Disco Intelligent Reflecting Surfaces: Active Channel Aging for Fully-Passive Jamming Attacks

Huan Huang, Ying Zhang, *Student Member, IEEE,* Hongliang Zhang, *Member, IEEE,* Yi Cai, *Member, IEEE,* A. Lee Swindlehurst, *Fellow, IEEE,* and Zhu Han, *Fellow, IEEE*

***Abstract*—Due to the open communications environment in wireless channels, wireless networks are vulnerable to jamming attacks. However, existing approaches for jamming rely on knowledge of the legitimate users' (LUs') channels, extra jamming power, or both. To raise concerns about the potential threats posed by illegitimate intelligent reflecting surfaces (IRSs), we propose an alternative method to launch jamming attacks on LUs without either LU channel state information (CSI) or jamming power. The proposed approach employs an adversarial IRS with random phase shifts, referred to as a "disco" IRS (DIRS), that acts like a "disco ball" to actively age the LUs' channels. Such active channel aging (ACA) interference can be used to launch jamming attacks on multi-user multiple-input single-output (MU-MISO) systems. The proposed DIRS-based fully-passive jammer (FPJ) can jam LUs with no additional jamming power or knowledge of the LU CSI, and it can not be mitigated by classical anti-jamming approaches. A theoretical analysis of the proposed DIRS-based FPJ that provides an evaluation of the DIRS-based jamming attacks is derived. Based on this detailed theoretical analysis, some unique properties of the proposed DIRS-based FPJ can be obtained. Furthermore, a design example of the proposed DIRS-based FPJ based on one-bit quantization of the IRS phases is demonstrated to be sufficient for implementing the jamming attack. In addition, numerical results are provided to show the effectiveness of the derived theoretical analysis and the jamming impact of the proposed DIRS-based FPJ.**

***Index Terms*—Jamming attacks, intelligent reflecting surface, multi-user MISO (MU-MISO), channel aging, low-power wireless networks.**

I. Introduction

Due to the intrinsically open communications environment in wireless channels, wireless networks are vulnerable to malicious attacks, and it is difficult to protect transmit signals from eavesdroppers [1]–[3]. To protect the confidentiality of transmit wireless signals, cryptographic techniques are used to prevent eavesdroppers from intercepting transmit information [4]. Secure communications using cryptographic techniques rely on the computational difficulty of the underlying mathematical process required to unravel the codes, and thus secure communications can be achieved unless the eavesdroppers have extensive computing capabilities.

However, malicious attacks such as jamming (also known as DoS-type attacks in the related literature [5], [6]), are more easily implemented than eavesdropping. Generally, jamming attacks can be launched by an active attacker, i.e., an active jammer (AJ), which inflicts intentional interference in order to block the communication between the base station (BS) and the legitimate users (LUs). As discussed below, physical-layer AJs can be divided into the following categories [2]: constant AJs, intermittent AJs, reactive AJs, and adaptive AJs.

1) Constant AJs: A constant AJ continuously broadcasts jamming signals, such as pseudorandom noise or modulated Gaussian waveforms [2]. However, the energy efficiency of a constant AJ is very low. In practice, energy constraints are an inherent drawback of AJs [5], [6]. As a result, the other jamming methods listed below have been investigated [7]–[9].
2) Intermittent AJs: As its name implies, an intermittent AJ only transmits jamming signals from time to time [7]. The jamming effectiveness of the intermittent AJ is limited since it may or may not be active at the time of communication between the BS and LUs.
3) Reactive AJs: To improve the jamming effectiveness, the reactive AJ approach has been proposed, in which jamming attacks are launched only when communication between the BS and LUs is detected [8]. As a result, the jamming effectiveness of a reactive AJ is higher than both constant and intermittent AJs.
4) Adaptive AJs: An adaptive AJ achieves the highest jamming effectiveness by adjusting its jamming power according to the time-varying wireless channels between the BS and the LUs [9]. For example, an adaptive AJ achieves better efficiency by reducing jamming power during deep fades or outages in the BS-LU channel, but this requires updated information about the BS-LU channel which is often difficult to obtain. Typically, an adaptive AJ is used as an idealized approach for benchmarking purposes [2].

Considering the inherent energy constraint of AJs, *can jamming attacks be launched without jamming power*? Thanks to emerging intelligent reflecting surfaces (IRSs) [10]–[16], an adversarial IRS-based passive jammer (PJ) without active pow-

This work was supported by the National Key R&D Program of China (2022YFB2903000) and the National Natural Science Foundation of China (62275185, 62250710164), and partially supported by the U.S. National Science Foundation (CNS-2107216, CNS-2128368, CMMI-2222810, ECCS-2030029, CNS-2107182), US Department of Transportation, Toyota, and Amazon (*Corresponding author: Huan Huang*).

H. Huang and Y. Cai are with Jiangsu Engineering Research Center of Novel Optical Fiber Technology and Communication Network, Suzhou Key Laboratory of Advanced Optical Communication Network Technology, Soochow University, Suzhou, Jiangsu 215006, China (e-mail: hhuang1799@gmail.com, yicai@ieee.org).

Y. Zhang is with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: yzhang1@std.uestc.edu.cn).

H. Zhang is with the School of Electronics, Peking University, Beijing 100871, China (email: hongliang.zhang92@gmail.com).

A. L. Swindlehurst is with the Electrical Engineering and Computer Science Department, University of California, Irvine, CA 92697, USA (e-mail: swindle@uci.edu).

Z. Han is with the Department of Electrical and Computer Engineering at the University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul, South Korea, 446-701 (email: hanzhu22@gmail.com).

er transmission has been proposed for single-user systems [17], which minimizes the received power at the LU by destructively adding the signal reflected from the IRS. However, the channel state information (CSI) of all channels involved must be known at the illegitimate IRS. CSI for the LU is difficult to obtain in practice, especially for an entirely passive IRS [18]–[20].

To acquire the CSI of IRS-aided channels [21], [22], the receivers (users) instead of the IRS send pilot signals to the transmitter, and the transmitter then estimates the IRS-aided channels using methods such as the least squares (LS) algorithm [18]. In other words, if the illegitimate IRS wants to obtain LU CSI, it needs to perform channel estimation jointly with the legitimate BS and LUs. Although an adversarial IRS can ideally impose a harmful impact on wireless networks [23], the assumption that the IRS knows the CSI of all channels involved is unrealistic for practical wireless networks.

Consequently, we ask the following research question: *Can jamming attacks be launched without either jamming power or LU CSI*? The authors of [24] have investigated the downlink of a multi-user MISO (MU-MISO) system jammed by an IRS-based fully-passive jammer (FPJ). The illegitimate IRS-based FPJ can jam LUs without jammer power and CSI by aging all involved channels during both the *pilot transmission (PT)* phase and the *data transmission (DT)* phase.

To raise concerns about the significant potential threats posed by illegitimate IRSs, we propose a disco-IRS-based (DIRS-based) FPJ that can launch jamming attacks on the LUs without relying on either jamming power or LU CSI. The main contributions[1] are summarized as follows:

- We investigate the uplink of an MU-MISO system jammed by the proposed DIRS-based FPJ, which is the first jamming attack proposed that can be launched without jamming power or LU CSI. Before the *DT* phase, channel estimation is performed by the legitimate system during the *PT* phase to provide the CSI for designing the decoder, during which time the illegitimate DIRS remains silent[2]. The DRIS is then activated during the *DT* phase, and the DIRS phase shifts are randomly generated. The DIRS with random phase shifts acts like a "disco ball" distributing the BS energy in random directions. Consequently, the BS-LU channels change rapidly, and serious interference, referred to as active channel aging (ACA) interference, is introduced. Since random IRS reflection coefficients are employed, there is no need for the DIRS to know the LU CSI.
- We perform a theoretical analysis of our proposed DIRS-based FPJ for cases where the BS uses the zero-forcing (ZF) or maximum-ratio combining (MRC) detector. More specifically, lower bounds on the ergodic achievable uplink rates achieved in the presence of the proposed DIRS-based FPJ are determined, which provides an evaluation of the jamming effectiveness of the proposed approach. The simulation results show that the derived lower bounds are close to the obtained ergodic achievable uplink rates.
- Based on the detailed theoretical analysis, we present some unique properties of the proposed DIRS-based FPJ as follows: 1) In contrast to AJs, the jamming impact of the proposed DIRS-based FPJ cannot be mitigated by increasing the transmit power; 2) The jamming impact of the proposed DIRS-based FPJ is not dependent on the quantization nor the distribution of the discrete random DIRS phase shifts.
- We show that the proposed DIRS-based FPJ can be implemented with reflecting elements whose individual phase shifts are determined by a single bit. Since the jamming impact is based on ACA interference introduced by the proposed DIRS, the characteristics of ACA interference, for instance, the carrier frequency and the bandwidth, are the same as the LUs' transmit signals. As a result, classic anti-jamming technologies such as frequency hopping are not valid for the proposed DIRS-based FPJ.

The rest of this paper is organized as follows. In Section II, the uplink of an MU-MISO system jammed by the proposed DIRS-based FPJ is modeled, and the performance metric used to quantify the jamming impact is given. Moreover, some useful results on random variables are presented. In Section III, the theoretical analysis of the proposed DIRS-based FPJ is performed. Then, some properties of the proposed DIRS-based FPJ are obtained based on the derived theoretical analysis. Simulation results are provided in Section IV to show the effectiveness of the derived theoretical analysis and the performance of the proposed DIRS-based FPJ. Finally, the main conclusions are given in Section V.

Notation: In this work, 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., N_t. The superscripts $(\cdot)^H$ and $(\cdot)^T$ denote the Hermitian transpose and the transpose, respectively. Moreover, the symbols $|\cdot|$ and $\|\cdot\|$ denote the absolute value and the Frobenius norm, respectively.

II. System Model and Preliminaries

In Section II-A, we illustrate the uplink of an MU-MISO system jammed by the proposed DIRS-based FPJ and give the general model of the DIRS-based jamming attacks. In Section II-B, we state the performance metric used to quantify the jamming impact of the proposed DIRS-based FPJ. The channel model is presented in Section II-C. In Section II-D, some important results on random variables are presented, which are used for the theoretical analysis in Section III.

A. Disco-IRS-Based Fully-Passive Jammer

Fig. 1 schematically illustrates the uplink of an MU-MISO system jammed by the proposed DIRS-based FPJ, where the DIRS-based jamming attacks on the LUs are launched without relying on either jamming power or LU CSI. The BS is equipped with an N_t-element uniform linear array (ULA) and communicates with K legitimate single-antenna users denoted by $\mathrm{LU}_1, \mathrm{LU}_2, \cdots, \mathrm{LU}_K$. A DIRS comprised of N_{D} reflecting

[1] A portion of this work was published in [24], where we have illustrated the impact of the FPJ on the downlink of an MU-MISO system using only simulations and not a theoretical analysis.

[2] The term "silent" means that the wireless signals are perfectly absorbed by the illegitimate IRS [25].

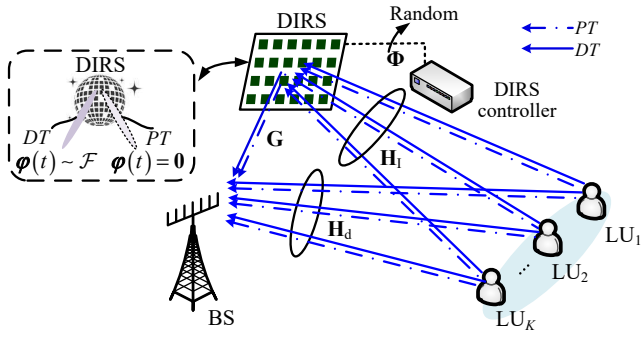

Fig. 1. The uplink of an MU-MISO system jammed by the disco-IRS-based fully-passive jammer (DIRS-based FPJ). During the *pilot transmission (PT)* phase, the DIRS is silent; During the *data transmission (DT)* phase, the phase shifts of the DIRS reflecting elements are randomly generated by the independent DIRS controller.

elements is deployed near the BS[3] to launch jamming attacks on the LUs.

Pilot Transmission: The LUs' CSI is obtained in the *PT* phase [26], [27] in order for the BS to design a decoder used during the *DT* phase, such as the ZF linear detector [28]. In particular, during the *PT* phase, the independent DIRS controller acts to make the DIRS absorb the wireless signals it receives. The pilot signal used by LU_k is denoted by $s_{\mathrm{p},k}$. Consequently, the received pilot vector $\boldsymbol{y}_{\mathrm{p},k} \in \mathbb{C}^{N_t \times 1}$ at the BS is given by

$$\boldsymbol{y}_{\mathrm{p},k} = \sqrt{p_{\mathrm{p},k}}\boldsymbol{h}_{\mathrm{d},k}s_{\mathrm{p},k} + \boldsymbol{n}_{\mathrm{p}}, \tag{1}$$

where $p_{\mathrm{p},k}$ is the power of the pilot signal sent by LU_k, and $\boldsymbol{h}_{\mathrm{d},k} \in \mathbb{C}^{N_t \times 1}$ represents the direct channel between LU_k and the BS during the *PT* phase. In addition, $\boldsymbol{n}_{\mathrm{p}} = [n_{\mathrm{p},1}, n_{\mathrm{p},2}, \cdots, n_{\mathrm{p},N_t}]^T$ denotes the received noise vector at the BS which is assumed to be composed of independent and identically distributed (i.i.d.) elements with zero mean and variance σ_{p}^2, i.e., $n_{\mathrm{p},i} \sim \mathcal{CN}\left(0, \sigma_{\mathrm{p}}^2\right), i = 1, 2, \cdots, N_t$.

Based on the received pilot signal $\boldsymbol{y}_{\mathrm{p},k}$, the direct channel $\boldsymbol{h}_{\mathrm{d},k}$ can be estimated by the BS. Similarly, the multi-user direct channel $\mathbf{H}_{\mathrm{d}}$ between BS and all LUs can be obtained, where $\mathbf{H}_{\mathrm{d}} = [\boldsymbol{h}_{\mathrm{d},1}, \boldsymbol{h}_{\mathrm{d},2}, \cdots, \boldsymbol{h}_{\mathrm{d},K}] \in \mathbb{C}^{N_t \times K}$. We assume that perfect CSI is obtained by the BS during the *PT* phase [27], as imperfect CSI is not a core concern in the jamming attack scenario, and the impact of imperfect CSI has also been well studied [28], [29].

Linear Detector Design: Two common approaches for decoding at the BS are the MRC and ZF detectors. The conventional MRC detector is given by

$$\mathbf{W}^H = \mathbf{H}_{\mathrm{d}}^H = [\boldsymbol{w}_1, \boldsymbol{w}_2, \cdots, \boldsymbol{w}_K]^H. \tag{2}$$

[3]Many existing performance-enhancing IRS-aided systems assume that legitimate IRSs are deployed close to users in order to maximize system performance [15]. However, in the jamming scenario presented here, we make the more robust assumption that the independent DIRS controller does not have any information about the LUs, such as the LUs' locations and CSI. The location of the BS is fixed, and thus we assume that the DIRS is deployed near the BS. Our deployment strategy is informed by the conclusion given in [15], which makes the impact of the DIRS as large as possible. In addition, the distance from the DIRS to the legitimate BS should be greater than the minimum channel correlation distance to ensure that the DIRS-based channel and the direct channel of each LU are independent.

On the other hand, the conventional ZF detector is

$$\mathbf{W}^H = \left(\mathbf{H}_{\mathrm{d}}^H\mathbf{H}_{\mathrm{d}}\right)^{-1}\mathbf{H}_{\mathrm{d}}^H = [\boldsymbol{w}_1, \boldsymbol{w}_2, \cdots, \boldsymbol{w}_K]^H. \tag{3}$$

Data Transmission: During the *DT* phase[4], the LUs transmit their data using the same time-frequency resource as the pilot data. Meanwhile, the DIRS controller tunes the illegitimate IRS to randomly generate phase shifts. Namely, the reflecting vector $\boldsymbol{\varphi}(t) = \left[e^{j\varphi_1(t)}, e^{j\varphi_2(t)}, \cdots, e^{j\varphi_{N_{\mathrm{D}}}(t)}\right]$ has random phase shifts, i.e., $\varphi_r(t) \sim \mathcal{F}\left([0, 2\pi]\right), r = 1, 2, \cdots, N_{\mathrm{D}}$. Since $[\varphi_1, \varphi_2, \cdots, \varphi_{N_{\mathrm{D}}}]$ are randomly generated, the DIRS controller does not use CSI to optimize $\boldsymbol{\varphi}(t)$.

In the proposed DIRS-based FPJ, the DIRS reflecting vector $\boldsymbol{\varphi}(t)$ is time-varying for the *PT* phase and the *DT* phase. Therefore, the illegitimate IRS with random phase shifts acts like a "disco ball", as shown in Fig. 1. Consequently, the multi-user DIRS-jammed channel between the BS and the LUs is expressed as

$$\mathbf{H}_{\mathrm{D}} = \mathbf{G}^H \mathrm{diag}\left(\boldsymbol{\varphi}(t)\right)\mathbf{H}_{\mathrm{I}} = [\boldsymbol{h}_{\mathrm{D},1}, \boldsymbol{h}_{\mathrm{D},2}, \cdots, \boldsymbol{h}_{\mathrm{D},K}], \tag{4}$$

where $\mathbf{G}$ represents the channel between the BS and the DIRS, $\mathbf{H}_{\mathrm{I}} = [\boldsymbol{h}_{\mathrm{I},1}, \boldsymbol{h}_{\mathrm{I},2}, \cdots, \boldsymbol{h}_{\mathrm{I},K}]$ represents the multi-user channel between the DIRS and the LUs, and $\boldsymbol{h}_{\mathrm{D},k}$ represents the DIRS-jammed channel between the BS and LU_k and can be written as $\boldsymbol{h}_{\mathrm{D},k} = \mathbf{G}^H \mathrm{diag}\left(\boldsymbol{\varphi}(t)\right)\boldsymbol{h}_{\mathrm{I},k}$.

The vector $\boldsymbol{y}_{\mathrm{d}}$ received at the BS is then expressed by

$$\boldsymbol{y}_{\mathrm{d}} = \sqrt{p_{\mathrm{d}}}\mathbf{W}^H\left(\mathbf{H}_{\mathrm{D}} + \mathbf{H}_{\mathrm{d}}\right)\boldsymbol{s}_{\mathrm{d}} + \mathbf{W}^H\boldsymbol{n}_{\mathrm{d}}, \tag{5}$$

where p_{d} is the average transmit power of each LU during the *DT* phase, and the vector of transmit symbols $\boldsymbol{s}_{\mathrm{d}}$ during the *DT* phase is given by $\boldsymbol{s}_{\mathrm{d}} = [s_{\mathrm{d},1}, s_{\mathrm{d},2}, \cdots, s_{\mathrm{d},K}]^T$ where $s_{\mathrm{d},k}$ denotes the symbol transmitted by LU_k. The receiver noise vector $\boldsymbol{n}_{\mathrm{d}}$ during the *DT* phase has zero mean independent elements with variance σ_{d}^2, and is written as $\boldsymbol{n}_{\mathrm{d}} = [n_{\mathrm{d},1}, n_{\mathrm{d},2}, \cdots, n_{\mathrm{d},N_t}]^T$, i.e., $n_{\mathrm{d},n} \sim \mathcal{CN}\left(0, \sigma_{\mathrm{d}}^2\right), n = 1, 2, \cdots, N_t$.

B. Ergodic Achievable Uplink Rate

The achievable uplink rate of the symbol transmitted by LU_k is written as $R_{\mathrm{d},k} = \log_2\left(1 + \gamma_k\right)$, where γ_k represents the received signal-to-interference-plus-noise ratio (SINR) of the k-th transmit symbol $s_{\mathrm{d},k}$. Based on (5), the k-th element of the received vector $\boldsymbol{y}_{\mathrm{d}}$ is expressed by

$$\begin{aligned} y_{\mathrm{d},k} = &\underbrace{\sqrt{p_{\mathrm{d}}}\boldsymbol{w}_k^H\boldsymbol{h}_{\mathrm{d},k}s_{\mathrm{d},k}}_{\text{signal}} + \underbrace{\sqrt{p_{\mathrm{d}}}\sum_{i\neq k, i=1}^{K}\boldsymbol{w}_k^H\boldsymbol{h}_{\mathrm{d},i}s_{\mathrm{d},i}}_{\text{inter-user interference}} \\ &+ \underbrace{\sqrt{p_{\mathrm{d}}}\sum_{i=1}^{K}\boldsymbol{w}_k^H\boldsymbol{h}_{\mathrm{D},i}s_{\mathrm{d},i}}_{\text{ACA interference}} + \underbrace{\boldsymbol{w}_k^H\boldsymbol{n}_{\mathrm{d}}}_{\text{noise}}, \end{aligned} \tag{6}$$

where the ACA interference is caused by the DIRS. Note that even if the DIRS-jammed channel $\mathbf{H}_{\mathrm{D}}$ is fixed, it can not be useful because the legitimate BS only knows the aged $\mathbf{H}_{\mathrm{D}}$.

[4]Similar to the assumption of reactive AJs in [30], a minimum reaction period is required to perform channel sensing and jamming initialization. Moreover, during the *PT* phase, we assume that the pilot signal could be transmitted without being jammed.

When the MRC detector is used, the ergodic rate $\overline{R}_{\mathrm{d},k}\big|_{\mathrm{MRC}}$ is expressed as

$$\begin{aligned}\overline{R}_{\mathrm{d},k}\big|_{\mathrm{MRC}} &= \mathbb{E}\left[\log_2\left(1+\gamma_k|_{\mathrm{MRC}}\right)\right] \\ &= \mathbb{E}\left[\log_2\left(1+\frac{p_{\mathrm{d}}\|\boldsymbol{h}_{\mathrm{d},k}\|^4}{p_{\mathrm{d}}\sum\limits_{i\neq k,i=1}^{K}\left|\boldsymbol{h}_{\mathrm{d},k}^H\boldsymbol{h}_{\mathrm{d},i}\right|^2+p_{\mathrm{d}}\sum\limits_{i=1}^{K}\left|\boldsymbol{h}_{\mathrm{d},k}^H\boldsymbol{h}_{\mathrm{D},i}\right|^2+\sigma_{\mathrm{d}}^2\left\|\boldsymbol{h}_{\mathrm{d},k}^H\right\|^2}\right)\right].\end{aligned} \tag{7}$$

For the ZF detector, the ergodic rate $\overline{R}_{\mathrm{d},k}\big|_{\mathrm{ZF}}$ reduces to

$$\begin{aligned}\overline{R}_{\mathrm{d},k}\big|_{\mathrm{ZF}} &= \mathbb{E}\left[\log_2\left(1+\gamma_k|_{\mathrm{ZF}}\right)\right] \\ &= \mathbb{E}\left[\log_2\left(1+\frac{p_{\mathrm{d}}}{p_{\mathrm{d}}\sum\limits_{i=1}^{K}\left|\boldsymbol{w}_k^H\boldsymbol{h}_{\mathrm{D},i}\right|^2+\sigma_{\mathrm{d}}^2\|\boldsymbol{w}_k\|^2}\right)\right].\end{aligned} \tag{8}$$

The introduced ACA interference is somewhat similar to the channel aging (CA) interference caused by imperfect CSI [31]. However, they are essentially different. For example, we can prove that $\overline{R}_{\mathrm{d},k}$ under the proposed DIRS-based jamming attack tends to zero as the number of DIRS reflecting elements increases. In other words, as the DIRS grows in size, the FPJ is able to ultimately prevent the BS from receiving any information transmitted by the LUs even though no jamming power nor LU CSI is exploited. For more unique properties of the proposed DIRS-based FPJ, please see Section III.

C. Channel Model

The DIRS is deployed close to the BS, and therefore we assume the BS-DIRS channel $\mathbf{G}$ follows Rician fading [11], [32]. On the other hand, we assume both the multi-user direct channel $\mathbf{H}_{\mathrm{d}}$ and the multi-user DIRS-LU channel $\mathbf{H}_{\mathrm{I}}$ follow Rayleigh fading. Specifically, the Rician fading channel $\mathbf{G}$ is modeled as [32]

$$\begin{aligned}\mathbf{G} &= \left[\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_{N_t}\right] \\ &= \sqrt{\mathscr{L}_{\mathrm{G}}}\left(\mathbf{G}^{\mathrm{LOS}}\sqrt{\mathscr{E}\left(\mathscr{E}+\mathbf{I}_{N_t}\right)^{-1}}+\mathbf{G}^{\mathrm{NLOS}}\sqrt{\left(\mathscr{E}+\mathbf{I}_{N_t}\right)^{-1}}\right),\end{aligned} \tag{9}$$

where $\mathscr{L}_{\mathrm{G}}$ denotes the geometric attenuation and log-normal shadow fading (the large-scale channel fading) between the BS and DIRS. Moreover, the $N_t\times N_t$ diagonal matrix $\mathscr{E}=\mathrm{diag}\left(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{N_t}\right)$ is comprised of the Rician factors, and each Rician factor represents the ratio of signal power in the line-of-sight (LOS) component to the scattered power in the non-line-of-sight (NLOS) component.

In (9), $\mathbf{G}^{\mathrm{LOS}}=\left[\boldsymbol{g}_1^{\mathrm{LOS}},\boldsymbol{g}_2^{\mathrm{LOS}},\cdots,\boldsymbol{g}_{N_t}^{\mathrm{LOS}}\right]$ represents the LOS component, and $\mathbf{G}^{\mathrm{NLOS}}=\left[\boldsymbol{g}_1^{\mathrm{NLOS}},\boldsymbol{g}_2^{\mathrm{NLOS}},\cdots,\boldsymbol{g}_{N_t}^{\mathrm{NLOS}}\right]$ denotes the NLOS component of $\mathbf{G}$. The NLOS component $\mathbf{G}^{\mathrm{NLOS}}$ follows Rayleigh fading, while element $\left[\mathbf{G}^{\mathrm{LOS}}\right]_{rn}$ in the LOS component $\mathbf{G}^{\mathrm{LOS}}$ is modeled as [11], [21], [32],

$$\left[\mathbf{G}^{\mathrm{LOS}}\right]_{rn}=e^{\jmath\frac{2\pi}{\lambda}d(n-1)\sin\theta_r},r=1,\cdots,N_{\mathrm{D}},n=1,\cdots,N_t, \tag{10}$$

where $\theta_r\in[-\theta_{\mathrm{A}},\theta_{\mathrm{A}}]$ $(0<\theta_{\mathrm{A}}\leq\pi)$ is the angle of arrival (AoA) from the r-th reflecting element, λ is the wavelength of the transmit symbols, and d represents the antenna-spacing of the ULA at the BS. Meanwhile, the NLOS component $\mathbf{G}^{\mathrm{NLOS}}$ has i.i.d. elements given by $\left[\mathbf{G}^{\mathrm{NLOS}}\right]_{rn}\sim\mathcal{CN}\left(0,1\right)$. The multi-user DIRS-LU channel $\mathbf{H}_{\mathrm{I}}$ and the multi-user direct channel $\mathbf{H}_{\mathrm{d}}$ are represented as

$$\mathbf{H}_{\mathrm{I}}=\widehat{\mathbf{H}}_{\mathrm{I}}\mathbf{D}_{\mathrm{I}}^{1/2}=\left[\sqrt{\mathscr{L}_{\mathrm{I},1}}\widehat{\boldsymbol{h}}_{\mathrm{I},1},\sqrt{\mathscr{L}_{\mathrm{I},2}}\widehat{\boldsymbol{h}}_{\mathrm{I},2},\cdots,\sqrt{\mathscr{L}_{\mathrm{I},K}}\widehat{\boldsymbol{h}}_{\mathrm{I},K}\right], \tag{11}$$

$$\mathbf{H}_{\mathrm{d}}=\widehat{\mathbf{H}}_{\mathrm{d}}\mathbf{D}_{\mathrm{d}}^{1/2}=\left[\sqrt{\mathscr{L}_{\mathrm{d},1}}\widehat{\boldsymbol{h}}_{\mathrm{d},1},\sqrt{\mathscr{L}_{\mathrm{d},2}}\widehat{\boldsymbol{h}}_{\mathrm{d},2},\cdots,\sqrt{\mathscr{L}_{\mathrm{d},K}}\widehat{\boldsymbol{h}}_{\mathrm{d},K}\right], \tag{12}$$

where elements of the $K\times K$ diagonal matrices $\mathbf{D}_{\mathrm{I}}=\mathrm{diag}\left(\mathscr{L}_{\mathrm{I},1},\mathscr{L}_{\mathrm{I},2},\cdots,\mathscr{L}_{\mathrm{I},K}\right)$ and $\mathbf{D}_{\mathrm{d}}=\mathrm{diag}\left(\mathscr{L}_{\mathrm{d},1},\mathscr{L}_{\mathrm{d},2},\cdots,\mathscr{L}_{\mathrm{d},K}\right)$ model the geometric attenuation and log-normal shadow fading, which are assumed to be independent over n [28]. The elements of $\widehat{\mathbf{H}}_{\mathrm{I}}$ and $\widehat{\mathbf{H}}_{\mathrm{d}}$ are i.i.d. Gaussian variables defined as $\left[\widehat{\mathbf{H}}_{\mathrm{I}}\right]_{rk},\left[\widehat{\mathbf{H}}_{\mathrm{d}}\right]_{nk}\sim\mathcal{CN}\left(0,1\right),r=1,2,\cdots,N_{\mathrm{D}},\ n=1,2,\cdots,N_t,\ k=1,2,\cdots,K$.

D. Review of Some Results on Random Variables

1) Jensen's Inequality: Consider a convex function $f:\mathcal{I}\rightarrow\mathbb{R}$, where $\mathcal{I}$ is an interval in $\mathbb{R}$. If a random variable $x\in\mathcal{I}$, and $f\left(\mathbb{E}\left[x\right]\right)$ and $\mathbb{E}\left[f\left(x\right)\right]$ are finite, then

$$\mathbb{E}\left[f\left(x\right)\right]\geq f\left(\mathbb{E}\left[x\right]\right). \tag{13}$$

2) Weak Law of Large Numbers: Consider the following random vector of i.i.d. Lebesgue integrable random variables: $\boldsymbol{x}\triangleq\left[x_1,x_2,\cdots,x_n\right]^T$, where $\mathbb{E}\left[x_1\right]=\mathbb{E}\left[x_2\right]=\cdots=\mathbb{E}\left[x_n\right]=\mu$. The weak law of large numbers states that

$$\overline{X}=\frac{\sum\limits_{i=1}^{n}x_i}{n}\xrightarrow{\mathrm{P}}\mu,\ \text{as}\ n\rightarrow\infty. \tag{14}$$

In other words, the sample average $\overline{X}$ converges in probability towards the expected value μ as $n\rightarrow\infty$.

3) Lindeberg-Lévy Central Limit Theorem: Suppose the random vector $\boldsymbol{x}\triangleq\left[x_1,x_2,\cdots,x_n\right]^T$ is a vector of i.i.d. random variables with mean $\mathbb{E}\left[x_1\right]=\mathbb{E}\left[x_2\right]=\cdots=\mathbb{E}\left[x_n\right]=\mu<\infty$ and variance $\mathrm{Var}\left[x_1\right]=\mathrm{Var}\left[x_2\right]=\cdots=\mathrm{Var}\left[x_n\right]=\sigma^2<\infty$. Then, the Lindeberg-Lévy central limit theorem states that the random variable $\sqrt{n}\left(\overline{X}-\mu\right)$ converges in distribution to $\mathcal{CN}\left(0,\sigma^2\right)$ as $n\rightarrow\infty$, i.e.,

$$\sqrt{n}\left(\overline{X}-\mu\right)=\frac{\sum\limits_{i=1}^{n}x_i}{\sqrt{n}}-\sqrt{n}\mu\xrightarrow{\mathrm{d}}\mathcal{CN}\left(0,\sigma^2\right),\ \text{as}\ n\rightarrow\infty. \tag{15}$$

III. Ergodic Achievable Uplink Rate Under DIRS-Based Jamming Attacks

In Section III-A, we determine lower bounds on the ergodic rates jammed by the proposed DIRS-based FPJ for the cases where the BS uses MRC and ZF detectors, respectively. Then, in Section III-B, we present various properties of the proposed

DIRS-based FPJ: 1) We compare the proposed DIRS-based FPJ to an IRS-based PJ to show that our approach is able to launch jamming attacks without any jamming power and any LU CSI; 2) In contrast to the AJs, the jamming impact of the proposed DIRS-based FPJ cannot be mitigated by increasing the LU transmit power; 3) The jamming impact of the proposed DIRS-based FPJ does not depend on the quantization nor the distribution of the random DIRS. In Section III-C, based on these properties, we describe a simple implementation of the proposed DIRS-based FPJ using a one-bit IRS with phase shifts following a uniform distribution.

A. Lower Bound of Ergodic Achievable Uplink Rate

A lower bound is derived in order to approximate the ergodic rate the BS can achieve under the proposed DIRS-based jamming attacks. The following lower bound can be obtained by using Jensen's inequality in a straightforward way:

$$\begin{aligned}\overline{R}_{\mathrm{d},k} &= \mathbb{E}\left[R_{\mathrm{d},k}\right] = \mathbb{E}\left[\log_2\left(1+\frac{1}{\gamma_k^{-1}}\right)\right] \\ &\geq \log_2\left(1+\frac{1}{\mathbb{E}\left[\gamma_k^{-1}\right]}\right), k=1,2,\cdots,K. \end{aligned} \tag{16}$$

Unfortunately, the lower bound in (16) is implicit. To this end, we present more-explicit lower bounds on the ergodic rate $\overline{R}_{\mathrm{d},k}$ for the cases where the BS uses the MRC and ZF detectors, given below respectively as Proposition 1 and Proposition 2.

When the MRC detector is used at the BS to receive the transmit symbol vector $\boldsymbol{s}_{\mathrm{d}}$, we can derive the following explicit lower bound on the ergodic rate $\overline{R}_{\mathrm{d},k}\big|_{\mathrm{MRC}}$ $(k=1,2,\cdots,K)$ under the jamming launched by the proposed DIRS-based FPJ.

Proposition 1: The lower bound on the ergodic rate $\overline{R}_{\mathrm{d},k}\big|_{\mathrm{MRC}}$ converges in probability towards a fixed value as $N_{\mathrm{D}}, N_t \to \infty$, i.e.,

$$\begin{aligned}\overline{R}_{\mathrm{d},k}\big|_{\mathrm{MRC}} &\geq \log_2\left(1+\frac{1}{\mathbb{E}\left[\gamma_k^{-1}\big|_{\mathrm{MRC}}\right]}\right) \\ &\xrightarrow{\mathrm{p}} \log_2\left(1+\frac{p_{\mathrm{d}}\left(N_t-1\right)\mathscr{L}_{\mathrm{d},k}}{p_{\mathrm{d}}\sum\limits_{i=1,i\neq k}^{K}\mathscr{L}_{\mathrm{d},i}+p_{\mathrm{d}}N_{\mathrm{D}}\sum\limits_{i=1}^{K}\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},i}+\sigma_{\mathrm{d}}^2}\right), \\ &\quad \text{as } N_{\mathrm{D}}, N_t \to \infty. \end{aligned} \tag{17}$$

Proof: See Appendix A. ∎

When the BS uses the ZF detector to receive $\boldsymbol{s}_{\mathrm{d}}$, the following explicit lower bound on the ergodic rate $\overline{R}_{\mathrm{d},k}\big|_{\mathrm{ZF}}$ $(k=1,2,\cdots,K)$ is presented in Proposition 2.

Proposition 2: The lower bound of the ergodic rate $\overline{R}_{\mathrm{d},k}\big|_{\mathrm{ZF}}$ converges in probability towards a fixed value as $N_{\mathrm{D}}, N_t \to \infty$, i.e.,

$$\begin{aligned}\overline{R}_{\mathrm{d},k}\big|_{\mathrm{ZF}} &\geq \log_2\left(1+\frac{1}{\mathbb{E}\left[\gamma_k^{-1}\big|_{\mathrm{ZF}}\right]}\right) \\ &\xrightarrow{\mathrm{p}} \log_2\left(1+\frac{p_{\mathrm{d}}\left(N_t-K\right)\mathscr{L}_{\mathrm{d},k}}{p_{\mathrm{d}}N_{\mathrm{D}}\sum\limits_{i=1}^{K}\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},i}+\sigma_{\mathrm{d}}^2}\right), \text{ as } N_{\mathrm{D}}, N_t \to \infty. \end{aligned} \tag{18}$$

Proof: See Appendix B. ∎

The lower bounds in (17) and (18) provide accurate estimates of ergodic rates. In Section IV, the simulation results show that the derived lower bounds are close to the actual ergodic rates.

B. Properties of Disco-IRS-Based Fully-Passive Jammer

In this subsection, we illustrate some unique properties of the proposed DIRS-based FPJ to show the difference between it and existing jammers.

1) Jamming Users Without Jamming Power and LU CSI: In Section II-B, we have illustrated that the proposed DIRS-based FPJ jams LUs via the DIRS-based ACA. To the best of our knowledge, this is the first instance of an illegitimate jammer that is able to launch jamming attacks without either jamming power or LU CSI.

Although the IRS-based PJ approach proposed in [17] can launch jamming attacks without jamming power, a very demanding requirement must be met to implement this PJ: the CSI of all channels involved, such as the direct channel and the IRS-aided channels, must be known. The IRS-based PJ proposed in [17] can be extended to MU-MISO systems by implementing the following optimization:

$$\begin{aligned}&\min_{\boldsymbol{\varphi}} \sum_{k=1}^{K} R_{\mathrm{d},k} \\ &= \min_{\boldsymbol{\varphi}} \sum_{k=1}^{K} \log_2\left(1+\frac{p_{\mathrm{d}}\left|\boldsymbol{w}_k^H\left(\boldsymbol{h}_{\mathrm{d},k}+\boldsymbol{h}_{\mathrm{D},k}\right)\right|^2}{p_{\mathrm{d}}\sum\limits_{i=1,i\neq k}^{K}\left|\boldsymbol{w}_k^H\left(\boldsymbol{h}_{\mathrm{d},i}+\boldsymbol{h}_{\mathrm{D},i}\right)\right|^2+\sigma_{\mathrm{d}}^2\|\boldsymbol{w}_k\|^2}\right) \end{aligned} \tag{19}$$

$$\text{s.t. } \boldsymbol{\varphi} = \left[e^{j\varphi_1}, e^{j\varphi_2}, \cdots, e^{j\varphi_{N_{\mathrm{D}}}}\right], \tag{20}$$

$$\varphi_r \in [0, 2\pi], r = 1, 2, \cdots, N_{\mathrm{D}}. \tag{21}$$

The objective function in (19) is a continuous and differentiable function of $\boldsymbol{\varphi}$, and the constraints in (20) and (21) create a complex circle manifold. Therefore, the above optimization problem can be computed by the Riemannian conjugate gradient (RCG) algorithm [22], [33] as follows: generate the Riemannian gradient; determine the search direction; and retract the tangent vector.

(1) Riemannian Gradient: For ease of presentation, we denote the objective function in (19) as

$$\mathcal{G}(\boldsymbol{\varphi})=\sum_{k=1}^{K}\log_2\left(1+\frac{p_{\mathrm{d}}\left|\boldsymbol{w}_k^H\left(\boldsymbol{h}_{\mathrm{d},k}+\boldsymbol{h}_{\mathrm{D},k}\right)\right|^2}{p_{\mathrm{d}}\sum\limits_{i=1,i\neq k}^{K}\left|\boldsymbol{w}_k^H\left(\boldsymbol{h}_{\mathrm{d},i}+\boldsymbol{h}_{\mathrm{D},i}\right)\right|^2+\sigma_{\mathrm{d}}^2\|\boldsymbol{w}_k\|^2}\right). \tag{22}$$

Consequently, the Riemannian gradient at $\boldsymbol{\varphi}$ is a tangent vector that denotes the greatest decreasing direction of $\mathcal{G}(\boldsymbol{\varphi})$, which is given by

$$\mathrm{grad}\mathcal{G}(\boldsymbol{\varphi})=\nabla\mathcal{G}(\boldsymbol{\varphi})-\mathrm{Re}\left\{\nabla\mathcal{G}(\boldsymbol{\varphi})\odot\boldsymbol{\varphi}^H\right\}\odot\boldsymbol{\varphi}, \tag{23}$$

where $\nabla\mathcal{G}(\boldsymbol{\varphi})$ represents the Euclidean gradient.

(2) Search Direction: The tangent vector conjugate to $\mathrm{grad}\mathcal{G}(\boldsymbol{\varphi})$ can be used as the search direction $\mathcal{D}$, which is expressed as

$$\mathcal{D}=-\mathrm{grad}\mathcal{G}(\boldsymbol{\varphi})+\rho_1(\tilde{\mathcal{D}}-\mathrm{Re}\{\tilde{\mathcal{D}}\odot\boldsymbol{\varphi}^H\}\odot\boldsymbol{\varphi}), \tag{24}$$

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

(3) Retraction: Retract the tangent vector back to the complex circle manifold described by (20). Mathematically,

$$\frac{\left(\boldsymbol{\varphi}+\rho_2\mathcal{D}\right)_n}{\left|\left(\boldsymbol{\varphi}+\rho_2\mathcal{D}\right)_n\right|}\mapsto\boldsymbol{\varphi}_n, \tag{25}$$

where ρ_2 represents the Armijo step size.

To solve the optimization problem via the RCG algorithm, the IRS controller requires significant computing power. Moreover, the requirement that the controller has access to the CSI of $\mathbf{H}_{\mathrm{d}}$, $\mathbf{G}$, and $\mathbf{H}_{\mathrm{I}}$ is difficult to realize due to the passive nature of the IRS [18]. In particular, to acquire the CSI of the IRS-aided channels $\mathbf{G}$ and $\mathbf{H}_{\mathrm{I}}$, the LUs instead of the IRS send pilot signals to the BS, and the BS then estimates the IRS-aided channels by traditional solutions, for instance, the least squares (LS) algorithm [18]. When a legitimate IRS is used to enhance system performance, the CSI of the IRS-aided channels can be jointly estimated by the BS, the LUs, and the IRS. However, acquiring the IRS-aided channels at the illegitimate IRS is not realistic in the jamming attack scenario.

The DIRS-based ACA interference is introduced by randomly generating phase shifts for the DIRS. Compared to the IRS-aided PJ, the proposed DIRS-based FPJ does not need significant computing power. On the other hand, the DIRS approach launches jamming attacks without requiring the LU CSI.

2) Larger Transmit Power Increases Jamming: Taking (18) as an example, if the LUs increase the average transmit power p_{d}, the term $p_{\mathrm{d}}N_{\mathrm{D}}\sum_{i=1}^{K}\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},i}$ in the denominator also increases. In other words, the jamming attacks launched by the proposed DIRS-based FPJ cannot be mitigated by increasing the average transmit power, since increasing the power leads to even more serious jamming.

Note that an AJ is also able to jam the vector $\boldsymbol{y}_{\mathrm{d}}$ received by the BS without LU CSI. More specifically, consider a single-antenna AJ that broadcasts the jamming signal symbol s_{J} with power p_{J}. The k-th element of the received vector $\boldsymbol{y}_{\mathrm{d}}$ under active jamming is given by

$$\begin{aligned}y_{\mathrm{d},k}=&\underbrace{\sqrt{p_{\mathrm{d}}}\boldsymbol{w}_k^H\boldsymbol{h}_{\mathrm{d},k}s_{\mathrm{d},k}}_{\text{signal}}+\underbrace{\sqrt{p_{\mathrm{d}}}\sum\nolimits_{i\neq k,i=1}^{K}\boldsymbol{w}_k^H\boldsymbol{h}_{\mathrm{d},i}s_{\mathrm{d},i}}_{\text{inter-user interference}}\\&+\underbrace{\sqrt{p_{\mathrm{J}}}\boldsymbol{w}_k^H\boldsymbol{h}_{\mathrm{J}}s_{\mathrm{J}}}_{\text{AJ interference}}+\underbrace{\boldsymbol{w}_k^H\boldsymbol{n}_{\mathrm{d}}}_{\text{noise}},\end{aligned} \tag{26}$$

where $\boldsymbol{h}_{\mathrm{J}}$ denotes the channel between the BS and the AJ whose elements have zero mean and variance $\mathscr{L}_{\mathrm{J}}$, which represents the geometric attenuation and log-normal shadow fading between the BS and the AJ. Specifically, $\boldsymbol{h}_{\mathrm{J}}=\sqrt{\mathscr{L}_{\mathrm{J}}}\widehat{\boldsymbol{h}}_{\mathrm{J}}$ and $\left[\widehat{\boldsymbol{h}}_{\mathrm{J}}\right]_n\sim\mathcal{CN}(0,1),n=1,2,\cdots,N_t$. Consequently, AJ interference proportional to the jamming power p_{J} is introduced into the achievable rate $R_{\mathrm{d},k}$. Mathematically, the achievable rate $R_{\mathrm{d},k}^{\mathrm{AJ}}$ under active jamming is formulated as

$$\begin{aligned}&R_{\mathrm{d},k}^{\mathrm{AJ}}\\&=\log_2\left(1+\frac{p_{\mathrm{d}}\left|\boldsymbol{w}_k^H\boldsymbol{h}_{\mathrm{d},k}\right|^2}{p_{\mathrm{d}}\sum\limits_{i=1,i\neq k}^{K}\left|\boldsymbol{w}_k^H\boldsymbol{h}_{\mathrm{d},i}\right|^2+p_{\mathrm{J}}\left|\boldsymbol{w}_k^H\boldsymbol{h}_{\mathrm{J}}\right|^2+\sigma_{\mathrm{d}}^2\|\boldsymbol{w}_k\|^2}\right).\end{aligned} \tag{27}$$

If we take the case where the BS adopts the ZF detector (3) to receive the symbols sent by the LUs, the achievable rate $R_{\mathrm{d},k}^{\mathrm{AJ}}\big|_{\mathrm{ZF}}$ expressed in (27) reduces to

$$R_{\mathrm{d},k}^{\mathrm{AJ}}\big|_{\mathrm{ZF}}=\log_2\left(1+\frac{p_{\mathrm{d}}}{p_{\mathrm{J}}\left|\boldsymbol{w}_k^H\boldsymbol{h}_{\mathrm{J}}\right|^2+\sigma_{\mathrm{d}}^2\|\boldsymbol{w}_k\|^2}\right). \tag{28}$$

Although the AJ can jam the LUs without their CSI, the jamming attacks launched by the AJ can be mitigated by increasing the average transmit power p_{d}. In order to achieve the desired jamming impact, the AJ has to increase its jamming power p_{J}. However, high-power jamming signals are more easily detected by the legitimate BS, which increases the risk of AJ exposure.

3) Ergodic Achievable Uplink Rate Independent of Precision and Stochastic Distribution of Reflecting Phase Shifts: Based on (17) and (18), an interesting property can be observed: the jamming impact of the proposed DIRS-based FPJ does not depend on the quantization of the IRS phase shifts. In other words, jamming launched by a one-bit DIRS-based FPJ is equivalent to that launched by the proposed FPJ using an infinite-precision DIRS.

In addition, the jamming impact of the proposed DIRS-based FPJ does not depend on the distribution of the random phase shifts. As long as the number of DIRS reflecting elements is large, the ergodic rate will tend to zero even if the proposed DIRS-based FPJ is implemented using a one-bit IRS with uniformly distributed (i.e., equally likely) one-bit phase shifts. In practice, it is easy to implement such a simple IRS with a large number of reflecting elements [34], [35].

An IRS is an ultra-thin surface inlaid with massive sub-wavelength reflecting elements whose electromagnetic responses (such as phase shifts) can be controlled, for example,

by simple programmable PIN diodes [35]. Based on the ON/OFF behavior of the PIN diodes, however, only a limited set of discrete phase shifts can be achieved by an IRS. Some existing work has investigated the trade-off between performance and the number of bits used to determine the phase shifts [36]–[38]. Empirically, the higher the resolution of the discrete IRS phase shifts, the higher the cost but the better the performance.

Taking the IRS-based PJ in (19) as an example, the optimization of the phase shifts via the RCG algorithm implicitly assumes continuously tunable phase shifts. Assuming that the illegal IRS has b-bit quantized phase shifts, the discrete reflecting phase shifts $\widetilde{\boldsymbol{\varphi}} = [\widetilde{\varphi}_1, \widetilde{\varphi}_2, \cdots, \widetilde{\varphi}_{N_\mathrm{D}}]$ must be calculated by finding the quantized values closest to the result of the optimization:

$$\min_{\widetilde{\boldsymbol{\varphi}}} \left\| \boldsymbol{\varphi} - \widetilde{\boldsymbol{\varphi}} \right\|^2 \tag{29}$$

$$\text{s.t. } \widetilde{\varphi}_r \in \left\{ 0, \frac{2\pi}{2^b}, \cdots, \frac{2\left(2^b-1\right)\pi}{2^b} \right\}, r = 1, 2, \cdots, N_\mathrm{D}. \tag{30}$$

Obviously, in this approach based on the LU CSI, the higher the quantization resolution, the more serious the jamming impact of the IRS-based PJ. Such a high resolution discrete phase-shift design is unnecessary in our proposed approach.

C. One-Bit DIRS-Based FPJ Nullifying Anti-Jamming Technologies

Based on the properties stated in Section III-B, the proposed DIRS-based FPJ can be implemented by using a one-bit IRS, where the reflecting phase shifts follow a simple discrete uniform distribution, i.e., $\varphi_r \sim \mathcal{U}(\{0, \pi\})$. Fig. 2 illustrates the proposed DIRS-based FPJ. By actively aging the wireless channels between the BS and the LUs, serious ACA interference is introduced.

The detector used at the BS is designed based only on the multi-user direct channel $\mathbf{H}_\mathrm{d}$. For example, the ZF decoder $\boldsymbol{w}_k$ is only orthogonal to the subspace of the direct co-user channels $\boldsymbol{h}_{\mathrm{d},1}, \cdots, \boldsymbol{h}_{\mathrm{d},k-1}, \boldsymbol{h}_{\mathrm{d},k+1}, \cdots, \boldsymbol{h}_{\mathrm{d},K}$, as depicted in Fig. 2, which is different from the DIRS-jammed co-user channel.

From (6), the jamming attacks launched by the proposed DIRS-based FPJ are implemented by introducing ACA interference. Since the characteristics of ACA interference, such as the carrier frequency, are the same as the LUs' transmit signals, classic anti-jamming technologies such as frequency hopping [39], [40] are not helpful for the proposed DIRS-based FPJ.

IV. Simulation Results and Discussion

In this section, we provide numerical results to evaluate the effectiveness of the proposed DIRS-based FPJ in Section II and that of the derived theoretical analysis in Section III. Consider an MU-MISO system with 24 single-antenna LUs jammed by the proposed DIRS-based FPJ in Section II. More specifically, the BS is located at (0m, 0m, 2m) and the 24 LUs are randomly distributed in the circular region S centered at (0m, 160m, 0m) with a radius of 10m. Furthermore, the DIRS with N_D reflecting elements is deployed at ($-d_\mathrm{BD}$m, 0m, 2m) to launch the proposed DIRS-based fully-passive jamming on the LUs. The distance between the BS and the DIRS, the number of DIRS reflecting elements, and the number of antennas at the BS are $d_\mathrm{BD} = 2$, $N_\mathrm{D} = 4096$, and $N_t = 256$. If not otherwise specified, the numbers of DIRS reflecting elements, antennas, and LUs, as well as the BS-DIRS distance default to these values. The influence of the numbers of reflecting elements, antennas, and LUs as well as that of the BS-DIRS distance are discussed next. The propagation parameters of wireless channels $\mathbf{H}_\mathrm{D}$, $\mathbf{H}_\mathrm{I}$, and $\mathbf{G}$ described in Section II-C are defined in Table I based on 3GPP propagation models [41], and the variance of the noise is $\sigma_\mathrm{d}^2 = -170 + 10\log_{10}(BW)$ dBm.

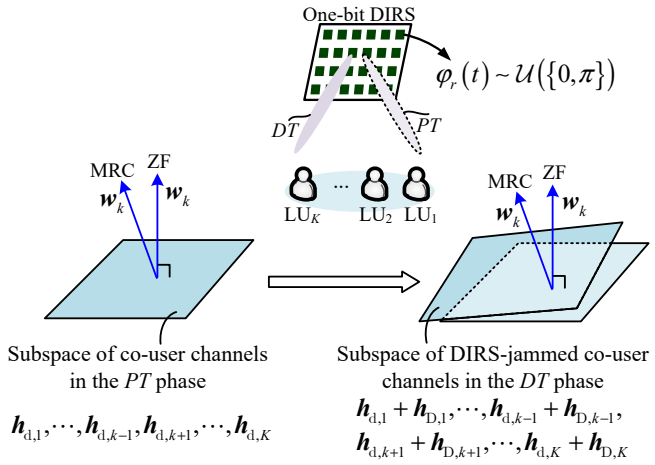

Fig. 2. One-bit disco-IRS-based fully-passive jammer (DIRS-based FPJ) by actively aging channels to launch jamming attacks on legitimate users (LUs), where the reflecting phase shifts follow a simple one-bit discrete distribution.

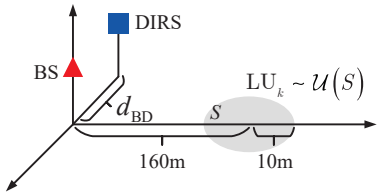

Fig. 3. A visualization of an MU-MISO system jammed by the proposed DIRS-based FPJ, where the BS is located at (0m, 0m, 2m), the DIRS with N_D reflecting elements is deployed at the location ($-d_\mathrm{BD}$m, 0m, 2m), and 24 LUs are randomly distributed in the circular region S centered at (0m, 160m, 0m) with a 10m radius.

In this section, we illustrate the performance of the following benchmarks: the ergodic rates resulting from an MU-MISO system without jamming attacks [28], where the BS adopts the ZF detector (ZF w/o Jamming) or the MRC detector (MRC w/o Jamming); the ergodic rates described in (28) resulting from an MU-MISO system jammed by an AJ with -4dBm jamming power (AJ w/ -4dBm) and 4dBm jamming power (AJ w/ 4dBm), where the AJ is deployed at (20m,160m,0m); and the ergodic rates given in (7) and (8) resulting from an MU-MISO system jammed by the proposed DIRS-based FPJ, where the BS also adopts the ZF detector (DIRS-FPJ & ZF)

TABLE I
WIRELESS CHANNEL SIMULATION PARAMETERS

Parameter	Notation	Value
Large-scale LOS fading	$\mathscr{L}_{\mathrm{G}}$	$35.6+22\log_{10}(d)$ (dB)
Large-scale NLOS fading	$\mathscr{L}_{\mathrm{d},k}, \mathscr{L}_{\mathrm{I},k}$	$32.6+36.7\log_{10}(d)$
Transmission bandwidth	BW	180 kHz
Rician factors	$\mathscr{E}$	$10\mathbf{I}_{N_t}$

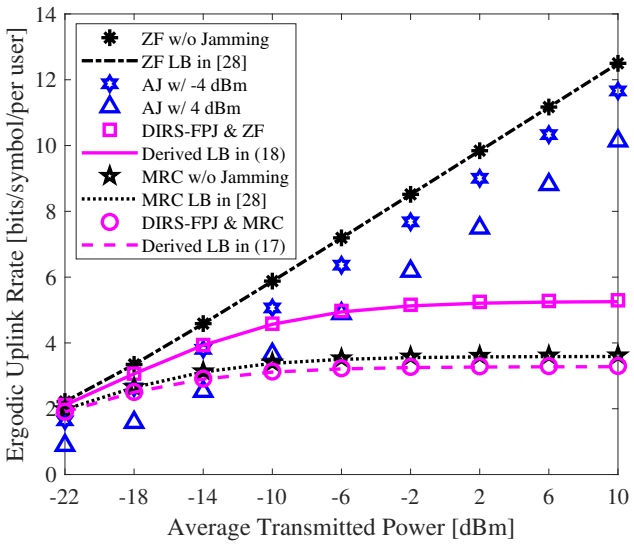

Fig. 4. Ergodic achievable uplink rate vs average transmit power of each LU for different benchmarks.

or the MRC detector (DIRS-FPJ & MRC).

1) Ergodic Achievable Uplink Rate Versus Average Transmit Power: Fig. 4 illustrates the relationship between the ergodic rates and the average transmit power of each LU. The ergodic rates of ZF w/o Jamming, AJ w/ -4dBm, AJ w/ 4dBm, DIRS-FPJ & ZF, MRC w/o Jamming, as well as DIRS-FPJ & MRC benchmarks are depicted, respectively. Meanwhile, the lower bounds of ZF w/o Jamming and MRC w/o Jamming given in [28] are shown in Fig. 4. To show the effectiveness of the theoretical analysis derived in Section III, the lower bounds of the proposed DIRS-based FPJ are also included in Fig. 4.

From Fig. 4, one can see that the proposed DIRS-based FPJ can effectively jam the LUs without either jamming power or LU CSI. The AJ approach requires a significant amount of extra jamming energy, but increased transmit power at the LUs not only fails to mitigate the jamming impact of the proposed DIRS-based FPJ but even aggravates it. As shown in Fig. 4, as the average transmit power of each LU increases, the jamming impact of the proposed DIRS-based FPJ gradually becomes stronger and eventually exceeds that of the AJ. Although an MU-MISO system using low-order modulations, such as quadrature phase shift keying (QPSK), can work in the low power domain to reduce DIRS-based ACA interference, we will see below that increasing the number of DIRS reflecting elements can ensure reasonable jamming attacks. Furthermore, if the transmit signal is in the low power domain, a relatively small amount of jamming can provide an effective jamming impact.

Compared to the case where the BS uses the MRC detector, the jamming impact of the proposed DIRS-based FPJ for ZF decoding is stronger, as can be seen from Fig. 4. In Section III-C, we have illustrated that the proposed DIRS-based FPJ jams the LUs by introducing ACA interference. However, serious inter-user interference (IUI), which is a type of multi-user interference (MUI), has been introduced when the BS uses the MRC detector to receive the signals transmitted by the LUs. As a result, the jamming impact caused by the ACA interference is suppressed. However, the IUI is well suppressed when the BS employs the ZF detector, and thus the jamming impact of the proposed DIRS-based FPJ is more evident.

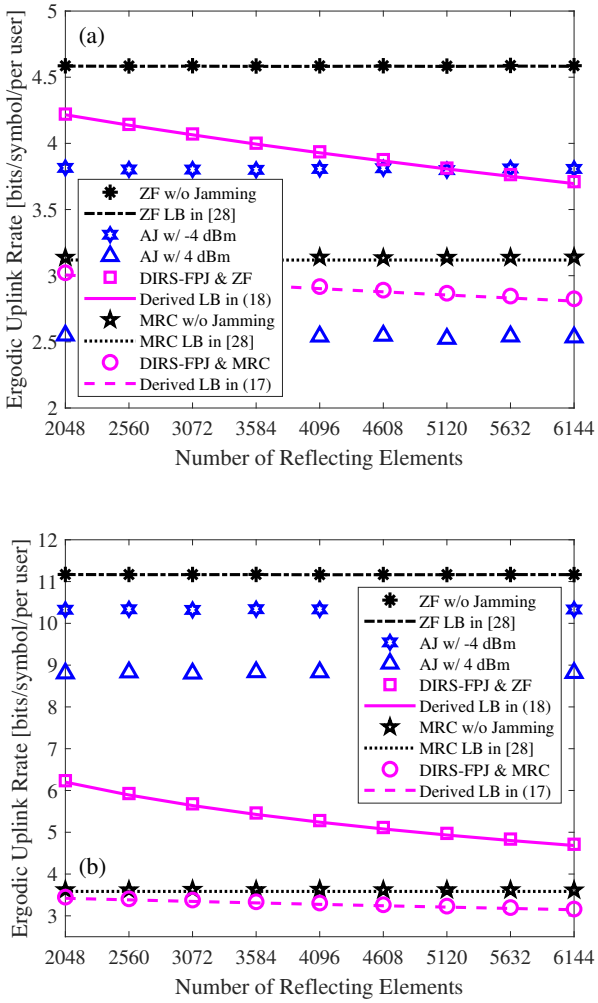

Fig. 5. Influence of the number of DIRS reflecting elements on the ergodic rates for (a) -14 dBm average transmit power and (b) 6 dBm average transmit power.

2) Ergodic Achievable Uplink Rate Versus Number of DIRS Reflecting Elements: Based on the theoretical analysis in Section III, the ergodic rates resulting from the MU-MISO system jammed by the proposed DIRS-based FPJ will tend to zero, as long as the number of DIRS reflecting elements is large. We show the effects of the number of DIRS reflecting

This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2023.3283133

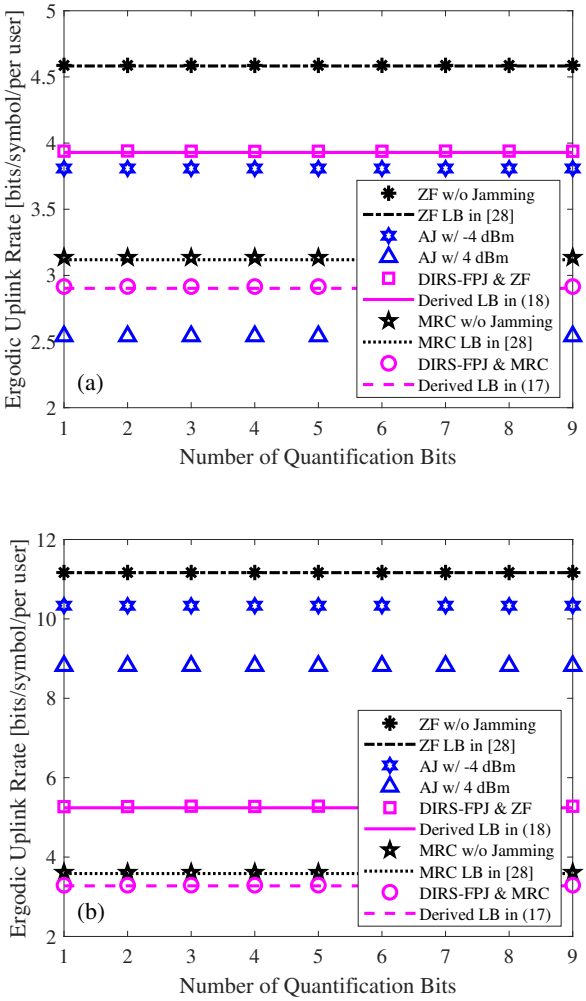

Fig. 6. Influence of the number of DIRS phase quantification bits on the ergodic rates for (a) -14 dBm average transmit power and (b) 6 dBm average transmit power.

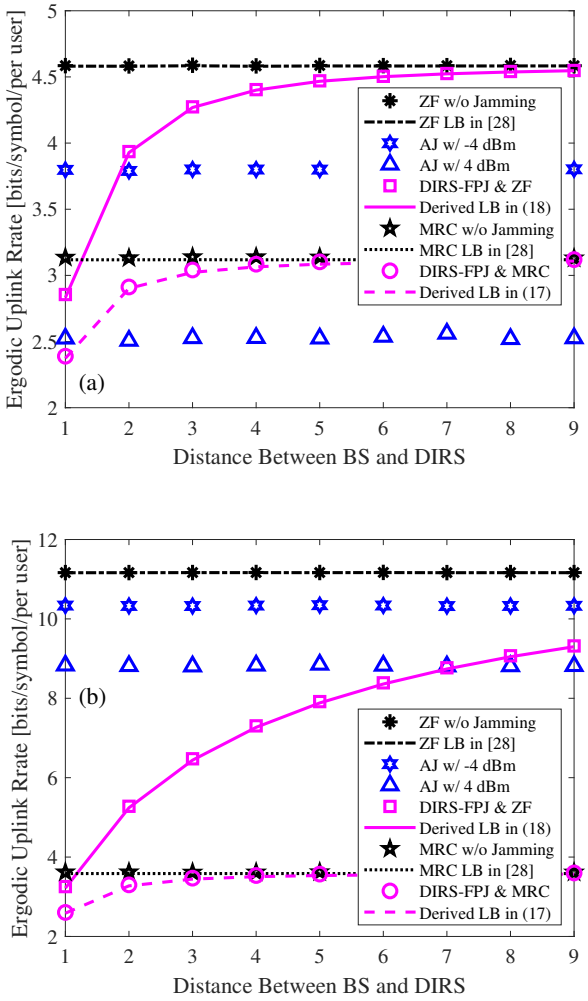

Fig. 7. Influence of the distance between the BS and the DIRS on the ergodic rates for (a) -14 dBm average transmit power and (b) 6 dBm average transmit power.

elements in Fig. 5 at both low transmit power ($p_{\rm d} = -14$ dBm) and high transmit power ($p_{\rm d} = 6$ dBm), which are plotted in Fig. 5 (a) and Fig. 5 (b), respectively.

One can see that the MU-MISO system is sensitive to active jamming attacks when the average transmit power of each LU is low. However, the active jamming attacks can be suppressed by classic anti-jamming techniques such as frequency hopping [39], [40], and an AJ requires a significant amount of extra jamming power. The jamming impact is more effective for high rather than low transmit power.

3) Ergodic Achievable Uplink Rate Versus DIRS Phase Resolution: Based on the theoretical analysis in Section III, one can see that the proposed DIRS-based FPJ has many unique properties. For example, the jamming impact of the proposed DIRS-based FPJ does not depend on the resolution of the DIRS phase shifts. It is clear from Fig. 6 that the jamming impact of the proposed DIRS-based FPJ does not increase with the number of bits used to quantize the DIRS phase shifts for either low or high average transmit power. Based on the results in Fig. 5 and 6, the proposed DIRS-based FPJ can be effectively implemented by using only a one-bit IRS with a large number reflecting elements whose phase randomly toggles between two values π radians apart.

4) Ergodic Achievable Uplink Rate Versus DIRS Location: In Fig. 7, the impact of the DIRS location on the ergodic rates is illustrated. The greater the distance, the greater the large-scale channel fading $\mathscr{L}_{\rm G}$ in the BS-DIRS channel. According to (17) and (18), the jamming effect of the proposed DIRS-based FPJ is weakened due to increased BS-DIRS distance $d_{\rm DB}$. To maximize the jamming effect of the proposed DIRS-based FPJ, the DIRS needs to be deployed as close to the BS as possible. If a near-BS deployment is not possible, based on Fig. 5 and Fig. 6, one solution to mitigating the weakening impact on jamming attacks is to increase the number of reflecting elements.

5) Ergodic Achievable Uplink Rate Versus Number of BS Antennas: In the next two figures, we demonstrate the jamming impact of the proposed DIRS-based FPJ on different MU-MISO systems. In Fig. 8, we show the influence of the number of BS antennas on the ergodic rates. At both low

This article has been accepted for publication in IEEE Transactions on Wireless Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TWC.2023.3283133

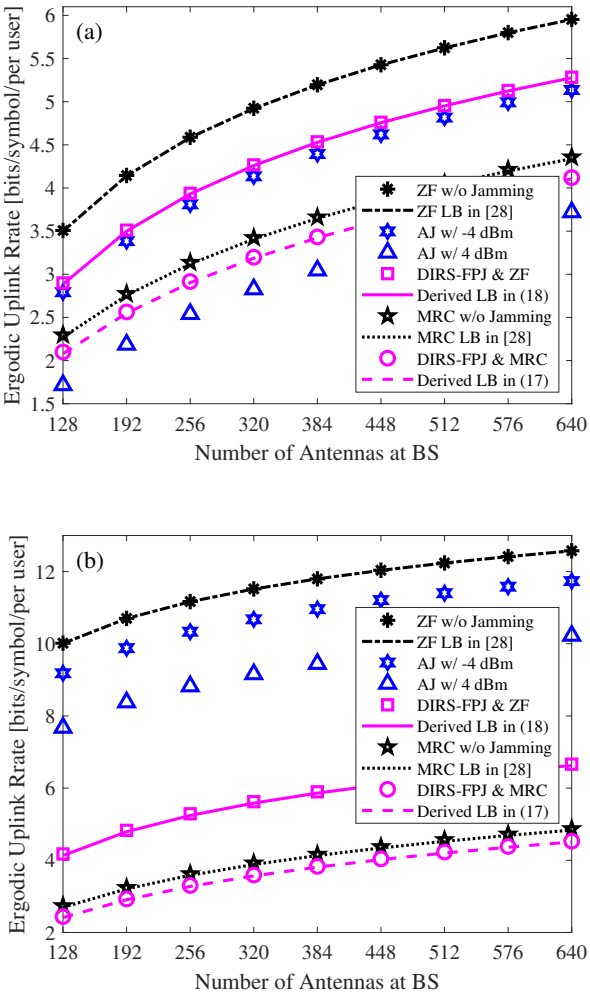

Fig. 8. Influence of the number of antennas deployed at the BS on the ergodic rates for (a) -14 dBm average transmit power and (b) 6 dBm average transmit power.

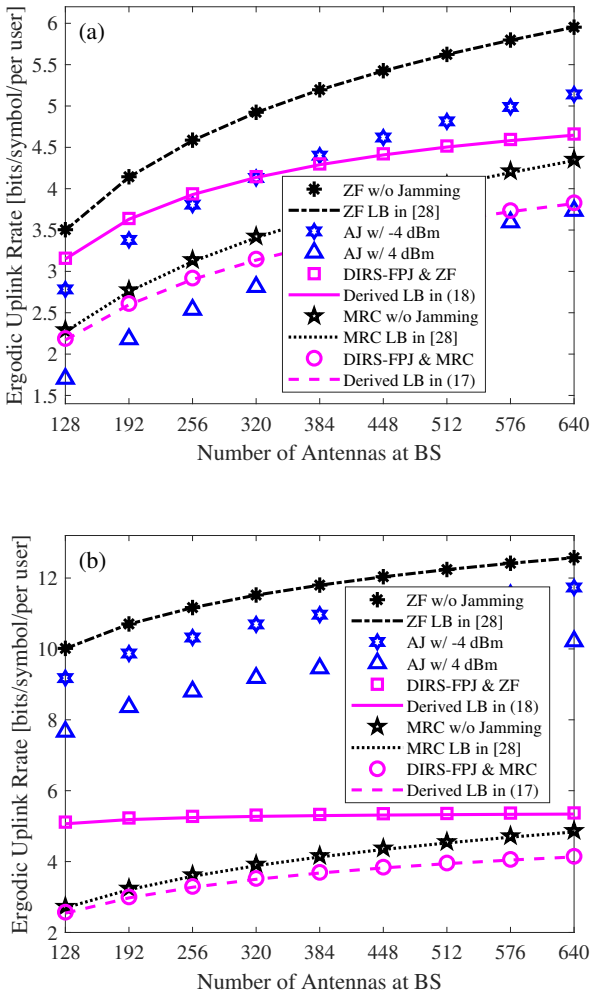

Fig. 9. Ergodic rates versus numbers of antennas and reflecting elements for (a) -14 dBm average transmit power and (b) 6 dBm average transmit power, where the number of reflecting elements is sixteen times the number of antennas ($N_{\mathrm{D}} = 16N_t$).

and high transmit powers, the ergodic rates achieved by all benchmarks increase with the number of antennas at the BS.

A possible way to mitigate the jamming attacks launched by the proposed DIRS-based FPJ is to increase the number of BS antennas. However, we see in Figs. 8 and 9 that the slopes of all ergodic rate curves decrease as the number of BS antennas continues to increase. In other words, continuing to increase the number of antennas at the BS cannot significantly mitigate the proposed DIRS-based jamming attacks when the number of antennas is large. Moreover, we can increase the number of reflecting elements deployed on the DIRS to counteract this mitigation, as shown in Fig. 9. It is clear that the ergodic rate resulting from the MU-MISO system jammed by the proposed DIRS-based FPJ does not increase with the number of BS antennas as long as the number of reflecting elements also increases. Compared to the cost of increasing the number of active antennas at the BS, the cost of increasing the number of passive reflecting elements on the DIRS is much lower, especially for those employing one-bit phase shifters [34], [35].

6) Ergodic Achievable Uplink Rate Versus Number of Legitimate Users: Fig. 10 shows the jamming impact of the proposed DIRS-based FPJ on MU-MISO systems communicating with different numbers of LUs. Even if an MU-MISO system is not subject to jamming attacks, the ergodic rate per LU decreases with the number of LUs. The drop in the ergodic rate is especially noticeable when the BS uses the MRC detector since it cannot suppress the IUI.

At both low and high transmit power, the jamming impact of the proposed DIRS-based FPJ becomes more significant as the number of LUs increases. Note that the ACA interference term in (6) also increases with the number of LUs. Moreover, as the number of LUs increases, one can see that the gap between ZF w/o Jamming and DIRS-FPJ & ZF is more significant than that between MRC w/o Jamming and DIRS-FPJ & MRC at both low and high transmit power. As before, the increased IUI diminishes the impact of the ACA interference.

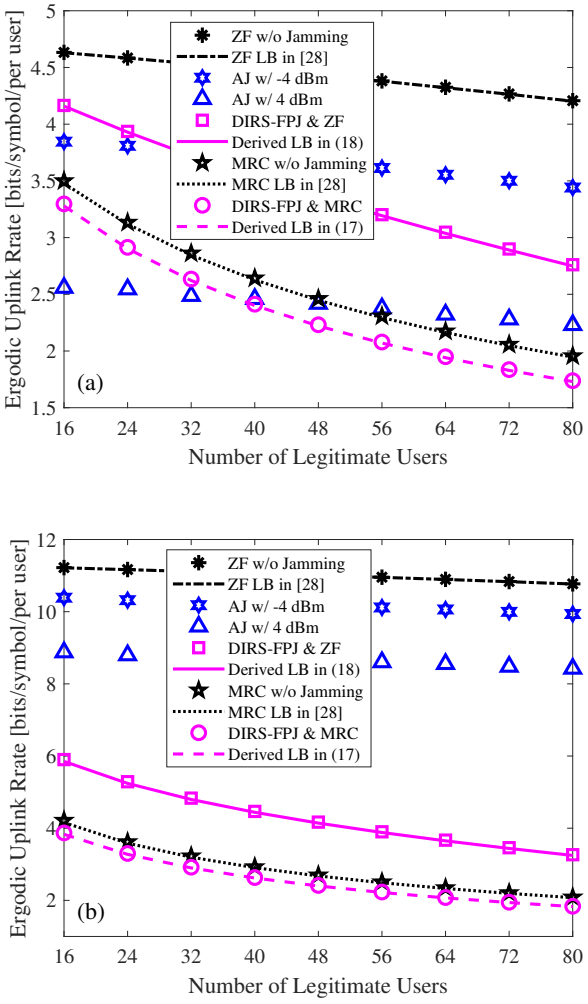

Fig. 10. Influence of the number of LUs on the ergodic rates for (a) -14 dBm average transmit power and (b) 6 dBm average transmit power.

V. Conclusions

In this paper, a novel DIRS-based FPJ has been proposed that can be implemented by a one-bit IRS. By introducing significant ACA interference, the proposed DIRS-based FPJ can launch jamming attacks on LUs with neither extra jamming power nor LU CSI. The following conclusions can be drawn from the theoretical analysis and numerical results, raising concerns about the significant potential threats posed by illegitimate IRSs.

1) In contrast to existing AJs and IRS-based PJ, the proposed DIRS-based FPJ launches jamming attacks by using ACA interference caused by the DIRS, and thus it requires no jamming power and no LU CSI.
2) The jamming impact of the proposed DIRS-based FPJ does not depend on how the DIRS phase shifts are quantized, nor on their distribution. As long as the number of DIRS reflecting elements is large, the ergodic rate will tend to zero even if the proposed DIRS-based FPJ is implemented with one-bit uniformly distributed phase shifts.
3) Increasing the transmit power at each LU will not mitigate the jamming attacks launched by the proposed DIRS-based FPJ and will even make them more deleterious. Furthermore, the DIRS-based FPJ can overcome classic anti-jamming technologies such as frequency hopping.
4) Although the BS can counter the proposed DIRS-based jamming attacks by increasing the number of its antennas, this suppression of the proposed DIRS-based jamming attacks can be weakened by increasing the number of reflecting elements on the DIRS.

We have illustrated the potential threats posed by illegal IRSs and demonstrated that even a one-bit DIRS can effectively jam LUs. Classic anti-jamming technologies are not effective for the proposed DIRS-based FPJ.

Appendix A
Proof of Proposition 1

Recall the ergodic $\overline{R}_{\mathrm{d},k}\big|_{\mathrm{MRC}}$ expressed as (7). We have the following lower bound by using Jensen's inequality:

$$\begin{aligned}\overline{R}_{\mathrm{d},k}\big|_{\mathrm{MRC}} &= \mathbb{E}\left[\log_2\left(1+\gamma_k\big|_{\mathrm{MRC}}\right)\right]\\ &\geq \log_2\left(1+\frac{1}{\mathbb{E}\left[\left(\gamma_k\big|_{\mathrm{MRC}}\right)^{-1}\right]}\right)\\ &= \log_2\left(1+\frac{1}{\mathbb{E}\left[\frac{p_{\mathrm{d}}\sum_{i=1,i\neq k}^{K}\left|\widetilde{h}_{\mathrm{d},i}\right|^2+p_{\mathrm{d}}\sum_{i=1}^{K}\left|\widetilde{h}_{\mathrm{D},i}\right|^2+\sigma_{\mathrm{d}}^2}{p_{\mathrm{d}}\|\boldsymbol{h}_{\mathrm{d},k}\|^2}\right]}\right),\end{aligned} \tag{31}$$

where $\widetilde{h}_{\mathrm{d},i}=\frac{\boldsymbol{h}_{\mathrm{d},k}^H\boldsymbol{h}_{\mathrm{d},i}}{\|\boldsymbol{h}_{\mathrm{d},k}\|}$ and $\widetilde{h}_{\mathrm{D},i}=\frac{\boldsymbol{h}_{\mathrm{d},k}^H\boldsymbol{h}_{\mathrm{D},i}}{\|\boldsymbol{h}_{\mathrm{d},k}\|}$. Conditioned on the fact that the random variables $\|\boldsymbol{h}_{\mathrm{d},k}\|$, $\widetilde{h}_{\mathrm{d},i}$, and $\widetilde{h}_{\mathrm{D},i}$ are independent, we can reduce the expectation in (31) to

$$\begin{aligned}&\mathbb{E}\left[\frac{p_{\mathrm{d}}\sum_{i=1,i\neq k}^{K}\left|\widetilde{h}_{\mathrm{d},i}\right|^2+p_{\mathrm{d}}\sum_{i=1}^{K}\left|\widetilde{h}_{\mathrm{D},i}\right|^2+\sigma_{\mathrm{d}}^2}{p_{\mathrm{d}}\|\boldsymbol{h}_{\mathrm{d},k}\|^2}\right]\\ &=\left(p_{\mathrm{d}}\sum_{i=1,i\neq k}^{K}\mathbb{E}\left[\left|\widetilde{h}_{\mathrm{d},i}\right|^2\right]+p_{\mathrm{d}}\sum_{i=1}^{K}\mathbb{E}\left[\left|\widetilde{h}_{\mathrm{D},i}\right|^2\right]+\sigma_{\mathrm{d}}^2\right)\mathbb{E}\left[\frac{1}{p_{\mathrm{d}}\|\boldsymbol{h}_{\mathrm{d},k}\|^2}\right].\end{aligned} \tag{32}$$

Based on the weak law of large numbers, the random vector $\frac{\boldsymbol{h}_{\mathrm{d},i}}{\|\boldsymbol{h}_{\mathrm{d},k}\|}$ with i.i.d. elements converges in probability towards $\frac{\boldsymbol{h}_{\mathrm{d},i}}{\sqrt{\mathscr{L}_{\mathrm{d},k}N_t}}$ as $N_t\to\infty$, i.e.,

$$\frac{\boldsymbol{h}_{\mathrm{d},i}}{\|\boldsymbol{h}_{\mathrm{d},k}\|}=\frac{\boldsymbol{h}_{\mathrm{d},i}}{\sqrt{\mathscr{L}_{\mathrm{d},k}\sum_{n=1}^{N_t}\left|\left[\widehat{\mathbf{H}}_{\mathrm{d}}\right]_{nk}\right|^2}}\xrightarrow{\mathrm{P}}\frac{\boldsymbol{h}_{\mathrm{d},i}}{\sqrt{\mathscr{L}_{\mathrm{d},k}N_t}},\ \text{as } N_t\to\infty. \tag{33}$$

According the central limit theorem, the random variable $\frac{\boldsymbol{h}_{\mathrm{d},k}^H\boldsymbol{h}_{\mathrm{d},i}}{\sqrt{N_t}}$ converges in distribution to a normal $\mathcal{CN}\left(0,\mathscr{L}_{\mathrm{d},k}\mathscr{L}_{\mathrm{d},i}\right)$ as $N_t\to\infty$, i.e.,

$$\frac{\boldsymbol{h}_{\mathrm{d},k}^H\boldsymbol{h}_{\mathrm{d},i}}{\sqrt{N_t}}\xrightarrow{\mathrm{d}}\mathcal{CN}\left(0,\mathscr{L}_{\mathrm{d},k}\mathscr{L}_{\mathrm{d},i}\right),\ \text{as } N_t\to\infty. \tag{34}$$

Based on (33) and (34), the random variable $\widetilde{h}_{\mathrm{d},i}$ converges in distribution to $\mathcal{CN}\left(0,\mathscr{L}_{\mathrm{d},i}\right)$ as $N_t\to\infty$,

$$\widetilde{h}_{\mathrm{d},i}\xrightarrow{\mathrm{d}}\mathcal{CN}\left(0,\mathscr{L}_{\mathrm{d},i}\right),\ \text{as } N_t\to\infty. \tag{35}$$

Consequently, the term $p_{\mathrm{d}}\sum_{i=1,i\neq k}^{K}\mathbb{E}\left[\left|\widetilde{h}_{\mathrm{d},i}\right|^2\right]$ in (32) is reduced to $p_{\mathrm{d}}\sum_{i=1,i\neq k}^{K}\mathscr{L}_{\mathrm{d},i}$.

On the other hand, from (9) to (11), the i.i.d. elements in the multi-user DIRS-based channel $\mathbf{H}_{\mathrm{D}}$ can be written as

$$\begin{aligned}\left[\mathbf{H}_{\mathrm{D}}\right]_{nk}=&\sqrt{\frac{\varepsilon_n\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},k}}{\varepsilon_n+1}}\sum_{r=1}^{N_{\mathrm{D}}}e^{-j\frac{2\pi}{\lambda}d(n-1)\sin\theta_r}e^{j\varphi_r}\left[\widehat{\mathbf{H}}_{\mathrm{I}}\right]_{rk}\\&+\sqrt{\frac{\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},k}}{\varepsilon_n+1}}\sum_{r=1}^{N_{\mathrm{D}}}\left[\mathbf{G}^{\mathrm{NLOS}}\right]_{rn}^{H}e^{j\varphi_r}\left[\widehat{\mathbf{H}}_{\mathrm{I}}\right]_{rk}.\end{aligned} \tag{36}$$

Assume that the elements in $\mathbf{H}_{\mathrm{D}}$ and $\mathbf{H}_{\mathrm{d}}$ are independent; therefore, we have that

$$\begin{aligned}\mathbb{E}\left[\left|\boldsymbol{h}_{\mathrm{d},i}^{H}\boldsymbol{h}_{\mathrm{D},k}\right|^2\right]&=\mathbb{E}\left[\sum_{n=1}^{N_t}\mathscr{L}_{\mathrm{d},i}\left(\left|\left[\widehat{\mathbf{H}}_{\mathrm{d}}\right]_{ni}\left[\mathbf{H}_{\mathrm{D}}\right]_{nk}\right|^2\right)\right]\\&=\mathscr{L}_{\mathrm{d},i}\sum_{n=1}^{N_t}\mathbb{E}\left[\left|\left[\mathbf{H}_{\mathrm{D}}\right]_{nk}\right|^2\right].\end{aligned} \tag{37}$$

According to (36), the expectation of $\left|\left[\mathbf{H}_{\mathrm{D}}\right]_{nk}\right|^2$ in (37) is given by,

$$\mathbb{E}\left[\left|\left[\mathbf{H}_{\mathrm{D}}\right]_{nk}\right|^2\right]=\mathbb{E}\left[\left[\mathbf{H}_{\mathrm{D}}\right]_{nk}^{H}\left[\mathbf{H}_{\mathrm{D}}\right]_{nk}\right]=\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},k}N_{\mathrm{D}}. \tag{38}$$

As a result, the expectation $p_{\mathrm{d}}\sum_{i=1}^{K}\left|\widetilde{h}_{\mathrm{D},i}\right|^2$ in (32) is reduced to $p_{\mathrm{d}}N_{\mathrm{D}}\sum_{i=1}^{K}\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},i}$. Furthermore, we can reduce the expectation in (31) to

$$\mathbb{E}\left[p_{\mathrm{d}}\sum_{i=1,i\neq k}^{K}\left|\widetilde{h}_{\mathrm{d},i}\right|^2+p_{\mathrm{d}}\sum_{i=1}^{K}\left|\widetilde{h}_{\mathrm{D},i}\right|^2+\sigma_{\mathrm{d}}^2\right]\mathbb{E}\left[\frac{1}{p_{\mathrm{d}}\|\boldsymbol{h}_{\mathrm{d},k}\|^2}\right] \tag{39}$$

$$\xrightarrow{\mathrm{p}}\left(p_{\mathrm{d}}\sum_{i=1,i\neq k}^{K}\mathscr{L}_{\mathrm{d},i}+p_{\mathrm{d}}N_{\mathrm{D}}\sum_{i=1}^{K}\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},i}+\sigma_{\mathrm{d}}^2\right)\mathbb{E}\left[\frac{1}{p_{\mathrm{d}}\|\boldsymbol{h}_{\mathrm{d},k}\|^2}\right]. \tag{40}$$

Next we exploit the following property of a central complex Wishart matrix [42], i.e.,

$$\mathbb{E}\left[\mathrm{tr}\left(\mathbf{W}^{-1}\right)\right]=\frac{m}{n-m}, \tag{41}$$

where $\mathbf{W}\sim\mathcal{W}\left(n,\mathbf{I}_n\right)$ is an $m\times m$ central complex Wishart matrix with n ($n>m$) degrees of freedom. Incorporating (41) into (40), the following equation is obtained:

$$\mathbb{E}\left[\frac{1}{p_{\mathrm{d}}\|\boldsymbol{h}_{\mathrm{d},k}\|^2}\right]=\frac{1}{p_{\mathrm{d}}\left(N_t-1\right)\mathscr{L}_{\mathrm{d},k}},\ \text{for } N_t>2. \tag{42}$$

Combining (42) and (40), the lower bound in Proposition 1, i.e., (17) is then derived.

APPENDIX B
PROOF OF PROPOSITION 2

Based on Jensen's inequality, the ergodic rate $\overline{R}_{\mathrm{d},k}\big|_{\mathrm{ZF}}$ in (8) reduces to

$$\overline{R}_{\mathrm{d},k}\big|_{\mathrm{ZF}}\geq\log_2\left(1+\frac{p_{\mathrm{d}}}{\mathbb{E}\left[p_{\mathrm{d}}\sum_{i=1}^{K}\left|\boldsymbol{w}_k^{H}\boldsymbol{h}_{\mathrm{D},i}\right|^2\right]+\mathbb{E}\left[\sigma_{\mathrm{d}}^2\|\boldsymbol{w}_k\|^2\right]}\right). \tag{43}$$

We can assume that the random vector $\boldsymbol{w}_k$ does not depend on $\boldsymbol{h}_{\mathrm{D},i}$, because the linear detector ZF is designed based on the multi-user direct channel $\mathbf{H}_{\mathrm{d}}$ without relying on $\mathbf{H}_{\mathrm{D}}$. Therefore, based on the definition in (36), we have the following result:

$$\mathbb{E}\left[p_{\mathrm{d}}\sum_{i=1}^{K}\left|\boldsymbol{w}_k^{H}\boldsymbol{h}_{\mathrm{D},i}\right|^2\right]=p_{\mathrm{d}}\sum_{i=1}^{K}\sum_{n=1}^{N_t}\mathbb{E}\left[\left|w_{kn}\right|^2\right]\mathbb{E}\left[\left|\left[\mathbf{H}_{\mathrm{D}}\right]_{ni}\right|^2\right], \tag{44}$$

where w_{kn} denotes the n-th element of the ZF detector vector $\boldsymbol{w}_k$.

According to (38) and (44), (43) is then converted to

$$\begin{aligned}\overline{R}_{\mathrm{d},k}\big|_{\mathrm{ZF}}&\geq\log_2\left(1+\frac{p_{\mathrm{d}}}{\mathbb{E}\left[p_{\mathrm{d}}\sum_{i=1}^{K}\left|\boldsymbol{w}_k^{H}\boldsymbol{h}_{\mathrm{D},i}\right|^2\right]+\mathbb{E}\left[\sigma_{\mathrm{d}}^2\|\boldsymbol{w}_k\|^2\right]}\right)\\&=\log_2\left(1+\frac{p_{\mathrm{d}}}{\left(p_{\mathrm{d}}N_{\mathrm{D}}\sum_{i=1}^{K}\mathscr{L}_{\mathrm{G}}\mathscr{L}_{\mathrm{I},i}+\sigma_{\mathrm{d}}^2\right)\mathbb{E}\left[\|\boldsymbol{w}_k\|^2\right]}\right).\end{aligned} \tag{45}$$

Based on (3), the following form of $\|\boldsymbol{w}_k\|$ can be obtained:

$$\|\boldsymbol{w}_k\|^2=\left[\mathbf{W}^{H}\mathbf{W}\right]_{kk}=\frac{1}{\mathscr{L}_{\mathrm{d},k}}\left[\left(\widehat{\mathbf{H}}_{\mathrm{d}}^{H}\widehat{\mathbf{H}}_{\mathrm{d}}\right)^{-1}\right]_{kk}. \tag{46}$$

Consequently,

$$\mathbb{E}\left[\|\boldsymbol{w}_k\|^2\right]=\frac{1}{K\mathscr{L}_{\mathrm{d},k}}\mathbb{E}\left[\mathrm{tr}\left(\widehat{\mathbf{H}}_{\mathrm{d}}^{H}\widehat{\mathbf{H}}_{\mathrm{d}}\right)^{-1}\right] \tag{47}$$

$$\overset{(a)}{=}\frac{1}{\left(N_t-K\right)\mathscr{L}_{\mathrm{d},k}}, \tag{48}$$

where (a) also comes from the identity (41).

Substituting (48) into (45), the lower bound (18) based on the use of ZF is derived.

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, Third Quarter 2014.

[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Spet. 2016.

[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] P. Christof, J. Pelzl, and B. Prenee, *Understanding Cryptography: A Textbook for Students and Practitioners*. New York, NY, USA: Springer-Verlag, 2010.

[5] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.

[6] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 3, pp. 843–852, May 2016.

[7] O. Besson, P. Stoica, and Y. Kamiya, "Direction finding in the presence of an intermittent interference," *IEEE Trans. Signal Process.*, vol. 50, no. 7, pp. 1554–1564, Jul. 2002.

[8] E. Lance and G. K. Kaleh, "A diversity scheme for a phase-coherent frequency-hopping spread-spectrum system," *IEEE Trans. Commun.*, vol. 45, no. 9, pp. 1123–1129, Sep. 1997.

[9] J. Jeung, S. Jeong, and J. Lim, "Adaptive rapid channel-hopping scheme mitigating smart jammer attacks in secure WLAN," in *Proc. Military Commun. Conf.*, Baltimore, MD, Nov. 2011, pp. 1231–1236.

[10] S. Tomasin, H. Zhang, A. Chorti, and H. V. Poor, "Challenge-response physical layer authentication over partially controllable channels," *IEEE Commun. Mag.*, vol. 60, no. 12, pp. 138–144, Dec. 2022.

[11] H. Zhang and B. Di, "Intelligent omni-surfaces: Simultaneous refraction and reflection for full-dimensional wireless communication," *IEEE Commun. Surv. Tut.*, vol. 24, no. 4, pp. 1997–2028, Aug. 2022.

[12] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface aided wireless communications: A tutorial," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3313–3351, Jan. 2021.

[13] M. A. ElMossallamy, H. Zhang, L. Song, K. G. Seddik, Z. Han, G. Y. Li, "Reconfigurable intelligent surfaces for wireless communications: Principles, challenges, and opportunities," *IEEE Trans. Cogn. Commun.*, vol. 6, no. 3, pp. 990–1002, Sept. 2020.

[14] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, Y.-C. Liang, "Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey," *IEEE Commun. Surv. Tut.*, vol. 22, no. 4, pp. 2283–2314, Fourth Quarter 2020.

[15] S. Zhang and R. Zhang, "Intelligent reflecting surface aided multi-user comunication: Capacity region and deployment strategy," *IEEE Trans. Commun.*, vol. 69, no. 9, pp. 5790–5806, Spet. 2021.

[16] C. Huang, S. Hu, G. C. Alexandropoulos, A. Zappone, C. Yuen, R. Zhang, M. Di Renzo, and M. Debbah, "Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 118–125, Jul. 2020.

[17] B. Lyu, D. T. Hoang, S. Gong, D. Niyato, and D. I. Kim, "IRS-based wireless jamming attacks: When jammers can attack without power," *IEEE Wireless Commun. Lett.*, vol. 9, no. 10, pp. 1663–1667, Oct. 2020.

[18] 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.

[19] L. Wei, C. Huang, G. C. Alexandropoulos, C. Yuen, Z. Zhang, and M. Debbah, "Channel estimation for RIS-empowered multi-user MISO wireless communications," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 4144–4157, Jun. 2021.

[20] C. Huang, R. Mo, and C. Yuen, "Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1839–1850, Aug. 2020.

[21] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, Nov. 2019.

[22] 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.

[23] Y. Wang, H. Lu, D. Zhao, Y. Deng, and A. Nallanathan, "Wireless communication in the presence of illegal reconfigurable intelligent surface: Signal leakage and interference attack," *IEEE Wireless Commun.*, vol. 29, no. 3, pp. 131-138, Jun. 2022.

[24] 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.*, early access, Mar. 2023, doi: 10.1109/TVT.2023.3261303.

[25] M. F. Imani, D. R. Smith, and P. Hougne, "Perfect absorption in a disordered medium with programmable meta-atom inclusions," *Adv. Functional Materials*, vol. 30, no. 52, 2005310, Sept. 2020.

[26] 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.

[27] 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.

[28] 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.

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

[30] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Jamming resilient communication using MIMO interference cancellation," *IEEE Trans. Inf. Forensic Secur.*, vol. 11, no. 7, pp. 1486–1499, Jul. 2016.

[31] K. T. Truong and R. W. Heath Jr., "Effects of channel aging in massive MIMO systems," *J. Commun. Netw-S. Kor.*, vol. 15, no. 4, pp. 338–351, Aug. 2013.

[32] J. Zhang, L. Dai, Z. He, S. Jin, and X. Li, "Performance analysis of mixed-ADC massive MIMO systems over Rician fading channels," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1327–1338, Jun. 2017.

[33] N. Boumal, B. Mishra, P.-A. Absil, and R. Sepulchre, "Manopt, a MATLAB toolbox for optimization on manifolds," *J. Mach. Learn. Res.*, vol. 15, no. 1, pp. 1455–1459, 2014.

[34] W. Tang, M. Z. Chen, X. Chen, J. Y. Dai, Y. Han, M. D. Renzo, Y. Zeng, S. Jin, Q. Cheng, and T. J. Cui, "Wireless communications with reconfigurable intelligent surface: Path loss modeling and experimental measurement," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 421-439, Jan. 2021.

[35] 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.

[36] B. Di, H. Zhang, L. Song, Y. Li, Z. Han, and H. V. Poor, "Hybrid beamforming for reconfigurable intelligent surface based multi-user communications: Achievable rates with limited discrete phase shifts," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1809–1822, Aug. 2020.

[37] B. Di, H. Zhang, L. Li, L. Song, Y. Li, and Z. Han, "Practical hybrid beamforming with finite-resolution phase shifters for reconfigurable intelligent surface based multi-user communications," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4565–4570, Apr. 2020.

[38] Q. Wu and R. Zhang, "Beamforming optimization for wireless network aided by intelligent reflecting surface with discrete phase shifts," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1838–1851, Jan. 2021.

[39] D. J. Torrieri, "Frequency hopping with multiple frequency-shift keying and hard decisions," *IEEE Trans. Commun.*, vol. 32, no. 5, pp. 574–582, May 1984.

[40] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *Proc. 26th Annu. IEEE Int. Conf. Comput. Commun.*, Anchorage, AK, USA, May 2007, pp. 2526–2530.

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

[42] A. M. Tulino, S. Verdú, "Random matrix theory and wireless communications," *Foundations Trends Commun. Inf. Theory*, vol. 1, no. 1, pp. 1-182, Jun. 2004.

APPENDIX C
BIOGRAPHY SECTION

Huan Huang received the M.S. and Ph.D. degrees from the University of Electronic Science and Technology of China (UESTC), in 2019 and 2023, respectively. He currently works at the School of Electronic and Information Engineering, Soochow University. His current research interests include massive MIMO, intelligent reflecting surface-assisted wireless communications, and fiber communications.

Ying Zhang is currently working toward the M.S. degree with the University of Electronic Science and Technology of China, Chengdu, China. Her research interests include intelligent reflecting surface.

Hongliang Zhang (S'15-M'19) received B.S. and Ph.D. degrees at the School of Electrical Engineering and Computer Science at Peking University, in 2014 and 2019, respectively, where he is currently an assistant professor with School of Electronics. His current research interests include reconfigurable intelligent surfaces, aerial access networks, Internet of Things, optimization theory, and game theory. He received the best doctoral thesis award from Chinese Institute of Electronics in 2019. He is also the recipient of 2021 IEEE Comsoc Heinrich Hertz Award for Best Communications Letters and 2021 IEEE ComSoc Asia-Pacific Outstanding Paper Award. He has served as a TPC Member and a workshop co-chair for many IEEE conferences. He is the winner of the Outstanding Leadership Award as the publicity chair for IEEE EUC in 2022. He is currently an Editor for IEEE Transactions on Vehicular Technology, IEEE Communications Letters, IET Communications, and Frontiers in Signal Processing. He has also served as a Guest Editor for several journals, such as IEEE Internet of Things Journal and Journal of Communications and Networks. He is an exemplary reviewer for IEEE Transactions on Communications in 2020.

Yi Cai (S'98-M'01) received the B.S. degree in optical engineering from Beijing Institute of Technology, Beijing, China, in 1992, the M.S. degree in electrical engineering from Shanghai Institute of Technical Physics, Chinese Academy of Sciences, Shanghai, China, in 1998, and the Ph.D. degree in electrical engineering from the University of Maryland Baltimore County, Baltimore, Maryland, USA, in 2001. He joined the Forward-Looking Research group at Tyco Telecommunications (now SubCom) as a Senior Member of Technical Staff in 2001. During the following ten years, he engaged in the research and development of several generations of long-haul submarine transmission systems and he was named a Distinguished Member of Technical Staff of Tyco Telecommunications. In 2011, he joined Huawei USA as a Director of the Optical Business Unit. In 2012, he joined ZTE USA as a Director of Digital Signal Processing. Dr. Cai is a fellow of the Optical Society of America (now Optica). He has published over 120 technical papers in academic conferences and journals, and 19 of these are invited papers. He holds 47 awarded and pending patents. He served as a TPC member for OFC, OECC, Photonic West, ACP. He severed as a technical program sub-committee chair for OFC 2020. His research has been focusing on the application of digital signal processing, coherent detection, advanced modulation formats, and forward error correction for optical fiber transmissions.

Lee Swindlehurst received the B.S. (1985) and M.S. (1986) degrees in Electrical Engineering from Brigham Young University (BYU), and the Ph.D. (1991) degree in Electrical Engineering from Stanford University. He was with the Department of Electrical and Computer Engineering at BYU from 1990-2007, and during 1996-97, he held a joint appointment as a visiting scholar at Uppsala University and the Royal Institute of Technology in Sweden. From 2006-07, he was on leave working as Vice President of Research for ArrayComm LLC in San Jose, California. Since 2007 he has been a Professor in the Electrical Engineering and Computer Science (EECS) Department at the University of California Irvine. During 2014-17 he was also a Hans Fischer Senior Fellow in the Institute for Advanced Studies at the Technical University of Munich. In 2016, he was elected as a Foreign Member of the Royal Swedish Academy of Engineering Sciences (IVA). His research focuses on array signal processing for radar, wireless communications, and biomedical applications, and he has over 400 publications in these areas. Dr. Swindlehurst is a Fellow of the IEEE and was the inaugural Editor-in-Chief of the IEEE Journal of Selected Topics in Signal Processing. He received the 2000 IEEE W. R. G. Baker Prize Paper Award, the 2006 IEEE Communications Society Stephen O. Rice Prize in the Field of Communication Theory, the 2006, 2010 and 2021 IEEE Signal Processing Societys Best Paper Awards, the 2017 IEEE Signal Processing Society Donald G. Fink Overview Paper Award, a Best Paper award at the 2020 IEEE International Conference on Communications, and the 2022 Claude Shannon-Harry Nyquist Technical Achievement Award from the IEEE Signal Processing Society.

Zhu Han (S'01-M'04-SM'09-F'14) received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively. From 2000 to 2002, he was an R&D Engineer of JDSU, Germantown, Maryland. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an assistant professor at Boise State University, Idaho. Currently, he is a John and Rebecca Moores Professor in the Electrical and Computer Engineering Department as well as in the Computer Science Department at the University of Houston, Texas. Dr. Han's main research targets on the novel game-theory related concepts critical to enabling efficient and distributive use of wireless networks with limited resources. His other research interests include wireless resource allocation and management, wireless communications and networking, quantum computing, data science, smart grid, security and privacy. Dr. Han received an NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the Journal on Advances in Signal Processing in 2015, IEEE Leonard G. Abraham Prize in the field of Communications Systems (best paper award in IEEE JSAC) in 2016, and several best paper awards in IEEE conferences. Dr. Han was an IEEE Communications Society Distinguished Lecturer from 2015-2018, AAAS fellow since 2019, and ACM distinguished Member since 2019. Dr. Han is a 1% highly cited researcher since 2017 according to Web of Science. Dr. Han is also the winner of the 2021 IEEE Kiyo Tomiyasu Award, for outstanding early to mid-career contributions to technologies holding the promise of innovative applications, with the following citation: "for contributions to game theory and distributed management of autonomous communication networks."