Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4617366, 7 pages
https://doi.org/10.1155/2022/4617366

Research Article

Optimal Element Allocation for RIS-Aided Physical Layer Security

Ying Zhang,[1] **Guoan Zhang**,[1] **Siyu Chen**,[1] **Jaeho Choi**,[2] **and Pin-Han Ho**[3]

[1]*School of Information Science and Technology, Nantong University, Nantong 226019, China*
[2]*Department of Electronic Engineering, Chonbuk National University, Jeonju 54896, Republic of Korea*
[3]*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada N2L 3G1*

Correspondence should be addressed to Guoan Zhang; gzhang@ntu.edu.cn

Received 26 July 2022; Accepted 8 September 2022; Published 21 September 2022

Academic Editor: Yingyang Chen

In this paper, we investigate an innovative physical layer security (PLS) scheme for an uncertain reconfigurable intelligent surface-(RIS-) assisted communication system under eavesdropping attack. Specifically, in our proposed system, we consider that the uncertain RIS is known to the legitimate user while not to the eavesdropper (Eve). In this manner, the reflective elements of the uncertain RIS are adjusted to strengthen the keen signals for the legitimate user while suppressing the signals for Eve via jamming. We analyze the system by assuming legitimate and wiretap channels, respectively, where the secrecy capacity maximization problem is formulated and its exact closed-form expression is derived. Simulation results verifying the accuracy of our analysis demonstrate the validity and superiority of the uncertain RIS-assisted communication system against its counterparts.

1. Introduction

Due to the fast development of the mobile communication network, the continuous emergence of new services, and the fulminic growth of information interaction, the fifth-generation (5G) wireless communications are anticipated to provide massive data transmissions and wide-area coverage as a new type of communication network [1]. For the upcoming applications of 5G, future wireless communication systems are anticipated to support more efficient, lower latency, more reliable, and secure designs. With the rapid evolution of science, lots of technologies have been implemented in 5G communication network to satisfy its diverse application scenarios, e.g., multiple access technology [2], deep learning (DL) [3], and beamforming [4]. Meanwhile, due to the explosive growth of information dissemination and massive information interaction, public communication networks and private communication networks are often mixed, which makes information security issues more important [5].

Physical layer security (PLS) enhancement has aroused extensive attentions in both industry and academia thanks to its superb capability of light-weight authentication on received signals against eavesdropping attacks [6]. Since the PLS takes advantage of the natural peculiarities and physical properties of propagation environment to promote the security performance of 5G communication network and secure the data transmission, it has attracted extensive attention in the academia and industry circles [7]. Several dimensions of designing PLS schemes have been identified in the literature, via nonorthogonal multiple access (NOMA) [8], artificial noise (AN), and cooperative interference [9]. Although effective, they may consume extra power and/or incur additional hardware cost, thus forming significant barriers in the real implementations.

Fortunately, with the rapid evolution of metamaterial technology, a low cost and energy efficient device named reconfigurable intelligent surface (RIS) offers an available way to strengthen the PLS [10]. The RIS is an artificial electromagnetic surface consisting a great many cheap passive reflecting elements governed by a preprogrammed controller, which can skillfully change the amplitude and/or phase shift of arriving galvanomagnetic signals to make the direction and strength of the signal greatly controllable at the destination. Thus, the RIS cannot only strengthen the required signals and restrain the undesirable signals by befittingly tuning the phase shifts of all reflecting components but also

effectively improves the radio transmission environment leading to the random channel state information (CSI) controllable [11, 12]. Therefore, it can be anticipated that the RIS will occupy an important position in the 5G wireless communication network [13].

With such characteristics, RIS has recently been considered to enable the PLS of wireless communication system to promote the secrecy capacity [14–18]. In [14], the minimum secrecy rate maximization problem of one downlink multiple-input single-output (MISO) broadcasting communication model was formulated and optimized via alternating optimization (AO) and path tracing algorithm. The authors in [15] introduced an RIS-based secure transmission framework aiming to obtain the minimum value of its communication network energy consumption within the scenarios of two different access point-(AP-) RIS channel models. In [16], the joint optimization of transmitter beamforming and RIS phase shifts by block coordinate descending (BCD) and majorization-minimization (MM) methods was studied to maximize the system security capacity for the secure wireless communication assisted with RIS. Cui et al. [17] considered a stronger eavesdropping channel than the legal one, where the AO and semidefinite relaxation (SDR) algorithms were explored to derive the maximum value of the security capacity in the secure wireless communication system. Wang et al. [18] investigated an RIS-aided MISO communication network with the unknown eavesdropping CSI, where the oblique manifold (OM) and MM algorithms were designed to promote the security of the communication network.

Note that the above mentioned studies [14–18] simply focused their attention on one function of RIS, i.e., enhancing or jamming, but the unknown situation of RIS was not considered. This paper investigates RIS-assisted secure wireless communication with the main contributions listed as follows:

(i) We propose a novel PLS communication system with an uncertain RIS aiming to enhance the secrecy rate, where the components of RIS are separated into two functional parts, one assisting the legitimate user and the other suppressing the achievable rate of eavesdropper as a jammer.

(ii) The optimal result of elements allocation for RIS is analyzed, and its exact closed-form expression is concluded to confirm the superiority of our proposed scheme.

(iii) Numerical results verifying the correctness of the derived expression show the advantage and validity of the designed scheme compared with its counterparts, especially under a great many reflecting elements.

2. System Model

An uncertain RIS-assisted secure communication system is considered, which consists of a source (S), a legitimate user (B), an eavesdropper (Eve), and an RIS, as depicted in Figure 1. To improve the secure wireless communication, the RIS with N reflecting elements is placed near by S, B, and Eve which are equipped with a single antenna. For the uncertain RIS, the size of each element is considered a lot smaller than the wavelength of RF signals resulting in that the reflecting element scatters the received signal in whole directions with approximately constant gain [19], and the phase shift of each passive units is controlled dynamically by RIS via an intelligent controller. It is also supposed that both S and B have the knowledge of the location information of RIS, while Eve is unable to acquire the location information of RIS, and that the CSI of the uncertain RIS is entirely known to S and B, but not for the Eve.

The direct links of $S \longrightarrow B$ and $S \longrightarrow$ Eve are considered, which are expressed by $h_{SB} \in \mathbb{C}$ and $h_{SE} \in \mathbb{C}$, respectively. Considering that the number of components is fixed to N, we divide the surface of RIS into two sectors, in which the one with η elements is used to serve as a jammer to Eve and the other with $(N-\eta)$ elements is applied to promote the information signals from S to B via high-quality virtual links. The source transmits the signal to legitimate user via the RIS to promote the information transmission for the legitimate user, and the channel coefficients of the links $S \longrightarrow$ RIS and RIS $\longrightarrow B$ are expressed by $\mathbf{h}_{SR_1} \in \mathbb{C}^{\eta \times 1}$ and $\mathbf{h}_{R_1 B} \in \mathbb{C}^{\eta \times 1}$, respectively. Since the eavesdropper attempts to wiretap the signal from S, it is assumed that the eavesdropper does not know the location of RIS, and hence, the reflected signals from RIS will be treated as jamming signals for the Eve, with the available links $S \longrightarrow$ RIS and RIS $\longrightarrow$ Eve denoted as $\mathbf{h}_{SR_2} \in \mathbb{C}^{(N-\eta)\times 1}$ and $\mathbf{h}_{R_2 E} \in \mathbb{C}^{(N-\eta)\times 1}$, respectively. Furthermore, it is assumed that each channel of the system follows independent Rayleigh fading distribution. Thus, the received signals at B and Eve are separately expressed as

$$y_B = \sqrt{P}\left(h_{SB} + \mathbf{h}_{R_1 B}^H \mathbf{\Theta}_1 \mathbf{h}_{SR_1}\right)s + n_1, \tag{1}$$

$$y_E = \sqrt{P} h_{SE} s + \sqrt{P}\mathbf{h}_{R_2 E}^H \mathbf{\Theta}_2 \mathbf{h}_{SR_2} s + n_2, \tag{2}$$

where s and P mean the data symbol and the transmit power for S and $\mathbb{E}[|s|^2] = 1$. $\mathbf{\Theta}_1 = \alpha$ diag $(e^{j\psi_1}, \cdots, e^{j\psi_{N-\eta}})$ and $\alpha \in (0, 1]$ stand for the channel coefficient matrix of the RIS sector serving B and the amplitude of the reflection coefficient, where $\alpha = 1$ represents the lossless reflection; $\psi_i \in [0, 2\pi)$ is the phase-shift produced by the i-th element for $i = 1, \cdots, N-\eta$. $\mathbf{\Theta}_2 = \alpha$ diag $(e^{j\phi_1}, \cdots, e^{j\phi_\eta})$ stands for the channel coefficients matrix of the RIS sector allocated for Eve, $\phi_j \in [0, 2\pi)$ is the phase-shift produced by the j-th element for $j = 1, \cdots, \eta$. In addition, n_1 and $n_2 \sim \mathcal{CN}(0, \sigma^2)$ are the additive white Gaussian noise (AWGN).

Since the signal from RIS will be treated as interference by the Eve because of the unknown CSI of RIS, the achievable SNR at B and SINR at Eve can be, respectively, obtained from

$$\gamma_B = \frac{P}{\sigma^2}\left|h_{SB} + \mathbf{h}_{R_1 B}^H \mathbf{\Theta}_1 \mathbf{h}_{SR_1}\right|^2, \tag{3}$$

$$\gamma_E = \frac{P|h_{SE}|^2}{P\left|\mathbf{h}_{R_2 E}^H \mathbf{\Theta}_2 \mathbf{h}_{SR_2}\right|^2 + \sigma^2}. \tag{4}$$

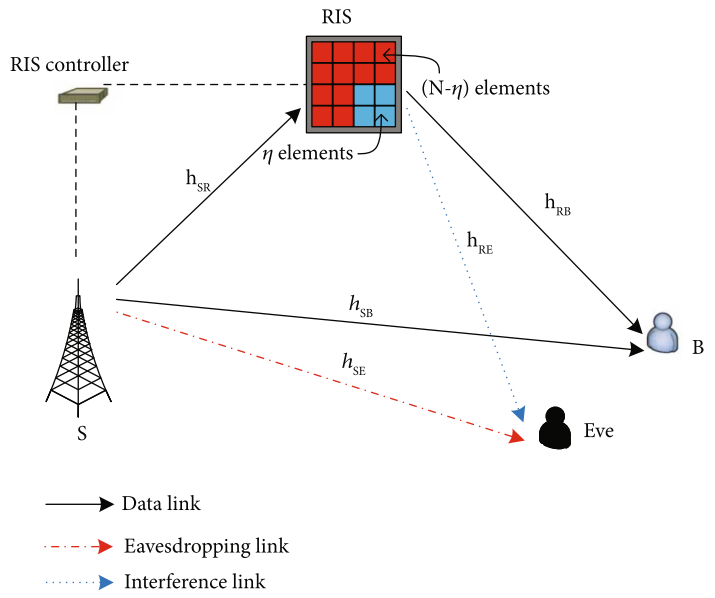

FIGURE 1: The uncertain RIS-assisted PLS system.

For any given $\boldsymbol{\Theta}_1$ and $\boldsymbol{\Theta}_2$, the data rate expressions for B and Eve can be achieved from the Shannon theory as $R_B = \log_2(1+\gamma_B)$ and $R_E = \log_2(1+\gamma_E)$.

From above observations, the secrecy capacity (SC) in our proposed scheme can be expressed as

$$C_S = [R_B - R_E]^+, \tag{5}$$

where $[x]^+ = \max(0, x)$. Considering that the deterministic channels for B and Eve are fully known for S, with the optimized phase shift variables, the SC optimization of the proposed uncertain RIS-assisted communication system is formulated as

$$\begin{aligned} \mathscr{P}_1 : &\max_{\{\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2\}} C_S, \\ \text{s.t.} \quad &\boldsymbol{\Theta}_1 = \text{diag}\left(e^{j\psi_1}, \cdots, e^{j\psi_{N-\eta}}\right), \end{aligned} \tag{6a}$$

$$\begin{aligned} &\left|e^{j\psi_i}\right| = 1, \psi_i \in [0, 2\pi), \quad \forall i \in (1, N-\eta), \\ &\boldsymbol{\Theta}_2 = \text{diag}\left(e^{j\phi_1}, \cdots, e^{j\phi_\eta}\right), \end{aligned} \tag{6b}$$

$$\left|e^{j\phi_j}\right| = 1, \phi_j \in [0, 2\pi), \quad \forall j \in (1, \eta). \tag{6c}$$

Clearly, it is quite challenging to solve this optimization problem straightforwardly. Thus, we turn to analyze its security performance with optimal elements allocation and derive the corresponding optimal solutions.

3. Performance Analysis

In the section, the optimization problem of maximizing SC for the proposed system is analyzed under the optimal elements allocation of RIS, and then we derive the optimal solution for such problem. Since the maximum SC must be nonnegative, the $[\cdot]^+$ operation can be omitted without loss of optimality. With the monotonic function $\log(\cdot)$, the objective function in $\mathscr{P}_1$ is reexpressed as

$$R = \max_{\{\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2\}} \frac{1+\gamma_B}{1+\gamma_E}. \tag{7}$$

For simplicity, the reflective passive beamforming with perfect CSI of RIS is taken into account, and we also assume entire elements of the RIS are with the same reflection amplitude [20]. Thus, we have $\mathbf{h}_{R_1B}^H \boldsymbol{\Theta}_1 \mathbf{h}_{SR_1} = \alpha \sum_{i=1}^{N-\eta} e^{j\psi_i} [\mathbf{h}_{SR_1}]_i [\mathbf{h}_{R_1B}]_i$ and $\mathbf{h}_{R_2E}^H \boldsymbol{\Theta}_2 \mathbf{h}_{SR_2} = \alpha \sum_{j=1}^{\eta} e^{j\phi_j} [\mathbf{h}_{SR_2}]_j [\mathbf{h}_{R_2E}]_j$. In the case that S knows the CSI of all channels completely, the optimal reflection phase shift can be obtained through channels. In addition, the optimal phase shift can be derived via the proposition as follows.

Proposition 1. *The optimal RIS phase shift of the communication network is expressed as*

$$\theta_n = \arg(h_{SU}) - \arg\left([\mathbf{h}_{SR}]_n [\mathbf{h}_{RU}]_n\right), \quad n = 1, \cdots, N, \tag{8}$$

where $[\mathbf{h}_{SR}]_n$ *and* $[\mathbf{h}_{RU}]_n$ *represent the n-th element of* $\mathbf{h}_{SR}$ *and* $\mathbf{h}_{RU}$*, respectively.* h_{SU} *and* $\mathbf{h}_{RU}$ *represent the links from BS and RIS to user, respectively, and* $\arg(\cdot)$ *denotes the phase operator.*

Proof. Note that the function $|h_{SU} + \mathbf{h}_{RU}^H \boldsymbol{\Theta} \mathbf{h}_{SR}|^2, U \in \{B, E\}$ can be rewritten as

$$\begin{aligned} &\left|h_{SU} + \mathbf{h}_{RU}^H \boldsymbol{\Theta} \mathbf{h}_{SR}\right|^2 \\ &\quad = |h_{SU}|^2 + \left|\mathbf{h}_{RU}^H \boldsymbol{\Theta} \mathbf{h}_{SR}\right|^2 + 2\left|\mathbf{h}_{RU}^H \boldsymbol{\Theta} \mathbf{h}_{SR}\right| |h_{SU}| \cos \\ &\quad \cdot \left[\arg(h_{SU}) - \arg\left(\mathbf{h}_{RU}^H \boldsymbol{\Theta} \mathbf{h}_{SR}\right)\right], \quad U \in \{B, E\}. \end{aligned} \tag{9}$$

From Equation (9), it can be easily verified that $|h_{SU} + \mathbf{h}_{RU}^H \boldsymbol{\Theta} \mathbf{h}_{SR}|^2$ achieves its maximum value for $\cos[\arg(h_{SU}) - \arg(\mathbf{h}_{RU}^H \boldsymbol{\Theta} \mathbf{h}_{SR})] = 1$, which means that the phase shifts of both direct and cascaded links between the U and S are identical, i.e. $\arg(h_{SU}) = \arg(\mathbf{h}_{RU}^H \boldsymbol{\Theta} \mathbf{h}_{SR})$. Therefore, Equation (8) can be derived, which completes this proof. □

As a result, the maximum achievable SNR can be obtained if the phase shifts satisfy $\psi_i = \arg(h_{SB}) - \arg([\mathbf{h}_{SR_1}]_i [\mathbf{h}_{R_1 B}]_i)$ and $\phi_j = \arg(h_{SE}) - \arg([\mathbf{h}_{SR_2}]_j [\mathbf{h}_{R_2 E}]_j)$, which means that the cascaded links via RIS are with the same phase as the corresponding direct links [21]. Therefore, we have

$$\gamma_B = \frac{P}{\sigma^2} \left| h_{SB} + \alpha \sum_{i=1}^{N-\eta} [\mathbf{h}_{SR_1}]_i [\mathbf{h}_{R_1 B}]_i \right|^2, \tag{10}$$

$$\gamma_E = \frac{P |h_{SE}|^2}{P \left| \alpha \sum_{j=1}^{\eta} [\mathbf{h}_{SR_2}]_j [\mathbf{h}_{R_2 E}]_j \right|^2 + \sigma^2}. \tag{11}$$

From Equations (10) and (11), it is easy to see that the SNR of B and SINR of Eve only rely on the amplitudes of the reflective elements, not on their phases. Therefore, we can reformulate the optimization problem as

$$\mathscr{P}_2 : \max_{\eta} \frac{1 + \gamma_B}{1 + \gamma_E}, \tag{12a}$$

$$\text{s.t.} \quad 0 \le \eta \le N. \tag{12b}$$

Clearly, $\mathscr{P}_2$ is nonconvex and hard to obtain its optimal result. Therefore, we turn to derive its closed form in an approximate way. Assuming the equivalent size for each RIS element, thus, it follows that all elements in $\mathbf{h}_{SR}$, $\mathbf{h}_{R_1 B}$, and $\mathbf{h}_{RE}$ have the same magnitude, respectively. For brevity, we have $|h_{SB}| = \sqrt{\beta_{SB}}$, $|h_{SE}| = \sqrt{\beta_{SE}}$, $1/(N-\eta)\sum_{i=1}^{N-\eta} |[\mathbf{h}_{SR_1}]_i [\mathbf{h}_{R_1 B}]_i| = \sqrt{\beta_{RB}}$, and $1/N\sum_{j=1}^{\eta} |[\mathbf{h}_{SR_2}]_j [\mathbf{h}_{R_2 E}]_j| = \sqrt{\beta_{RE}}$. In addition, $\beta_{RB} = h_{SR} h_{RB}$ and $\beta_{RE} = h_{SR} h_{RE}$, where h_{SR}, h_{RB}, and h_{RE} are the channel coefficients of S, B, and Eve related to a single element of RIS, respectively [22]. It is known that, for a small number of components, the channel gain provided by RIS should be smaller than that of the direct channel. However, as the amount of reflective components grows, the channel gain provided by RIS significantly improves and becomes much larger than that of direct channel. Then, we can reformulate Equations (10) and (11) in the more compact forms as

$$\gamma_B = \frac{P}{\sigma^2} \left(\sqrt{\beta_{SB}} + (N - \eta) \alpha \sqrt{\beta_{RB}} \right)^2, \tag{13}$$

$$\gamma_E = \frac{P \beta_{SE}}{P \alpha^2 \beta_{RE} \eta^2 + \sigma^2}. \tag{14}$$

Since $\gamma_B \gg 1$, letting $1 + \gamma_B \approx \gamma_B$ and with Equations (13) and (14), the secrecy capacity maximization problem can be obtained from

$$\begin{aligned} \frac{\gamma_B}{1 + \gamma_E} &= \frac{(P/\sigma^2) \left(\sqrt{\beta_{SB}} + (N - \eta) \alpha \sqrt{\beta_{RB}} \right)^2}{1 + (P \beta_{SE} / (P \beta_{RE} \alpha^2 \eta^2 + \sigma^2))} \\ &= \frac{P}{\sigma^2} (\alpha_{SB} + (N - \eta) \alpha_{RB})^2 \left(1 - \frac{P \alpha_{SE}^2}{P \alpha_{SE}^2 + P \alpha_{RE}^2 \eta^2 + \sigma^2} \right), \end{aligned} \tag{15}$$

where $\alpha_{SB} = \sqrt{\beta_{SB}}$, $\alpha_{RB} = \alpha \sqrt{\beta_{RB}}$, $\alpha_{SE} = \sqrt{\beta_{SE}}$, and $\alpha_{RE} = \alpha \sqrt{\beta_{RE}}$. Since the term P/σ^2 has no influence on solving the optimization problem in Equation (15) and the approximation $P\alpha_{SE}^2 + \sigma_E^2 \approx P\alpha_{SE}^2$ holds due to $P\alpha_{SE}^2 \gg \sigma_E^2$, the above maximization problem can be simplified as

$$R(\eta) = (\alpha_{SB} + \alpha_{RB}(N - \eta))^2 \left(1 - \frac{\alpha_{SE}^2}{\alpha_{SE}^2 + \alpha_{RE}^2 \eta^2} \right). \tag{16}$$

Since the function in Equation (16) is continuous, we can derive the following expression by its first-derivations as

$$\begin{aligned} \frac{\partial R(\eta)}{\partial \eta} = &\frac{2 \alpha_{SE}^2 (\alpha_{SB} + \alpha_{RB}(N - \eta))}{\left(\alpha_{SE}^2 + \alpha_{RE}^2 \eta^2 \right)^2} \\ &\cdot \left(\alpha_{RB} \alpha_{SE}^2 + (\alpha_{SB} + N \alpha_{RB}) \alpha_{RE}^2 \eta \right) \\ &- 2 \alpha_{RB} (\alpha_{SB} + \alpha_{RB}(N - \eta)). \end{aligned} \tag{17}$$

It is quite difficult to analyze its trend directly from the above formula; then, the second-derivation is derived and simplified as

$$\begin{aligned} \frac{\partial^2 R(\eta)}{\partial \eta^2} = &\frac{2}{\left(\alpha_{SE}^2 + \alpha_{RE}^2 \eta^2 \right)^3} \left(\left(\alpha_{SE}^2 \alpha_{RE}^2 (\alpha_{SB} + \alpha_{RB}(N - 2\eta)) - \alpha_{RB} \alpha_{RE}^4 \eta^3 \right) \right. \\ &\cdot \left(\alpha_{RB} \alpha_{RE}^2 \eta^2 (2\eta - 3N) - 3 \alpha_{SB} \alpha_{RE}^2 \eta^2 + \alpha_{RB} \alpha_{SE}^2 (N - 2\eta) \right. \\ &\left. + \alpha_{SB} \alpha_{SE}^2 \right) - (\alpha_{SB} + \alpha_{RB}(N - \eta)) \left(\alpha_{SE}^2 + \alpha_{RE}^2 \eta^2 \right) \\ &\left. \cdot \left(2 \alpha_{RB} \alpha_{SE}^2 \alpha_{RE}^2 \eta + 3 \alpha_{RB} \alpha_{RE}^4 \eta^3 \right) \right). \end{aligned} \tag{18}$$

Through the positive and negative judgment in Equation (18), we can acquire the monotonicity of the first-derivation expression and further determine whether it has a zero point in the value range. For simplicity let $G_1(\eta) = \alpha_{SE}^2 \alpha_{RE}^2 (\alpha_{SB} + \alpha_{RB}(N - 2\eta)) - \alpha_{RB} \alpha_{RE}^4 \eta^3$, $G_2(\eta) = \alpha_{RB} \alpha_{RE}^2 \eta^2 (2\eta - 3N) - 3\alpha_{SB} \alpha_{RE}^2 \eta^2 + \alpha_{RB} \alpha_{SE}^2 (N - 2\eta) + \alpha_{SB} \alpha_{SE}^2$, and $G_3(\eta) = -(\alpha_{SB} + \alpha_{RB}(N - \eta))(\alpha_{SE}^2 + \alpha_{RE}^2 \eta^2)(2\alpha_{RB} \alpha_{SE}^2 \alpha_{RE}^2 \eta + 3\alpha_{RB} \alpha_{RE}^4 \eta^3)$. Due to the positive characteristic of $2/(\alpha_{SE}^2 + \alpha_{RE}^2 \eta^2)^3$, Equation (18) can be simplified as

$$\frac{\partial^2 R(\eta)}{\partial \eta^2} = G_1(\eta) G_2(\eta) + G_3(\eta). \tag{19}$$

Clearly, $G_1(\eta)$, $G_2(\eta)$, and $G_3(\eta)$ are monotonically decreasing with η, where $G_1(0) > 0$, $G_1(N) < 0$, $G_2(0) > 0$, $G_2(N) < 0$, and $G_3(\eta)$ are always smaller than 0 with the increase of η. Therefore, one can conclude that $G_1(\eta)$ and $G_2(\eta)$ have

zero points in their effective domain, which are denoted by ξ_1 and ξ_2, respectively. For the sake of illustration, letting $\xi_1 < \xi_2$, we have

$$G_1(\eta)G_2(\eta)\begin{cases} >0, & \text{for } 0 \le \eta < \xi_1, \\ <0, & \text{for } \xi_1 \le \eta < \xi_2, \\ >0, & \text{for } \xi_2 \le \eta \le N. \end{cases} \tag{20}$$

Since $G_3(\eta)$ is always smaller than 0 with the increase of η, it can be regarded as a constant and has no effect on the trend of $G_1(\eta)G_2(\eta)$, but it determines their zero points. According to Equation (18), $\partial^2 R(\eta)/\partial\eta^2|_{\eta=0} = 0$. However, the positive or negative of Equation (18) cannot be determined; thus we discuss each case separately. For the case $\partial^2 R(\eta)/\partial\eta^2|_{\eta=N} > 0$, the monotonicity of Equation (18) is similar to that of $G_1(\eta)G_2(\eta)$. However, when $\partial^2 R(\eta)/\partial\eta^2|_{\eta=N} < 0$, the zero point of Equation (18) denoted by ζ exists, and hence, we can conclude

$$\frac{\partial^2 R(\eta)}{\partial\eta^2}\begin{cases} >0, & \text{for } 0 \le \eta < \zeta, \\ <0, & \text{for } \zeta \le \eta < N. \end{cases} \tag{21}$$

Through observing the positive and negative of $\partial^2 R(\eta)/\partial\eta^2$, we know that the first-derivation of $R(\eta)$ tends to increase and then decreases and then maybe increase again with the increase of η, where $\partial R(\eta)/\partial\eta|_{\eta=0} = 0$ and $\partial R(\eta)/\partial\eta|_{\eta=N} < 0$. Therefore, there exists a maximum value of the secrecy rate for the formulated optimization problem, within the scope of its first derivative in solving extreme result. Thus, we can derive the optimal solution by calculating the equation of $\partial R(\eta)/\partial\eta = 0$, and the maximum secrecy capacity is also determined. Letting $\partial R(\eta)/\partial\eta = 0$, the objective function can be simplified as

$$\alpha_{RB}\alpha_{RE}^2\eta^3 + 2\alpha_{RB}\alpha_{SE}^2\eta - \alpha_{SE}^2(\alpha_{SB} + N\alpha_{RB}) = 0. \tag{22}$$

Since $\alpha_{RB}\alpha_{RE}^2 \neq 0$, we can eliminate the coefficient of the first term in Equation (22) and obtain the following equation:

$$\eta^3 + 2\frac{\alpha_{SE}^2}{\alpha_{RE}^2}\eta - \frac{\alpha_{SE}^2}{\alpha_{RB}\alpha_{RE}^2}(\alpha_{SB} + N\alpha_{RB}) = 0. \tag{23}$$

Clearly, Equation (23) is a special cubic equation, which can be solved by the Cardano formula method. From Equation (23), we can find that $\alpha_{SE}^2/\alpha_{RE}^2 \ge 0$ and $\alpha_{SE}^2/\alpha_{RB}\alpha_{RE}^2(\alpha_{SB} + N\alpha_{RB}) \ge 0$, it can be converted into the form of

$$\eta^3 + p\eta + q = 0, \tag{24}$$

where $p = 2\alpha_{SE}^2/3\alpha_{RE}^2$ and $q = -\alpha_{SE}^2/\alpha_{RB}\alpha_{RE}^2(\alpha_{SB} + N\alpha_{RB})$. In addition, due to $p \neq 0$ and $q \neq 0$, letting $\eta = u + v$, we have

$$\eta^3 = (u+v)^3 = u^3 + v^3 + 3uv(u+v) = u^3 + v^3 + 3uv\eta. \tag{25}$$

Comparing the coefficients of Equations (24) and (25) and after some mathematical manipulations, we can obtain

$$\begin{cases} u^3 + v^3 = -q, \\ u^3v^3 = \left(\frac{-p}{3}\right)^3. \end{cases} \tag{26}$$

According to $q^2 + (4p^3/27) > 0$, u^3 and v^3 are two roots of the equation $x^2 + qx - (p/3)^3 = 0$, which can be found by the root formula; the corresponding closed-form expressions can be obtained from

$$\begin{cases} u^* = \sqrt[3]{\frac{-q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}, \\ v^* = \sqrt[3]{\frac{-q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}. \end{cases} \tag{27}$$

In this manner, the optimal solution of Equation (15) can be finally expressed as

$$\eta^* = \lceil u^* + v^* \rceil, \tag{28}$$

where $\lceil\cdot\rceil$ is the ceiling function. Thus, from the closed-form expression of η^*, $N - \eta^*$ can thus be obtained as the optimal number of elements allocated for serving B.

4. Numerical Result Comparison

In the section, we validate the expression of the analysis and evaluate the performance of our considered system with the assistance of the uncertain RIS via simulation results. All links in the system are assumed to follow independent Rayleigh fading with the path loss exponent of 2.2, and the noise variance is -94 dBm. For simplicity, the following node locations are considered: $(x_S, y_S) = (0, 0)$, $(x_R, y_R) = (40, 10)$, $(x_B, y_B) = (50, 0)$, and $(x_E, y_E) = (45, -5)$.

Figure 2 illustrates the variation of achieved rate as the number of elements for Eve with the fixed transmit power $P = 1$W varies, and the total number of elements is set to 1,000. The achievable rates of B and Eve are decreasing when the number of the elements for Eve increases, as shown in the figure. However, the achievable rate at Eve decreases significantly than that of the one at B. It also illustrates that the achievable secrecy rate is first increasing and then decreasing with an increasing number of elements for Eve. Thus, there exits an optimal value of elements for B and Eve as the result of 10.0392 bps/Hz. Through observation, it is known that 450 is the optimal value in the simulation results which are equal to the optimal value obtained from our analysis in Equation (28).

In Figure 3, we compare different schemes of elements allocation versus the transmit power with the power from 1 W to 30 W. By means of the simulation, we compare several models including the proposed scheme, all elements of RIS to enhance secure communication at B, all elements of RIS to interfere Eve, and the model without RIS. For the system without RIS, its achievable secrecy rate is 0 since the

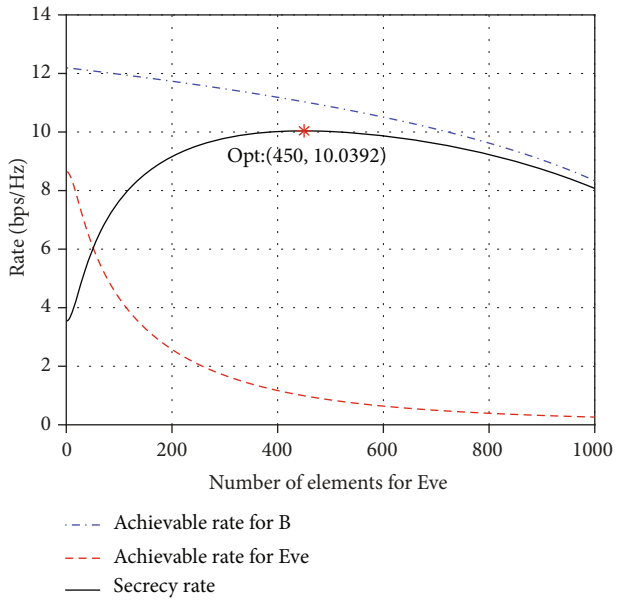

Figure 2: Achievable rate vs. the number of elements for jamming Eve η.

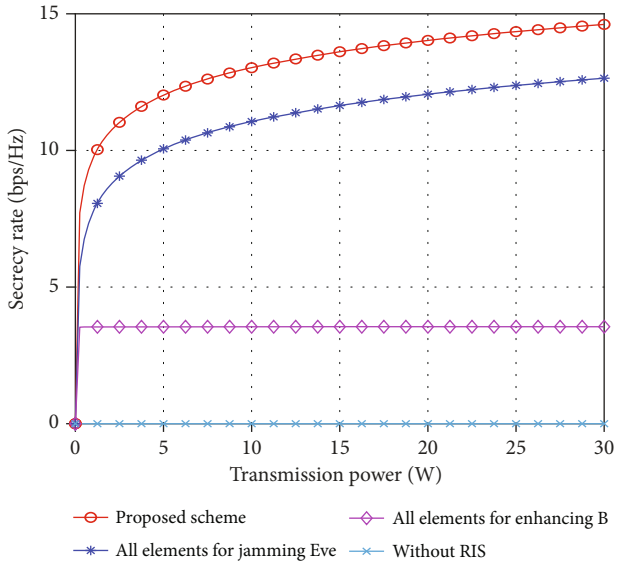

Figure 3: Comparisons of the proposed scheme and other schemes.

achievable rate at Eve is higher than that at B. And when all the components of RIS are used to improve the legitimate communication, the secrecy rate is determined by the CSI instead of the transmission power of base station; thus, the secrecy rate keeps constant under varying transmit power. The achievable secrecy capacity for our considered scheme and the one that all elements to interfere Eve monotonically increase with the increasing transmit power, and our proposed scheme achieves better results. Moreover, it also verifies that our proposed scheme has a higher secrecy capacity than other schemes, which makes it superior compared with than other schemes.

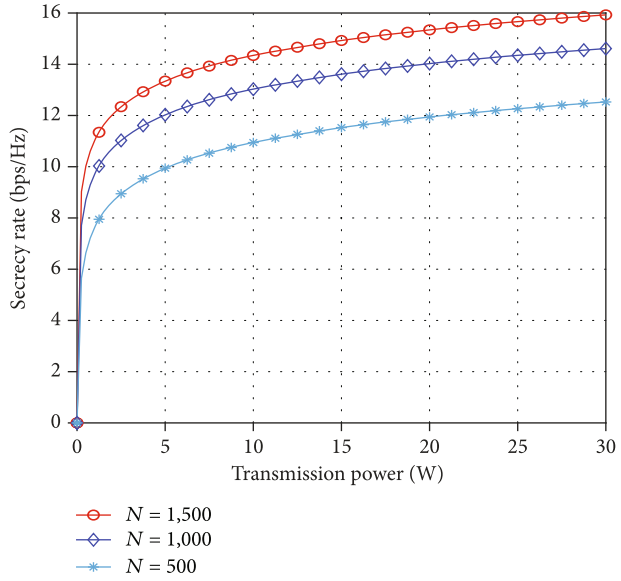

Figure 4: Secrecy rate vs. transmission power P with N = 500,1000,1500.

Figure 4 demonstrates the variation of achievable secrecy rate with total number of elements for RIS, in which N is set to be 500, 1,000, and 1,500. According to the figure, the achievable secrecy capacity is increasing as the transmit power increases. In addition, it reveals that the secrecy rate in the uncertain RIS-assisted communication network increases with an increasing number of components.

5. Conclusions

This paper investigated uncertain RIS-assisted PLS, with the presence of an eavesdropper. The uncertain RIS can enhance the signal for the legitimate user while jamming the eavesdropper by separating the components of RIS into two functional sections. The optimal element allocation and achievable secrecy rate can be obtained in their closed forms by solving the formulated problem. Numerical results verifying the accuracy of the derived expression show the advantage of our considered scheme compared with its counterparts.

Data Availability

The simulation data used to support the findings of this study are available from the author upon request, who can be contacted at 2010310034@stmail.ntu.edu.cn

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grants 61971245 and 61801249.

References

[1] W. Duan, J. Gu, M. Wen, G. Zhang, Y. Ji, and S. Mumtaz, "Emerging technologies for 5G-IoV networks: applications, trends and opportunities," *IEEE Network*, vol. 34, no. 5, pp. 283–289, 2020.

[2] X. Pei, Y. Chen, M. Wen, H. Yu, E. Panayirci, and H. V. Poor, "Next-generation multiple access based on NOMA with power level modulation," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 4, pp. 1072–1083, 2022.

[3] W. Xu, F. Gao, J. Zhang, X. Tao, and A. Alkhateeb, "Deep learning based channel covariance matrix estimation with user location and scene images," *IEEE Transactions on Communications*, vol. 69, no. 12, pp. 8145–8158, 2021.

[4] F. Gao, B. Lin, C. Bian, T. Zhou, J. Qian, and H. Wang, "FusionNet: enhanced beam prediction for mmWave communications using Sub-6 GHz channel and a few pilots," *IEEE Transactions on Communications*, vol. 69, no. 12, pp. 8488–8500, 2021.

[5] M. Wen, Q. Li, K. J. Kim et al., "Private 5G networks: concepts, architectures, and research landscape," *IEEE Journal of Selected Topics in Signal Processing*, vol. 16, no. 1, pp. 7–25, 2022.

[6] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: a review," *China Communications*, vol. 14, no. 12, pp. 1–14, 2017.

[7] C. Huang, S. Hu, G. C. Alexandropoulos et al., "Holographic MIMO surfaces for 6G wireless networks: opportunities, challenges, and trends," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 118–125, 2020.

[8] W. Duan, Y. Ji, J. Hou, B. Zhuo, M. Wen, and G. Zhang, "Partial-DF full-duplex D2D-NOMA systems for IoT with/without an eavesdropper," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6154–6166, 2021.

[9] D.-H. Ha, T. T. Duy, P. N. Son, T. Le-Tien, and M. Voznak, "Security-reliability trade-off analysis for rateless codes-based relaying protocols using NOMA, cooperative jamming and partial relay selection," *IEEE Access*, vol. 9, pp. 131087–131108, 2021.

[10] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: intelligent reflecting surface aided wireless network," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, 2020.

[11] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.

[12] C. Huang, R. Mo, and C. Yuen, "Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 8, pp. 1839–1850, 2020.

[13] Z. Chen, X. Ma, C. Han, and Q. Wen, "Towards intelligent reflecting surface empowered 6G terahertz communications: a survey," *China Communications*, vol. 18, no. 5, pp. 93–119, 2021.

[14] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: a programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82599–82612, 2019.

[15] B. Feng, Y. Wu, and M. Zheng, "Secure transmission strategy for intelligent reflecting surface enhanced wireless system," in *2019 11th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–6, Xi'an, China, Oct. 2019.

[16] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," in *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Waikoloa, HI, USA, Dec. 2019.

[17] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.

[18] H.-M. Wang, J. Bai, and L. Dong, "Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI," *IEEE Signal Processing Letters*, vol. 27, pp. 1300–1304, 2020.

[19] Ö. Özdogan, E. BjÖrnson, and E. G. Larsson, "Intelligent reflecting surfaces: physics, propagation, and pathloss modeling," *IEEE Wireless Communications Letters*, vol. 9, no. 5, pp. 581–585, 2020.

[20] M. Wang, W. Duan, G. Zhang, M. Wen, J. Choi, and P. -H. Ho, "On the achievable capacity of cooperative NOMA networks: RIS or relay?," *IEEE Wireless Communications Letters*, vol. 11, no. 8, 2022.

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

[22] E. Björnson, Ö. Özdogan, and E. G. Larsson, "Intelligent reflecting surface versus decode-and-forward: how large surfaces are needed to beat relaying?," *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 244–248, 2020.