Intelligent Reflecting Surface Aided Multi-Antenna Secure Transmission

Zheng Chu, *Member, IEEE*, Wanming Hao, *Member, IEEE* Pei Xiao, *Senior Member, IEEE*, and Jia Shi, *Member, IEEE*

***Abstract*—In this paper, we propose intelligent reflecting surface (IRS) aided multi-antenna physical layer security. We present a power efficient scheme to design the secure transmit power allocation and the surface reflecting phase shift. It aims to minimize the transmit power subject to the secrecy rate constraint at the legitimate user. Due to the non-convex nature of the formulated problem, we propose an alternative optimization algorithm and the semidefinite programming (SDP) relaxation to deal with this issue. Also, the closed-form expression of the optimal secure beamformer is derived. Finally, simulation results are presented to validate the proposed algorithm, which highlights the performance gains of the IRS to improve the secure transmission.**

***Index Terms*—Intelligent reflecting surface, physical-layer secrecy, secure beamforming, phase shift.**

I. Introduction

With the evolution of the fifth-generation (5G) and beyond, high data rate and massive wireless connectivity are in great demand, causing more concerns on the network energy consumption [1]. The energy constrain is a critical issue in various practical applications. Generally, the energy constrain challenge can be overcome by joint utilization of renewable energy source, energy-efficient devices, effective deployment techniques, as well as energy-efficient resource allocation and signal processing algorithms [2], [3]. However, several renewable energy sources and energy-efficient devices may incur high hardware cost. Thus, it is necessary to design an energy-efficient technique with low hardware cost to build a sustainable and green wireless network [4].

On the other hand, the security of communications should be guaranteed for protecting the important/privacy information transmission, e.g., bank card information, pricing information, and mobile data message. Traditionally, secure transmission is realized by conventional cryptographic methods in the network layer, but those schemes lead to variety of technical challenges on the key distribution and management in the communication link. Thus, physical layer security is developed based on the information theory and a novel metric, secrecy capacity, of the random channel [5]. Recently, variety of resource allocation approaches have been widely applied to physical layer security to improve the secrecy capacity. Also, physical layer security has been considered in the multi-antenna scenario, and resource allocation and signal processing algorithms [6]–[8]. In secure transmissions, the transmit power consumption is an important indicator for the improvement of the secrecy capacity, and the transmit power at the BS should be minimized to guarantee the transmission requirement of secrecy metric [9], [10].

In order to ensure the secure communication with low power consumption, this paper first proposes a novel transceiver-like technique, i.e., intelligent reflecting surface (IRS)[1], to support the multi-antenna secure communication. IRS, a planar array, is composed of some reconfigurable reflector elements, and controlled by a communication-oriented software (e.g. IRS controller) [11], [12]. The IRS reflecting elements are generally made of small, very low-cost, and low energy consumption components which efficiently reflect the desired signal with an appropriate phase shift without a dedicated RF processing, en/de-coding, or re-transmission [11]. In [12], large IRS is introduced to shape the radio waves, improving the network coverage, also it backscatters the radio waves generated by cellular base stations to smart devices. Unlike the active intelligent surface based massive multiple-input multiple-output (MIMO) in [13], the IRS owns flexible operation mechanism and an array architecture to passively receive and reflects the desired signal to maximize the total received power at the user. In comparison with the existing secure transmission schemes, e.g., information-jamming-aided secure communication [14] and the relaying-aided secure communication [15], the IRS-aided secure transmission does not employ an extra transmitter (i.e., information jammer or relay) to generate the same/new signals to enhance the receive power at the legitimate user or to introduce more interference to degrade the reception at the eavesdropper. Thus, this transmission mechanism introduces no extra power consumption. In addition, by operating in the full duplex (FD) mode, the IRS-aided scheme achieves higher spectrum efficiency than the relay-aided scheme with the half duplex (HD) mode [11]. Inspired by those desired properties of the IRS, we apply the IRS technique to secure communications, where the desired signal can be reflected by the IRS elements. By adjusting the phase shifts of the IRS, the transmit power at the base station (BS) is minimized while quarantining the secure transmission quality of the legitimate user.

In this paper, we consider a classic multi-antenna secrecy channel, where a multi-antenna BS with the aid of an IRS establishes a secure link with a single-antenna legitimate

This work was supported by the U.K. Engineering and Physical Sciences Research Council under Grant EP/R001588/1. The authors also would like to acknowledge the support of the University of Surrey 5GIC (http://www.surrey.ac.uk/5gic) members for this work.

Z. Chu, and P. Xiao are working with the Institute for Communication Systems, University of Surrey, Guildford GU2 7XH, UK. (Email: zheng.chu@surrey.ac.uk, p.xiao@surrey.ac.uk)

W. Hao is working with the School of Information Engineering, Zhengzhou University, Zhengzhou 450000, China. (Email: wmhao@hotmail.com)

J. Shi is working with The State Key Laboratory of Integrated Service Networks, Xidian University, Xian 710071, China. (Email: jiashi@xidian.edu.cn)

[1]It is also known as reconfigurable intelligent surface (RIS).

user in the presence of a single-antenna eavesdropper. *The contributions of this paper are summarized as follows:*

1) We minimize the transmit power at the BS subject to the secrecy rate constraint. Our aim is to design the secure transmit beamformer at the BS and the reflecting beamformer via the phase shifter at the IRS. Due to non-convexity of this problem, we propose an alternative optimization algorithm[2] and semidefinite programming (SDP) relaxation to tackle this non-convex optimization problem.
2) In order to gain more insights and reduce the computation complexity, we derive a closed-form transmit beamforming vector via dual problem and KKT conditions. In addition, a randomization technique is applied to generate the feasible solution for the high-rank phase shift matrix.

II. System Model

In this paper, we consider an IRS-aided multi-antenna secure transmission as depicted in Fig. 1, where a multi-antenna BS establishes a reliable link with a single-antenna legitimate user in the presence of a single-antenna passive eavesdropper. Each receiver (i.e., legitimate user/eavesdropper) generally probes two path superimposed signals from both the BS-user/eavesdropper link and BS-IRS-user/eavesdropper link. We assume that the BS is equipped with N_T transmit antennas, the IRS is mounted with N_R reflecting units. The IRS controller is required to coordinate its working modes, including reception mode to estimate the channel state information (CSI) and reflection mode for data transmission. The channel coefficients of the BS-user link, the BS-eavesdropper link, the BS-IRS link, the IRS-user link, and the IRS-eavesdropper link are denoted by $\mathbf{h}_s \in \mathbb{C}^{N_T\times 1}$, $\mathbf{h}_e \in \mathbb{C}^{N_T\times 1}$, $\mathbf{G}_1 \in \mathbb{C}^{N_T\times N_R}$, $\mathbf{h}_{rs} \in \mathbb{C}^{N_R\times 1}$, and $\mathbf{h}_{re} \in \mathbb{C}^{N_R\times 1}$, respectively.

The IRS elements receive all multi-path received signals at a physical point, and reflect this combined signal from this point via IRS planar array. We denote $\boldsymbol{\Psi} =$

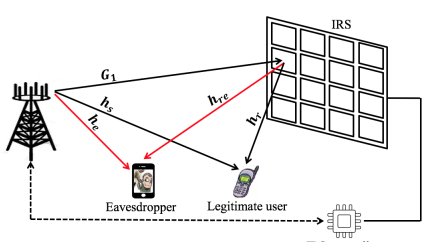


Fig. 1: An IRS-aided multi-antenna secure communication.

$\mathrm{Diag}\left(\beta\exp(j\alpha_1), \beta\exp(j\alpha_2), \cdots, \beta\exp(j\alpha_{N_R})\right)$ as the diagonal matrix associated with the effective phase shifts in all IRS elements, where $\alpha_n \in [0, 2\pi]$ and $\beta \in [0, 1]$ are the phase shift and amplitude reflection coefficient on the combined desired signal, respectively [11].[3] Thus, the received signal at the legitimate user and the eavesdropper can be written, respectively, as

$$y_s = \left(\mathbf{h}_s^H + \mathbf{h}_{rs}^H \boldsymbol{\Psi}\mathbf{G}_1\right)\mathbf{x} + n_s,\ \ y_e = \left(\mathbf{h}_e^H + \mathbf{h}_{re}^H \boldsymbol{\Psi}\mathbf{G}_1\right)\mathbf{x} + n_e,$$

where $n_i \sim \mathcal{CN}(0, \sigma_i^2)$, $i \in (s, e)$ denote the thermal noise at the legitimate user or the eavesdropper with a zero-mean complex circularly symmetric Gaussian variable with variance σ_i^2, respectively. Also, $\mathbf{x} = \mathbf{w}\mathbf{s}$ denotes the desired signal at the BS, where $\mathbf{s}$ denotes the desired signal for the legitimate user with $\mathbb{E}\{|s|^2\} = 1$, and $\mathbf{w} \in \mathbb{C}^{N_T\times 1}$ is the secure transmit beamformer. Accordingly, the mutual information at the user and the eavesdropper can be given by $\mathcal{R}_u = \log_2\left(1 + \frac{\left|\left(\mathbf{h}_s^H + \mathbf{h}_{rs}^H \boldsymbol{\Psi}\mathbf{G}_1\right)\mathbf{w}\right|^2}{\sigma_s^2}\right)$, and $\mathcal{R}_e = \log_2\left(1 + \frac{\left|\left(\mathbf{h}_e^H + \mathbf{h}_{re}^H \boldsymbol{\Psi}\mathbf{G}_1\right)\mathbf{w}\right|^2}{\sigma_e^2}\right)$. The achievable secrecy rate is given by $\mathcal{R}_s = \left[\mathcal{R}_u - \mathcal{R}_e\right]^+$, where $[x]^+ = \max(x, 0)$.

A. Problem Formulation

In this subsection, we consider a power efficient design to optimize the secure transmit power allocation and the surface reflecting phase shift. We aim to minimize the secure transmit power subject to the secrecy rate constraints, which can be formulated as

$$\min_{\mathbf{w}, \boldsymbol{\Psi}} \ \|\mathbf{w}\|^2,$$
$$s.t.\ \mathcal{R}_s(\mathbf{w}, \boldsymbol{\Psi}) \geq \bar{R}, \tag{1a}$$
$$|\exp(j\alpha_n)| = 1,\ \forall n = 1, ..., N_R, \tag{1b}$$

where $\bar{R}$ is the target secrecy rate. Problem (1) is non-convex due to the secrecy rate constraint (1a), and thus it cannot be solved directly to jointly design the optimal secure transmit beamformer $\mathbf{w}$ and IRS phase shift α_n. In the following, we propose an alternative algorithm to optimize the secure transmit beamformer and the phase shift.

III. Solution to Problem (1)

In this section, we propose an alternative optimization algorithm to design the secure transmit beamformer $\mathbf{w}$ and the phase shift $\boldsymbol{\Psi}$ alternatively. In addition, the optimal beamformer is derived in terms of closed-form solution. Furthermore, a randomization scheme is presented to tackle the high-rank phase shift matrix due to the SDP relaxation.

A. Optimal Secure Transmit Beamformer Design

In this section, we solve problem (1) to achieve the optimal secure transmit beamformer $\mathbf{w}$ for given phase shift $\boldsymbol{\Psi}$. Thus, problem (1) can be simplified as

$$\min_{\mathbf{w}} \ \|\mathbf{w}\|^2, \tag{2a}$$
$$s.t.\ \mathcal{R}_u - \mathcal{R}_e \geq \bar{R}. \tag{2b}$$

[2] Although similar alternative optimization algorithms have been employed in our work, the solution in [11] and [16] are not applicable to our work which mainly focuses on the secrecy communication.

[3] In this paper, we assume $\beta = 1$ which is to maximize the reflected signal for each element of the IRS [11]. Note that the phase shifts is assumed to be continuously located in $[0, 2\pi]$. However, they are in practical selected with a finite number of discrete phase shift codebooks from 0 to 2π for the circuit implementation [16]. Particularly, we first need to require a proper initialization of the discrete phase shifts, which is gained via solving the formulated problem in Section III-A, and then quantizing these continuous phase shifts to their nearest points from the discrete phase shift codebooks.

Problem (2) is still non-convex. Next, we consider semidefinite programming (SDP) relaxation to solve it. Let us denote $\bar{\mathbf{h}}_s = \left(\mathbf{h}_s^H + \mathbf{h}_{rs}^H \mathbf{\Psi} \mathbf{G}_1\right)^H$, $\bar{\mathbf{h}}_e = \left(\mathbf{h}_e^H + \mathbf{h}_{re}^H \mathbf{\Psi} \mathbf{G}_1\right)^H$, and define $\mathbf{W} = \mathbf{w}\mathbf{w}^H$, we have

$$\min_{\mathbf{W}} \ \mathrm{Tr}(\mathbf{W}), \ s.t. \ \mathrm{rank}(\mathbf{W}) = 1,$$

$$\frac{1}{\sigma_s^2}\mathrm{Tr}\left[\bar{\mathbf{h}}_s \bar{\mathbf{h}}_s^H \mathbf{W}\right] - \frac{2^{\bar{R}}}{\sigma_e^2}\mathrm{Tr}\left[\bar{\mathbf{h}}_e \bar{\mathbf{h}}_e^H \mathbf{W}\right] \geq 2^{\bar{R}} - 1, \tag{3a}$$

$$\mathbf{W} \succeq \mathbf{0}. \tag{3b}$$

Problem (3) is a standard SDP via removing the non-convex rank-one constraint, which can be solved by convex optimization solvers [17], e.g., CVX. In order to gain more insights and reduce the computational complexity, we derive a closed-form solution for the secure beamformer $\mathbf{w}$.

Theorem 1: The optimal solution to problem (2) is derived in terms of following closed-form expression $p^* = \mu^*(2^{\bar{R}} - 1), \mathbf{w}^* = \sqrt{p^*}\mathbf{v}^*$, $\mu^* = \frac{1}{\lambda_{\max}\left(\frac{1}{\sigma_s^2}\bar{\mathbf{h}}_s\bar{\mathbf{h}}_s^H - \frac{2^{\bar{R}}}{\sigma_e^2}\bar{\mathbf{h}}_e\bar{\mathbf{h}}_e^H\right)}$, $\mathbf{v}^* = \frac{\bar{\mathbf{w}}^*}{\|\bar{\mathbf{w}}^*\|_2}$, and $\bar{\mathbf{w}}^* = \nu_{\max}\left(\frac{1}{\sigma_s^2}\bar{\mathbf{h}}_s\bar{\mathbf{h}}_s^H - \frac{2^{\bar{R}}}{\sigma_e^2}\bar{\mathbf{h}}_e\bar{\mathbf{h}}_e^H\right)$, where $\lambda_{\max}(*)$ denotes the maximum eigenvalue, and $\nu_{\max}(*)$ is the eigenvector associated with the maximum eigenvalue.

Proof: Refer to Appendix. ■

B. Phase Shift Design

In this subsection, we design the IRS phase shift $\mathbf{\Psi}$ for given secure transmit beamformer $\mathbf{w}$ obtained in Section III-A. We denote $b_i = \mathbf{h}_i^H \mathbf{w}$, $\mathbf{r}^H \mathbf{a}_i = \mathbf{h}_{ri}^H \mathbf{\Psi} \mathbf{G}_1 \mathbf{w}$, $\forall i \in \{s, e\}$, where $\mathbf{r} = [\exp(j\alpha_1), \exp(j\alpha_1), \cdots, \exp(j\alpha_N)]^H$ and $a_i = \mathrm{Diag}\left(\mathbf{h}_{ri}\right)\mathbf{G}_1\mathbf{w}$, $\forall i \in \{s, e\}$ and problem (1) can be reduced to

$$\textbf{Find} \ \ \mathbf{r}, \ s.t. \ \log_2 \frac{1 + \frac{1}{\sigma_s^2}\left|\mathbf{r}^H \mathbf{a}_s + b_s\right|^2}{1 + \frac{1}{\sigma_e^2}\left|\mathbf{r}^H \mathbf{a}_e + b_e\right|^2} \geq \bar{R}, \tag{4a}$$

$$|\mathbf{r}(n)|^2 = 1, \ \forall n \in [1, N]. \tag{4b}$$

Problem (4) is still intractable due to (4a), thus, we consider the following equivalent modifications to deal with this non-convex constraint $\left|\mathbf{r}^H \mathbf{a}_i + b_i\right|^2 = \bar{\mathbf{r}}^H \mathbf{V}_i \bar{\mathbf{r}}$, where $\bar{\mathbf{r}} = \left[\mathbf{r}^H \ 1\right]^H$, and $\mathbf{V}_i = \begin{bmatrix} \mathbf{a}_i \mathbf{a}_i^H & \mathbf{a}_i b_i^H \\ b_i \mathbf{a}_i^H & |b_i|^2 \end{bmatrix}$, $\forall i \in \{s, e\}$. To this end, (4) is equivalently modified as

$$\textbf{Find} \ \mathbf{r}, \ s.t. \ \frac{1}{\sigma_s^2}\bar{\mathbf{r}}^H \mathbf{V}_s \bar{\mathbf{r}} - \frac{2^{\bar{R}}}{\sigma_e^2}\bar{\mathbf{r}}^H \mathbf{V}_e \bar{\mathbf{r}} \geq 2^{\bar{R}} - 1, \ (4b). \tag{5}$$

Next, we employ SDP relaxation to deal with (5) by defining $\mathbf{R} = \bar{\mathbf{r}}\bar{\mathbf{r}}^H$. This definition guarantees $\mathbf{R} \succeq \mathbf{0}$ and $\mathrm{rank}(\mathbf{R}) = 1$. Thus, (5) can be relaxed as

$$\textbf{Find} \ \ \mathbf{R}, \ s.t. \ \frac{1}{\sigma_s^2}\mathrm{Tr}\left[\mathbf{R}\mathbf{V}_s\right] - \frac{2^{\bar{R}}}{\sigma_e^2}\mathrm{Tr}\left[\mathbf{R}\mathbf{V}_e\right] \geq 2^{\bar{R}} - 1,$$

$$\mathbf{R}(n, n) = 1, \ \forall n \in [1, N], \ \mathbf{R} \succeq \mathbf{0}, \ \mathrm{rank}(\mathbf{R}) = 1. \tag{6}$$

It is easily verified that problem (6) is a standard SDP via removing the non-convex rank-one constraint, which can be solved in a similar way to Section III-A. In general, the relaxed problem (6) may not yield a rank-one solution, i.e., $\mathrm{rank}(\mathbf{R}) \neq 1$, which reveals that the SDP relaxation is not tight. Thus, we develop a construction method to obtain a rank-one solution. Particularly, we employ the eigenvalue decomposition of $\mathbf{R}$ as $\mathbf{R} = \mathbf{U}\mathbf{\Theta}\mathbf{U}^H$, and the feasible beamforming vector of (5) is constructed as

$$\bar{\mathbf{r}} = \mathbf{U}\mathbf{\Theta}^{\frac{1}{2}}\boldsymbol{\kappa}, \tag{7}$$

where $\mathbf{U} \in \mathbb{C}^{(N_R+1)\times(N_R+1)}$ and $\mathbf{\Theta} \in \mathbb{C}^{(N_R+1)\times(N_R+1)}$ are a unitary matrix and diagonal matrix with eigenvalues arranged in decreasing order, respectively, and $\boldsymbol{\kappa}$ is a vector of complex circularly symmetric uncorrelated Gaussian random variables with zero-mean and unit variance. However, problem (6) may not guarantee its constraints with the independently generation of Gaussian random vector $\boldsymbol{\kappa}$. Thus, we need to re-scale the phase shift vector $\bar{\mathbf{r}}$ with an appropriate scaling factor ξ to satisfy all constraints,

$$\tilde{\mathbf{r}} = \xi\bar{\mathbf{r}}. \tag{8}$$

We substitute (8) into problem (6),

$$\textbf{Find} \ \ \xi, \ s.t. \ \frac{1}{\sigma_s^2}\mathrm{Tr}\left[\tilde{\mathbf{R}}\mathbf{V}_s\right] - \frac{2^{\bar{R}}}{\sigma_e^2}\mathrm{Tr}\left[\tilde{\mathbf{R}}\mathbf{V}_e\right] \geq 2^{\bar{R}} - 1,$$

$$\tilde{\mathbf{R}}(n, n) = 1, \ \forall n \in [1, N], \ \tilde{\mathbf{R}} \succeq \mathbf{0}, \tag{9}$$

where $\tilde{\mathbf{R}} = \rho\bar{\mathbf{r}}\bar{\mathbf{r}}^H$, $\rho = \xi^2$. The above problem is a standard linear programming (LP), which can be solved easily, and then $\bar{\mathbf{r}}$ can be generated via (7) and (8). Finally, we recover the solution $\mathbf{r}$ to problem (4) via $\mathbf{r} = \exp\left(j\arg\left(\left[\frac{\bar{\mathbf{r}}}{\bar{\mathbf{r}}(N+1)}\right]_{(1:N)}\right)\right)$, where $[\mathbf{x}]_{1:N_R}$ is the first N_R elements of the vector $\mathbf{x}$, and $\arg(\mathbf{x})$ represents each element of the vector $\mathbf{x}$ corresponding to the phase. We summarize the proposed algorithm in *Algorithm* 1.

Algorithm 1: Alternative optimization algorithm to solve problem (1).

---

1) **Initialization**: IRS phase shift $\boldsymbol{\alpha}^{(0)} = [\alpha_1^0, \alpha_1^{(0)}, \cdots, \alpha_{N_R}^{(0)}]$.
2) **Repeat**:
   a) **Obtain** the optimal secure transmit beamformer $\mathbf{w}^{(n)}$ via *Theorem* 1 or solving problem (3) for given $\boldsymbol{\alpha}^{(n)}$.
   b) **Solve** problem (6) for given $\mathbf{w}^{(n)}$ to obtain the solution of the IRS phase shift according to (7) and (8).
   c) **Update** $n = n + 1$.
3) **Until** Convergence

Now, we analyze the computational complexity of **Algorithm 1**. According to [18], the complexity is given by $\mathcal{O}\left(m\sqrt{\psi}\ln\left(\frac{1}{\omega}\right)(N^3 + 1 + N) + m(N^2 + 1 + N) + m^2\right)$, where ω is iteration accuracy, $\psi = N$ denotes the threshold parameter related to the constraints, and $m = \mathcal{O}(N^2)$.

To proceed, we characterize the convergence of *Algorithm* 1 via the following *lemma*:

Lemma 1: The secure transmit power allocation is non-increasing over each iteration via *Algorithm* 1.

Proof: Refer to [11]. ■

IV. Simulation Results

In this section, numerical results are presented to validate the effectiveness of the proposed scheme. It is assumed that the number of the transmit antennas is $N_T = 8$. An uniform rectangular array (URA) is deployed at the IRS in x-axis and y-axis, i.e., $N_R = N_R^x N_R^y$ where N_R^x and N_R^y denote the numbers of reflecting elements along with the

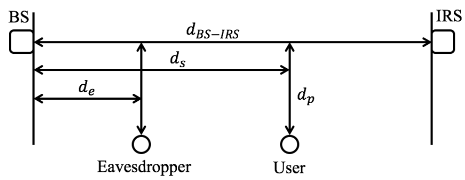


Fig. 2: System deployment.

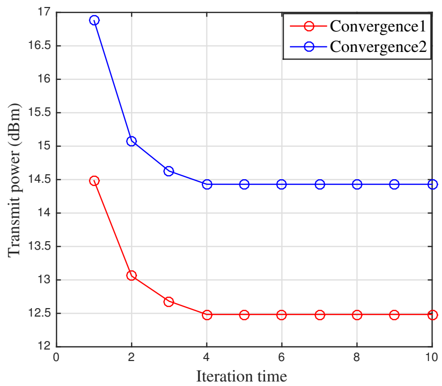
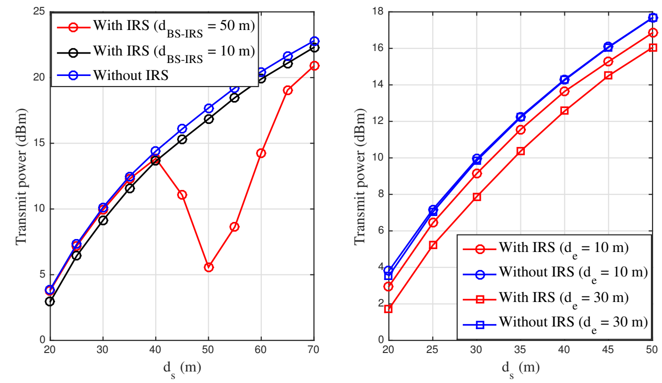


Fig. 3: Convergence of *Algorithm* 1.

x-axis and y-axis, respectively. We set $N_R^x = 5$ and linearly increases N_R^y with N_R. We assume that the noise power is $\sigma_s^2 = \sigma_e^2 = 10^{-9}$ W. All small-scale channel coefficients are generated as the identical and circularly complex Gaussian random variable with zero mean and unit variance. The large-scale path loss is dependent on the distance between any two nodes, which is given by $PL = A\left(\frac{d}{d_0}\right)^{-\rho}$, where A denotes the path loss at the reference distance $d_0 = 1$ m which is set to $A = -10$ dB. d represents the communication link distance of the BS-user (i.e., $d_{\text{BS-user}}$), the BS-eavesdropper (i.e., $d_{\text{BS-eve}}$), the BS-IRS (i.e., $d_{\text{BS-IRS}}$), the IRS-user (i.e., $d_{\text{IRS-user}}$) and the IRS-eavesdropper (i.e., $d_{\text{IRS-eve}}$), respectively. ρ is the path loss exponent. As illustrated in Fig. 2, it is assumed that the legitimate user and eavesdropper are placed in parallel to that of the BS and the IRS, where we consider two different cases in the simulation. The distance between the BS and the IRS is set to $d_{\text{BS-IRS}} = 50$ m or 10 m, and the distances of the vertical line is assumed $d_p = 2$ m. Accordingly, the distances of the BS-user link, the BS-eve link, the IRS-user, and the IRS-eve link are given by $d_{\text{BS-user}} = \left(d_s^2 + d_p^2\right)^{\frac{1}{2}}$, $d_{\text{BS-eve}} = \left(d_e^2 + d_p^2\right)^{\frac{1}{2}}$, $d_{\text{IRS-user}} = \left((d_{\text{BS-IRS}} - d_s)^2 + d_p^2\right)^{\frac{1}{2}}$, $d_{\text{IRS-eve}} = \left((d_{\text{BS-IRS}} - d_e)^2 + d_p^2\right)^{\frac{1}{2}}$. The path loss exponents of the BS-user link, the BS-eve link, the IRS-user link, the IRS-eve link, and the BS-IRS link are set to $\rho_{\text{BS-user}} = \rho_{\text{BS-user}} = 4$, $\rho_{\text{IRS-user}} = \rho_{\text{IRS-eve}} = \rho_{\text{BS-IRS}} = 2$, respectively.

First, we evaluate the convergence of *Algorithm* 1 in Fig. 3. From this figure, it is observed that the secure transmit power first decreases and then converges to a fixed value, which verifies the effectiveness of the proposed alternative optimization algorithm.



(a) Case 1

(b) Case 2

Fig. 4: Transmit power versus distance d_s.

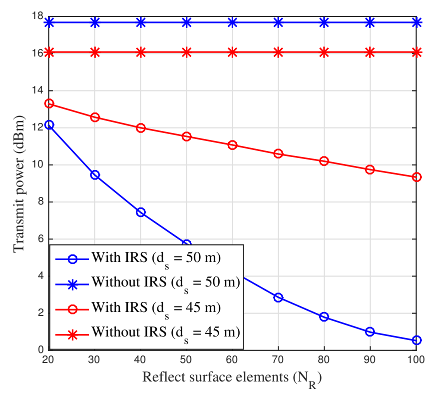


Fig. 5: Transmit power versus reflecting surface elements N_R.

Next, we evaluate the secure transmit power versus the distance d_s in Fig. 4 for two cases (i.e., $d_{\text{BS-IRS}} = 50$ m and $d_{\text{BS-IRS}} = 10$ m). From Fig. 4(a), one can observe that the power consumption of the proposed IRS aided scheme increases with the distance d_s from 20 m to 40 m, and it is comparable to the scheme without the IRS. This is due to the fact that the user moves farther away from the BS, which leads to increasing power consumption, also the IRS cannot reap its advantage to improve the security. When d_s increases to approximately 40 m to 50 m, the power consumption of the IRS-aided scheme begins to decrease and obviously outperforms that without the IRS. This is owing to the fact that when the legitimate user moves closer to the IRS, it will receive a strong reflected signal from the IRS, manifesting the benefits of the IRS. As the distance d_s continues to increase, i.e., $d_s \geq 50$ m, the reflected signal from the IRS becomes weaker, thus more transmit power is consumed but still achieves a better performance than that without the IRS. In Fig. 4(b), the secure transmit power is evaluated with the distance $d_{\text{BS-IRS}} = 10$ m. It is observed from this figure that the IRS-aided scheme outperforms that without the IRS in terms of the secure transmit power, which also highlights the effectiveness of the IRS.

Fig. 5 shows the secure transmit power versus the reflecting surface elements N_R with d_s in order to highlight the

IRS. The legitimate user is placed nearer to the IRS, i.e., $d_s = 45,$ or 50 m, the IRS-aided scheme becomes more effective as the reflecting surface elements N_R increases, and it outperforms that without the IRS which remains constant with N_R. This is due to the fact that larger reflecting elements of the IRS brings a stronger reflected signal to enhance the reception at the legitimate user.

V. Conclusion

This paper proposed IRS aided multi-antenna secure communications. The power efficient design is investigated to minimize the transmit power subject to the secrecy rate constraint at the legitimate user. Due to the non-convex nature of the formulated problem, we propose an alternative optimization algorithm and the SDP relaxation to optimize the secure transmit power allocation and the surface reflecting phase shift alternatively. In addition, the optimal secure beamformer is derived in terms of the closed-form expression, and the rank-relaxation methods for the reflecting phase shift matrix is presented. Finally, simulation results were presented to demonstrate the effectiveness of the proposed algorithm and superiority of the IRS-aided scheme compared to the scheme without the IRS.

Appendix

In order to prove *Theorem* 1, the dual problem to (2) is first investigated, and the Lagrange function is given by $\mathcal{L}(\mathbf{w},\mu)=\mathbf{w}^H\mathbf{w} + \mu\left[2^{\bar{R}}\left(1+\frac{1}{\sigma_s^2}\mathbf{w}^H\bar{\mathbf{h}}_e\bar{\mathbf{h}}_e^H\mathbf{w}\right)-\left(1+\frac{1}{\sigma_e^2}\mathbf{w}^H\bar{\mathbf{h}}_s\bar{\mathbf{h}}_s^H\mathbf{w}\right)\right]$, where $\mu \geq 0$ is the Lagrange multiplier associated with the constraint (2b). The dual problem to (2) is expressed as

$$\max_{\mu\geq 0}\mu(2^{\bar{R}}-1), s.t.\ \mathbf{A}=\mathbf{I}-\mu\left(\frac{1}{\bar{\sigma}_s^2}\mathbf{h}_s\mathbf{h}_s^H-\frac{2^{\bar{R}}}{\bar{\sigma}_e^2}\mathbf{h}_e\mathbf{h}_e^H\right)\succeq\mathbf{0}. \quad (10)$$

Next, we consider the Lagrangian function of (3) as $\mathcal{L}(\mathbf{W},\mu_1,\mathbf{B}) = \mathrm{Tr}\left[\left(\mathbf{I}+\frac{2^{\bar{R}}\mu_1}{\sigma_e^2}\bar{\mathbf{h}}_e\bar{\mathbf{h}}_e^H-\frac{\mu_1}{\sigma_s^2}\bar{\mathbf{h}}_s\bar{\mathbf{h}}_s^H-\mathbf{B}\right)\mathbf{W}\right] + \mu_1(2^{\bar{R}}-1)$, where $\mu_1 \geq 0$ and $\mathbf{B}\succeq\mathbf{0}$ are the dual variables with the constraints (3a) and (3b), respectively. Thus, its dual problem is given by

$$\max_{\mu_1\geq 0}\mu_1(2^{\bar{R}}-1), s.t.\mathbf{B}=\mathbf{I}-\mu_1\left(\frac{1}{\sigma_s^2}\bar{\mathbf{h}}_s\bar{\mathbf{h}}_s^H-\frac{2^{\bar{R}}}{\sigma_e^2}\bar{\mathbf{h}}_e\bar{\mathbf{h}}_e^H\right)\succeq\mathbf{0}. \quad (11)$$

One can observe that the dual problems (10) and (11) are identical. Therefore, both problems hold the same solution. To proceed, we need to show that there exists at least one zero eigenvalue in $\mathbf{B}$, which indicates the same property holds in $\mathbf{A}$ as well. By exploiting matrix rank property [19], i.e., $\mathrm{rank}(\mathbf{X}-\mathbf{Y}) \geq \mathrm{rank}(\mathbf{X}) - \mathrm{rank}(\mathbf{Y})$, we have

$$\mathrm{rank}(\mathbf{B})\geq\mathrm{rank}(\mathbf{Y})-\mathrm{rank}\left(\frac{\mu_1}{\sigma_s^2}\bar{\mathbf{h}}_s\bar{\mathbf{h}}_s^H\right), \quad (12)$$

where $\mathbf{Y} = \mathbf{I} + \frac{\mu_1 2^{\bar{R}}}{\sigma_e^2}\mathbf{h}_e\mathbf{h}_e^H$. From (12), it is observed that $\mathrm{rank}(\mathbf{B})$ is either N_T or $N_T - 1$. If $\mathrm{rank}(\mathbf{B}) = N_T$, it leads to $\mathbf{W} = \mathbf{0}$, which violates $\bar{R} > 0$. Thus, $\mathrm{rank}(\mathbf{B}) = N_T - 1$ holds, which shows that there exists at least one zero eigenvalue for $\mathbf{B}$. Similarly, $\mathbf{A}$ includes at least one zero eigenvalue as well. On the other hand, the optimal solution of μ is the maximum value to guarantee the constraint in (10), which is derived as $\mu^* = \frac{1}{\lambda_{\max}\left(\frac{1}{\sigma_s^2}\bar{\mathbf{h}}_s\bar{\mathbf{h}}_s^H-\frac{2^{\bar{R}}}{\sigma_e^2}\bar{\mathbf{h}}_e\bar{\mathbf{h}}_e^H\right)}$. Since problem (2) can be reformulated into a convex optimization problem, the strong duality holds between problem (2) and its dual problem (10). Thus, the minimum transmit power is given by $p^* = \mu^*(2^{\bar{R}} - 1)$. Problem (2) is equivalently modified as

$$\min_{\mathbf{v},p} p\mathbf{v}^H\mathbf{v}, s.t.\frac{\mathbf{v}^H(\mathbf{I}+\frac{p}{\sigma_s^2}\bar{\mathbf{h}}_s\bar{\mathbf{h}}_s^H)\mathbf{v}}{\mathbf{v}^H(\mathbf{I}+\frac{p}{\sigma_e^2}\bar{\mathbf{h}}_e\bar{\mathbf{h}}_e^H)\mathbf{v}}\geq 2^{\bar{R}}, \mathbf{v}^H\mathbf{v}=1, p\geq 0. \quad (13)$$

According to (13) and the fact that the optimal secure beamformer $\mathbf{w}$ lies in the null space of $\mathbf{Y}$, we have $\mathbf{w}^*=\sqrt{p^*}\mathbf{v}^*$, $\mathbf{v}^*=\frac{\bar{\mathbf{w}}^*}{\|\bar{\mathbf{w}}^*\|_2}$, and $\bar{\mathbf{w}}^*=\nu_{\max}\left(\frac{1}{\sigma_s^2}\bar{\mathbf{h}}_s\bar{\mathbf{h}}_s^H-\frac{2^{\bar{R}}}{\sigma_e^2}\bar{\mathbf{h}}_e\bar{\mathbf{h}}_e^H\right)$.

References

[1] Y. Chen, S. Zhang, S. Xu, and G. Y. Li, "Fundamental trade-offs on green wireless networks," *IEEE Commun. Mag.*, vol. 49, no. 6, pp. 30–37, Jun. 2011.

[2] C. Huang, G. C. Alexandropoulos, A. Zappone, M. Debbah, and C. Yuen, "Energy efficient multi-user MISO communication using low resolution large intelligent surfaces," in *IEEE GLOBECOM Workshops,* Abu Dhabi, United Arab Emirates, pp. 1–6, Dec. 2018.

[3] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *to appear in IEEE Trans. Wireless Commun.*, 2019.

[4] Q. Wu, G. Y. Li, W. Chen, D. W. K. Ng, and R. Schober, "An overview of sustainable green 5G networks," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 72–80, Aug. 2017.

[5] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[6] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[7] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[8] F. Zhou, Z. Li, J. Cheng, Q. Li, and J. Si, "Robust AN-aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT," *IEEE Trans. Wireless Commun.*, vol. 16, no. 4, pp. 2450–2464, Apr. 2017.

[9] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[10] D. W. K. Ng and R. Schober, "Secure and green SWIPT in distributed antenna networks with limited backhaul capacity," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5082–5097, Sept. 2015.

[11] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network: Joint active and passive beamforming design," *to appear in IEEE Trans. Wireless Commun.*, 2019.

[12] Renzo, Marco Di, et. al., "Smart radio environments empowered by reconfigurable AI meta-surfaces: an idea whose time has come," *EURASIP J. Wirel. Commun. Netw.*, no. 129, pp. 1–20, May 2019.

[13] S. Hu, F. Rusek, and O. Edfors, "Beyond massive MIMO: The potential of positioning with large intelligent surfaces," *IEEE Trans. Signal Process.*, vol. 66, no. 7, pp. 1761–1774, Apr. 2018.

[14] H. Zhang and L. Duan, "Going beyond secrecy rate via information jamming," in *IEEE GLOBECOM*, pp. 1–6, Dec. 2018.

[15] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[16] Q. Wu and R. Zhang, "Beamforming optimization for intelligent reflecting surface with discrete phase shifts," in *Proc. ICASSP 2019*, pp. 7830–7833, May 2019.

[17] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2004.

[18] K. Wang, A. M. So, T. Chang, W. Ma, and C. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: Tractable approximations by conic optimization," *IEEE Trans. Signal Process.*, vol. 62, no. 21, pp. 5690–5705, Nov. 2014.

[19] R. A. Horn and C. R. Johnson, *Matrix Analysis.* New York, NY, USA: Cambridge University Press, 2012.