Physical Layer Security for Intelligent Reflecting Surface Assisted Two–Way Communications

Mevan Wijewardena, *Student Member, IEEE*, Tharaka Samarasinghe, *Senior Member, IEEE*, Kasun T. Hemachandra, *Member, IEEE*, Saman Atapattu, *Senior Member, IEEE*, and Jamie S. Evans, *Senior Member, IEEE*

***Abstract*— This letter investigates the exploitation of an intelligent reflecting surface (IRS) to communicate securely in a two-way network consisting of an untrusted user. In particular, the transmit powers and the phase shift at each element of the IRS are optimized to maximize the sum-secrecy rate, such that the IRS-reflected and non-IRS-reflected signals are added destructively at the untrusted user. The proposed iterative algorithm converges rapidly to a feasible solution of high accuracy with a few iterations. Numerical results demonstrate sum-secrecy rate gains up to 120% compared to naive or partially optimized schemes.**

***Index Terms*— Intelligent reflecting surface, physical-layer security, secrecy rate, two-way communications.**

I. Introduction

DUE to advancements in wireless technologies, integrating intelligent reflecting surfaces (IRS) into the beyond 5G wireless networks is envisioned to enable many diversified applications [1], [2]. However, the IRS environment is vulnerable to potential attacks by malicious users. Thus, optimal transmit power allocation and IRS phase shift optimization based on physical-layer (PHY) security, are considered crucial in enabling reliable IRS-assisted communications [3]–[15].

Secrecy rate is the commonly used optimization objective in the literature for security provisioning, where the sum-secrecy rate is considered for network-wide performance optimization [5], [16], and the user-fairness-secrecy rate is used for individual user-based performance optimization [17]. Maximizing the secrecy rate in the presence of a transmitter, receiver, eavesdropper and an IRS is studied in the literature, with the knowledge of perfect channel state information (CSI) [5], [6]. Extensions to multiple eavesdroppers [7], [13], and optimization based on the knowledge of statistical CSI of the eavesdropper [13] are also available. However, all these works consider PHY security for one-way communications.

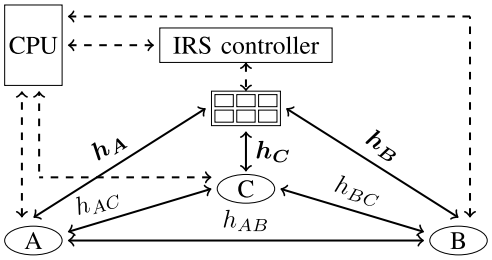

Fig. 1. The IRS-assisted two-way communication model.

Recently, IRS-assisted systems are proposed for two–way wireless communications in [18], which highlights the superiority of two–way communications under proper residual interference cancellation. Subsequently, an IRS assisted secure multiuser two-way communication system is considered in [19], where the signal of one user is exploited as information jamming to disrupt the reception of the other user's signal at an eavesdropper. In contrast to [19], this letter applies the most commonly used PHY security technique for two-way communications of exploiting CSI to allocate power at the transmitters and design passive beamformers at the IRS, by maximizing the sum-secrecy rate. The letter also considers a channel model, where both non-IRS-reflected and IRS-reflected channels between the users are considered in the design process. Our main contributions are summarized below:

- We propose an algorithm that maximizes the sum-secrecy rate of an IRS-assisted two-way communication system operating in the in-band full-duplex (FD) mode, in the presence of an untrusted user. The system is controlled by a central node equipped with a central processing unit (CPU), by adjusting the transmit powers at the two trusted users and the phase shifts introduced by the IRS, in an iterative manner. The convergence of the algorithm is proved analytically and illustrated numerically.
- The performance of the proposed algorithm is compared with other beamformer design schemes, numerically, while considering different placements of the untrusted user. It is shown that the algorithm harvests gains reaching 35% when the untrusted user is located in close proximity to the IRS, and gains reaching 120% when he is in close proximity to a user.

II. System Model

Consider a wireless communication system having three active users, Alice, Bob, and Charlie, as shown in Fig. 1. The users are equipped a transmit antenna and a receive

Manuscript received February 15, 2021; revised March 8, 2021; accepted March 8, 2021. Date of publication March 23, 2021; date of current version July 10, 2021. This work was supported in part by the Australian Research Council (ARC) through the Discovery Project (DP) under Grant DP180101205. The associate editor coordinating the review of this letter and approving it for publication was M. Wen. *(Corresponding author: Saman Atapattu.)*

Mevan Wijewardena and Kasun T. Hemachandra are with the Department of Electronic and Telecommunication Engineering, University of Moratuwa, Moratuwa 10400, Sri Lanka (e-mail: mevan96@ieee.org; kasunh@uom.lk).

Tharaka Samarasinghe is with the Department of Electronic and Telecommunication Engineering, University of Moratuwa, Moratuwa 10400, Sri Lanka, and also with the Department of Electrical and Electronic Engineering, The University of Melbourne, Parkville, VIC 3010, Australia (e-mail: tharakas@uom.lk).

Saman Atapattu and Jamie S. Evans are with the Department of Electrical and Electronic Engineering, The University of Melbourne, Parkville, VIC 3010, Australia (e-mail: saman.atapattu@unimelb.edu.au; jse@unimelb.edu.au).

Digital Object Identifier 10.1109/LCOMM.2021.3068102

antenna, enabling in-band FD communications. Confidential two-way information exchange between Alice and Bob is assisted by a passive IRS with L reflective elements. Charlie is considered an untrusted user. The system is centralized such that the three users and the IRS are connected to a CPU, via low bandwidth links. These channels are used for CSI and control information sharing. It is assumed that while Alice and Bob are communicating, there are no other scheduled transmissions in the network. Throughout the letter, we use subscripts A, B and C to differentiate between notations defined for Alice, Bob, and Charlie, respectively. To this end, the channels between the IRS and the three users are denoted by $\boldsymbol{h}_j \in \mathbb{C}^{L\times 1}$, $j \in \{A, B, C\}$. Also, we denote the non-IRS-reflected channels between the individual users by $h_{ij} \in \mathbb{C}$, $i, j \in \{A, B, C\}$ and $i \neq j$. For simplicity, it is assumed that $\boldsymbol{h}_j$ and h_{ij} capture the effects of both path loss and small-scale fading, which can follow an arbitrary continuous distribution (e.g Rayleigh, Rician, etc.). Furthermore, the system operates in the in-band FD mode, leading to channel reciprocity [18], [19]. It is assumed that all users have access to perfect CSI of channels between themselves and the IRS, as well as the channels between other users. The CSI is acquired using channel estimation techniques discussed in [20]. The CSI can be estimated at Alice and Bob by using reciprocity properties.

Let $\boldsymbol{w}_{\text{ind}}^{\dagger} = \left[\mathrm{e}^{j\phi_1}, \ldots, \mathrm{e}^{j\phi_L}\right]$, where $\phi_i \in [0, 2\pi)$ for $i \in \{1, \ldots, L\}$, denote the phase shift of the i-th IRS element, such that $(\cdot)^{\dagger}$ represents the conjugate transpose. We assume unit reflection amplitudes to maximize the IRS reflection power, simplify its hardware design, and also for the mathematical tractability of our problem. For $j \in \{A, B\}$, P_j and $s_j \in \mathcal{CN}(0, 1)$ denote the transmit power and the information symbol of the respective user. Without loss of generality, we assume s_A and s_B are uncorrelated. The self-interference (SI), which is the users own data reflected back form the IRS, can be fully subtracted using the available CSI and the knowledge of $\boldsymbol{w}_{\text{ind}}^{\dagger}$ obtained from the CPU. After SI cancellation, the received signal at Alice can be written as

$$y_A = \sqrt{P_B}\boldsymbol{w}^{\dagger}\boldsymbol{H}_A s_B + l_A + n_A, \tag{1}$$

where $\boldsymbol{w}^{\dagger} = \left[\boldsymbol{w}_{\text{ind}}^{\dagger}\, 1\right]$, $\boldsymbol{H}_A^{\top} = \left[\boldsymbol{h}_B^{\top}\,\mathrm{diag}\,(\boldsymbol{h}_A)\; h_{AB}\right]$, n_A is the additive white Gaussian noise (AWGN) with mean zero and variance σ_A^2, l_A is the residual loop-interference from FD operation, which is assumed to be a Gaussian random variable with mean zero and variance $\sigma_{l_A}^2$, and $\mathrm{diag}\,(\boldsymbol{x})$ represents the diagonal matrix with entries of vector $\boldsymbol{x}$ along its main diagonal [19]. Thus, the achievable information rate for Alice can be written as $I(y_A; s_B) = \log_2\left(1 + \frac{P_B|\boldsymbol{w}^{\dagger}\boldsymbol{H}_A|^2}{\sigma_{t_A}^2}\right)$ bps/Hz, where $\sigma_{t_A}^2 = \sigma_A^2 + \sigma_{l_A}^2$. The received signal at Bob, y_B, and the achievable information rate for Bob, $I(y_B; s_A)$, can be similarly obtained.

The signal received by Charlie is given by $y_C = \sqrt{P_A}\boldsymbol{w}^{\dagger}\boldsymbol{H}_{CA}s_A + \sqrt{P_B}\boldsymbol{w}^{\dagger}\boldsymbol{H}_{CB}s_B + n_C$, where $\boldsymbol{H}_{CA}^{\top} = \left[\boldsymbol{h}_A^{\top}\boldsymbol{H}_C\, h_{AC}\right]$, $\boldsymbol{H}_{CB}^{\top} = \left[\boldsymbol{h}_B^{\top}\boldsymbol{H}_C\, h_{BC}\right]$, and $\boldsymbol{H}_C = \mathrm{diag}\,(\boldsymbol{h}_C)$. Then, the maximum information rate leaked to Charlie can be written as $I(y_C; \boldsymbol{s}) = \log_2\left(1 + \frac{P_A|\boldsymbol{w}^{\dagger}\boldsymbol{H}_{CA}|^2 + P_B|\boldsymbol{w}^{\dagger}\boldsymbol{H}_{CB}|^2}{\sigma_C^2}\right)$bps/Hz, where $\boldsymbol{s}^{\top} = [s_A,\ s_B]$. Since, $I(y_C; \boldsymbol{s})$ is an upper bound for the achievable information rate of Charlie, the worst case sum-secrecy rate of the system can be given as

$$R_{\text{sum}} = [I(y_B; s_A) + I(y_A; s_B) - I(y_C; \boldsymbol{s})]^{+}, \tag{2}$$

where $[x]^{+} = \max(0, x)$ [16].

III. Sum-Secrecy Rate Maximization

In this section, we present the sum-secrecy rate maximization problem subject to a sum-power constraint, and propose an iterative approach to set the IRS phase shifts and the transmit powers of Alice and Bob. The sum-secrecy rate maximization problem can be stated as follows:

$$\begin{aligned}
\text{(P1):}\ \underset{\boldsymbol{w}, P_A, P_B}{\text{maximize}}\quad & R_{\text{sum}} && \text{(3a)}\\
\text{subject to}\quad & P_i^{\min} \leq P_i \quad i \in \{A, B\}, && \text{(3b)}\\
& P_A + P_B \leq P^{\max}, && \text{(3c)}\\
& |w^{(j)}| = 1 \quad \forall 1 \leq j \leq L, && \text{(3d)}\\
& w^{(L+1)} = 1, && \text{(3e)}
\end{aligned}$$

where $P^{\max}$ denotes the aggregate maximum transmit power, $w^{(j)}$ is the j-th element of vector $\boldsymbol{w}$, and $P_A^{\min}$ and $P_B^{\min}$ are the minimum allowed transmit powers of Alice and Bob, respectively. Hence, the constraint (3b) is added to ensure user fairness. The values of $P_A^{\min}$ and $P_B^{\min}$ can be adjusted to ensure the required minimum information rate at Alice and Bob. The constraint (3d) ensures the elements of $\boldsymbol{w}$ only contribute to the phase of the reflected signal. The constraint (3e) follows from the definition of $\boldsymbol{w}$ in (1). The centralized network architecture motivates the sum-secrecy rate maximization problem with a sum power constraint, which leads to superior performance compared to individual power constraints. However, the analysis can be trivially extended to a case with individual maximum transmit power constraints at Alice and Bob, which is discussed in Section III-D.

From (2), it is interesting to note that R_{sum} is invariant to a phase shift, given it is identical for all elements in $\boldsymbol{w}$. Thus, for a phase shift θ, we define $\tilde{\boldsymbol{w}} = \mathrm{e}^{j\theta}\boldsymbol{w}$, and find $\tilde{\boldsymbol{w}}$ that maximizes R_{sum} without any loss in optimality. With this manipulation, the constraint (3e) can be absorbed into the constraint (3d) by letting $1 \leq i \leq L + 1$. However, (P1) is still not jointly convex in $(\tilde{\boldsymbol{w}}, P_A, P_B)$, and hence, it is difficult to solve (P1) with polynomial complexity. To obtain a solution with polynomial complexity, we consider a relaxed optimization problem with a tight approximation for the objective function.

The main challenge of the optimization problem is the non-convexity of the constraint (3d). To overcome this, we first use the substitution $|\tilde{\boldsymbol{w}}^{\dagger}\boldsymbol{H}|^2 = \mathrm{Tr}(\boldsymbol{H}\boldsymbol{H}^{\dagger}\boldsymbol{W})$, where $\boldsymbol{W} = \tilde{\boldsymbol{w}}\tilde{\boldsymbol{w}}^{\dagger}$, and apply semidefinite relaxation (SDR) [7]. Then, after omitting the constant multipliers and addends that have no impact on the analysis, the objective function $G(\boldsymbol{W}, P_A, P_B)$ can be expressed as a function of $(\boldsymbol{W}, P_A, P_B)$ where

$$\begin{aligned}
G(\boldsymbol{W}, P_A, P_B) = {} & \log_2\left(\sigma_{t_B}^2 + P_A\,\mathrm{Tr}\left(\tilde{\boldsymbol{H}}_B\boldsymbol{W}\right)\right)\\
& + \log_2\left(\sigma_{t_A}^2 + P_B\,\mathrm{Tr}\left(\tilde{\boldsymbol{H}}_A\boldsymbol{W}\right)\right)\\
& - \log_2 F(\boldsymbol{W}, P_A, P_B),
\end{aligned} \tag{4}$$

$F(\boldsymbol{\Omega}, \alpha, \beta) = \sigma_C^2 + \alpha\,\mathrm{Tr}(\tilde{\boldsymbol{H}}_{CA}\boldsymbol{\Omega}) + \beta\,\mathrm{Tr}(\tilde{\boldsymbol{H}}_{CB}\boldsymbol{\Omega})$, $\tilde{\boldsymbol{H}}_A = \boldsymbol{H}_A\boldsymbol{H}_A^{\dagger}$, $\tilde{\boldsymbol{H}}_B = \boldsymbol{H}_B\boldsymbol{H}_B^{\dagger}$, $\tilde{\boldsymbol{H}}_{CA} = \boldsymbol{H}_{CA}\boldsymbol{H}_{CA}^{\dagger}$ and $\tilde{\boldsymbol{H}}_{CB} = \boldsymbol{H}_{CB}\boldsymbol{H}_{CB}^{\dagger}$. Moreover, SDR allows the feasible region of $\boldsymbol{W}$ to be restricted to positive semidefinite matrices and the

non-convex constraint (3d) to be replaced by the constraint on all the main diagonal elements of $\boldsymbol{W}$ being 1. However, observe that the objective function is still not jointly convex in $(\boldsymbol{W}, P_A, P_B)$ due to the manner in which (P_A, P_B) and $\boldsymbol{W}$ are coupled. Hence, finding a tight approximation which leads to joint convexity is non-trivial. This motivates us to use an alternating optimization technique. We first find P_A and P_B while keeping $\boldsymbol{W}$ fixed according to section III-A, and then find $\boldsymbol{W}$ while keeping P_A and P_B fixed according to section III-B. This iterative process runs, until the convergence condition is reached.

A. Transmit Power Optimization

The problem of optimizing transmit powers P_A and P_B for a fixed $\boldsymbol{W}$ can be formulated as

$$\text{(P2):} \quad \underset{P_A,P_B}{\text{maximize}} \; G(\boldsymbol{W}, P_A, P_B) \tag{5a}$$
$$\text{subject to } P_i^{\min} \leq P_i \quad i \in \{A, B\}, \tag{5b}$$
$$P_A + P_B \leq P^{\max}. \tag{5c}$$

The objective function has the form of a difference of convex (DC) function, which is not generally convex. Therefore, transmit power optimization can be solved readily using DC programming algorithms. However, a simpler approach can be developed by careful inspection of the feasible region R_G of (P2). Considering the partial derivatives, it can be identified that, G is monotonic in P_A for fixed P_B, given that P_A, $P_B \in R_G$. A similar observation can be made with respect to P_B for fixed P_A. Hence, we claim that it suffices to consider only points on the boundary $P_A + P_B = P^{\max}$ and the three vertices of R_G to obtain the optimal solution for (P2). This follows since, given any point (P_A^0, P_B^0) strictly inside R_G satisfies $G(\boldsymbol{W}, P_A^{\min}, P_B^0) \geq G(\boldsymbol{W}, P_A^0, P_B^0)$ or $G(\boldsymbol{W}, P^{\max} - P_B^0, P_B^0) \geq G(\boldsymbol{W}, P_A^0, P_B^0)$. Hence it is sufficient to consider only the boundary of R_G to obtain the solution for (P2). Given any point $(P_A^{\min}, P_B^0)$ on the boundary $P_A = P_A^{\min}$, $P_B^{\min} \leq P_B^0 \leq P^{\max} - P_A^{\min}$, we have either $G(\boldsymbol{W}, P_A^{\min}, P_B^{\min}) \geq G(\boldsymbol{W}, P_A^{\min}, P_B^0)$ or $G(\boldsymbol{W}, P_A^{\min}, P^{\max} - P_A^{\min}) \geq G(\boldsymbol{W}, P_A^{\min}, P_B^0)$. Similar claim follows for the points on the boundary $P_B = P_B^{\min}$, which validates our claim. The optima on the boundary $P_A + P_B = P^{\max}$ can be calculated by solving $\frac{\partial G}{\partial P_A}\big|_{P_B = P^{\max} - P_A} = 0$ which leads to a quadratic equation of P_A. Hence we set (P_A, P_B) to be the point which leads to the maximum value of objective (5a) out of the points $(P_i^{\min}, P^{\max} - P_i^{\min})$ for $i \in \{A, B\}$, $(P_A^{\min}, P_B^{\min})$ and $\{(P_A, P_B) | \frac{\partial G}{\partial P_A}\big|_{P_B = P^{\max} - P_A} = 0, (P_A, P_B) \in R_G\}$.

B. IRS Phase Shift Optimization

Firstly, observe that (4) is not necessarily convex with respect to $\boldsymbol{W}$, even when P_A and P_B are fixed due to the subtraction of log terms. Hence, to obtain the IRS phase shifts, we seek an approximation for $G(\boldsymbol{W}, P_A, P_B)$ using a function which is concave with respect to $\boldsymbol{W}$, for fixed P_A and P_B. To this end, we apply first-order Taylor series expansion for the concave function $\log_2(F(\boldsymbol{W}, P_A, P_B))$ in (4) around $\hat{\boldsymbol{W}}$, to obtain a lower-bound given by

$$G_{\hat{\boldsymbol{W}}}(\boldsymbol{W}, P_A, P_B) = (\ln 2)^{-1} \Big\{ \ln\left(\sigma_{t_B}^2 + P_A \operatorname{Tr}\left(\tilde{\boldsymbol{H}}_B \boldsymbol{W}\right)\right) + \ln\left(\sigma_{t_A}^2 + P_B \operatorname{Tr}\left(\tilde{\boldsymbol{H}}_A \boldsymbol{W}\right)\right) - \ln\left(F\left(\hat{\boldsymbol{W}}, P_A, P_B\right)\right) - \frac{F\left(\boldsymbol{W} - \hat{\boldsymbol{W}}, P_A, P_B\right) - \sigma_C^2}{F(\hat{\boldsymbol{W}}, P_A, P_B)} \Big\}. \tag{6}$$

It can be shown that when $\left\|\boldsymbol{W} - \hat{\boldsymbol{W}}\right\|$ is bounded above, the approximation error is also bounded above. Therefore, using this approximation, we reformulate the problem of finding optimal $\boldsymbol{W}$ for given (P_A, P_B) values as

$$\text{(P3):} \quad \underset{\boldsymbol{W}}{\text{maximize}} \; G_{\hat{\boldsymbol{W}}}(\boldsymbol{W}, P_A, P_B) \tag{7a}$$
$$\text{subject to } \boldsymbol{W} \succeq 0, \tag{7b}$$
$$\operatorname{diag}(\boldsymbol{W}) = 1, \tag{7c}$$
$$\left\|\boldsymbol{W} - \hat{\boldsymbol{W}}\right\| < \xi. \tag{7d}$$

It can be observed that (P3) is convex with respect to $\boldsymbol{W}$. The constraint (7c) is to set the diagonal elements of the matrix $\boldsymbol{W}$ to 1, while the constraint (7d) limits the error of the first-order approximation. An iterative procedure can be used to fine tune the solution of (P3) by re-initializing $\hat{\boldsymbol{W}}$ to the optimal value of $\boldsymbol{W}$ found in the previous iteration.

Algorithm 1 Alternating Optimization Algorithm

Data: $\tilde{\boldsymbol{H}}_A$, $\tilde{\boldsymbol{H}}_B$, $\tilde{\boldsymbol{H}}_{CB}$, $\tilde{\boldsymbol{H}}_{CA}$, σ_A, σ_B, σ_C, σ_{l_A}, σ_{l_B}
Result: IRS phase shift vector $\boldsymbol{w}^*$ and transmit powers (P_A^*, P_B^*)
Initialize $\boldsymbol{W} = \hat{\boldsymbol{W}} = \boldsymbol{w}\boldsymbol{w}^\dagger$ such that $\boldsymbol{w} \in \mathbb{C}^{L+1}$ and $|w_i| = 1$ for $1 \leq i \leq L+1$ and o_it = 0;
repeat
  Fix $\boldsymbol{W}$ and solve (P2) for optimal (P_A^*, P_B^*) ;
  Initialize in_it = 0;
  repeat
    Fix (P_A, P_B) and solve (P3) for optimal $\boldsymbol{W}^*$;
    Set $\hat{\boldsymbol{W}} = \boldsymbol{W}^*$;
    Update in_it = in_it+1
  until *fractional increase in* (4) $< \epsilon_i$ *or* in_it $\geq I_i$;
  Set $\boldsymbol{W} = \hat{\boldsymbol{W}}$;
  Update o_it = o_it+1;
until *fractional increase in* (4) $< \epsilon_o$ *or* o_it $\geq I_o$;
$\hat{\boldsymbol{w}}^* \leftarrow$ RankOne($\boldsymbol{W}$);
$w^{*(i)} \leftarrow \exp\left(j\angle\left(\frac{\hat{w}^{*(i)}}{\hat{w}^{*(L+1)}}\right)\right), \forall\, 1 \leq i \leq L+1$;

C. Alternating Optimization Algorithm

By combining the transmit power and the IRS phase shift optimization procedures introduced in section III-A and section III-B, we solve the problem as an alternating optimization problem. It is important to note that we have previously relaxed the rank-one constraint on $\boldsymbol{W}$. Thus, after finding $\boldsymbol{W}$ from the alternating optimization algorithm, we adopt Gaussian randomization and obtain a rank-one approximation $\hat{\boldsymbol{w}}$. The elements of $\boldsymbol{w}$ are then found using $w^{(i)} = \exp\left(j\angle\left(\frac{\hat{w}^{(i)}}{\hat{w}^{(L+1)}}\right)\right), \forall\, 1 \leq i \leq L+1$, where $\angle(x)$ denotes the phase of complex number x [3], [7]. These ideas are formally presented through Algorithm 1.

As we have shown for transmit powers, it can be shown that the value of (4) increases after an iteration of optimizing the IRS phase shifts. Consider a particular iteration. Let $\boldsymbol{W}_b$ and $\boldsymbol{W}_a$ be the values of $\boldsymbol{W}$ before and after solving (P3), respectively. We have $G(\boldsymbol{W}_b, P_A, P_B) =_{(a)}$

$G_{\boldsymbol{W}_b}(\boldsymbol{W}_b, P_A, P_B) \leq_{(b)} G_{\boldsymbol{W}_b}(\boldsymbol{W}_a, P_A, P_B) \leq_{(c)} G(\boldsymbol{W}_a, P_A, P_B)$, where (a) follows from the first-order approximation at $\boldsymbol{W}_b$, (b) follows from $\boldsymbol{W}_a$ being an updated solution to (P3), and (c) results from (6) being a lower bound to (4). Since $G(\boldsymbol{W}, P_A, P_B)$ is bounded from above for a given channel initialization, we can claim that both the inner and the outer iterations of Algorithm 1 converge.

With regards to the computational complexity of the algorithm, it is not difficult to see that the complexity of an inner iteration of Algorithm 1 mainly depends on solving problem (P3), which is known to be $\mathcal{O}(L^6)$. Moreover, the complexity of Gaussian randomization is $\mathcal{O}(L^3 N_S)$, where N_S is the generated number of Gaussian random vectors. Hence, the worst case computational complexity of Algorithm 1 is given by $\mathcal{O}(I_o I_i L^6 + L^3 N_S)$.

D. Extension to Individual Maximum Power Constraints

To represent individual power constraints, (3c) in (P1) should be replaced with the two constraints, $P_A \leq P_A^{\max}$ and $P_B \leq P_B^{\max}$, where $P_A^{\max}$ and $P_B^{\max}$ are the maximum transmit power levels at Alice and Bob, respectively. We employ the steps of Algorithm 1 with only the power optimization problem modified. Let the modified power optimization problem be (P4). Observe that the feasibility region of (P4) is now a rectangle. Thus, due to the properties of the objective function (5a) of (P2) mentioned in Section III-A, it suffices to consider only the four vertices of the feasible region, and simply pick the point which maximizes (5a). Note that when $P_A^{\max} + P_B^{\max} = P^{\max}$, the feasible set of (P4) will be a subset of the feasible set of (P2). Hence, from the network point of view, using a sum power constraint is more favorable.

IV. Numerical Results

In this section, we present the numerical results obtained through the proposed algorithm and compare the achievable performance with four baseline schemes. We consider two configurations, one where Charlie is close to the IRS (C1), and another in which Charlie is close to Bob (C2). The positions of Alice and Bob are fixed at $(-30, 0, 0)$ and $(40, 0, 0)$ in the three dimensional Euclidean space. The IRS is a rectangular array with 5 rows and $L/5$ columns. The center of the IRS is at $(0, 10, 0)$. The coordinates of Charlie for the two configurations are taken as $(0, 0, 0)$ and $(32, 2, 0)$, respectively. We consider four different schemes for each configuration. Scheme S: $(\boldsymbol{w}^*, \boldsymbol{P}^*)$ refers to Algorithm 1, and S: $(\boldsymbol{w}^*, \boldsymbol{P}^{\text{box}})$ is the scheme which is described in section III-D. In scheme S: $(\boldsymbol{w}, \boldsymbol{P}^*)$, the IRS phase shifts are set randomly and the transmit powers are optimized by solving (P2), while scheme S: (No-IRS, $\boldsymbol{P}^*$) represents a system without an IRS, where the power is optimized by solving (P2). Furthermore, for small L, we also consider the scheme S:(ES, $\boldsymbol{P}^*$), where exhaustive search is used to find the optimal IRS phase shifts.

For the numerical results, it is assumed that channels between Alice, Bob, and Charlie follow Rician fading while the user-IRS channels follow Rayleigh fading. A general model for the channel coefficient $\tilde{h}_{ij}$ between entities i and j can be given as $\tilde{h}_{ij} = \sqrt{L_0 d_{ij}^{-c_{ij}}}\left(\sqrt{\frac{\beta_{ij}}{1+\beta_{ij}}} g_{ij}^{LoS} + \sqrt{\frac{1}{1+\beta_{ij}}} g_{ij}^{NLoS}\right)$, where g_{ij}^{LoS} and g_{ij}^{NLoS} denote the line of sight (LoS) and the non-LoS components of the channel, L_0 is the path loss at a reference distance of 1m, and β_{ij}, d_{ij} and c_{ij} denote the Rician factor, distance, and the path loss exponent for the channel between i and j, respectively [7]. All channel coefficients are assumed to be independently distributed. We let $c_{ij} = 2$, and $\beta_{ij} = 0$ for user-IRS channels, $c_{ij} = 3$, and $\beta_{ij} = 8$ for the channels between users, and $L_0 = -30$ dB. We set $\sigma_A^2 = \sigma_B^2 = \sigma_C^2 = -105$ dBm, $\sigma_{l_A}^2 = \sigma_{l_B}^2 = -100$ dBm, $P_A^{\min} = P_B^{\min} = 0$ dBm and $P^{\max} = 15$ dBm. For S: $(\boldsymbol{w}^*, \boldsymbol{P}^{\text{box}})$, $P_A^{\max}$ and $P_B^{\max}$ are set $0.5P^{\max}$. Both ϵ_o and ϵ_i are set to 10^{-3} and the value of ξ can be chosen to achieve faster convergence. In fact, the algorithm is guaranteed to converge irrespective of the value of ξ, but setting it too small or large may lead to slow convergence. We used ξ to be 2. I_i is set to 6 and I_o is set to 10.

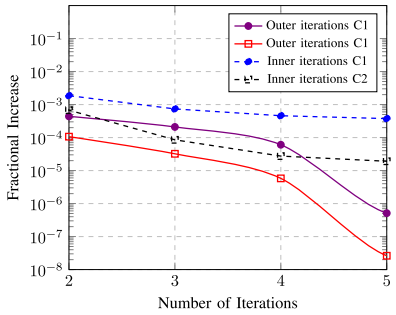

Fig. 2. Average fractional increase of (4) vs no. of outer/inner iterations of Algorithm 1 for $L = 20$.

TABLE I

S: $(\boldsymbol{w}^*, \boldsymbol{P}^*)$ VS S:(ES, $\boldsymbol{P}^*$) FOR C1 AND C2

L	C1		C2	
	S:$(\boldsymbol{w}^*, \boldsymbol{P}^*)$	S:(ES, $\boldsymbol{P}^*$)	S:$(\boldsymbol{w}^*, \boldsymbol{P}^*)$	S:(ES, $\boldsymbol{P}^*$)
1	2.417026	2.417026	0.091384	0.091384
2	2.487426	2.487426	0.097806	0.097806
3	2.550649	2.550650	0.103917	0.103917
4	2.616444	2.616449	0.110251	0.110251
5	2.682116	2.682121	0.118121	0.118121

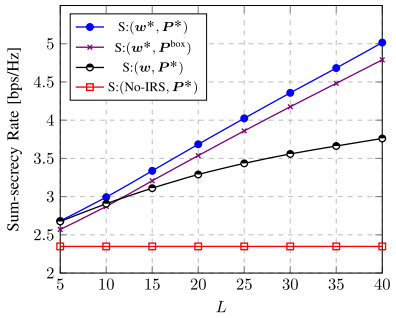

Fig. 3. Sum-secrecy rate vs the number of IRS elements for C1.

Fig. 2 shows the average fractional increase in (4), which we use to decide on the convergence, against the number of outer and inner iterations of Algorithm 1. Observe that, on average, an outer iteration converges within 3 inner iterations and the algorithm converges within 3 outer iterations for the considered parameter values.

Next, the performance of Algorithm 1 is compared with S:(ES, $\boldsymbol{P}^*$) for smaller values of L. The results, which are shown in Table I, depict a close match between two schemes. The behavior of the sum-secrecy rate with the number of IRS elements considering the two configurations is illustrated in Fig. 3 and Fig. 4. Firstly, we can observe Algorithm 1

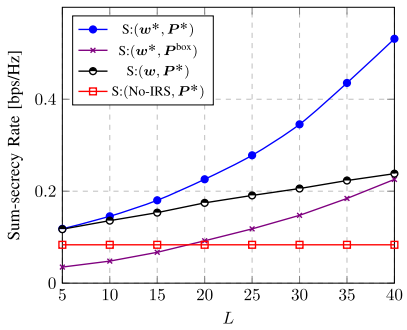

Fig. 4. Sum-secrecy rate vs the number of IRS elements for C2.

resulting in considerable gains of the sum-secrecy rate, clearly highlighting the importance of the optimization problem of interest. We observe a gain of approximately 35% through the proposed scheme relative to S: $(\boldsymbol{w}, P^*)$ for $L = 40$ in C1, whereas the respective gain is approximately 120% in C2.

When comparing C1 and C2, it can be seen that allocating more power leads to higher information leakage to Charlie in C2. Hence, Bob uses the minimum transmit power, $P_B^{\min}$. Note that Bob refrains from transmission if $P_B^{\min} = 0$. On the other hand, the leakage is not a major concern in C1, and the sum-secrecy rate increases with transmit power at the two legitimate users. Thus, the power allocated at both Bob and Alice is close to $0.5P^{\max}$. Also, it can be observed that the sum-secrecy rate achieved for the proposed scheme is lower for C2 compared to C1. The effectiveness of the IRS diminishes as the intruder tends towards a user. Charlie being close to Bob makes it prohibitively difficult for the IRS to provide a good information rate for Bob while simultaneously reducing the information leakage to Charlie, which leads to the aforementioned disparity.

Sum-secrecy rate vs L curves exhibit different trends with the proposed scheme for C1 and C2. As discussed earlier, the effectiveness of the IRS is lower for C2. Small values of L further reduce the degrees of freedom of the IRS, and prohibits the system from achieving non-zero sum-secrecy rates for most channel realizations in that configuration. Increasing L ameliorates this issue, thus we observe the trend in Fig. 4. On the other hand, zero sum-secrecy rate is rare in C1, even when L is small, thus the sum-secrecy grows at a steady rate. Observe that, S: $(\boldsymbol{w}^*, P^*)$ attains better sum-secrecy rates compared to S: $(\boldsymbol{w}^*, P^{\text{box}})$, proving the fact mentioned in section III-D. In C1, the gain of S: $(\boldsymbol{w}^*, P^*)$ with respect to S: $(\boldsymbol{w}^*, P^{\text{box}})$ is less since the transmit power of the two users approach $\frac{1}{2}P^{\max}$ for both S: $(\boldsymbol{w}^*, P^*)$ and S: $(\boldsymbol{w}^*, P^{\text{box}})$. However, in C2, the power allocated at Alice's end is close to $P^{\max} - P_B^{\min}$ for S: $(\boldsymbol{w}^*, P^*)$, which is not attainable in S: $(\boldsymbol{w}^*, P^{\text{box}})$. This is well depicted by the high gain of S: $(\boldsymbol{w}^*, P^*)$ with respect to S: $(\boldsymbol{w}^*, P^{\text{box}})$ in C2. Scheme S: $(\boldsymbol{w}, P^*)$ performs reasonably well for small L, but as expected, the performance gap with S: $(\boldsymbol{w}^*, P^*)$ increases for large L.

V. Conclusion

This letter introduced an iterative algorithm to maximize the sum-secrecy rate of an IRS-aided two-way communication system by adjusting the user transmit powers and the IRS phase shifts. The convergence of the algorithm was proved analytically and fast convergence was illustrated numerically. The achievable sum-secrecy rate of the algorithm was compared with four baseline schemes and the performance gains were quantified. Maximizing secrecy fairness between users, multi-antenna systems and multi-user networks are possible future extensions of the work presented in this letter.

References

[1] 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.

[2] C. Huang *et al.*, "Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 118–125, Oct. 2020.

[3] 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.

[4] 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.

[5] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. D. Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12296–12300, Oct. 2020.

[6] 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.

[7] 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.

[8] W. Jiang, Y. Zhang, J. Wu, W. Feng, and Y. Jin, "Intelligent reflecting surface assisted secure wireless communications with multiple-transmit and multiple-receive antennas," *IEEE Access*, vol. 8, pp. 86659–86673, May 2020.

[9] B. Feng, Y. Wu, M. Zheng, X.-G. Xia, Y. Wang, and C. Xiao, "Large intelligent surface aided physical layer security transmission," *IEEE Trans. Signal Process.*, vol. 68, pp. 5276–5291, Sep. 2020.

[10] 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, Sep. 2019.

[11] 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.

[12] P. Dharmawansa, S. Atapattu, and M. D. Renzo, "Performance analysis of a two–tile reconfigurable intelligent surface assisted 2×2 MIMO system," *IEEE Wireless Commun. Lett.*, vol. 10, no. 3, pp. 493–497, Mar. 2021.

[13] P. Xu, G. Chen, G. Pan, and M. D. Renzo, "Ergodic secrecy rate of RIS-assisted communication systems in the presence of discrete phase shifts and multiple eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 10, no. 3, pp. 629–633, Mar. 2021.

[14] G. C. Alexandropoulos, K. Katsanos, M. Wen, and D. B. D. Costa, "Safeguarding MIMO communications with reconfigurable metasurfaces and artificial noise," 2020, *arXiv:2005.10062*. [Online]. Available: http://arxiv.org/abs/2005.10062

[15] V. P. Tuan and I. P. Hong, "Secrecy performance analysis and optimization of intelligent reflecting surface-aided indoor wireless communications," *IEEE Access*, vol. 8, pp. 109440–109452, Jun. 2020.

[16] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.

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

[18] S. Atapattu, T. A. Tsiftsis, R. Fan, P. Dharmawansa, G. Wang, and J. Evans, "Reconfigurable intelligent surface assisted two–way communications: Performance analysis and optimization," *IEEE Trans. Commun.*, vol. 68, no. 10, pp. 6552–6567, Oct. 2020.

[19] L. Lv, Q. Wu, Z. Li, N. Al-Dhahir, and J. Chen, "Secure two-way communications via intelligent reflecting surfaces," *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 744–748, Mar. 2021.

[20] 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.