IRS-Enhanced Anti-Jamming Precoding Against DISCO Physical Layer Jamming Attacks

Huan Huang*, Hongliang Zhang†, Yi Cai*, Yunjing Zhang*, A. Lee Swindlehurst‡, and Zhu Han§
* Electronic Information School, Soochow University, Suzhou, China
† State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics, Peking University, Beijing, China
‡ Department of Electrical and Computer Engineering, University of Houston, Houston, USA
§ Center for Pervasive Communications and Computing, University of California, Irvine, USA

***Abstract*—Illegitimate intelligent reflective surfaces (IRSs) can pose significant physical layer security risks on multi-user multiple-input single-output (MU-MISO) systems. Recently, a DISCO approach has been proposed an illegitimate IRS with random and time-varying reflection coefficients, referred to as a "disco" IRS (DIRS). Such DIRS can attack MU-MISO systems without relying on either jamming power or channel state information (CSI), and classical anti-jamming techniques are ineffective for the DIRS-based fully-passive jammers (DIRS-based FPJs). In this paper, we propose an IRS-enhanced anti-jamming precoder against DIRS-based FPJs that requires only statistical rather than instantaneous CSI of the DIRS-jammed channels. Specifically, a legitimate IRS is introduced to reduce the strength of the DIRS-based jamming relative to the transmit signals at a legitimate user (LU). In addition, the active beamforming at the legitimate access point (AP) is designed to maximize the signal-to-jamming-plus-noise ratios (SJNRs). Numerical results are presented to evaluate the effectiveness of the proposed IRS-enhanced anti-jamming precoder against DIRS-based FPJs.**

***Index Terms*—Physical layer security, intelligent reflective surface, multi-user MISO (MU-MISO), transmit precoding, jamming suppression, channel aging.**

I. Introduction

Due to the broadcast and superposition properties of wireless channels, wireless communications are vulnerable to malicious attacks such as physical layer jamming [1]–[3]. Traditional active jammers (AJs) broadcast jamming signals, such as pseudorandom noise or modulated Gaussian noise, to intentionally disrupt legitimate wireless communications like Wi-Fi, Bluetooth, the Internet of Things (IoT), and cellular networks [1]–[3]. Fortunately, energy constraints are an inherent drawback of AJs, severely limiting their use. Moreover, classical anti-jamming approaches [3], such as spread spectrum and frequency-hopping techniques can be used to effectively relieve the jamming impact imposed by AJs.

Recently, the interesting idea of disco intelligent reflective surfaces (DIRSs) has been reported [2], [4]–[8], where illegitimate IRSs with time-varying random reflection coefficients act like "disco balls" to actively age wireless channels. Such active channel aging (ACA) can be used to jam legitimate users (LUs) without either jamming power or LU channel state information (CSI). An IRS configured in this way is referred to as a DIRS-based fully-passive jammer (FPJ). Moreover, some works have also investigated the use of DIRSs to break key consistency in channel reciprocity-based key generation [9]–[11]. Some unique properties of the DIRS-based FPJs are that their jamming impact cannot be mitigated by increasing transmit power [6] and classical anti-jamming approaches [3], such as spread spectrum and frequency-hopping techniques, are not effective for DIRS-based FPJs.

To address the serious concerns raised by DIRS-based FPJs, the previous work in [7], [8] provided a possible approach. This work showed that the elements of the DIRS-jammed channels converge to a complex Gaussian distribution as the number of the DIRS reflective elements becomes large, and then designed an anti-jamming precoder for the DIRS-based FPJs that requires only statistical rather than instantaneous CSI. Furthermore, an approach to estimate the statistical characteristics of the DIRS-based channels was proposed in [8]. However, this anti-jamming precoder cannot achieve good jamming suppression at high transmit power [7], [8].

The investigation conducted in [2] suggested that the legitimate AP can decrease the amount of DIRS-based ACA interference relative to the strength of the transmit signals to enhance the effect of the anti-jamming precoder [7], [8]. Based on this heuristic investigation, one can introduce legitimate IRSs to weaken the strength of the DIRS-based ACA interference relative to the transmit signals. However, for real-world applications, the following two difficulties should be addressed when jointly designing passive and active beamforming:

1) *The joint passive and active beamforming should be designed without cooperating with the illegitimate DIRS;*
2) *The joint passive and active beamforming should be designed without the instantaneous CSI of the DIRS-based channels which are unavailable to the AP.*

Given the two practical difficulties, we investigate legitimate IRS-assisted anti-jamming precoding against DIRS-based FPJs. The main contributions are summarized as follows:

- A legitimate IRS is introduced to suppress DIRS-based ACA interference, and a practical IRS model is considered in which the reflecting phase shifts of both the DIRS and the legitimate IRS are discrete. Moreover, we

This work was supported by the National Natural Science Foundation of China (62275185, 62250710164, 62371011) (*Corresponding author: Yi Cai; Email: yicai@ieee.org*).

ICC 2024 - IEEE International Conference on Communications | 978-1-7281-9054-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICC51166.2024.10622846

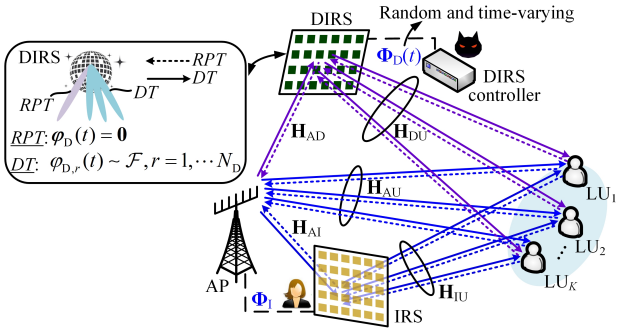

Fig. 1. The downlink of an MU-MISO system jammed by a temporal DIRS-based FPJ, where a legitimate IRS is introduced to resist the fully passive attacks launched by the temporal DIRS-based FPJ.

consider the above two real-world difficulties and then design the passive beamforming at the legitimate IRS by maximizing the received power of the transmit signals at each LU, which reduces the strength of the DIRS-based ACA interference relative to that of the transmit signals.

- To address time-varying DIRS phase shifts and the unknown CSI of the DIRS-related channels, we first derive the statistical characteristics of the DIRS-jammed channels. Then, a more explicit expression for the signal-to-jamming-plus-noise ratios (SJNRs) is given. In addition, we also design the active beamforming at the AP to maximize the SJNRs given the configuration of the legitimate IRS passive beamforming.

The rest of this paper is organized as follows. In Section II, we first describe an MU-MISO system jammed by a temporal DIRS-based FPJ, where a legitimate IRS is introduced to mitigate the DIRS-based ACA interference. We also define the SJNR to quantify performance. In Section II-B, the various channel models are defined and the optimization problem is formulated. In Section III-A, we first derive a more-explicit form for the SJNR based on the statistical characteristics of the DIRS-jammed channels. Then, the active beamforming at the AP is designed. In Section III-B, the passive beamforming at the legitimate IRS is designed via the Riemannian conjugate gradient (RCG) algorithm. In Section IV, simulation results are presented to evaluate the effectiveness of the proposed IRS-enhanced anti-jamming precoder. Finally, conclusions are given in Section V.

Notation: We employ bold capital letters for a matrix, e.g., $\mathbf{W}$, lowercase bold letters for a vector, e.g., $\boldsymbol{w}_k$, and italic letters for a scalar, e.g., K. The superscripts $(\cdot)^T$ and $(\cdot)^H$ represent the transpose and the Hermitian transpose, respectively, and the symbols $\|\cdot\|$ and $|\cdot|$ represent the Frobenius norm and the absolute value, respectively.

II. System Description

A. Temporal DIRS-based Fully-Passive Jamming

Fig. 1 schematically illustrates the downlink of an MU-MISO system in which a legitimate IRS with N_{I} reflective elements is controlled by an N_A-antenna AP to mitigate the fully-passive jamming launched by a temporal DIRS-based FPJ using an N_{D}-element illegitimate IRS [6], [7]. We assume that the AP communicates with K single-antenna LUs denoted as LU_1, LU_2, $\cdots$, LU_K, and the transmit symbol for LU_k $(1\le k\le K)$ during the DT phase satisfies $\mathbb{E}\left[|s_{DT,k}|^2\right]=1$. Consequently, the received signal at LU_k is given by

$$\begin{aligned} y_{DT,k} &= \boldsymbol{h}_{DT,k}^H\sum_{u=1}^{K}\boldsymbol{w}_u s_{DT,u}+n_k \\ &= \left(\boldsymbol{h}_{\mathrm{IU},k}^H\boldsymbol{\Phi}_{\mathrm{I}}\mathbf{H}_{\mathrm{AI}}+\boldsymbol{h}_{\mathrm{AU},k}^H+\boldsymbol{h}_{\mathrm{DU},k}^H\boldsymbol{\Phi}_{\mathrm{D}}(t)\mathbf{H}_{\mathrm{AD}}\right)\sum_{u=1}^{K}\boldsymbol{w}_u s_{DT,u}+n_k, \end{aligned} \tag{1}$$

where $\boldsymbol{w}_k$ is the transmit precoder for user k, $n_k\sim CN(0,\sigma^2)$ is additive Gaussian noise, $\boldsymbol{h}_{\mathrm{IU},k}\in\mathbb{C}^{N_{\mathrm{I}}\times 1}$ denotes the channel between the IRS and LU_k, $\mathbf{H}_{\mathrm{AI}}\in\mathbb{C}^{N_{\mathrm{I}}\times N_{\mathrm{A}}}$ denotes the channel between the AP and the IRS, $\boldsymbol{h}_{\mathrm{AU},k}\in\mathbb{C}^{N_{\mathrm{A}}\times 1}$ denotes the channel between the AP and LU_k, $\boldsymbol{h}_{\mathrm{DU},k}\in\mathbb{C}^{N_{\mathrm{D}}\times 1}$ denotes the channel between the DIRS and LU_k, $\mathbf{H}_{\mathrm{AD}}\in\mathbb{C}^{N_{\mathrm{D}}\times N_{\mathrm{A}}}$ denotes the channel between the DIRS and the AP, and $\boldsymbol{\Phi}_{\mathrm{I}}=\mathrm{diag}(\boldsymbol{\varphi}_{\mathrm{I}})=\mathrm{diag}(e^{\varphi_{\mathrm{I},1}},\cdots,e^{\varphi_{\mathrm{I},N_{\mathrm{I}}}})$ and $\boldsymbol{\Phi}_{\mathrm{D}}(t)=\mathrm{diag}(\boldsymbol{\varphi}_{\mathrm{D}}(t))=\mathrm{diag}\left(e^{\varphi_{\mathrm{D},1}(t)},\cdots,e^{\varphi_{\mathrm{D},N_{\mathrm{D}}}(t)}\right)$ represent the IRS reflecting vector and the time-varying DIRS reflecting vector during the DT phase. For ease of presentation, we denote the time-varying DIRS-jammed channel and the IRS-cascaded channel between the AP and LU_k by $\boldsymbol{h}_{\mathrm{D},k}(t)=\boldsymbol{h}_{\mathrm{DU},k}^H\boldsymbol{\Phi}_{\mathrm{D}}(t)\,\mathbf{H}_{\mathrm{AD}}$ and $\boldsymbol{h}_{\mathrm{I},k}=\boldsymbol{h}_{\mathrm{IU},k}^H\boldsymbol{\Phi}_{\mathrm{I}}\mathbf{H}_{\mathrm{AI}}$, respectively. Moreover, the overall DIRS-LU channel $\mathbf{H}_{\mathrm{DU}}$, the overal IRS-LU channel $\mathbf{H}_{\mathrm{IU}}$, the overall direct channel $\mathbf{H}_{\mathrm{d}}$, the overall DIRS-jammed channel $\mathbf{H}_{\mathrm{D}}$, and the overall IRS-cascaded channel $\mathbf{H}_{\mathrm{I}}$ are denoted by $\mathbf{H}_{\mathrm{DU}}^H=[\boldsymbol{h}_{\mathrm{DU},1}^H,\cdots,\boldsymbol{h}_{\mathrm{DU},K}^H]$, $\mathbf{H}_{\mathrm{IU}}^H=[\boldsymbol{h}_{\mathrm{IU},1}^H,\cdots,\boldsymbol{h}_{\mathrm{IU},K}^H]$, $\mathbf{H}_{\mathrm{AU}}^H=[\boldsymbol{h}_{\mathrm{AU},1}^H,\cdots,\boldsymbol{h}_{\mathrm{AU},K}^H]$, $\mathbf{H}_{\mathrm{D}}^H=[\boldsymbol{h}_{\mathrm{D},1}^H,\cdots,\boldsymbol{h}_{\mathrm{D},K}^H]$, and $\mathbf{H}_{\mathrm{I}}^H=[\boldsymbol{h}_{\mathrm{I},1}^H,\cdots,\boldsymbol{h}_{\mathrm{I},K}^H]$.

An IRS is an ultra-thin surface consisting of massive reflective elements whose phase shifts and amplitudes are controlled by simple programmable PIN or varactor diodes [12]. We will assume the use of PIN diodes, whose ON/OFF behavior only allows for discrete phase shifts. Furthermore, the DIRS reflecting phase shifts $\varphi_{\mathrm{D},r}$ $(r=1,\cdots,N_{\mathrm{D}})$ are randomly selected from a discrete set $\mathcal{Q}_D$ with b_1-bit quantized phase shifts $\{\omega_1,\cdots,\omega_{2^{b_1}}\}$ and follow a stochastic distribution $\mathcal{F}$, i.e., $\varphi_{\mathrm{D},r}\sim\mathcal{F}(\mathcal{Q}_{\mathrm{D}})$. Meanwhile, the IRS reflecting phase shifts $\varphi_{\mathrm{I},r}$ $(r=1,\cdots,N_{\mathrm{I}})$ also come from a discrete and finite set $\mathcal{Q}_I=\{\psi_1,\cdots,\psi_{2^{b_2}}\}$ with b_2-bit quantized phase shifts.

In a channel coherence interval, prior to data transmission, CSI for $\mathbf{H}_{\mathrm{IU}}$, $\mathbf{H}_{\mathrm{AI}}$, and $\mathbf{H}_{\mathrm{d}}$ is acquired during the *RPT* phase [13], [14]. We assume that the DIRS remains "silent" during the *RPT* phase [6], [7], i.e., the DIRS-jammed channel $\mathbf{H}_{\mathrm{D}}(t)$ does not exist during the *RPT* phase. As long as the period during which the DIRS phase shifts are changing is about the same as the length of the *RPT* phase, the legitimate AP cannot acquire any useful knowledge about $\mathbf{H}_{\mathrm{D}}(t)$ via retraining [8]. Therefore, the temporal DIRS-based FPJ introduces ACA interference during the *DT* phase.

To quantify the impact of the DIRS-based ACA interference, we also define the SJNR for LU_k represented by η_k with reference to the work in [7], [8] and the definition of the signal-to-leakage-plus-noise ratio [15], i.e.,

$$\eta_k = \frac{\mathbb{E}\left[\left|\boldsymbol{h}_{DT,k}^H \boldsymbol{w}_k\right|^2\right]}{\sum\limits_{u\neq k}\mathbb{E}\left[\left|\boldsymbol{h}_{DT,u}^H \boldsymbol{w}_k\right|^2\right] + \sigma^2}. \tag{2}$$

Following [15], we use a sum-rate-like metric based on the SJNR instead of signal-to-interference-plus-noise ratio: $R = \sum_{k=1}^{K}\log_2(1+\eta_k)$. We will refer to this as the SJNR rate.

B. Channel Model and Problem Formulation

Based on the existing work in [5]–[8], a DIRS should be positioned near the legitimate AP to maximize the jamming impact. Moreover, the DIRS must contain a large number of reflective elements to cope with the multiplicative large-scale channel fading in the DIRS-jammed channel. Therefore, the AP-DIRS channel $\mathbf{H}_{\mathrm{AD}}$ is constructed based on the near-field model [16], i.e.,

$$\mathbf{H}_{\mathrm{AD}} = \sqrt{\mathscr{L}_{\mathrm{AD}}}\left(\sqrt{\frac{\varepsilon_{\mathrm{AD}}}{1+\varepsilon_{\mathrm{AD}}}}\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{LOS}} + \sqrt{\frac{1}{1+\varepsilon_{\mathrm{AD}}}}\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{NLOS}}\right), \tag{3}$$

where $\mathscr{L}_{\mathrm{AD}}$ denotes the large-scale channel fading between the AP and the DIRS, and $\varepsilon_{\mathrm{AD}}$ represents the Rician factor for $\mathbf{H}_{\mathrm{AD}}$, and $\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{NLOS}}$ is assumed to follow Rayleigh fading [17], [18], i.e., $\left[\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{NLOS}}\right]_{r,n} \sim \mathcal{CN}(0,1), r = 1,\cdots,N_{\mathrm{D}}$ and $n = 1,\cdots,N_{\mathrm{A}}$. The elements of the line-of-sight (LOS) channel $\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{NLOS}}$ are given by [7], [8], [16]

$$\left[\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{NLOS}}\right]_{r,n} = e^{-j\frac{2\pi}{\lambda}(D_n^r - D_n)}, \tag{4}$$

where λ is the wavelength of the transmit signals, and D_n^r and D_n represent the distance between the n-th antenna and the r-th DIRS reflective element and the distance between the n-th antenna and the centre (origin) of the DIRS, respectively. We will assume that the distances between two adjacent transmit antennas and two adjacent DIRS reflective elements are both $d = \lambda/2$.

The DIRS-LU channel $\mathbf{H}_{\mathrm{DU}}$ and the direct AP-LU channel $\mathbf{H}_{\mathrm{AU}}$ are modeled based on Rayleigh fading:

$$\mathbf{H}_{\mathrm{DU}} = \mathbf{L}_{\mathrm{DU}}^{\frac{1}{2}}\widehat{\mathbf{H}}_{\mathrm{DU}} = \left[\sqrt{\mathscr{L}_{\mathrm{DU},1}}\widehat{\boldsymbol{h}}_{\mathrm{DU},1},\cdots,\sqrt{\mathscr{L}_{\mathrm{DU},K}}\widehat{\boldsymbol{h}}_{\mathrm{DU},K}\right], \tag{5}$$

$$\mathbf{H}_{\mathrm{AU}} = \mathbf{L}_{\mathrm{AU}}^{\frac{1}{2}}\widehat{\mathbf{H}}_{\mathrm{AU}} = \left[\sqrt{\mathscr{L}_{\mathrm{AU},1}}\widehat{\boldsymbol{h}}_{\mathrm{AU},1},\cdots,\sqrt{\mathscr{L}_{\mathrm{AU},K}}\widehat{\boldsymbol{h}}_{\mathrm{AU},K}\right], \tag{6}$$

where the elements of $\mathbf{L}_{\mathrm{DU}} = \mathrm{diag}(\mathscr{L}_{\mathrm{DU},1},\cdots,\mathscr{L}_{\mathrm{DU},K})$ and $\mathbf{L}_{\mathrm{AU}} = \mathrm{diag}(\mathscr{L}_{\mathrm{AU},1},\cdots,\mathscr{L}_{\mathrm{AU},K})$ denote the large-scale channel fading coefficients, which are assumed to be independent. The elements of $\widehat{\mathbf{H}}_{\mathrm{DU}}$ and $\widehat{\mathbf{H}}_{\mathrm{AU}}$ are assumed to be independent and identically distributed (i.i.d.) Gaussian random variables [18], i.e., $\left[\widehat{\mathbf{H}}_{\mathrm{DU}}\right]_{r,k}, \left[\widehat{\mathbf{H}}_{\mathrm{AU}}\right]_{n,k} \sim \mathcal{CN}(0,1), r = 1,\cdots,N_{\mathrm{D}}$, $n = 1,\cdots,N_{\mathrm{A}}$, and $k = 1,\cdots,K$.

The legitimate IRS is carefully pre-positioned, ensuring that the cascaded IRS-aided AP-LU links are not blocked [17], [19]. Therefore, the AP-IRS channel $\mathbf{H}_{\mathrm{AI}}$ and the IRS-LU channel $\mathbf{H}_{\mathrm{IU}}$ are assumed to follow Rician fading, which is modeled as [5], [17], [19]

$$\mathbf{H}_{\mathrm{AI}} = \sqrt{\mathscr{L}_{\mathrm{AI}}}\left(\sqrt{\frac{\varepsilon_{\mathrm{AI}}}{1+\varepsilon_{\mathrm{AI}}}}\widehat{\mathbf{H}}_{\mathrm{AI}}^{\mathrm{LOS}} + \sqrt{\frac{1}{1+\varepsilon_{\mathrm{AI}}}}\widehat{\mathbf{H}}_{\mathrm{AI}}^{\mathrm{NLOS}}\right), \tag{7}$$

$$\mathbf{H}_{\mathrm{IU}} = \left[\sqrt{\mathscr{L}_{\mathrm{IU},1}}\widehat{\boldsymbol{h}}_{\mathrm{IU},1},\cdots,\sqrt{\mathscr{L}_{\mathrm{IU},K}}\widehat{\boldsymbol{h}}_{\mathrm{IU},K}\right], \tag{8}$$

where $\mathscr{L}_{\mathrm{AI}}$ and $\mathscr{L}_{\mathrm{IU},k}$ respectively represent the large-scale channel fading coefficients between the AP and the IRS and between the IRS and LU_k, and $\varepsilon_{\mathrm{AI}}$ is the Rician factor for $\mathbf{H}_{\mathrm{AI}}$. Moreover, $\widehat{\boldsymbol{h}}_{\mathrm{IU},k}$ can be expressed by

$$\widehat{\boldsymbol{h}}_{\mathrm{IU},k} = \left(\sqrt{\frac{\varepsilon_{\mathrm{IU},k}}{1+\varepsilon_{\mathrm{IU},k}}}\widehat{\boldsymbol{h}}_{\mathrm{IU},k}^{\mathrm{LOS}} + \sqrt{\frac{1}{1+\varepsilon_{\mathrm{IU}}}}\widehat{\boldsymbol{h}}_{\mathrm{IU},k}^{\mathrm{NLOS}}\right). \tag{9}$$

where $\varepsilon_{\mathrm{IU},k}$ denotes the Rician factor of the channel $\boldsymbol{h}_{\mathrm{IU},k}, k = 1,\cdots,K$. The LOS channels $\widehat{\mathbf{H}}_{\mathrm{AI}}^{\mathrm{LOS}}$ and $\widehat{\boldsymbol{h}}_{\mathrm{IU},k}^{\mathrm{LOS}}$ are written as [5], [17]

$$\widehat{\mathbf{H}}_{\mathrm{AI}}^{\mathrm{LOS}} = \sqrt{N_{\mathrm{I}}N_{\mathrm{A}}}\boldsymbol{\alpha}_{\mathrm{I}}(\vartheta,\theta)\,\boldsymbol{\alpha}_{\mathrm{A}}^H(\phi), \tag{10}$$

$$\widehat{\boldsymbol{h}}_{\mathrm{IU},k}^{\mathrm{LOS}} = \sqrt{N_{\mathrm{I}}}\boldsymbol{\alpha}_{\mathrm{I}}(\vartheta_k,\theta_k), \tag{11}$$

where $\boldsymbol{\alpha}_{\mathrm{A}}$ and $\boldsymbol{\alpha}_{\mathrm{I}}$ represent the array responses.

In this work, we aim to maximize the performance metric R obtained from the MU-MISO system by optimizing the transmit precoder $\mathbf{W} = [\boldsymbol{w}_1,\cdots,\boldsymbol{w}_k]$ and the IRS reflecting vector $\boldsymbol{\varphi}_{\mathrm{I}}$. For a practical IRS, its gains are the tion of its corresponding phase shifts [20]. Mathematically, the optimization problem is expressed as

$$(\mathrm{P1}): \max_{\boldsymbol{\varphi}_{\mathrm{I}},\mathbf{W}} R = \sum_{k=1}^{K}\log_2(1+\eta_k) \tag{12}$$

$$\text{s.t. } \|\mathbf{W}\|^2 \le P_0, \tag{13}$$

$$\boldsymbol{\varphi}_{\mathrm{I}} = \mathrm{diag}(e^{\varphi_{\mathrm{I},1}},\cdots,e^{\varphi_{\mathrm{I},N_{\mathrm{I}}}}), \forall\varphi_{\mathrm{I},r} \in \mathcal{Q}_I. \tag{14}$$

(P1) is a typical mixed integer nonlinear programming (MINLP) problem, which is NP-hard. In addition, the DIRS-jammed channel $\mathbf{H}_{\mathrm{D}}$ includes the time-varying i.i.d. random variables $\{\varphi_{\mathrm{D},1}(t),\cdots,\varphi_{\mathrm{D},N_{\mathrm{D}}}(t)\}$ in each channel coherence interval. Moreover, the legitimate AP cannot train to learn the CSI of the DIRS-related channels $\mathbf{H}_{\mathrm{AD}}$ and $\mathbf{H}_{\mathrm{DU}}$. These difficulties make (P1) very challening to solve. We assume that the perfect CSI of the AP-IRS channel $\mathbf{H}_{\mathrm{AI}}$, the IRS-LU channel $\mathbf{H}_{\mathrm{IU}}$, and the direct AP-LU channel $\mathbf{H}_{\mathrm{AU}}$ is available via training with the IRS and the LUs during the *RPT* phase [21], as imperfect CSI is not a primary concern in the jamming scenario here, and its impact has also been thoroughly studied [15], [22].

III. IRS-Enhanced Anti-Jamming Precoding Against DIRS-Based FPJ

A. Active Beamforming Design

Based on the definition of η_k in (2), the time-varying reflecting vector $\boldsymbol{\varphi}_{\mathrm{D}}(t)$ and the lack of CSI of the DIRS-related channels $\mathbf{H}_{\mathrm{AD}}$ and $\mathbf{H}_{\mathrm{DU}}$, it is infeasible to solve (P1) directly.

To find a more tractable solution, we derive a more-explicit expression for η_k.

Proposition 1: Under the condition that $\boldsymbol{h}_{\mathrm{I},k}$, $\boldsymbol{h}_{\mathrm{D},k}(t)$, and $\boldsymbol{h}_{\mathrm{d},k}$ are independent and $\boldsymbol{h}_{\mathrm{I},k}$ and $\boldsymbol{h}_{\mathrm{d},k}$ are unchanged during channel coherence time, η_k defined in (2) reduces to

$$\overline{\eta}_k = \frac{\boldsymbol{w}_k^H\left(\left(\boldsymbol{h}_{\mathrm{I},k}+\boldsymbol{h}_{\mathrm{d},k}\right)\left(\boldsymbol{h}_{\mathrm{I},k}+\boldsymbol{h}_{\mathrm{d},k}\right)^H+\beta_k\mathbf{I}_{N_\mathrm{A}}\right)\boldsymbol{w}_k}{\sum\limits_{u\neq k}\boldsymbol{w}_k^H\left(\left(\boldsymbol{h}_{\mathrm{I},u}+\boldsymbol{h}_{\mathrm{d},u}\right)\left(\boldsymbol{h}_{\mathrm{I},u}+\boldsymbol{h}_{\mathrm{d},u}\right)^H+\beta_k\mathbf{I}_{N_\mathrm{A}}\right)\boldsymbol{w}_k+\sigma^2}, \quad \text{as } N_\mathrm{D}\to\infty, \tag{15}$$

where $\beta_k = \mathscr{L}_\mathrm{G}\mathscr{L}_{\mathrm{I},k}N_\mathrm{D}$, and $\mathbf{I}_{N_\mathrm{A}}$ is an $N_\mathrm{A}\times N_\mathrm{A}$ unit matrix.

Proof: See Appendix A. ∎

Consequently, (P1) reduces to the following form:

$$(\mathrm{P2}): \max_{\boldsymbol{\varphi}_\mathrm{I},\mathbf{W}} \overline{R} = \sum_{k=1}^{K}\log_2(1+\overline{\eta}_k) \tag{16}$$
$$\text{s.t. (13) and (14).}$$

When the IRS reflecting vector $\boldsymbol{\varphi}_\mathrm{I}$ is determined, (P2) reduces to the following subproblem:

$$(\mathrm{P2-S1}): \max_{\mathbf{W}} \overline{R}\big|_{\boldsymbol{\varphi}_\mathrm{I}} = \sum_{k=1}^{K}\log_2\left(1+\overline{\eta}_k|_{\boldsymbol{\varphi}_\mathrm{I}}\right) \tag{17}$$
$$\text{s.t. (13).}$$

Based on the work in [7], [8], an anti-jamming precoder $\mathbf{W}^\mathrm{o}$ for (P2 − S1) which can maximize the SJNRs is given by

$$\boldsymbol{w}_k^\mathrm{o} \propto \max.\text{eigenvector}\left(\mathbf{A}_k\right), \tag{18}$$

where

$$\mathbf{A}_k = \left(\boldsymbol{h}_{\mathrm{L},k}\boldsymbol{h}_{\mathrm{L},k}^H+\widetilde{\beta}_k\mathbf{I}_{N_\mathrm{A}}\right)\left(\widetilde{\mathbf{H}}_{\mathrm{L},k}\widetilde{\mathbf{H}}_{\mathrm{L},k}^H+\left(\frac{\sigma^2K}{P_0}+\sum_{u\neq k}\widetilde{\beta}_u\right)\mathbf{I}_{N_\mathrm{A}}\right)^{-1}, \tag{19}$$

$\widetilde{\mathbf{H}}_{\mathrm{L},k} = [\boldsymbol{h}_{\mathrm{L},1},\cdots,\boldsymbol{h}_{\mathrm{L},k-1},\boldsymbol{h}_{\mathrm{L},k+1},\cdots,\boldsymbol{h}_{\mathrm{L},K}]$, $\boldsymbol{h}_{\mathrm{L},k} = \boldsymbol{h}_{\mathrm{I},k} + \boldsymbol{h}_{\mathrm{d},k}$, and $\{\widetilde{\beta}_k\}_{k=1}^K$ are estimates of $\{\beta_k\}_{k=1}^K$ in (15). A frame structure has been designed in [8] to acquire the estimates since it is unrealistic for the AP to know the values of $\{\beta_k\}_{k=1}^K$ in advance. Therefore, only the estimated $\{\widetilde{\beta}_k\}_{k=1}^K$ can be used in the design of the IRS-enhanced anti-jamming precoder.

B. Passive Beamforming Design

The work in [2] showed that the legitimate AP can increase the strength of the transmit signals to counter the DIRS-based ACA attacks. Inspired by this investigation, we compute $\boldsymbol{\varphi}_\mathrm{I}^\mathrm{o}$ by maximising the overall effective channel power P_E, where the overall effective channel is $\mathbf{H}_\mathrm{E} = \mathbf{H}_\mathrm{I} + \mathbf{H}_\mathrm{AU}$, i.e.,

$$(\mathrm{P3}): \max_{\boldsymbol{\varphi}_\mathrm{I}} P_\mathrm{E} = \|\mathbf{H}_\mathrm{E}\|^2 \tag{20}$$
$$\text{s.t. (14).} \tag{21}$$

However, (P3) is still difficult to solve due to the discrete variables $\{\varphi_{\mathrm{I},r}\}_{r=1}^{N_\mathrm{I}}$. Therefore, we further relax $\{\varphi_{\mathrm{I},r}\}_{r=1}^{N_\mathrm{I}}$ to continuous variables. As a result, (P3) is relaxed to

$$(\mathrm{P3-R1}): \max_{\boldsymbol{\varphi}_\mathrm{I}} P_\mathrm{E} = \|\mathbf{H}_\mathrm{E}\|^2 \tag{22}$$
$$\text{s.t.}\ \boldsymbol{\varphi}_\mathrm{I} = \mathrm{diag}\left(e^{\varphi_{\mathrm{I},1}},\cdots,e^{\varphi_{\mathrm{I},N_\mathrm{I}}}\right), \forall\varphi_{\mathrm{I},r}\in[0,2\pi]. \tag{23}$$

Algorithm 1 IRS-enhanced anti-jamming precoding algorithm

Input: $\mathbf{H}_\mathrm{IU}$, $\mathbf{H}_\mathrm{AI}$, $\mathbf{H}_\mathrm{AU}$, $\{\widetilde{\beta}_k\}_{k=1}^K$, K, N_A, and P_0.
Initialize: $\boldsymbol{\Phi}_\mathrm{I} = \mathbf{I}_{N_\mathrm{I}}$.
1: Compute $\boldsymbol{\varphi}_\mathrm{I}^{RCG}$ by solving (P3 − R1);
2: Calculate $\boldsymbol{\varphi}_\mathrm{I}^\mathrm{o}$ by solving (P4);
3: Substitute $\boldsymbol{\varphi}_\mathrm{I}^\mathrm{o}$ to (P2 − S1)
4: Compute $\mathbf{W}^\mathrm{o}$ by (18);
Output: $\mathbf{W}^\mathrm{o}$ and $\boldsymbol{\varphi}_\mathrm{I}^\mathrm{o}$.

The objective function in (22) is a continuous and differentiable function of the relaxed continuous $\boldsymbol{\varphi}_\mathrm{I}$. Furthermore, the constraint in (23) creates a complex circle manifold. Therefore, we can use the RCG algorithm to solve (P3−R1) [6], [23].

1) Riemannian Gradient: The Riemannian gradient $\mathrm{grad}(P_\mathrm{E})$ at the relaxed $\boldsymbol{\varphi}_\mathrm{I}$ is a tangent vector that denotes the greatest decreasing direction of P_E, i.e.,

$$\mathrm{grad}(P_\mathrm{E}) = \nabla(P_\mathrm{E}) - \mathrm{Re}\{\nabla(P_\mathrm{E})\odot\boldsymbol{\varphi}_\mathrm{I}^H\}\odot\boldsymbol{\varphi}_\mathrm{I}, \tag{24}$$

where $\nabla(P_\mathrm{E})$ represents the Euclidean gradient.

2) Search Direction: The tangent vector conjugate to $\mathrm{grad}(P_\mathrm{E})$ can be used as the search direction $\mathcal{D}$, i.e.,

$$\mathcal{D} = -\mathrm{grad}(P_\mathrm{E}) + \rho_1(\tilde{\mathcal{D}} - \mathrm{Re}\{\tilde{\mathcal{D}}\odot\boldsymbol{\varphi}_\mathrm{I}^H\}\odot\boldsymbol{\varphi}_\mathrm{I}), \tag{25}$$

where ρ_1 and $\tilde{\mathcal{D}}$ denote the conjugate gradient update parameter and the previous search direction, respectively.

3) Retraction: The tangent vector is retracted back to the complex circle manifold described by (23), i.e.,

$$\frac{(\boldsymbol{\varphi}_\mathrm{I}+\rho_2\mathcal{D})_r}{|(\boldsymbol{\varphi}_\mathrm{I}+\rho_2\mathcal{D})_r|} \mapsto \varphi_{\mathrm{I},r}, \tag{26}$$

where ρ_2 denotes the Armijo step size and $r = 1,\cdots,N_\mathrm{I}$.

Based on the continuous $\boldsymbol{\varphi}_\mathrm{I}^{RCG}$ obtained from (P3 − R1), the discrete solution $\boldsymbol{\varphi}_\mathrm{I}^\mathrm{o}$ is found by choosing the closest value in the discrete phase set:

$$(\mathrm{P4}): \boldsymbol{\varphi}_\mathrm{I}^\mathrm{o} = \arg\min_{\boldsymbol{\varphi}_\mathrm{I}} \left\|\boldsymbol{\varphi}_\mathrm{I} - \boldsymbol{\varphi}_\mathrm{I}^{RCG}\right\|^2 \tag{27}$$
$$\text{s.t. (14).}$$

Based on the computed $\boldsymbol{\varphi}_\mathrm{I}^\mathrm{o}$, we then calculate $\mathbf{W}^\mathrm{o}$ by (18). The pseudo-code for the proposed IRS-enhanced anti-jamming precoding algorithm is given in Algorithm 1.

IV. Simulation Results and Discussion

In this section, numerical results are presented to evaluate the effectiveness of the IRS-enhanced anti-jamming precoder. We consider an MU-MISO system in which the legitimate AP equipped with 32 antennas is assisted by a (16×8)-element IRS to communicate with 16 single-antenna LUs, and the DIRS has (64×32) elements, i.e., $N_\mathrm{A} = 32$, $N_\mathrm{I} = 128$, $K = 16$, and $N_\mathrm{D} = 2048$. Similar to [5]–[8], we further assume that a one-bit DIRS is implemented, where $\varphi_{\mathrm{D},r}\in\mathcal{Q}_\mathrm{D} = \left\{\frac{\pi}{9},\frac{6\pi}{5}\right\}$. Meanwhile, the IRS phase shifts are quantified by 2 bits, i.e., $\varphi_{\mathrm{I},r}\in\mathcal{Q}_\mathrm{I} = \left\{0,\frac{\pi}{2},\pi,\frac{3\pi}{2}\right\}$.

The centers of the legitimate AP, the legitimate IRS, and the DIRS are located at (2m, 0m, 5m), (10m, 280m, 5m), and

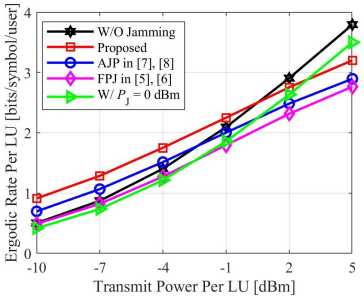

Fig. 2. Ergodic rate per LU vs transmit power per LU.

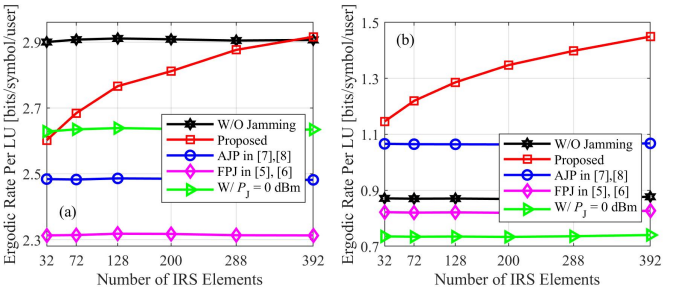

Fig. 3. Relationship between the ergodic rate per LU and the number of IRS reflective elements for different benchmarks, where the transmit power per LU is (a) 0 dBm and (b) -7 dBm, respectively.

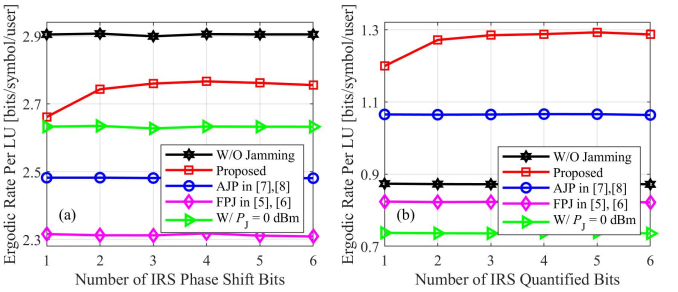

Fig. 4. Relationship between the ergodic rate per LU and the number of IRS quantified bits for different benchmarks, where the transmit power per LU is (a) 0 dBm and (b) -7 dBm, respectively.

(2m, 0m, 2m), respectively. The LUs are randomly distributed in a circular region centred at (0m, 300m, 0m) with a radius of 20m. According to the 3GPP propagation model [25], the propagation parameters of the wireless channels modelled in Section II-B are described as follows: $\mathscr{L}_{\mathrm{AD}}, \mathscr{L}_{\mathrm{AI}}, \mathscr{L}_{\mathrm{IU},k} = 35.6 + 22\log_{10}(d_i)$ and $\mathscr{L}_{\mathrm{AU},k}, \mathscr{L}_{\mathrm{DU},k} = \mathscr{L}_{\mathrm{I},k} = 32.6 + 36.7\log_{10}(d_i)$, where $d_i \in \{d_{\mathrm{AD}}, d_{\mathrm{AI}}, d_{\mathrm{IU},k}, d_{\mathrm{AU},k}, d_{\mathrm{DU},k}\}$ is the propagation distance. Moreover, the AWGN variance is $\sigma^2 = -170 + 10\log_{10}(BW)$ dBm, and the bandwidth is $BW = 180$ kHz. If not otherwise specified, the above parameters default to these values.

Herein, we show the ergodic rate per LU (i.e., $\frac{R}{K}$) achieved by the following benchmarks: 1) the rate resulting from a traditional MU-MISO system without jamming attacks (W/O Jamming), 2) the rate resulting from an MU-MISO system using the IRS-enhanced anti-jamming precoder presented in Algorithm 1 (Proposed), 3) the rate resulting from an MU-MISO system using the anti-jamming precoder given in [7], [8] (AJP in [7], [8]), 4) the rate resulting from an MU-MISO system with a temporal DIRS-based FPJ [5], [6] (FPJ in [5], [6]) without any anti-jamming, and 5) the rate resulting from an MU-MISO system with an AJ located at (2m, 0m, 5m) broadcasting AWGN signals with 0 dBm jamming power (W/ $P_{\mathrm{J}} = 0$ dBm).

Fig. 2 illustrates the ergodic rate as a function of the transmit power per LU. We can see that the proposed IRS-enhancedanti-jamming precoder achieves better ergodic rates per LU than the anti-jamming precoder designed in [7], [8]. The work in [7], [8] has shown that the anti-jamming precoder can to some extent use the DIRS-jammed channels to increase the the ergodic rates of LUs. As a result, when the transmit power per LU (i.e., $\frac{P_0}{K}$) is low, the rate from the anti-jamming precoder in [7], [8] is higher than that without any jamming. The precoder proposed in this paper also achieves some gain from the DIRS-jammed channels, and it improves the rate by exploiting the legitimate IRS. Therefore, the proposed IRS-enhanced anti-jamming precoder achieves better performance compared to the work in [7], [8].

Fig. 3 (a) and (b) illustrate the influence of the size of the legitimate IRS for high (0 dBm) and low (-7 dBm) transmit power cases, respectively. As the number of IRS reflective elements increases, the impact of the DIRS-based ACA interference can gradually be diminished out even for high transmit power. However, the slope of the ergodic rate curve over the proposed precoder decreases as the number of IRS reflective elements continues to increase. We see that the proposed IRS-enhanced anti-jamming precoder provides a possible approach to mitigate the DIRS-based ACA interference.

Fig. 4 illustrates the relationship between the ergodic rate per LU and the number of phase shift quantization bits. We can see that the rate of the proposed IRS-enhanced anti-jamming precoder increases only slightly when the number of quantization bits is greater than 3. The difference between the rate uusing a 2-bit versus a 3-bit IRS is also marginal. To offer a good compromise between the ergodic rate per LU and the complexity of solving (P4), we suggest that using a legitimate IRS with 2-bit phase shift quantization is sufficient.

V. Conclusions

In this paper, an IRS-enhanced anti-jamming precoder was proposed. Since the AP can not access the CSI of the DIRS-related channels and acquire knowledge of the time-varying DIRS phase shifts in real-world applications, we maximized the received signal power by using the RCG algorithm to design the passive beamforming at the IRS. Moreover, based on our investigations, using a 2-bit IRS provided a good trade-off between computational complexity and performance. Compared with the previous work in [7], [8], the proposed IRS-enhanced anti-jamming precoder can better mitigate the impact of DIRS-based ACA interference at high transmit power. In particular, the simulations showed that using an IRS that is one-seventh the size of the DIRS can essentially

suppress the impact of DIRS-based fully-passive jamming at 0 dBm transmit power.

APPENDIX A
PROOF OF PROPOSITION 1

According to (3) and (6), $[\mathbf{H}_{\mathrm{D}}(t)]_{k,n}$ can be rewritten as

$$[\mathbf{H}_{\mathrm{D}}(t)]_{k,n} = \sqrt{\frac{\varepsilon_n \mathscr{L}_{\mathrm{AD}} \mathscr{L}_{\mathrm{DU},k}}{\varepsilon_n + 1}} \widehat{\boldsymbol{h}}_{\mathrm{DU},k} \odot \boldsymbol{\varphi}_{\mathrm{D}}(t) \left[\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{LOS}}\right]_{:,n} + \sqrt{\frac{\mathscr{L}_{\mathrm{AD}} \mathscr{L}_{\mathrm{DU},k}}{\varepsilon_n + 1}} \widehat{\boldsymbol{h}}_{\mathrm{DU},k} \odot \boldsymbol{\varphi}_{\mathrm{D}}(t) \left[\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{NLOS}}\right]_{:,n}, \quad (28)$$

where $\odot$ represents the Hadamard product. Furthermore,

$$[\mathbf{H}_{\mathrm{D}}(t)]_{k,n} = \sqrt{\frac{\varepsilon_n \mathscr{L}_{\mathrm{AD}} \mathscr{L}_{\mathrm{DU},k}}{\varepsilon_n + 1}} \sum_{r=1}^{N_{\mathrm{D}}} \left(\left[\widehat{\boldsymbol{h}}_{\mathrm{DU},k}\right]_r e^{j\varphi_{\mathrm{D},r}(t)} \left[\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{LOS}}\right]_{r,n} \right) + \sqrt{\frac{\mathscr{L}_{\mathrm{AD}} \mathscr{L}_{\mathrm{DU},k}}{\varepsilon_n + 1}} \sum_{r=1}^{N_{\mathrm{D}}} \left(\left[\widehat{\boldsymbol{h}}_{\mathrm{DU},k}\right]_r e^{j\varphi_{\mathrm{D},r}(t)} \left[\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{NLOS}}\right]_{r,n} \right). \quad (29)$$

Conditioned on the fact that the random variables in (29) are independent, we have the following expectations

$$\mathbb{E}\left[\left[\widehat{\boldsymbol{h}}_{\mathrm{DU},k}\right]_r e^{j\varphi_{\mathrm{D},r}(t)} \left[\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{LOS}}\right]_{r,n} \right] = 0, \quad (30)$$

$$\mathbb{E}\left[\left[\widehat{\boldsymbol{h}}_{\mathrm{DU},k}\right]_r e^{j\varphi_{\mathrm{D},r}(t)} \left[\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{NLOS}}\right]_{r,n} \right] = 0. \quad (31)$$

Moreover, the variances of $([\widehat{\boldsymbol{h}}_{\mathrm{DU},k}]_r e^{j\varphi_{\mathrm{D},r}(t)} [\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{LOS}}]_{r,n})$ and $([\widehat{\boldsymbol{h}}_{\mathrm{DU},k}]_r e^{j\varphi_{\mathrm{D},r}(t)} [\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{NLOS}}]_{r,n})$ are calculated as

$$\mathrm{Var}\left[\left[\widehat{\boldsymbol{h}}_{\mathrm{DU},k}\right]_r e^{j\varphi_{\mathrm{D},r}(t)} \left[\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{LOS}}\right]_{r,n} \right] = 1, \quad (32)$$

$$\mathrm{Var}\left[\left[\widehat{\boldsymbol{h}}_{\mathrm{DU},k}\right]_r e^{j\varphi_{\mathrm{D},r}(t)} \left[\widehat{\mathbf{H}}_{\mathrm{AD}}^{\mathrm{NLOS}}\right]_{r,n} \right] = 1. \quad (33)$$

Based on the Lindeberg-Lévy central limit theorem, the elements $[\mathbf{H}_{\mathrm{D}}(t)]_{k,n}$ converge in distribution to a Gaussian distribution with zero mean and variance β_k when the number of the DIRS reflective elements is large enough, i.e.,

$$[\mathbf{H}_{\mathrm{D}}(t)]_{k,n} \xrightarrow{\mathrm{d}} \mathcal{CN}(0, \beta_k), \text{as } N_{\mathrm{D}} \to \infty, \quad (34)$$

where $\beta_k = \mathscr{L}_{\mathrm{G}} \mathscr{L}_{\mathrm{I},k} N_{\mathrm{D}}$. Substituting (34) to (2), we can reduce η_k to the form in (15).

REFERENCES

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quarter 2014.

[2] H. Huang, L. Dai, H. Zhang, C. Zhang, Z. Tian, Y. Cai, A. L. Swindlehurst, and Z. Han, "DISCO might not be funky: Random intelligent reflective surface configurations that attack," *arXivpreprint arXiv:2310.00687*, Oct. 2023.

[3] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surv. Tut.*, vol. 24, no. 2, pp. 767–809, 2nd Quarter 2022.

[4] H. Wang, Z. Han, and A. L. Swindlehurst, "Channel reciprocity attacks using intelligent surfaces with non-diagonal phase shifts," *arXivpreprint arXiv: 2309.11665*, Sep. 2023.

[5] H. Huang, Y. Zhang, H. Zhang, C. Zhang, and Z. Han, "Illegal intelligent reflecting surface based active channel aging: When jammer can attack without power and CSI," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, pp. 11018–11022, Aug. 2023.

[6] H. Huang, Y. Zhang, H. Zhang, Y. Cai, A. L. Swindlehurst, and Z. Han, "Disco intelligent reflecting surfaces: Active channel aging for fully-passive jamming attacks," *IEEE Trans. Wireless Commun.*, vol. 23, no. 1, pp. 806–819, Jan. 2024.

[7] H. Huang, H. Zhang, Y. Cai, A. L. Swindlehurst, and Z. Han, "An anti-jamming strategy for disco intelligent reflecting surfaces based fully-passive jamming attacks," in *Proc. IEEE Global Commun. Conf. (Globecom'23)*, Kuala Lumpur, Malaysia, Dec. 2023.

[8] H. Huang, L. Dai, H. Zhang, Z. Tian, Y. Cai, C. Zhang, A. L. Swindlehurst, and Z. Han, "Anti-jamming precoding for disco intelligent reflecting surfaces based fully-passive jamming attacks," *IEEE Trans. Wireless Commun.*, early access, Feb. 2024, doi: 10.1109/TWC.2024.3360728.

[9] G. Li, P. Staat, H. Li, M. Heinrichs, C. Zenger, R. Kronberger, H. Elders-Boll, C. Paar, A. Hu, "RIS-jamming: Breaking key consistency in channel reciprocity-based key generation," *arXivpreprint arXiv: arXiv:2303.07015*, Mar. 2023.

[10] P. Staat, H. Elders-Boll, M. Heinrichs, C. Zenger, and C. Paar, "Mirror, mirror on the wall: Wireless environment reconfiguration attacks based on fast software-controlled surfaces," in *Proc. 2022 ACM on Asia Conf. Comput. Commun. Secur., (ASIA CCS '22)*, New York, May 2022.

[11] L. Hu, G. Li, H. Luo, and A. Hu, "On the RIS manipulating attack and its countermeasures in physical-layer key generation," in *Proc. Veh. Technol. Conf., (VTC'21-Fall)*, Norman, OK, Sept. 2021.

[12] T. Cui, M. Qi, X. Wan, J. Zhao, and Q. Cheng, "Coding metamaterials, digital metamaterials and programmable metamaterials," *Light-Sci. Appl.*, vol. 3, e218, Oct. 2014.

[13] X. Zhou, B. Maham, and A. Hjϕrungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[14] X. Wei, D. Shen, and L. Dai, "Channel estimation for RIS assisted wireless communications: Part I-fundamentals, solutions, and future opportunities," *Commun. Lett.*, vol. 25, no. 5, pp. 1398–1402, May 2021.

[15] T. X. Tran and K. C. Teh, "Spectral and energy efficiency analysis for SLNR precoding in massive MIMO systems with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 4017–4027, Jun. 2018.

[16] M. Cui and L. Dai, "Channel estimation for extremely large-scale MIMO: Far-field or near-field?" *IEEE Trans. Commun.*, vol. 70, no. 4, pp. 2663–2677, Apr. 2022.

[17] 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, Aug. 2019.

[18] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge Univ. Press, Cambridge, U.K., 2005.

[19] H. Huang, Y. Zhang, H. Zhang, Z. Zhao, C. Zhang, and Z. Han, "Multi-IRS-aided millimeter-wave multi-user MISO systems for power minimization using generalized Benders decomposition," *IEEE Trans. Wireless Commun.*, vol. 22, no. 11, pp. 7873–7886, Nov. 2023.

[20] S. Zeng, H. Zhang, B. Di, Z. Han, and L. Song, "Reconfigurable intelligent surface (RIS) assisted wireless coverage extension: RIS orientation and location optimization," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 269–273, Jan. 2021.

[21] H. Guo and V. K. N. Lau, "Uplink cascaded channel estimation for intelligent reflecting surface assisted multiuser MISO systems," *IEEE Trans. Signal Process.*, vol. 70, pp. 3964–3977, Jul. 2022.

[22] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Trans. Wireless Commun.* vol. 61, no. 4, pp. 1436–1449, Apr. 2013.

[23] H. Guo, Y.-C. Liang, J. Chen, and E. G. Larsson, "Weighted sum-rate maximization for reconfigurable intelligent surface aided wireless networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 3064–3076, May 2020.

[24] E. Björnson, M. Bengtsson, and B. Ottersten, "Optimal multiuser transmit beamforming: A difficult problem with a simple solution structure," *IEEE Signal Process. Mag.*, vol. 31, no. 4, pp. 142–148, Jun. 2014.

[25] Further Advancements for E-UTRA Physical Layer Aspects (Release 9), document 3GPP TS 36.814, Mar. 2010.