IJICTR
International Journal of Information & Communication Technology Research

Volume 17- Number 1 – 2025 (13-20)

# Securing RIS-aided Wireless Networks Against Full Duplex Active Eavesdropping

**Atefeh Zakeri**
Department of Electrical Engineering
Iran University of Science and Technology (IUST)
Tehran, Iran
azakeri@iust.ac.ir

**S.Mohammad Razavizadeh***
Department of Electrical Engineering
Iran University of Science and Technology (IUST)
Tehran, Iran
smrazavi@iust.ac.ir

Received: 26 June 2024 – Revised: 17 August 2024 - Accepted: 8 September 2024

*Abstract*—**This paper investigates the physical layer security of a wireless network assisted by a Reconfigurable Intelligent Surface (RIS) in the presence of full-duplex active eavesdropping. In this scenario, the RIS cooperates with the Base Station (BS) to transfer information to the intended user while an active attacker attempts to intercept the information through a wiretap channel. In addition, the attacker sends jamming signals to obstruct with the legitimate user's signal reception and increase the eavesdropping rate. Our objective is to maximize the secrecy rate by jointly optimizing the active and passive beamformers at the BS and RIS, respectively. To solve the resulting non-convex optimization problem, we propose a solution that decomposes it into two disjoint beamforming design sub-problems solved iteratively using Alternating Optimization (AO) techniques. Numerical analysis is conducted to evaluate the effects of varying the number of active attacking antennas and elements of the RIS on the secrecy performance of the considered systems under the presence of jamming signals sent by the attacker. The results demonstrate the importance of considering the impact of jamming signals on physical layer security in RIS-aided wireless networks. Overall, our work contributes to the growing body of literature on RIS-aided wireless networks and highlights the need to address the effects of jamming and active eavesdropping signals in such systems.**

**Keywords:** Secrecy rate maximization, Reconfigurable Intelligent Surface (RIS), Active eavesdropping, Full-duplex communications, Beamforming design.

**Article type:** Research Article


Publisher: ICT Research Institute

## I. INTRODUCTION

Ensuring security is crucial in 5G and 6G wireless communication networks, as wireless networks have become an essential part of our everyday life for exchanging data and communicating with ease. However, malicious activities such as eavesdropping and jamming attacks can compromise the secrecy and integrity of wireless communications [1]. The use of encryption algorithms is a common method to ensure security in wireless networks, but due to the rapid development of technology and computing power, physical layer security checks have been introduced as a supplement to conventional methods. This approach

* Corresponding Author

can evaluate the security performance of wireless networks using parameters like the secrecy rate, which indicates the maximum effective rate that can be delivered effectively. Passive eavesdropping attacks involve intercepting signals without transmitting any of their own, while active eavesdropping attacks send disruptive signals to interfere with legitimate transmissions. An active attack whose sole purpose is to cause interference is known as a jamming attack [2], [3].

Reflective Intelligent Surfaces (RIS) are a fundamental technology that can improve performance of wireless communications and increase system transmission rates by adjusting reflection coefficients. RIS comprises a flat surface that consists of numerous reflective elements, each capable of inducing independent amplitude or phase shifts to the propagated signal [4], [5]. RIS has important applications in new wireless networks as it offers various benefits including reduced interference, better coverage, and improved energy efficiency. Additionally, RIS can be used in conjunction with existing wireless systems, making it a viable option for improving the security and efficiency of both current and future wireless networks[6].

The use of RIS for enhancing physical layer security has been extensively examined in literature. For instance, [7] investigated the maximization of coverage rate between the transmitter and the receiver in the presence of an attacker when RIS is present. References [8], [9] investigate how RIS can improve physical layer security in wireless communications against multi-antenna eavesdroppers. An effective algorithm was introduced to jointly optimize active and passive beamforming. A secure wireless communication system was proposed in reference [10] that utilizes Multi-Input Multi-Output (MIMO) based on RIS. Multiple antennas are used by the Base Station (BS) to communicate with a legitimate multi-antenna user while protecting against multi-antenna passive eavesdroppers. The design of the transfer covariance matrix to maximize the secrecy rate was proposed using an alternating optimization algorithm that combines the Taylor series expansion method and predicted gradient ascent method. Authors in [11] analyzed the influence of RIS on secure wireless transmission, whereby an RIS is implemented to aid the secure MIMO system to improve privacy performance. Artificial Noise (AN) is employed to mislead the passive eavesdropper. Reference [12] investigated the advantage of using RIS in multi-user Multi-Input Single-Output (MISO) systems when passive eavesdroppers are present. They showed that the secrecy rate could be maximized by co-designing secure beamforming, AN, and RIS phase shift. An iterative optimization method was suggested to deal with the formulated non-convex problem. Reference [13] proposed a RIS-assisted anti-jamming strategy for wireless communication security. Their goal was to increase the system's rate when a clever jammer was present, which aims to deteriorate the quality of the intended communications by jamming the signal on the channels used by legitimate users. A backscatter communication system that uses RIS was considered by reference [14] to prevent jamming attacks. Here, the attacker tries to jam the signal in order to keep the legitimate user from getting the desired signal. In order to fend off the jamming attack, an RIS is placed close to the user and acts as a transmitter to transform all the received signals into the intended signal. The objective of this paper is to maximize the

Signal-to-Interference-plus-Noise Ratio (SINR) at the user, subject to power constraints at the source. In reference [15], an aerial RIS was proposed, whereby the impact of jamming attacks can be reduced by increasing the legal signal and transmission rate. Conversely, in reference [16], legal communication was attacked using RIS as a jammer, without the use of any internal energy to create jamming signals, which minimizes the received signal power in the legitimate receiver. To achieve secure transmission, RIS is used as a jamming device to create and broadcast jamming signals, thereby disturbing the reception of eavesdroppers, as shown in references [17], [18]. In reference [19], a co-jammer was introduced in the presence of RIS, who tries to mislead the eavesdroppers. This increases the secrecy rate and effective energy by jamming signal transmission.

Full-duplex communication is a promising technique that allows radio signals to be transmitted and received simultaneously on the same frequency. Consequently, in future wireless networks, it can greatly increase spectrum efficiency and decrease communication latency [20], [21]. In a communication system based on RIS, to improve performance, reference [22], [23] considered a Full-duplex legal receiver that sends the jamming signal to the receiver to mitigate the eavesdropper. This leads to the joint optimization of received beamforming, signal jamming, and passive beamforming, thereby seeking to increase the security rate.

As discussed above, in most of the previous papers on RIS-assisted networks, only passive or active attacks have been considered. Motivated by the need for improved wireless network security, in this paper, we focus on a more professional adversarial attack in which a full-duplex active attacker can act as an eavesdropper and a jammer at the same time. In particular, we investigate the secrecy rate maximization problem by optimizing the beamforming vector at the BS and phase matrix at the IRS. To solve the resulting non-convex optimization problem, we propose an alternating algorithm. Through computer simulations, we show the superiority of our proposed method. The paper presents several contributions, including:

- Investigating the security problem of the physical layer in a system based on RIS in the presence of a full-duplex active attacker who can act as an eavesdropper and jammer simultaneously.
- Including direct channel performance evaluation assuming low probability of disconnection between the BS and user, unlike many previous studies that ignore this aspect.
- Formulating a non-convex optimization problem for secrecy rate maximization by jointly optimizing beamforming and reflection coefficients for the RIS network. To solve the problem as two separate sub-problems, an alternative algorithm is suggested.

- Demonstrating through simulation results the significant impact of a jammer on secrecy rate and emphasizing the importance of RIS in improving it. The impact of changing the number of active attacking antennas is also analyzed, the number of active attacking antennas has increased, resulting in an increase in the secrecy rate.

The structure of the rest of this paper is as follows. In Section II, the system model is covered. Section III presents the formula for the problem, the secrecy rate that can be achieved, and the suggested algorithm for solving the optimization problem. Simulation results can be obtained in Section IV. Section V includes concluding remarks.

## II. SYSTEM MODEL

This paper focuses on a communication system that utilizes RIS, as depicted in Fig.1, where a base station that has $K$ antennas is used to serve a user with one antenna that an active eavesdropper (denoted as "eve") is present. The eavesdropper is equipped with $N_r$ receiving antennas and $N_t$ transmitting antennas, and is assumed to have perfect self-interference cancellation, as described in [24], [25]. By altering the phase of the signal received from the base station, the RIS, consisting of $L$ reflecting elements, and base station collaborate to deliver information to the user. However, the full-duplex active eavesdropper listens to the information through the wiretap channel and sends a jamming signal to the RIS and the user to disrupt the legitimate user's reception of the signal and decrease the secrecy rate.

The channel gains from BS to the RIS, BS to the user, BS to the active eavesdropper, RIS to the user, RIS to the active eavesdropper are denoted as $\mathbf{H}_{BI} \in \mathbb{C}^{L\times K}$, $\mathbf{h}_{Bu} \in \mathbb{C}^{K\times 1}$, $\mathbf{H}_{Be} \in \mathbb{C}^{N_r\times K}$, $\mathbf{h}_{Iu} \in \mathbb{C}^{L\times 1}$ and $\mathbf{H}_{Ie} \in \mathbb{C}^{N_r\times L}$ respectively. The channels that equivalent to the baseband from eavesdropper to RIS and eavesdropper to user are indicated by $\mathbf{G}_{eI} \in \mathbb{C}^{L\times N_t}$ and $\mathbf{g}_{eu} \in \mathbb{C}^{N_t\times 1}$. We make the assumption in this paper that the Channel State Information (CSI) of all the channels is fully known. This can be accomplished by techniques like local oscillator power leakage from the RF frontend of the eavesdropper receivers [26] or eavesdropper can also be an active user in the secure transmission system but not be trusted by user [8]. The signals that the eavesdropper and legitimate user received are given as

$$Y_u = \mathbf{h}_{Bu}^H \mathbf{w}s + \mathbf{g}_{eu}^H \mathbf{v}a + \mathbf{h}_{Iu}^H \boldsymbol{\theta}(\mathbf{H}_{BI}\mathbf{w}s + \mathbf{G}_{eI}\mathbf{v}a) + n_u \quad (1)$$

$$Y_e = \mathbf{H}_{Be}\mathbf{w}s + \mathbf{H}_{Ie}\boldsymbol{\theta}(\mathbf{H}_{BI}\mathbf{w}s + \mathbf{G}_{eI}\mathbf{v}a) + n_e \quad (2)$$

we denote $\theta = diag(B_1 e^{ja_1}, B_2 e^{ja_2}, \dots, B_L e^{ja_L})$ as the reflection coefficient matrix of the RIS. $a_l$ and $B_l$ with $l = [1,2,\dots,L]$ are the phase shift and amplitude at the $l$th RIS element. The signal transmitted from the BS is given by $\mathbf{x} = \mathbf{w}s$, where $\mathbf{w}$ and $s \sim CN(0,1)$ denote beamforming vector and information bearing for user, respectively. Additionally, The jamming signal $a$ is transmitted by means of vector $\mathbf{v}$, which represents the beamforming vector at the eavesdropper. The additive white gaussian noise (AWGN) associated with the user and the eavesdropper is $n_u$ and $n_e \sim CN(0,\sigma^2)$. The rates that can be attained at the active eavesdropper and the legitimate user are provided by

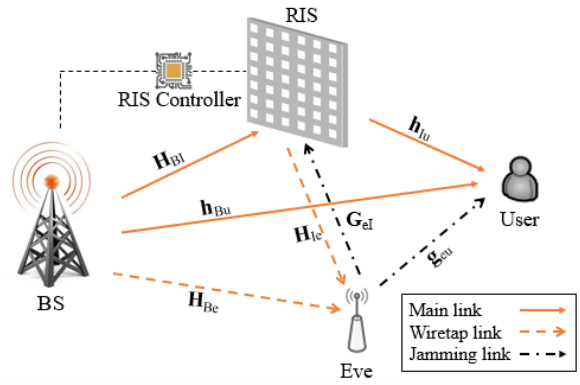


Figure 1. System Model of the RIS-assisted Communication Network Against an Active Eavesdropper

$$R_u = log\left(1 \frac{|(\mathbf{h}_{Bu}^H + \mathbf{h}_{Iu}^H \theta \mathbf{H}_{BI})\mathbf{w}|^2}{|(\mathbf{g}_{eu}^H + \mathbf{h}_{Iu}^H \theta \mathbf{G}_{eI})\mathbf{v}|^2 + \sigma_u^2}\right) \quad (3)$$

$$R_e = log\left(1 + \frac{\|(\mathbf{H}_{Be} + \mathbf{H}_{Ie}\theta\mathbf{H}_{BI})\mathbf{w}\|^2}{\|(\mathbf{H}_{Ie}\theta\mathbf{G}_{eI})\mathbf{v}\|^2 + \sigma_e^2}\right) \quad (4)$$

Consequently, the attainable secrecy rate can be expressed as

$$R_s = [R_u - R_e]^+ \quad (5)$$

Since the cases with a non-positive secrecy rate lack meaning in the context of this study, $[z]^+ = max(z,0)$, for the discussions henceforth we delete the $[.]^+$ operation [27].

## III. BEAMFORMING DESIGN

This study aims to maximize the secrecy rate by jointly optimizing the transmit beamforming vector $\mathbf{w}$ at the BS and the phase shifts $\boldsymbol{\theta}$ at the RIS, building on the discussion above. This problem can be expressed as

$$\max_{w,\theta} \quad R_s \quad (6a)$$

$$s.t. \quad \| \mathbf{w} \|_2 \leq P_{BS} \quad (6b)$$

$$|\theta_l| = 1, \quad l \in [1,2,\dots,L] \quad (6c)$$

Evidently, this is a Non-deterministic Polynomial-time hard (NP-hard) problem due to the unit modulus constraints and non-convex objective function. The optimal solution cannot be found directly by utilizing existing algorithms. This study proposes a low-complexity AO-based algorithm in order to address this challenge. In this way, we turn the optimization problem into two separate sub-problems and examine each of the created sub-problems separately. In the following, a method to solve these sub-problems will be discussed.

### *A. Active Beamforming*

First, we assume that the parameter $\theta$ are fixed and derive the optimal value of $\mathbf{w}$. Therefore, it is

necessary to rewrite problem (6)'s objective function.

$$\max_{w} \quad R_s \tag{7a}$$

$$s.t. \quad \| \mathbf{w} \|_2 \leq P_{BS} \tag{7b}$$

This problem has a non-convex objective function. By defining $\mathbf{W} = \mathbf{w}\mathbf{w}^H$ and $\mathbf{V} = \mathbf{v}\mathbf{v}^H$, the terms within the rate have been rearranged in order to streamline the discussions

$$R_u = log(I + (\mathbf{H}_{Bu}\mathbf{W}\mathbf{H}_{Bu}^H)(I + \mathbf{G}_{eu}\mathbf{V}\mathbf{G}_{eu}^H)^{-1}) \tag{8}$$

$$R_e = log(I + (\mathbf{H}_{BeI}\mathbf{W}\mathbf{H}_{BeI}^H)(I + \mathbf{H}_{IeI}\mathbf{V}\mathbf{H}_{IeI}^H)^{-1}) \tag{9}$$

Where $\mathbf{H}_{Bu} = \frac{1}{\sigma_u}(\mathbf{h}_{Bu}^H + \mathbf{h}_{Iu}^H\theta\mathbf{H}_{BI}), \mathbf{G}_{eu} = \frac{1}{\sigma_u}(\mathbf{g}_{eu}^H + \mathbf{h}_{Iu}^H\theta\mathbf{G}_{eI})$, $\mathbf{H}_{BeI} = \frac{1}{\sigma_e}(\mathbf{H}_{Be} + \mathbf{H}_{Ie}\theta\mathbf{H}_{BI})$ and $\mathbf{H}_{Bu} = \frac{1}{\sigma_e}(\mathbf{H}_{Ie}\theta\mathbf{G}_{eI})$. The following problem is a result of transforming problem (7).

$$\max_{\mathbf{w}} \quad \underbrace{log(1 + (\mathbf{H}_{Bu}\mathbf{w}\mathbf{w}^H\mathbf{H}_{Bu}^H)(1 + \mathbf{G}_{eu}\mathbf{v}\mathbf{v}^H\mathbf{G}_{eu}^H)^{-1})}_{A_1}$$

$$+ \underbrace{\log(\mathbf{H}_{IeI}\mathbf{v}\mathbf{v}^H\mathbf{H}_{IeI}^H)}_{A_2} \quad - \tag{10a}$$

$$\underbrace{log((\mathbf{H}_{IeI}\mathbf{v}\mathbf{v}^H\mathbf{H}_{IeI}^H) + (\mathbf{H}_{BeI}\mathbf{w}\mathbf{w}^H\mathbf{H}_{BeI}^H))}_{A_3}$$

$$s.t. \quad \| \mathbf{w} \|_2 \leq P_{BS} \tag{10b}$$

Problem (10) is still non-convex and intractable. Therefore, the objective function is converted into an equivalent counterpart by using the Weighted Minimum Mean Square Error (WMMSE) idea to manipulate alliteratively using the BCD technique[28]. The first step in our process is to introduce the auxiliary matrices $(\varepsilon_i, (i \in 1,2,3), x_j, (j \in 1,2))$, which we use to reformulate $A_1, A_2$ and $A_3$ in the problem's objective function, respectively. The Mean Square Error (MSE) matrix function of $A_1$ should be considered as follows:

$$E_1(x_1, w) = (I - x_1^H\mathbf{H}_{Bu}\mathbf{w})(I - x_1^H\mathbf{H}_{Bu}\mathbf{w})^H + x_1^H(I + \mathbf{G}_{eu}\mathbf{v}\mathbf{v}_H\mathbf{G}_{eu})x_1 \tag{11}$$

Similarly, $A_2$ is given by

$$E_2(x_2, w) = (I - x_2^H\mathbf{H}_{IeI}\mathbf{v})(I - x_2^H\mathbf{H}_{IeI}\mathbf{v})^H + x_2^H x_2 \tag{12}$$

The following lemma is necessary to solve this problem.

*Lemma* 1: [29] Denoting $\mathbf{E} \in \mathbb{C}^{d\times d}$ as any positive definite matrix, we obtain the following function

$$-log(\mathbf{E}) = \max_{S\in\mathbb{C}^{d\times d}, S\geq 0} \quad \delta(S) \tag{13}$$

Where $\delta(S) = -Tr(SE) + log|S| + N$, the optimal solution for problem (13) is known as $S^{opt} = E^{-1}$. Based on *Lemma*1, we can obtain the following equalities,

$$A_1 = \max_{\varepsilon_1>0, x_1} \quad log(\varepsilon_1) - Tr[\varepsilon_1(E_1(x_1, \mathbf{w}))] \tag{14}$$

$$A_2 = \max_{\varepsilon_2>0, x_2} \quad log(\varepsilon_2) - Tr[\varepsilon_2(E_2(x_2, \mathbf{w}))] \tag{15}$$

$$A_3 = \max_{\varepsilon_3>0} \quad log(\varepsilon_3) - Tr[\varepsilon_3((\mathbf{H}_{IeI}\mathbf{v}\mathbf{v}^H\mathbf{H}_{IeI}^H)(\mathbf{H}_{BeI}\mathbf{w}\mathbf{w}^H\mathbf{H}_{BeI}^H))] \tag{16}$$

We substitute the formulas above into problem (10), which has been rewritten as

$$\max_{\Omega} \quad \log(\varepsilon_1) - Tr[\varepsilon_1\big((I - x_1^H\mathbf{H}_{Bu}\mathbf{w})(I - x_1^H\mathbf{H}_{Bu}\mathbf{w})^H + x_1^H(I + \mathbf{G}_{eu}\mathbf{v}\mathbf{v}^H\mathbf{G}_{eu}^H)x_1\big)] + \log(\varepsilon_2)) \quad -Tr[\varepsilon_2\big((I - x_2^H\mathbf{H}_{IeI}\mathbf{v})(I - x_2^H\mathbf{H}_{IeI}\mathbf{v})^H + x_2^H x_2\big)] + \log(\varepsilon_3) \quad -Tr\big[\varepsilon_3\big((\mathbf{H}_{IeI}\mathbf{v}\mathbf{v}^H\mathbf{H}_{IeI}^H) + (\mathbf{H}_{BeI}\mathbf{w}\mathbf{w}^H\mathbf{H}_{BeI}^H)\big)\big] \tag{17a}$$

$$s.t. \quad \| \mathbf{w} \|^2 \leq P_{BS} \tag{17b}$$

$$\Omega = \{\varepsilon_1, \varepsilon_2, \varepsilon_3 > 0, \ x_1, x_2, \ \mathbf{w}\} \tag{17c}$$

Then, we use the BCD algorithm and to separate problem (17) into three sub-problem. In the sequel, We first solve problem (17) to optimize $x_1, x_2$, given $\mathbf{w}$ and $\varepsilon_1, \varepsilon_2, \varepsilon_3$.

$$x_1 = \operatorname{argmin}_{x_1} \quad Tr[\varepsilon_1 E_1(x_1, \mathbf{w})] \tag{18}$$

$$x_2 = \operatorname{argmin}_{x_2} \quad Tr[\varepsilon_2 E_2(x_2, \mathbf{w})] \tag{19}$$

In order to solve problems above, we consider their respective first-order derivatives, and the closed-form solution of $x_1$ and $x_2$ is given by

$$x_1 = (I + \mathbf{G}_{eu}\mathbf{v}\mathbf{v}^H\mathbf{G}_{eu}^H + \mathbf{H}_{Bu}\mathbf{w}\mathbf{w}^H\mathbf{H}_{Bu}^H)^{-1}\mathbf{H}_{Bu}\mathbf{w} \tag{20}$$

$$x_2 = (I + \mathbf{H}_{IeI}\mathbf{v}\mathbf{v}^H\mathbf{H}_{IeI}^H)^{-1}\mathbf{H}_{IeI}\mathbf{v} \tag{21}$$

In the next step, the goal of solving problem (17) is to optimize $\varepsilon_1, \varepsilon_2, \varepsilon_3$, based on $x_1, x_2$ and $\mathbf{w}$. It has been observed that the objective function of problem (17) is independent of the matrices $\varepsilon_1, \varepsilon_2, \varepsilon_3$. By employing *Lemma*1, the closed-form solutions of $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are driven as

$$\varepsilon_1 = [(I - x_1^H\mathbf{H}_{Bu}\mathbf{w})(I - x_1^H\mathbf{H}_{Bu}\mathbf{w})^H + x_1^H(I + \mathbf{G}_{eu}\mathbf{v}\mathbf{v}^H\mathbf{G}_{eu}^H)x_1]^{-1} \tag{22}$$

$$\varepsilon_2 = [(I - x_2^H\mathbf{H}_{IeI}\mathbf{v})(I - x_2^H\mathbf{H}_{IeI}\mathbf{v})^H + x_2^H x_2]^{-1} \tag{23}$$

$$\varepsilon_3 = [I + \mathbf{H}_{IeI}\mathbf{v}\mathbf{v}^H\mathbf{H}_{IeI}^H + \mathbf{H}_{BeI}\mathbf{w}\mathbf{w}^H\mathbf{H}_{BeI}^H]^{-1} \tag{24}$$

Next, problem (17) is solved to design $\mathbf{w}$ optimally, given $x_1, x_2$ and $\varepsilon_1, \varepsilon_2, \varepsilon_3$. In order to continue, problem (17) should be rewritten in terms of $\mathbf{w}$, as

$$\min_{w} \quad -\log(\varepsilon_1) + Tr[\varepsilon_1((I - x_1^H\mathbf{H}_{Bu}\mathbf{w})(I - x_1^H\mathbf{H}_{Bu}\mathbf{w})^H + x_1^H(I + \mathbf{G}_{eu}\mathbf{v}\mathbf{v}^H\mathbf{G}_{eu}^H)x_1)] - log(\varepsilon_2) \quad +Tr[\varepsilon_2((I - x_2^H\mathbf{H}_{IeI}\mathbf{v})(I - x_2^H\mathbf{H}_{IeI}\mathbf{v})^H + x_2^H x_2)] \quad -log(\varepsilon_3) \quad +Tr[\varepsilon_3((\mathbf{H}_{IeI}\mathbf{v}\mathbf{v}^H\mathbf{H}_{IeI}^H) + (\mathbf{H}_{BeI}\mathbf{w}\mathbf{w}^H\mathbf{H}_{BeI}^H))] \tag{25a}$$

$$s.t. \quad \| \mathbf{w} \|^2 \leq P_{BS} \tag{25b}$$

Here we are looking for $\mathbf{w}$, so we assume other values to be constant and ignore them. After simplification, we reach the following final problem:

$$\min_{w} \quad Tr(\varepsilon_1 x_1^H \mathbf{H}_{Bu}\mathbf{w}\mathbf{w}^H\mathbf{H}_{Bu}^H x_1) - Tr(\varepsilon_1 x_1^H \mathbf{H}_{Bu}\mathbf{w}) - Tr(\varepsilon_1 \mathbf{w}^H\mathbf{H}_{Bu}^H x_1) + Tr(\varepsilon_3 \mathbf{H}_{BeI}\mathbf{w}\mathbf{w}^H\mathbf{H}_{BeI}^H) \quad (26a)$$

$$s.t. \quad \| \mathbf{w} \|^2 \leq P_{BS} \quad (26b)$$

In MATLAB, CVX toolbox can solve the objective function of the equivalent main problem, which is a linear and convex function.

*A. Passive Beamforming*

In this subsection, the passive beamforming at the RIS is designed while the transmit beamforming at the BS is fixed. To this end, problem (6) is reformulated. Therefore, the sub-problem will be

$$\max_{\theta} \quad R_s \quad (27a)$$

$$s.t. \quad |\theta_l| = 1, \quad l \in [1,2,\dots,L] \quad (27b)$$

The objective and constraint functions of the problem (27) are non-convex. The transmission model's terms are rearranged to streamline the discussions.

$$(\mathbf{h}_{Bu}^H + \mathbf{h}_{Iu}^H\theta\mathbf{H}_{BI})\mathbf{w} = (\mathbf{h}_{Bu}^H\mathbf{w}) + \mathbf{h}_{Iu}^H diag(\varphi)\mathbf{H}_{BI}\mathbf{w} = \mathbf{h}_{Bu}^H + \mathbf{h}_{Iu}^H diag(\mathbf{H}_{BI}\mathbf{w})\varphi \quad (28a)$$

Then we consider changing the following variables.

$$[\mathbf{h}_{Bu}^H\mathbf{w}, \mathbf{h}_{Iu}^H diag(\mathbf{H}_{BI}\mathbf{w})] = \mathbf{H}_{BIu} \quad (29a)$$

$$[1, \varphi]^H = \varphi \quad (29b)$$

By applying these relations, we will be

$$\| (\mathbf{h}_{Bu}^H + \mathbf{h}_{Iu}^H\theta\mathbf{H}_{BI})\mathbf{w} \|^2 = \varphi^H\mathbf{H}_{BIu}^H\mathbf{H}_{BIu}\varphi = Tr(\mathbf{E}_{BID}\Theta) \quad (30)$$

Where $\Theta = \varphi \ \varphi^H$. Similarly, we have

$$[\mathbf{g}_{eu}^H\mathbf{v}, \mathbf{h}_{Iu}^H diag(\mathbf{G}_{eI}\mathbf{v})][1, \varphi]^H = \mathbf{G}_{eIu}\varphi \quad (31a)$$

$$\| (\mathbf{g}_{eu}^H + \mathbf{h}_{Iu}^H\theta\mathbf{G}_{eIu})\mathbf{v} \|^2 = \varphi^H\mathbf{G}_{eIu}^H\mathbf{G}_{eIu}\varphi = Tr(\mathbf{E}_{eIu}\Theta) \quad (31b)$$

$$[\mathbf{H}_{Be}\mathbf{w}, \mathbf{H}_{Ie} diag(\mathbf{H}_{Be}\mathbf{w})][1, \varphi]^H = \mathbf{H}_{BIe}\varphi \quad (32a)$$

$$\| (\mathbf{H}_{Be} + \mathbf{H}_{Ie}\theta\mathbf{H}_{BI})\mathbf{w} \|^2 = \varphi^H\mathbf{H}_{BIe}^H\mathbf{H}_{BIe}\varphi = Tr(\mathbf{E}_{BIe}\Theta) \quad (32b)$$

and finally

$$[0, \mathbf{H}_{Ie} diag(\mathbf{G}_{eI}\mathbf{v})][1, \varphi]^H = \mathbf{G}_{eIeI}\varphi \quad (33a)$$

$$\| (\mathbf{H}_{Ie}\theta\mathbf{G}_{eI})\mathbf{v} \|^2 = \varphi^H\mathbf{G}_{eIeI}^H\mathbf{G}_{eIeI}\varphi = Tr(\mathbf{E}_{eIeI}\Theta) \quad (33b)$$

The secrecy rate has been reinterpreted using the definitions above.

$$R_s = log\left(1 + \frac{Tr(\mathbf{E}_{BID}\Theta)}{Tr(\mathbf{E}_{eIu}\Theta)+\sigma_u^2}\right) - log\left(1 + \frac{Tr(\mathbf{E}_{BIe}\Theta)}{Tr(\mathbf{E}_{eIeI}\Theta)+\sigma_e^2}\right) = \log\left(Tr(\mathbf{E}_{eIu}\Theta) + \sigma_u^2 + Tr(\mathbf{E}_{BID}\Theta)\right) - log(Tr(\mathbf{E}_{eIeI}\Theta) + \sigma_e^2 + Tr(\mathbf{E}_{BIe}\Theta)) - log(Tr(\mathbf{E}_{eIu}\Theta) + \sigma_u^2) + log(Tr(\mathbf{E}_{eIeI}\Theta) + \sigma_e^2) \quad (34)$$

By introducing auxiliary variables $\varepsilon_4$ and $\varepsilon_5$, we can achieve the following equalities by applying the same method as in (14)

$$-log(Tr(\mathbf{E}_{eIeI}\Theta) + \sigma_e^2 + Tr(\mathbf{E}_{BIe}\Theta)) = \max_{\varepsilon_4>0}\{-\varepsilon_4\big(Tr(\mathbf{E}_{eIeI}\Theta) + \sigma_e^2 + Tr(\mathbf{E}_{BIe}\Theta)\big) + log(\varepsilon_4)\} \quad (35)$$

$$-\log\left(Tr(\mathbf{E}_{eIu}\Theta) + \sigma_u^2\right) = \max_{\varepsilon_5>0}\{-\varepsilon_5(Tr(\mathbf{E}_{eIu}\Theta) + \sigma_u^2)) + log(\varepsilon_5)\} \quad (36)$$

The optimization problem for secrecy rate has been restructured with the reformulations above.

$$\min_{\varepsilon_4,\varepsilon_5,\Theta} \quad R_s = -log(Tr(\mathbf{E}_{eIu}\Theta) + \sigma_u^2 + Tr(\mathbf{E}_{BIu}\Theta) + \sigma_u^2) + \varepsilon_4(Tr(\mathbf{E}_{eIeI}\Theta) + \sigma_e^2 + Tr(\mathbf{E}_{BIe}\Theta) + \sigma_e^2) - log(Tr(\mathbf{E}_{eIeI}\Theta) + \sigma_e^2) + \varepsilon_5(Tr(\mathbf{E}_{eIu}\Theta) + \sigma_u^2) - log(\varepsilon_4) - log(\varepsilon_5) \quad (37a)$$

$$s.t. \quad \varepsilon_4 > 0, \ \varepsilon_5 > 0 \quad (37b)$$

$$\Theta \geq 0, \quad rank(\Theta) = 1 \quad (37c)$$

$$\Theta_{l,l} = 1, \quad \forall l \in L \quad (37d)$$

For problem (37), the optimized $\varepsilon_4$ and $\varepsilon_5$ is obtained:

$$\varepsilon_4 = \frac{1}{Tr(\mathbf{E}_{eIeI}\Theta)+Tr(\mathbf{E}_{BIe}\Theta+\sigma_e^2)} \quad (38)$$

$$\varepsilon_5 = \frac{1}{Tr(\mathbf{E}_{eIu}\Theta)+\sigma_u^2} \quad (39)$$

We can use toolboxes like CVX to tackle the phase shift problem, ignoring the rank-1 requirement and turning to semi-definite relaxation. If the found optimal does not satisfy the rank-1 constraint, Gaussian randomization can be employed [22], [30].

*C. Algorithm Design*

At this point in the process, according to the two defined sub-problems, the general algorithm presented for solving the combined problem of RIS phase shift optimization and beamforming vectors is shown in Algorithm 1. The inputs of this algorithm are channel parameters and $\epsilon$, which is the maximum acceptable relative error for the minimum user security rate. In the $t$ th iteration of this algorithm, the active beamforming sub-problem is solved by using the values obtained in the previous iteration of the algorithm for the RIS phase shift in the passive beamforming sub-problem, and its answer is used as the required values to solve the passive beamforming sub-problem. This process continues until the relative error associated with the minimum security rate of the user is less than $\epsilon$.

Moreover, we evaluate the computational complexities of the proposed algorithm. Considering the computational complexity of the sub-problem related to the active beamforming, which is defined as $\mathcal{O}(K^2 + 2N_r^3)$ and the sub-problem related to the passive beamforming, while it reaches convergence in $T_1$ iteration, it is defined as $\mathcal{O}(T_1(L+1)^{4.5})$. Each iteration's main algorithm's computational complexity is equal to the sum of their complexity, i.e. $\mathcal{O}(((K^2 + 2N_r^3) + T_1(L+1)^{4.5})log(\epsilon))$. Now, assuming that the algorithm converges in $T_2$, the computational complexity of this algorithm is $\mathcal{O}(T_2(((K^2 + 2N_r^3) + T_1(L+1)^{4.5}))log(\epsilon))$.

**Algorithm1** alternating iterative algorithm for solving security rate

**Input**: channel parameters, $\epsilon$

1) **Initialization**: $t=0$, set $\mathbf{w}^t$, $\theta^t$.

2) **Repeat**

   **a)** Given $\theta^t$,$\mathbf{w}^t$ obtain $\varepsilon_{1,2,3}^{t+1}, x^{t+1}$

   **b)** Given $\theta^t, \varepsilon_{1,2,3}^{t+1}, x^{t+1}$ obtain $\mathbf{w}^{t+1}$

   **c)** Given $\theta^t, \varepsilon_{1,2,3}^{t+1}, x^{t+1}, \mathbf{w}^{t+1}$ obtain $\varepsilon_{4,5}^{t+1}$

   **d)** Given $\varepsilon_{1,2,3}^{t+1}, x^{t+1}, \mathbf{w}^{t+1}, \varepsilon_{4,5}^{t+1}$ obtain $\theta^{t+1}$

3) **Until** $\frac{|R_s^t - R_s^{t-1}|}{R_s^{t-1}} \le \epsilon$

**Output** Optimal transmit beamforming, passive beamforming.

## IV. Numerical Result

We provide numerical results in this part to assess the suggested system. We assume that a BS with K antennas is situated in the center of the polar coordinates in our simulations. Additionally, to help with signal transmissions, RIS with L reflecting components are put around the BS at permanent points. We suppose that the RIS is situated on a circle with a radius of 40 and an angle of $\frac{\pi}{4}$ that is centered at the BS. Also, the location of the user and the eavesdropper is $(30, \beta)$ and $(25, \beta)$, respectively, where $\beta = U[0, \frac{\pi}{2}]$. The noise variances are set as $\sigma_u = \sigma_e = -105dBm$. We assume $H = \sqrt{L_0 d^{-\varepsilon}} Q$ generates all of the channel coefficients involved, where the path loss at reference distance $d_0 = 1m$ is referred to as $L_0 = -30dB$, $d$ is the link distance, $\varepsilon$ signifies the exponent of the path loss. The corresponding path loss exponents is set as $\varepsilon_{Bu} = \varepsilon_{Be} = 3.75$ , $\varepsilon_{BI} = \varepsilon_{Iu} = \varepsilon_{Ie} = 2.2$, $\varepsilon_{eu} = \varepsilon_{eI} = 2.5$ and $Q$ is the Rician components is given by [27], [31]:

$$Q = \sqrt{\frac{k}{k+1}} Q^{LoS} + \sqrt{\frac{1}{1+k}} Q^{NLoS} \quad (40)$$

where $k = 1$ is the Rician factor, $Q^{LoS}$ is the deterministic Line of Sight (LoS), and the NLoS components $Q^{NLoS}$ are i.i.d. complex Gaussian distributed with zero mean and unit variance. The los component is given by

$$Q^{LoS} = a_{D_r}(\nu^{AoA}) a_{D_t}^H(\nu^{AoD}) \quad (41)$$

where $a_{D_r}(\nu^{AoA})$ and $a_{D_t}^H(\nu^{AoD})$ are defined as

$$a_{D_r}(\nu^{AoA}) = [1, e^{2\pi j \times \frac{d}{\lambda} \times sin\nu^{AoA}}, \dots, e^{2\pi j \times \frac{d}{\lambda} \times (D_r - 1) sin\nu^{AoA}}]^T \quad (42)$$

$$a_{D_t}(\nu^{AoD}) = [1, e^{2\pi j \times \frac{d}{\lambda} \times sin\nu^{AoD}}, \dots, e^{2\pi j \times \frac{d}{\lambda} \times (D_t - 1) sin\nu^{AoD}}]^T \quad (43)$$

Where $D_r$ and $D_t$ represent the numbers of antennas at the receiver and transmitter sides, respectively. The variable $d$ refers to the distance between the antennas, while $\lambda$ represents the wavelength, $\nu^{AoD}$ is the angle of departure and $\nu^{AoA}$ is the angle of arrival, Both of them are considered to be randomly distributed within $[0,2\pi]$. For simplicity, we set $\frac{d}{\lambda} = \frac{1}{2}$. The stopping threshold for the alternating optimization techniques is defined as $\epsilon = 10^{-3}$. The eavesdropper is a full duplex, but the without jamming scheme is used as a benchmark, where the Eve is deployed with Nr antennas to evaluate the impact of the eavesdropping. Furthermore, the scheme without RIS is also used as a benchmark, where only the beamformer w is optimize.

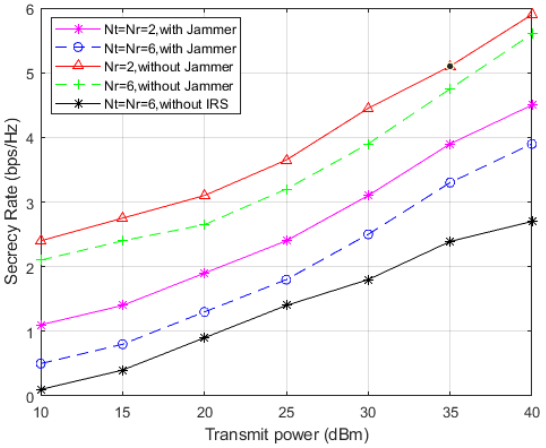


Figure 2. Achievable Secrecy Rate vs. the Transmit Power

The possible secrecy rate for both situations with and without a jammer is displayed against the transmit power of the BS in Fig.2. The number of antennas ($K$) and reflecting elements in RIS ($L$) are set to 3 and 36, respectively. As we can see, in every scenario, the secrecy rate rises as the BS's transmit power grows. This increase occurs because as the power of the BS increases, the effect of beamforming on the power received by the user also increases, leading to an increase in the signal-to-noise ratio (SNR) at the user end. Additionally, increasing the BS's transmit power also increases the power of the received signal in the RIS, which leads to a greater effect of the RIS phase shift optimization on the system's secrecy rate. In other words, the RIS can optimize the phase shift of the reflected signals to enhance the desired signal's power and reduce the interference from the eavesdropper. Moreover, we can infer from Fig.2 that an increase in the number of eavesdropping antennas leads to a reduction in the secrecy rate of the system. This is because with more eavesdropping antennas, the eavesdropper can capture more information about the transmitted signal, making it more difficult to maintain secrecy.

Fig.3 illustrates the effect of increasing the number of antennas at the base station on network secrecy rate when the power of the base station and reflecting elements in RIS are set to 30 dBm and 36 dBm, respectively. As shown in the figure, increasing the number of antennas allows for more precise beamforming, resulting in a higher overall secrecy rate. Similarly, an increase in the number of eavesdropper antennas also leads to better beam shaping capabilities, which decreases the secrecy rate. Active attack strategies effectively reduce the achievable secrecy rate

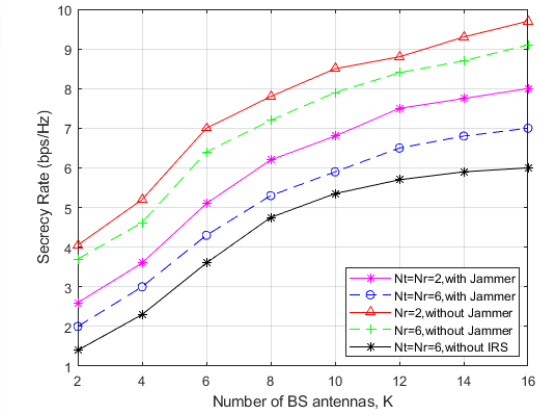


Figure 3. Achievable Secrecy Rate vs. Number of BS's Antennas

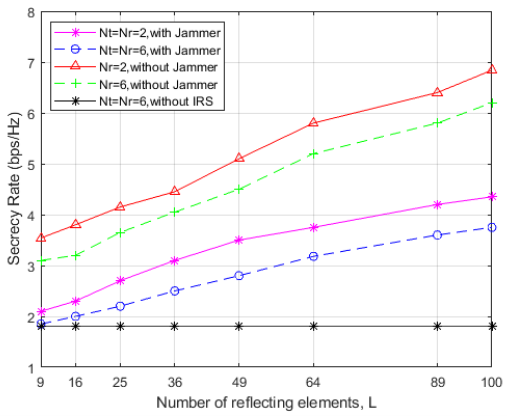


Figure 4. Achievable Secrecy Rate vs. Number of Reflecting Elements of the RIS

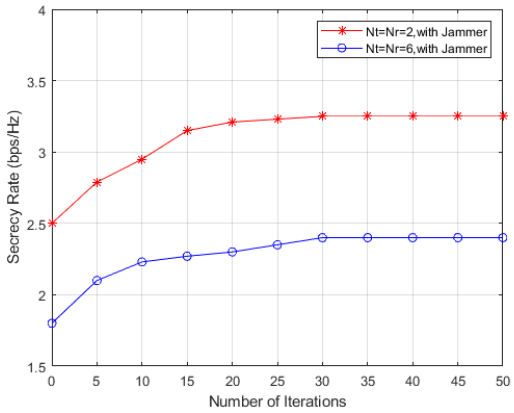


Figure 5. Converge of the Proposed BCD Algorithm

by disrupting communication between legitimate transmitter and receiver nodes through jamming signals. Therefore, advanced encryption techniques and physical layer security mechanisms such as artificial noise generation, beamforming, and power control should be deployed to combat these attacks and optimize network security and performance.

Fig.4 depicts the secrecy rate versus the number of reflecting elements at the RIS, where $P_{BS} = 30dBm$ and $K = 3$. As expected, an increase in the number of RIS elements results in higher secrecy rates, as more phase shift optimization centers become available. Conversely, without reflective elements, the secrecy rate remains constant regardless of the number of such elements added. Interestingly, the gap between the secrecy rates in the presence and absence of a jammer widens with increasing numbers of RIS reflection elements. This is due to the presence of malicious signals sent to the RIS via the jammer, which adversely affects the secrecy rate.

Fig.5 demonstrates the convergence of Algorithm 1 in relation to the secrecy rate as a function of the number of iterations, with varying numbers of active attacker antennas. The plot shows that as the number of iterations increases, the achieved security rate exhibits a non-decreasing trend. Specifically, it can be observed that as the number of iterations increases, the secrecy rate also increases, and Algorithm 1 requires approximately 18 iterations to converge, depending on the number of antennas used. This figure evaluates the effectiveness of the algorithm in solving the problem of maximizing the secrecy rate, clearly demonstrating the increasing trend of the secrecy rate with the number of iterations.

## V. CONCLUSION

This paper investigates the security of a RIS-assisted system in the presence of a full-duplex active attacker. The beamforming vector of the base station and the RIS reflecting elements' phases are jointly optimized to maximize the network secrecy rate. We therefore suggest an innovative approach based on alternating techniques to address the ensuing non-convex optimization issue. According to our numerical results, A full-duplex attacker can substantially decrease the network's secrecy rate especially when the number of antennas is high. The findings indicate that wireless networks using Reconfigurable Intelligent Surface can benefit from an increased rate of secrecy by raising the number of reflective elements, Base Station power, and the number of antennas. Considering these factors is vital when designing secure RIS-assisted systems in the presence of potential attackers.

## REFERENCES

[1] Ijaz Ahmad, Shahriar Shahabuddin, Tanesh Kumar, Jude Okwuibe, and Andrei Gurtov. Security for 5G and Beyond. *IEEE Communications Surveys and Tutorials*, 21(4):3682 – 3722, 2019.

[2] Hao Chen, Gang Yang, and Ying-Chang Liang. Joint Active and Passive Beamforming for Reconfigurable Intelligent Surface Enhanced Symbiotic Radio System. *IEEE Wireless Communications Letters*, 10(5):1056 – 1060, 2021.

[3] Jie Chen, Ying Chang Liang, Yiyang Pei, and Huayan Guo. Intelligent Reflecting Surface: A Programmable Wireless Environment for Physical Layer Security. *IEEE Access*, 7:82599 – 82612, 2019.

[4] Tingjun Chen, Sasank Garikapati, Aravind Nagulu, Aditya Gaonkar, Manav Kohli, and Igor Kadota. A Survey and Quantitative Evaluation of Integrated CircuitBased Antenna Interfaces and Self-Interference Cancellers for Full-Duplex. *IEEE Open Journal of the Communications Society*, 2(4):1753 – 1776, 2021.

[5] Jung Il Choi, Mayank Jain, Kannan Srinivasan, Phil Levis, and Sachin Katti. Achieving single channel, full duplex wireless communication. *in: Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking*, pages 1 – 12, 2010.

[6] Zheng Chu, Wanming Hao, Pei Xiao, De Mi, Zilong Liu, and Mohsen Khalily. Secrecy Rate Optimization for Intelligent Reflecting Surface Assisted MIMO System. *IEEE Transactions on Information Forensics and Security*, 16:1655 – 1669, 2020.

[7] Miao Cui, Guangchi Zhang, and Rui Zhang. Secure Wireless Communication via Intelligent Reflecting Surface. *IEEE Wireless Communications Letters*, 8(5):1410 – 1414, 2019.

[8] Keming Feng, Xiao Li, Yu Han, Shi Jin, and Yijian Chen. Physical Layer Security Enhancement Exploiting Intelligent Reflecting Surface. *IEEE Communications Letters*, 25(3):734–738, 2021.

[9] Jubin Jose, Narayan Prasad, Mohammad Khojastepour, and Sampath Rangarajan. On Robust Weighted-Sum Rate Maximization in MIMO Interference Networks. *in: 2011 IEEE International Conference on Communications, ICC*, 2011.

[10] Waqas Khalid, Heejung Yu, Dinh-Thuan Do, Zeeshan Kaleem, and Song Noh. RIS-Aided Physical Layer Security With Full-Duplex Jamming in Underlay D2D Networks. *IEEE Access*, 9:99667 – 99679, 2021.

[11] Majid H. Khoshafa, Telex M N Ngatched, and Mohamed Hossam Ahmed. Reconfigurable Intelligent Surfaces-Aided Physical Layer Security Enhancement in D2D Underlay Communications. *IEEE Communications Letters*, 25:1443 – 1447, 2021.

[12] Jie Liu, Jun Zhang, Qi Zhang, Jue Wang, and Xinghua Sun. Secrecy Rate Analysis for Reconfigurable Intelligent Surface assisted MIMO Communications with Statistical CSI. *IEEE China Communications*, 18(3):52 – 62, 2021.

[13] Yiliang Liu, Hsiao-Hwa Chen, and Liangmin Wang. Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges. *IEEE Communications Surveys & Tutorials*, 19(1):347 – 376, 2017.

[14] Xiao Lu, Ekram Hossain, Taniya Shafique, Shaohan Feng, Hai Jiang, and Dusit Niyato. Intelligent Reflecting Surface Enabled Covert Communications in Wireless Networks. *IEEE Network*, 34(5):148 – 155, 2020.

[15] Bin Lyu, Dinh Thai Hoang, Shimin Gong, Dusit Niyato, and Dong In Kim. IRS-based Wireless Jamming Attacks: When Jammers can Attack without Power. *IEEE Wireless Communications Letters*, 9(10):1663 – 1667, 2020.

[16] Amitav Mukherjee and A Lee Swindlehurst. Detecting passive eavesdroppers in the MIMO wiretap channel. *in: 2012 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP*, pages 2809 – 2812, 2012.

[17] Faisal Naeem, Mansoor Ali, Georges Kaddoum, Chongwen Huang, and Chau Yuen. Security and Privacy for Reconfigurable Intelligent Surface in 6G: A Review of Prospective Applications and Challenges. *IEEE Open Journal of the Communications Society*, 4:1196 – 1217, 2023.

[18] Hehao Niu, Zheng Chu, Fuhui Zhou, Zhengyu Zhu, Miao Zhang, and Kai-Kit Wong. Weighted Sum Secrecy Rate Maximization Using Intelligent Reflecting Surface. *IEEE Transactions on Communications*, 69(9):6170 – 6184, 2021.

[19] Chinaemerem David Nwankwo, Lei Zhang, Atta Quddus, Muhammad Ali Imran, and Rahim Tafazolli. A Survey of Self-Interference Management Techniques for Single Frequency Full Duplex Systems. *IEEE Access*, 6:30242 – 30268, 2017.

[20] Cunhua Pan, Hong Ren, Kezhi Wang, Wei Xu, Maged Elkashlan, and Arumugam Nallanathan. Multicell MIMO Communications Relying on Intelligent Reflecting Surfaces. *IEEE Transactions on Wireless Communications*, 19(8):5218 – 5233, 2020.

[21] Ashutosh Sabharwal, Philip Schniter, Dongning Guo, Daniel W Bliss, Sampath Rangarajan, and Risto Wic. In-band full-duplex wireless: challenges and opportunities. *IEEE Journal on Selected Areas in Communications*, 32(9):1637 – 1652, 2014.

[22] Qingjiang Shi, Meisam Razaviyayn, Zhi-Quan Luo, and Chen He. An iteratively weighted MMSE approach to distributed sum-utility maximization for a MIMO interfering broadcast channel. *IEEE Transactions on Signal Processing*, 59(9):4331 – 4340, 2011.

[23] Xiao Tang, Xunqiang Lan, Daosen Zhai, Ruonan Zhang, and Zhu Han. Securing Wireless Transmissions with RIS-Receiver Coordination: Passive Beamforming and Active Jamming. *IEEE Transactions on Vehicular Technology*, 70(6):6260 – 6265, 2021.

[24] Xiao Tang, Dawei Wang, Ruonan Zhang, Zheng Chu, and Zhu Han. Jamming Mitigation via Aerial Reconfigurable Intelligent Surface: Passive Beamforming and Deployment Optimization. *IEEE Transactions on Vehicular Technology*, 70(6):6232 – 6237, 2021.

[25] Qun Wang, Fuhui Zhou, Rose Qingyang Hu, and Yi Qian. Energy-Efficient Beamforming and Cooperative Jamming in IRS-Assisted MISO Networks. *in: IEEE International Conference on Communications, ICC*, 2020.

[26] Qingqing Wu, Shuowen Zhang, Beixiong Zheng, Changsheng You, and Rui Zhang. Intelligent Reflecting Surface-Aided Wireless Communications: A Tutorial. *IEEE Transactions on Communications*, 69(5):3313 – 3351,, 2021.

[27] Yongpeng Wu, Ashish Khisti, Chengshan Xiao, Giuseppe Caire, Kai Kit Wong, and Xiqi Gao. A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. *IEEE Journal on Selected Areas in Communications*, 36(4):679 – 695, 2018.

[28] Sai Xu, Jiajia Liu, and Yurui Cao. Intelligent Reflecting Surface Empowered Physical Layer Security: Signal Cancellation or Jamming? *IEEE Internet of Things Journal*, 9(2):1265 – 1275, 2022.

[29] Sai Xu, Jiajia Liu, and Jie Zhang. Resisting Undesired Signal Through RIS-Based Backscatter Communication System. *IEEE Communications Letters*, 25(8):2743 – 2747, 2021.

[30] Helin Yang, Zehui Xiong, Jun Zhao, Dusit Niyato, Qingqing Wu, and H Vincent Poor. Intelligent Reflecting Surface Assisted Anti Jamming Communications: A Fast Reinforcement Learning Approach. *IEEE Transactions on Wireless Communications*, 20(3):1963 – 1974, 2021.

[31] Jiayi Zhang, Hongyang Du, Qiang Sun, Bo Ai, and Derrick Wing Kwan Ng. Physical Layer Security Enhancement With Reconfigurable Intelligent Surface-Aided Networks. *IEEE Transactions on Information Forensics and Securit*, 16:3480 – 3495, 2021.

**Atefeh Zakeri** received her B.Sc. degree in Electrical Engineering from Urmia University, Urmia, Iran, in 2019, and her M.Sc. degree in Communication Systems from the Iran University of Science and Technology (IUST), Tehran, Iran, in 2022. Her research interests include wireless communication, reconfigurable intelligent surfaces, and physical layer security.

**S. Mohammad Razavizadeh** (Senior Member, IEEE) received his B.Sc., M.Sc., and Ph.D. degrees in Electrical Engineering from the Iran University of Science and Technology (IUST) in 1997, 2000, and 2006, respectively. He currently serves as an Associate Professor at the School of Electrical Engineering at IUST. His research interests include wireless and mobile communications, with a particular focus on physical layer techniques such as MIMO and physical layer security.