Illegal Intelligent Reflecting Surface Based Active Channel Aging: When Jammer Can Attack Without Power and CSI

Huan Huang, *Student Member, IEEE,* Ying Zhang, Hongliang Zhang, *Member, IEEE,*
Chongfu Zhang, *Senior Member, IEEE,* and Zhu Han, *Fellow, IEEE*

***Abstract*—Illegal intelligent reflecting surfaces (I-IRSs), i.e., the illegal deployment and utilization of IRSs, impose serious harmful impacts on wireless networks. The existing I-IRS-based illegal jammer (IJ) requires channel state information (CSI) or extra power or both, and therefore, the I-IRS-based IJ seems to be difficult to implement in practical wireless networks. To raise concerns about significant potential threats posed by I-IRSs, we propose an alternative method to jam legitimate users (LUs) without relying on the CSI. By using an I-IRS to actively change wireless channels, the orthogonality of multi-user beamforming vectors and the co-user channels is destroyed, and significant inter-user interference is then caused, which is referred to as active channel aging. Such a fully-passive jammer (FPJ) can launch jamming attacks on multi-user multiple-input single-output (MU-MISO) systems via inter-user interference caused by active channel aging, where the IJ requires no additional transmit power and instantaneous CSI. The simulation results show the effectiveness of the proposed FPJ scheme. Moreover, we also investigate how the transmit power and the number of quantization phase shift bits influence the jamming performance.**

***Index Terms*—Intelligent reflecting surface, jamming attacks, multi-user MISO, low-power wireless networks.**

I. Introduction

DUE to the intrinsic characteristics of wireless channels, i.e., broadcast and superposition, wireless networks are vulnerable to jamming attacks (also referred as to interference attacks), and it is difficult to protect transmitted signals from unauthorized recipients [1]. Intelligent reflecting surfaces (IRSs) has been an emerging wireless technology for 5G, 6G and beyond [2], [3]. Legitimate IRSs can be used to provide an important approach for enhancing the physical layer security (PLS) in wireless networks [4], [5].

Therefore, many previous studies have investigated the use of legitimate IRSs to improve PLS [6], [7]. In [6], IRSs combined with artificial noise (AN) or friendly jamming at the access point (AP) are used for security enhancement in the presence of illegal eavesdroppers. In [7], the authors proposed an IRS-assisted anti-jamming scheme against jamming attacks, where a friendly IRS is used to prevent the illegal jammer (IJ) from jamming legitimate users (LUs). Note that the legitimate AP in the legitimate IRS aided scenario knows the legitimate IRS's information, like its location, and can control the reflecting phase shifts of the legitimate IRS.

In contrast, illegal IRSs (I-IRSs) represent the illegal deployment and utilization of IRSs [8], where the legitimate AP does not know the I-IRSs' information and also can not control the I-IRSs. Due to the passive nature, the I-IRSs are hard to be detect. Consequently, the I-IRSs impose a more serious harmful impact on PLS. For example, an I-IRS has been employed to deteriorate signals at LUs in the presence of jamming attacks [8], where the I-IRS aggravates the AN generated by the IJ to reduce the received signal-to-noise ratio (SNR) or the signal-to-interference-noise ratio (SINR). However, there are two requirements in existing methods to achieve the I-IRS-based IJ.

1) I-IRSs need to know the channel state information (CSI) of all channels involved. Yet, the uplink channel estimation for IRS-aided channels remains difficult due to the passive nature of IRSs [9]. Acquiring the I-IRS-aided channels' CSI at IJ is too idealistic to implement in practice. Although illegal jamming can be achieved without the CSI by broadcasting the AN [10], the performance gain obtained by implementing an I-IRS, in this case, is limited as reflecting phase shifts of the I-IRS are hard to optimize without the CSI.

2) A large amount of power is needed to transmit jamming signals continuously. Even a few papers attempt to realize an I-IRS-based passive jammer (PJ) without the transmit power for single-user systems [11], which minimizes the received power at the LU by destructively adding the signal from the AP-IRS-User channel. However, this I-IRS-based PJ still requires the CSI of IRS-aided channels to optimize the I-IRS's reflecting phase shifts.

Limited by these two requirements above, especially the CSI acquisition, the I-IRS-based IJ seems to be difficult to implement in practical wireless networks. So in this paper, we try to answer the following research question: *Can IJs jam LUs without both the transmit power and the CSI?*

To draw attention to the impact of I-IRSs on multi-user multiple-input single-output (MU-MISO) systems, we propose an I-IRS-based fully-passive jammer (FPJ) that can launch jamming attacks without relying on the transmit power and the CSI. To the best of our knowledge, it is the first time that an IJ can jam LUs without the CSI.

- An I-IRS is exploited to actively change wireless channels, and therefore, the orthogonality of the multi-user

This work was supported by the National Key R&D Program of China (2018YFB1801302), and partially supported by NSF CNS-2107216, CNS-2128368, CMMI-2222810, US Department of Transportation, Toyota and Amazon. (*Corresponding author: Chongfu Zhang*)

H. Huang, Y. Zhang, and C. Zhang are with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: hhuang@std.uestc.edu.cn; yzhang1@std.uestc.edu.cn; cfzhang@uestc.edu.cn).

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

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).

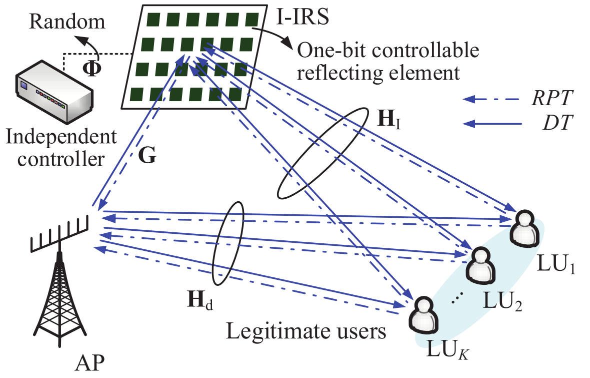

Fig. 1. Illustration of a MU-MISO system jammed by the I-IRS-based FPJ, where phase shifts of the I-IRS are randomly generated by the independent I-IRS controller. RPT: reverse pilot transmission; DT: data transmission.

active beamforming vectors and the co-user channels is destroyed, which is referred to as **active channel aging**[1].

- During *the reverse pilot transmission (RPT) phase*, we randomly generate reflecting phase shifts for the I-IRS. During *the data transmission (DT) phase*, we randomly generate other reflecting phase shifts. The I-IRS acts like a **"disco ball"** without optimizing its phase shifts based on the CSI. The resulting serious inter-user interference due to active channel aging jams the LUs effectively.

Notation: We use bold capital type for a matrix, e.g., $\boldsymbol{\Phi}$, small bold type for a vector, e.g., $\boldsymbol{\varphi}$, and italic type for a scalar, e.g., K. Moreover, the superscripts $(\cdot)^H$ and $(\cdot)^T$ denote the Hermitian transpose and the transpose. Moreover, the symbols $|\cdot|$ and $\|\cdot\|$ denote the absolute value and the Frobenius norm.

II. System Statement

In this section, first, we describe the general mode of an MU-MISO system jammed by the I-IRS-based FPJ. Then, we give the optimization metric and state the two communications phases: *the RPT phase* and *the DT phase*.

A. System Model and Channel Model

Figure 1 schematically illustrates a MU-MISO system jammed by the I-IRS-based FPJ, where the legitimate AP is equipped with an N_A-element uniform linear array (ULA) and communicates with K single-antenna LUs termed $\mathrm{LU}_1, \mathrm{LU}_2, \cdots, \mathrm{LU}_K$. An I-IRS comprised of N_I one-bit controllable reflecting elements is deployed near the AP[2] to jam LUs. When the data signal $s_k \in \mathbb{C}$ for LU_k $(1 \leq k \leq K)$ is normalized to unit power, the signal received at LU_k is expressed as

$$y_k = \boldsymbol{h}_{\mathrm{com},k}^H \sum_{u=1}^{K} \boldsymbol{w}_u s_u + n_k, \tag{1}$$

where $\boldsymbol{h}_{\mathrm{com},k}^H = \left(\boldsymbol{h}_{\mathrm{I},k}^H \boldsymbol{\Phi} \mathbf{G} + \boldsymbol{h}_{\mathrm{d},k}^H\right) \in \mathbb{C}^{1\times N_\mathrm{A}}$ denotes the combined channel between the legitimate AP and LU_k, $\boldsymbol{h}_{\mathrm{I},k} \in \mathbb{C}^{N_\mathrm{I}\times 1}$ denotes the channel between the I-IRS and LU_k, $\mathbf{G} \in \mathbb{C}^{N_\mathrm{I}\times N_\mathrm{A}}$ denotes the channel between the legitimate AP and the I-IRS, and $\boldsymbol{h}_{\mathrm{d},k} \in \mathbb{C}^{N_\mathrm{A}\times 1}$ denotes the direct channel between the legitimate AP and LU_k.

In (1), $\boldsymbol{\Phi} = \mathrm{diag}(\boldsymbol{\varphi}) \in \mathbb{C}^{N_\mathrm{I}\times N_\mathrm{I}}$ represents the reflecting matrix of the I-IRS, where the one-bit reflecting vector $\boldsymbol{\varphi}$ is expressed as $\boldsymbol{\varphi} = \left[e^{j\varphi_1}, \cdots, e^{j\varphi_{N_I}}\right]^H$, and $\varphi_n \in \Omega = \{0, \pi\}$ $(1 \leq n \leq N_\mathrm{I})$ denotes reflecting phase shift of the n-th reflecting element. The independent I-IRS controller generates $\boldsymbol{\varphi}$ and then controls the I-IRS to implement the corresponding phase shifts. Besides, $\boldsymbol{w}_k$ denotes the active beamforming at the AP for LU_k, and n_k denotes the additive white Gaussian noise with 0 mean and σ^2 variance, i.e., $n_k \sim \mathcal{CN}\left(0, \sigma^2\right)$.

For ease of representation, we further define the multi-user direct channel between the AP and the LUs, the multi-user channel between the I-IRS and the LUs, as well as the multi-user combined channel between the AP and all LUs as $\mathbf{H}_\mathrm{d}^H = \left[\boldsymbol{h}_{\mathrm{d},1}, \boldsymbol{h}_{\mathrm{d},2}, \cdots, \boldsymbol{h}_{\mathrm{d},K}\right]^H$, $\mathbf{H}_\mathrm{I}^H = \left[\boldsymbol{h}_{\mathrm{I},1}, \boldsymbol{h}_{\mathrm{I},2}, \cdots, \boldsymbol{h}_{\mathrm{I},K}\right]^H$, and $\mathbf{H}_\mathrm{com}^H = \left[\boldsymbol{h}_{\mathrm{com},1}, \boldsymbol{h}_{\mathrm{com},2}, \cdots, \boldsymbol{h}_{\mathrm{com},K}\right]^H$, respectively. Furthermore, the multi-user active beamforming at the AP is denoted as $\mathbf{W} = [\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_K]$.

The multi-user direct channel $\mathbf{H}_\mathrm{d}$ follows Rayleigh fading, while the IRS-aided channels $\mathbf{G}$ and $\boldsymbol{h}_{\mathrm{I},k}$ follow Rician fading [14]. Specifically, $\mathbf{G}$ and $\boldsymbol{h}_{\mathrm{I},k}$ are modeled as

$$\begin{aligned} \mathbf{G} &= \mathscr{L}_\mathrm{G}\left(\sqrt{\frac{\kappa_\mathrm{G}}{1+\kappa_\mathrm{G}}}\mathbf{G}^\mathrm{LOS} + \sqrt{\frac{1}{1+\kappa_\mathrm{G}}}\mathbf{G}^\mathrm{NLOS}\right), \\ \boldsymbol{h}_{\mathrm{I},k} &= \mathscr{L}_{\mathrm{I},k}\left(\sqrt{\frac{\kappa_\mathrm{I}}{1+\kappa_\mathrm{I}}}\boldsymbol{h}_{\mathrm{I},k}^\mathrm{LOS} + \sqrt{\frac{1}{1+\kappa_\mathrm{I}}}\boldsymbol{h}_{\mathrm{I},k}^\mathrm{NLOS}\right), \end{aligned} \tag{2}$$

where $\mathscr{L}_\mathrm{G}$ and $\mathscr{L}_{\mathrm{I},k}$ represent the large-scale path loss between the AP and the I-IRS and that between the I-IRS and LU_k, and κ_G and κ_I are the Rician factors of $\mathbf{G}$ and $\boldsymbol{h}_{\mathrm{I},k}$.

In (2), $\mathbf{G}^\mathrm{LOS}$ and $\boldsymbol{h}_{\mathrm{I},k}^\mathrm{LOS}$ are the line-of-sight (LOS) components of $\mathbf{G}$ and $\boldsymbol{h}_{\mathrm{I},k}$, and $\mathbf{G}^\mathrm{NLOS}$ and $\boldsymbol{h}_{\mathrm{I},k}^\mathrm{NLOS}$ are non-line-of-sight (NLOS) components. The NLOS components follow Rayleigh fading, while the LOS components are [14]

$$\begin{aligned} \mathbf{G}^\mathrm{LOS} &= \sqrt{N_\mathrm{I} N_\mathrm{A}}\boldsymbol{\alpha}_\mathrm{I}(\vartheta, \theta)\boldsymbol{\alpha}_\mathrm{A}^H(\phi), \\ \boldsymbol{h}_{\mathrm{I},k}^\mathrm{LoS} &= \sqrt{N_\mathrm{I}}\boldsymbol{\alpha}_\mathrm{I}(\vartheta_{\mathrm{I},k}, \theta_{\mathrm{I},k}), \end{aligned} \tag{3}$$

where $\boldsymbol{\alpha}_\mathrm{A}$ and $\boldsymbol{\alpha}_\mathrm{I}$ are the array responses [14].

B. Wireless Communications: The RPT and DT Phases

In practice, the main aim of a MU-MISO system is to maximize a certain performance metric that generally is a strictly-increasing utility function of SINR [15]. Specifically, a widely-used performance metric is the sum rate, which is expressed as $R_\mathrm{sum} = \sum_{k=1}^{K} R_k = \sum_{k=1}^{K} \log_2(1+\gamma_k)$. According to (1), the received SINR γ_k at LU_k is stated as,

$$\gamma_k = \frac{\left|\boldsymbol{h}_{\mathrm{com},k}^H \boldsymbol{w}_k\right|^2}{\sum\limits_{u\neq k}\left|\boldsymbol{h}_{\mathrm{com},k}^H \boldsymbol{w}_u\right|^2 + \sigma^2}. \tag{4}$$

[1] Channel aging is CSI inaccuracy due to time variation of wireless channels and delays in the computation [12]. In this work, we actively introduce CSI inaccuracy by using an I-IRS. To differentiate, we call it active channel aging.

[2] Based on the existing literature on the IRS's deployment location [13], the IRS should be deployed as close to users or as close to the AP as possible to increase its effect. Yet, in the jamming scenario, we make the more robust assumption that the IJ does not know any information about LUs, for instance, LUs' locations and CSI. Therefore, we deploy the I-IRS near the AP.

1) Acquiring CSI During The RPT Phase: From (4), it can be seen that the optimization of multi-user active beamforming $\mathbf{W} = [\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_K]$ at the AP aims to maximize the signal term $\left|\boldsymbol{h}_{\mathrm{com},k}^H \boldsymbol{w}_k\right|$ while minimizing the inter-user interference term $\sum_{u \neq k} \left|\boldsymbol{h}_{\mathrm{com},k}^H \boldsymbol{w}_u\right|$. In order to optimize $\mathbf{W}$, the CSI of $\mathbf{H}_{\mathrm{com}}$ must be obtained at the AP[3]. Generally, the CSI can be acquired during *the RPT phase* according to the pilot estimation, as shown in Fig. 1. More specifically, to acquire the CSI of $\boldsymbol{h}_{\mathrm{com},k}$, the LU_k sends pilot signals to the legitimate AP, and the AP then estimates $\boldsymbol{h}_{\mathrm{com},k}$ by certain traditional solutions, for instance, the least square (LS) algorithm [9].

2) Precoding During The DT Phase: Based on the obtained CSI in *the RPT phase*, the multi-user active beamforming used during *the DT phase* can be designed. Generally, the multi-user active beamforming optimization problem is a nondeterministic polynomial-time (NP)-hard problem, and therefore, computing the optimal multi-user active beamforming is difficult. To this end, some heuristic beamforming designs, which can achieve near-optimal performance, have been investigated.

A widely known beamforming solution is the zero-forcing beamforming (ZFBF) algorithm [15], which causes zero inter-user interference. Specifically, the multi-user active beamforming $\mathbf{W}_{\mathrm{ZF}}$ computed via the ZFBF algorithm is written as

$$\mathbf{W}_{\mathrm{ZF}} = \frac{\mathbf{H}_{\mathrm{com}}\left(\mathbf{H}_{\mathrm{com}}^H \mathbf{H}_{\mathrm{com}}\right)^{-1} \mathbf{P}^{\frac{1}{2}}}{\left\|\mathbf{H}_{\mathrm{com}}\left(\mathbf{H}_{\mathrm{com}}^H \mathbf{H}_{\mathrm{com}}\right)^{-1}\right\|^2}, \tag{5}$$

where $\mathbf{P}^{\frac{1}{2}} = \mathrm{diag}\left(\sqrt{p_1}, \sqrt{p_2}, \cdots, \sqrt{p_K}\right)$, and p_k represents the transmit power allocated to LU_k. The power allocation must satisfy the constraint that $\sum_{k=1}^K p_k \leq P_0$, where P_0 is the total transmit power at the AP. The optimal power allocation can be calculated by the water-filling algorithm [15].

3) Orthogonal Interference Subspace: According to (4), the ratio of inter-user interference to noise (I/N) $\mathscr{I}$ is equal to

$$\mathscr{I} = \sum_{k=1}^K \sum_{u \neq k} \frac{\left|\boldsymbol{h}_{\mathrm{com},k}^H \boldsymbol{w}_u\right|^2}{\sigma^2}. \tag{6}$$

Incorporating (5) into (6), it is clear that $\mathscr{I} = 0$ due to the presence of the pseudoinverse $\left(\mathbf{H}_{\mathrm{com}}^H \mathbf{H}_{\mathrm{com}}\right)^{-1}$. In other words, ZFBF causes zero inter-user interference by projecting the user channel $\boldsymbol{h}_{\mathrm{com},k}$ onto the subspace that is orthogonal to the co-user channels $\boldsymbol{h}_{\mathrm{com},1}, \cdots, \boldsymbol{h}_{\mathrm{com},k-1}, \boldsymbol{h}_{\mathrm{com},k+1}, \cdots, \boldsymbol{h}_{\mathrm{com},K}$, i.e., the orthogonal interference subspace.

III. I-IRS-based Fully-Passive Jammer via Active Channel Aging

To raise concerns about the potential threat that an I-IRS could launch jamming attacks without the transmit power or even the CSI, we introduce a CSI-based PJ without the transmit power in Section III-A, i.e., the extension of [11]. Furthermore, the results from the CSI-based PJ are used as benchmarks. In Section III-B, we propose an I-IRS-based FPJ via active channel aging. By destroying the orthogonality of the multi-user active beamforming vectors and the co-user channels, the proposed I-IRS-based FPJ can jam LUs without the transmit power and the CSI.

A. CSI-Based Jamming Attacks Without Power

To implement the extension of [11], it is necessary to consider the most ideal case for jamming attacks: the legitimate AP only knows the CSI of $\mathbf{H}_{\mathrm{d}}$ and then calculates the multi-user active beamforming $\mathbf{W}_{\mathrm{d}}$ via the ZFBF algorithm, while the independent I-IRS controller knows the CSI of $\mathbf{H}_{\mathrm{d}}$, $\mathbf{H}_{\mathrm{I}}$, and $\mathbf{G}$ as well as $\mathbf{W}_{\mathrm{d}}$. The CSI-based PJ can launch jamming attacks without the transmit power, where the reflecting vector for the I-IRS is optimized by minimizing a certain performance metric. Taking the example of minimizing the sum rate R_{sum} received at LUs, the optimization of the one-bit reflecting vector is mathematically represented as

$$\min_{\boldsymbol{\varphi}} R_{\mathrm{sum}} = \min_{\boldsymbol{\varphi}} \sum_{k=1}^K \log_2\left(1 + \frac{\left|\boldsymbol{h}_{\mathrm{com},k}^H \boldsymbol{w}_{\mathrm{d},k}\right|^2}{\sum\limits_{u \neq k} \left|\boldsymbol{h}_{\mathrm{com},k}^H \boldsymbol{w}_{\mathrm{d},u}\right|^2 + \sigma^2}\right) \tag{7}$$

$$\text{s.t.} \;\; \varphi_n \in \Omega, n = 1, 2, \cdots, N_{\mathrm{I}}. \tag{8}$$

The phase shift optimization problem in (7) can be solved by enumerating all possible $\{\varphi_n\}_{n=1}^{N_{\mathrm{I}}}$ combinations. However, there are $2^{N_{\mathrm{I}}}$ different combinations, and thus the computational complexity is large.

To this end, we first relax the discrete phase shift constraint in (8) to a continuous constraint. Mathematically, the reflecting vector optimization is relaxed to

$$\max_{\bar{\boldsymbol{\varphi}}} \sum_{k=1}^K -\log_2\left(1 + \frac{\left|\left(\bar{\boldsymbol{\varphi}} \mathrm{diag}(\boldsymbol{h}_{\mathrm{I},k}^H)\mathbf{G} + \boldsymbol{h}_{\mathrm{d},k}^H\right)\boldsymbol{w}_{\mathrm{d},k}\right|^2}{\sum\limits_{u \neq k} \left|\left(\bar{\boldsymbol{\varphi}} \mathrm{diag}(\boldsymbol{h}_{\mathrm{I},k}^H)\mathbf{G} + \boldsymbol{h}_{\mathrm{d},k}^H\right)\boldsymbol{w}_{\mathrm{d},u}\right|^2 + \sigma^2}\right) \tag{9}$$

$$\text{s.t.} \;\; \bar{\varphi}_n \in [0, 2\pi], n = 1, 2, \cdots, N_{\mathrm{I}}. \tag{10}$$

The objective function in (9) is then a continuous and differentiable function of $\bar{\boldsymbol{\varphi}}$, and the constraint in (10) creates a complex circle manifold. Therefore, the optimization problem in (9) can be computed by the Riemannian conjugate gradient (RCG) algorithm [16]. After computing the continuous reflecting vector $\bar{\boldsymbol{\varphi}}$, the discrete reflecting vector is obtained by

$$\min_{\boldsymbol{\varphi}} \|\boldsymbol{\varphi} - \bar{\boldsymbol{\varphi}}\|^2 \tag{11}$$
$$\text{s.t.} \;\; (8).$$

The complexity of the benchmarking CSI-based PJ is $\mathcal{O}\left(I_{\mathrm{R}} K^2 N_{\mathrm{I}}^2\right)$, where I_{R} represents the iteration times of the RCG algorithm. In each iteration, the complexity comes mainly from calculating the Euclidean gradient [16]. Specifically, the complexity of the Euclidean gradient calculation is

[3] In the MU-MISO system under I-IRS-based jamming attacks, it is impractical to acquire the CSI of IRS-aided channels and the direct channel, respectively. The legitimate AP cannot know any information about the I-IRS, like its location, much less jointly train the IRS-based channels with the I-IRS. Namely, the legitimate AP can only obtain the CSI of $\mathbf{H}_{\mathrm{com}}$. Note that the CSI of $\mathbf{H}_{\mathrm{com}}$ is easily obtained at the legitimate AP when $\boldsymbol{\Phi}$ is determined, which is the traditional MISO channel estimation. The phase shifts of the I-IRS are generated at random by the independent I-IRS controller, and therefore, $\boldsymbol{\Phi}$ is always determined for the legitimate AP, as shown in Fig. 1.

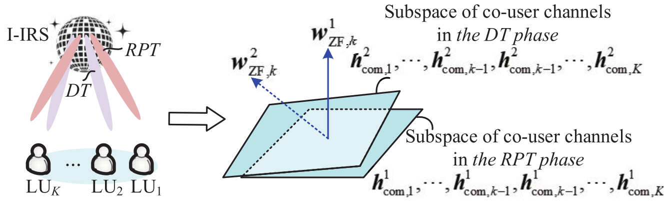
I-IRS
RPT
DT
$\boldsymbol{w}_{\mathrm{ZF},k}^{1}$
$\boldsymbol{w}_{\mathrm{ZF},k}^{2}$
Subspace of co-user channels in *the DT phase*
$\boldsymbol{h}_{\mathrm{com},1}^{2},\cdots,\boldsymbol{h}_{\mathrm{com},k-1}^{2},\boldsymbol{h}_{\mathrm{com},k-1}^{2},\cdots,\boldsymbol{h}_{\mathrm{com},K}^{2}$
Subspace of co-user channels in *the RPT phase*
$\boldsymbol{h}_{\mathrm{com},1}^{1},\cdots,\boldsymbol{h}_{\mathrm{com},k-1}^{1},\boldsymbol{h}_{\mathrm{com},k-1}^{1},\cdots,\boldsymbol{h}_{\mathrm{com},K}^{1}$
LU_K ··· LU_2 LU_1

Fig. 2. I-IRS-based FPJ via **active channel aging**, where the I-IRS acts like a **“disco ball”** and ZFBF cannot project the user channel to the orthogonal interference subspace.

$\mathcal{O}\big(K^2N_{\mathrm{I}}^2\big)$. Moreover, the complexity of the discreteization of $\bar{\varphi}$ expressed by (11) is $\mathcal{O}(2N_{\mathrm{I}})$. When the number of reflecting elements packed on the I-IRS is large ($N_{\mathrm{I}} \gg 1$), the complexity of the discreteization, i.e., $\mathcal{O}(2N_{\mathrm{I}})$, can be ignored.

B. I-IRS-Based Jamming Attacks Without Power and CSI

Although the CSI-based PJ proposed in Section III-A can jam without the transmit power, the CSI of all channels needs to be obtained at the independent I-IRS controller, which is difficult to satisfy in practice. In wireless communications, the AP needs to obtain the CSI during *the RPT phase* before *the DT phase*, as stated in Section II-B.

1) The RPT Phase: During *the RPT phase*, the one-bit reflecting vector for the I-IRS is generated by tuning the n-th reflecting element to a random phase shift belonging to Ω, i.e., $\varphi_n^1 \sim \mathscr{U}(\Omega)$. More particularly, the reflecting vector $\boldsymbol{\varphi}^1$ follows the uniform distribution denoted $\boldsymbol{\varphi}^1 \sim \mathscr{U}\left(\Omega^{N_{\mathrm{I}}}\right)$. It is worth noting that the independent I-IRS controller in the proposed scheme does not need to optimize the reflecting phase shifts of the I-IRS.

Consequently, the multi-user combined channel estimated by the AP is written as

$$\begin{aligned}(\mathbf{H}_{\mathrm{com}}^1)^H &= \mathbf{H}_{\mathrm{I}}^H \mathrm{diag}\left(\boldsymbol{\varphi}^1\right)\mathbf{G} + \mathbf{H}_{\mathrm{d}}^H \\ &= \left[\boldsymbol{h}_{\mathrm{com},1}^1, \boldsymbol{h}_{\mathrm{com},2}^1, \cdots, \boldsymbol{h}_{\mathrm{com},K}^1\right]^H. \end{aligned} \tag{12}$$

Based on $\mathbf{H}_{\mathrm{com}}^1$, the AP can compute the multi-user active beamforming used in *the DT phase* that is expressed as

$$\begin{aligned}\mathbf{W}_{\mathrm{ZF}}^1 &= \frac{\mathbf{H}_{\mathrm{com}}^1\left((\mathbf{H}_{\mathrm{com}}^1)^H\mathbf{H}_{\mathrm{com}}^1\right)^{-1}\mathbf{P}^{\frac{1}{2}}}{\left\|\mathbf{H}_{\mathrm{com}}^1((\mathbf{H}_{\mathrm{com}}^1)^H\mathbf{H}_{\mathrm{com}}^1)^{-1}\right\|^2} \\ &= \left[\boldsymbol{w}_{\mathrm{ZF},1}^1, \boldsymbol{w}_{\mathrm{ZF},2}^1, \cdots, \boldsymbol{w}_{\mathrm{ZF},K}^1\right], \end{aligned} \tag{13}$$

where $\boldsymbol{w}_{\mathrm{ZF},k}^1$ is orthogonal to the subspace of the co-user channels $\boldsymbol{h}_{\mathrm{com},1}^1, \cdots, \boldsymbol{h}_{\mathrm{com},k-1}^1, \boldsymbol{h}_{\mathrm{com},k+1}^1, \cdots, \boldsymbol{h}_{\mathrm{com},K}^1$.

2) The DT Phase: Then, during *the DT phase*, the one-bit reflecting vector of the I-IRS is formed according to another reflecting vector $\boldsymbol{\varphi}^2$ that also follows the uniform distribution in Ω, i.e., $\boldsymbol{\varphi}^2 \sim \mathscr{U}\left(\Omega^{N_{\mathrm{I}}}\right)$. Therefore, during *the DT phase*, the multi-user combined channel is changed to

$$\begin{aligned}(\mathbf{H}_{\mathrm{com}}^2)^H &= \mathbf{H}_{\mathrm{I}}^H \mathrm{diag}\left(\boldsymbol{\varphi}^2\right)\mathbf{G} + \mathbf{H}_{\mathrm{d}}^H \\ &= \left[\boldsymbol{h}_{\mathrm{com},1}^2, \boldsymbol{h}_{\mathrm{com},2}^2, \cdots, \boldsymbol{h}_{\mathrm{com},K}^2\right]^H. \end{aligned} \tag{14}$$

As illustrated in Fig. 2, $\boldsymbol{w}_{\mathrm{ZF},k}^1$ is orthogonal to the subspace of $\boldsymbol{h}_{\mathrm{com},1}^1, \cdots, \boldsymbol{h}_{\mathrm{com},k-1}^1, \boldsymbol{h}_{\mathrm{com},k+1}^1, \cdots, \boldsymbol{h}_{\mathrm{com},K}^1$ instead of that of $\boldsymbol{h}_{\mathrm{com},1}^2, \cdots, \boldsymbol{h}_{\mathrm{com},k-1}^2, \boldsymbol{h}_{\mathrm{com},k+1}^2, \cdots, \boldsymbol{h}_{\mathrm{com},K}^2$. Based on (14), the active beamforming that orthogonal to the subspace of $\boldsymbol{h}_{\mathrm{com},1}^2, \cdots, \boldsymbol{h}_{\mathrm{com},k-1}^2, \boldsymbol{h}_{\mathrm{com},k+1}^2, \cdots, \boldsymbol{h}_{\mathrm{com},K}^2$ is given by

$$\begin{aligned}\mathbf{W}_{\mathrm{ZF}}^2 &= \frac{\mathbf{H}_{\mathrm{com}}^2\left((\mathbf{H}_{\mathrm{com}}^2)^H\mathbf{H}_{\mathrm{com}}^2\right)^{-1}\mathbf{P}^{\frac{1}{2}}}{\left\|\mathbf{H}_{\mathrm{com}}^2((\mathbf{H}_{\mathrm{com}}^2)^H\mathbf{H}_{\mathrm{com}}^2)^{-1}\right\|^2} \\ &= \left[\boldsymbol{w}_{\mathrm{ZF},1}^2, \boldsymbol{w}_{\mathrm{ZF},2}^2, \cdots, \boldsymbol{w}_{\mathrm{ZF},K}^2\right]. \end{aligned} \tag{15}$$

Including (13) and (14) into (4), the actual received SINR $\bar{\gamma}_k$ at LU_k during *the DT phase* is

$$\bar{\gamma}_k = \frac{\left|(\boldsymbol{h}_{\mathrm{com},k}^2)^H \boldsymbol{w}_{\mathrm{ZF},k}^1\right|^2}{\sum\limits_{u \neq k}\left|(\boldsymbol{h}_{\mathrm{com},k}^2)^H \boldsymbol{w}_{\mathrm{ZF},u}^1\right|^2 + \sigma^2}. \tag{16}$$

The complexity of our proposed scheme comes from randomly generating the two reflecting vectors used in *the RPT phase* and *the DT phase*, which is only $\mathcal{O}(2N_{\mathrm{I}})$. Compared with the benchmarking CSI-based PJ, the I-IRS's controller in the proposed I-IRS-based FPJ not only does not require the CSI of all channels involved, but also the complexity of the proposed I-IRS-based FPJ is much lower.

3) Active Channel Aging: Based on (13) and (14), the reflecting vectors for the I-IRS are different and random during *the RPT phase* and *the DT phase* (like a “disco ball” shown in Fig. 2), which destroys the orthogonality generated from ZFBF due to active channel aging. The $\boldsymbol{w}_{\mathrm{ZF},k}^1$ in (13) is only orthogonal to the subspace of co-user channels $\boldsymbol{h}_{\mathrm{com},1}^1, \cdots, \boldsymbol{h}_{\mathrm{com},k-1}^1, \boldsymbol{h}_{\mathrm{com},k+1}^1, \cdots, \boldsymbol{h}_{\mathrm{com},K}^1$, while the multi-user combined channel during *the DT phase* is changed to $\mathbf{H}_{\mathrm{com}}^2$. Consequently, $\mathscr{I}$ in (6) is equal to $\sum_{k=1}^{K}\sum_{u \neq k}\frac{\left|(\boldsymbol{h}_{\mathrm{com},k}^2)^H \boldsymbol{w}_{\mathrm{ZF},u}^1\right|^2}{\sigma^2}$, which is no longer zero due to active channel aging. It is worth noting that $\mathscr{I}$ in (6) is equal to zero 0 when and only when the multi-user active beamforming is computed by (15). The orthogonality of the multi-user active beamforming vectors and the co-user channels is destroyed, and significant inter-user interference is then caused.

As a result, the actual received SINR $\bar{\gamma}_k$ in (16) achieved under the proposed I-IRS-based FPJ is dramatically reduced compared to that without attacks. We stated that the reflecting vector for the I-IRS is different during *the RPT phase* and *the DT phase*. In fact, there is no need for precise synchronization in practical implementation. Assuming that the periods of *the RPT phase* and *the DT phase* are T_{r} and T_{d} ($T_{\mathrm{r}} \leq T_{\mathrm{d}}$), the reflecting vector changes randomly with a period of no more than T_{r}, and active channel aging then occurs.

IV. Simulation Results and Discussion

Consider a MU-MISO system with four single-antenna LUs, where the legitimate AP is equipped with a 12-element ULA [15] and an I-IRS contains 1,024 reflecting elements ($N_{\mathrm{I,y}} = N_{\mathrm{I,z}} = 32$). Moreover, the AP is located at (0m, 0m, 0m) and the four LUs are randomly distributed in a circle centered at (200m, 0m, 0m) with a radius of 10m, while the I-IRS is deployed at (5m, 5m, 2m).

Most of the existing performance-enhancing IRS-aided systems make the assumption that $\mathbf{H}_{\mathrm{d}}$ has significant large-scale

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. 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/TVT.2023.3261303

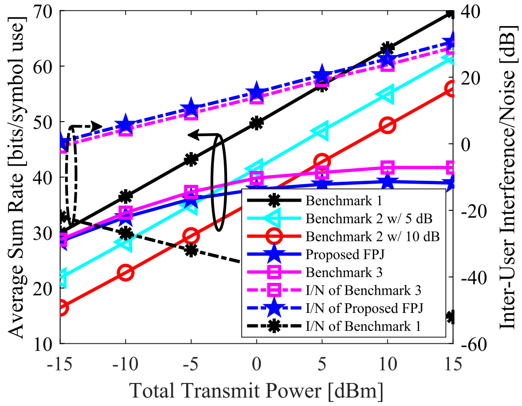

Fig. 3. Average sum rates (left, solid lines) and I/N (right, dash-dot lines) of different schemes vs total transmit power.

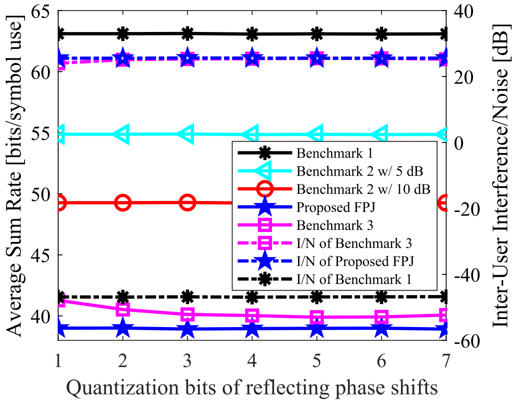

Fig. 4. Influence of quantization reflecting phase shift bits.

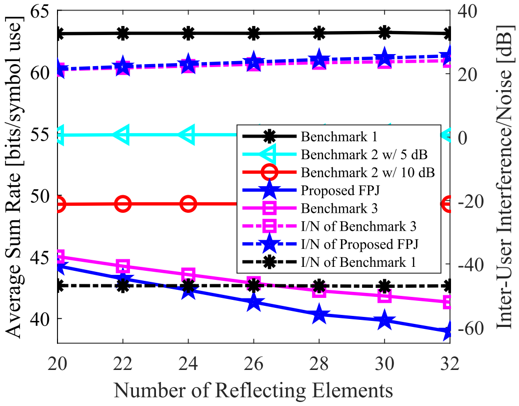

Fig. 5. Influence of the number of reflecting elements.

path loss or is blocked, while the large-scale path losses of $\mathbf{G}$ and $\mathbf{H}_{\mathrm{I}}$ are much smaller [14], [16]. However, this assumption is too idealistic for jamming attacks. According to the 3GPP propagation environment [17], the large-scale path losses $\mathscr{L}_k$, $\mathscr{L}_{\mathrm{G}}$ and $\mathscr{L}_{\mathrm{I,k}}$ are set as $\mathscr{L}_k = 32.6 + 22\log_{10}(d_k)$, $\mathscr{L}_{\mathrm{G}} = 35.6 + 20\log_{10}(d_{\mathrm{G}})$ and $\mathscr{L}_{\mathrm{I},k} = 35.6 + 22\log_{10}(d_{\mathrm{I},k})$, where d_k is the distance between the AP and LU_k, d_{G} is the distance between the AP and and the I-IRS, and $d_{\mathrm{I},k}$ is the distance between the I-IRS and LU_k $(1 \leq k \leq 4)$. Moreover, $\sigma^2 = -170 + 10\log_{10}(BW)$ dBm, where BW denotes the transmission bandwidth and $BW = 180$ kHz [16]. We compare the proposed I-IRS-based FPJ with three benchmarks.

1) Benchmark 1: The average sum rates without IJ (w/o IJ) are computed based on the multi-user direct channel, where the received SINR γ_k at LU_k is $\gamma_k = \frac{\left|\boldsymbol{h}_{\mathrm{d},k}^H \boldsymbol{w}_{\mathrm{d},k}\right|^2}{\sum_{u \neq k} \left|\boldsymbol{h}_{\mathrm{d},k}^H \boldsymbol{w}_{\mathrm{d},u}\right|^2 + \sigma^2}$.

2) Benchmark 2: The average sum rates under the active jammer (w/ AJ/N) with different ratios of the jamming power to the noise power (AJ/N) at each LU. More specifically, the received SINR γ_k at LU_k under active jamming is expressed as $\gamma_k = \frac{\left|\boldsymbol{h}_{\mathrm{d},k}^H \boldsymbol{w}_{\mathrm{d},k}\right|^2}{\sum_{u \neq k} \left|\boldsymbol{h}_{\mathrm{d},k}^H \boldsymbol{w}_{\mathrm{d},u}\right|^2 + P_J + \sigma^2}$, where AJ/N = P_J/σ^2=5 dB and 10 dB, respectively.

2) Benchmark 3: The CSI-based PJ in Section III-A, i.e., the extension of [11].

Fig. 3 illustrates the average sum rates via the proposed FPJ and the above three benchmarks, where $\mathscr{I}$ generated from them is also given. By destroying the orthogonality of the multi-user active beamforming vectors and the co-user channels, the inter-user interference becomes significant due to active channel aging. The reflecting vector in the proposed FPJ affects both the multi-user combined channel and the multi-user active beamforming, while the reflecting vector in the CSI-based PJ just impacts the multi-user combined channel. As shown in Fig. 3, $\mathscr{I}$ from the proposed FPJ is more serious than that from the CSI-aided PJ (Benchmark 3). Therefore, the proposed FPJ can jam LUs without the transmit power and the CSI, even more effectively than the CSI-aided PJ.

From Fig. 3, one can see that the sum rate of Proposed FPJ is smaller than that of Benchmark 2 with 5 dB AJ/N when the total transmit power is greater than 0 dBm. In contrast to the active jamming, the jamming launched by the proposed FPJ cannot be mitigated by increasing the total transmit power.

To show the influence of the number of quantization reflecting phase shift bits, the relationships between the average sum rates and quantization bits are illustrated in Fig. 4. One can see that the proposed FPJ is robust to the quantization bits since the reflecting vector is randomly generated. Based on the proposed FPJ, the one-bit I-IRS is enough to launch effective jamming attacks on LUs. The greater the number of quantization bits, the smaller the difference $\|\boldsymbol{\varphi} - \bar{\boldsymbol{\varphi}}\|^2$ in (11) is. Although the sum rate achieved by Benchmark 3 decreases with the number of quantization bits, the high-bit I-IRS requires high physical implementation costs.

Moreover, Fig. 5 shows the relationship between the sum rates and the number of reflecting elements as well as that between I/N and the number of reflecting elements. The difference between the sum rates achieved by Benchmark 3 and Proposed FPJ increases with the number of reflecting elements. On the one hand, active channel aging becomes more significant with the number of reflecting elements, and thus the corresponding jamming attacks are more effective. On the other hand, the minimum value of $\|\boldsymbol{\varphi} - \bar{\boldsymbol{\varphi}}\|^2$ in (11) gets bigger with the number of reflecting elements. In practice, an IRS generally consists of massive reflecting elements, which is beneficial to the proposed I-IRS-based FPJ.

V. Conclusions

In this paper, we investigated the impact of I-IRSs on MU-MISO systems, where an I-IRS-based FPJ was proposed. By exploiting an I-IRS to cause active channel aging, we have demonstrated that the proposed FPJ can jam without relying on the transmit power and the CSI. Due to the impacts on both the multi-user combined channel and the multi-user active beamforming, the jamming launched by the proposed FPJ is even more effective than that launched by the CSI-aided PJ. Meanwhile, the proposed FPJ is robust to the number of quantization reflecting phase shift bits. Different from the active jamming attacks, the jamming attacks launched by the proposed FPJ cannot be mitigated by increasing the total transmit power at the legitimate AP. When the legitimate AP has large transmit power, the proposed FPJ can jam LUs more effectively. Moreover, the proposed FPJ can be perfectly hidden in wireless environments because it does not require additional transmit power and instantaneous CSI.

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. Zhang and B. Di, "Intelligent omni-surfaces: Simultaneous refraction and reflection for full-dimensional wireless communications," *IEEE Commun. Surv. Tut.*, vol. 24, no. 4, pp. 1997–2028, 4th Quarter 2022.

[3] 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.

[4] W. Tan, C. Zhang, J. Peng, L. Dai, S. Fu, and K. Qiu, "Secure transmission via IUI engineering for IRS-assisted NOMA systems," *IEEE Wireless Commun. Lett.*, vol. 11, no. 7, pp. 1369–1373, Apr. 2022.

[5] S. Tomasin, H. Zhang, A. Chorti and H. V. Poor, "Challenge-Response Physical Layer Authentication over Partially Controllable Channels," *IEEE Wireless Mag.*, vol. 60, no. 12, pp. 138–144, Dec. 2022.

[6] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, Jun. 2020.

[7] H. Yang, Z. Xiong, J. Zhao, D. Niyato, Q. Wu, H. V. Poor, and M. Tornatore, "Intelligent reflecting surface assisted anti-jamming communications: A fast reinforcement learning approach," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 1963–1974, Mar. 2021.

[8] 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.

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

[10] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 487–490, May 2012.

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

[16] 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. 3064–30769, May 2020.

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