Intelligent Reflecting Surface Enhanced Secure Transmission Against Both Jamming and Eavesdropping Attacks

Yifu Sun, Kang An, Junshan Luo, Yonggang Zhu, Gan Zheng, Fellow, IEEE, and Symeon Chatzinotas, Senior Member, IEEE

Abstract—Both the jammer and the eavesdropper pose severe threat to wireless communications due to the broadcast nature of wireless channels. In this paper, an intelligent reflecting surface (IRS) assisted secure communication system is considered, where a base station (BS) wishes to reliably convey information to a user, in the presence of both a jammer and an eavesdropper whose transmit informations are not completely known. Specifically, with the imperfect third-party node’s channel state information (CSI) and no knowledge of the jammer’s transmit beamforming, we aim to maximize the system achievable rate by jointly designing the BS’s transmit beamforming and the IRS’s reflect beamforming, while limiting the information leakage to the potential eavesdropper. Due to the non-convexity and intractability of the original problem induced by the incompletely known information, we utilize the auxiliary variables, Cauchy-Schwarz inequality, and General Sign-Definiteness transformation to convert the original optimization problem into a tractable convex optimization problem, and then obtain the high-quality optimal solution by using the successive convex approximation and penalty convex concave procedure. Numerical simulations demonstrate the superiority of our proposed optimization algorithm compared with existing approaches, and also reveal the impact of key parameters on the achievable system performance.

Index Terms—Intelligent reflecting surface, anti-jamming, physical-layer security, robust beamforming optimization, incompleted information.

I. INTRODUCTION

The advancement of the next generation wireless communication explosively increases the demands on data transmission. However, due to the broadcast nature of wireless channels, the associated security vulnerabilities and threats have raised growing concerns, including both the passive eavesdropping for data interception and the active jamming for disrupting legitimate transmissions [1]. Various technologies have been proposed to enhance wireless security against the jamming and eavesdropping attacks. Frequency hopping [2] and power control [3] are extensively adopted to address the jamming attacks. However, frequency hopping consumes extra spectrum resources, and power control is not suitable for the case of large jamming power. In terms of the eavesdropping, the existing literatures usually applied cooperative relaying [4] and artificial noise-aided beamforming [5] schemes. Nevertheless, cooperative relaying and transmitting artificial noise consume additional power.

To overcome these shortcomings of existing approaches, a new paradigm, called intelligent reflecting surface (IRS), has been recently proposed to enhance both secrecy performance and spectrum efficiency [6]–[12]. An IRS is comprised of many passive low-cost reflecting elements, where each unit can adaptively adjust its phase and/or amplitude to reconfigure the wireless propagation environment, thus boosting and/or suppressing the received signals at the users [6]–[8]. In [7], by leveraging the passive IRS, the authors jointly optimized the active beamforming at the BS and the passive beamforming at the IRS to improve the coverage of wireless network. Aiming to maximize the achievable secrecy rate, the authors in [8] and [9] used IRS to protect secure transmission from eavesdropping attacks. The works in [10] further studied the IRS-assisted secure beamforming and artificial noise scheme to maximize the secrecy rate in the multiple-input multiple-output (MIMO) system. Considering the channel state information (CSI) is not perfectly known at the base station (BS), a transmit power minimization problem is formulated in [11] for anti-eavesdropping with imperfect CSI. Despite the above works focusing on the anti-eavesdropping scenarios, a prior work in [12] first used IRS for anti-jamming communications with the aim of maximizing the system achievable rate under the minimum SINR requirement, where the perfect jammer’s CSI and transmit beamforming were known at the BS. To the best of our knowledge, no exiting work has considered the utilization and associated design of the IRS-assisted secure transmission against both jamming and eavesdropping attacks.

In this paper, we propose an IRS-enhanced secure communication system for protecting the wireless transmission from both jamming and eavesdropping attacks, where the third-party node’s CSI is not perfectly known at the BS and the jammer’s transmit beamforming cannot be obtained by the system. The contributions of this paper are summarized as follows:

1) A generalized framework of the IRS-assisted secure transmission against both the jammer and the eavesdropper is first proposed. In addition, we consider the robust beamforming design with incomplete information, namely the imperfect CSI and unknown transmit beamforming. Specifically, considering the third-party node’s bounded CSI error and having no knowledge of the jammer’s transmit beamforming, the achievable system rate is maximized by jointly optimizing the active transmit beamforming at the BS and the passive reflecting beamforming at the IRS, while the information leakage to the potential eavesdropper is constrained.

2) Owing to the non-convexity and intractability of optimization problem, we firstly transform the non-convex objective function into convex one by adding a auxiliary variable, and subsequently, the General Sign-Definiteness transformation and Cauchy-Schwarz inequality are applied to address the incompletely known information. As such, the successive convex approximation (SCA) and penalty convex concave procedure (P-CCP) are proposed to solve the optimization problem.

3) Numerical results demonstrate the effectiveness and superiority of the proposed scheme, through comparison to the existing approach.
and \((BU_\nu = C_\nu x = diag (H_\nu x) + \Delta H_\nu)\) with are unknown CSI error. and \(P\) denotes the CSI + \(\sim CN\) and \(\sim \mathcal{CN}\) denotes the distribution of a circularly symmetric complex Gaussian random vector. Accordingly, the system achievable rate and the secrecy rate can be respectively expressed as

\[
R_U (w_T, v) = \log_2 \left( 1 + \frac{|h_{BUU} w_T|^2}{|h_{IU} w_T|^2 + \sigma_U^2} \right),
\]

\[
C_{sec} (w_T, v) = [R_U (w_T, v) - R_E (w_T, v)]^+, \]

where \(R_E (w_T, v) = \log_2 \left( 1 + \frac{|h_{BEU} w_T|^2}{\sigma_E^2} \right)\).

B. Problem Formulation

In this paper, a worst-case robust rate maximization problem is formulated for the incompletely informed [16]. In particular, with the imperfect third-party node’s CSI and no knowledge of the jammer’s transmit beamforming, we aim to maximize the system achievable rate by jointly designing the transmit beamforming \(w_T\) at the BS and the reflecting beamforming vector \(v\) at the IRS against both jamming and eavesdropping attacks, while keeping the information leakage to the eavesdropper below a target. Thus, the corresponding problem \(^2\) can be formulated as

\[
\mathcal{F} : \max_{w_T, v} \min_{\Delta H_{IU}, \Delta H_{BE}} R_U (w_T, v),
\]

subject to \(C_1 : \max_{\Delta H_{IU}, \Delta H_{BE}} R_E (w_T, v) \leq \tau, \)

\(C_2 : ||w_T||^2 \leq P_{max}, \) \(C_3 : |v_i| = 1, \forall i, \)

where \(\tau\) is the target secrecy rate. Note that the optimization problem \(\mathcal{F}\) is non-convex and we cannot solve it directly, due to the coupled variables \(w_T\) and \(v\) in both the objective function and the constraints. In addition, the incomplete information is considered in the problem, which leads to infinite non-convex constraints in the objective function and \(C_1\), which forms another challenge for solving the problem \(\mathcal{F}\). Thus, we propose an alternative algorithm (AO) to solve the problem in the following section.

III. SYSTEM ACHIEVABLE RATE MAXIMIZATION

In this section, we divide problem \(\mathcal{F}\) into two subproblems, i.e., the robust secure beamforming and phase shift design, and then \(w_T\) and \(v\) can be obtained in an iterative manner.

\(^1\)Due to the cooperation between the jammer and the eavesdropper, the jammer can design the beam pattern which positions the eavesdropper in the null space of the jamming signal by using the multi-antenna technique [14]. In addition, the work in [15] has summarized some signal processing methods to address the interference problem, where the receivers can use Code Division Multiple Access (CDMA), core decoding, and detection technique to eliminate the interference. Therefore, it is reasonable to assume that the jamming signal received by the eavesdropper can be eliminated.

\(^2\)According to [9], the constraint \(C_1\) guarantees the system secrecy rate is bounded from \(C_{sec} (w_T, v) \geq R_U (w_T, v) - \tau\).
A. Robust Secure Beamforming Design

Given the phase shift \( \nu \), we try to achieve the robust secure beamforming \( w_T \) under imperfect CSI in this subsection. Since the term \( |h_{1u}w_j| \) in problem \( \mathcal{F} \) does not involve \( w_T \), we can regard it as a fixed received jamming power \( J \) in the subproblem. Hence, the incompleteness in the objective function can be ignored due to the abovementioned operation, and then the problem \( \mathcal{F} \) can be reformulated as

\[
Q^w_0 := \max_{w_T} |\hat{h}_{BU}w_T|^2 \quad s.t. \quad C1, C2.
\]  

Indeed, problem \( Q^w_0 \) remains non-convex as its objective function and constraints are non-convex. To address this difficulties, we first convert the infinite non-convex constraint \( C1 \) into a tractable form by utilizing the following proposition.

Proposition 1: Constraint \( C1 \) has the following equivalent tractable form \( \mathcal{C}T \), which is formulated as

\[
\begin{bmatrix}
\hat{A}_BE & \hat{h}_{BE} & 0_{1 \times M} & 0_{1 \times M} \\
\hat{A}_BE & 1 - u_2 & \xi_{BE}w_T^H & \xi_{BE}w_T^H \\
0_{M \times 1} & \xi_{BE}w_T & u_1 & 0_{M \times 1} \\
0_{M \times 1} & \xi_{BE}w_T & u_1 & 0_{M \times 1}
\end{bmatrix} \geq 0,
\]

where \( \hat{A}_{BE} = (\hat{h}_{BE} + \nu \hat{H}_{BE})w_T \), \( \hat{A}_{BE} = \sigma_E^2 (2^*-1) - u_1 N - u_2 \), and \( u_1, u_2 \geq 0 \) are slack variables.

Proof: By dropping the log function and adopting Schur’s complement [17] in \( C1 \), the constraint \( C1 \) can be equivalently transformed to

\[
\left( \begin{array}{cc}
\sigma_E^2 (2^*-1) & \hat{h}_{BE}w_T \\
w_T^H (\hat{h}_{BE}^H + \nu \hat{H}_{BE}^H) & 1
\end{array} \right) \geq 0.
\]

Then, substituting \( h_{BE} = \hat{h}_{BE} + \Delta h_{BE}, h_{BE} = \hat{h}_{BE} + \Delta h_{BE} \) into (10) and after some mathematical transformations, we can obtain that

\[
\begin{bmatrix}
\sigma_E^2 (2^*-1) & \nu h_{BE}^H w_T \\
w_T^H (\hat{H}_{BE}^H + \nu \hat{H}_{BE}^H) & 1
\end{bmatrix}
- \left[ 0_{0 \times M} w_T \right] \left[ \Delta h_{BE} 0_{M \times 1} \right] - \left[ 0_{0 \times M} w_T \right] \left[ \Delta h_{BE} 0_{M \times 1} \right]
- \left[ 0_{0 \times N} w_T \right] \left[ \Delta h_{BE} 0_{N \times 1} \right] - \left[ 0_{0 \times N} w_T \right] \left[ \Delta h_{BE} 0_{N \times 1} \right].
\]

Next, we utilize General Sign-Definiteness transformation to make further manipulations, which is expressed as

Lemma 1: \( (General \ Sign-Definiteness \ [18]) \) Given matrices \( B = B^H \) and \( |C_i|, D_i \), the linear matrix inequality (LMI) \( B \geq \sum_{i=1}^{\nu} (C_i^H X D_i + D_i^H C_i^H) \), \( \forall i, \|X\| \leq \xi \) hold only if there exists \( \xi \geq 0, \forall i, \) such that

\[
B = \begin{bmatrix}
\sigma_E^2 (2^*-1) & \hat{h}_{BE}^H w_T \\
w_T^H (\hat{h}_{BE}^H + \nu \hat{H}_{BE}^H) & 1
\end{bmatrix} \geq 0.
\]

Proof: Please refer to [18].

In order to use lemma 1, we choose the following parameters to replace the terms in (11), as

\[
B = \begin{bmatrix}
\sigma_E^2 (2^*-1) & \hat{h}_{BE}^H w_T \\
w_T^H (\hat{h}_{BE}^H + \nu \hat{H}_{BE}^H) & 1
\end{bmatrix}.
\]

\[
C_1 = C_2 = -\left[ 0_{M \times 1} w_T \right], \quad D_1 = [\nu 0_{N \times 1}] \quad D_2 = I.
\]

\[
X_1 = \Delta \hat{H}_{BE}^H, \quad X_2 = \left[ \Delta \hat{H}_{BE}^H 0_{M \times 1} \right].
\]

Applying the lemma 1, by introducing slack variables \( u_2, u_3 \), and combining \( \| \Delta \hat{H}_{BE} \| \leq \xi_{BE}, \| \Delta \hat{H}_{BE} \| \leq \xi_{BE} \), (11) can be transformed into a LMI \( \mathcal{C}T \).

Hence, the proof is completed.

Note that the objective function in the problem \( Q^w_0 \) is non-convex with respect to \( w_T \). Nevertheless, we can approximate it via SCA. By utilizing the first-order Taylor inequality, i.e., for any complex scalar variable \( x \) and \( x^{(n)} \),

\[
|z|^2 \geq 2\text{Re} \{ x^{(n)} x - x^{(n)} x^{(n)} \},
\]

we can obtain \( \| h_{BU}w_T \|^2 \geq 2\text{Re} \{ h_{BU}w_T^H \hat{h}_{BU}w_T \} - h_{BU}w_T^H \hat{H}_{BU}w_T \), where \( \hat{H}_{BU} \) is optimal solution obtained at iteration \( n \). Here, the superscript \( * \) and \( T \) represent the conjugate and transpose, respectively. Thus, after dropping the constraint, the problem \( Q^w_0 \) can be recast as

\[
Q^w := \max_{w_T \in \mathbb{C}^M} \text{Re} \left\{ w_T^H \hat{h}_{BU}w_T \right\} \quad s.t. \quad \mathcal{C}T, C2.
\]

Obviously, the convex problem \( Q^w \) can be solved by using the CVX tool [19]. Therefore, a first-order optimum solution of \( w_T \) given \( \nu \) can be achieved by utilizing SCA to solve the problem \( Q^w \) until convergence.

B. Phase Shift Design

Given the transmit beamforming \( w_T \), recall the transformed constraint \( \mathcal{C}T \), and then the phase shift design problem can be expressed as

\[
Q^2_0 := \max_{w_T \in \mathbb{C}^M} \min_{\Delta h_{BE} \in \mathcal{H}_{BU}} \left( \frac{\| h_{BU}w_T \|^2}{\| h_{BU}w_T \|^2 + \sigma_0^2} \right) \quad s.t. \quad \mathcal{C}T, C3.
\]

However, problem \( Q^2_0 \) is still non-convex due to \( \nu \) and the infinite concave bounded estimation error objective function. To solve this problem, we first convert the objective function into a more tractable form by adding an auxiliary variable \( \eta \geq 0 \), and then problem \( Q^2_0 \) can be reformulated as

\[
Q^2 := \max_{w_T \in \mathbb{C}^M} \min_{\Delta h_{BE} \in \mathcal{H}_{BU}} \left( \frac{\| h_{BU}w_T \|^2}{\eta + \sigma_0^2} \right) \quad s.t. \quad \mathcal{C}T, C3, C4 : \| h_{BU}w_j \|^2 \leq \eta.
\]

Due to the fact that the BS has no knowledge of the jammer’s transmit beamforming \( w_i \), problem \( Q^2 \) is NP-hard [17]. To make problem \( Q^2 \) feasible for practical implementation, inspired by [20], we utilize the Cauchy-Schwarz inequality to obtain the upper bound of \( C4 \), i.e., \( \| h_{BU}w_j \|^2 \leq P_j \| h_{BU} \|^2 \), where \( P_j \) denotes the power value of \( \| w_j \|^2 \), which can be obtained by using the signal strength and channel gains [20], [21]. However, owing to the CSI uncertainties of the jammer’s channels, \( P_j \) can not be accurately acquired. Following [22], we adopt \( P_j - P_j \leq \epsilon_j \) to denote the estimation error of \( \| w_j \|^2 \), where \( \epsilon_j \) is the estimation value. As such, one obtains the worst-case constraint that \( \| h_{BU}w_j \|^2 \leq \eta_j (1 - \epsilon_j) \leq \eta_j / P_j \). Then, similar to the proposition 1, the constraint \( C4 \) can be equivalently transformed to \( \mathcal{C}T \), which is given by

\[
\begin{bmatrix}
\hat{A}_{BU} \hat{A}_{BU} & \hat{A}_{BU} & 0_{N \times L} & 0_{N \times L} \\
\hat{A}_{BU} & 1 - p_2 I_L & \xi_{BU}I_L & \xi_{BU}I_L \\
0_{N \times 1} & \xi_{BU}I_L & p_2 I_L & 0_{N \times 1} \\
0_{N \times 1} & \xi_{BU}I_L & p_2 I_L & p_2 I_L
\end{bmatrix} \geq 0.
\]
where $\tilde{A}_{UU} = \tilde{H}_{UU} + v^H \tilde{H}_{UU}, \tilde{A}_{IU} = \tilde{H}_{IU} = \tilde{N}_{P_1} - N_{P_1} - N_{P_2},$ and $p_1, p_2 \geq 0$ are slack variables.

Proof: Please refer to the proof of Proposition 1.

Therefore, by using the aforementioned manipulation, problem $Q_2^v$ can be equivalently transformed to

$$Q_2^v : \max_{v, \{p_1, p_2, u_1, u_2, \eta\} \in \mathbb{R}^+} \frac{\|H_{BU} w_T\|^2}{\eta + \sigma U^2} \quad \text{s.t.} \ C_1, C_2, C_3, C_4.$$  \hspace{1cm} (19)

Note that in the problem $Q_2^v$, the system achievable rate is determined by $v$ and $\eta$, which cannot be solved simultaneously. Thus, in this subsection, we first achieve a proper region of $\eta$ numerically, and then utilize the SCA and P-CCP to optimize $v$ with fixed $\eta$. Finally, the optimal $\eta^{\text{opt}}$ can be obtained by using sampling method in its region [16].

Specifically, in this paper, we define that the achievable rate must satisfy $R_U(w_T, v) \geq 1$ bps/Hz, and thus one obtains that

$$\eta + \sigma U^2 \leq \left\| H_{BU} w_T \right\|^2 = \left\| w_T \right\|^2 \left\| H_{BU} + v^H H_{BU} \right\|^2$$

$$\leq \left\| w_T \right\|^2 \left\| (H_{BU} h_{BU} + 2Re \left\{ v^H H_{BU} h_{BU}^H \right\} + v^H H_{BU} H_{BU}^H v) \right\|^2.$$  \hspace{1cm} (20)

Since $w_T$ is fixed in this subsection, the work can be reduced to maximize $\phi(v) = H_{BU} h_{BU}^H + 2Re \left\{ v^H H_{BU} h_{BU}^H \right\} + v^H H_{BU} H_{BU}^H v$, which corresponds to the following problem

$$Q_2^v : \min_v \left\{ \left( - H_{BU} H_{BU}^H \right) v - 2Re \left\{ v^H H_{BU} h_{BU}^H \right\} \right\} \text{s.t.} C_3.$$  \hspace{1cm} (21)

We note that the objective function in problem $Q_2^v$ is concave, which makes the problem non-convex. However, it can be solved via SCA. To approximate the objective function, the following key lemma is needed.

Lemma 2 [23]: Assuming $Q$ be an $N \times N$ Hermitian matrix, for any $x^{(n)} \in \mathbb{C}^{N \times 1}$, one obtains that $x^H Q x \leq x^H \lambda_i (Q) x - 2Re \{ x^H (\lambda_i (Q) I - Q) x^{(n)} \} + x^{(n), H} (\lambda_i (Q) I - Q) x^{(n)}$, where the term $\lambda_i (Q)$ denotes the maximum eigenvalues of $Q$.

Proof: Please refer to [23].

Utilizing lemma 2, the upper bound of objective function in problem $Q_2^v$ can be formulated as

$$\nu^H \left( - H_{BU} H_{BU}^H \right) v - 2Re \left\{ \nu^H H_{BU} h_{BU}^H \right\}$$

$$\leq \nu^H \lambda_i \left( - H_{BU} H_{BU}^H \right) v - 2Re \left\{ \nu^H H_{BU} h_{BU}^H \right\}$$

$$- 2Re \left\{ \nu^H \left( \lambda_i \left( - H_{BU} H_{BU}^H \right) I + H_{BU} H_{BU}^H \right) v^{(n)} \right\}$$

$$+ v^{(n), H} \left( \lambda_i \left( - H_{BU} H_{BU}^H \right) I + H_{BU} H_{BU}^H \right) v^{(n)}.$$  \hspace{1cm} (22)

Since $\nu^H v = N$, the first term of (22) can be regarded as a constant. Therefore, by dropping the constant terms in (22), the majorized problem $Q_2^v$ is given by

$$Q_2^v : \max \Re \left\{ \nu^H \left( R_{BU} + H_{BU} h_{BU}^H \right) \right\} \text{s.t.} C_3,$$  \hspace{1cm} (23)

where $R_{BU} = \lambda_i \left( - H_{BU} H_{BU}^H \right) I + H_{BU} H_{BU}^H$. According to [23], a first-order optimal closed-form solution of $\nu$ in problem $Q_2^v$ can be obtained, i.e.,

$$\nu^{\text{opt}} = \exp \left\{ j \underset{\arg \left( R_{BU} + H_{BU} h_{BU}^H \right) \in \mathbb{R}^+} \arg \left( R_{BU} + H_{BU} h_{BU}^H \right) \right\}.$$  \hspace{1cm} (24)

Thus, the upper bound of $\eta$ can be finally obtained as $\mathcal{U}(\nu^{\text{opt}}) = \left\| w_T \right\|^2 \left\| H_{BU} + \nu^{\text{opt}, H} H_{BU} \right\|^2 / \sigma U^2$. Then, problem $Q_3^v$ can be equivalently expressed as

$$Q_3^v : \max_{\eta} \eta = \mathcal{U}(\nu^{\text{opt}}), \text{s.t.} 0 \leq \eta \leq \mathcal{U}(\nu^{\text{opt}}).$$
where $R_U(w_T^{(k)}, v^{(k)})$ and $v^{(k)}$ are the solutions in the iteration $k$. In addition, since $w_T$ is bounded by the constraint C2, and $v$ is bounded by the constraint C1, $R_U(w_T^{(k)}, v^{(k)})$ is guaranteed to converge to a limit optimal point $[w_T^{opt}, v^{opt}]$. According to [17], the complexity of optimizing $w_T$ given $v$ during each SCA iteration is $O(M + 2)^2$, and that of optimizing $v$ given $w_T$ with fixed $\eta$ is $O(3N + 4)^2$. Moreover, the complexity of solving $\eta$ via (23) and SCA is about $O(N^3)$.

IV. SIMULATION RESULTS

In this section, numerical simulations are provided to validate the proposed algorithm. We consider a BS equipped with $M = 8$ antennas and the antenna number of jammer is $L = 2$. It is assumed that the BS, the user, and the IRS are located at (0,0), (150,0), and (10,5) in meter (m) in a 2-D plane, respectively. Jammer is randomly located in a circle centered at (200,0) with radius of 10m, and eavesdropper is randomly situated in a circle centered at (160,0) with radius of 5m. Based on the 3GPP UMi model with 3.5 GHz carrier frequency [25], we assume that all involved channel coefficients are generated by $H = \sqrt{L_o(d/d_0)^H}$, where $L_o = -40$ dB denotes the path loss at reference distance $d_0 = 1$ m, $d$ is the link distance, $\rho$ denotes the path loss exponent, and $H$ is the Rician components with Rician factors $K$ [7]. The corresponding path loss exponents and Rician factors are set as $\rho_{HI} = \rho_{JI} = 2.2$, $\rho_{HU} = \rho_{UB} = \rho_{BE} = \rho_{UB} = 3$, and $K_{HI} = K_{JI} = K_{BU} = K_{JU} = K_{BE} = K_{HU} = K_{BE} = 1$, respectively, by referring to [8]. And the sampling interval of $\eta$ is set as 0.01. Other system settings as follows: $\sigma^2_U = \sigma^2_E = -80$ dBm as in [8], $\xi_H = 0.01$, and the jammer’s beamforming is set to $w_J = \sqrt{P_J} T_J \text{opt}$ as in [12], where $P_J = 30$ dBm. We compare the following schemes: 1) Algorithm in [8]: the scheme only considers anti-eavesdropping requirement in the presence of both the jammer and the eavesdropper with the perfect information; 2) Non-IRS: under the perfect information assumption, we design $w_T$ by solving problem $Q_w$ without IRS. We obtain the simulation results by averaging over 200 random channel realizations.

Figure 2 shows the system achievable rate versus the number of IRS elements $N$, where $\tau = 1$ and $P_{max} = 30$ dBm. We find that all the proposed algorithms can achieve higher system rate compared to the existing approaches. In particular, the system rate of the heuristic algorithm in [8] is lower than that of proposed algorithms, which verifies the serious threat of the jammer to the system. Meanwhile, it is observed that the system rate of all schemes with IRS increase with $N$, but the increase speed of system rate decreases with $N$. This can be explained that more RIS elements can not only exploit more degrees of freedom to enhance desired signal, but also boost the jamming signal. Hence, $N$ needs to be carefully chosen for achieving satisfactory performance. Moreover, we can also see that the system rate decreases with CSI uncertainty level, and the CSI uncertainty associated with jamming channels has a larger impact on the system rate as compared with that associated with wiretap channels.

Fig. 3 depicts the feasibility rate versus different $\xi$. It is observed that the feasibility rate decreases with $\xi$, and the feasibility rate of reflection channel ($\xi_{HI}$) is higher than that of direct channel ($\xi_d$). This is because $\xi_{HI}$ is associated with $N$, will lead to the increase of total channel estimation errors. In addition, we can see that $\xi_{HI}, \xi_{JI}$, $\xi_{BE}$, and the feasibility rate of $N = 20$ is significantly smaller than that of $N \geq 50$. This can be explained by the reason that the C4 is stricter than C1, and small $N$ cannot guarantee that the desired power is large enough so that $R_U(w_T, v) \geq 1$ bps/Hz can be satisfied, thus $\eta^{opt}$ cannot be found. As such, $N$ should be properly selected for achieving satisfactory feasibility.

V. CONCLUSION

In this paper, we have proposed a novel IRS-assisted secure transmission system against both jamming and eavesdropping attacks with incomplete information, and studied the joint active transmit and passive reflecting beamforming optimization scheme to maximize the system achievable rate with transmit power and secrecy rate constraints. Specifically, the initial optimization problem was converted into a convex one by adding the auxiliary variables and utilizing General Sign-Defininiteness transformation, and then SCA with P-CCP was proposed to solve the intractable problem. Numerical results confirmed that the proposed algorithm has the superior performance compared with other existing schemes, and the impact of CSI uncertainty on the performance was also revealed.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," IEEE Proc., vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
[2] L. Liang, W. Cheng, W. Zhang, and H. Zhang, "Mode hopping in radio vortex wireless communications," IEEE Trans. Veh. Technol., vol. 67, no. 8, pp. 7018–7032, Aug. 2018.
[3] S. Feng and S. Haykin, "Cognitive radio control for anti-jamming V2V communications in autonomous vehicle networks," IEEE Trans. Veh. Technol., vol. 68, no. 10, pp. 9920–9934, Oct. 2019.
[11022] IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 70, NO. 10, OCTOBER 2021

[4] A. Mayouche, D. Spano, C. G. Tsinos, S. Chatzinotas, and B. Ottersten, “Learning-assisted eavesdropping and symbol-level precoding countermeasures for downlink MU-MISO systems,” IEEE Open J. Commun. Soc., vol. 1, pp. 535–549, Jun. 2020.

[5] S. Yan, N. Yang, I. Land, R. Malaney, and J. Yuan, “Three artificial-noise-aided secure transmission schemes in wiretap channels,” IEEE Trans. Veh. Technol., vol. 67, no. 4, pp. 3669–3673, Apr. 2018.

[6] C. Pan et al., “Intelligent reflecting surface aided MIMO broadcasting for simultaneous wireless information and power transfer,” IEEE J. Sel. Areas Commun., vol. 38, no. 8, pp. 1719–1734, Aug. 2020.

[7] 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. 7851–7866, Dec. 2020.

[14] Q. Liu, M. Li, X. Kong, and N. Zhao, “Disrupting MIMO communications with optimal jamming signal design,” IEEE Trans. Wireless Commun., vol. 14, no. 10, pp. 5313–5325, Oct. 2015.

[15] J. Andrews, “Interference cancellation for cellular systems: A contemporary overview,” IEEE Wireless Commun., vol. 12, no. 2, pp. 19–29, Apr. 2005.

[16] L. Dong, H.-M. Wang, and H. Xiao, “Secure cognitive radio communication via intelligent reflecting surface,” IEEE Trans. Commun., vol. 69, no. 7, pp. 4678–4690, Jul. 2021.

[17] S. Boyd and L. Vandenberghe, in Convex optimization. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[18] I. R. Petersen, “A stabilization algorithm for a class of uncertain linear systems,” Syst. Control Lett., vol. 17, no. 2, pp. 351–357, 1987.

[19] M. Grant and S. Boyd, “CVX: MATLAB software for disciplined convex programming,” 2016, [Online]. Available: http://cvxr.com/cvx.

[20] Z. Shen, K. Xu, and X. Xia, “Beam-domain anti-jamming transmission for downlink massive MIMO systems: A stackelberg game perspective,” IEEE Trans. Informat. Forensics Secur., vol. 16, pp. 2727–2742, Feb. 2021.

[21] R. Schmidt, “Multiple emitter location and signal parameter estimation,” IEEE Trans. Antennas and Propag., vol. 34, no. 3, pp. 276–280, Mar. 1986.

[22] L. Xiao, T. Chen, J. Liu, and H. Dai, “Anti-jamming transmission stackelberg game with observation errors,” IEEE Commun. Lett., vol. 19, no. 6, pp. 949–952, Jun. 2015.

[23] 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.

[24] T. Lipp and S. Boyd, “Variations and extension of the convex-concave procedure,” Optim. Eng., vol. 17, no. 2, pp. 263–287, 2016.

[25] 3GPP, “Technical specification group radio access network; study on 3D channel model for LTE (release 12),” TR 36.873 V12.7.0, Dec. 2017.