Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Correspondence:

XL-RIS empowered near-field physical layer security against jamming and eavesdropping attacks*

Zelong CUI[1], Jun LIU[1], Gang YANG‡[1,2]

[1]*National Key Laboratory of Wireless Communications, University of Electronic Science and Technology of China, Chengdu 611731, China*

[2]*Shenzhen Institute for Advanced Study, University of Electronic Science and Technology of China, Shenzhen 518110, China*

E-mail: zlcui@std.uestc.edu.cn; junl@std.uestc.edu.cn; yanggang@uestc.edu.cn

Received June 4, 2024; Revision accepted Oct. 10, 2024; Crosschecked Nov. 28, 2024

https://doi.org/10.1631/FITEE.2400477

Wireless communication is vulnerable to malicious jamming and eavesdropping attacks due to the broadcast nature of wireless channels. An extremely-large-scale reconfigurable intelligent surface (XL-RIS) demonstrates its abilities to enhance the physical layer security (PLS) and compensate for the severe path loss. We investigate an XL-RIS empowered near-field PLS communication system against jamming and eavesdropping attacks with the help of artificial noise (AN). To maximize the secrecy capacity, we propose an alternating optimization (AO) based algorithm to jointly optimize the beamformers at the base station (BS) and the reflection coefficient matrix at the XL-RIS, subject to the BS's maximum transmit power and the XL-RIS's unit-modulus constraints. For the beamforming and AN design at the BS, auxiliary variables are introduced to reformulate the subproblem into a more tractable problem, which is solved by the proposed successive convex approximation (SCA) based algorithm. For the reflection coefficient matrix design at the XL-RIS, a manifold optimization (MO) based algorithm is proposed to address the challenge of large-scale variables and unit-modulus constraints. Numerical results show that XL-RIS can ensure secure communication even if the eavesdropper is located at the same direction as the legitimate user and closer to the XL-RIS.

1 Introduction

The sixth-generation (6G) networks start a new era of wireless communications with high speed, ultra-low latency, massive access, and strong security, which will support ubiquitous connectivity for various devices, such as mobile terminals, industrial equipment, wearable devices, and autonomous driving vehicles (Nguyen et al., 2021). Specifically, many applications involve sensitive information exchange, so it is crucial to ensure transmission security against malicious attacks, such as eavesdropping and jamming. Several technologies have been used to resist these attacks, such as beamforming, relay, frequency hopping (Liang et al., 2018), and AN (Yan et al., 2018).

However, the frequency-hopping technology consumes extra spectrum resources, and AN and relay consume additional power (Sun et al., 2022b). To further enhance the secure communication against

‡ Corresponding author

* Project supported by the Shenzhen Science and Technology Program (Nos. JCYJ20220530164814032 and JCYJ20220818103201004) and the National Natural Science Foundation of China (No. 62071093)

Electronic supplementary materials: The online version of this article (https://doi.org/10.1631/FITEE.2400477) contains supplementary materials, which are available to authorized users

ORCID: Gang YANG, https://orcid.org/0000-0002-3959-4761

jamming and eavesdropping attacks, reconfigurable intelligent surface (RIS) has been studied recently (Cheng et al., 2023; Zhao et al., 2023). RIS is composed of a large number of low-cost reflection elements and consumes lower power. RIS can reconfigure an electromagnetic propagation environment (Pan et al., 2020) and enhance the secure communication. Liu J et al. (2024a) employed a RIS to enhance the desired signals and suppress the jamming signals with the imperfect jammer-related channel state information (CSI). Sun et al. (2022b) proposed an AO-based algorithm to jointly design the received decoder at the user, the digital precoder, and AN at the BS, as well as the analog precoder at the RIS, to combat jamming and eavesdropping attacks with the imperfect CSI. Ma et al. (2024) further introduced a hybrid active–passive RIS into a secure communication system to combat jamming and eavesdropping attacks. The hybrid RIS, which integrates active and passive elements, provides a balance between cost and performance, enabling it to enhance desired signals while suppressing jamming or leakage signals.

However, there are some weaknesses in the existing studies on RIS-assisted PLS communication systems. First, with the increase of frequency in wireless networks and the limited number of reflection elements, the performance enhancement will be heavily restricted due to the double-fading effect (di Renzo et al., 2020). Second, these studies focus mainly on the planar-wave propagation in far-field communication systems, resulting in limited secrecy capacity for scenarios with spatial correlation. When the eavesdropper and the legitimate user are correlated in the angular domain, the secrecy capacity will decrease dramatically under the planar-wave model.

Recently, XL-RIS was studied. Liu J et al. (2024b) employed XL-RIS for covert transmission in the near-field region. The large-scale low-cost reflection elements can expand the array aperture of XL-RIS, thus enhancing the reflected signals significantly. With the increase of array aperture and operating frequency, it becomes inevitable that wireless communication systems operate in the near-field region. The Rayleigh distance is commonly used to distinguish between the near-field and far-field regions; it is given by $\frac{2D^2}{\lambda}$, with D and λ denoting the array aperture and the wavelength, respectively (Liu YW et al., 2023). The characteristics of electromagnetic propagation in the near field are modeled as a spherical-wave channel model. Compared with the planar-wave model, the spherical-wave channel model depends on both angular and distance, introducing the extra distance degree of freedom in the propagation characteristics (Liu YW et al., 2023). Hence, in contrast to the far-field channel model, the near-field channel model can ensure secure communication even when the legitimate user and the eavesdropper are highly correlated in the angular domain (Zhang et al., 2024).

To the best of our knowledge, the XL-RIS empowered near-field PLS communication system against jamming and eavesdropping attacks has not been studied yet in the literature. Existing studies focus on the RIS-assisted far-field PLS communication system against jamming and eavesdropping attacks (Sun et al., 2022b; Ma et al., 2024). In this study, XL-RIS and AN are introduced to improve the secrecy capacity of the system. The main contributions are as follows:

1. We study an XL-RIS empowered near-field PLS communication system. An optimization problem is formulated to maximize the secrecy capacity of the communication system, subject to the transmit power and unit-modulus constraints. This problem involves coupled variables and unit-modulus constraints, making it challenging to solve.

2. An AO-based algorithm is proposed to solve the optimization problem. For the beamforming and AN design at the BS, we propose an SCA-based algorithm. For the reflection coefficient matrix design at the XL-RIS, an MO-based algorithm is proposed to address the other subproblems with large-scale variables and unit-modulus constraints.

3. Numerical results show that: (1) XL-RIS can ensure secure communication even if the eavesdropper is located at the same direction as the legitimate user and closer to the XL-RIS, which cannot be realized in conventional far-field communications. (2) The secrecy capacity is improved as the size of the XL-RIS reflecting elements increases. Specifically, when the transmit power at the BS is set as 40 dBm, the secrecy capacity of the XL-RIS empowered system with 800 reflection elements can increase by 35.9% compared with that with 680 reflection elements. (3) The AN can improve the secrecy capacity. In our results, the secrecy capacity of the proposed algorithm increases by 23.6% compared to that of

the benchmark scheme without AN.

The notations are presented in the supplementary materials.

2 System model

In this section, we present the system description, far-field and near-field channel models, the signal model for the XL-RIS empowered near-field PLS communication system, and the formulated optimization problem.

2.1 System description

As depicted in Fig. 1, we consider an XL-RIS empowered near-field communication system against jamming and eavesdropping attacks, which consists of a legitimate transmitter (referred to as BS) equipped with M ($M>1$) antennas, a legitimate user equipped with a single antenna, an eavesdropper equipped with a single antenna, and a jammer equipped with L ($L>1$) antennas. A uniform planar array (UPA) is employed at the XL-RIS, having N_{H} horizontal rows and N_{V} vertical columns, with the total number of reflection elements $N=N_{\mathrm{H}}\times N_{\mathrm{V}}$. The BS sends AN symbols to contaminate the received legitimate signal at the eavesdropper. The eavesdropper intercepts the legitimate information and obtains the content by eavesdropping maliciously. The jammer disturbs the transmitted signal from the BS to the legitimate user with specific symbol sequences, which are previously known by the eavesdropper due to the cooperation between them. Thus, the jamming sequences can be eliminated by the eavesdropper (Moon et al., 2018).

The user, eavesdropper, and jammer are assumed to be located within the near-field region of

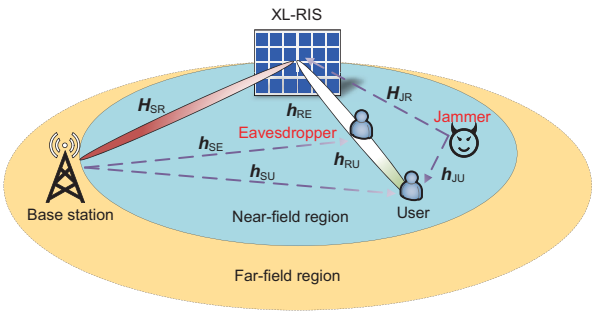

Fig. 1 Illustration of an XL-RIS empowered near–far field PLS communication system against jamming and eavesdropping attacks (PLS: physical layer security)

the XL-RIS. It can be observed from $\frac{2D^2}{\lambda}$ that the Rayleigh distance is proportional to the square of the array aperture. With the increasing antenna aperture of the XL-RIS, the near-field region will be further expanded. As a result, the user, eavesdropper, and jammer are more likely to be located in the near-field region. For instance, if the frequency is 28 GHz and the array aperture of the XL-RIS is $D_{\mathrm{R}}=0.532$ m, the Rayleigh distance is 52.77 m. For the BS, it is considered to be in the far field of the XL-RIS (Sun et al., 2022b).

2.2 Channel model

As illustrated in Fig. 1, let $\boldsymbol{H}_{\mathrm{SR}}\in\mathbb{C}^{N\times M}$ denote the channel matrix between the BS and the XL-RIS, $\boldsymbol{h}_{\mathrm{SU}}\in\mathbb{C}^{M\times 1}$ the channel matrix between the BS and the user, $\boldsymbol{h}_{\mathrm{SE}}\in\mathbb{C}^{M\times 1}$ the channel matrix between the BS and the eavesdropper, $\boldsymbol{h}_{\mathrm{RU}}\in\mathbb{C}^{N\times 1}$ the channel matrix between the XL-RIS and the user, $\boldsymbol{h}_{\mathrm{RE}}\in\mathbb{C}^{N\times 1}$ the channel matrix between the XL-RIS and the eavesdropper, $\boldsymbol{H}_{\mathrm{JR}}\in\mathbb{C}^{N\times L}$ the channel matrix between the jammer and the XL-RIS, and $\boldsymbol{h}_{\mathrm{JU}}\in\mathbb{C}^{L\times 1}$ the channel matrix between the jammer and the user. The phase-shift matrix of the XL-RIS is defined as a diagonal matrix $\boldsymbol{\Theta}=\mathrm{diag}\left(\mathrm{e}^{\mathrm{j}\varphi_1},\mathrm{e}^{\mathrm{j}\varphi_2},\ldots,\mathrm{e}^{\mathrm{j}\varphi_N}\right)$, where $\varphi_i\in[0,2\pi)$ is the phase shift of the i^{th} reflection element. We use θ_i to represent $\mathrm{e}^{\mathrm{j}\varphi_i}$ and $\boldsymbol{\Theta}$ can be expressed as $\mathrm{diag}\left(\boldsymbol{\theta}^{\mathrm{H}}\right)$, where $\boldsymbol{\theta}\triangleq[\theta_1,\theta_2,\ldots,\theta_N]^{\mathrm{H}}$.

The XL-RIS is deployed on the yz-plane of the three-dimensional (3D) coordinate system. Its center is located at $(0,0,0)$. We define d as the distance between the two adjacent reflection elements of the XL-RIS. Then, the element in the n_1^{th} column and n_2^{th} row of the XL-RIS can be expressed as $(0,n_1d,n_2d)$, where $n_1=\frac{-N_y+1}{2},\ldots,\frac{N_y-1}{2}$ and $n_2=\frac{-N_z+1}{2},\ldots,\frac{N_z-1}{2}$. Similarly, the l^{th} antenna at the jammer can be given as $(x_{\mathrm{J}},y_{\mathrm{J}}+\tilde{l}d,0)$, where $\tilde{l}=l-\frac{L-1}{2}$. The line-of-sight (LoS) near-field channel between the jammer and the XL-RIS is modeled as follows:

$$\boldsymbol{H}_{\mathrm{JR}}=[\boldsymbol{h}_1,\boldsymbol{h}_2,\ldots,\boldsymbol{h}_L]^{\mathrm{T}}, \tag{1}$$

where $\boldsymbol{h}_l=\left(1/\sqrt{N}\right)\left[\chi_{l,1}\mathrm{e}^{-\mathrm{j}\frac{2\pi f}{c}(r_{l,1}-r_l)},\chi_{l,2}\mathrm{e}^{-\mathrm{j}\frac{2\pi f}{c}(r_{l,2}-r_l)},\ldots,\chi_{l,N}\mathrm{e}^{-\mathrm{j}\frac{2\pi f}{c}(r_{l,N}-r_l)}\right]^{\mathrm{T}}$, $r_{l,n}$ denotes the distance between the n^{th} ($n=(n_1-1)N_{\mathrm{V}}+n_2$) element of the XL-RIS and the l^{th} element of the jammer, r_l is defined as the reference distance

from $(0,0,0)$ to $(x_{\mathrm{J}}, y_{\mathrm{J}}+\tilde{l}d, 0)$, and $\chi_{l,n}=\frac{c}{4\pi f r_{l,n}}$ is the free-space large-scale path loss between the n^{th} element of the XL-RIS and the l^{th} element of the jammer. $\boldsymbol{h}_{\mathrm{RU}}$ and $\boldsymbol{h}_{\mathrm{RE}}$ can be modeled in the same way. The eavesdropper and the user are both equipped with a single antenna, so the channels $\boldsymbol{h}_{\mathrm{RU}}$ and $\boldsymbol{h}_{\mathrm{RE}}$ can be easily obtained by the similar channel model.

The far-field channel model between the BS and the XL-RIS is modeled as the Saleh-Valenzuela channel model. The channel between the BS and the XL-RIS $\boldsymbol{H}_{\mathrm{SR}}$ can be given as follows:

$$\boldsymbol{H}_{\mathrm{SR}}=\sqrt{\frac{MN\chi_{\mathrm{ar}}}{L_{\mathrm{p}}}}\sum_{i=1}^{L_{\mathrm{p}}}\alpha_i\boldsymbol{a}_{\mathrm{UPA}}\left(\vartheta_{\mathrm{ar,r}}^{i},\phi_{\mathrm{ar,r}}^{i}\right)\boldsymbol{a}_{\mathrm{ULA}}^{\mathrm{H}}\left(\vartheta_{\mathrm{ar,t}}^{i}\right), \tag{2}$$

where L_{p} represents the cumulative count of resolvable signal paths, χ_{ar} represents the average path loss, the complex channel gain of the i^{th} path is defined as α_i, $\boldsymbol{a}_{\mathrm{UPA}}$ is the UPA-associated normalized array response vector, $\vartheta_{\mathrm{ar,r}}^{i}$ and $\phi_{\mathrm{ar,r}}^{i}$ denote the azimuth and elevation angles of arrival (AoAs) associated with the XL-RIS, $\boldsymbol{a}_{\mathrm{ULA}}$ is the uniform linear array (ULA) associated normalized array response vector, and $\vartheta_{\mathrm{ar,t}}^{i}$ represents the angle of departure (AoD) associated with BS. Specifically, $\boldsymbol{a}_{\mathrm{ULA}}$ with M elements is given by

$$\boldsymbol{a}_{\mathrm{ULA}}(\vartheta)=\frac{1}{\sqrt{M}}\left[1,\ldots,\mathrm{e}^{\mathrm{j}\frac{2\pi d'}{\lambda}(m-1)\sin\vartheta},\ldots,\mathrm{e}^{\mathrm{j}\frac{2\pi d'}{\lambda}(M-1)\sin\vartheta}\right]^{\mathrm{T}}, \tag{3}$$

where d' is the antenna spacing. For UPA, $\boldsymbol{a}_{\mathrm{UPA}}$ with $N=N_{\mathrm{H}}\times N_{\mathrm{V}}$ elements is given by

$$\begin{aligned}\boldsymbol{a}_{\mathrm{UPA}}(\vartheta,\phi)=&\frac{1}{\sqrt{N}}[1,\mathrm{e}^{\mathrm{j}\frac{2\pi d}{\lambda}\sin\vartheta\cos\phi},\ldots,\mathrm{e}^{\mathrm{j}\frac{2\pi d}{\lambda}(N_y-1)\sin\vartheta\cos\phi}]^{\mathrm{T}}\\&\otimes[1,\mathrm{e}^{\mathrm{j}\frac{2\pi d}{\lambda}\sin\phi},\ldots,\mathrm{e}^{\mathrm{j}\frac{2\pi d}{\lambda}(N_z-1)\sin\phi}]^{\mathrm{T}}.\end{aligned} \tag{4}$$

For legitimate channels, the CSI can be estimated accurately by calculating the angles of arrival and departure or sending a pilot (Sun et al., 2022a). In Sun et al. (2023), all the involved legitimate CSI can be obtained by the user by sending a pilot to the BS. We assume that the CSI of the eavesdropper and the legitimate user is available at the BS. This assumption is based on the following two scenarios. First, when the eavesdropper pretends to be a legitimate user, its instantaneous CSI is naturally known to the BS due to the legitimate interactions within the network, such as sending pilots (Zhou et al., 2020). Second, when the eavesdropper is unauthorized, the BS can detect the local oscillator leakage power of the passive eavesdropper (Mukherjee and Swindlehurst, 2012). Besides, we assume that the CSI of the cascaded channel is known to the BS. The methods of alternating least squares and vector approximate message passing are adopted to estimate the channel from the matrix slices (Wei et al., 2021). Finally, we assume that the CSI of the jammer is also known to the BS. The BS can perform the estimation scheme based on the ambient noise floor to measure the strength of jamming signals and further estimate the position of the jammer (Liu ZH et al., 2014).

2.3 Signal model

The transmitted signal at the BS can be expressed as follows:

$$\boldsymbol{x}=\boldsymbol{w}s+\boldsymbol{v}a, \tag{5}$$

where $\boldsymbol{w}\in\mathbb{C}^{M\times 1}$ denotes the beamforming vector of the legitimate user, s denotes the legitimate data symbols with $\mathbb{E}(ss^*)=1$, $\boldsymbol{v}\in\mathbb{C}^{M\times 1}$ denotes the beamforming vector of AN, and a denotes AN symbols with $\mathbb{E}(aa^*)=1$. The jammer transmits the jamming data symbol c with $\mathbb{E}(cc^*)=1$, and the beamforming vector is $\boldsymbol{m}$. Therefore, the received signal at the legitimate user can be expressed as

$$\begin{aligned}y_{\mathrm{u}}=&(\boldsymbol{h}_{\mathrm{RU}}^{\mathrm{H}}\boldsymbol{\Theta}\boldsymbol{H}_{\mathrm{SR}}+\boldsymbol{h}_{\mathrm{SU}}^{\mathrm{H}})(\boldsymbol{w}s+\boldsymbol{v}a)\\&+(\boldsymbol{h}_{\mathrm{RU}}^{\mathrm{H}}\boldsymbol{\Theta}\boldsymbol{H}_{\mathrm{JR}}+\boldsymbol{h}_{\mathrm{JU}}^{\mathrm{H}})\boldsymbol{m}c+n_{\mathrm{u}},\end{aligned} \tag{6}$$

where $n_{\mathrm{u}}\sim\mathcal{CN}\left(0,\sigma_{\mathrm{u}}^2\right)$ is the additive white Gaussian noise (AWGN). The signal-to-interference-plus-noise ratio (SINR) of the user can be expressed as Eq. (7) at the bottom of this page.

Similarly, the received signal at the eavesdropper can be expressed as follows:

$$y_{\mathrm{e}}=(\boldsymbol{h}_{\mathrm{RE}}^{\mathrm{H}}\boldsymbol{\Theta}\boldsymbol{H}_{\mathrm{SR}}+\boldsymbol{h}_{\mathrm{SE}}^{\mathrm{H}})(\boldsymbol{w}s+\boldsymbol{v}a)+n_{\mathrm{e}}, \tag{8}$$

$$\gamma_{\mathrm{u}}(\boldsymbol{w},\boldsymbol{v},\boldsymbol{\Theta})=\frac{\left|(\boldsymbol{h}_{\mathrm{RU}}^{\mathrm{H}}\boldsymbol{\Theta}\boldsymbol{H}_{\mathrm{SR}}+\boldsymbol{h}_{\mathrm{SU}}^{\mathrm{H}})\boldsymbol{w}\right|^2}{\left|(\boldsymbol{h}_{\mathrm{RU}}^{\mathrm{H}}\boldsymbol{\Theta}\boldsymbol{H}_{\mathrm{SR}}+\boldsymbol{h}_{\mathrm{SU}}^{\mathrm{H}})\boldsymbol{v}\right|^2+\left|(\boldsymbol{h}_{\mathrm{RU}}^{\mathrm{H}}\boldsymbol{\Theta}\boldsymbol{H}_{\mathrm{JR}}+\boldsymbol{h}_{\mathrm{JU}}^{\mathrm{H}})\boldsymbol{m}\right|^2+\sigma_{\mathrm{u}}^2}. \tag{7}$$

where $n_{\mathrm{e}} \sim \mathcal{CN}\left(0, \sigma_{\mathrm{e}}^2\right)$ is the AWGN at the eavesdropper. The SINR of the eavesdropper can be expressed as follows:

$$\gamma_{\mathrm{e}}\left(\boldsymbol{w}, \boldsymbol{v}, \boldsymbol{\Theta}\right) = \frac{\left|\left(\boldsymbol{h}_{\mathrm{RE}}^{\mathrm{H}} \boldsymbol{\Theta} \boldsymbol{H}_{\mathrm{SR}} + \boldsymbol{h}_{\mathrm{SE}}^{\mathrm{H}}\right)\boldsymbol{w}\right|^2}{\left|\left(\boldsymbol{h}_{\mathrm{RE}}^{\mathrm{H}} \boldsymbol{\Theta} \boldsymbol{H}_{\mathrm{SR}} + \boldsymbol{h}_{\mathrm{SE}}^{\mathrm{H}}\right)\boldsymbol{v}\right|^2 + \sigma_{\mathrm{e}}^2}. \quad (9)$$

The rate of the legitimate user can be written as

$$R_{\mathrm{u}}\left(\boldsymbol{w}, \boldsymbol{v}, \boldsymbol{\Theta}\right) = \log_2\left(1 + \gamma_{\mathrm{u}}\left(\boldsymbol{w}, \boldsymbol{v}, \boldsymbol{\Theta}\right)\right). \quad (10)$$

Similarly, the rate of the eavesdropper can be written as

$$R_{\mathrm{e}}\left(\boldsymbol{w}, \boldsymbol{v}, \boldsymbol{\Theta}\right) = \log_2\left(1 + \gamma_{\mathrm{e}}\left(\boldsymbol{w}, \boldsymbol{v}, \boldsymbol{\Theta}\right)\right). \quad (11)$$

The secrecy capacity of the system can be defined as

$$C_{\mathrm{S}}\left(\boldsymbol{w}, \boldsymbol{v}, \boldsymbol{\Theta}\right) = \left[R_{\mathrm{u}}\left(\boldsymbol{w}, \boldsymbol{v}, \boldsymbol{\Theta}\right) - R_{\mathrm{e}}\left(\boldsymbol{w}, \boldsymbol{v}, \boldsymbol{\Theta}\right)\right]^+, \quad (12)$$

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

2.4 Problem formulation

In this study, we aim to maximize the secrecy capacity C_{S} given in Eq. (12) by optimizing the beamforming vectors at the BS and the reflection coefficient matrix at the XL-RIS. The formulated problem can be expressed as follows:

$$\begin{aligned} &\max_{\boldsymbol{w}, \boldsymbol{v}, \boldsymbol{\Theta}} C_{\mathrm{S}}\left(\boldsymbol{w}, \boldsymbol{v}, \boldsymbol{\Theta}\right) \\ &\text{s.t.} \begin{cases} \|\boldsymbol{w}\|_2^2 + \|\boldsymbol{v}\|_2^2 \le P, \\ |\theta_i| = 1, \forall i = 1, 2, \ldots, N, \end{cases} \end{aligned} \quad (13)$$

where P is the maximum transmit power of the BS, and $|\theta_i| = 1$ $(i = 1, 2, \ldots, N)$ represents the phase shift constraint of the reflection elements. Problem (13) is a challenging optimization problem due to the non-convex optimization objective function with non-convex constraints. It is difficult to obtain the solution due to the mutual coupling of large-scale optimization variables.

3 Joint beamforming design for PLS communication

In this section, we propose an AO-based algorithm to deal with the coupling optimization problem. First, when $\boldsymbol{\Theta}$ is fixed, we introduce auxiliary variables to reformulate the subproblem into a more tractable problem and then propose the SCA-based algorithm to solve the reformulated problem. Second, when $\boldsymbol{w}$ and $\boldsymbol{v}$ are fixed, we reformulate the subproblem at the XL-RIS and propose an MO-based algorithm to solve it.

3.1 Transmit beamforming and AN design

When $\boldsymbol{\Theta}$ is fixed, we introduce auxiliary variables $\boldsymbol{g} = [g_1, g_2, g_3, g_4]^{\mathrm{T}}$ (Zhou et al., 2021) to reformulate the subproblem at the BS, which satisfy

$$\log_2\left(\boldsymbol{w}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{U}} \boldsymbol{w} + \boldsymbol{v}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{U}} \boldsymbol{v} + c_{\mathrm{U1}}\right) \ge g_1, \quad (14a)$$

$$\log_2\left(\boldsymbol{v}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{U}} \boldsymbol{v} + c_{\mathrm{U1}}\right) \le g_2, \quad (14b)$$

$$\log_2\left(\boldsymbol{w}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{E}} \boldsymbol{w} + \boldsymbol{v}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{E}} \boldsymbol{v} + \sigma_{\mathrm{e}}^2\right) \le g_3, \quad (14c)$$

$$\log_2\left(\boldsymbol{v}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{E}} \boldsymbol{v} + \sigma_{\mathrm{e}}^2\right) \ge g_4, \quad (14d)$$

where $\boldsymbol{A}_{\mathrm{U}}$, $\boldsymbol{A}_{\mathrm{E}}$, and c_{U1} are provided in the supplementary materials, such that $R_{\mathrm{U}} \ge g_1 - g_2$ and $R_{\mathrm{E}} \le g_3 - g_4$. The original optimization problem (13) is reformulated to maximize $g_1 - g_2 - g_3 + g_4$, subject to the transmit power constraint in (13) and the constraints in (14). The reformulated problem can be easily proved to be equivalent to (13), as the constraints in (14) hold equality at the optimization solution. Furthermore, we introduce auxiliary variables $\boldsymbol{t}_{\mathrm{f}} = [t_{\mathrm{f},1}, t_{\mathrm{f},2}, t_{\mathrm{f},3}, t_{\mathrm{f},4}]^{\mathrm{T}}$ to reformulate (14a) and (14b) as follows:

$$\log_2(t_{\mathrm{f},1}) \ge g_1, \quad (15a)$$

$$\log_2(t_{\mathrm{f},2}) \le g_2, \quad (15b)$$

$$\boldsymbol{w}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{U}} \boldsymbol{w} + \boldsymbol{v}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{U}} \boldsymbol{v} + c_{\mathrm{U1}} \ge t_{\mathrm{f},1}, \quad (15c)$$

$$\boldsymbol{v}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{U}} \boldsymbol{v} + c_{\mathrm{U1}} \le t_{\mathrm{f},2}. \quad (15d)$$

Similarly, (14c) and (14d) can be reformulated as

$$\log_2(t_{\mathrm{f},3}) \le g_3, \quad (16a)$$

$$\log_2(t_{\mathrm{f},4}) \ge g_4, \quad (16b)$$

$$\boldsymbol{w}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{E}} \boldsymbol{w} + \boldsymbol{v}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{E}} \boldsymbol{v} + \sigma_{\mathrm{e}}^2 \le t_{\mathrm{f},3}, \quad (16c)$$

$$\boldsymbol{v}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{E}} \boldsymbol{v} + \sigma_{\mathrm{e}}^2 \ge t_{\mathrm{f},4}. \quad (16d)$$

It is obvious that (15b), (15c), (16a), and (16d) are concave. The first-order Taylor approximation can be introduced to reformulate these concave constraints (Boyd et al., 2006):

$$\log_2(\bar{t}_{\mathrm{f},2}) + \frac{t_{\mathrm{f},2} - \bar{t}_{\mathrm{f},2}}{\bar{t}_{\mathrm{f},2} \ln 2} \le g_2, \quad (17a)$$

$$\mathrm{Re}\left\{\bar{\boldsymbol{w}}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{U}} \boldsymbol{w}\right\} - \bar{\boldsymbol{w}}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{U}} \bar{\boldsymbol{w}} + c_{\mathrm{U1}} \ge t_{\mathrm{f},1}, \quad (17b)$$

$$\log_2(\bar{t}_{\mathrm{f},3}) + \frac{t_{\mathrm{f},3} - \bar{t}_{\mathrm{f},3}}{\bar{t}_{\mathrm{f},3} \ln 2} \le g_3, \quad (17c)$$

$$\mathrm{Re}\left\{\bar{\boldsymbol{v}}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{E}} \boldsymbol{v}\right\} - \bar{\boldsymbol{v}}^{\mathrm{H}} \boldsymbol{A}_{\mathrm{E}} \bar{\boldsymbol{v}} + \sigma_{\mathrm{e}}^2 \ge t_{\mathrm{f},4}, \quad (17d)$$

where $\bar{\boldsymbol{w}}$, $\bar{\boldsymbol{v}}$, $\bar{t}_{\mathrm{f},2}$, and $\bar{t}_{\mathrm{f},3}$ are the solutions of the last iteration. Then, the problem can be expressed as

$$\max_{\boldsymbol{w},\boldsymbol{v},\boldsymbol{p},\boldsymbol{t}_{\mathrm{f}},\boldsymbol{g}} \ g_1-g_2-g_3+g_4$$
$$\text{s.t.} \begin{cases} \|\boldsymbol{w}\|_2^2+\|\boldsymbol{v}\|_2^2\le P, \\ (15\mathrm{a}),(15\mathrm{d}),(16\mathrm{b}),(16\mathrm{c}), \\ (17\mathrm{a}),(17\mathrm{b}),(17\mathrm{c}),(17\mathrm{d}), \end{cases} \tag{18}$$

which is a convex optimization problem and can be solved with optimization solvers such as CVX (Boyd and Vandenberghe, 2004).

3.2 Reflection coefficient matrix design

When $\boldsymbol{\Theta}$ is fixed, $\left|\left(\boldsymbol{h}_{\mathrm{RU}}^{\mathrm{H}}\boldsymbol{\Theta}\boldsymbol{H}_{\mathrm{SR}}+\boldsymbol{h}_{\mathrm{SU}}^{\mathrm{H}}\right)\boldsymbol{w}\right|^2$ can be expressed as $\boldsymbol{s}^{\mathrm{H}}\boldsymbol{G}_{\mathrm{u},1}\boldsymbol{s}+b_{\mathrm{u},1}$ where $\boldsymbol{s}^{\mathrm{H}}=[\boldsymbol{\theta}^{\mathrm{H}},1]$ and $\boldsymbol{G}_{\mathrm{u},1}$, $b_{\mathrm{u},1}$ are defined in the supplementary materials. Similarly, the formula manipulation can be introduced to obtain $\boldsymbol{s}^{\mathrm{H}}\boldsymbol{G}_{\mathrm{u},2}\boldsymbol{s}+b_{\mathrm{u},2}$, $\boldsymbol{s}^{\mathrm{H}}\boldsymbol{G}_{\mathrm{e},1}\boldsymbol{s}+b_{\mathrm{e},1}$, $\boldsymbol{s}^{\mathrm{H}}\boldsymbol{G}_{\mathrm{e},2}\boldsymbol{s}+b_{\mathrm{e},2}$, and $\boldsymbol{s}^{\mathrm{H}}\boldsymbol{G}_{\mathrm{j}}\boldsymbol{s}+b_{\mathrm{j}}$. Note that the equations are provided in the supplementary materials.

Thus, γ_{u} can be formulated as follows:

$$\gamma_{\mathrm{u}}=\frac{\boldsymbol{s}^{\mathrm{H}}\boldsymbol{G}_{\mathrm{u},1}\boldsymbol{s}+b_{\mathrm{u},1}}{\boldsymbol{s}^{\mathrm{H}}\boldsymbol{G}_{\mathrm{u},2}\boldsymbol{s}+b_{\mathrm{u},2}+\boldsymbol{s}^{\mathrm{H}}\boldsymbol{G}_{\mathrm{j}}\boldsymbol{s}+b_{\mathrm{j}}+\sigma_{\mathrm{u}}^2}, \tag{19}$$

and γ_{e} can be formulated as follows:

$$\gamma_{\mathrm{e}}=\frac{\boldsymbol{s}^{\mathrm{H}}\boldsymbol{G}_{\mathrm{e},1}\boldsymbol{s}+b_{\mathrm{e},1}}{\boldsymbol{s}^{\mathrm{H}}\boldsymbol{G}_{\mathrm{e},2}\boldsymbol{s}+b_{\mathrm{e},2}+\sigma_{\mathrm{e}}^2}. \tag{20}$$

With the reformulation, the objective function C_{S} can be expressed as follows:

$$C_{\mathrm{S}}=\max\{\log_2(1+\gamma_{\mathrm{u}})-\log_2(1+\gamma_{\mathrm{e}}),0\}. \tag{21}$$

The constraint set of $\boldsymbol{s}$ is a complex circle manifold. Thus, the vector $\boldsymbol{s}$ can be obtained by the MO algorithm (Guo et al., 2020). MO is divided mainly into three steps, which are presented in the supplementary materials.

The overall algorithm is summarized as Algorithm 1. We provide the convergence and complexity analysis for Algorithm 1 in the supplementary materials.

4 Numerical results

This section presents the numerical results of the proposed algorithm in the XL-RIS empowered PLS communication system. As depicted in Fig. 2, considering a 3D Cartesian coordinate system, the

Algorithm 1 Alternating optimization of $\boldsymbol{w}$, $\boldsymbol{v}$, and $\boldsymbol{\theta}$

1: Initialization: secrecy capacity accuracy ε, beamforming vectors $\boldsymbol{w}^{(0)}$, $\boldsymbol{v}^{(0)}$, and $\boldsymbol{\theta}^{(0)}$, secrecy capacity $C_{\mathrm{S}}^{(0)}$ calculated by $\boldsymbol{w}^{(0)}$, $\boldsymbol{v}^{(0)}$, and $\boldsymbol{\theta}^{(0)}$, $t=0$
2: **repeat**
3: $t=t+1$
4: Update $\boldsymbol{w}$ and $\boldsymbol{v}$ by solving problem (18)
5: Update $\boldsymbol{\theta}$ by using the MO algorithm
6: Update $C_{\mathrm{S}}^{(t)}$ by using the updated $\boldsymbol{w}$, $\boldsymbol{v}$, and $\boldsymbol{\theta}$
7: **until** $\left|C_{\mathrm{S}}^{(t)}-C_{\mathrm{S}}^{(t-1)}\right|<\varepsilon$
Ensure: $C_{\mathrm{S}}^{\star}$

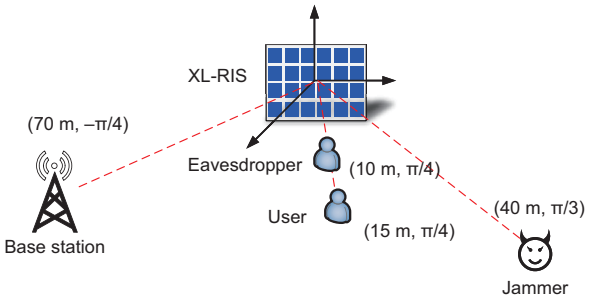

Fig. 2 Deployment of an XL-RIS empowered near-field PLS communication system against jamming and eavesdropping (PLS: physical layer security)

XL-RIS is deployed on the yz-plane, and its center is located at $(0,0,0)$. The BS, eavesdropper, and jammer are deployed on the xy-plane. To facilitate coordinate representation, we use polar coordinates to denote the positions. The origin of the polar coordinate system is set at the center of the XL-RIS, and its polar axis is aligned with the x-axis of the 3D Cartesian coordinate system. The center of the XL-RIS is located at $(0,0)$. The BS is located at $(70\ \mathrm{m},\ -\pi/4)$. An extreme scenario is considered where the eavesdropper is located between the XL-RIS and the user with the same azimuth angles. The locations of the eavesdropper, legitimate user, and jammer are set as $(10\ \mathrm{m},\pi/4)$, $(15\ \mathrm{m},\pi/4)$, and $(40\ \mathrm{m},\pi/3)$ within the near-field region, respectively. We assume that the channels between the BS and the eavesdropper, the BS and the user, and the jammer and the user are independent Rayleigh fading channels. The path loss is modeled as follows:

$$\mathrm{PL}(d)=C_0\left(\frac{d}{d_0}\right)^{-\alpha}, \tag{22}$$

where $C_0=-75$ dB is the loss at the reference distance $d_0=1$ m, d represents the distance between two devices, and α denotes the path loss factor. The path loss factors between the BS and the user, the BS and the eavesdropper, and the jammer and the

user are set as 4.5, 4.5, and 4, respectively. We assume that the links between the BS and the XL-RIS are LoS dominated, and the corresponding path loss is modeled as $(30+20.0\lg(D_{\mathrm{AX}}/\mathrm{m}))$ dB, where D_{AX} denotes the distance in meters. The other parameters are set as $N_{\mathrm{V}}=8$, $L=4$, $f=28$ GHz, $d=\frac{\lambda}{2}$, $\sigma_{\mathrm{u}}^2=-100$ dBm, $\sigma_{\mathrm{e}}^2=-100$ dBm, and $\varepsilon=10^{-3}$. With the parameters, the Rayleigh distance between the XL-RIS with $N_{\mathrm{H}}=100$ and the jammer, the XL-RIS and the user, and the XL-RIS and the eavesdropper can be calculated as 56.01, 52.77, and 52.77 m, respectively.

In the following simulation, the jammer is assumed to perform the maximum ratio transmission (MRT) to disturb the transmitted signal from the BS to the legitimate user. Due to the double fading effect, the cascade channel is weaker than the direct channel. Thus, we consider that the jammer performs MRT to the direct link of the legitimate user. The beamforming vector of the jammer is set as $\boldsymbol{m}=\sqrt{P_{\mathrm{J}}}\frac{\boldsymbol{h}_{\mathrm{JU}}}{\|\boldsymbol{h}_{\mathrm{JU}}\|}$, where P_{J} is the transmit power of the jammer.

Fig. 3 shows the convergence behaviors of secrecy capacity with different sizes of the XL-RIS. We set $M=16$, $P=40$ dBm, and $P_{\mathrm{J}}=10$ dBm. It can be observed that the secrecy at the legitimate user increases monotonically and converges within a few number of iterations. Moreover, the secrecy capacity increases as the number of reflection elements of the XL-RIS increases. The secrecy capacity of the XL-RIS empowered system with 800 reflection elements increases by 22.1% compared with that with 720 reflection elements.

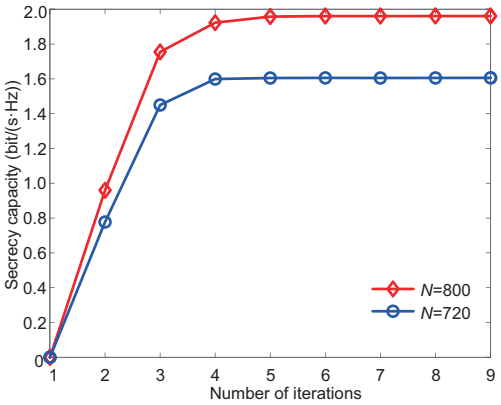

Fig. 3 Convergence behaviors of the proposed algorithm for different sizes of XL-RIS

Fig. 4 shows the secrecy capacity versus varying transmit power P with different baseline schemes. We set $N_{\mathrm{H}}=100$, $M=16$, and $P_{\mathrm{J}}=10$ dBm. We compare three baseline schemes including the proposed algorithm without AN, the transmit beamforming and the AN design with the random reflection phase, and the proposed scheme without the XL-RIS. It can be observed that the secrecy capacity of the proposed algorithm is higher than that of the three other baseline schemes, especially when the transmit power of the BS reaches 40 dBm. When $P=40$ dBm, the secrecy capacity of the proposed algorithm increases by 23.6%, 288.5%, and 521.3% compared with that of the three other schemes, respectively. We also compare the secrecy capacity of different schemes under varying transmit power at the jammer in the supplementary materials.

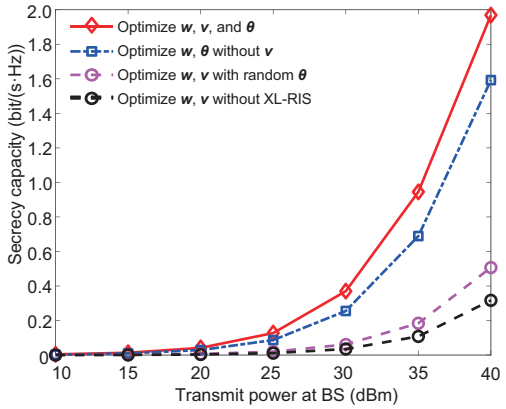

Fig. 4 Secrecy capacity comparison versus transmit power P for different baseline schemes

Fig. 5 shows the secrecy capacity versus different BS transmit power P for different sizes of XL-RIS. We set $M=16$ and $P_{\mathrm{J}}=10$ dBm. It can be observed that when the BS transmit power P is fixed, the secrecy capacity increases as the number of reflection elements increases. When $P=40$ dBm, the secrecy capacity of the XL-RIS with 800 reflection elements increases by 35.9% compared with that of the XL-RIS with 680 reflection elements.

Fig. 6 shows the secrecy capacity versus different locations of the eavesdropper for different sizes of XL-RIS. We set $M=16$, $P=40$ dBm, and $P_{\mathrm{J}}=10$ dBm. It can be observed that when the location of the eavesdropper moves from $(3\ \mathrm{m},\pi/4)$ to $(27\ \mathrm{m},\pi/4)$, the secrecy capacity decreases first and then increases as the eavesdropper moves toward first and then away from the legitimate user.

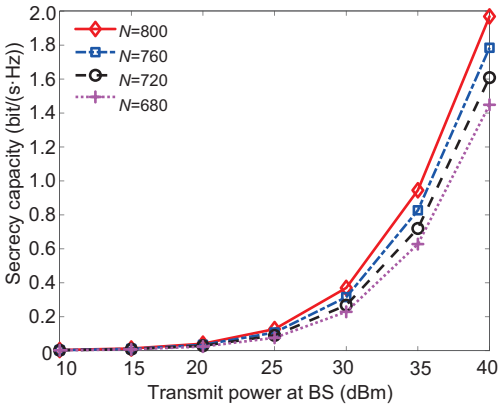

Fig. 5 Secrecy capacity comparison versus transmit power P for various sizes of XL-RIS N

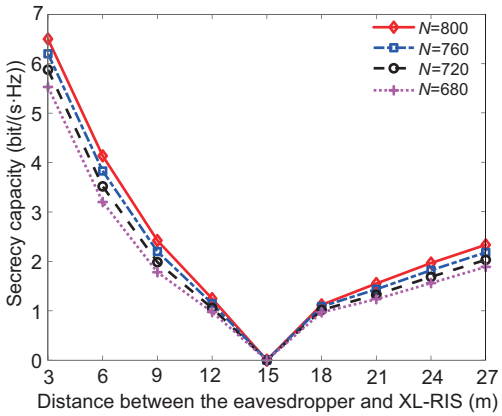

Fig. 6 Secrecy capacity comparison versus locations of the eavesdropper for various sizes of XL-RIS N

This indicates that the XL-RIS can ensure secure communication even if the eavesdropper is located at the same direction as the legitimate user and closer to the XL-RIS, which cannot be realized in conventional far-field secure communications. Besides, the secrecy capacity when the eavesdropper is at the same distance from the user but closer to the XL-RIS (3 m) is higher than when it is further away from the XL-RIS (27 m). This indicates that with the eavesdropper moving closer to the XL-RIS, the beam focusing ability of the XL-RIS becomes stronger. Consequently, less legitimate signal energy is leaked to the eavesdropper.

Fig. 7 shows the secrecy capacity versus varying transmit power P under the perfect and imperfect CSI. Let u denote the actual value of the channel, and $\hat{u}$ the corresponding estimate. The normalized mean squared error (NMSE) value is calculated as $\rho = \frac{\mathbb{E}\left[|u-\hat{u}|^2\right]}{\mathbb{E}\left[|\hat{u}|^2\right]}$. We compare the schemes under the imperfect CSI with a ρ of 0.05, 0.1, or 0.5 to the scheme under the perfect CSI. When the transmit power at the BS is low, the imperfect CSI condition has a slight influence on the proposed scheme. Even at the transmit power of 40 dBm, the inaccuracy in channel estimation results in only 4.5% and 7.4% reduction in secrecy capacity with a ρ of 0.05 and 0.1, respectively. When ρ is set as 0.5, the reduction in secrecy capacity rises to 24.7%. This indicates that the proposed scheme exhibits strong robustness even with relatively small channel estimation errors.

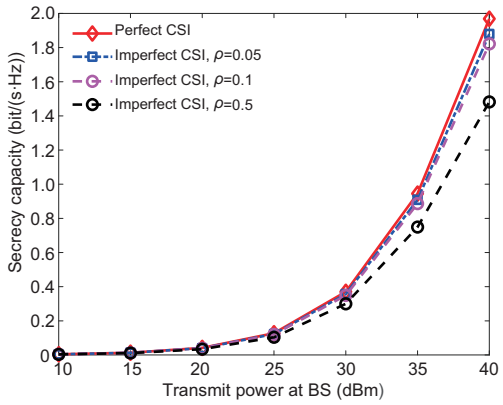

Fig. 7 Secrecy capacity comparison versus transmit power P for the perfect and imperfect CSI (CSI: channel state information)

5 Conclusions

In this paper, we have studied an XL-RIS empowered near-field PLS communication system against jamming and eavesdropping attacks. We introduced AN to contaminate the received legitimate signal at the eavesdropper and formulated an optimization problem. Numerical results demonstrated the effectiveness of the proposed algorithm in improving the secrecy capacity. Even in the extreme scenario where the eavesdropper was located in the same direction as the legitimate user and closer to the XL-RIS, the proposed algorithm could still improve the secrecy capacity greatly. The proposed algorithm can be further extended to other PLS communication systems with multiple eavesdroppers or statistical/partial CSI.

Contributors

Zelong CUI performed the experiments and drafted the paper. Gang YANG established the optimization model. Jun LIU helped design the optimization algorithm. Gang YANG and Jun LIU revised and finalized the paper.

Conflict of interest

All the authors declare that they have no conflict of interest.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

Boyd S, Vandenberghe L, 2004. Convex Optimization. Cambridge University Press, Cambridge, UK.

Boyd S, Vandenberghe L, Faybusovich L, 2006. Convex optimization. *IEEE Trans Autom Contr*, 51(11):1859. https://doi.org/10.1109/TAC.2006.884922

Cheng Q, Jin S, Cui TJ, 2023. Reconfigurable intelligent surfaces for wireless communications. *Front Inform Technol Electron Eng*, 24(12):1665-1668. https://doi.org/10.1631/FITEE.2320000

di Renzo M, Zappone A, Debbah M, et al., 2020. Smart radio environments empowered by reconfigurable intelligent surfaces: how it works, state of research, and the road ahead. *IEEE J Sel Areas Commun*, 38(11):2450-2525. https://doi.org/10.1109/JSAC.2020.3007211

Guo HY, Liang YC, Chen J, et al., 2020. Weighted sum-rate maximization for reconfigurable intelligent surface aided wireless networks. *IEEE Trans Wirel Commun*, 19(5):3064-3076. https://doi.org/10.1109/TWC.2020.2970061

Liang LP, Cheng WC, Zhang W, et al., 2018. Mode hopping for anti-jamming in radio vortex wireless communications. *IEEE Trans Veh Technol*, 67(8):7018-7032. https://doi.org/10.1109/TVT.2018.2825539

Liu J, Yang G, Liang YC, et al., 2024a. Max-min fairness in RIS-assisted anti-jamming communications: optimization versus deep reinforcement learning approaches. *IEEE Trans Commun*, 72(7):4476-4492. https://doi.org/10.1109/TCOMM.2024.3371359

Liu J, Yang G, Liu YW, et al., 2024b. RIS empowered near-field covert communications. *IEEE Trans Wirel Commun*, 23(10):15477-15492. https://doi.org/10.1109/TWC.2024.3430328

Liu YW, Wang ZL, Xu JQ, et al., 2023. Near-field communications: a tutorial review. *IEEE Open J Commun Soc*, 4:1999-2049. https://doi.org/10.1109/OJCOMS.2023.3305583

Liu ZH, Liu HB, Xu WY, et al., 2014. An error-minimizing framework for localizing jammers in wireless networks. *IEEE Trans Parall Distrib Syst*, 25(2):508-517. https://doi.org/10.1109/TPDS.2013.33

Ma YD, Liu K, Liu YM, et al., 2024. Secure transmission via hybrid active-passive RIS against eavesdropping and jamming. *IEEE Wirel Commun Lett*, 13(7):1978-1982. https://doi.org/10.1109/LWC.2024.3399782

Moon J, Lee H, Song C, et al., 2018. Proactive eavesdropping with full-duplex relay and cooperative jamming. *IEEE Trans Wirel Commun*, 17(10):6707-6719. https://doi.org/10.1109/TWC.2018.2863287

Mukherjee A, Swindlehurst AL, 2012. Detecting passive eavesdroppers in the MIMO wiretap channel. Proc IEEE Int Conf on Acoustics, Speech and Signal Processing, p.2809-2812. https://doi.org/10.1109/ICASSP.2012.6288501

Nguyen VL, Lin PC, Cheng BC, et al., 2021. Security and privacy for 6G: a survey on prospective technologies and challenges. *IEEE Commun Surv Tutor*, 23(4):2384-2428. https://doi.org/10.1109/COMST.2021.3108618

Pan CH, Ren H, Wang KZ, et al., 2020. Intelligent reflecting surface aided MIMO broadcasting for simultaneous wireless information and power transfer. *IEEE J Sel Areas Commun*, 38(8):1719-1734. https://doi.org/10.1109/JSAC.2020.3000802

Sun YF, An K, Luo JS, et al., 2022a. Outage constrained robust beamforming optimization for multiuser IRS-assisted anti-jamming communications with incomplete information. *IEEE Int Things J*, 9(15):13298-13314. https://doi.org/10.1109/JIOT.2022.3140752

Sun YF, An K, Zhu YG, et al., 2022b. RIS-assisted robust hybrid beamforming against simultaneous jamming and eavesdropping attacks. *IEEE Trans Wirel Commun*, 21(11):9212-9231. https://doi.org/10.1109/TWC.2022.3174629

Sun YF, An K, Li C, et al., 2023. Joint transmissive and reflective RIS-aided secure MIMO systems design under spatially-correlated angular uncertainty and coupled PSEs. *IEEE Trans Inform Forens Secur*, 18:3606-3621. https://doi.org/10.1109/TIFS.2023.3283130

Wei L, Huang CW, Alexandropoulos GC, et al., 2021. Channel estimation for RIS-empowered multi-user MISO wireless communications. *IEEE Trans Commun*, 69(6):4144-4157. https://doi.org/10.1109/TCOMM.2021.3063236

Yan SH, Yang N, Land I, et al., 2018. Three artificial-noise-aided secure transmission schemes in wiretap channels. *IEEE Trans Veh Technol*, 67(4):3669-3673. https://doi.org/10.1109/TVT.2017.2779508

Zhang Z, Liu YW, Wang ZL, et al., 2024. Physical layer security in near-field communications. *IEEE Trans Veh Technol*, 73(7):10761-10766. https://doi.org/10.1109/TVT.2024.3366115

Zhao YJ, 2023. Reconfigurable intelligent surfaces for 6G: applications, challenges, and solutions. *Front Inform Technol Electron Eng*, 24(12):1669-1688. https://doi.org/10.1631/FITEE.2200666

Zhou G, Pan CH, Ren H, et al., 2020. Robust beamforming design for intelligent reflecting surface aided MISO communication systems. *IEEE Wirel Commun Lett*, 9(10):1658-1662. https://doi.org/10.1109/LWC.2020.3000490

Zhou G, Pan CH, Ren H, et al., 2021. Secure wireless communication in RIS-aided MISO system with hardware impairments. *IEEE Wirel Commun Lett*, 10(6):1309-1313. https://doi.org/10.1109/LWC.2021.3064992

List of supplementary materials

1 Supplement to notations and formula definitions

2 Supplement to convergence, complexity, and additional result analysis

Fig. S1 Secrecy capacity comparison versus transmit power P_{J} for different baseline schemes with $M = 8$