

Enabling Secure Wireless Communications via Intelligent Reflecting Surfaces

Xianghao Yu, Dongfang Xu, and Robert Schober
Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
Email: {xianghao.yu, dongfang.xu, robert.schober}@fau.de

Abstract—In this paper, we propose to utilize intelligent reflecting surfaces (IRSs) for enhancing the physical layer security of wireless communications systems. In particular, an IRS-assisted secure wireless system is considered, where a multi-antenna transmitter communicates with a single-antenna receiver in the presence of an eavesdropper. To maximize the secrecy rate, both the beamformer at the transmitter and the IRS phase shifts are jointly optimized. Based on the block coordinate descent (BCD) and minorization maximization (MM) techniques, two efficient algorithms are developed to solve the resulting non-convex optimization problem for small- and large-scale IRSs, respectively. Simulation results show that IRSs can significantly improve physical layer security if the proposed algorithms are employed. Furthermore, we reveal that deploying large-scale IRSs is more efficient than enlarging the antenna array size of the transmitter for both boosting the secrecy rate and enhancing the energy efficiency.

I. INTRODUCTION

Physical layer security has received considerable attention from both academia and industry in recent years [1]. Various approaches to improve physical layer security have been proposed in the literature, e.g., cooperative relaying schemes, artificial noise-aided beamforming [2], and cooperative jamming [3]. However, deploying a large number of relays or other helpers in secure wireless systems inevitably incurs an excessive cost. Furthermore, cooperative jamming and transmitting artificial noise consume additional power for security provisioning. These shortcomings of existing approaches urgently call for a new paradigm for secure wireless systems, which is both cost-effective and energy-efficient.

With the rapid development of radio frequency (RF) micro-electro-mechanical systems (MEMS), programmable and re-configurable meta-surfaces have recently found abundant applications in the public and civil domains, among which intelligent reflecting surfaces (IRSs) have drawn special attention for their applications in wireless communications [4]. The artificial thin films of IRSs can be easily coated on existing infrastructures such as walls of buildings, which reduces implementation cost and complexity. In addition, unlike conventional communication transceivers, IRSs consume no power as they are passive devices. Furthermore, different from conventional transceivers, IRSs help transmit information without generating new signals. Instead, they smartly transform or recycle existing signals. To sum up, IRSs are passive cost-effective devices with the ability to control the radio propagation environment [5]. These characteristics make IRSs promising key enablers for improving the physical layer security of wireless communications in an economical and energy-efficient manner.

There are several studies on the design of IRS-assisted wireless systems [6]–[9]. A point-to-point multiple-input single-output (MISO) system was investigated in [6], [7], where the IRS is implemented with continuous and discrete phase shifters, respectively. Based on the semidefinite relaxation (SDR) method, approximate solutions for the beamformer at the access point and the phase shifts at the IRS were developed. The authors of [8] considered a downlink multiuser communication system, where the signal-to-interference-plus-noise ratio (SINR) was maximized for given phase shifts. Energy efficiency maximization was tackled in [9], where sub-optimum zero-forcing beamforming was assumed at the access point. We note that none of these existing works considers physical layer security, despite its great importance for modern wireless systems.

To fill this gap, this paper investigates physical layer security provisioning for IRS-assisted wireless systems. Assume a transmitter equipped with multiple antennas communicates with one legitimate receiver in the presence of an eavesdropper. Both the legitimate receiver and the eavesdropper are assumed to use a single antenna, and the IRS is implemented via programmable phase shifters. Our goal is to maximize the secrecy rate of the considered system by optimizing both the beamformer at the transmitter and the phase shifts at the IRS, which leads to a non-convex optimization problem. Based on the block coordinate descent (BCD) and minorization maximization (MM) techniques, two efficient algorithms are proposed for solving the problem. The first algorithm is more suitable for small-scale IRSs, while the second algorithm is advantageous for large-scale IRSs. Unlike existing works [6], [8], [9], we obtain locally optimal solutions for both the beamformer and the phase shifts. To the best of the authors' knowledge, this is the first work that studies the design of secure IRS-assisted wireless systems.

Notations: The imaginary unit of a complex number is denoted by $j = \sqrt{-1}$. Matrices and vectors are denoted by boldface capital and lower-case letters, respectively. $\mathbb{C}^{m \times n}$ denotes the set of all $m \times n$ complex-valued matrices. \mathbf{I}_m is the m -dimensional identity matrix. The i -th element of vector \mathbf{a} is denoted as a_i . \mathbf{A}^* and \mathbf{A}^H stand for the conjugate and conjugate transpose of matrix \mathbf{A} . $\text{diag}(a_1, \dots, a_n)$ denotes a diagonal matrix whose diagonal entries are a_1, \dots, a_n . The largest eigenvalue of matrix \mathbf{A} and the corresponding eigenvector are denoted by $\lambda_{\max}(\mathbf{A})$ and $\mathbf{\lambda}_{\max}(\mathbf{A})$, respectively. \triangleq means “defined as”. Expectation and the real part of a complex number are denoted by $\mathbb{E}[\cdot]$ and $\Re(\cdot)$, respectively. The operation $\angle(\mathbf{A})$ constructs a matrix by extracting the

phases of the elements of matrix \mathbf{A} .

II. SYSTEM MODEL

Consider an IRS-assisted communication system, which consists of a transmitter, one legitimate receiver, an eavesdropper, and an IRS, as shown in Fig. 1. We assume that the transmitter is equipped with N_t antennas, while the legitimate receiver and the eavesdropper use a single receive antenna, respectively. The passive IRS is deployed in the network to improve the physical layer security, and employs M phase shifters. Equipped with a controller, the phase shifts of the IRS are programmable. Furthermore, we assume a quasi-static flat-fading channel model and perfect channel state information (CSI) knowledge at both the transmitter and the IRS¹. The received baseband signals at the legitimate receiver and the eavesdropper can be expressed as

$$\begin{aligned} y_l &= \mathbf{h}_l^H \Phi \mathbf{G} \mathbf{f} x + n_l, \\ y_e &= \mathbf{h}_e^H \Phi \mathbf{G} \mathbf{f} x + n_e, \end{aligned} \quad (1)$$

where $\mathbf{h}_l \in \mathbb{C}^{M \times 1}$ and $\mathbf{h}_e \in \mathbb{C}^{M \times 1}$ represent the channels from the IRS to the legitimate receiver and eavesdropper, respectively. The phase shift matrix Φ of the IRS is given by $\Phi = \text{diag}(e^{j\theta_1}, e^{j\theta_2}, \dots, e^{j\theta_M})$, where θ_k is the phase shift of the k -th reflecting element of the IRS [6]. The channel matrix from the transmitter to the IRS is denoted as $\mathbf{G} \in \mathbb{C}^{M \times N_t}$, and the linear beamforming vector at the transmitter side is denoted as $\mathbf{f} \in \mathbb{C}^{N_t \times 1}$. The signal transmitted to the legitimate receiver is denoted as x , where $\mathbb{E}[|x|^2] = 1$ without loss of generality. n_l and n_e are additive complex Gaussian noises with variances σ_l^2 and σ_e^2 , respectively.

The achievable secrecy rate of the IRS-assisted MISO wireless system is given by [10]

$$C = \left[\log \left(1 + \frac{1}{\sigma_l^2} |\mathbf{h}_l^H \Phi \mathbf{G} \mathbf{f}|^2 \right) - \log \left(1 + \frac{1}{\sigma_e^2} |\mathbf{h}_e^H \Phi \mathbf{G} \mathbf{f}|^2 \right) \right]^+, \quad (2)$$

where $[x]^+ = \max\{0, x\}$. Our goal in this paper is to maximize the secrecy rate by optimizing the transmit beamforming vector \mathbf{f} and the phase shift matrix Φ of the IRS. We note that dropping the operator $[\cdot]^+$ in (2) has no impact on the optimization². The resulting optimization is formulated as

$$\begin{aligned} \mathcal{P}_1 : \quad & \underset{\mathbf{f}, \Phi}{\text{maximize}} \quad \frac{1 + \frac{1}{\sigma_l^2} |\mathbf{h}_l^H \Phi \mathbf{G} \mathbf{f}|^2}{1 + \frac{1}{\sigma_e^2} |\mathbf{h}_e^H \Phi \mathbf{G} \mathbf{f}|^2} \\ & \text{subject to} \quad \|\mathbf{f}\|^2 \leq P \\ & \quad \Phi = \text{diag}(e^{j\theta_1}, e^{j\theta_2}, \dots, e^{j\theta_M}), \end{aligned} \quad (3)$$

where $P \geq 0$ is the given total transmit power.

¹While the CSI of the eavesdropper is generally difficult to acquire, the results in this paper serve as theoretical performance upper bounds for the considered system. These bounds and the insights gained from them can be used to guide the system design for the case when the CSI of the eavesdropper is not perfectly known.

²The secrecy rate is zero if the transmission is turned off. Hence, the term $\log \left(1 + \frac{1}{\sigma_l^2} |\mathbf{h}_l^H \Phi \mathbf{G} \mathbf{f}|^2 \right) - \log \left(1 + \frac{1}{\sigma_e^2} |\mathbf{h}_e^H \Phi \mathbf{G} \mathbf{f}|^2 \right)$ will always be non-negative if the beamformer and the phase shifts are optimized to maximize the secrecy rate.

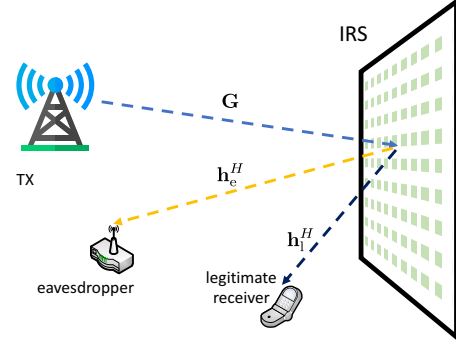


Fig. 1. An IRS-assisted secure communication system.

Remark 1: Note that, different from secure wireless systems without IRSs, in the second constraint of optimization problem \mathcal{P}_1 , each diagonal element in the phase shift matrix Φ has unit modulus, i.e., $|e^{j\theta_k}| = 1$. This non-convex constraint together with the non-convex objective function makes \mathcal{P}_1 a non-convex problem. The globally optimal solution of non-convex optimization problems with unit modulus constraints is in general not tractable [11].

III. DESIGN OF SECURE IRS-ASSISTED WIRELESS SYSTEMS

Block coordinate descent (BCD) methods optimize the objective function with respect to different subsets (blocks) of optimization variables in each iteration while the other blocks are fixed. BCD has been shown to be a widely applicable and empirically successful approach in many applications [11], [12], and typically leads to a sub-optimal solution for non-convex problems. In this paper, we resort to this approach as the main methodology for solving \mathcal{P}_1 efficiently.

A. Transmit Beamformer Design

According to the principle of BCD, we first investigate the optimization of beamforming vector \mathbf{f} for a fixed phase shift matrix Φ . The beamformer design problem is accordingly given by

$$\mathcal{P}_2 : \underset{\|\mathbf{f}\|^2 \leq P}{\text{maximize}} \quad \frac{1 + \frac{1}{\sigma_l^2} |\mathbf{h}_l^H \Phi \mathbf{G} \mathbf{f}|^2}{1 + \frac{1}{\sigma_e^2} |\mathbf{h}_e^H \Phi \mathbf{G} \mathbf{f}|^2}, \quad (4)$$

and the optimal solution is provided in the following lemma.

Lemma 1. Given the phase shift matrix Φ of the IRS, the optimal solution for beamforming vector \mathbf{f} is given by

$$\mathbf{f}^* = \sqrt{P} \lambda_{\max} (\mathbf{X}_e^{-1} \mathbf{X}_l), \quad (5)$$

where

$$\mathbf{X}_i = \mathbf{I}_{N_t} + \frac{P}{\sigma_i^2} \mathbf{G}^H \Phi^H \mathbf{h}_i \mathbf{h}_i^H \Phi \mathbf{G}, \quad i \in \{l, e\}. \quad (6)$$

Proof: It was shown in [13] that allocating all transmit power for beamforming is optimal, i.e., $\|\mathbf{f}^*\|^2 = P$. Then, the numerator and denominator of the objective function of \mathcal{P}_2 can be rewritten as

$$1 + \frac{P}{\sigma_l^2} |\mathbf{h}_l^H \Phi \mathbf{G} \tilde{\mathbf{f}}|^2 = \tilde{\mathbf{f}}^H \tilde{\mathbf{f}} + \frac{P}{\sigma_l^2} \tilde{\mathbf{f}}^H (\mathbf{G}^H \Phi^H \mathbf{h}_l \mathbf{h}_l^H \Phi \mathbf{G}) \tilde{\mathbf{f}}$$

$$\tilde{\theta}_k = \arctan \frac{c_{e,k}d_{1,k} \cos(p_{1,k}) - c_{1,k}d_{e,k} \cos(p_{e,k})}{c_{e,k}d_{1,k} \sin(p_{1,k}) - c_{1,k}d_{e,k} \sin(p_{e,k})} - \arccos \frac{d_{1,k}d_{e,k} \sin(p_{e,k} - p_{1,k})}{\sqrt{c_{e,k}^2d_{1,k}^2 + c_{1,k}^2d_{e,k}^2 - 2c_{1,k}c_{e,k}d_{1,k}d_{e,k} \cos(p_{1,k} - p_{e,k})}} \quad (12)$$

$$\triangleq \tilde{\mathbf{f}}^H \mathbf{X}_i \tilde{\mathbf{f}}, \quad (7)$$

where $\tilde{\mathbf{f}} = \mathbf{f}/\sqrt{P}$ is a unit vector. By substituting (7) into the objection function of \mathcal{P}_2 , we can rewrite \mathcal{P}_2 as

$$\underset{\|\tilde{\mathbf{f}}\|^2=1}{\text{maximize}} \quad \frac{\tilde{\mathbf{f}}^H \mathbf{X}_1 \tilde{\mathbf{f}}}{\tilde{\mathbf{f}}^H \mathbf{X}_e \tilde{\mathbf{f}}}. \quad (8)$$

In this way, we transform \mathcal{P}_2 to a generalized eigenvalue problem, whose optimal solution is given by (5). ■

Remark 2: The result in Lemma 1 is similar to secure beamforming design for MISO communications without IRSs, for which a closed-form solution is available [13]. In particular, the beamformer \mathbf{f} is designed to be as orthogonal to the effective eavesdropping channel $\mathbf{h}_e^H \Phi \mathbf{G}$ as possible, while being as aligned with the effective legitimate receiver channel $\mathbf{h}_1^H \Phi \mathbf{G}$ as possible. Compared to conventional secure communications systems, the incorporation of the IRS adds another degree of freedom (DoF) to establish favorable effective channels $\mathbf{h}_1^H \Phi \mathbf{G}$ and $\mathbf{h}_e^H \Phi \mathbf{G}$ by carefully choosing the phase shift matrix Φ .

To the best of the authors' knowledge, there is no general approach for the optimal design of the phase shift matrix Φ . Hence, in the following two subsections, we propose two different approaches for optimizing Φ in the BCD procedure.

B. Element-Wise BCD

In this subsection, we adopt an element-wise BCD for optimizing the phase shift matrix Φ . In other words, we take each phase shift θ_k as one block in the BCD. The corresponding optimization problem is given by

$$\mathcal{P}_3 : \underset{\theta_k}{\text{maximize}} \quad \frac{1 + \frac{1}{\sigma_1^2} |\mathbf{h}_1^H \Phi \mathbf{G} \mathbf{f}|^2}{1 + \frac{1}{\sigma_e^2} |\mathbf{h}_e^H \Phi \mathbf{G} \mathbf{f}|^2} \quad (9)$$

subject to $\Phi = \text{diag}(e^{j\theta_1}, \dots, e^{j\theta_k}, \dots, e^{j\theta_M})$.

The optimal solution is presented in the following lemma.

Lemma 2. *Given the beamforming vector \mathbf{f} and phase shifts $\{\theta_m\}_{m \neq k}$, the optimal solution for θ_k is given by*

$$\theta_k^* = \begin{cases} \tilde{\theta}_k + \pi & c_{e,k}d_{1,k} \cos(p_{1,k}) < c_{1,k}d_{e,k} \cos(p_{e,k}) \\ \tilde{\theta}_k & \text{otherwise,} \end{cases} \quad (10)$$

where

$$c_{i,k} = \frac{1}{2} \left(1 + \frac{1}{\sigma_i^2} |h_{i,k}^* \mathbf{g}_k^H \mathbf{f}|^2 + \frac{1}{\sigma_i^2} \left| \sum_{m \neq k} h_{i,m}^* e^{j\theta_m} \mathbf{g}_m^H \mathbf{f} \right|^2 \right),$$

$$d_{i,k} = \frac{1}{\sigma_i^2} \left| h_{i,k}^* \mathbf{g}_k^H \mathbf{f} \sum_{m \neq k} h_{i,m} e^{-j\theta_m} \mathbf{f}^H \mathbf{g}_m \right|, \quad (11)$$

$$p_{i,k} = \angle \left(h_{i,k}^* \mathbf{g}_k^H \mathbf{f} \sum_{m \neq k} h_{i,m} e^{-j\theta_m} \mathbf{f}^H \mathbf{g}_m \right), \quad i \in \{1, e\},$$

Algorithm 1 Element-Wise BCD

- 1: Construct an initial $\Phi^{(0)}$ and set $t = 0$;
 - 2: **repeat**
 - 3: Fix $\Phi^{(t)}$ and optimize $\mathbf{f}^{(t)}$ according to (5);
 - 4: **for** $k = 1$ **to** M **do**
 - 5: Optimize the phase shift $\theta_k^{(t+1)}$ according to (10);
 - 6: **end for**
 - 7: $t \leftarrow t + 1$;
 - 8: **until** convergence;
-

\mathbf{g}_k^H is the k -th row of matrix \mathbf{G} , and $\tilde{\theta}_k$ is given by (12) shown on top of this page.

Proof: See Appendix A. ■

With Lemmas 1 and 2 at hand, the element-wise BCD is summarized in **Algorithm 1**. As the closed-form globally optimal solutions in (5) and (10) are used in each block of the element-wise BCD, the objective function monotonically increases. In addition, it is easy to verify that the objective function is upper bounded by the point-to-point MISO channel capacity. These two properties together guarantee that **Algorithm 1** converges to a locally optimal solution of \mathcal{P}_1 . However, the number of BCD blocks is $M + 1$ since each phase shift is a block. This leads to a slow convergence for large IRS sizes M .

C. Alternating Optimization With MM

Instead of treating each phase θ_k as a single block in the BCD, in this subsection, we take the entire phase shift matrix Φ as one block. Consequently, there are only two blocks in the BCD. Hence, the BCD reduces to the special case of alternating optimization (AO). By leveraging the minorization maximization (MM) technique, we update all phase shifts $\{\theta_k\}_{k=1}^M$ in parallel in each iteration.

We reformulate the optimization of the phase shift matrix Φ as follows. Using

$$\mathbf{h}_i^H \Phi \mathbf{G} = \mathbf{v}^H \mathbf{R}_i, \quad i \in \{1, e\}, \quad (13)$$

where $\mathbf{v} = [e^{j\theta_1}, \dots, e^{j\theta_M}]^H$ and $\mathbf{R}_i = \text{diag}(\mathbf{h}_i^H) \mathbf{G}$, the numerator and denominator in (9) can be rewritten as

$$1 + \frac{1}{\sigma_i^2} |\mathbf{h}_i^H \Phi \mathbf{G} \mathbf{f}|^2 \stackrel{(a)}{=} \frac{1}{M} \mathbf{v}^H \mathbf{v} + \frac{1}{\sigma_i^2} \mathbf{v}^H \mathbf{R}_i \mathbf{f} \mathbf{f}^H \mathbf{R}_i^H \mathbf{v} \triangleq \mathbf{v}^H \mathbf{Y}_i \mathbf{v}, \quad (14)$$

where $\mathbf{Y}_i = \frac{1}{M} \mathbf{I}_M + \frac{P}{\sigma_i^2} \mathbf{R}_i \mathbf{f} \mathbf{f}^H \mathbf{R}_i^H$, and step (a) exploits $\mathbf{v}^H \mathbf{v} = M$. Therefore, optimization problem \mathcal{P}_3 can be recast as

$$\mathcal{P}_4 : \underset{\mathbf{v}}{\text{maximize}} \quad g(\mathbf{v}) = \frac{\mathbf{v}^H \mathbf{Y}_1 \mathbf{v}}{\mathbf{v}^H \mathbf{Y}_e \mathbf{v}} \quad (15)$$

subject to $|v_k| = 1, \quad k \in \{1, 2, \dots, M\}$.

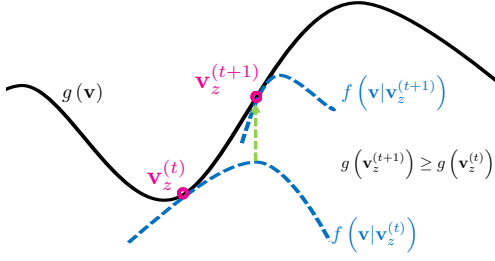


Fig. 2. The procedure of minorization maximization.

Remark 3: The main difficulty in solving \mathcal{P}_4 is the unit modulus constraint, which is element-wise and highly non-convex. By introducing $\mathbf{V} = \mathbf{v}\mathbf{v}^H$ as the optimization variable and relaxing the rank-one constraint of \mathbf{V} , \mathcal{P}_4 can be solved via semidefinite relaxation (SDR). The resulting problem is a quasi-convex problem, whose optimal solution can be obtained by solving a series of semidefinite programming (SDP) problems. However, there is no guarantee that the obtained solution \mathbf{V} is a rank-one matrix, and therefore the SDR approach can only provide an approximate solution for \mathbf{v} . As a result, the objective function does not necessarily increase in each iteration of the AO, and the convergence of the SDR-based algorithm cannot be guaranteed. In addition, the computational complexity of solving a large number of SDP problems in each iteration of the AO is prohibitively high.

In this paper, we propose to solve \mathcal{P}_4 by the MM technique [14], whose main idea is illustrated in Fig. 2. In particular, assuming the value of \mathbf{v} in the t -th iteration of the AO is denoted as $\mathbf{v}_z^{(t)}$, we construct a lower bound on the objective function $g(\mathbf{v})$ that touches the objective function at point $\mathbf{v}_z^{(t)}$, denoted as $f(\mathbf{v}|\mathbf{v}_z^{(t)})$. We adopt this lower bound as a surrogate objective function, and the maximizer of this surrogate objective function is then taken as the value of \mathbf{v} in the next iteration of the AO, i.e., $\mathbf{v}_z^{(t+1)}$. In this way, the objective value is monotonically increasing from one iteration to the next, i.e., $g(\mathbf{v}_z^{(t+1)}) \geq g(\mathbf{v}_z^{(t)})$. The key to the success of MM lies in constructing a surrogate objective function $f(\mathbf{v}|\mathbf{v}_z^{(t)})$ for which the maximizer $\mathbf{v}_z^{(t+1)}$ is easy to find. For phase shift matrix optimization problem \mathcal{P}_4 , a surrogate objective function is composed in the following lemma.

Lemma 3. The objective function $g(\mathbf{v})$ is lower bounded by

$$g(\mathbf{v}) = \frac{\mathbf{v}^H \mathbf{Y}_1 \mathbf{v}}{\mathbf{v}^H \mathbf{Y}_e \mathbf{v}} \geq f(\mathbf{v}|\mathbf{v}_z) + [g(\mathbf{v}_z) - f(\mathbf{v}_z|\mathbf{v}_z)], \quad (16)$$

where

$$f(\mathbf{v}|\mathbf{v}_z) = 2 \frac{\Re(\mathbf{v}_z^H \mathbf{Y}_1 \mathbf{v})}{\mathbf{v}_z^H \mathbf{Y}_e \mathbf{v}_z} - \frac{\mathbf{v}_z^H \mathbf{Y}_1 \mathbf{v}_z}{(\mathbf{v}_z^H \mathbf{Y}_e \mathbf{v}_z)^2} \left\{ \mathbf{v}^H \lambda_{\max}(\mathbf{Y}_e) \mathbf{v} + 2\Re(\mathbf{v}_z^H [\mathbf{Y}_e - \lambda_{\max}(\mathbf{Y}_e) \mathbf{I}_M] \mathbf{v}) \right\}, \quad (17)$$

and $g(\mathbf{v}_z) - f(\mathbf{v}_z|\mathbf{v}_z)$ is a constant term that is irrelevant for optimization.

Proof: Defining $y = \mathbf{v}^H \mathbf{Y}_e \mathbf{v}$, the objective function $g(\mathbf{v}) \triangleq \frac{\mathbf{v}^H \mathbf{Y}_1 \mathbf{v}}{y}$ is jointly convex in $\{\mathbf{v}, y\}$ since $\mathbf{Y}_1 = \frac{1}{M} \mathbf{I}_M +$

Algorithm 2 Alternating Optimization With Minorization Maximization (AO-MM)

- 1: Construct an initial $\mathbf{v}_z^{(0)}$ and set $t = 0$;
 - 2: **repeat**
 - 3: Fix $\mathbf{v}_z^{(t)}$ and optimize $\mathbf{f}^{(t)}$ according to (5);
 - 4: Optimize $\mathbf{v}_z^{(t+1)}$ according to (20) and (21);
 - 5: $t \leftarrow t + 1$;
 - 6: **until** convergence.
-

$\frac{P}{\sigma_1^2} \mathbf{R}_1 \mathbf{f} \mathbf{f}^H \mathbf{R}_1^H$ is positive definite. Because of the convexity, we have the following inequality

$$\begin{aligned} \frac{\mathbf{v}^H \mathbf{Y}_1 \mathbf{v}}{\mathbf{v}^H \mathbf{Y}_e \mathbf{v}} &\geq 2 \frac{\Re(\mathbf{v}_z^H \mathbf{Y}_1 \mathbf{v})}{\mathbf{v}_z^H \mathbf{Y}_e \mathbf{v}_z} - \frac{\mathbf{v}_z^H \mathbf{Y}_1 \mathbf{v}_z}{(\mathbf{v}_z^H \mathbf{Y}_e \mathbf{v}_z)^2} \mathbf{v}^H \mathbf{Y}_e \mathbf{v} \\ &\stackrel{(b)}{\geq} f(\mathbf{v}|\mathbf{v}_z) + [g(\mathbf{v}_z) - f(\mathbf{v}_z|\mathbf{v}_z)], \end{aligned} \quad (18)$$

where (b) applies [15, Lemma 1]. ■

Proposition 1. The phase shift optimization problem in each iteration of the AO is equivalent to

$$\mathcal{P}_5 : \mathbf{v}_z^{(t+1)} = \arg \max_{|v_i|=1} \Re \left[\left(\mathbf{w}^{(t)} \right)^H \mathbf{v} \right], \quad (19)$$

where

$$\begin{aligned} \mathbf{w}^{(t)} &= \frac{\mathbf{Y}_1 \mathbf{v}_z^{(t)}}{\left(\mathbf{v}_z^{(t)} \right)^H \mathbf{Y}_e \mathbf{v}_z^{(t)}} - \frac{\left(\mathbf{v}_z^{(t)} \right)^H \mathbf{Y}_1 \mathbf{v}_z^{(t)}}{\left[\left(\mathbf{v}_z^{(t)} \right)^H \mathbf{Y}_e \mathbf{v}_z^{(t)} \right]^2} \\ &\quad \times [\mathbf{Y}_e - \lambda_{\max}(\mathbf{Y}_e) \mathbf{I}_M] \mathbf{v}_z^{(t)}. \end{aligned} \quad (20)$$

The optimal solution of \mathcal{P}_5 is given by³

$$\angle \left(\mathbf{v}_z^{(t+1)} \right) = \angle \left(\mathbf{w}^{(t)} \right). \quad (21)$$

Proof: With Lemma 3, the optimization problem that needs to be solved is the maximization of $f(\mathbf{v}|\mathbf{v}_z)$ in (17) with respect to \mathbf{v} . Since $\mathbf{v}^H \mathbf{v}$ is a constant, the proposition can be proved with basic algebraic manipulations. ■

The AO-MM algorithm is presented in **Algorithm 2**. With the closed-form solutions in (5) and (21), the objective function is guaranteed to monotonically increase and to converge to a local optimum. There are some open issues that require further remarks.

(1) *Initial point:* In both the element-wise BCD and AO-MM algorithms, we require an initialization for the phase shifts of the IRS. As \mathcal{P}_1 is a non-convex problem, the quality of the sub-optimal solution depends to some extent on the initialization. Here, we propose an effective way to construct the initial values of the phase shifts. In particular, we set

$$\angle \left(\mathbf{v}_z^{(0)} \right) = \angle(\mathbf{u}), \quad \Phi^{(0)} = \text{diag} \left(\mathbf{v}_z^{(0)} \right), \quad (22)$$

where \mathbf{u} is the dominant left singular vector of \mathbf{R}_1 in (13). This initialization is a heuristic obtained by ignoring the denominator of the objective function.

³Since \mathbf{v}_z is a unit modulus vector, it is sufficient to determine the phases of the elements of the vector.

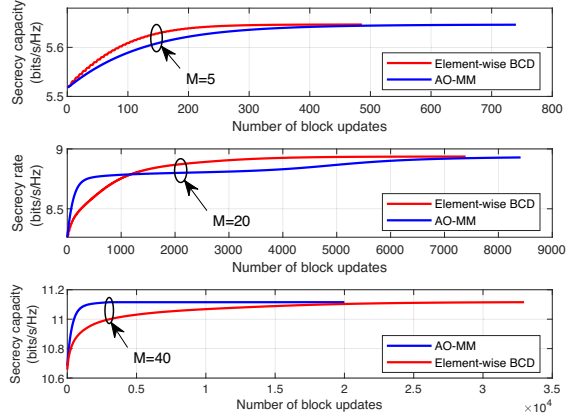


Fig. 3. Convergence of the proposed algorithms for different values of M when $N_t = 5$, $\alpha = 4$, $P = 5$ dBm, $r_{TR} = 250$ m, $r_{RI} = r_{Re} = 160$ m.

(2) *Complexity comparison*: As closed-form solutions are obtained for all the blocks of both algorithms, the computational complexity of the proposed algorithms is critically determined by the total number of block updates until convergence. In particular, the number of blocks in each iteration of the element-wise BCD algorithm is $\frac{M+1}{2}$ times higher than that of the AO-MM algorithm. On the other hand, as globally optimal solutions (11) are obtained for all the blocks of the element-wise BCD algorithm, the number of iterations needed for convergence is less than for the AO-MM algorithm, in which the phase shifts are updated in parallel but sub-optimally by (21). Therefore, there is a trade-off between the number of blocks per iteration and the number of iterations required for convergence, which shall be investigated in the next section.

IV. SIMULATION RESULTS

In this section, we numerically evaluate the performance of the proposed algorithms. The channels are assumed to be independent Rayleigh fading, and the path loss exponent is denoted by α with reference distance 10 meters. The noise power at both the legitimate receiver and the eavesdropper is set to $\sigma_1^2 = \sigma_e^2 = -80$ dBm. The distance between the transmitter and the IRS is denoted as r_{TR} , while r_{RI} and r_{Re} are the distances from the IRS to the legitimate receiver and the eavesdropper, respectively. The simulation results in Figs. 4 and 5 are averaged over 1000 channel realizations.

A. Comparison of the Proposed Algorithms

The convergence of the proposed algorithms is investigated for three typical examples in Fig. 3. The stopping criterion for convergence is that the increment of the normalized objective function is less than $\epsilon = 10^{-6}$. We first investigate the scenario where the thin film employed to implement the IRS has a small area, e.g., $M = 5$. Although the number of blocks per iteration of the element-wise BCD algorithm is slightly larger for the AO-MM algorithm (6 versus 2), the element-wise BCD algorithm needs much fewer iterations for convergence since globally optimal solutions are obtained for all the blocks. Therefore, the element-wise BCD algorithm converges faster when M is relatively small. On the other hand, as the value of

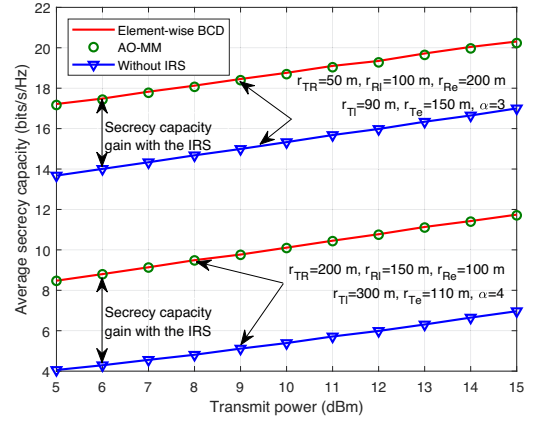


Fig. 4. Average secrecy rate achieved by different algorithms when $M = 10$ and $N_t = 8$.

M gradually increases, i.e., $M = 40$, a large number of blocks (41 blocks) have to be updated in each iteration of the element-wise BCD algorithm, which slows down the convergence. In contrast, only two blocks per iteration have to be updated in the AO-MM algorithm. This offsets the drawback that the AO-MM requires more iterations due to the sub-optimal solutions for each phase shift update block. In summary, the element-wise BCD algorithm is suitable for small-scale IRS systems while the AO-MM algorithm is preferable for large-scale IRS systems.

B. Average Secrecy Rate Evaluation

In Fig. 4, the average achievable secrecy rate is plotted for different algorithms. First, we observe that the average secrecy rate achieved by both proposed algorithms is the same. We also compare our approach with a benchmark system which does not employ an IRS for security provisioning. In this case, the distance between the transmitter and the legitimate receiver is denoted by r_{TI} while the distance between the transmitter and the eavesdropper is denoted by r_{Te} ⁴. To maximize the secrecy rate, optimal transmit beamforming according to (5) is adopted. As can be observed from Fig. 4, the system with IRS provides a significant performance gain in terms of the secrecy rate, which indicates that deploying IRSs is a promising approach for improving the physical layer security of wireless communications systems.

C. Massive MIMO or Massive IRS?

For conventional wireless communications systems, deploying large-scale antenna arrays at the transceivers is an effective way to boost communication performance, including the network capacity and physical layer security. Therefore, it is intriguing to investigate how much performance gain we can obtain from large-scale IRSs. In Fig. 5, we first increase the number of reflecting elements of the IRS while keeping the number of antenna elements as $N_t = 10$ (red curve). In addition, to illustrate the effectiveness of the IRS, we

⁴ The values of r_{TI} and r_{Te} and the performance gains achievable with IRSs depend on the geometry of the network. In Fig. 4, we investigate different geometries by providing one example with $r_{TI} < r_{RI}$ and $r_{Te} < r_{Re}$, and one example with $r_{TI} > r_{RI}$ and $r_{Te} > r_{Re}$.

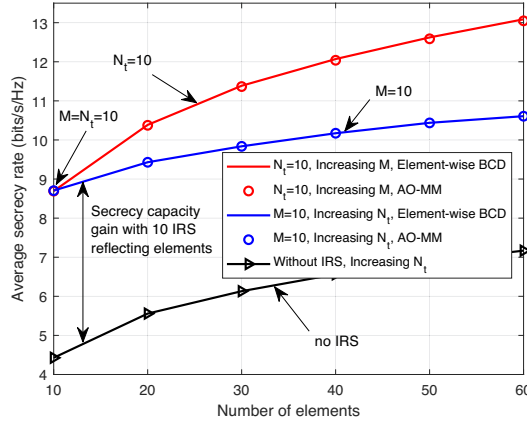


Fig. 5. Average secrecy rate achieved for different values of M and N_t , when $P = 5$ dBm, $\alpha = 4$, $r_{TR} = 200$ m, $r_{RI} = 150$ m, $r_{Re} = 100$ m, $r_{TI} = 300$ m, and $r_{Te} = 110$ m.

also evaluate the average secrecy rate achieved for different numbers of transmit antenna elements when using an IRS with $M = 10$ (blue curve). As can be observed from Fig. 5, increasing the number of IRS reflecting elements is more beneficial for improving the secrecy rate than increasing the number of antenna elements. Moreover, as the IRS is a passive device, deploying large-scale IRSs is more energy-efficient than installing more energy-consuming RF chains and power amplifiers as is needed for increasing the number of antenna elements at the transmitter. These results clearly demonstrate the superiority of IRSs compared with conventional system designs in terms of both communication performance and energy consumption.

V. CONCLUSIONS

In this paper, we proposed to improve the physical layer security of wireless communications networks by deploying IRSs. Two efficient algorithms, i.e., the element-wise BCD and AO-MM algorithms, were developed for joint optimization of the beamformer at the transmitter and the phase shifts at the IRS. The element-wise BCD algorithm was shown to be preferable for small-scale IRS-assisted systems, while the AO-MM algorithm is advantageous for wireless systems with large-scale IRSs. Simulation results have confirmed the huge potential of IRSs to improve the security and energy efficiency of future communications systems.

APPENDIX

As the phase shift matrix Φ is a diagonal matrix, the objective function of \mathcal{P}_3 can be rewritten as a function of the k -th reflecting element as follows:

$$\frac{1 + \frac{1}{\sigma_1^2} |\mathbf{h}_1^H \Phi \mathbf{G} \mathbf{f}|^2}{1 + \frac{1}{\sigma_e^2} |\mathbf{h}_e^H \Phi \mathbf{G} \mathbf{f}|^2} = \frac{c_{1,k} + d_{1,k} \cos(\theta_k + p_{1,k})}{c_{e,k} + d_{e,k} \cos(\theta_k + p_{e,k})}, \quad (23)$$

where $c_{i,k}$, $d_{i,k}$, and $p_{i,k}$ are given in (11). By taking the derivative of the objective function with respect to θ_k , and setting the derivative to zero, we obtain the following equation

$$\begin{aligned} & d_{1,k} \sin(\theta_k + p_{1,k}) [c_{e,k} + d_{e,k} \cos(\theta_k + p_{e,k})] \\ &= d_{e,k} \sin(\theta_k + p_{e,k}) [c_{1,k} + d_{1,k} \cos(\theta_k + p_{1,k})]. \end{aligned} \quad (24)$$

This equation can be further simplified by some basic trigonometric manipulations as follows,

$$A_k \sin \theta_k + B_k \cos \theta_k = d_{1,k} d_{e,k} \sin(p_{e,k} - p_{1,k}), \quad (25)$$

where

$$\begin{aligned} A_k &\triangleq c_{e,k} d_{1,k} \cos p_{1,k} - c_{1,k} d_{e,k} \cos p_{e,k}, \\ B_k &\triangleq c_{e,k} d_{1,k} \sin p_{1,k} - c_{1,k} d_{e,k} \sin p_{e,k}. \end{aligned} \quad (26)$$

When $A_k \geq 0$, by introducing an auxiliary angle, the equation can be recast as

$$\cos\left(\theta_k - \arctan \frac{A_k}{B_k}\right) = \frac{d_{1,k} d_{e,k} \sin(p_{e,k} - p_{1,k})}{\sqrt{A_k^2 + B_k^2}}. \quad (27)$$

It can be readily shown by checking the second derivative that the objective function is maximized when

$$\theta_k = \arctan \frac{A_k}{B_k} - \arccos \frac{d_{1,k} d_{e,k} \sin(p_{e,k} - p_{1,k})}{\sqrt{A_k^2 + B_k^2}}. \quad (28)$$

The optimal solution when $A_k < 0$ can be obtained in a similar manner, which completes the proof.

REFERENCES

- [1] Y. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.
- [2] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Robust and secure resource allocation for full-duplex MISO multicarrier NOMA systems," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 4119–4137, Sep. 2018.
- [3] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
- [4] M. Di Renzo *et al.*, "Smart radio environments empowered by AI reconfigurable meta-surfaces: An idea whose time has come," *arXiv:1903.08925*, Mar. 2019.
- [5] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 162–169, Sep. 2018.
- [6] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network: Joint active and passive beamforming design," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–6.
- [7] —, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *arXiv:1905.00152*, May 2019.
- [8] Q.-U.-A. Nadeem, A. Kammoun, A. Chaaban, M. Debbah, and M.-S. Alouini, "Large intelligent surface assisted MIMO communications," *arXiv:1903.08127*, Mar. 2019.
- [9] 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.*, to appear.
- [10] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
- [11] P. Netrapalli, P. Jain, and S. Sanghavi, "Phase retrieval using alternating minimization," in *Proc. Adv. in Neural Inf. Process. Syst. (NIPS)*, Lake Tahoe, NV, USA, Dec. 2013, pp. 2796–2804.
- [12] X. Yu, J.-C. Shen, J. Zhang, and K. B. Letaief, "Alternating minimization algorithms for hybrid precoding in millimeter wave MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 485–500, Apr. 2016.
- [13] S. Shafiee and S. Ulukus, "Achievable rates in gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 2466–2470.
- [14] Y. Sun, P. Babu, and D. P. Palomar, "Majorization-minimization algorithms in signal processing, communications, and machine learning," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 794–816, Feb. 2017.
- [15] J. Song, P. Babu, and D. P. Palomar, "Optimization methods for designing sequences with low autocorrelation sidelobes," *IEEE Trans. Signal Process.*, vol. 63, no. 15, pp. 3998–4009, Aug. 2015.