IRS-Aided Uplink Security Enhancement via Energy-Harvesting Jammer

Tiantian Qiao, Yang Cao, Jie Tang, *Senior Member, IEEE*, Nan Zhao, *Senior Member, IEEE*, and Kai-Kit Wong, *Fellow, IEEE*

***Abstract*—In this paper, we investigate the security enhancement by combining intelligent reflecting surface (IRS) and energy harvesting (EH) jammer for the uplink transmission. Specifically, we propose an IRS-aided secure scheme for the uplink transmission via an EH jammer, to fight against the malicious eavesdropper. The proposed scheme can be divided into an energy transfer (ET) phase and an information transmission (IT) phase. In the first phase, the friendly EH jammer harvests energy from the base station (BS) aided by IRS. We maximize the harvested energy of jammer by obtaining the closed-form solution to the phase-shift matrix of IRS. In the second phase, the user transmits confidential information to the BS while the jamming is generated to confuse the eavesdropper without affecting the legitimate transmission. The phase-shift matrix of IRS and time switching factor are jointly optimized to maximize the secrecy rate. To tackle the non-convex problem, we first decompose it into two sub-problems. The one of IRS can be approximated to convex with fixed time switching factor. Then, the time switching factor can be solved by Lagrange duality. Thus, the solution to the original problem can be obtained by alternately optimizing these two sub-problems. Simulation results show that the proposed Jammer-IRS assisted secure transmission scheme can significantly enhance the uplink security.**

***Index Terms*—Energy harvesting, intelligent reflecting surface, jamming, physical layer security, time switching.**

I. Introduction

Physical layer security (PLS), as a promising technique to improve the security of wireless communications, has been widely studied recently in many directions, e.g., beamforming design [2], [3], artificial jamming (AJ) [4], [5], cooperative relaying [6], [7], *etc*. According to [8], the principle of PLS is to take the advantage of wireless channels, such as fading, noise and interference, to fight against the malicious eavesdropping and achieve security enhancement. In particular, secrecy rate, the key performance metric of PLS, depends on the channel condition difference between the transmitter-to-receiver and the transmitter-to-eavesdropper. AJ has been regarded as an effective approach to enlarge the above channel condition difference, so as to improve the secure communication of wireless networks.

In the downlink, AJ can be transmitted by a transmitter equipped with multiple antennas. However, in the uplink, due to the physical structure and power constraint of user devices, there is not enough spatial freedom or power to transmit AJ, which motives the emerging of cooperative jamming [9]–[11]. Cooperative jamming can be achieved by deploying an extra cooperating node, called the friendly jammer, to transmit AJ to confuse the eavesdropper [12]. Nevertheless, devices are usually energy-limited or selfish in practical networks. To tackle this challenge, energy harvesting (EH) is adopted to scavenge energy from the environment for continuous energy supply [13]. Thus, EH jammer is induced by integrating the EH technique into a friendly jammer, which makes that the friendly jammer is capable of energy harvesting.

On the other hand, intelligent reflecting surface (IRS) provides a new degree of freedom for the performance enhancement of wireless communications by creating an additional reflecting link [14]. IRS, a plane consisting of a number of low-cost passive reflecting elements, can be controlled by a software based smart controller to individually alter the amplitude and phase of the incident signals [15]. Hence, a programmable and controllable wireless environment can be created by enhancing the desired signal power and attenuating the interference directionally via passive beamforming. Compared to traditional related approaches like amplify-and-forward relaying, backscattering and conventional reflecting surfaces, IRS has the advantages of low energy consumption, low cost, easy deployment and reconfigure reflecting coefficients [16]. Due to these merits, IRS has been utilized in various scenarios to improve the capacity [17], [18], energy efficiency [19], [20], PLS [21], [22], *etc*.

As mentioned above, IRS can be deployed in the uplink communication to enhance PLS. However, the effect of IRS-aided security enhancement may be compromised by the location of the IRS deployment and the number of IRS elements. To prevent this issue, EH jammer can cooperate with IRS to further enhance the security performance. Thus, the combination of IRS and EH jammer is expected to provide a "double guarantee" for the secure communication. Up to the present, there are only a few works focusing on the combination of IRS and friendly jammer [23]. However, the work in [23] focused on the energy efficiency of the downlink MISO network, while the secrecy rate maximization problem for uplink secure communication is still not well investigated. Thus, we propose a Jammer-IRS scheme to enhance the

Tiantian Qiao, Yang Cao and Nan Zhao are with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, P. R. China (e-mail: qiaotiantian@mail.dlut.edu.cn, cy216@mail.dlut.edu.cn, zhaonan@dlut.edu.cn).

Jie Tang is with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China (e-mail: eejtang@scut.edu.cn).

Kai-Kit Wong is with the Department of Electronic and Electrical Engineering, University College London, London WC1E 6BT, U.K. (e-mail: kai-kit.wong@ucl.ac.uk).

Part of this paper will be presented at IEEE GLOBECOM 2022 [1]. (*Corresponding Author: Nan Zhao*)

secrecy performance where a friendly EH jammer transmits jamming signal to confuse the eavesdropper, and the IRS is deployed to enhance both the harvested energy by the jammer and the uplink transmission. The main contributions of this paper are summarized as follows.

- In this paper, we propose a "Jammer-IRS" scheme to provide double guarantee for the uplink secure communication. Particularly, each time frame can be divided into two phases, i.e., the energy transfer (ET) phase and the information transmission (IT) phase, where the duration trade-off between the ET phase and the IT phase is designed to adaptively balance the role of EH jammer and IRS in the security improvement.
- In the ET phase, the jammer harvests energy from the BS, and thus an energy maximization problem is considered by designing the phase-shift matrix of IRS. In the IT phase, aided by IRS, the user transmits confidential information to the BS in the presence of eavesdropper, while the jammer uses the energy collected in the previous phase to confuse the eavesdropper. Then, secrecy rate can be maximized by jointly optimizing the phase-shift matrix and the time switching factor.
- In the ET phase, the closed-form solution to the IRS's phase-shift matrix is derived resorting to the upper bound of triangle inequality. Then, in the IT phase, we decouple the challenging non-convex optimization problem into two sub-problems. The phase-shift matrix of IRS can be obtained by applying semi-definite relaxation (SDR). After using Taylor series approximation, the solution to the time switching factor can be obtained efficiently by solving its Lagrange dual problem. Then, an algorithm based on the alternating optimization is proposed to iteratively optimize the phase-shift matrix and the time switching factor until convergence.

The remainder of this paper is arranged as follows. Section III presents the system model. In Section IV, the proposed scheme is presented with the optimization problem formulated. In Section V, an efficient algorithm to solve the problem is designed. Simulation results are shown in Section VI, and the paper is concluded in Section VII.

Notation: a, $\mathbf{a}$, and $\mathbf{A}$ denote the scalar, vector and matrix, respectively. $\mathbb{C}^{N\times M}$ is the space of $N\times M$ complex matrices. $\mathbf{A}^T$ and $\mathbf{A}^\dagger$ denote the transpose and Hermitian transpose of $\mathbf{A}$, respectively. $\mathrm{diag}(\mathbf{a})$ is a diagonal matrix with its diagonal elements from $\mathbf{a}$. $\mathcal{CN}(\mu,\sigma^2)$ is the complex Gaussian distribution with mean μ and variance σ^2. $|a|$ and $\|\mathbf{a}\|$ are the absolute value of a and Euclidean norm of $\mathbf{a}$, respectively. $E(a)$ represents expectation. $\mathbf{I}_M$ is the identity matrix with dimension of M. $(\mathbf{a})^{-1}$ is the inverse operation of $\mathbf{a}$. $\mathbf{A}\succeq 0$ is a Hermitian positive semi-definite matrix. $\arg\max f(x)$ means the optimal solution to maximize the objective function $f(x)$.

II. Related Works

A. AJ-aided Communication

AJ is often used in the downlink to ensure the secure transmission [24]–[27]. In [24], Lv *et al*. presented a novel AJ-assisted secrecy beamforming scheme to improve the security in the downlink multiple-input single-output non-orthogonal multiple access (MISO-NOMA) system with two users. For downlink large-scale networks, Liu *et al*. validated that generating AJ at the base station (BS) is an effective way to improve the secrecy performance of NOMA networks [25]. In [26], Zeng *et al*. studied that the combination of AJ and massive multiple-input multiple-output (MIMO) can significantly promote downlink NOMA networks on the basis of secrecy performance. In [27], the AJ-aided directional jamming was designed by Wang *et al*. for the secure communication in massive MIMO Rician channels.

B. EH Jammer-aided Communication

The EH technique is often integrated with other nodes, such as IRS [28] and jammer, to make the node self-sustainable, which divides the whole communication into two phases for ET and IT respectively. In [28], Xu *et al*. focused on the computational task offloading of mobile edge computing networks by integrating EH technique with IRS. Different from that of [28], existing works [29]–[31] and our proposed scheme integrated the EH technique into a friendly jammer to improve the uplink security performance. In [29], Cao *et al*. exploited the EH jammer to greatly benefit the uplink NOMA secure transmission, and three schemes for selecting a friendly jammer from multiple EH receivers were proposed. By applying the friendly EH jammer in [30], the secure transmission between the source and destination in the presence of an eavesdropper was realized by Liu *et al*. Moon *et al*. considered two different levels of eavesdropping channel state information (CSI) in [31], and the secrecy performance was ensured by proposing an uplink wireless powered network with the aid of an EH jammer.

C. IRS-aided Communication

As a novel and revolutionary technology, IRS has provided appealing solutions to improving PLS by enhancing the strength of legitimate links while attenuating the eavesdropping via passive beamforming [14]. Existing works have explored IRS to enhance the security of wireless communications [32]–[35]. In [32], the secrecy rate was maximized for IRS-assisted multi-antenna systems by Shen *et al*. via an efficient alternating algorithm. In [33], Cui *et al*. found that deploying IRS can greatly improve wireless security in the challenging scenario where the legitimate channel is weaker than the eavesdropping channel and they are spatially highly correlated. With two cases of full CSI and no eavesdropping CSI, Dong *et al*. studied the secrecy rate of an IRS-assisted Gaussian MIMO wiretap channel in [34]. Yu *et al*. presented a novel multiple IRSs assisted scheme in [35] to improve the PLS in a challenging radio environment where the legitimate users do not have a line-of-sight (LoS) link to the access point in downlink multiuser MISO systems.

III. System Model

As shown in Fig. 1, we consider an uplink wireless communication system consisting of one BS, one legitimate user and

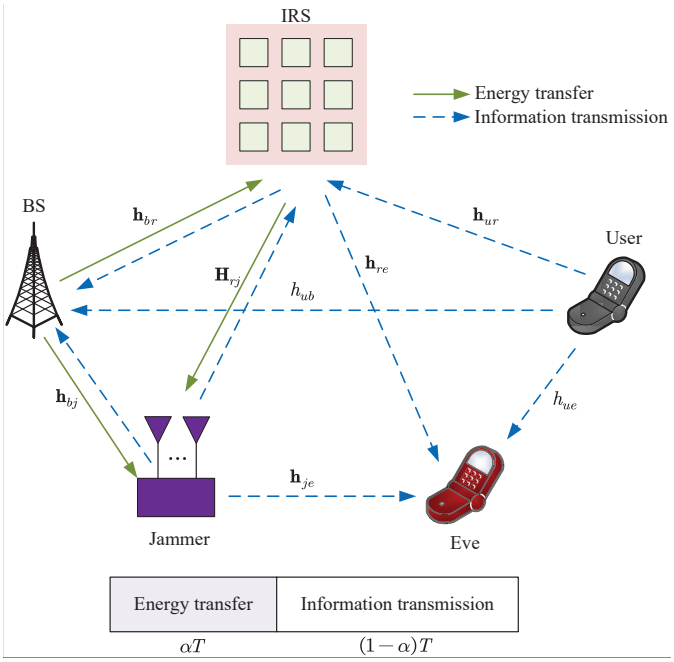


Fig. 1. Uplink system model with the help of IRS and jammer.

one malicious eavesdropper (Eve). To effectively fight against the Eve, a friendly EH jammer (Jam) and an IRS[1] with N reflecting elements are introduced. Assume that the BS, the user and the Eve are all equipped with a single antenna, while the number of antennas at the Jam is M. Since the Jam harvests energy before transmitting AJ, the whole transmission process can be divided into an ET phase with αT and an IT phase with $(1-\alpha)T$. $0 < \alpha < 1$ denotes the time switching factor between ET and IT while T represents the duration of a frame. In the ET phase, the BS transfers wireless power to the Jam. To maximize the harvested energy, we optimize the phase-shift matrix of IRS. In the second phase, the user transmits the confidential message to the BS, which can be overheard by the Eve as well. In this case, the IRS and the Jam are deployed to jointly protect the transmission of confidential information, i.e., the Jam uses the energy harvested from the previous phase to transmit AJ to confuse the Eve while the IRS optimizes the phase-shift matrix to further improve the performance of security.

For all channels, they suffer from the quasi-static flat-fading. We consider the time division duplex (TDD) system with channel reciprocity for uplink and downlink transmissions [37]. Hence, according to the existing channel estimation methods discussed in [14], [38], [39], all channels information can be acquired based on the uplink-downlink channel reciprocity provided by TDD protocol. Thus, the CSI of all channels can be assumed to be perfectly known. $\mathbf{h}_{bj} \in \mathbb{C}^{M\times 1}$, $\mathbf{h}_{je} \in \mathbb{C}^{1\times M}$ and $h_{uf}(f \in \{b, e\})$ denote the channel coefficients of direct links for BS $\rightarrow$ Jammer, Jammer $\rightarrow$ Eve, User $\rightarrow$ BS and User $\rightarrow$ Eve, respectively, while the channel coefficient vectors of IRS-assisted links for BS $\rightarrow$ IRS, User $\rightarrow$ IRS, IRS $\rightarrow$ Eve and IRS $\rightarrow$ Jammer are denoted as $\mathbf{h}_g(g \in \{br, ur, re\}) \in \mathbb{C}^{N\times 1}$ and $\mathbf{H}_{rj} \in \mathbb{C}^{N\times M}$, respectively. Rayleigh fading and Rician fading are assumed for direct links and reflecting links respectively, while BS-Jammer is regarded as a LoS link. Their corresponding channel coefficients can be generated as

$$h_{uf} = \sqrt{L_0 d_{uf}^{-a_d}}\, \mathrm{g}_{uf}^{\mathrm{NLoS}}, f \in \{b, e\}, \tag{1}$$

$$\mathbf{h}_{bj} = \sqrt{L_0 d_{bj}^{-a_{bj}}}\, \mathbf{g}_{bj}^{\mathrm{LoS}}, \tag{2}$$

$$\mathbf{h}_g = \sqrt{L_0 d_g^{-a_r}} \left(\sqrt{\frac{K}{K+1}} \mathbf{g}_g^{\mathrm{LoS}} + \sqrt{\frac{1}{K+1}} \mathbf{g}_g^{\mathrm{NLoS}} \right), \quad g \in \{br, ur, re\}, \tag{3}$$

where K is the Rician factor, $\mathbf{g}_{bj}^{\mathrm{LoS}}$ and $\mathbf{g}_g^{\mathrm{LoS}}$ denote the deterministic LoS components, and $\mathrm{g}_{uf}^{\mathrm{NLoS}}$ and $\mathbf{g}_g^{\mathrm{NLoS}}$ denote the Rayleigh fading components. L_0 denotes the path loss at 1 m. Set the exponents of direct and reflecting path loss as a_d and a_r, respectively. a_{bj} is assumed for the direct link of BS-Jammer. d_{AB} denote the distance from A to B where A and B are the specific nodes of the system. $\mathbf{h}_{je}$ and $\mathbf{H}_{rj}$ adopt the channels as shown in (1) and (3), respectively.

In this work, we assume that IRS is a square array with a number of $\sqrt{N}$ elements in both the horizontal and vertical directions. Let $\boldsymbol{\theta} = [\theta_1, \ldots, \theta_n, \ldots, \theta_N]^T$ and $v_n = \beta_n e^{j\theta_n}$, where $\theta_n \in [0, 2\pi)$ and $\beta_n \in [0, 1]$ denote the phase shift and amplitude reflection coefficient of the IRS's n-th element. $\boldsymbol{\Phi} = \mathrm{diag}(v_1, \cdots, v_n, \cdots, v_N)$ denotes the phase-shift matrix of IRS. $\beta_n = 1$ is set to maximize the signal reflection in the following analysis. In addition, we denote the complex additive white Gaussian noise (AWGN) at the Jam, the BS and the Eve as $\mathbf{n}_j \sim \mathcal{CN}(\mathbf{0}, \sigma^2\mathbf{I})$ and $n_l \sim \mathcal{CN}(0, \sigma^2), l \in \{b, e\}$, respectively.

IV. Two Phases for the Jammer-IRS Scheme

In this section, we propose the Jammer-IRS scheme and present the optimization problems in two phases.

A. First Phase: Energy Transfer

During the first phase, the BS transmits with the fixed power P_b. We denote the transmitted signal as x_b with $E[|x_b|^2] = 1$. $\mathbf{u}_J$ is the combining vector with the dimension of $M \times 1$. To maximize the harvested energy at the Jam, $\mathbf{u}_J$ is derived through using the maximal ratio combining (MRC) as

$$\mathbf{u}_J = \frac{\mathbf{H}_{rj}^{\dagger}\boldsymbol{\Phi}_1\mathbf{h}_{br} + \mathbf{h}_{bj}}{\left\|\mathbf{H}_{rj}^{\dagger}\boldsymbol{\Phi}_1\mathbf{h}_{br} + \mathbf{h}_{bj}\right\|}. \tag{4}$$

The signal received at the Jam can be expressed as

$$y_j = \mathbf{u}_J^{\dagger}(\mathbf{H}_{rj}^{\dagger}\boldsymbol{\Phi}_1\mathbf{h}_{br} + \mathbf{h}_{bj})\sqrt{P_b}x_b + \mathbf{u}_J^{\dagger}\mathbf{n}_j, \tag{5}$$

where $\boldsymbol{\Phi}_1 = \mathrm{diag}(v_{1,1}, v_{1,2}, \cdots, v_{1,n}, \cdots, v_{1,N})$ denotes the phase-shift matrix of IRS with $|v_{1,n}| = 1, n = 1, \cdots, N$. The energy harvested by the Jam can be expressed as $E_J = \alpha T \eta P_b \left|\mathbf{u}_J^{\dagger}(\mathbf{H}_{rj}^{\dagger}\boldsymbol{\Phi}_1\mathbf{h}_{br} + \mathbf{h}_{bj})\right|^2$, where $0 < \eta < 1$ denotes

[1]The IRS is assumed as a passive reflector in this paper. When the IRS is used as a backscatter device to generate AJ [36], additional signal processing units are required, which may increase the difficulty of IRS design and result in the transmission delay. These issues are beyond the scope of this paper and will be discussed in the future.

the EH efficiency. Within the remaining $(1-\alpha)T$, the Jam will use the harvested energy to transmit the jamming signal. Therefore, the transmit power of Jam can be expressed as

$$\begin{aligned} P_J &= \frac{E_J}{(1-\alpha)T} \\ &= \frac{\alpha\eta P_b \left\| \mathbf{H}_{rj}^{\dagger}\mathbf{\Phi}_1\mathbf{h}_{br}+\mathbf{h}_{bj}\right\|^2}{1-\alpha}. \end{aligned} \tag{6}$$

In order to improve the security performance, in the ET phase, we maximize the harvested energy at the Jam by optimizing the phase-shift matrix of IRS. By doing so, on one hand, the transmit power of Jam can be maximized to transmit the AJ, which can confuse the eavesdropper effectively; on the other hand, more time will be saved for the information transmission in the second phase. As a result, the secure transmission in the second phase can be greatly enhanced based on the above benefits. To achieve this goal, let $\mathbf{v}_1 = [v_{1,1}, v_{1,2}, \ldots, v_{1,n}, \ldots, v_{1,N}]$, and we have

$$\left\| \mathbf{H}_{rj}^{\dagger}\mathbf{\Phi}_1\mathbf{h}_{br}+\mathbf{h}_{bj}\right\| = \left\| \mathbf{H}_{rj}^{\dagger}\mathrm{diag}\left(\mathbf{h}_{br}\right)\mathbf{v}_1^{\mathrm{T}}+\mathbf{h}_{bj}\right\|. \tag{7}$$

During this phase, IRS is deployed to maximize the harvested power at the Jam, the optimization problem can be formulated as

$$\begin{aligned} (\mathrm{P1}): \max_{\mathbf{v}_1} \quad & \left\| \mathbf{H}_{rj}^{\dagger}\mathrm{diag}\left(\mathbf{h}_{br}\right)\mathbf{v}_1^{\mathrm{T}}+\mathbf{h}_{bj}\right\|^2 && \text{(8a)} \\ s.t. \quad & |v_{1,n}| = 1, n = 1, \ldots, N, && \text{(8b)} \end{aligned}$$

where (8b) is the unit modulus constraints on the phase of IRS. By optimizing the phase-shift matrix of IRS to maximize (8a), enough energy can be harvested as fast as possible to allow more time for information transmission. The specific process to solve this problem is described in the section V.

B. Second Phase: Information Transmission

In the second phase, the transmit power of user is P_u. We denote the transmitted signal as $x_r, r \in \{u, j\}$ with $E[|x_r|^2] = 1$. The signal received at the BS and Eve can be expressed as

$$\begin{aligned} y_b = &\left(\mathbf{h}_{br}^{\dagger}\mathbf{\Phi}_2\mathbf{h}_{ur}+h_{ub}\right)\sqrt{P_u}x_u + \\ &\left(\mathbf{h}_{br}^{\dagger}\mathbf{\Phi}_2\mathbf{H}_{rj}+\mathbf{h}_{bj}^{\dagger}\right)\mathbf{w}_J\sqrt{P_J}x_j + n_b, \end{aligned} \tag{9}$$

$$\begin{aligned} y_e = &\left(\mathbf{h}_{re}^{\dagger}\mathbf{\Phi}_2\mathbf{h}_{ur}+h_{ue}\right)\sqrt{P_u}x_u + \\ &\left(\mathbf{h}_{re}^{\dagger}\mathbf{\Phi}_2\mathbf{H}_{rj}+\mathbf{h}_{je}\right)\mathbf{w}_J\sqrt{P_J}x_j + n_e, \end{aligned} \tag{10}$$

where $\mathbf{\Phi}_2$=diag$(v_{2,1}, v_{2,2}, \cdots, v_{2,n}, \cdots, v_{2,N})$ with $|v_{2,n}| = 1, n$=$1, \cdots, N$.

To prevent the impact of jamming on the BS, we should perform zero-forcing (ZF), and the precoding vector $\mathbf{w}_J$ should satisfy

$$\left(\mathbf{h}_{br}^{\dagger}\mathbf{\Phi}_2\mathbf{H}_{rj}+\mathbf{h}_{bj}^{\dagger}\right)\mathbf{w}_J = 0. \tag{11}$$

As a result, $\mathbf{w}_J$ can be derived as

$$\mathbf{w}_J = \left(\mathbf{I}_M - \left(\bar{\mathbf{h}}_{jb}^{\dagger}\left(\bar{\mathbf{h}}_{jb}\bar{\mathbf{h}}_{jb}^{\dagger}\right)^{-1}\bar{\mathbf{h}}_{jb}\right)\right)\mathbf{w}_0, \tag{12}$$

where

$$\bar{\mathbf{h}}_{jb} = \mathbf{h}_{br}^{\dagger}\mathbf{\Phi}_2\mathbf{H}_{rj}+\mathbf{h}_{bj}^{\dagger}. \tag{13}$$

$\mathbf{w}_0$ is the arbitrary vector with the dimension of M. Accordingly, the Jam only disturbs the Eve without affecting the legitimate transmission. Let $\mathbf{v}_2$=$[v_{2,1}, v_{2,2}, \ldots, v_{1,n}, \ldots, v_{2,N}]$, thus the corresponding received signal-to-interference-plus-noise ratio (SINR) can be denoted as

$$\gamma_B = \rho_u \left|\tilde{\mathbf{v}}_2^{\dagger}\mathbf{a}_B\right|^2, \tag{14}$$

$$\gamma_E = \frac{\rho_u \left|\tilde{\mathbf{v}}_2^{\dagger}\mathbf{a}_E\right|^2}{1+\rho_j\left|\tilde{\mathbf{v}}_2^{\dagger}\mathbf{A}_{JE}\mathbf{w}_J\right|^2}, \tag{15}$$

where $\rho_u = \frac{P_u}{\sigma^2}$, $\rho_j = \frac{P_J}{\sigma^2}$, and $\tilde{\mathbf{v}}_2 = \begin{bmatrix}\mathbf{v}_2^{\dagger}\\ 1\end{bmatrix}$. $\mathbf{a}_B$, $\mathbf{a}_E$ and $\mathbf{A}_{JE}$ can be denoted as

$$\mathbf{a}_B = \begin{bmatrix}\mathrm{diag}(\mathbf{h}_{br}^{\dagger})\mathbf{h}_{ur}\\ h_{ub}\end{bmatrix}, \tag{16}$$

$$\mathbf{a}_E = \begin{bmatrix}\mathrm{diag}(\mathbf{h}_{re}^{\dagger})\mathbf{h}_{ur}\\ h_{ue}\end{bmatrix}, \tag{17}$$

$$\mathbf{A}_{JE} = \begin{bmatrix}\mathrm{diag}(\mathbf{h}_{re}^{\dagger})\mathbf{H}_{rj}\\ \mathbf{h}_{je}\end{bmatrix}. \tag{18}$$

In addition, $\bar{\mathbf{h}}_{jb} = \tilde{\mathbf{v}}_2^{\dagger}\mathbf{A}_{BJ}$ can be obtained with $\mathbf{A}_{BJ} = \begin{bmatrix}\mathrm{diag}(\mathbf{h}_{br}^{\dagger})\mathbf{H}_{rj}\\ \mathbf{h}_{bj}^{\dagger}\end{bmatrix}$ to update $\mathbf{w}_J$.

In this phase, the phase-shift matrix of IRS is optimized to utilize IRS to improve the uplink secure transmission, and the time switching factor is optimized to balance the role of EH jammer and IRS in the security improvement. As a result, with the help of the EH jammer and IRS, we aim at maximizing the uplink secrecy rate through optimizing the phase-shift matrix of IRS and the time switching factor. Hence, the optimization problem can be modeled as

$$\begin{aligned} (\mathrm{P2}): \max_{\mathbf{\Phi}_2,\alpha} \quad & C_s && \text{(19a)} \\ s.t. \quad & |v_{2,n}| = 1, n = 1, \cdots, N, && \text{(19b)} \\ & 0 \le \alpha \le 1. && \text{(19c)} \end{aligned}$$

C_s is the achievable secrecy rate, which can be expressed as

$$C_s = (1-\alpha)[\log_2(1+\gamma_B) - \log_2(1+\gamma_E)]^+, \tag{20}$$

where $[x]^+ = \max(x, 0)$. (19b) represents the unit modulus constraints of the phase of IRS in the IT phase, and (19c) is the constraint of the time switching factor. (P2) is non-convex due to multi-variable coupling and unit modulus constraints. To tackle this problem, we divide it into two sub-problems, and an alternating optimization based algorithm is proposed. The specific analysis for the problem is detailed in the next section.

$$\varphi(\tilde{\mathbf{V}},t_e)=\ln\left(1+\rho_u\mathrm{tr}\left(\tilde{\mathbf{V}}\boldsymbol{\psi}_B\right)\right)+\ln\left(1+\rho_j\mathrm{tr}\left(\tilde{\mathbf{V}}\mathbf{A}_{JE}\mathbf{w}_J\mathbf{w}_J^{\dagger}\mathbf{A}_{JE}^{\dagger}\right)\right)-t_e\left(1+\rho_u\mathrm{tr}\left(\tilde{\mathbf{V}}\boldsymbol{\psi}_E\right)+\rho_j\mathrm{tr}\left(\tilde{\mathbf{V}}\mathbf{A}_{JE}\mathbf{w}_J\mathbf{w}_J^{\dagger}\mathbf{A}_{JE}^{\dagger}\right)\right)+\ln t_e+1. \quad (32)$$

V. Optimization for Beamforming and Time Allocation

To obtain the effective solutions to the proposed scheme, we first derive the closed-form solution to the problem (P1). Then, the problem (P2) is divided into two sub-problems and solved with the alternating algorithm.

A. Optimizing Phase-Shift Matrix in the First Phase

Since the Euclidean norm is satisfied with the triangle inequality, (8a) should satisfy

$$\begin{aligned}\left\|\mathbf{H}_{rj}^{\dagger}\mathrm{diag}(\mathbf{h}_{br})\mathbf{v}_1^{\mathrm{T}}+\mathbf{h}_{bj}\right\|&\le\left\|\mathbf{H}_{rj}^{\dagger}\mathrm{diag}\left(\mathbf{h}_{br}\right)\mathbf{v}_1^{\mathrm{T}}\right\|+\|\mathbf{h}_{bj}\|\\&=\left|\underbrace{\sum_{m=1}^{M}\left[\mathbf{H}_{rj}^{\dagger}\mathrm{diag}\left(\mathbf{h}_{br}\right)\right]_m}_{\mathbf{d}}\mathbf{v}_1^{\mathrm{T}}\right|+\left|\underbrace{\sum_{m=1}^{M}\left[\mathbf{h}_{bj}\right]_m}_{d_0}\right|.\end{aligned} \quad (21)$$

For (21), the equality holds if and only if $\angle(\mathbf{d}\mathbf{v}_1^{\mathrm{T}})=\angle(d_0)$, where $\angle(x)$ denotes the phase of x [40]. Thus, the problem (P1) can be converted as

$$\begin{aligned}(\mathrm{P3}):\max_{\mathbf{v}_1}\quad&\left|\mathbf{d}\mathbf{v}_1^{\mathrm{T}}\right|^2 && (22)\\ s.t.\quad&|v_{1,n}|=1,n=1,\ldots,N, && (23)\\&\angle(\mathbf{d}\mathbf{v}_1^{\mathrm{T}})=\angle(d_0). && (24)\end{aligned}$$

The objective function of (P3) obtains the optimal solution only when (24) holds, and we can verify that the optimal solution to the problem (P3) can be obtained by

$$\mathbf{v}_1^{\star}=e^{j(\angle(d_0)-\angle(\mathbf{d}))}. \quad (25)$$

Then, $\boldsymbol{\Phi}_1^{\star}=\mathrm{diag}(\mathbf{v}_1^{\star})$ can be obtained accordingly.

B. Optimizing Phase-Shift Matrix and Time Switching Factor in the Second Phase

For the second phase, the problem (P2) is non-convex because of the coupling of $\boldsymbol{\Phi}_2$ and α, which is difficult to solve directly. However, it is observed that the original problem can be effectively solved if only one variable is expected to be solved. Thus, the alternating optimization approach is adopted to solve the problem (P2) sub-optimally, similar to that of [39], [41], [42]. To be specific, we first convert the sub-problem with a fixed α into a convex one using SDR [43]. Then, the sub-problem with a fixed $\boldsymbol{\Phi}_2$ can be solved by adopting the linear approximation. Finally, the sub-optimal solutions to the original problem (P2) can be derived by alternately optimizing the two sub-problems at each iteration until convergence. The detailed process to solve each sub-problem is detailed in the following subsections.

1) Optimizing $\boldsymbol{\Phi}_2$ for Given α:

For a fixed time switching factor α, the constraint on it in the problem (P2) can be removed. Let $\tilde{\mathbf{V}}=\tilde{\mathbf{v}}_2\tilde{\mathbf{v}}_2^{\dagger}$ and $\boldsymbol{\psi}_q=\mathbf{a}_q\mathbf{a}_q^{\dagger}\,(q\in\{B,E\})$, and we have

$$|\tilde{\mathbf{v}}_2^{\dagger}\mathbf{a}_q|^2=\mathrm{tr}\left(\tilde{\mathbf{V}}\boldsymbol{\psi}_q\right). \quad (26)$$

Meanwhile, $\tilde{\mathbf{V}}\succeq 0$ and rank($\tilde{\mathbf{V}}$)=1 should also hold. However, the rank-1 constraint is non-convex. This leads us to apply the SDR to relax this constraint [43]. Thus, the problem (P2) can be transformed as

$$\begin{aligned}(\mathrm{P4}):\max_{\tilde{\mathbf{v}}_2}\quad&(1-\alpha)\left[\log_2\left(1+\rho_u\mathrm{tr}\left(\tilde{\mathbf{V}}\boldsymbol{\psi}_B\right)\right)-\right.\\&\left.\log_2\left(1+\frac{\rho_u\mathrm{tr}\left(\tilde{\mathbf{V}}\boldsymbol{\psi}_E\right)}{1+\rho_j\mathrm{tr}\left(\tilde{\mathbf{V}}\mathbf{A}_{JE}\mathbf{w}_J\mathbf{w}_J^{\dagger}\mathbf{A}_{JE}^{\dagger}\right)}\right)\right] && (27)\\ s.t.\quad&\tilde{\mathbf{V}}\succeq 0,\tilde{\mathbf{V}}_{n,n}=1,n=1,\ldots,N+1. && (28)\end{aligned}$$

Since the problem (P4) is still non-convex, the non-convex terms of (27) can be transformed according to the following lemma [42].

Lemma 1: For the function $\varphi(t)=-tx+lnt+1,\forall x>0$, $-\ln x=\max_{t>0}\varphi(t)$ is satisfied when $t=\frac{1}{x}$. ■

By applying Lemma 1 and setting

$$\begin{aligned}x&=1+\rho_u\mathrm{tr}\left(\tilde{\mathbf{V}}\boldsymbol{\psi}_E\right)+\rho_j\mathrm{tr}\left(\tilde{\mathbf{V}}\mathbf{A}_{JE}\mathbf{w}_J\mathbf{w}_J^{\dagger}\mathbf{A}_{JE}^{\dagger}\right), && (29)\\ t&=t_e, && (30)\end{aligned}$$

C_s can be changed into

$$\frac{C_s\ln 2}{1-\alpha}=\max_{t_e>0}\varphi(\tilde{\mathbf{V}},t_e), \quad (31)$$

where $\varphi(\tilde{\mathbf{V}},t_e)$ is shown in (32).

We can omit "$\ln 2$" and "$1-\alpha$" since they are constant. Therefore, the optimization problem (P4) for a given α can be rewritten as

$$\begin{aligned}(\mathrm{P5}):\max_{\tilde{\mathbf{V}},t_e}\quad&\varphi(\tilde{\mathbf{V}},t_e) && (33)\\ s.t.\quad&\tilde{\mathbf{V}}\succeq 0, && (34)\\&\tilde{\mathbf{V}}_{n,n}=1,n=1,\ldots,N+1, && (35)\\&t_e>0. && (36)\end{aligned}$$

It is obvious that (P5) is convex with respect to either $\tilde{\mathbf{V}}$ or t_e. Hence, it can be solved through alternately optimizing $\tilde{\mathbf{V}}$ and t_e. According to Lemma 1, the optimal solution to t_e in each iteration can be derived as

$$t_e^{*}=\left(1+\rho_u\mathrm{tr}\left(\tilde{\mathbf{V}}\boldsymbol{\psi}_E\right)+\rho_j\mathrm{tr}\left(\tilde{\mathbf{V}}\mathbf{A}_{JE}\mathbf{w}_J\mathbf{w}_J^{\dagger}\mathbf{A}_{JE}^{\dagger}\right)\right)^{-1}. \quad (37)$$

While for the fixed t_e^{*}, the optimal $\tilde{\mathbf{V}}$ can be obtained by using convex optimization solvers, e.g., CVX, which can be expressed as

$$\tilde{\mathbf{V}}^{*}=\arg\max_{\tilde{\mathbf{V}}_{n,n}=1}\varphi(\tilde{\mathbf{V}},t_e^{*}). \quad (38)$$

Algorithm 1 Proposed algorithm to solve the problem (P4).

Input: α, ρ_u, ρ_j, $\boldsymbol{\psi}_B$, $\boldsymbol{\psi}_E$, $\mathbf{A}_{JE}$ and $\mathbf{A}_{BJ}$.
Output: $\mathbf{v}_2^\star$.
1: Initialize $\mathbf{v}_2$ and $\tilde{\mathbf{v}}_2$ in the constraint (28).
2: Set $s=1$ as the index of iteration, and $\tilde{\mathbf{V}}^{(0)}=\tilde{\mathbf{v}}_2\tilde{\mathbf{v}}_2^\dagger$.
3: **repeat**
4: Obtain the optimal $t_e^{(s)}$ according to (37) for the given $\tilde{\mathbf{V}}^{(s-1)}$.
5: Obtain the optimal $\tilde{\mathbf{V}}^{(s)}$ according to (38) for the given $t_e^{(s)}$.
6: Update $s=s+1$.
7: **until** The objective value of the problem (P5) converges.
8: Recover $\tilde{\mathbf{v}}_2$ from $\tilde{\mathbf{V}}$ and obtain $\mathbf{v}_2$ from (39).

Since the rank-1 constraint in the problem (P4) is relaxed by applying SDR, $\tilde{\mathbf{v}}_2^*$ can be obtained from $\tilde{\mathbf{V}}=\tilde{\mathbf{v}}_2\tilde{\mathbf{v}}_2^\dagger$ through using the eigenvalue decomposition if $\tilde{\mathbf{V}}$ is a rank-1 matrix, otherwise $\tilde{\mathbf{v}}_2^*$ can be obtained roughly by the Gaussian randomization. After extracting $\tilde{\mathbf{v}}_2^*$ from $\tilde{\mathbf{V}}^*$, the reflection coefficients can be obtained as

$$v_{2,n}^*=e^{j\angle\frac{\tilde{v}_n}{\tilde{v}_{N+1}}}, n=1.\ldots,N. \tag{39}$$

By alternately updating $\tilde{\mathbf{V}}$ and t_e, the objective function of the problem (P5) tends to converge. Thus, the optimal solution $\boldsymbol{\Phi}_2^\star$ can be derived by $v_{2,n}^\star$ accordingly. The details are summarized as Algorithm 1.

In each iteration of Algorithm 1, the objective function of the problem (P5) is maximized by alternately optimizing t_e and $\tilde{\mathbf{V}}$. Thus, as the number of iterations increases, the objective value of the problem (P4) is monotonically non-decreasing, i.e. the secrecy rate obtained in each iteration is greater or closer to the secrecy rate obtained in the previous iteration. Furthermore, the feasible domain of the problem (P4) with respect to the reflecting phase vector $\tilde{\mathbf{v}}_2$, is bounded and closed. According to the above two properties, Algorithm 1 is guaranteed to converge to an optimal solution.

In the sub-problem for optimizing $\boldsymbol{\Phi}_2$, there are N^2 variables and the iteration accuracy is denoted as ϵ_1. As a result, the computational complexity of Algorithm 1 can be deduced as $\mathcal{O}\left(N^2\log\frac{1}{\epsilon_1}\right)^{3.5}$ [44].

2) Optimizing α for Given $\boldsymbol{\Phi}_2$:

Similarly, for a given $\boldsymbol{\Phi}_2$, the unit modulus constraint on $\boldsymbol{\Phi}_2$ can be ignored. We first set C, D and E for simplicity as

$$C=\frac{\eta P_b\left\|\mathbf{H}_{rj}^\dagger\boldsymbol{\Phi}_1\mathbf{h}_{br}+\mathbf{h}_{bj}\right\|^2\mathrm{tr}\left(\tilde{\mathbf{V}}\mathbf{A}_{JE}\mathbf{w}_J\mathbf{w}_J^\dagger\mathbf{A}_{JE}^\dagger\right)}{\sigma^2}, \tag{40}$$

$$D=1+\rho_u\mathrm{tr}\left(\tilde{\mathbf{V}}\boldsymbol{\psi}_E\right), \tag{41}$$

$$E=\log_2\left(1+\rho_u\mathrm{tr}\left(\tilde{\mathbf{V}}\boldsymbol{\psi}_B\right)\right). \tag{42}$$

After introducing $t_1=\alpha$ and $t_2=1-\alpha$, C_s can be rewritten as a function of $\mathbf{t}=[t_1,t_2]$ as

$$C_s=t_2E+t_2\log_2\left(1+\frac{t_1}{t_2}C\right)-t_2\log_2\left(D+\frac{t_1}{t_2}C\right). \tag{43}$$

Accordingly, the problem (P2) can be transformed as

$$(\mathrm{P6}):\max_{t_1,t_2}\quad C_s \tag{44}$$

$$s.t.\quad t_1+t_2\le 1, \tag{45}$$

$$0\le t_1,t_2\le 1. \tag{46}$$

We can observe that the objective function of the problem (P6) is non-convex. We should first convert the non-convex item of the problem (P6) to make it solvable. Define a function $f(x_1,x_2)$ with variables $x_1\ge 0$ and $x_2\ge 0$ as

$$f\left(x_1,x_2\right)=\begin{cases}x_1\log\left(1+\frac{x_2}{x_1}\mu\right), & x_1>0,\\ 0, & x_1=0.\end{cases} \tag{47}$$

According to [45], it is known that $f(x_1,x_2)$ is a jointly concave function with respect to x_1 and x_2. Therefore, define the non-convex item in the problem (P6) as

$$f(t_1,t_2)=-t_2\log_2\left(D+\frac{t_1}{t_2}C\right). \tag{48}$$

It needs to be converted to convex using its linear approximation form, i.e., the first-order Taylor series expansion at the fixed point $(\bar{t}_1,\bar{t}_2)$ as

$$\begin{aligned}f(t_1,t_2|\bar{t}_1,\bar{t}_2)=&-\left[\log_2\left(\frac{\bar{t}_1C}{\bar{t}_2}+D\right)+\frac{1}{\ln 2}\left(\frac{D}{\frac{\bar{t}_1C}{\bar{t}_2}+D}-1\right)\right]t_2\\&-\left[\frac{1}{\ln 2}\left(\frac{C}{\frac{\bar{t}_1C}{\bar{t}_2}+D}\right)\right]t_1\\=&-Ft_2-Gt_1.\end{aligned} \tag{49}$$

Since $f(t_1,t_2)\ge f(t_1,t_2|\bar{t}_1,\bar{t}_2)$, the equality holds when $t_1=\bar{t}_1$ and $t_2=\bar{t}_2$. Thus, C_s can be changed as

$$C_s=t_2\log_2\left(1+\frac{t_1}{t_2}C\right)+(E-F)t_2-Gt_1. \tag{50}$$

It can be observed that (50) is a concave function of $\mathbf{t}$ and the constraint in (45) is affine. Thus, the optimization problem (P6) is convex and satisfies the Slater's condition [46], and thus the Lagrange duality method can be used to solve it. Based on (44)-(46), the Lagrangian function of the problem (P6) can be expressed as

$$\begin{aligned}\mathcal{L}(t_1,t_2,\lambda)=&C_s-\lambda\left(t_1+t_2-1\right)\\=&t_2\log_2\left(1+\frac{t_1}{t_2}C\right)+(E-F-\lambda)t_2-(G+\lambda)t_1+\lambda,\end{aligned} \tag{51}$$

where λ denotes the Lagrange multiplier related to the constraint in (45). Therefore, we can denote the dual problem of (P6) as

$$\min_{\lambda>0}\max_{t_1\ge 0,t_2\ge 0}\mathcal{L}\left(t_1,t_2,\lambda\right), \tag{52}$$

The optimal solution $\mathbf{t}^*$ can be easily found by solving the dual problem.

Proposition 1: The optimal solution to $\mathbf{t}^* = [t_1^*, t_2^*]$ can be calculated as

$$t_1^* = \left(\frac{t_2^*}{(G+\lambda^*)\ln 2} - \frac{t_2^*}{C} \right)^+, \tag{53}$$

$$t_2^* = \frac{t_1^* C}{z^*}, \tag{54}$$

where $\lambda^* > 0$ denotes the optimal dual solution and z^* denotes the solution to the following equation.

$$\begin{aligned} f(z) &= \ln(1+z) - \frac{z}{1+z} \\ &= (F - E + \lambda)\ln 2. \end{aligned} \tag{55}$$

Proof: To solve the optimization problem (P6), the Karush-Kuhn-Tucker (KKT) conditions need to be satisfied as follows.

$$\begin{aligned} \frac{\partial \mathcal{L}}{\partial t_1^*} &= \frac{C}{\left(1 + \frac{t_1^*}{t_2^*}C\right)\ln 2} - (G + \lambda^*) \\ &= 0, \end{aligned} \tag{56}$$

$$\begin{aligned} \frac{\partial \mathcal{L}}{\partial t_2^*} &= \ln\left(1 + \frac{t_1^*}{t_2^*}C\right) - \frac{\frac{t_1^*}{t_2^*}C}{\left(1 + \frac{t_1^*}{t_2^*}C\right)} + (E - F - \lambda^*)\ln 2 \\ &= 0, \end{aligned} \tag{57}$$

$$\lambda^* \left(t_1^* + t_2^* - 1\right) = 0. \tag{58}$$

Since $t_1^* + t_2^* = 1$ should hold for the problem (P6), we assume that $\lambda^* > 0$ without loss of generality. From (56), we have t_1^* in (53) with the given t_2^* and λ^*. Let $z^* = \frac{t_1^* C}{t_2^*}$, and thus (57) can be transformed as

$$f(z) = (F - E + \lambda^*)\ln 2, \tag{59}$$

where $f(z)$ is given in (55). It should be noticed that $f(z)$ is monotonically increasing of $z \geq 0$ with $f(0) = 0$. In order to obtain a unique solution z^* to (55), $\lambda^* \geq E - F$ has to be satisfied. After solving the equation (55), t_2^* can be obtained as per (54). ∎

From Proposition 1, we can obtain the optimal solutions t_1^* and t_2^* by fixing one of them to optimize another in turn with a given λ. With $\mathbf{t}^*$ obtained for each given λ, the optimal λ^* can be found within the range as

$$(\text{P7}): find \quad \lambda^* \tag{60}$$

$$s.t. \quad \lambda \leq \frac{C}{\ln 2} - G, \tag{61}$$

$$\lambda \geq (E - F)^+, \tag{62}$$

$$t_1^*(\lambda) + t_2^*(\lambda) = 1. \tag{63}$$

Since t_1 and t_2 are non-negative, (61) and (62) can be obtained from (56) and (57), respectively. (53) and (54) show that t_1^* and t_2^* are the functions of λ, and thus (63) can be obtained with $t_1^* + t_2^* = 1$. It can be seen that $g(\lambda) = t_1^*(\lambda) + t_2^*(\lambda) - 1$ increases as λ decreases until $g(\lambda^*) = 0$, where λ^* can be obtained by the bisection method. If λ is not within the feasible range, i.e., there is no solution λ^* that can satisfy the problem (P7). Let $t_1^* = 0$ and $t_2^* = 1$, that is, all the time is used for the information transmission. Finally, the optimal $\lambda^\star$ and $\mathbf{t}^\star$ can be obtained by alternatively optimizing with one of them fixed until the secrecy rate converges. Then, the optimal time switching factor $\alpha^\star$ can be determined by $\alpha^\star = t_1^\star$. Thus, we can solve the problem (P6) according to Algorithm 2.

Algorithm 2 Proposed algorithm to solve the problem (P6).

Input: C, D and E.
Output: $\alpha^\star$.
1: Initialize $t_1^{(0)}$, $t_2^{(0)}$, $\bar{t}_1^{(0)}$, $\bar{t}_2^{(0)}$, $F^{(0)}$ and $G^{(0)}$.
2: Set $k = 0$ as the index of iteration.
3: **repeat**
4: Update $k = k + 1$.
5: Obtain the optimal $\lambda^{(k)}$ by solving the problem (P7) for given $t_1^{(k-1)}$ and $t_2^{(k-1)}$.
6: Obtain the optimal $t_1^{(k)}$ according to (53) for given $\bar{t}_2^{(k-1)}$ and $\lambda^{(k)}$.
7: Obtain the optimal $t_2^{(k)}$ according to (54) for given $t_1^{(k)}$ and $\lambda^{(k)}$.
8: Update $\bar{t}_1^{(k)} = t_1^{(k)}$, $\bar{t}_2^{(k)} = t_2^{(k)}$, $F^{(k)}$ and $G^{(k)}$.
9: **until** The objective value of the problem (P6) converges.
10: The optimal solution $\alpha^\star = t_1$.

In Algorithm 2, the optimal solution to the problem (P6) ensures that the objective value is monotonically non-decreasing as the increasing number of iterations, i.e., $C_s\left(\alpha^{(k)}\right) \geq C_s\left(\alpha^{(k-1)}\right)$. where k is the index of iteration and $C_s(x)$ represents the objective value based on the variable x for the problem (P6). Furthermore, due to the constraints of the time switching factor, Algorithm 2 can converge to a stable local optimum.

In the specific process to solve this sub-problem, we start from the lower bound $\lambda_0 = (E - F)^+$ of λ and increase in steps $e_1 = 1.5$ until we find a λ_1 such that $t_1(\lambda_1) + t_2(\lambda_2) \leq 1$ is satisfied. Then, λ^* can be found using the bisection method between λ_0 and λ_1. Assuming that $Q = \lambda_1 - \lambda_0$, the computational complexity of the algorithm used to find λ_1 is equal to $\mathcal{O}\left(\frac{Q}{e_1}\right)$ and the computational complexity of the bisection method is $\mathcal{O}(\log Q)$. The number of iterations of Algorithm 2 is defined as A. Therefore the computational complexity of Algorithm 2 can be deduced as

$$\mathcal{O}\left(A\left(\frac{Q}{e_1} + \log Q\right)\right). \tag{64}$$

C. Overall Algorithm

Algorithm 3 shows the overall algorithm to solve the proposed scheme, where ϵ denotes a small threshold. In conclusion, the optimal closed-form solution to IRS's phase-shift matrix in the first phase can be given first. Then, to tackle the non-convex problem (P2), we divide it into two sub-problems by fixing one variable and solving the other one. The optimal solutions $\mathbf{\Phi}_2^\star$ and $\alpha^\star$ are obtained by alternately running Algorithm 1 and Algorithm 2 until convergence. As a result, the phase-shifting matrix and the time allocation factor can be optimally achieved to significantly improve the secrecy performance for the proposed secure scheme aided by both the IRS and EH jammer. The convergence of Algorithm 3 is proved by the following proposition.

Algorithm 3 Overall algorithm to solve the proposed scheme.

Input: ρ_u, ρ_j, $\boldsymbol{\psi}_B$, $\boldsymbol{\psi}_E$, $\boldsymbol{A}_{JE}$, $\mathbf{A}_{BJ}$, C, D and E.
Output: $\boldsymbol{\Phi}_1^\star$, $\boldsymbol{\Phi}_2^\star$, $\alpha^\star$.

1: Obtain the optimal closed-form solution $\mathbf{v}_1^\star$ according to (25).
2: Initialize $\tilde{\mathbf{v}}_2^{(0)}$ and $C_s^{(0)}$.
3: set $p=0$ as the index of iteration.
4: **repeat**
5: Update $p=p+1$.
6: Obtain the optimal $\tilde{\mathbf{v}}_2^{(p)}$ by using Algorithm 1 for a given $\alpha^{(p-1)}$.
7: Obtain the optimal $\alpha^{(p)}$ by using Algorithm 2 for a given $\tilde{\mathbf{v}}_2^{(p)}$.
8: Update $C_s^{(p)}$ with the solution $\tilde{\mathbf{v}}_2^{(p)}$ and $\alpha^{(p)}$.
9: **until** $C_s^{(p)} - C_s^{(p-1)} < \epsilon$ or the maximum number of iterations is reached.
10: Recover $\mathbf{v}_2$ from $\tilde{\mathbf{v}}_2$ and obtain the optimal solutions $\boldsymbol{\Phi}_1^\star = \mathrm{diag}(\mathbf{v}_1^\star)$ and $\boldsymbol{\Phi}_2^\star = \mathrm{diag}(\mathbf{v}_2^\star)$.

Proposition 2: On the basis of the convergence of Algorithm 1 and Algorithm 2, the secrecy rate continues to increase and then converge to a stable value with iterations, which is guaranteed by the alternate optimization in Algorithm 3.

Proof: Set the feasible solution to the problem (P2) in the $(p-1)$th iteration as $\left(\tilde{\mathbf{v}}_2^{(p-1)}, \alpha^{(p-1)}\right)$, and thus the secrecy rate can be expressed as $C_s\left(\tilde{\mathbf{v}}_2^{(p-1)}, \alpha^{(p-1)}\right)$ correspondingly. In the pth iteration, $\tilde{\mathbf{v}}_2^{(p)}$ is the optimal solution to Algorithm 1 for given $\alpha^{(p-1)}$, and thus the secrecy rate $C_s\left(\tilde{\mathbf{v}}_2^{(p)}, \alpha^{(p-1)}\right)$ of Step 6 satisfies

$$C_s\left(\tilde{\mathbf{v}}_2^{(p)}, \alpha^{(p-1)}\right) \geq C_s\left(\tilde{\mathbf{v}}_2^{(p-1)}, \alpha^{(p-1)}\right). \tag{65}$$

In the following Step 7, $\alpha^{(p)}$ is obtained as the optimal solution to Algorithm 2, and thus

$$C_s\left(\tilde{\mathbf{v}}_2^{(p)}, \alpha^{(p)}\right) \geq C_s\left(\tilde{\mathbf{v}}_2^{(p)}, \alpha^{(p-1)}\right). \tag{66}$$

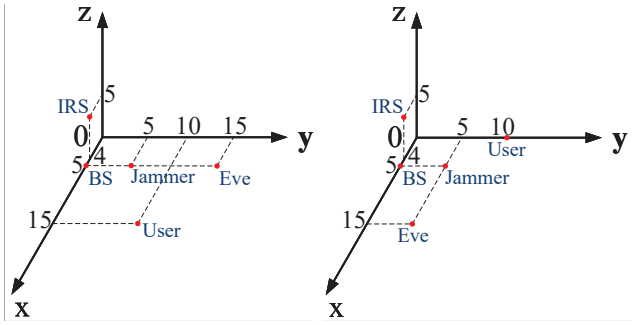
As such, we have

$$C_s\left(\tilde{\mathbf{v}}_2^{(p)}, \alpha^{(p)}\right) \geq C_s\left(\tilde{\mathbf{v}}_2^{(p-1)}, \alpha^{(p-1)}\right). \tag{67}$$

Therefore, the secrecy rate is monotonically increasing with the number of iterations and has an upper bound due to the constraints of time switching factor and IRS elements. This means that Algorithm 3 is convergent. ■

The computational complexities of Algorithm 1 and Algorithm 2 has been obtained above. In order to obtain the optimal solutions, Algorithm 3 iterates alternately over Algorithm 1 and Algorithm 2. Define the number of iterations as B, and thus the computational complexity of the overall algorithm can be expressed as

$$\mathcal{O}\left(B\left(\left(N^2\log\frac{1}{\epsilon_1}\right)^{3.5} + A\left(\frac{Q}{e_1}+\log Q\right)\right)\right). \tag{68}$$



(a) $d_{ue} < d_{ub}$ (b) $d_{ue} > d_{ub}$

Fig. 2. Coordinate setups of the simulations

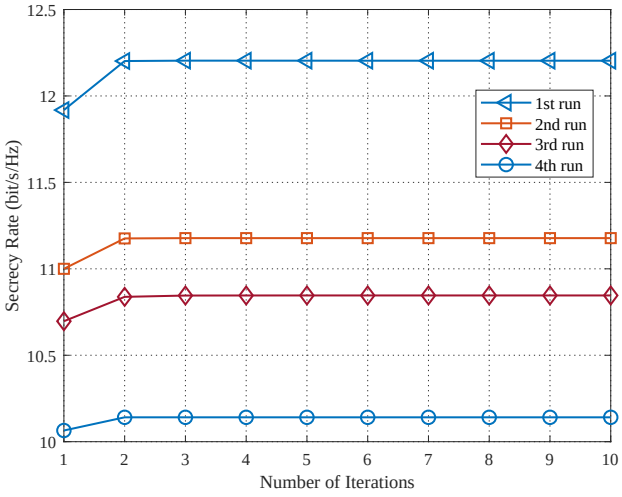


Fig. 3. Convergence performance for Algorithm 3 of four random runs with the number of iterations.

VI. Simulation Results and Discussion

In this section, we demonstrate the performance of the proposed Jammer-IRS scheme through simulations. Set the situation $d_{ue} < d_{ub}$ and $d_{ue} > d_{ub}$ as Case 1 and Case 2, respectively. As shown in Fig. 2(a), the locations of Case 1 are set as BS (5, 0, 0), IRS (4, 0, 5), User (15, 10, 0), Eve (5, 15, 0) and Jam (5, 5, 0) in meters, unless otherwise specified. User (0, 10, 0) and Eve (15, 5, 0) in Case 2, as shown in Fig. 2(b), are different from Case 1. Assume that the IRS with a square array grows in the manner of $(\sqrt{N})^2$. We set the number of antennas at the Jam $M = 2$ and the Rician factor $K = 3$ dB. The transmit power of BS and the user are $P_b = 40$ dBm and $P_u = 20$ dBm, respectively, except where else stated. Set the path loss $L_0 = -30$ dB, the power of AWGN $\sigma^2 = -110$ dBm, the EH efficiency $\eta = 0.5$ and the threshold $\epsilon = 10^{-2}$. The exponents of path loss are $a_d = 3.6$, $a_r = 2.2$ and $a_{bj} = 2$, respectively.

In order to verify the convergence performance of Algorithm 3, we randomly conduct four simulations of Case 1 and record the secrecy rate as the number of iterations increases, shown in Fig. 3. From the results, we can observe that with the increasing number of iterations, the secrecy rate first increases and then converges to a fixed value rapidly within only

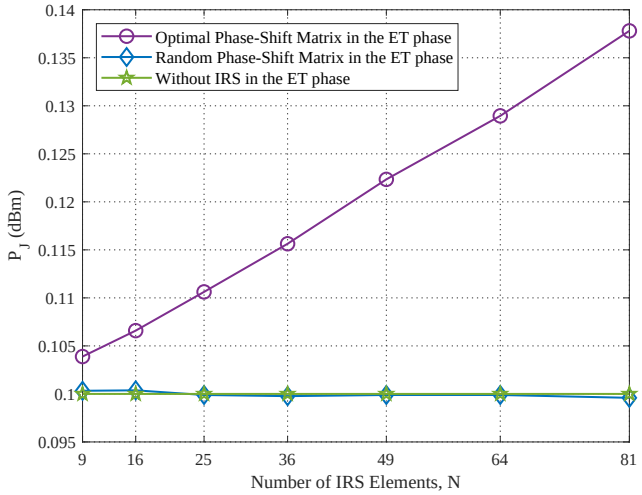


Fig. 4. Transmit power of Jam comparison of optimized IRS, random IRS and non-IRS with different N for a given α.

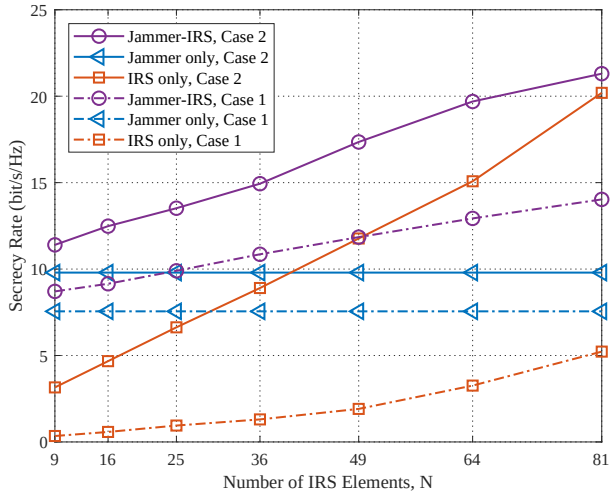


Fig. 5. Secrecy rate comparison between the proposed scheme and benchmarks with different N.

3 iterations. Thus, the convergence of Algorithm 3 can be verified.

As shown in Fig. 4, with a given $\alpha = 0.2$, the transmit power of Jam remains almost constant when the IRS is not used or it is with a random phase-shift matrix in the ET phase. Furthermore, the transmit power of Jam with the random phase-shift matrix is almost equal to that without IRS, which confirms that the IRS with random phase-shift matrix cannot help the Jam harvest energy. On the contrary, by optimizing IRS's phase-shift matrix in the ET phase, the energy harvested by the Jam is significantly better than that of IRS with a random phase-shift matrix and without IRS. Furthermore, when N increases, the amount of harvested energy obviously increases when the phase-shift matrix is optimized. This validates that the proposed scheme can maximize the harvested energy at the Jam. Besides, the results indicate that the IRS with optimal phase-shift matrix can help jammer to harvest the required energy with a smaller time switching factor α, and thus can facilitate the information transmission of the second phase and improve the secrecy performance.

Under different locations Case 1 and Case 2, the secrecy rate C_s and the time switching factor α are compared in Fig. 5 and Fig. 6, respectively. For comparison, we consider the following two benchmarks.

- **IRS only**: During the whole time frame, the user transmits confidential information to the BS aided by IRS in the presence of eavesdropper.
- **Jammer only**: In the ET phase, the EH jammer harvests energy from the BS without IRS. In the IT phase, the EH jammer transmits jamming signal to help the legitimate uplink transmission without IRS.

The secrecy rate of the proposed "Jammer-IRS" scheme in Case 1 and Case 2 is compared in Fig. 5 with the benchmarks including "IRS only" in Case 1 and 2, and "Jammer only" in Case 1 and 2, with different N. Notice that the secrecy rate of both the schemes "Jammer-IRS" and "IRS only" increases with N, while the "Jammer only" scheme remains constant.

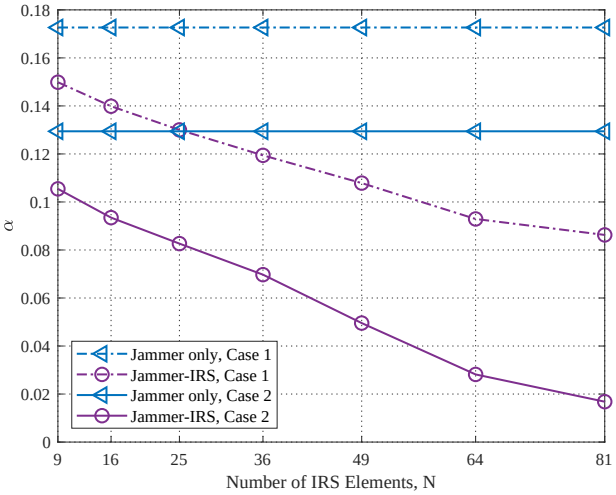


Fig. 6. Time switching factor α comparison between the proposed scheme and the "Jammer only" benchmark with different N.

It is also shown that the proposed scheme outperforms the benchmarks. Specifically, in Case 2, with a small N, both the proposed scheme and the "Jammer only" benchmark perform better than "IRS only" when the Jam contributes more to the improvement of secrecy performance. With the increase of N, the performance of "Jammer-IRS" is gradually close to that of "IRS only", indicating that the IRS plays a greater role in the security enhancement. However, even in Case 1 where the eavesdropper is a threat, the "Jammer-IRS" always outperforms the "IRS only", which shows that the combination of jammer and IRS can significantly enhance the security.

As shown in Fig. 6, we compare the time switching factor between the the proposed scheme and the "Jammer only" benchmark with different N. We can find that the value of time switching factor α in the "Jammer-IRS" scheme is always smaller than that in the "Jammer only" benchmark in both Case 1 and Case 2. This is because deploying IRS is helpful

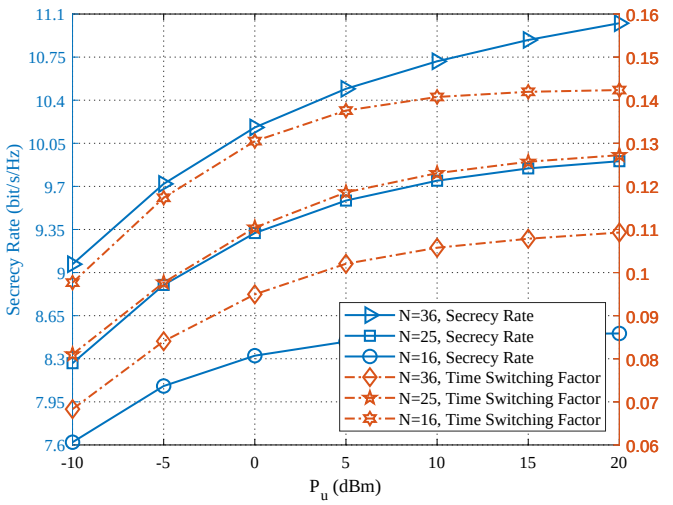


Fig. 7. Performance comparison of secrecy rate and time switching factor α with different user transmit power. N = 16, 25 and 36.

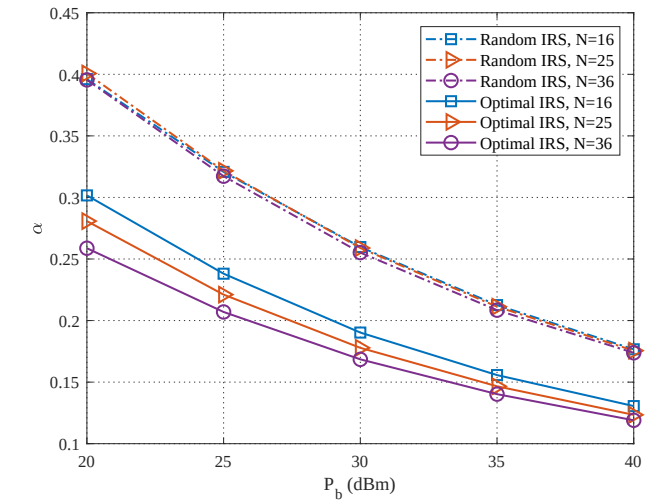


Fig. 8. Time switching factor α comparison between the optimal IRS scheme and the random IRS benchmark with the growth of P_b and N.

to the Jam's energy harvesting in the first phase, and thus the value of α decreases accordingly. Meanwhile, with the increasing of N, the reflection capacity of IRS is enhanced and more time can be allocated for the second phase. Therefore, with the growing N, α decreases in the proposed scheme, while remains constant in the "Jammer only" benchmark without IRS.

Both the secrecy rate and the time switching factor are compared in Fig. 7 under different user transmit power, with N = 16, 25 and 36. As P_u increases, what can be clearly seen in this figure is the growth of both the secrecy rate and time switching factor α. An explanation for this is that the risk of confidential information leakage increases influenced by the increasing transmit power of user, and thus more time is allocated to the ET phase for EH to enhance the security of information transmission. The secrecy rate also increases thanks to the well-protected transmission of confidential information. With different N = 16, 25 and 36, it can be seen that IRS with a higher number of elements N has stronger reflecting ability, which can help jammer to harvest energy faster in the ET phase, and then enhance legal information transmission and weaken eavesdropping information simultaneously in the IT phase. Therefore, α is smaller while the secrecy rate is higher with a larger N. Another important finding is that the growth rate of α is small when P_u is relatively large, which means that the time switching factor α tends to a stable value. At this time, for IRS with a smaller number of reflecting elements N, the increase in secrecy rate is smaller due to the weaker reflecting ability of IRS. As the number of reflecting elements N increases, the reflecting ability of IRS increases and thus the growth rate of the secrecy rate becomes faster with larger P_u and near-constant α.

Fig. 8 compares the time switching factor α between the proposed scheme and the random IRS benchmark with different P_b and N, where the IRS benchmark adopts a random phase-shift matrix in both ET and IT phase. From the results, we can see that α decreases with P_b in both optimal IRS

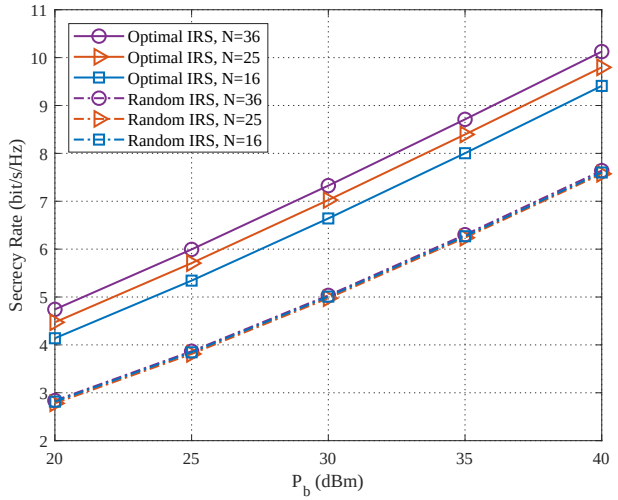


Fig. 9. Secrecy performance comparison between the optimal IRS scheme and the random IRS benchmark with different P_b and N.

scheme and random IRS benchmark. Increasing the transmit power of BS can help the Jam collect the energy faster, and thus α decreases accordingly. Compared with the random IRS benchmark, the proposed scheme can help the Jam harvest energy to effectively reduce the duration of the first phase. In addition, with the increase of N, the ability of IRS in the proposed scheme can be enhanced, and thus α can be also reduced accordingly while α of the random IRS benchmark is not affected by the number of IRS elements.

With different P_b and N, the secrecy rate between the proposed scheme and the random IRS benchmark is compared in Fig. 9. Contrary to Fig. 8, the secrecy rate increases with P_b. This is because the increase of P_b can lead to the decrease in the time switching factor α, which is shown in Fig. 8. As α decreases, more time will be allocated for the IT phase to improve the secrecy rate. Affected by increasing number of IRS elements, the secrecy performance of the proposed scheme

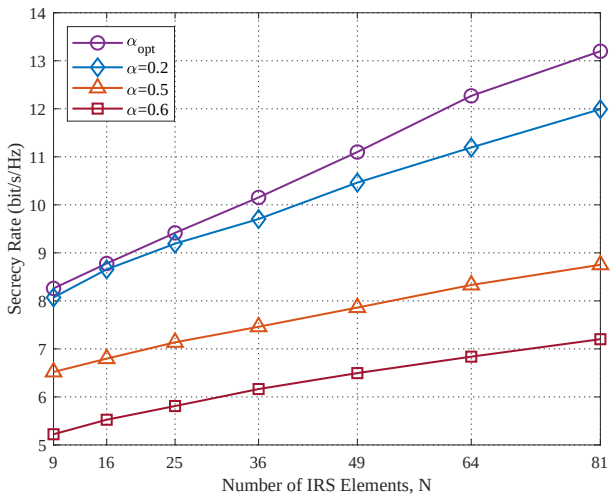


Fig. 10. Secrecy performance comparison between the optimal α and the fixed α of 0.2, 0.5 and 0.6, with different N.

can be enhanced whereas the secrecy rate of the random IRS benchmark remains almost unchanged. Furthermore, it is obvious that the proposed scheme can significantly improve the secrecy rate compared to the benchmark of random IRS, which verifies the effectiveness of the proposed scheme in security enhancement.

Fig. 10 compares the secrecy rate with the optimal α by using Algorithm 2 and fixed α of 0.2, 0.5 and 0.6. From the results, we can see that the secrecy rate with the optimal α via Algorithm 2 is better than that with a fixed α, which demonstrates that optimizing α can significantly improve the secrecy performance. To be specific, with a small N, such as 9 and 16, the secrecy rate of the optimized α is close to that with the fixed α = 0.2, but still much higher than that when α = 0.5 and 0.6, this indicates that the optimal α is close to 0.2 at this time. As N increases, the optimal α via Algorithm 2 decreases, which leads to a larger gap of the secrecy rate with that of α = 0.2.

VII. Conclusions

In this paper, we have proposed a secure uplink transmission scheme assisted by both the IRS and EH jammer. In the first phase, the harvested energy at the Jam is maximized by designing the phase-shift matrix of IRS. In the second phase, the secrecy rate is maximized by jointly optimizing the phase-shift matrix of IRS and the time switching factor. By applying triangle inequality in the ET phase, the closed-form solution to the phase-shift matrix of IRS can be derived first. In the IT phase, the non-convex problem with the phase-shift matrix of IRS and the time switching factor is decoupled into two sub-problems. One of the non-convex sub-problems is approximated as a convex one by SDR to obtain the optimal solution of phase-shift matrix of IRS. The other non-convex sub-problem with the time switching factor is converted into a Lagrange duality one to solve. With optimal solutions to the two sub-problems, this initial coupling problem can be solved by the proposed iterative algorithm. Compared with the benchmarks via simulations, it is shown that the proposed scheme can effectively improve the security performance of the uplink wireless communications. In the future work, the energy compensation among frames will be further considered.

References

[1] T. Qiao, Y. Cao, J. Tang, N. Zhao, and K.-K. Wong, "Uplink secure communication via intelligent reflecting surface and energy-harvesting jammer," in *Proc. IEEE GLOBECOM*, pp. 1–6, Rio de Janeiro, Brazil, Dec. 2022.

[2] F. Zhu and M. Yao, "Improving physical-layer security for CRNs using SINR-based cooperative beamforming," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1835–1841, Mar. 2016.

[3] Y. Cao, N. Zhao, F. R. Yu, M. Jin, Y. Chen, J. Tang, and V. C. M. Leung, "Optimization or alignment: Secure primary transmission assisted by secondary networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 905–917, Apr. 2018.

[4] D. Li, Y. Cao, Z. Yang, Y. Chen, S. Zhang, N. Zhao, and Z. Ding, "Secrecy analysis in NOMA full-duplex relaying networks with artificial jamming," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 8781–8794, Sept. 2021.

[5] X. Chen, J. Chen, H. Zhang, Y. Zhang, and C. Yuen, "On secrecy performance of multiantenna-jammer-aided secure communications with imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8014–8024, Oct. 2016.

[6] Y. Cao, N. Zhao, G. Pan, Y. Chen, L. Fan, M. Jin, and M.-S. Alouini, "Secrecy analysis for cooperative NOMA networks with multi-antenna full-duplex relay," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5574–5587, Aug. 2019.

[7] J.-H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[8] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart. 2017.

[9] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2734–2771, 3rd Quart. 2019.

[10] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[11] C. Wang, H.-M. Wang, X.-G. Xia, and C. Liu, "Uncoordinated jammer selection for securing SIMOME wiretap channels: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2596–2612, May 2015.

[12] M. Kim, S. Kim, and J. Lee, "Securing communications with friendly unmanned aerial vehicle jammers," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1972–1977, Feb. 2021.

[13] Y. Bi and A. Jamalipour, "Accumulate then transmit: Toward secure wireless powered communication networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6301–6310, Jul. 2018.

[14] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.

[15] X. Pang, M. Sheng, N. Zhao, J. Tang, D. Niyato, and K.-K. Wong, "When UAV meets IRS: Expanding air-ground networks via passive reflection," *IEEE Wireless Commun.*, vol. 28, no. 5, pp. 164–170, Oct. 2021.

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

[17] Y. Zhang, C. Zhong, Z. Zhang, and W. Lu, "Sum rate optimization for two way communications with intelligent reflecting surface," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 1090–1094, May 2020.

[18] Y. Han, W. Tang, S. Jin, C.-K. Wen, and X. Ma, "Large intelligent surface-assisted wireless communication exploiting statistical CSI," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8238–8242, Aug. 2019.

[19] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, Aug. 2019.

[20] Y. Mi and Q. Song, "Energy efficiency maximization for IRS-aided WPCNs," *IEEE Wireless Commun. Lett.*, vol. 10, no. 10, pp. 2304–2308, Oct. 2021.

[21] Z. Chu, W. Hao, P. Xiao, and J. Shi, "Intelligent reflecting surface aided multi-antenna secure transmission," *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 108–112, Jan. 2020.

[22] L. Dong and H.-M. Wang, "Secure MIMO transmission via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 787–790, Jun. 2020.

[23] Q. Wang, F. Zhou, R. Q. Hu, and Y. Qian, "Energy efficient robust beamforming and cooperative jamming design for IRS-assisted MISO networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 4, pp. 2592–2607, Apr. 2021.

[24] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700–6705, Jul. 2018.

[25] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[26] M. Zeng, N.-P. Nguyen, O. A. Dobre, and H. V. Poor, "Securing downlink massive MIMO-NOMA networks with artificial noise," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 685–699, Jun. 2019.

[27] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, Dec. 2015.

[28] S. Xu, Y. Du, J. Liu, and J. Li, "Intelligent reflecting surface based backscatter communication for data offloading," *IEEE Trans. Commun.*, vol. 70, no. 6, pp. 4211–4221, Jun. 2022.

[29] K. Cao, B. Wang, H. Ding, L. Lv, R. Dong, T. Cheng, and F. Gong, "Improving physical layer security of uplink NOMA via energy harvesting jammers," *IEEE Trans. Inf. Forens. Security*, vol. 16, pp. 786–799, Sept. 2020.

[30] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401–415, Jan. 2016.

[31] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy performance optimization for wireless powered communication networks with an energy harvesting jammer," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 764–774, Feb. 2017.

[32] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1488–1492, Sept. 2019.

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

[34] L. Dong and H.-M. Wang, "Enhancing secure MIMO transmission via intelligent reflecting surface," *IEEE Trans. Wireless Commun.*, vol. 19, no. 11, pp. 7543–7556, Nov. 2020.

[35] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2637–2652, Nov. 2020.

[36] S. Xu, J. Liu, and Y. Cao, "Intelligent reflecting surface empowered physical-layer security: Signal cancellation or jamming?," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1265–1275, Jan. 2022.

[37] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless communications: A tutorial," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3313–3351, Jan. 2021.

[38] B. Zheng and R. Zhang, "Intelligent reflecting surface-enhanced OFDM: Channel estimation and reflection optimization," *IEEE Wireless Commun. Lett.*, vol. 9, no. 4, pp. 518–522, Apr. 2020.

[39] J. Li, L. Zhang, K. Xue, Y. Fang, and Q. Sun, "Secure transmission by leveraging multiple intelligent reflecting surfaces in MISO systems," *IEEE Trans. Mob. Comput.*, to appear.

[40] B. Zheng, C. You, and R. Zhang, "Double-IRS assisted multi-user MIMO: Cooperative passive beamforming design," *IEEE Trans. Wireless Commun.*, vol. 20, no. 7, pp. 4513–4526, Jul. 2021.

[41] J. Li, K. Xue, D. S. L. Wei, J. Liu, and Y. Zhang, "Energy efficiency and traffic offloading optimization in integrated satellite/terrestrial radio access networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 4, pp. 2367–2381, Jan. 2020.

[42] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, Jun. 2020.

[43] Z.-q. Luo, W.-k. Ma, A. M.-c. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.

[44] A. Khalili, S. Zargari, Q. Wu, D. W. K. Ng, and R. Zhang, "Multi-objective resource allocation for IRS-aided SWIPT," *IEEE Wireless Commun. Lett.*, vol. 10, no. 6, pp. 1324–1328, Jun. 2021.

[45] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 418–428, Jan. 2014.

[46] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge University Press, 2004.