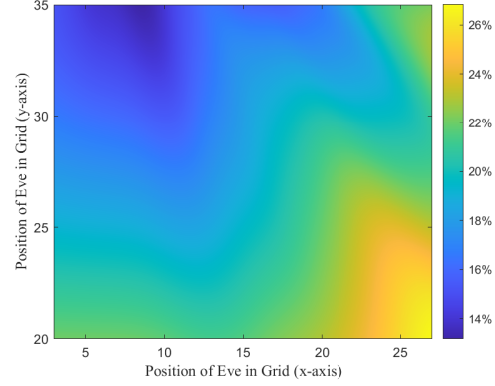
(b) Spatial rate gain at Eve between the random configuration and the "RX Only" scheme.
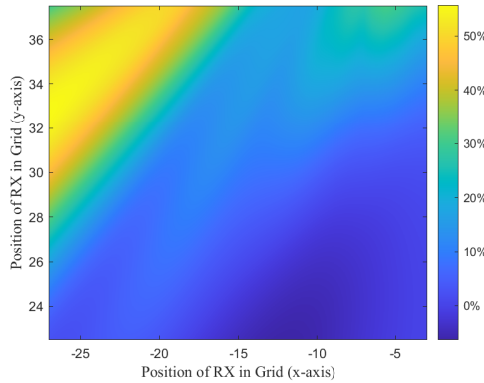
(c) Spatial rate gain at RX between the random configuration and the proposed secrecy spatial rate maximization scheme.

(d) Spatial rate gain at Eve between the random configuration and the proposed secrecy spatial rate maximization scheme.

Fig. 2: Gain in percentage in the achievable spatial rates at the legitimate RX and Eve between the random BS/RIS beamforming configuration and the proposed optimized schemes for the transmit power level $P_T = 35$ dBm.

REFERENCES

[1] W. Saad *et al.*, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, Jun. 2020.

[2] C. Huang *et al.*, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, Aug. 2019.

[3] G. C. Alexandropoulos *et al.*, "Reconfigurable intelligent surfaces and metamaterials: The potential of wave propagation control for 6G wireless communications," *IEEE ComSoc TCCN Newslett.*, vol. 6, no. 1, pp. 25–37, Jun. 2020.

[4] M. Di Renzo *et al.*, "Smart radio environments empowered by AI reconfigurable meta-surfaces: An idea whose time has come," *EURASIP J. Wireless Commun. Netw.*, vol. 129, pp. 1–20, May 2019.

[5] J. Xu *et al.*, "Reconfiguring wireless environments via intelligent surfaces for 6G: reflection, modulation, and security," *Sci. China Inf. Sci.*, vol. 66, no. 3, p. 130304, Mar. 2023.

[6] G. C. Alexandropoulos *et al.*, "Safeguarding MIMO communications with reconfigurable metasurfaces and artificial noise," in *Proc. IEEE ICC*, Montreal Canada, Jun. 2021, pp. 1–6.

[7] K. D. Katsanos and G. C. Alexandropoulos, "Secrecy spectral efficiency optimization in RIS-enabled MIMO communication systems," in *Proc. VLSI-SoC*, Patras, Greece, Oct. 2022, pp. 1–6.

[8] G. C. Alexandropoulos *et al.*, "Counteracting eavesdropper attacks through reconfigurable intelligent surfaces: A new threat model and secrecy rate optimization," *IEEE Open J. Commun. Soc.*, 2023, early access.

[9] L. Yang *et al.*, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12 296–12 300, Oct. 2020.

[10] J. Zhang *et al.*, "Physical layer security enhancement with reconfigurable intelligent surface-aided networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3480–3495, May 2021.

[11] Z. Li *et al.*, "Outage constrained secrecy rate maximization of intelligent reflecting surface aided transmission," in *Proc. IEEE ICC*, Montreal, Canada, Jun. 2021, pp. 1–6.

[12] J. Bai *et al.*, "Robust IRS-aided secrecy transmission with location optimization," *IEEE Trans. Commun.*, vol. 70, no. 9, pp. 6149–6163, Sep. 2022.

[13] G. C. Alexandropoulos *et al.*, "RIS-enabled smart wireless environments: Deployment scenarios, network architecture, bandwidth and area of influence," *EURASIP J. Wireless Commun. Netw.*, 2023.

[14] L. Mucchi *et al.*, "A new metric for measuring the security of an environment: The secrecy pressure," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3416–3430, May 2017.

[15] H. L. Royden and P. Fitzpatrick, *Real analysis*. Macmillan New York, 1988, vol. 32.

[16] H.-M. Wang *et al.*, "Multiple antennas secure transmission under pilot spoofing and jamming attack," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 860–876, Apr. 2018.

[17] Y. Sun *et al.*, "Majorization-minimization algorithms in signal processing, communications, and machine learning," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 794–816, Feb. 2016.