# Integrated Sensing and Communication Under DISCO Physical-Layer Jamming Attacks

Huan Huang, *Member, IEEE*, Hongliang Zhang, *Member, IEEE*, Weidong Mei, *Member, IEEE*, Jun Li, Yi Cai, *Senior Member, IEEE*, A. Lee Swindlehurst, *Fellow, IEEE*, and Zhu Han *Fellow, IEEE*

***Abstract*—Integrated sensing and communication (ISAC) systems traditionally presuppose that sensing and communication (S&C) channels remain approximately constant during their coherence time. However, a "DISCO" reconfigurable intelligent surface (DRIS), i.e., an illegitimate RIS with random, time-varying reflection properties that acts like a "disco ball," introduces a paradigm shift that enables active channel aging more rapidly during the channel coherence time. In this letter, we investigate the impact of DISCO jamming attacks launched by a DRIS-based fully-passive jammer (FPJ) on an ISAC system. Specifically, an ISAC problem formulation and a corresponding waveform optimization are presented in which the ISAC waveform design considers the trade-off between the S&C performance and is formulated as a Pareto optimization problem. Moreover, a theoretical analysis is conducted to quantify the impact of DISCO jamming attacks. Numerical results are presented to evaluate the S&C performance under DISCO jamming attacks and to validate the derived theoretical analysis.**

***Index Terms*—Channel aging, integrated sensing and communication, physical-layer security, Pareto optimization, reconfigurable intelligent surface.**

## I. Introduction

INTEGRATED sensing and communication (ISAC) is a promising candidate technology for future sixth generation (6G) wireless communication systems and has attracted increasing attention. In particular, ISAC implements joint target sensing and data communication using the same RF hardware and computing platform [1], [2], offering an exciting opportunity to implement sensing using traditional wireless communication infrastructure [3]. The added sensing functionality enabled by the collection of environmental data makes ISAC a fundamental component of future smart environments. In particular, ISAC is applicable to vehicle-to-everything communications, smart homes, and smart manufacturing. There has been considerable research on ISAC-related problems, including ISAC waveform design [4], [5]. Considering the difficulties of optimization problems involving the mean squared error (MSE) or the Cramér-Rao lower bound (CRLB), most existing works use simpler alternative optimization criteria such as the transmit beampattern [4], [5], [6].

Recently, reconfigurable intelligent surfaces (RISs) are also anticipated to play a critical role in future 6G wireless communications. These surfaces are embedded with many elements whose reflection coefficients can be tuned by simple programmable PIN or varactor diodes [7], [8], [9], [10]. By properly tuning these reflection coefficients, the electromagnetic environment can be reshaped to enhance signal transmission to improve both sensing and communication (S&C) [6], [11], [12]. However, the S&C performance enhancement relies on the *basic premise* that the S&C channels are approximately constant during the channel coherence time. This basic premise is normally valid, but can be negated when so-called DISCO RISs (DRISs) are deployed [13].

The DRIS concept was first introduced with DRIS-based fully-passive jammer (FPJ) [14], where a DRIS with time-varying reflection properties acts like a "disco ball." The DRIS introduces active channel aging (ACA), and thus the wireless channels will vary more rapidly than the channel coherence time [14], [15], [16]. Such ACA can be used to jam communication users or degrade the accuracy of target sensing without the use of either jamming power or channel state information (CSI). This type of ACA interference (ACAI) is referred to as a DISCO jamming attack, and renders the above basic premise for ISAC systems invalid.

In this letter, we aim to characterize the impact of DISCO jamming attacks on ISAC systems. To the best of our knowledge, this is the first time that the validity of the basic premise has been investigated for ISAC systems. The main contributions are summarized as follows:

- A DRIS-based FPJ is introduced into an ISAC system to launch DISCO jamming attacks. Furthermore, a practical RIS model is considered for the DRIS-based FPJ, where the DRIS phase shifts of the reflective elements are discrete and the DRIS amplitudes are a function of their corresponding phase shifts.
- In the ISAC waveform design, the desired sensing waveform and the signal-to-interference-plus-noise

Manuscript received 4 July 2024; revised 3 August 2024; accepted 3 August 2024. Date of publication 6 August 2024; date of current version 8 November 2024. This work was supported in part by the National Natural Science Foundation of China under Grant 62250710164, Grant 62275185, and Grant 62371011; in part by the U.S. National Science Foundation under Grant CNS–2107216, Grant CNS–2128368, Grant CNS–2107182, Grant CMMI–2222810, Grant ECCS-2302469, and Grant ECCS–2030029; in part by the U.S. Department of Transportation; in part by Toyota; and in part by Amazon. The associate editor coordinating the review of this article and approving it for publication was T. Le. *(Corresponding authors: Huan Huang; Yi Cai.)*

Huan Huang, Jun Li, and Yi Cai are with the School of Electronic and Information Engineering, Soochow University, Suzhou 215006, Jiangsu, China (e-mail: hhuang1799@gmail.com; ljun@suda.edu.cn; yicai@ieee.org).

Hongliang Zhang is with the School of Electronics, Peking University, Beijing 100871, China (e-mail: hongliang.zhang92@gmail.com).

Weidong Mei is with the National Key Laboratory of Wireless Communications, University of Electronic Science and Technology of China, Chengdu 610054, China (e-mail: wmei@uestc.edu.cn).

A. Lee Swindlehurst is with the Center for Pervasive Communications and Computing, University of California at Irvine, Irvine, CA 92697 USA (e-mail: swindle@uci.edu).

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

Digital Object Identifier 10.1109/LWC.2024.3439398

2162-2345 © 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:35:18 UTC from IEEE Xplore. Restrictions apply.

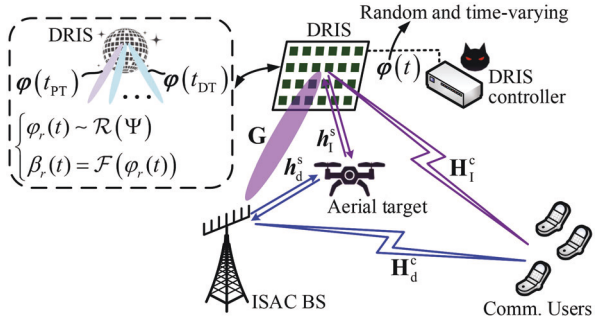


Fig. 1. The downlink of an ISAC system jammed by a DRIS-based FPJ, where the time-varying DRIS reflection coefficients are randomly generated by the DRIS controller.

ratio (SINR) are used as S&C performance metrics. Consequently, the ISAC waveform design problem under DISCO jamming attacks is formulated as a Pareto optimization problem. We present a corresponding ISAC waveform design by considering the trade-off between the S&C performance metrics.

- We show that the DISCO jamming attacks lead to biased estimation of the target parameters and impair the communication sum rate. Moreover, a theoretical analysis is performed to quantify the impact of the DISCO jamming attacks.

*Notation:* We employ bold capital letters for a matrix, e.g., $\mathbf{X}$, lowercase bold letters for a vector, e.g., $\boldsymbol{x}_l$, and italic letters for a scalar, e.g., $k$. The superscripts $(\cdot)^T$ and $(\cdot)^*$ represent the transpose and the Hermitian transpose, respectively, and the symbols $\|\cdot\|_{\mathrm{F}}$ and $|\cdot|$ represent the Frobenius norm and the absolute value, respectively.

## II. System Description

In this section, we first illustrate DISCO jamming attacks launched by a DRIS-based FPJ in Section II-A. Then, the model of the ISAC system under DISCO jamming attacks is given in Section II-B.

### A. DRIS-Based Active Channel Aging

Fig. 1 shows an ISAC system under DISCO jamming attacks launched by a DRIS-based FPJ [14]. The DRIS with $N_{\mathrm{D}} = N_{\mathrm{D},h} \times N_{\mathrm{D},v}$ reflective elements is implemented using PIN diodes, whose ON/OFF behavior only allows for discrete phase shifts. Therefore, the time-varying DRIS phase shifts $\varphi_r(t)$ $(r = 1, \ldots, N_{\mathrm{D}})$ are randomly selected from a discrete set $\Psi$ with $b$-bit quantized values $\{\phi_1, \ldots, \phi_{2^b}\}$ and follow a stochastic distribution denoted as $\varphi_r(t) \sim \mathcal{R}(\Psi)$. The amplitude of the reflection coefficient $\beta_r$ is a function of $\varphi_r(t)$ and represented by $\beta_r(t) = \mathcal{F}(\varphi_r(t))$, where $\mathcal{F}(\Psi) = \Xi = \{\mu_1, \ldots, \mu_{2^b}\}$. As a result, the time-varying DRIS reflecting vector $\boldsymbol{\varphi}(t)$ is given by $\boldsymbol{\varphi}(t) = [\beta_1(t)e^{j\varphi_1(t)}, \ldots, \beta_{N_{\mathrm{D}}}(t)e^{j\varphi_{N_{\mathrm{D}}}(t)}]$.

In traditional wireless systems, the wireless channels are assumed to be fixed during the channel coherence time. Consequently, the CSI estimated during the pilot transmission (PT) phase can be used to design the waveform used in the remaining data transmission (DT) phase of each channel coherence time. Before S&C data transmission, the ISAC base station (BS) first learns the CSI during the PT phase via existing methods such as the least squares (LS) algorithm. Mathematically, the CSI[1] estimated during the PT phase is written as

$$\mathbf{H}_{\mathrm{PT}}^{\mathrm{c}} = \mathbf{H}_{\mathrm{d}}^{\mathrm{c}} + \mathbf{G}\mathrm{diag}(\boldsymbol{\varphi}(t_{\mathrm{PT}}))\mathbf{H}_{\mathrm{I}}^{\mathrm{c}}, \tag{1}$$

where $\mathbf{H}_{\mathrm{d}}^{\mathrm{c}}$ and $\mathbf{H}_{\mathrm{D}}^{\mathrm{c}} = \mathbf{G}\mathrm{diag}(\boldsymbol{\varphi}(t_{\mathrm{PT}}))\mathbf{H}_{\mathrm{I}}^{\mathrm{c}}$ represent the direct channel and the time-varying DRIS-jammed channel between the ISAC BS and the communication users, respectively.

Due to the random and time-varying DRIS reflecting coefficients, ACA is introduced within the channel coherence time. The time between changes in the DRIS reflection coefficients is typically assumed to be about the same as the length of the PT phase [13], [16]. As a result, the DRIS rapidly ages the wireless channels, and effectively produces a channel with a coherence interval approximately equal to the PT phase. Mathematically, the ACA channel during the DT phase is

$$\mathbf{H}_{\mathrm{ACA}}^{\mathrm{c}} = \mathbf{H}_{\mathrm{DT}}^{\mathrm{c}} - \mathbf{H}_{\mathrm{PT}}^{\mathrm{c}} = \mathbf{G}\mathrm{diag}(\boldsymbol{\varphi}(t_{\mathrm{DT}}) - \boldsymbol{\varphi}(t_{\mathrm{PT}}))\mathbf{H}_{\mathrm{I}}^{\mathrm{c}}, \tag{2}$$

where $\mathbf{G}$ and $\mathbf{H}_{\mathrm{I}}^{\mathrm{c}}$ denote the channel between the ISAC BS and the DRIS and the channel between the DRIS and all communication users.

### B. ISAC Under DISCO Jamming

*Communication Model:* In Fig. 1, the ISAC BS is equipped with $N$ transmit antennas to communicate with $K_{\mathrm{c}}$ single-antenna users. During the DT phase, the ISAC BS transmits $L$ symbols to these users, and thus the length of the data frame is $L$. The received signals at the communication users are

$$\mathbf{Y}_{\mathrm{c}} = \mathbf{S} + \underbrace{(\mathbf{H}_{\mathrm{PT}}^{\mathrm{c}}\mathbf{X} - \mathbf{S})}_{\mathrm{MUI}} + \underbrace{\mathbf{H}_{\mathrm{ACA}}^{\mathrm{c}}\mathbf{X}}_{\mathrm{ACAI}} + \mathbf{N}_{\mathrm{c}}, \tag{3}$$

where $\mathbf{S}$ denotes the $K \times L$ desired constellation symbol matrix, $\mathbf{X} = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_L]$ represents the $N \times L$ transmitted signal matrix used as the ISAC waveform for both the communication and sensing functions [4], [5], and $\mathbf{N}_{\mathrm{c}}$ is a $K \times L$ Gaussian noise matrix composed of independent and identically distributed (i.i.d.) elements with zero mean and variance $\sigma_{\mathrm{c}}^2$, i.e., $n_{k,l}^{\mathrm{c}} \sim \mathcal{CN}(0, \sigma_{\mathrm{c}}^2)$. Based on (3), we can see that the DRIS-based FPJ imposes ACAI on the signals in addition to multi-user interference (MUI) [4]. Referring to [4], [15], the SINR at the $k$-th user is given by

$$\gamma_k = \frac{\mathbb{E}\left[|s_{k,l}|^2\right]}{\mathbb{E}\left[\left|\left(\left(\boldsymbol{h}_{\mathrm{PT},k}^{\mathrm{c}}\right)^* \boldsymbol{x}_l - s_{k,l}\right) + \left(\boldsymbol{h}_{\mathrm{ACA},k}^{\mathrm{c}}\right)^* \boldsymbol{x}_l\right|^2\right] + \sigma_{\mathrm{c}}^2}. \tag{4}$$

Consequently, the sum rate can be computed based on (4), i.e., $R_{\mathrm{sum}} = \sum_{k=1}^{K} R_k = \sum_{k=1}^{K} \log_2(1 + \gamma_k)$.

*Sensing Model:* To quantify the sensing performance, we use the quality of the estimated target angle $\theta$ [18]. As shown in Fig. 1, we assume that the target is airborne, such as an unmanned aerial vehicle (UAV). The $L$ symbols are reflected by the target and then received at the ISAC BS, resulting in [11]

$$\mathbf{Y}_{\mathrm{s}} = \chi(\boldsymbol{h}_{\mathrm{d}}^{\mathrm{s}} + \boldsymbol{h}_{\mathrm{D}}^{\mathrm{s}})(\boldsymbol{h}_{\mathrm{d}}^{\mathrm{s}} + \boldsymbol{h}_{\mathrm{D}}^{\mathrm{s}})^*\mathbf{X} + \mathbf{N}_{\mathrm{s}}, \tag{5}$$

[1]We assume that perfect CSI is available as imperfect CSI is not a primary concern in the jamming scenario, and its impact has been thoroughly studied [17].

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:35:18 UTC from IEEE Xplore. Restrictions apply.

where $0 \leq \chi \leq 1$ represents the reflection cross-section of the target, $\boldsymbol{h}_{\mathrm{d}}^{\mathrm{s}} = \sqrt{\mathscr{L}_{\mathrm{d}}^{\mathrm{s}}}\boldsymbol{\alpha}(N,\theta)$ denotes the direct sensing path, $\boldsymbol{h}_{\mathrm{D}}^{\mathrm{s}} = \sqrt{\mathscr{L}_{\mathrm{cas}}^{\mathrm{s}}}\mathbf{G}\mathrm{diag}(\boldsymbol{\varphi}(t))\boldsymbol{\alpha}(N_h,N_v,\phi_h,\phi_v)$ denotes the time-varying DRIS-jammed sensing path, $\mathscr{L}_{\mathrm{d}}^{\mathrm{s}}$ and $\mathscr{L}_{\mathrm{cas}}^{\mathrm{s}}$ are the large-scale channel fading coefficients of $\boldsymbol{h}_{\mathrm{d}}^{\mathrm{s}}$ and $\boldsymbol{h}_{\mathrm{D}}^{\mathrm{s}}$, and $\mathbf{N}_{\mathrm{s}}$ is an $N \times L$ noise matrix whose i.i.d. elements have zero mean and variance $\sigma_{\mathrm{s}}^2$. Furthermore, the steering vectors of the ISAC BS antenna array and the DRIS are respectively defined as

$$\boldsymbol{\alpha}(N,\theta) = \left[1, e^{j2\pi\Delta\sin\theta}, \ldots, e^{j2\pi(N-1)\Delta\sin\theta}\right]^T \tag{6}$$

and

$$\boldsymbol{\alpha}(N_h,N_v,\phi_h,\phi_v) = \boldsymbol{\alpha}(N_h,\phi_h) \otimes \boldsymbol{\alpha}(N_v,\phi_v), \tag{7}$$

where $\Delta$ denotes the array spacing normalized by the wavelength, and $\otimes$ represents the Kronecker product.

To estimate $\theta$, we exploit the MUSIC algorithm [19]. The sample covariance matrix computed based on $L$ snapshots in (5) is

$$\widetilde{\mathbf{R}}_{\mathbf{X}} = \frac{1}{L}\mathbf{Y}_{\mathrm{s}}\mathbf{Y}_{\mathrm{s}}^*, \tag{8}$$

and the MUSIC spectral function $V(\vartheta)$ is then computed from $\widetilde{\mathbf{R}}_{\mathbf{X}}$. However, based on (5), the time-varying DRIS-jammed sensing path $\boldsymbol{h}_{\mathrm{D}}^{\mathrm{s}}$ has been introduced into $\widetilde{\mathbf{R}}_{\mathbf{X}}$, which perturbs the location of the spectral peak in $V(\vartheta)$ and leads to a biased DoA estimation.

## III. ISAC Waveform Design Under DISCO Jamming

In this section, we first formulate the ISAC waveform design problem under DISCO jamming attacks and give a waveform optimization design for the ISAC system under these attacks in Section III-A. In Section III-B, a theoretical analysis is derived to quantify the impact of the DISCO jamming attacks.

### A. Problem Formulation And ISAC Waveform Design

According to (3) and (4), the optimum ISAC waveform should be designed to minimize the power of the multi-user interference (MUI) and ACAI. However, due to the time-varying and random DRIS reflecting vector $\boldsymbol{\varphi}(t)$, the ISAC BS can not obtain $\mathbf{H}_{\mathrm{ACA}}^{\mathrm{c}}$. Therefore, we consider designing the ISAC waveform by minimizing the MUI. Mathematically, the ISAC waveform design problem is formulated as

$$(\mathrm{P1}):\ \min_{\mathbf{X}} \|\mathbf{H}_{\mathrm{PT}}^{\mathrm{c}}\mathbf{X} - \mathbf{S}\|_{\mathrm{F}}^2 \tag{9}$$

$$\text{s.t. } \mathbf{C}_{\mathbf{X}} = \frac{1}{L}\mathbf{X}\mathbf{X}^* = \frac{P_0}{N}\mathbf{I}_N, \tag{10}$$

where $P_0$ is the total transmit power at the ISAC BS and $\mathbf{I}_N$ is an $N \times N$ identity matrix. We assume $N \leq L$ to ensure that $\mathbf{C}_{\mathbf{X}}$ is positive-definite.

The strict equality constraint (10) ensures that the ISAC waveform has the same properties as the best sensing waveform, although the communication performance may be degraded as a result [4]. Therefore, there should be a trade-off between the sensing capability and the communication rate in (P1), so we introduce a trade-off factor $\kappa$ ($0 \leq \kappa \leq 1$) into (P1), Denoting the solution to (P1) as $\mathbf{X}_0$, the following Pareto optimization problem can be obtained:

$$(\mathrm{P2}):\ \min_{\mathbf{X}} \kappa\|\mathbf{H}_{\mathrm{PT}}^{\mathrm{c}}\mathbf{X} - \mathbf{S}\|_{\mathrm{F}}^2 + (1-\kappa)\|\mathbf{X} - \mathbf{X}_0\|_{\mathrm{F}}^2 \tag{11}$$

$$\text{s.t. } \|\mathbf{X}\|_{\mathrm{F}}^2 = LP_0. \tag{12}$$

For different $\kappa$, the solution to (P2) makes different trade-offs between S&C performance. More specifically, the smaller the $\kappa$, the better the sensing performance, but the worse the communication performance.

To solve (P2), we first compute $\mathbf{X}_0$ from (P1). Since (P1) is a classical orthogonal Procrustes problem, a simple closed-form solution to (P1) can be obtained based on the singular value decomposition (SVD), i.e., $\mathbf{X}_0 = \sqrt{\frac{P_0 L}{N}}\mathbf{U}\mathbf{I}_{N\times L}\mathbf{V}^*$, where $\mathbf{U}$ and $\mathbf{V}$ are the left and right singular value matrices of $\mathbf{H}_{\mathrm{PT}}^{\mathrm{c}}\mathbf{S}$ and satisfy $\mathbf{U}^{\circ}\mathbf{V}^* = \mathbf{H}_{\mathrm{PT}}^{\mathrm{c}}\mathbf{S}$.

Consequently, we transform Problem (P2) into the following form using the approach of [4],

$$(\mathrm{P2-E1}):\ \min_{\mathbf{X}} \|\mathbf{A}\mathbf{X} - \mathbf{B}\|_{\mathrm{F}}^2$$

$$\text{s.t. } (12), \tag{13}$$

where $\mathbf{A} = [\sqrt{\kappa}(\mathbf{H}_{\mathrm{PT}}^{\mathrm{c}})^T, \sqrt{1-\kappa}\mathbf{I}_N t]^T$ and $\mathbf{B} = [\sqrt{\kappa}\mathbf{S}^T, \sqrt{1-\kappa}\mathbf{X}_0^T]^T$. It is worth noting that (P2−E1) can be transformed into a semidefinite programming (SDP) problem using semidefinite relaxation (SDR), and it has only one quadratic constraint, i.e., (12). Therefore, the rank-1 SDR solution is its globally optimal solution.

### B. Impact of DISCO Jamming Attacks

For a given ISAC waveform, the sum rate is affected not only by the MUI due to sensing functionality considerations, but also by the ACAI. The impact of MUI has been investigated in the existing literature, such as [4], [5] so we focus on the impact of the ACAI imposed by the DRIS-based FPJ. For ease of presentation, we rewrite the interference term in (4) as

$$\begin{aligned}\mathscr{I} = &\left|(\boldsymbol{h}_{\mathrm{PT},k}^{\mathrm{c}})^*\boldsymbol{x}_l - s_{k,l}\right|^2 + \left((\boldsymbol{h}_{\mathrm{PT},k}^{\mathrm{c}})^*\boldsymbol{x}_l - s_{k,l}\right)\boldsymbol{x}_l^*\boldsymbol{h}_{\mathrm{ACA},k}^{\mathrm{c}} \\ &+ \left((\boldsymbol{h}_{\mathrm{PT},k}^{\mathrm{c}})^*\boldsymbol{x}_l - s_{k,l}\right)^*\left(\boldsymbol{h}_{\mathrm{ACA},k}^{\mathrm{c}}\right)^*\boldsymbol{x}_l \\ &+ \left|(\boldsymbol{h}_{\mathrm{ACA},k}^{\mathrm{c}})^*\boldsymbol{x}_l\right|^2.\end{aligned} \tag{14}$$

The DRIS must be equipped with a large number of reflective elements to overcome the multiplicative propagation loss in the DRIS-jammed channels. The elements of $\mathbf{H}_{\mathrm{ACA}}^{\mathrm{c}}$ have the statistical characteristics outlined in Proposition 1.

*Proposition 1:* The elements of $\mathbf{H}_{\mathrm{ACA}}^{\mathrm{c}}$ converge in distribution to $\mathcal{CN}(0, \mathscr{L}_{\mathrm{cas},k}N_{\mathrm{D}}\overline{\mu})$ as $N_{\mathrm{D}} \to \infty$, i.e.,

$$[\mathbf{H}_{\mathrm{ACA}}^{\mathrm{c}}]_{n,k} \xrightarrow{\mathrm{d}} \mathcal{CN}\left(0, \mathscr{L}_{\mathrm{cas},k}^{\mathrm{c}}N_{\mathrm{D}}\overline{\mu}\right), \forall n,k, \tag{15}$$

where $\mathscr{L}_{\mathrm{cas},k}^{\mathrm{c}}$ is the large-scale channel fading coefficient of the DRIS-jammed channel between the ISAC BS and the $k$-th communication user, $\overline{\mu} = \sum_{i1=1}^{2^b}\sum_{i2=1}^{2^b} p_{i1}p_{i2}(\mu_{i1}^2 + \mu_{i2}^2 - 2\mu_{i1}\mu_{i2}\cos(\phi_{i1} - \phi_{i2}))$, $\mu_{i1}, \mu_{i2} \in \Xi$, $\phi_{i1}, \phi_{i2} \in \Psi$, and $p_{i1}, p_{i2}$ are the probabilities of the random phases $\phi_{i1}, \phi_{i2}$.

*Proof:* See [16]. ■

Based on Proposition 1, the impact of the ACAI is mathematically quantified by Theorem 1 below.

*Theorem 1:* Under DISCO jamming attacks launched by the DRIS-based FPJ, a lower bound for the SINR received

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:35:18 UTC from IEEE Xplore. Restrictions apply.

at the $k$-th communication user $\gamma_k$ for any ISAC waveform computed from (P2-E1) converges in distribution to

$$\gamma_k \geq \frac{\mathbb{E}\left[\left|s_{k,l}\right|^2\right]}{\mathbb{E}\left[\left|\left(\left(\boldsymbol{h}^{\mathrm{c}}_{\mathrm{PT},k}\right)^* \boldsymbol{x}_l - s_{k,l}\right)\right|^2\right] + \mathbb{E}\left[\left\|\boldsymbol{h}^{\mathrm{c}}_{\mathrm{ACA},k}\right\|^2\right]\mathbb{E}\left[\|\boldsymbol{x}_l\|^2\right] + \sigma^2},$$
$$\xrightarrow{\mathrm{d}} \frac{\mathbb{E}\left[\left|s_{k,l}\right|^2\right]}{\mathbb{E}\left[\left|\left(\left(\boldsymbol{h}^{\mathrm{c}}_{\mathrm{PT},k}\right)^* \boldsymbol{x}_l - s_{k,l}\right)\right|^2\right] + P_0 \mathscr{L}^{\mathrm{c}}_{\mathrm{cas},k} N_{\mathrm{D}} \overline{\mu} + \sigma^2}. \quad (16)$$

*Proof:* Since the ISAC waveform $\mathbf{X}$ computed from (P2−E1) is optimized only based on $\mathbf{H}^{\mathrm{c}}_{\mathrm{PT}}$, we can assume that $\mathbf{X}$ is independent of the ACA communication channel $\mathbf{H}^{\mathrm{c}}_{\mathrm{ACA}}(t)$. Consequently, the expectation of $\mathscr{I}$ in (14) is

$$\mathbb{E}[\mathscr{I}] = \mathbb{E}\left[\left|\left(\boldsymbol{h}^{\mathrm{c}}_{\mathrm{PT},k}\right)^* \boldsymbol{x}_l - s_{k,l}\right|^2\right] + \mathbb{E}\left[\left|\left(\boldsymbol{h}^{\mathrm{c}}_{\mathrm{ACA},k}\right)^* \boldsymbol{x}_l\right|^2\right]. \quad (17)$$

According to the Cauchy–Schwarz inequality and Proposition 1, we have

$$\mathbb{E}\left[\left|\left(\boldsymbol{h}^{\mathrm{c}}_{\mathrm{ACA},k}\right)^* \boldsymbol{x}_l\right|^2\right] \leq \mathbb{E}\left[\left\|\boldsymbol{h}^{\mathrm{c}}_{\mathrm{ACA},k}\right\|^2\right]\mathbb{E}\left[\|\boldsymbol{x}_l\|^2\right] \xrightarrow{\mathrm{d}} P_0 \mathscr{L}^{\mathrm{c}}_{\mathrm{cas},k} N_{\mathrm{D}} \overline{\mu}. \quad (18)$$

Substituting (17) and (18) into (4), (16) is derived. ∎

The numerical results given in the next section will indicate that the waveform design based on (P2−E1) achieves performance that is very close to the derived lower bound in Theorem 1. This indicates that without any knowledge of the DRIS-jammed channels, there is no "better" waveform design that could provide a significant improvement over the lower bound. Fortunately, Proposition 1 gives the statistical characteristics of the ACA channel $\mathbf{H}_{\mathrm{ACA}}$, which may provide a potential approach to designing an anti-jamming scheme [16].

## IV. Simulation Results and Discussion

We consider an ISAC system equipped with a 16-element antenna array located at (0m, 0m, 3m) and jammed by the DRIS-based FPJ. The ISAC BS communicates with 8 single-antenna users that are randomly distributed in the circular region $S$ centered at (0m, 180m, 0m) with a radius of 20m. The DRIS with 1024 $(N_{\mathrm{D},h} = 32, N_{\mathrm{D},v} = 32)$ reflective elements is deployed at (2m, 0m, 2m) to launch DISCO physical-layer jamming attacks. We assume that the DRIS has one-bit quantized phase shifts and gain values taken from $\Psi = \{\frac{\pi}{9}, \frac{7\pi}{6}\}$ and $\Xi = \mathcal{F}(\Theta) = \{0.8, 1\}$ [8], and the two phase shifts are chosen with equal probability. Consequently, $\overline{\mu}$ in Theorem 1 is 1.6078. The length of the data frame is $L = 18$ and the trade-off factor in (P2) is $\kappa = 0.2$.

Based on the settings above, the wireless channel $\mathbf{G}$ is constructed using a near field channel model, while the wireless channels $\mathbf{H}^{\mathrm{c}}_{\mathrm{I}}$ and $\mathbf{H}^{\mathrm{c}}_{\mathrm{d}}$ are both based on far field channel models [14], [15], [16], [18]. The large-scale line-of-sight (LoS) and non-line-of-sight (NLoS) channel fading coefficients are defined in Table I based on 3GPP propagation models [20], and the variance of the noise is $\sigma^2_{\mathrm{c}} = -170 + 10\log_{10}(BW)$ dBm with a transmission bandwidth of 180 KHz.

Fig. 2 illustrates the results obtained by the following approaches: 1) the sum rate obtained without MUI or ACAI (Theoretical ISAC Up-Bound); 2) the sum rate achieved by a traditional ISAC system [4] (T-ISAC W/ $\kappa = 0.2$ in [4]); 3) the sum rate achieved by an ISAC system under DISCO jamming attacks, i.e., (P2−E1) (Proposed T-ISAC W/ DISCO); 4) the theoretical analysis of Proposed T-ISAC W/ DISCO based on Theorem 1 (Theoretical T-ISAC W/ DISCO); 5) the sum rate achieved by the ISAC system [4] with the strict equality constraint (10) (S-ISAC in [4]); 6) the sum rate achieved by an ISAC system under DISCO jamming attacks with the strict equality constraint (10), i.e., (P1) (Proposed S-ISAC W/ DISCO); 7) the theoretical analysis of Proposed S-ISAC W/ DISCO based on Theorem 1 (Theoretical S-ISAC W/ DISCO).

TABLE I
Wireless Channel Simulation Parameters

| Parameter | Value |
|---|---|
| Large-scale LoS fading | $35.6 + 22\log_{10}(d)$ (dB) |
| Large-scale NLoS fading | $32.6 + 36.7\log_{10}(d)$ |

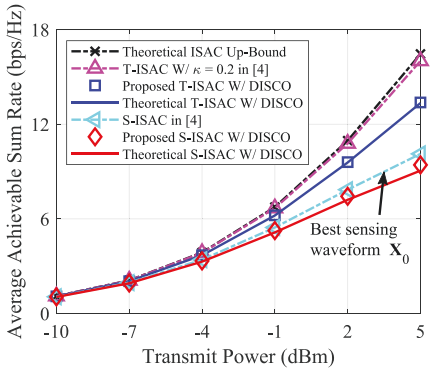


Fig. 2. Average achievable sum rate vs. total power.

We can see from Fig. 2 that by considering the trade-off between the S&C performance, the gap between Theoretical ISAC Up-Bound and T-ISAC W/ $\kappa = 0.2$ in [4] is small. In other words, the sum rate is not seriously affected by the sensing functionality when the ISAC waveform is well designed. However, the performance is severely compromised by DISCO jamming attacks. Without any knowledge of the DRIS-jammed channels, the results of Proposed T-ISAC W/ DISCO and Proposed S-ISAC W/ DISCO are very close to the ideal lower-bounded performance of Theoretical T-ISAC W/ DISCO and Theoretical S-ISAC W/ DISCO. Therefore, the use of the statistical characteristics in Proposition 1 as side knowledge to improve the ISAC waveform design in Section III is a worthwhile pursuit.

Based on Theorem 1, the impact of DISCO jamming attacks on the sum rate can be quantified by $P_0 \mathscr{L}^{\mathrm{c}}_{\mathrm{cas},k} N_{\mathrm{D}} \overline{\mu}$. To evaluate the validity of Theorem 1, the relationship between the sum rate and the number of DRIS reflective elements is given in Fig. 3. We can see that the sum rate decreases with the number of DRIS elements $N_D$, and the achieved sum rates for different $N_{\mathrm{D}}$ are close to the theoretical lower bound.

Fig. 4 shows the impact of the ISAC waveform and the DISCO jamming attacks on the sensing performance. We assume that the echo SNR from the direct sensing path $\boldsymbol{h}^{\mathrm{s}}_{\mathrm{d}}$ is 10 dB. We denote the spectral functions obtained from the best sensing waveform $\mathbf{X}_0$ without DISCO jamming attacks

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:35:18 UTC from IEEE Xplore. Restrictions apply.

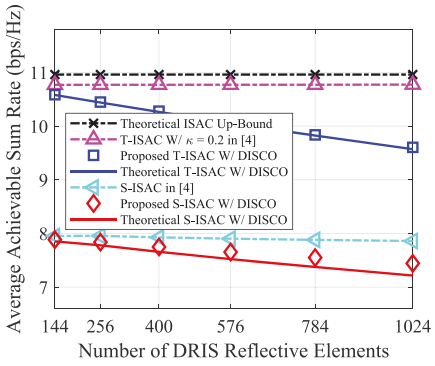


Fig. 3. Average achievable sum rate vs. the number of DRIS reflective elements, where the transmit power is 2 dBm.

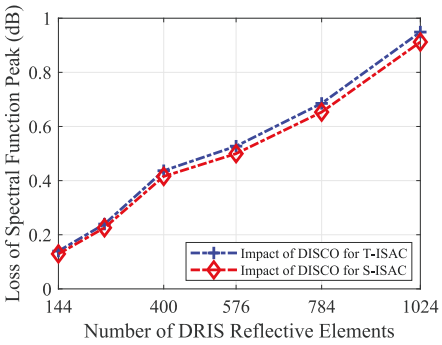


Fig. 4. Difference between the spectral function peaks.

and $\mathbf{X}_0$ under DISCO jamming attacks, the ISAC waveform $\mathbf{X}$ obtained from (P2−E1) without DISCO jamming attacks, and $\mathbf{X}$ under DISCO jamming attack as $V_{\mathrm{S}}(\theta)$, $V_{\text{S-D}}(\theta)$, $V_{\mathrm{T}}(\theta)$, and $V_{\text{T-D}}(\theta)$, respectively. The loss of spectral function peaks [5], [18] between $V_{\mathrm{S}}(\theta)$ and $V_{\text{S-D}}(\theta)$ is shown by the red diamond (Impact of DISCO for S-ISAC), and that between $V_{\mathrm{T}}(\theta)$ and $V_{\text{T-D}}(\theta)$ is plotted by the blue "+" symbol (Impact of DISCO for T-ISAC).

From Fig. 4, we can see that DISCO jamming attacks impair the sensing performance of the MUSIC algorithm. Based on (5), the DRIS-based FPJ introduces extra interference terms $\chi \boldsymbol{h}_{\mathrm{d}}^{\mathrm{s}}(\boldsymbol{h}_{\mathrm{D}}^{\mathrm{s}})^{*}\mathbf{X}$, $\chi \boldsymbol{h}_{\mathrm{D}}^{\mathrm{s}}(\boldsymbol{h}_{\mathrm{d}}^{\mathrm{s}})^{*}\mathbf{X}$, and $\chi \boldsymbol{h}_{\mathrm{D}}^{\mathrm{s}}(\boldsymbol{h}_{\mathrm{D}}^{\mathrm{s}})^{*}\mathbf{X}$ into the received echo signals compared to traditional ISAC systems [4], [5]. Since $\boldsymbol{h}_{\mathrm{D}}^{\mathrm{s}}$ is random and time-varying and cannot be accessed by the legitimate ISAC BS, the sensing performance is then degraded by the DISCO jamming attacks. From Fig. 4, the resulting impact on the sensing performance also increases with the number of DRIS reflective elements.

## V. Conclusion

In this letter, we have investigated the trade-off between the S&C performance in ISAC systems under DISCO jamming attacks. The ISAC waveform design was formulated as a Pareto optimization problem with a trade-off factor. The CSI during the channel coherence time is no longer fixed due to the ACA introduced by the DRIS-based PFJ. We quantified the impact of DISCO jamming attacks on the sum rate for any given ISAC waveform. In addition, the DISCO jamming leads to biased DoA estimation, which in turn degrades the sensing performance of the system. The amount of the bias can be increased by increasing the number of DRIS reflective elements. To characterize the sensing performance degradation due to the DRIS-induced biases, a theoretical analysis based on the CRLB will be conducted in our future work.

## References

[1] H. Zhang, H. Zhang, B. Di, and L. Song, "Holographic integrated sensing and communications: Principles, technology, and implementation," *IEEE Commun. Mag.*, vol. 61, no. 5, pp. 83–89, May 2023.

[2] J. A. Zhang, K. Wu, X. Huang, Y. J. Guo, D. Zhang, and R. W. Heath, "Integration of radar sensing into communications with asynchronous transceivers," *IEEE Commun. Mag.*, vol. 60, no. 11, pp. 106–112, Nov. 2022.

[3] F. Liu et al., "Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1728–1767, Jun. 2022.

[4] F. Liu, L. Zhou, C. Masouros, A. Li, W. Luo, and A. Petropulu, "Toward dual-functional radar-communication systems: Optimal waveform design," *IEEE Trans. Signal Process.*, vol. 66, no. 16, pp. 4264–4279, Aug. 2018.

[5] F. Liu, C. Masouros, A. Li, H. Sun, and L. Hanzo, "MU-MIMO communications with MIMO radar: From co-existence to joint transmission," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2755–2770, Apr. 2018.

[6] R. Liu, M. Li, H. Luo, Q. Liu, and A. L. Swindlehurst, "Integrated sensing and communication with reconfigurable intelligent surfaces: Opportunities, applications, and future directions," *IEEE Wireless Commun.*, vol. 30, no. 1, pp. 50–57, Feb. 2023.

[7] K. Zhi, C. Pan, H. Ren, K. K. Chai, and M. Elkashlan, "Active RIS versus passive RIS: Which is superior with the same power budget?" *IEEE Commun. Lett.*, vol. 26, no. 5, pp. 1150–1154, May 2022.

[8] H. Zhang et al., "Intelligent omni-surfaces for full-dimensional wireless communications: Principles, technology, and implementation," *IEEE Commun. Mag.*, vol. 60, no. 2, pp. 39–45, Feb. 2022.

[9] W. Mei, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface aided wireless networks: From single-reflection to multi-reflection design and optimization," *Proc. IEEE*, vol. 110, no. 9, pp. 1380–1400, Sep. 2022.

[10] W. Mei et al., "Intelligent omni-surfaces: Ubiquitous wireless transmission by reflective-refractive metasurfaces," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 219–233, Jan. 2022.

[11] Z. Wang, X. Mu, and Y. Liu, "STARS enabled integrated sensing and communications," *IEEE Trans. Wireless Commun.*, vol. 22, no. 10, pp. 6750–6767, Oct. 2023.

[12] Z. Yu et al., "Active RIS-aided ISAC systems: Beamforming design and performance analysis," *IEEE Trans. Commun.*, vol. 72, no. 3, pp. 1578–1595, Mar. 2024.

[13] H. Huang et al., "DISCO might not be funky: Random intelligent reflective surface configurations that attack," *IEEE Wireless Commun.*, early access, Jul. 15, 2024, doi: 10.1109/MWC.014.2300470.

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

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

[16] H. Huang et al., "Anti-jamming precoding for disco intelligent reflecting surfaces based fully-passive jamming attacks," *IEEE Trans. Wireless Commun.*, early access, Feb. 7, 2024, doi: 10.1109/TWC.2024.3360728.

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

[18] Z. Wang, X. Mu, Y. Liu, "Near-field integrated sensing and communications," *IEEE Commun. Lett.*, vol. 27, no. 8, pp. 2048–2052, Aug. 2023.

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

[20] "Further advancements for E-UTRA physical layer aspects; (Release 9)," 3GPP, Sophia Antipolis, France, document TS 36.814, Mar. 2010.

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:35:18 UTC from IEEE Xplore. Restrictions apply.