ACCEPTED FROM OPEN CALL

DISCO Might Not Be Funky: Random Intelligent Reflective Surface Configurations That Attack

Huan Huang, Lipeng Dai, Hongliang Zhang, Chongfu Zhang, Zhongxing Tian, Yi Cai, A. Lee Swindlehurst, and Zhu Han

Abstract

Emerging intelligent reflective surfaces (IRSs) significantly improve system performance, but also pose a significant risk for physical layer security (PLS). Unlike the extensive research on legitimate IRS-enhanced communications, in this article we present an adversarial IRS-based, fully-passive jammer (FPJ). We describe typical application scenarios for disco IRS (DIRS)-based FPJ, where an illegitimate IRS with random, time-varying reflection properties acts like a "disco ball" to randomly change the propagation environment. We introduce the principles of DIRS-based FPJ and overview existing investigations of the technology, including a design example employing one-bit phase shifters. The DIRS-based FPJ can be implemented without either jamming power or channel state information (CSI) for the legitimate users (LUs). It does not suffer from the energy constraints of traditional active jammers, nor does it require any knowledge of the LU channels. In addition to the proposed jamming attack, we also propose an anti-jamming strategy that requires only statistical rather than instantaneous CSI. Furthermore, we present a data frame structure that enables the legitimate access point (AP) to estimate the DIRS-jammed channels' statistical characteristics in the presence of the DIRS jamming. Typical cases are discussed to show the impact of the DIRS-based FPJ and the feasibility of the anti-jamming precoder (AJP). Moreover, we outline future research directions and challenges for the DIRS-based FPJ and its anti-jamming precoding to stimulate this line of research and pave the way for practical applications.

Introduction

Due to the broadcast and superposition nature of wireless channels, the open wireless air interface is vulnerable to malicious attacks such as jamming or denial-of-service attacks [1, 2]. Jamming attacks can be launched to intentionally disrupt wireless communication networks such as WiFi, Bluetooth, Internet of Things (IoT), and cellular networks. In traditional wireless systems, active jammers (AJs), which impose intentional interference on the communication between an access point (AP) and its legitimate users (LUs), have been widely investigated. In general, physical-layer AJs can be classified as constant AJs, intermittent AJs, reactive AJs, and adaptive AJs [1]. A constant AJ continuously broadcasts jamming signals, such as pseudorandom noise or Gaussian-modulated waveforms, over the wireless air interface to prevent the AP from communicating with the LUs. However, constant AJs are energy-inefficient because they constantly consume power. To address this issue, intermittent AJs, reactive AJs, and adaptive AJs have been proposed whose basic motivation is to reduce the duration of the jamming transmission and hence reduce the energy consumption. However, all types of active jamming require a certain amount of energy consumption to effectively attack the LUs.

Recently, intelligent reflective surfaces (IRSs) [3–5], which reflect electromagnetic waves in a controlled manner, have been proposed as a promising technology for future 6G systems. An IRS is an ultra-thin surface equipped with multiple subwavelength reflective elements whose electromagnetic responses (e.g., amplitudes and phase shifts) can be configured, for instance, by simple programmable PIN or varactor diodes. Previous works have mainly focused on using legitimate IRSs to improve performance, assuming that the legitimate AP knows the IRS-related channel state information (CSI), and can control their phase responses. At the same time, a handful of works have examined the risk that illegitimate IRSs pose to physical layer security (PLS) [6, 7]. For example, the authors in [6] illustrated that illegitimate IRSs can be used to help the AJs enhance their jamming attacks, especially in the case of AJ-LU link blocking. However, illegitimate IRS-aided AJs also have the inherent disadvantage of requiring significant energy consumption. Considering this inherent energy consumption drawback, *can jamming attacks be launched without jamming power?*

The authors in [8] have reported an adversarial IRS-based passive jammer (PJ) for single-user multiple-input single-output (SU-MISO) systems that essentially consumes no power. This adversarial IRS destructively adds the reflected path signal

Huan Huang, Zhongxing Tian, and Yi Cai (corresponding author) are with Soochow University, China; Lipeng Dai and Chongfu Zhang are with University of Electronic Science and Technology of China, China; Hongliang Zhang is with Peking University, China; A. Lee Swindlehurst is with University of California, Irvine, USA; Zhu Han is with University of Houston, USA, and also with Kyung Hee University, South Korea.

Digital Object Identifier: 10.1109/MWC.014.2300470

to the direct path signal to minimize the received power at the LU. Although this PJ can launch jamming attacks without consuming power, the CSI of all wireless channels involved must be known at the unauthorized IRS. Due to the passive nature of IRSs, the CSI of IRS-related channels is estimated jointly with that of the AP and LUs. In other words, if the illegitimate IRS aims to acquire LU CSI, it must train to learn CSI jointly with the legitimate AP and LUs. Therefore, the assumption that the illegitimate IRS knows the CSI of all channels is unrealistic. Given the difficulty of illegitimate IRSs in acquiring CSI, *can jamming attacks be launched without either jamming power or LU CSI?*

The emergence of IRSs in support of existing wireless systems significantly improves their performance without noticeably increasing the power consumption or cost. However, it also poses a significant risk for PLS. For example, the authors in [9] have summarized some typical IRS-based attack strategies such as IRS-based jamming and eavesdropping. In this article, we explore the potential of illegitimate IRSs in launching fully-passive jamming attacks and present a new attack approach referred to as Disco IRS (DIRS)-based fully passive jammer (FPJ). We discuss the principle, advantages, and implementation of this new attack. In view of the great threat that such fully-passive attacks pose to communication networks, we further discuss an anti-jamming precoding strategy to counteract it. Moreover, we outline future research directions and challenges.

Disco IRS Based Active Channel Aging: A New Jamming Attack

Fundamentals

To implement an FPJ without relying on either jamming power or LU CSI, the interesting idea of DIRS was first proposed in [10], which described an illegitimate IRS with random reflection properties that acts like a "disco ball." It is worth noting that the DIRS-based FPJ does not require jamming power, but it does consume a relatively small amount of circuit power to control its operation. While a disco ball makes dancing more funky, in a wireless communication system the result is not so pleasing. In a DIRS system, the controller generates a single realization of random independently and identically distributed (i.i.d.) phase shifts once during the pilot transmission (PT) phase, and then a different i.i.d. set of phase shifts during the subsequent data transmission (DT) phase. As a result, serious active channel aging (ACA) interference, that is, a type of inter-user interference (IUI), is introduced. Note that the DIRS-based ACA is different from the channel aging (CA) in traditional MU-MISO systems, which is caused by channels that vary between when they are learned at the legitimate AP and when they are used for precoding due to time variations in the channel and delays in the computation [11].

Based on this ACA idea [10], the work in [12] further illustrated that the DIRS-based ACA interference can also be introduced by turning off the illegitimate IRS (i.e., the wireless signals are perfectly absorbed by the DIRS) during the PT phase and then generating i.i.d. random reflecting vectors multiple times during the DT phase. It is worth noting that such a temporal DIRS-based FPJ must know when the PT phase ends and the DT phase begins, which requires some synchronization with the legitimate system. The DIRS-based FPJs in [10, 12] which require neither jamming power nor LU CSI, pose a significant risk to PLS. For example, the theoretical analysis in [12] showed that a DIRS-based FPJ using only one-bit quantized phase shifts can achieve the desired jamming effects as long as the number of DIRS reflective elements is large enough. The immediate question, therefore, is *how to mitigate the DIRS-based ACA interference* [12].

To address this issue, [13] first proposed an anti-jamming precoder (AJP) to counteract the temporal DIRS-based FPJ. In particular, the statistical characteristics of the DIRS-jammed channels were derived and an AJP that can achieve the maximum signal-to-jamming-plus-noise ratio (SJNR) was developed. The work in [9] showed how the legitimate AP can acquire the statistical characteristics in a practical way, and also extended the AJP in [13] to address persistent DIRS-based fully-passive jamming. Since the DIRS-based FPJs in [10] and [12] are included in the persistent DIRS-based FPJ model, the AJP is suitable for all DIRS-based fully-passive attacks.

DIRS Features

The above prior work also derived some interesting properties of this temporal DIRS-based ACA via theoretical analysis. For example, the jamming impact of the DIRS-based FPJ proposed in [12] cannot be mitigated by increasing the transmit power, and classical anti-jamming approaches, such as spread spectrum and frequency-hopping techniques, cannot be used against an FPJ because the source of the jamming attacks is the transmit signals themselves and has the same characteristics (e.g., carrier frequencies, etc).

Multi-input multi-output (MIMO) interference cancellation has also been studied as an important anti-jamming approach [14]. However, MIMO interference cancellation is effective for DIRS-based ACA interference only if the legitimate AP has knowledge of the LU and DIRS-jammed channels. Since the DIRS is passive and the phase shifts and amplitudes are randomly generated, the DIRS-based ACA interference cannot be mitigated by MIMO interference cancellation. Table 1 compares the characteristics of AJs, PJs, and FPJs.

DIRS Applications

Figure 1 illustrates different types of wireless communications systems that can be jammed by persistent DIRS-based FPJs. Note that there are many possible deployment strategies for DIRSs, for instance near a legitimate AP, on an unmanned aerial vehicle (UAV) [5], or on public transportation vehicles. The existing works [9, 10, 12, 13] have only investigated fixed DIRS deployments near the legitimate AP, and DIRS placement on mobile platforms (e.g., UAVs) is worthy of further investigation, including optimization of the UAV-based DIRS route, and so on.

DIRS Principles

In a persistent DIRS-based FPJ, a random sequence with i.i.d. random elements generated by a controller is used to adjust the DIRS phase shifts. While the IRS phase shifts is controlled, the amplitudes

The emergence of IRSs in support of existing wireless systems significantly improves their performance without noticeably increasing the power consumption or cost. However, it also poses a significant risk for PLS.

Category	Jamming energy	Channel knowledge	MIMO-based cancellation	Frequency-hopping/ spread spectrum
Active jammer (AJ) [1]	Required	Not Required	✓	✓
IRS-aided AJ [6]	Required	Required	✓	✓
Passive jammer (PJ) [8]	Not Required	Required	✓	×
Fully-passive jammer (FPJ) [10, 12]	Not Required	Not Required	×	×

The mark ✓ represents that the scheme works;
The mark × represents that the scheme does not work.

TABLE 1. Comparison of different jammers.

of the reflective elements are a function of their corresponding phase shifts due to the unique electromagnetic properties of typical IRS elements [3].

In an MU-MIMO/MISO system, the legitimate AP jointly trains the CSI with the LUs during the PT phase, and the CSI is used to design a precoder for transmitting signals to the LUs during the DT phase. The LU CSI can be jointly estimated using existing algorithms, such as for example the least squares (LS) algorithm. In general, wireless channels are assumed to remain unchanged during a channel coherence interval consisting of a PT phase followed by a DT phase. Based on this assumption, the legitimate AP can design a transmit precoder based on the CSI obtained from the PT phase. However, the programmable IRS provides the ability to actively age the wireless channels within their coherence interval and thus produces a situation where the CSI obtained in the PT phase is different from that in the DT phase.

Inspired by this idea, a DIRS is introduced to actively age the wireless channels [10, 12]. Specifically, assume that the length of the PT phase is T_P and that of the DT phase is $T_D = CT_P$, that is, the length of a channel coherence interval is $T_C = T_P + T_D = (C + 1)T_P$. We can exploit the DIRS to rapidly age the wireless channels, and effectively produce a channel with coherence interval much less than T_C. As a result, serious DIRS-based ACA interference is introduced, and the LUs are then jammed. In a persistent DIRS-based FPJ, the DIRS controller generates a single i.i.d. random sequence used to tune the reflecting phase shifts during the PT phase, and then generates different i.i.d. random sequences to change the reflecting phases shifts $Q(Q \geq C)$ times during the DT phase. If the DIRS controller sets the DIRS reflecting vector to zero during the PT phase, this corresponds to the case investigated in [12]. Moreover, if we let $Q = 1$ during the DT phase, the persistent DIRS-based FPJ reduces to the one studied in [10].

Taking a legitimate AP with the widely-used ZF transmit precoder as an example, in a traditional MU-MISO/MIMO system, the AP calculates the ZF precoder based on the CSI obtained in the PT phase to transmit signals during the DT phase. If the wireless channels remain unchanged in a channel coherence interval, the transmit precoding vector wk for the k-th LU is always orthogonal to the subspace of the other co-channel users, as shown in Fig. 1. However, when the DIRS-based ACA interference is introduced, the wireless channels during the DT phase are not the same as those during the PT phase, and the transmit precoding vector wk is no longer orthogonal to the co-channel user subspaces during the DT phase. As a result, serious ACA interference is introduced by the persistent DIRS-based FPJ. As illustrated in Fig. 1, DIRSs cause the signals from the DIRS-jammed channels to behave like additive Gaussian white noise (AWGN) [9, 12, 13]. As a result, the LUs are jammed.

Implementation of Persistent DIRS-Based FPJ Using One-Bit Phase Shifts

An implementation example of a persistent DIRS-based FPJ using an IRS with one-bit phase shifters is shown in Fig. 2. Each reflective element has one-bit quantized phase shifts and corresponding reflection amplitudes denoted as $\{\theta_1, \theta_2\}$ and $\{a_1, a_2\}$, respectively. Furthermore, we assume that the DIRS phase shifts follow the stochastic distribution $\mathcal{F}$. To implement this DISCO approach, the DIRS controller first generates an i.i.d. random sequence following $\mathcal{F}$ to control the DIRS phase shifts and amplitudes during the PT phase, where the diagonal reflecting matrix is denoted by $\Phi(t_0)$. Then, the wireless channel of the k-th LU can be written as $h_{PT,k}(t_0)$, whose CSI is estimated jointly by the legitimate AP and the k-th LU during the PT phase. The DIRS controller subsequently generates a set of m different i.i.d. random sequences, also following $\mathcal{F}$, in order to adjust the DIRS phase shifts and amplitudes during the DT phases, where the diagonal reflecting matrices are denoted by $\Phi(t_1)$, $\Phi(t_2)$, ..., $\Phi(t_m)$. As a result, the k-th LU channel is no longer $h_{PT,k}(t_0)$ during the DT phase, but varies randomly according to the random IRS reflections.

Due to the use of the persistent DIRS-based FPJ, the acquired CSI from the PT phase is rapidly aged within a channel coherence interval. We assume that the DIRS controller generates i.i.d. random sequences Q times during the DT phase. In fact, using C different i.i.d. random sequences (i.e., $Q = C$) to change the wireless channels C times is enough to shorten the original channel coherence from T_C to T_P, in which case there is essentially no time available for data transmission. The work in [12] has shown that the DIRS-based ACA interference generated by a one-bit DIRS can jam the LU rates to zero as long as the number of DIRS elements is large enough. As discussed in [7], countermeasures based on channel separation can only be used to resist AWGN-like ACA interference with high multipath resolution such as wideband OFDM. However, it is challenging to mitigate the DIRS-based ACA interference for cases with low multipath resolution [7], such as narrowband systems.

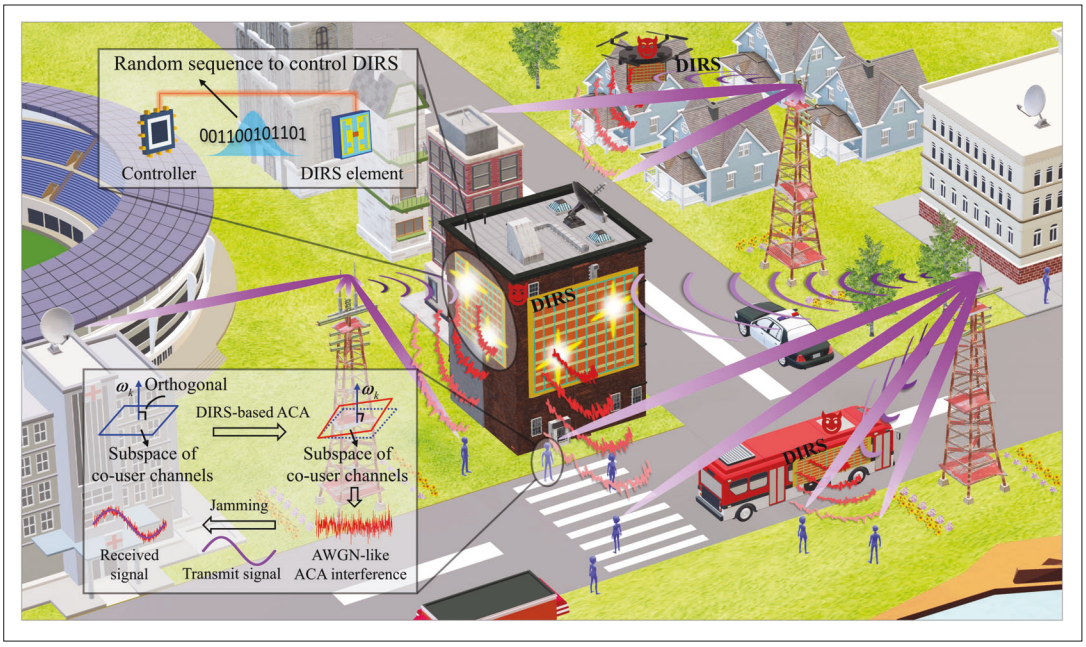

FIGURE 1. Implementation of disco intelligent reflective surface (DIRS) based fully-passive jamming attacks, where the DIRS reflection properties, that is, the phase shifts and amplitudes are randomly and independently generated by the DIRS controller.

An Anti-Jamming Precoding Strategy for Persistent DIRS-Based FPJ

To design a practical AJP for persistent DIRS-based FPJs, legitimate systems must consider the following constraints: the anti-jamming precoding must be computed without any useful information from the illegitimate DIRS; and the implementation of the anti-jamming precoding cannot require any changes to the existing system architecture. Fortunately, the pioneering works in [9, 12, 13] have proved that the elements of DIRS-jammed channels converge to a complex Gaussian distribution as the number of the DIRS reflective elements is large enough. In practice, to cope with the multiplicative large-scale channel fading in cascaded DIRS-jammed channels, the DIRS must be equipped with a large number of reflective elements to ensure a significant jamming impact [12, 13, 9]. Based on the properties of Gaussian distributions, one possible AJP for the k-th LU against persistent DIRS-based FPJ is given by

$$w_{\text{Anti},k} \propto max.\,\text{eigenvector}\left(\frac{h_{PT,k}h_{PT,k}^{H}+\delta_k^2\mathbf{I}_{N_A}}{\widetilde{\mathbf{H}}_{PT,k}\widetilde{\mathbf{H}}_{PT,k}^{H}+\left(\frac{\delta^2 K}{P_0+\sum_{u\neq k}\delta_u^2}\right)\mathbf{I}_{N_A}}\right), \quad (1)$$

where $h_{PT,k}^{H}$ is the k-th LU channel estimated during the PT phase, δ_k, k = 1, 2,... K represents a certain statistical characteristic of the DIRS-jammed channel between the AP and the k-th LU, and $\widetilde{\mathbf{H}}_{PT,k} = [h_{PT,1}, \cdots, h_{PT,k-1}, h_{PT,k+1}, \ldots, h_{PT,K}]$ denotes the co-user channels of the k-th LU during the PT phase. In addition, P_0 and δ^2 represent the total transmit power and the variance of the received signals during the DT phase.

Note that the implementation of the anti-jamming precoding in Eq. 1 requires the statistical characteristics of the DIRS-jammed channels, that is, $\{\delta_k\}_{k=1}^{K}$. A feasible data frame structure that can be used by the legitimate AP to estimate these statistical characteristics is illustrated in Fig. 3.

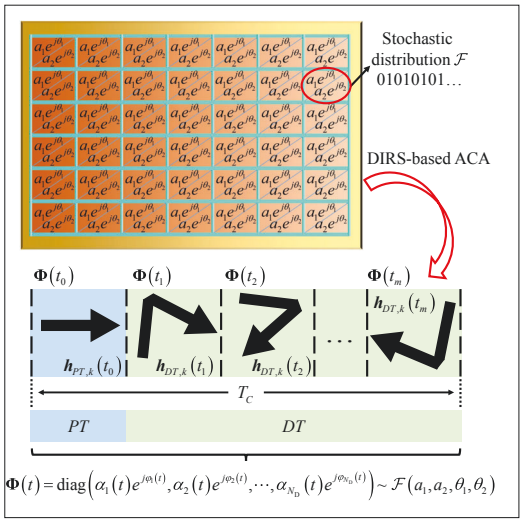

FIGURE 2. Implementation example of a persistent DIRS-based FPJ using an IRS with one-bit quantized phase shifts, where the DIRS with random reflection properties actively ages wireless channels within a channel coherence interval.

In the designed frame structure, the LUs only need to feed their received power values back to the AP when they detect that they are being jammed, for example, when they detect a degradation of their SJNRs. Only a few bits are required to feed back the received power values since they are only scalars. During a channel coherence interval, we assume that the power information is fed back m times, and the s-th feedback set of received power values is denoted as $\{p_k^s\}_{k=1}^{K}(1 \le s \le m)$. Consequently, the s-th estimate of the statistical characteristics $\{\delta_k^2 \mid_s\}_{k=1}^{K}$ can be computed as shown in Fig. 3. Then, we can substitute the s-th estimate into Eq. 1 to compute the AJP WsAnti,k. The work in [9] has shown only one or two feedback mes-

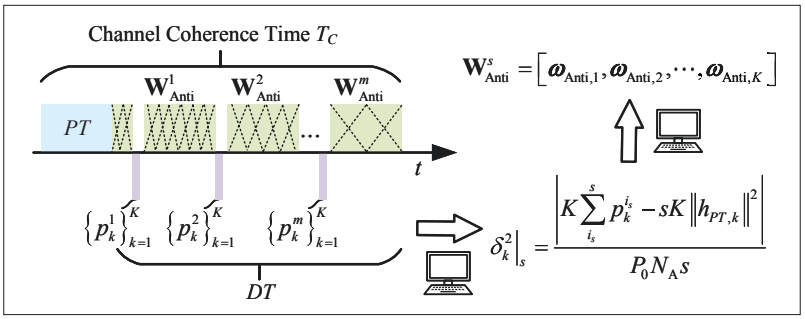

FIGURE 3. A data frame structure for the legitimate AP to estimate the statistical characteristics of DIRS-jammed channels for the anti-jamming precoder.

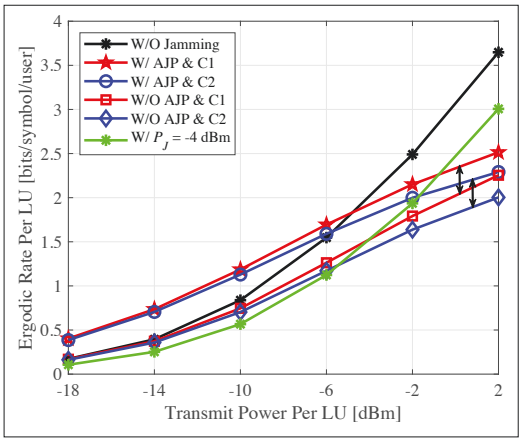

FIGURE 4. Ergodic rate vs transmit power for different benchmarks under attacks launched by the persistent DIRS-based FPJ.

sages are sufficient to effectively estimate the statistical characteristics for the AJP.

It is seen that the AJP for persistent DIRS-based FPJs has the following interesting properties:

- Regardless of the DIRS phase distribution used by the persistent DIRS-based FPJ, the proposed AJP is valid as long as the number of the DIRS reflective elements is large enough.
- The legitimate system can acquire the statistical characteristics of the DIRS-jammed channels without changing its architecture or cooperating with the illegitimate DIRS.

Case Study

Consider a persistent DIRS-based FPJ case in which an MU-MISO system is jammed by a 2048-element one-bit DIRS with phase shifts and amplitudes randomly chosen from $\{\pi/9, 7\pi/6\}$ and $\{0.8, 1\}$ [3]. The legitimate AP equipped with 16 antennas is located at (0 m, 0 m, 5 m) and communicates with 12 single-antenna LUs which are randomly distributed in a circular region with a radius of 20 m and centered at (0 m, 180 m, 0 m). The DIRS is deployed at ($-d_{\text{AD}}$ m, 0 m, 5 m) and $d_{\text{AD}} = 2$.

To show the difference between the persistent DIRS-based FPJs with different phase shift distributions, we consider the following two cases: *Case 1* — for each DIRS element, the probability of choosing phase shift $\pi/9$ is 0.25 and the probability of choosing phase shift $7\pi/6$ is 0.75; *Case 2* — each phase shift is equally likely. The following benchmarks are compared: the legitimate AP uses the ZF precoder without a DIRS-based jamming attack (W/O Jamming), that is, no DIRS; the legitimate AP is jammed by the persistent DIRS-based FPJ while the random DIRS phase shifts follow the distributions in *Case 1* (W/O AJP and C1) and in *Case 2* (W/O AJP and C2); the legitimate AP adopts the AJP for *Case 1* (W/ AJP and C1) and *Case 2* (W/ AJP and C2); the legitimate AP suffers from an AJ with −4 dBm jamming power (AJ w/ P_J = −4 dBm), where the AJ is deployed at (−2 m, 0 m, 5 m).

Figure 4 illustrates the relationship between the rate per LU [13, 9] under the persistent DIRS-based fully-passive jamming attacks and the transmit power per LU (i.e., P_0/K). From Fig. 4, we can see that the persistent DIRS-based FPJ can effectively impair the LU rate with neither jamming power nor LU CSI. Specifically, the persistent DIRS-based FPJ in *Case 1* and *Case 2* reduces the rate per LU by 28 percent and 34.6 percent at −2 dBm transmit power, respectively. As the transmit power increases, the jamming impact of the persistent DIRS-based FPJ gradually becomes stronger and eventually exceeds that of the AJ. Therefore, we can see that the rates per LU for W/O AJP and C1 and W/O AJP and C2 are even worse than that of AJ w/ P_J = −4 dBm when the transmit power is greater than −6dBm. The traditional AJ approach requires significant jamming power, and increasing the AP transmit power can mitigate the AJ attacks. However, increasing the transmit power not only fails to mitigate the jamming impact of the persistent DIRS-based FPJ but even aggravates it.

Compared to the rates per LU obtained from W/O Jamming, the results for W/ AJP and C1 and W/ AJP and C2 are better in the low power domain. This is because the proposed AJP can to some extent exploit the signals transmitted through the DIRS-jammed channels to improve performance. Many practical MU-MISO systems using low-order modulations, such as quadrature phase shift keying (QPSK), can work in the low transmit power domain. Moreover, the AJP can mitigate the DIRS-based jamming attacks with different phase shift distributions (e.g., *Cases 1* and *2*). Specifically, the AJP in *Case 1* and *Case 2* improves the rate per user by 19.2 percent and 21.1 percent at -2 dBm transmit power, respectively.

Figure 5 illustrates the influence of the AP-DRIS distance d_{AR}. As d_{AR} increases, the large-scale fading also increases, and the jamming impact of the persistent DIRS-based FPJ is weakened. The anti-jamming precoder can achieve a rate similar to the case without jamming when the jamming impact is weak. More Specifically, the results from the AJP, that is, W/ AJP and C1 and W/ AJP and C2, achieve better performance when $d_{\text{AR}} > 4$. This is because the gain obtained from the DIRS-based channels using the anti-jamming precoding is greater than the degradation due to the persistent DIRS-based FPJ. However, the results of W/O AJP and C1 and W/O AJP and C2 are always lower than the rates of W/O Jamming.

Future Directions

Based on our investigations, we further outline the following research directions.

DIRS-Based ACA

An attacker that wants to achieve a sufficient jamming impact from a persistent DIRS-based FPJ must ensure that the signals in the DIRS-jammed channels are sufficiently strong. Based on our

observations, it is possible that an attacker using a persistent DIRS-based FPJ can enhance its jamming impact as follows:

- The attacker can employ a DIRS with one-bit reflective elements whose reflection gain is as large as possible. Furthermore, the attacker can deploy multiple illegitimate IRSs that use the DISCO approach. However, a corollary question is how does the attacker control the phase shifts of all DIRSs in a coordinated manner to maximize the jamming impact?
- The attacker can optimize the DIRS phase shift distribution to improve its jamming impact, since we have shown that the performance of a persistent DIRS-based FPJ can vary with different phase shift distributions. However, what is the optimal phase distribution?
- The attacker can use an active IRS [15] to replace the passive DIRS to cope with the multiplicative large-scale channel fading. However, optimizing the active IRS gains is challenging because the attacker has no knowledge of the LU channels.

Anti-Jamming Precoder

Jamming attacks and their anti-jamming strategies can be seen as a form of "hand-to-hand combat," where each side is constantly trying to gain the upper hand. For the proposed AJP, our investigation has the following important implication: as long as the intensity of the DIRS-based ACA interference relative to the transmit signals can be suppressed below a certain threshold value, the persistent DIRS-based FPJ does not degrade the performance of the MU-MISO system, but enhances it due to the proposed AJP. This suggests that the legitimate AP should minimize the amount of DIRS-based ACA interference relative to the strength of the useful signals, and then use the AJP against the persistent DIRS-based FPJ.

One possible approach to suppressing the strength of DIRS-based ACA interference relative to the transmit signals is to introduce legitimate IRSs to enhance the desired signals and reduce the relative impact of the DIRS-based ACA interference. However, DIRS-based ACA interference is also generated from the legitimate IRS-related channels. Therefore, a precoding strategy for legitimate IRSs that significantly enhances the desired signals and does not significantly enhance the DIRS-based ACA interference is needed. In addition, methods for detecting the presence of DIRS-based fully-passive jamming attacks and their detection probability and false-alarm probability performance should be investigated.

Conclusions

To raise concerns about the potential threats posed by illegitimate IRSs, we presented a persistent DIRS-based FPJ that can be implemented using a simple one-bit IRS. By introducing significant ACA interference, the persistent DIRS-based FPJ can launch significant fully-passive jamming attacks on LUs with neither jamming power nor LU CSI. To address the significant threats posed by a persistent DIRS-based FPJ, an AJP has been developed that exploits only the statistical characteristics of the DIRS-jammed channels instead of their instantaneous CSI. A data frame structure that can be used by the legitimate AP to estimate the statistical characteristics has also been designed. The simulation results show that the DIRS-based FPJ with different phase shift distributions (i.e., Case 1 and 2) reduces the rate per LU by 28 percent and 34.6 percent at –2 dBm transmit power, but the AJP can improve the rate per user by 19.2 percent and 21.1 percent, respectively.

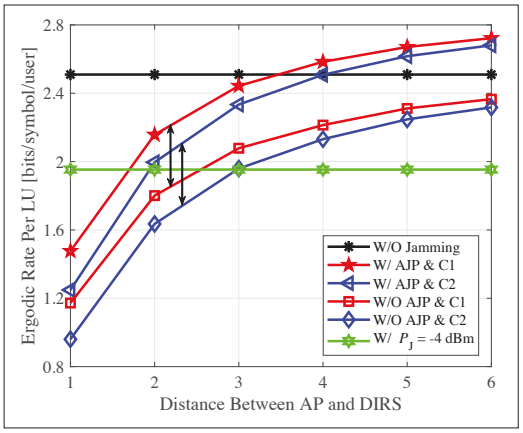

FIGURE 5. Relationship between the ergodic rate per LU and the AP-DIRS distance for different benchmarks under jamming attacks launched by the persistent DIRS-based FPJ at –2 dBm transmit power per LU.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (62250710164, 62275185, 62371011), and partially supported by the U.S. National Science Foundation (CNS — 2107216, CNS — 2128368, CNS — 2107182, CMMI — 2222810, ECCS-2302469, ECCS — 2030029), US Department of Transportation, Toyota, Amazon, and Japan Science and Technology Agency (JST) Adopting Sustainable Partnerships for Innovative Research Ecosystem (ASPIRE) JPMJAP2326.

References

[1] A. Mukherjee *et al.*, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, 3rd Qtr. 2014, pp. 1550–73.

[2] Y. Zou *et al.*, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proc. IEEE*, vol. 104, no. 9, Sept. 2016, pp. 1727–65.

[3] H. Zhang *et al.*, "Intelligent Omni-Surfaces for Full-Dimensional Wireless Communications: Principles, Technology, and Implementation," *IEEE Commun. Mag.*, vol. 60, no. 2, Feb. 2022, pp. 39–45.

[4] Q. Wu and R. Zhang, "Towards Smart and Reconfigurable Environment: Intelligent Reflecting Surface Aided Wireless Network," *IEEE Commun. Mag.*, vol. 58, no. 1, Jan. 2020, pp. 106–12.

[5] T. Cui *et al.*, "Coding Metamaterials, Digital Metamaterials and Programmable Metamaterials," *Light-Sci. Appl.*, vol. 3, e218, Oct. 2014.

[6] Y. Wang *et al.*, "Wireless Communication in the Presence of Illegal Reconfigurable Intelligent Surface: Signal Leakage and Interference Attack," *IEEE Wireless Commun.*, vol. 29, no. 3, June 2022, pp. 131–38.

[7] G. Li *et al.*, "Reconfigurable Intelligent Surface for Physical Layer Key Generation: Constructive or Destructive?" *IEEE Wireless Commun.*, vol. 29, no. 4, Aug. 2022, pp. 146–53.

[8] B. Lyu *et al.*, "IRS-Based Wireless Jamming Attacks: When Jammers Can Attack Without Power," *IEEE Wireless Commun. Lett.*, vol. 9, no. 10, Oct. 2020, pp. 1663–67.

[9] H. Huang *et al.*, "Anti-Jamming Precoding for Disco Intelligent Reflecting Surfaces Based Fully-Passive Jamming Attacks," *IEEE Trans. Wireless Commun.*, early access, Feb. 2024, doi: 10.1109/TWC.2024.3360728.

[10] H. Huang *et al.*, "Illegal Intelligent Reflecting Surface Based Active Channel Aging: When Jammer Can Attack Without Power and CSI," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, Aug. 2023, pp. 11,018–22.

[11] 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, Aug. 2013, pp. 338–51.
[12] H. Huang *et al.*, "Disco Intelligent Reflecting Surfaces: Active Channel Aging for Fullypassive Jamming Attacks," *IEEE Trans. Wireless Commun.*, vol. 23, no. 1, Jan. 2024, pp. 806–19.
[13] H. Huang *et al.*, "An Anti-Jamming Strategy for Disco Intelligent Reflecting Surfaces Based Fullypassive Jamming Attacks," *Proc. 2023 IEEE Global Commun. Conf.*, Kuala Lumpur, Malaysia, Dec. 2023.
[14] Q. Yan *et al.*, "Jamming Resilient Communication Using MIMO Interference Cancellation," *IEEE Trans. Inf. Forensic Secur.*, vol. 11, no. 7, July 2016, pp. 1486–99.
[15] R. Long *et al.*, "Active Reconfigurable Intelligent Surface-Aided Wireless Communications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 8, Aug. 2021, pp. 4962–75.

Biography

Huan Huang [S'21, M'24] 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 is currently an Instructor in the School of Electronic and Information Engineering, Soochow University, Suzhou, Jiangsu, China. His research interests include massive MIMO, intelligent reflective surfaces, physical layer security, and digital signal processing. He has published more than 30 papers in academic conferences and journals. He is currently an Area Editor of Physical Communication. He also served as a TPC Member for IEEE GLOBECOM'23 and a Co-Chair of IEEE WCNC workshop in 2024.

Lipeng Dai is currently working toward the M.S. degree with the University of Electronic Science and Technology of China (UESTC), Chengdu, China. He won a national scholarship in 2023. His research focuses on intelligent reflecting surface, physical layer security, and jamming.

Hongliang Zhang [S'15, M'19] is an assistant professor at the School of Electronics, Peking University, Beijing, China. He received the Ph.D. degree at the School of Electrical Engineering and Computer Science at Peking University in 2019. His current research interest includes reconfigurable intelligent surfaces, aerial access networks, and game theory. He received the best doctoral thesis award from Chinese Institute of Electronics in 2019. He is the recipient of 2021 IEEE Comsoc Heinrich Hertz Award for Best Communications Letters.

Chongfu Zhang received the Ph.D. degree from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2009. From 2013 to 2014, he was a Visiting Scholar with the University of Southern California, Los Angeles, CA, USA. He is currently a Full Professor with UESTC. He has authored or coauthored more than 100 articles and holds 70 patents. His research interests include broadband access networks, microwave photonics, and communication security.

Zhongxing Tian received the M.S. degree from the Soochow University, Suzhou, China, in 2023, where he is currently working the Ph.D. degree. He joined the Jiangsu Hengxin Semitech Co., Ltd of the Hengtong group as a Digital Signal Processing (DSP) Algorithm Engineer in 2023.
His research interests include coherent optical communications, medium- and short-reach optical transmissions, and free space optical communications.

Yi Cai [S'98, M'01] received the Ph.D. degree in electrical engineering from the University of Maryland Baltimore County, Baltimore, Maryland, USA, in 2001. He 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. 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 is Professor and Chair of the EECS Department at UC Irvine. He is a Foreign Member of the Royal Swedish Academy of Engineering Sciences, and a former Hans Fischer Senior Fellow in the Institute for Advanced Studies at the Technical University of Munich. His research focuses on multi-antenna signal processing for wireless communications, radar and biomedicine. He is an IEEE Fellow and has received several IEEE awards, including the Baker Prize Paper Award, the Communications Society Stephen O. Rice Prize, three Signal Processing Society (SPS) Best Paper Awards, and the SPS Donald G. Fink Overview Paper Award.

Zhu Han [S'01, M'04, SM'09, F'14] received his Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park. Currently, he is a professor in the Electrical and Computer Engineering Department as well as in the Comp at the University of Houston, Texas. He is an AAAS fellow since 2019. He is 1 percent highly cited researcher since 2017 according to Web of Science, and winner of 2021 IEEE Kiyo Tomiyasu Award.