A Novel Pilot Spoofing Scheme via Intelligent Reflecting Surface Based On Statistical CSI

Jie Yang, Xinsheng Ji, Feihu Wang, Kaizhi Huang, Lin Guo

Abstract—Pilot spoofing attack brings new challenges to physical layer secure transmission. However, this method will not work without any knowledge about the pilot sequence and active eavesdropping can be detected by constructing random pilot sequence. Intelligent reflecting surface (IRS), with the real-time programmable features for wireless channels, provides new possibilities for effective pilot spoofing. In this paper, the IRS is deployed near the legitimate users and the legitimate signal can always be passively reflected. Then the control strategy is embedded into the communication process under time-division duplex mode to assist eavesdroppers to conduct pilot spoofing. By setting different phase shifts at the IRS during the uplink phase and downlink phase, the channel reciprocity disappears, and thus secure beamforming vector is biased towards the eavesdropper. Furthermore, in order to overhear more information, the average secrecy rate minimization problem based on statistical channel state information is established by carefully designing the phase shifts, which is non-trivial to solve. With alternating optimization and Charnes-Cooper transformation technique, the original problem is transformed into convex form and a near optimal solution is achieved. Finally, simulation results show that our proposed scheme can pose serious secure threat without any energy footprint. What's more, if the IRS is not utilized by the internal users properly, it will bring more threat.

Index Terms—Pilot spoofing, Intelligent reflecting surface, Average secrecy rate, Charnes-Cooper transformation, Alternating optimization

I. INTRODUCTION

RECENTLY, the openness of wireless communication provides high-speed data transmission for our daily lives, while it also brings the risk of information being eavesdropped. As a complement to conventional cryptographic techniques, physical layer security (PLS) technology, which exploits the channel differences between different users to guarantee secure communication, has attracted growing attention [1] [2]. Specifically, secure beamforming (SB) technique, which exploits multiple antennas to enhance the signal quality at the legitimate users, is a well-known approach. Moreover, with the application of 5G, massive multiple-input multiple-output

(MIMO) technology is proposed, which can provide more spatial degrees of freedom to improve secrecy capacity.

However, there exist some shortcomings for this technology, which may be utilized by malicious users. As we know, accurate channel state information (CSI) is an essential prerequisite in designing SB vectors. Different from passive eavesdropper, which only wiretaps information, active eavesdropper can attack the channel training phase of legitimate links to improve wiretapping performance, which is a serious threat especially for time-division duplex (TDD) systems. In a TDD system, the process of obtaining downlink CSI is briefly described as follows: the legitimate receiver (LR) transmits pilot sequence to the legitimate transmitter (LT) during uplink training phase. Then, in order to reduce the interaction overhead, the probed uplink link is regarded as the downlink link by exploiting channel reciprocity in coherent time, and SB vector based on this CSI is designed and utilized to transmit confidential data to the LR. However, if the uplink training phase is attacked by an adversary through sending the same pilot sequence as the LR, the probed CSI obtained at the LT is a weighted combination of the legitimate link and the eavesdropping link. With this false CSI, the beam designed by the LT will be oriented towards both the LR and the eavesdropper, which leads to severe information leakage. In [3], the authors first propose this active eavesdropping method and name it as pilot spoofing attack (PSA). Then its severe consequences are analyzed. In [4], a PSA approach carried out by multiple eavesdroppers cooperatively with the goal of maximizing the wiretapping signal-to-noise ratio is investigated. The authors extend PSA in a multi-user massive MIMO system and simulation results show that the network throughput can be degraded by more than 50% [5]. Being aware of this attack, some works follow with interest the PSA and propose some detection methods. In [6], the random training sequence is added to the normal training sequence. And by comparing the probed CSI difference in two training phases, the PSA can be detected effectively. Moreover, in [7], a complex attack model where Eve superimposes its random sequence on the training is discussed and a detection algorithm based on higher-order statistics of the data is proposed. It is worth noting that these detection methods work rely on a key assumption: the received combination pilot signal contains the channel characteristics of eavesdroppers, which LT can use some methods to distinguish. And if there exists an attack method where no signal is actively transmitted, the above detection methods may become disabled.

Meanwhile, Intelligent reflecting surface (IRS), which can flexibly manipulate electromagnetic waves, has been viewed

Copyright (c) 2015 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

This work was supported in part by the National Natural Science Foundation of China under Grant 61871404 and Grant 61701538, in part by National Natural Science Foundation Innovative Groups Project of China under Grant 61521003, and in part by key universities and academic disciplines construction project. (Corresponding author: Xinsheng Ji)

J. Yang, X. Ji, F. Wang, K. Huang are with Information Engineering University, Zhengzhou, 450002, China. (e-mails: yj_csu@126.com, jxs_ndsc@126.com, fhw_wang@sina.com, huangkaizhi@tsinghua.org.cn)

L. Guo is with Central South University, Changsha 410075, China. (e-mail: guolincsu@csu.edu.cn)

as an appealing technology for 6G network [8]. IRS is a planar array consisting of massive number of low-cost passive elements and each element can tune the reflection coefficient on the incident signal independently whereby the reflected signal can be enhanced or weakened at target users. Besides, the state switching time at each element can be low to the order of microsecond (μs) [9], which is much smaller than the typical channel coherence time that is on the order of millisecond (ms), and thus IRS is well suited for time-varying channels. Therefore, IRS has been studied in many applications such as coverage extension [10], novel wireless transmitter [11], physical layer security [12], [13], and so on. However, few literatures consider reverse application, where IRS is utilized to facilitate eavesdropping.

Actually, due to the openness of the communication protocol, the control strategy of the IRS can be seamlessly embedded in the protocol and the IRS can be utilized to maliciously manipulate the wireless channel. Then the reciprocity of uplink and downlink channels can be destroyed, which may bring new threat to legal communication. Moreover, with massive low-cost passive reflecting elements, more design parameters brought by the IRS can be utilized to moderate link quality and the problem is usually intractable. In [14], Huang et al. consider the concept of IRS-aided pilot spoofing, while it does not point out how to maximize the wiretapping capability. Motivated by above, a novel adverse application of IRS based on statistical CSI is investigated for enhancing eavesdropping performance. The control protocol of the IRS is designed to make LT misestimate the channel during the uplink phase and the eavesdropper overhear signal more clearly during the downlink phase. Consequently, this active attack can lead to more information leakage without leaving any energy footprint. Our main contributions are summarized as follows:

- 1) A novel pilot attack scheme in a three-node model with the aid of the IRS is proposed. In this model, the IRS is covertly deployed near the LT and remotely controlled by the eavesdropper. The phase shifts at the IRS are different during uplink phase and downlink phase, and thus the downlink CSI estimated by the LT is different from the actual downlink CSI. Then the designed SB vector will be shifted from LR. Furthermore, by carefully pre-designing the phase shifts, the eavesdropper can wiretap more information.
- 2) The average secrecy rate minimization problem based on statistical CSI is formulated and solved. Since instantaneous information is difficult to obtain for eavesdroppers, the average secrecy rate is considered as the performance metric and the optimization problem is established by jointly designing the phase shifts at the uplink and downlink phases. First, the approximate expression of the problem is derived, then non-convex problem is efficiently solved by exploiting alternating optimization algorithm and Charnes-Cooper transformation method. Moreover, the computational complexity is analyzed.
- 3) Numerical results show the impact of parameters, such as the transmit power, the transmit antennas and the Ri-

cian factor, on security performance. Compared with the existing pilot spoofing schemes, our proposed scheme can significantly degrade security performance. As the number of transmit antennas increases, security threat brought by IRS will not be weakened. If the eavesdropper is served by the same network and located close to LT, more serious threat will be brought. Moreover, when the number of low cost reflecting units increases, the security performance can be further cut down, which illustrates the advantages of the scheme.

The remainder of this paper is organized as follows. Section II proposes and analyzes the pilot spoofing attack scheme via IRS. Section III establishes the optimization problem and presents the solution methodology. Section IV provides the simulation results. Section V gives conclusions and future work.

II. PROPOSAL AND ANALYSIS OF THE SCHEME

A. The Proposal of the Scheme

Fig. 1: IRS-assisted pilot spoofing model

As depicted in Fig. 1, we consider a three-node point-to-point communication model, where the transmitter Alice intends to send confidential information to the receiver Bob under TDD mode, and the eavesdropper Eve tries to overhear

the downlink signal. Alice is equipped with M_a antennas, where $M_a > 1$, while Bob and Eve are equipped with single antenna, respectively. Meanwhile, one IRS is deployed near Alice and is controlled remotely by Eve through a private wireless channel¹. The IRS is composed of N reflecting units and $\Phi = \text{diag}(e^{j\theta_1}, e^{j\theta_2}, \dots, e^{j\theta_N})$ denotes the reflection phase shift matrix at the IRS, where $\theta_n \in [0, 2\pi]$ denotes the phase shift on the incident signal at its n th element². Suppose that there exist some low-power sensors integrated into the IRS and the reflected CSI can be probed by these sensors [15] [16]. Different from [3], where Eve sends jamming pilot sequence during the uplink pilot phase to induce Alice to obtain the false uplink CSI, in this model, Eve controls the IRS remotely to change its phase shifts several times in coherent time to conduct pilot spoofing attack. The specific implementation process is shown in Fig. 2.

Fig. 2: Flow chart of pilot spoofing via IRS

1) Silent stage

Alice and Bob communicate normally, while Eve keeps silent and tries to establish synchronization with legitimate users by utilizing their location information and the signal exchange between Alice and Bob³.

2) Pilot spoofing stage

① Before Bob sends the uplink pilot, Eve turns on the IRS and sets the uplink phase shifts. Then during the uplink pilot slot, Alice estimates the uplink CSI by receiving the pilot sequence from Bob. As shown in Fig. 1 (a), the estimated CSI contains the direct path Bob-Alice and the reflection path Bob-IRS-Alice. Furthermore, with the channel reciprocity, Alice regards the uplink probed CSI as the downlink CSI, and designs the downlink SB vector.

② During the uplink data slot, Bob transmits uplink data to Alice. Alice performs channel equalization and information

decoding. At this time, the phase shifts at the IRS are maintained.

③ Before Alice transmits downlink data, Eve sets the downlink phase shifts.

3) Eavesdropping stage

During the downlink slot, Alice conducts secure beamforming to send confidential data as shown in Fig. 1(b), while Eve tries to overhear data.

As can be seen from the above process, if the phase shifts are set differently during the uplink phase and downlink phase, the channel reciprocity disappears. Then the uplink CSI probed by Alice is no longer consistent with the actual downlink CSI. Since the SB vector is designed based on the uplink CSI, the downlink beam cannot be aligned with Bob, resulting in information leakage. At the same time, by carefully designing the phase shifts at different stage, the beam can be towarded to Eve, and thus more information is leaked to Eve.

It should be noted that although pilot spoofing performs during the uplink stage, the uplink receiving beam is still aligned with Bob. This is because that the estimated uplink CSI is the actual uplink CSI. Therefore, the security threat for the uplink transmission is relatively small. And in order to better illustrate the advantage of the proposed scheme on downlink eavesdropping, uplink eavesdropping is not discussed here.

B. The Analysis of the Scheme

Physical layer secure transmission technology provides information-theoretic security by using the wireless channel differences, while the proposed scheme utilizes the agility features of IRS to reconfigure the wireless environment to combat physical layer security technique. Compared with the existing pilot spoofing methods, our scheme has the following advantages:

1) It is easy to imagine finding a similar way to replace IRS to change the wireless environment, such as deploying controllable mirrors or moving small objects. These methods seem theoretically feasible. But there exist two problems. Firstly, precise timing control is difficult to realize, especially for high speed transmission. To achieve synchronization, a complex mechanical control structure is required, while for the IRS, only a micro-controller is needed. Secondly, the IRS can tune the phase of the incident signal and by designing the optimal reflection coefficients, the difference between uplink and downlink channel can be maximized. However, the channels reconstructed by other objects are uncontrollable. There is no guarantee that the transmit beam is deflected towards the eavesdropper, and it may even lead to worse signal quality for the eavesdropper.

2) For the traditional pilot spoofing methods, the pilot sequence needs to be known in advance. If legitimate users construct private pilot sequence, these methods will fail or even be detected. While, for our proposed scheme, since the signal from legitimate users is always passively reflected, pilot spoofing can be performed even if the pilot sequence is unknown, which makes existing detection methods invalid.

3) Extra energy is required for sending pilot sequence, which is not conducive to the concealment of eavesdropping.

¹With the feature of low profile and conformal geometry [9], the IRS is difficult to be detected by Alice.

²Considering the complexity of hardware design, the IRS reflection amplitude reflection factor is set to 1.

³Since the protocol of the communication system is publicly known, the frame format, transmission frequency and etc. can be obtained in advance. The details on how accurate synchronization is achievable are beyond the scope of this work [3].

While, due to the passive nature of the IRS, few energy is consumed except for its own state switching, which further increases the detection difficulty.

Therefore, our scheme provides new opportunities for implementing effective pilot spoofing. Moreover, it is worth studying how to maximize eavesdropping capability under this scheme, which will be discussed in the following section.

III. PROBLEM FORMULATION AND SOLVED

A. Problem Formulation

In this section, we consider exploiting the IRS to construct the difference between the uplink and downlink channels, which is beneficial to the eavesdropper. The three node signal model with IRS is firstly analyzed. The channels are expressed as follows: the channel from Alice to Bob consists of a direct channel and a reflection channel, where the direct channel is denoted by $\mathbf{h}_{ab}^H \in \mathbb{C}^{1 \times M_a}$, and the reflection channel consists of two parts, the channel from Alice to IRS is denoted by $\mathbf{H}_{ar}^H \in \mathbb{C}^{N \times M}$, the channel from IRS to Bob is denoted by $\mathbf{h}_{rb}^H \in \mathbb{C}^{1 \times N}$. Similarly, the channel from Alice to Eve consists of the reflection channel and the direct channel, where the direct channel is denoted by $\mathbf{h}_{ae}^H \in \mathbb{C}^{1 \times M_a}$, and the reflection channel is also composed of two parts, the channel from Alice to IRS $\mathbf{H}_{ar}^H$, the channel from IRS to Eve $\mathbf{h}_{re}^H \in \mathbb{C}^{1 \times N}$.

In the uplink phase, Eve turns on the IRS and sets the phase shifts as Φ_1 , then the uplink CSI estimated by Alice is expressed as

$$\mathbf{h}_{abu}^H = \mathbf{h}_{ab}^H + \mathbf{h}_{rb}^H \Phi_1 \mathbf{H}_{ar} \quad (1)$$

With the probed CSI $\mathbf{h}_{abu}^H$, the downlink transmit SB vector is designed based on the maximum-ratio transmission (MRT) criterion⁴ and is given by

$$\mathbf{w} = \sqrt{P_t} \frac{\mathbf{h}_{abu}}{\|\mathbf{h}_{abu}\|} = \sqrt{P_t} \frac{(\mathbf{h}_{ab}^H + \mathbf{h}_{rb}^H \Phi_1 \mathbf{H}_{ar})^H}{\|\mathbf{h}_{ab}^H + \mathbf{h}_{rb}^H \Phi_1 \mathbf{H}_{ar}\|} \quad (2)$$

where P_t denotes the transmit power at Alice.

In the downlink phase, Eve sets the phase shifts as Φ_2 , then the received signal at Bob is expressed as:

$$y_b = (\mathbf{h}_{ab}^H + \mathbf{h}_{rb}^H \Phi_2 \mathbf{H}_{ar}) \mathbf{w} s + n_b \quad (3)$$

where $n_b \sim \mathcal{CN}(0, \sigma_n^2)$ is the additive Gaussian white noise (AWGN) at Bob. And the actual downlink CSI is given by

$$\mathbf{h}_{abd}^H = \mathbf{h}_{ab}^H + \mathbf{h}_{rb}^H \Phi_2 \mathbf{H}_{ar} \quad (4)$$

Then the signal-to-interference-plus noise ratio (SINR) at Bob can be derived as

$$\text{SINR}_b = \frac{P_t |(\mathbf{h}_{ab}^H + \mathbf{h}_{rb}^H \Phi_2 \mathbf{H}_{ar})(\mathbf{h}_{ab} + \mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb})|^2}{\sigma_n^2 \|\mathbf{h}_{ab} + \mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb}\|_2^2} \quad (5)$$

From (3)-(5), we can see that due to the inconsistency between Φ_1 and Φ_2 , the downlink CSI perceived by Alice is misled and the SINR obtained by Bob is not the optimal.

⁴From the perspective of Alice, in the case of not knowing the existence of the eavesdropper, MRT-based secure beamforming is the optimal criterion [17]. Thus it can be regarded as a priori information for Eve.

Further, the received signal at Eve is expressed as

$$y_e = (\mathbf{h}_{ae}^H + \mathbf{h}_{re}^H \Phi_2 \mathbf{H}_{ar}) \mathbf{w} s + n_e \quad (6)$$

where $n_e \sim \mathcal{CN}(0, \sigma_n^2)$ denotes the AWGN at Eve.

The corresponding SINR at Eve is derived as:

$$\text{SINR}_e = \frac{P_t |(\mathbf{h}_{ae}^H + \mathbf{h}_{re}^H \Phi_2 \mathbf{H}_{ar})(\mathbf{h}_{ab} + \mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb})|^2}{\sigma_n^2 \|\mathbf{h}_{ab} + \mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb}\|_2^2} \quad (7)$$

Then the downlink secrecy rate is written as

$$R_d = [R_b - R_e]^+ = [\log_2(1 + \text{SINR}_b) - \log_2(1 + \text{SINR}_e)]^+ \quad (8)$$

where the notation $[x]^+ = \max\{x, 0\}$ is used.

Therefore, in order to overhear more downlink information, our goal is to minimize the downlink secrecy rate by carefully designing Φ_1 and Φ_2 ⁵. Hence, the optimization problem can be established as

$$\min_{\Phi_1, \Phi_2} R_d \quad (9a)$$

$$\text{s.t. } |\Phi_{1,(i,j)}| = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases} \quad (9b)$$

$$|\Phi_{2,(i,j)}| = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases} \quad (9c)$$

However, directly designing the reflection coefficient matrix based on instantaneous CSI in problem (9) seems impractical. One reason is that during the uplink phase, channel estimation has not conducted, and Eve cannot perceive instantaneous CSI in advance, thus the reflection coefficient matrixs Φ_1 and Φ_2 cannot be designed. The other reason is that Eve eavesdrops on the communication channel passively, and it is relatively difficult to obtain the CSI of each channel, especially for the channel from Alice to Bob. The methods to obtain the global instantaneous CSI are depicted in [18] [19], which need excessive communication overhead. Note that statistical CSI mainly depends on users' location information, which can be obtained with out-of-band side-information [20]. After long-term observation, it is reasonable that statistical CSI of each channel can be obtained by Eve. Hence, average secrecy rate as a performance metric is considered and the original optimization problem can be transformed to minimize average secrecy rate. Since Eve does not cooperate with Alice, the transmit power P_t is difficult to obtain. However, in order to meet the quality-of-service requirements, the SINR at terminals usually lies in high region, and problem (9) can be asymptotically expressed as

$$\begin{aligned} & \min_{\Phi_1, \Phi_2} \mathbb{E}(R_b - R_e) \\ & = \mathbb{E}(\log_2(1 + \text{SINR}_b) - \log_2(1 + \text{SINR}_e)) \end{aligned} \quad (10a)$$

$$\stackrel{(a)}{\simeq} \mathbb{E} \left\{ \log_2 \left(\frac{f_1(\Phi_1, \Phi_2)}{g_1(\Phi_1, \Phi_2)} \right) \right\}$$

$$f_1(\Phi_1, \Phi_2) = |(\mathbf{h}_{ab}^H + \mathbf{h}_{rb}^H \Phi_2 \mathbf{H}_{ar})(\mathbf{h}_{ab} + \mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb})|^2 \quad (10b)$$

$$g_1(\Phi_1, \Phi_2) = |(\mathbf{h}_{ae}^H + \mathbf{h}_{re}^H \Phi_2 \mathbf{H}_{ar})(\mathbf{h}_{ab} + \mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb})|^2 \quad (10c)$$

⁵In fact, Φ_1 can affect both the uplink and downlink eavesdropping. It is difficult to minimize the uplink and downlink secrecy rate simultaneously. However, we can establish the joint optimization problem by setting a weighting factor, which is left for future study.

where the approximation in equal (a) is a standard assumption [21], [22].

Note that with statistical CSI, the uplink and downlink phase shifts can be computed in advance, and set at the corresponding stage. And when the statistical characteristics of channels change, the phase shifts need to be updated. In this way, the required channel estimation overhead for Eve is relatively low.

Further, it is hard to obtain closed-form solution for problem (10). Fortunately, according to the theorem in [23], an approximate expression can be obtained

$$\begin{aligned} & \min_{\Phi_1, \Phi_2} \mathbb{E} \left\{ \log_2 \left(\frac{f_1(\Phi_1, \Phi_2)}{g_1(\Phi_1, \Phi_2)} \right) \right\} \\ & \approx \min_{\Phi_1, \Phi_2} \left\{ \log_2 \frac{\mathbb{E}(f_1(\Phi_1, \Phi_2))}{\mathbb{E}(g_1(\Phi_1, \Phi_2))} \right\} \end{aligned} \quad (11)$$

In this paper, a typical quasi-static Rician fading environment is considered [24]. The channel between node i to node j is modeled as $h_{ij} = \sqrt{L_0 d_{ij}^{-c_{ij}}} g_{ij}$, where L_0 denotes the path loss at the reference distance $d_0 = 1\text{m}$, d_{ij} denotes the distance from i to j , and c_{ij} denotes the corresponding path loss exponent. Besides, the small-scale fading component g_{ij} is given by

$$g_{ij} = \sqrt{\frac{\beta_{ij}}{1 + \beta_{ij}}} g_{ij}^{\text{LoS}} + \sqrt{\frac{1}{1 + \beta_{ij}}} g_{ij}^{\text{NLoS}} \quad (12)$$

where β_{ij} denotes the Rician factor, g_{ij}^{LoS} and g_{ij}^{NLoS} represent the line-of-sight (LoS) and non-LoS (NLoS) components, respectively.

Therefore, the direct channel from Alice to Eve is re-expressed as

$$\mathbf{h}_{ae} = \tilde{\mathbf{h}}_{ae} + \bar{\mathbf{h}}_{ae} \quad (13)$$

where $\bar{\mathbf{h}}_{ae}$ denotes the LoS component, $\tilde{\mathbf{h}}_{ae}$ denotes the NLoS component with zero-mean complex Gaussian random variables with variance $\sigma_{ae}^2 = \frac{L_0 d_{ae}^{-c_{ae}}}{1 + \beta_{ae}}$ [25].

Similarly, the corresponding LoS and NLoS components of other channels can be obtained. Note that since the IRS is deployed vertically high [26] and is located near Alice, less scattering environment from Alice to IRS is expected, namely $\mathbf{H}_{ar} = \bar{\mathbf{H}}_{ar} + \tilde{\mathbf{H}}_{ar} \approx \bar{\mathbf{H}}_{ar}$. Then (10b) and (10c) can be rewritten as (14) and (15).

Theorem 1. *With the natures of Gaussian distribution, the expected operation can be removed and the original problem is given by*

$$\begin{aligned} & \min_{\Phi_1, \Phi_2} \log_2 \left(\frac{\mathbb{E}(f_1(\Phi_1, \Phi_2))}{\mathbb{E}(g_1(\Phi_1, \Phi_2))} \right) \\ & = \min_{\Phi_1, \Phi_2} \log_2 \left(\frac{f_2(\Phi_1, \Phi_2)}{g_2(\Phi_1, \Phi_2)} \right) \end{aligned} \quad (16a)$$

$$\begin{aligned} f_2(\Phi_1, \Phi_2) = & |(\bar{\mathbf{h}}_{ab}^H + \bar{\mathbf{h}}_{rb}^H \Phi_2 \bar{\mathbf{H}}_{ar})(\bar{\mathbf{h}}_{ab} + \bar{\mathbf{H}}_{ar}^H \Phi_1 \bar{\mathbf{h}}_{rb})|^2 \\ & + \sigma_{ab}^2 |(\bar{\mathbf{h}}_{rb}^H \Phi_1 \bar{\mathbf{H}}_{ar} + \bar{\mathbf{h}}_{ab}^H)|^2 + \sigma_{ab}^2 |(\bar{\mathbf{h}}_{rb}^H \Phi_2 \bar{\mathbf{H}}_{ar} + \bar{\mathbf{h}}_{ab}^H)|^2 \\ & + \sigma_{rb}^2 |(\bar{\mathbf{h}}_{rb}^H \Phi_2 \bar{\mathbf{H}}_{ar} + \bar{\mathbf{h}}_{ab}^H) \bar{\mathbf{H}}_{ar}^H|^2 \\ & + \sigma_{rb}^2 |(\bar{\mathbf{h}}_{rb}^H \Phi_1 \bar{\mathbf{H}}_{ar} + \bar{\mathbf{h}}_{ab}^H) \bar{\mathbf{H}}_{ar}^H|^2 + C_1 \end{aligned} \quad (16b)$$

$$\begin{aligned} C_1 = & M_a \sigma_{ab}^4 + 2 \sigma_{ab}^2 \sigma_{rb}^2 \text{Tr}(\bar{\mathbf{H}}_{ar} \bar{\mathbf{H}}_{ar}^H) \\ & + \sigma_{rb}^4 \text{Tr}(\bar{\mathbf{H}}_{ar} \bar{\mathbf{H}}_{ar}^H \bar{\mathbf{H}}_{ar} \bar{\mathbf{H}}_{ar}^H) \end{aligned} \quad (16c)$$

$$\begin{aligned} g_2(\Phi_1, \Phi_2) = & |(\bar{\mathbf{h}}_{ae}^H + \bar{\mathbf{h}}_{re}^H \Phi_2 \bar{\mathbf{H}}_{ar})(\bar{\mathbf{h}}_{ab} + \bar{\mathbf{H}}_{ar}^H \Phi_1 \bar{\mathbf{h}}_{rb})|^2 \\ & + \sigma_{ae}^2 |(\bar{\mathbf{h}}_{rb}^H \Phi_1 \bar{\mathbf{H}}_{ar} + \bar{\mathbf{h}}_{ab}^H)|^2 + \sigma_{ab}^2 |(\bar{\mathbf{h}}_{re}^H \Phi_2 \bar{\mathbf{H}}_{ar} + \bar{\mathbf{h}}_{ab}^H)|^2 \\ & + \sigma_{rb}^2 |(\bar{\mathbf{h}}_{re}^H \Phi_2 \bar{\mathbf{H}}_{ar} + \bar{\mathbf{h}}_{ab}^H) \bar{\mathbf{H}}_{ar}^H|^2 \\ & + \sigma_{re}^2 |(\bar{\mathbf{h}}_{rb}^H \Phi_1 \bar{\mathbf{H}}_{ar} + \bar{\mathbf{h}}_{ab}^H) \bar{\mathbf{H}}_{ar}^H|^2 + C_2 \end{aligned} \quad (16d)$$

$$\begin{aligned} C_2 = & M_a \sigma_{ae}^2 \sigma_{ab}^2 + \sigma_{ae}^2 \sigma_{rb}^2 \text{Tr}(\bar{\mathbf{H}}_{ar} \bar{\mathbf{H}}_{ar}^H) \\ & + \sigma_{ab}^2 \sigma_{re}^2 \text{Tr}(\bar{\mathbf{H}}_{ar} \bar{\mathbf{H}}_{ar}^H) + \sigma_{re}^2 \sigma_{rb}^2 \text{Tr}(\bar{\mathbf{H}}_{ar} \bar{\mathbf{H}}_{ar}^H \bar{\mathbf{H}}_{ar} \bar{\mathbf{H}}_{ar}^H) \end{aligned} \quad (16e)$$

Proof: See Appendix A.

Then let $\mathbf{v}_1 = [v_{1,1}, v_{1,2}, \dots, v_{1,N}]^H$, $\mathbf{v}_2 = [v_{2,1}, v_{2,2}, \dots, v_{2,N}]^H$, where $v_{1,n} = \Phi_{1,(n,n)}$, $v_{2,n} = \Phi_{2,(n,n)}$, $\forall n$. Then we denote $\tilde{\mathbf{v}}_1^H = e^{j\bar{w}_1} [\mathbf{v}_1^H, 1]$, $\tilde{\mathbf{v}}_2^H = e^{j\bar{w}_2} [\mathbf{v}_2^H, 1]$, where $\bar{w}_1, \bar{w}_2 \in [0, 2\pi]$ are the introduced slack variables without any effect on the optimal solution. By denoting $\bar{\mathbf{H}}_{arb} = \text{diag}(\bar{\mathbf{h}}_{rb}^H) \bar{\mathbf{H}}_{ar}$ and $\bar{\mathbf{H}}_{are} = \text{diag}(\bar{\mathbf{h}}_{re}^H) \bar{\mathbf{H}}_{ar}$, we have $\bar{\mathbf{h}}_{rb}^H \Phi_1 \bar{\mathbf{H}}_{ar} = \mathbf{v}_1^H \bar{\mathbf{H}}_{arb}$, $\bar{\mathbf{h}}_{rb}^H \Phi_2 \bar{\mathbf{H}}_{ar} = \mathbf{v}_2^H \bar{\mathbf{H}}_{arb}$. Then (16b) and (16d) can be rewritten as:

$$\begin{aligned} f_2(\tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2) = & |\tilde{\mathbf{v}}_2^H \bar{\mathbf{H}}_{ab} \bar{\mathbf{H}}_{ab}^H \tilde{\mathbf{v}}_1|^2 + \sigma_{ab}^2 |\tilde{\mathbf{v}}_1^H \bar{\mathbf{H}}_{ab}^H|^2 \\ & + \sigma_{ab}^2 |\tilde{\mathbf{v}}_2^H \bar{\mathbf{H}}_{ab}^H|^2 + \sigma_{rb}^2 |\tilde{\mathbf{v}}_2^H \bar{\mathbf{H}}_{ab} \bar{\mathbf{H}}_{ar}^H|^2 \\ & + \sigma_{rb}^2 |\tilde{\mathbf{v}}_1^H \bar{\mathbf{H}}_{ab} \bar{\mathbf{H}}_{ar}^H|^2 + C_1 \end{aligned} \quad (17a)$$

$$\begin{aligned} g_2(\tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2) = & |\tilde{\mathbf{v}}_2^H \bar{\mathbf{H}}_{ae} \bar{\mathbf{H}}_{ab}^H \tilde{\mathbf{v}}_1|^2 + \sigma_{ae}^2 |\tilde{\mathbf{v}}_1^H \bar{\mathbf{H}}_{ab}^H|^2 \\ & + \sigma_{ab}^2 |\tilde{\mathbf{v}}_2^H \bar{\mathbf{H}}_{ae}^H|^2 + \sigma_{rb}^2 |\tilde{\mathbf{v}}_2^H \bar{\mathbf{H}}_{ae} \bar{\mathbf{H}}_{ar}^H|^2 \\ & + \sigma_{re}^2 |\tilde{\mathbf{v}}_1^H \bar{\mathbf{H}}_{ab} \bar{\mathbf{H}}_{ar}^H|^2 + C_2 \end{aligned} \quad (17b)$$

where $\bar{\mathbf{H}}_{ab} = \begin{bmatrix} \bar{\mathbf{H}}_{arb} \\ \bar{\mathbf{h}}_{ab}^H \end{bmatrix}$, $\bar{\mathbf{H}}_{ae} = \begin{bmatrix} \bar{\mathbf{H}}_{are} \\ \bar{\mathbf{h}}_{ae}^H \end{bmatrix}$.

Further, with the monotonicity of logarithmic function, the original problem can be rewritten as

$$\min_{\tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2} \frac{f_2(\tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2)}{g_2(\tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2)} \quad (18a)$$

$$s.t. (9b), (9c), (16c), (16e), (17a), (17b) \quad (18b)$$

It is worth noting that due to the non-concave fractional constraints as well as the coupling variables and unit-modulus constraints, problem (18) is non-convex and intractable. In the following section, an efficient algorithm is developed to find a near optimal solution.

B. Optimal Phase Shifts Design

In this section, firstly, alternating optimization is utilized to separate the original problem into two sub-problems. Then, the Charnes-Cooper transformation [19] and SDR techniques are utilized to solve each sub-problem respectively.

1) *Optimizing $\tilde{\mathbf{v}}_1$ for given $\tilde{\mathbf{v}}_2$:* Let $\hat{\mathbf{V}}_1 = \tilde{\mathbf{v}}_1 \tilde{\mathbf{v}}_1^H$, $\hat{\mathbf{V}}_2 = \tilde{\mathbf{v}}_2 \tilde{\mathbf{v}}_2^H$, then we have $\text{Rank}(\hat{\mathbf{V}}_1) = 1$, $\text{Rank}(\hat{\mathbf{V}}_2) = 1$. With the nature of matrix trace, problem (18) can be rewritten with $\hat{\mathbf{V}}_1$ and $\hat{\mathbf{V}}_2$, which is omitted for brief.

Since the objective function (18a) is non-convex, Charnes-Cooper transformation is utilized to transform the fractional operation. First, we introduce an auxiliary variable $s_1 > 0$, which satisfies $s_1 \times g_2(\tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2) = 1$, and define a new matrix $\hat{\mathbf{E}}_1 = s_1 \hat{\mathbf{V}}_1$. Then new functions $g_3(\hat{\mathbf{E}}_1, \hat{\mathbf{V}}_2)$ and $f_3(\hat{\mathbf{E}}_1, \hat{\mathbf{V}}_2)$ can be constructed as

$$f_1(\Phi_1, \Phi_2) = \left| ((\bar{\mathbf{h}}_{ab}^H + \tilde{\mathbf{h}}_{ab}^H) + (\bar{\mathbf{h}}_{rb}^H + \tilde{\mathbf{h}}_{rb}^H)\Phi_2\bar{\mathbf{H}}_{ar}))((\bar{\mathbf{h}}_{ab} + \tilde{\mathbf{h}}_{ab}) + \bar{\mathbf{H}}_{ar}^H\Phi_1^H(\bar{\mathbf{h}}_{rb} + \tilde{\mathbf{h}}_{rb})) \right|^2 \quad (14)$$

$$g_1(\Phi_1, \Phi_2) = \left| ((\bar{\mathbf{h}}_{ae}^H + \tilde{\mathbf{h}}_{ae}^H) + (\bar{\mathbf{h}}_{re}^H + \tilde{\mathbf{h}}_{re}^H)\Phi_2\bar{\mathbf{H}}_{ar}))((\bar{\mathbf{h}}_{ab} + \tilde{\mathbf{h}}_{ab}) + \bar{\mathbf{H}}_{ar}^H\Phi_1^H(\bar{\mathbf{h}}_{rb} + \tilde{\mathbf{h}}_{rb})) \right|^2 \quad (15)$$

$$\begin{aligned} g_3(\hat{\mathbf{E}}_1, \hat{\mathbf{V}}_2) &= s_1 \times g_2(\tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2) \\ &= \sigma_{ab}^2 \text{Tr}(\hat{\mathbf{V}}_2 \bar{\mathbf{H}}_{ae} \bar{\mathbf{H}}_{ae}^H) + \sigma_{ae}^2 \text{Tr}(\hat{\mathbf{E}}_1 \bar{\mathbf{H}}_{ab} \bar{\mathbf{H}}_{ab}^H) \\ &+ \text{Tr}(\hat{\mathbf{V}}_2 \bar{\mathbf{H}}_{ae} \bar{\mathbf{H}}_{ab}^H \hat{\mathbf{E}}_1 \bar{\mathbf{H}}_{ab} \bar{\mathbf{H}}_{ae}^H) + \sigma_{rb}^2 \text{Tr}(\hat{\mathbf{V}}_2 \bar{\mathbf{H}}_{ae} \bar{\mathbf{H}}_{ar}^H \bar{\mathbf{H}}_{ar} \bar{\mathbf{H}}_{ae}^H) \\ &+ \sigma_{re}^2 \text{Tr}(\hat{\mathbf{E}}_1 \bar{\mathbf{H}}_{ab} \bar{\mathbf{H}}_{ar}^H \bar{\mathbf{H}}_{ar} \bar{\mathbf{H}}_{ab}^H) + s_1 C_2 \end{aligned} \quad (19)$$

$$\begin{aligned} f_3(\hat{\mathbf{E}}_1, \hat{\mathbf{V}}_2) &= s_1 \times f_2(\tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2) \\ &= \sigma_{ab}^2 \text{Tr}(\hat{\mathbf{V}}_2 \bar{\mathbf{H}}_{ab} \bar{\mathbf{H}}_{ab}^H) + \sigma_{ab}^2 \text{Tr}(\hat{\mathbf{E}}_1 \bar{\mathbf{H}}_{ab} \bar{\mathbf{H}}_{ab}^H) \\ &+ \text{Tr}(\hat{\mathbf{V}}_2 \bar{\mathbf{H}}_{ab} \bar{\mathbf{H}}_{ab}^H \hat{\mathbf{E}}_1 \bar{\mathbf{H}}_{ab} \bar{\mathbf{H}}_{ab}^H) + \sigma_{rb}^2 \text{Tr}(\hat{\mathbf{V}}_2 \bar{\mathbf{H}}_{ab} \bar{\mathbf{H}}_{ar}^H \bar{\mathbf{H}}_{ar} \bar{\mathbf{H}}_{ab}^H) \\ &+ \sigma_{rb}^2 \text{Tr}(\hat{\mathbf{E}}_1 \bar{\mathbf{H}}_{ab} \bar{\mathbf{H}}_{ar}^H \bar{\mathbf{H}}_{ar} \bar{\mathbf{H}}_{ab}^H) + s_1 C_1 \end{aligned} \quad (20)$$

Then problem (18) is equivalently transformed as:

$$\min_{\hat{\mathbf{E}}_1} f_3(\hat{\mathbf{E}}_1, \hat{\mathbf{V}}_2) \quad (21a)$$

$$s.t. \quad g_3(\hat{\mathbf{E}}_1, \hat{\mathbf{V}}_2) = 1 \quad (21b)$$

$$\hat{\mathbf{E}}_{1(n,n)} = s_1, \quad n = 1, 2, \dots, (N+1), \quad s_1 > 0 \quad (21c)$$

$$\text{Rank}(\hat{\mathbf{E}}_1) = 1 \quad (21d)$$

Note that problem (21) is non-convex due to constraint (21d). Then, the Rank-1 constraint is firstly discarded and problem (21) is transformed to a convex semidefinite programming problem with linear constraints and can be efficiently solved via the CVX solver. Since the constraint of Rank-1 is relaxed in problem (21), it is necessary to verify whether the obtained solution satisfies Rank-1. If the obtained solution is not Rank-1, gaussian randomization is applied for recovering vector approximately [12]. Moreover, numerical results show that the optimal $\hat{\mathbf{E}}_1$ always satisfies Rank-1, which illustrates that the rank relaxation is tight.

2) *Optimizing $\tilde{\mathbf{v}}_2$ for given $\tilde{\mathbf{v}}_1$* : Similarly, auxiliary variable $s_2 > 0$ is introduced. And new matrix $\hat{\mathbf{E}}_2 = s_2 \hat{\mathbf{V}}_2$ is defined. Then new functions $g_4(\hat{\mathbf{V}}_1, \hat{\mathbf{E}}_2)$, $f_4(\hat{\mathbf{V}}_1, \hat{\mathbf{E}}_2)$ are defined as follows

$$g_4(\hat{\mathbf{V}}_1, \hat{\mathbf{E}}_2) = s_2 \times g_2(\tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2) \quad (22)$$

$$f_4(\hat{\mathbf{V}}_1, \hat{\mathbf{E}}_2) = s_2 \times f_2(\tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2) \quad (23)$$

Next the original problem is equivalently given by:

$$\min_{\hat{\mathbf{E}}_2} f_4(\hat{\mathbf{V}}_1, \hat{\mathbf{E}}_2) \quad (24a)$$

$$s.t. \quad g_4(\hat{\mathbf{V}}_1, \hat{\mathbf{E}}_2) = 1 \quad (24b)$$

$$\hat{\mathbf{E}}_{2(n,n)} = s_2, \quad n = 1, 2, \dots, (N+1), \quad s_2 > 0 \quad (24c)$$

$$\text{Rank}(\hat{\mathbf{E}}_2) = 1 \quad (24d)$$

Similarly, by dropping Rank-1 constraint (24d), problem (24) can be efficiently solved via the CVX solver. And then Gaussian randomization method is utilized to recover $\tilde{\mathbf{v}}_2$.

3) *Overall Algorithm*: To summarize, the outline of solving problem (18) is given in Algorithm 1, where L denotes the maximum iteration number.

Algorithm 1 proposed algorithm for solving problem (18)

1. Initialize the phase shifts of the IRS as $\tilde{\mathbf{v}}_1^{*(0)} = e^{j\bar{w}_1} \begin{bmatrix} \mathbf{v}_1^{(0)} \\ 1 \end{bmatrix}$, $\tilde{\mathbf{v}}_2^{*(0)} = e^{j\bar{w}_2} \begin{bmatrix} \mathbf{v}_2^{(0)} \\ 1 \end{bmatrix}$ with random values $\bar{w}_1, \bar{w}_2 \in [0, 2\pi]$, and set $l = 1$;
2. Repeat
3. Solve (21) for given $\tilde{\mathbf{v}}_2^{(l-1)}$, and obtain the solution as $\tilde{\mathbf{v}}_1^{(l)}$.
4. Solve (24) for given $\tilde{\mathbf{v}}_1^{(l)}$, and obtain the solution as $\tilde{\mathbf{v}}_2^{(l)}$.
5. Update $l = l + 1$.
6. Until the fractional decrease of the objective value is below the error ε or the iteration number meets $l = L$.

Convergence Analysis: For the l th alternating iteration, denote $R(\tilde{\mathbf{v}}_1^{(l)}, \tilde{\mathbf{v}}_2^{(l)})$ as the value of objective function, where $(\tilde{\mathbf{v}}_1^{(l)}, \tilde{\mathbf{v}}_2^{(l)})$ is the feasible solution. Then for the $(l+1)$ th iteration, $(\tilde{\mathbf{v}}_1^{(l+1)}, \tilde{\mathbf{v}}_2^{(l)})$ is the feasible solution of problem (21), and $(\tilde{\mathbf{v}}_1^{(l+1)}, \tilde{\mathbf{v}}_2^{(l+1)})$ is the feasible solution of problem (24). Then, we have

$$R(\tilde{\mathbf{v}}_1^{(l)}, \tilde{\mathbf{v}}_2^{(l)}) \stackrel{(a)}{\geq} R(\tilde{\mathbf{v}}_1^{(l+1)}, \tilde{\mathbf{v}}_2^{(l)}) \stackrel{(b)}{\geq} R(\tilde{\mathbf{v}}_1^{(l+1)}, \tilde{\mathbf{v}}_2^{(l+1)}) \quad (25)$$

where inequality (a) holds due to the fact that problem (21) is solved optimally in step 3, equality (b) holds due to step 4. This indicates that the object value given in the $(l+1)$ th iteration is not larger than that in the l th iteration. That is to say, after each iteration, the object value is non-increasing. Furthermore, along with the QoS constraint, the secrecy rate is lower bounded and thus it must converge after some iterations.

Complexity Analysis: The complexity of Algorithm 1 mainly lies on the Step 3, 4. For Step 3, the complexity for solving (23) using the interior-point method, which is denoted as $\mathcal{O}_1$, is determined by the number and size of variables and constraints, which is summarized in Table I. Since (24) is similar to (21), the complexity of Step 4 is equal to that of Step 3. Therefore, the major complexity of Algorithm 1 is given by $2 \times I_{ao} \times \mathcal{O}_1$, where I_{ao} is the alternating number.

IV. NUMERICAL RESULTS

In this section, we present numerical results to validate the performance of the proposed scheme. Simulation setups are shown in Fig. 3, where Alice, Bob, IRS, Eve are located

TABLE I: Computational complexity analysis for the proposed algorithm

Algorithm	Variables		PSD constraints	Slack constraints
	design variables (size, number)	Slack variables (size, number)	(size, number)	(number)
Step3	$(N \times N, 1)$	$(1 \times 1, 1)$	$(N \times N, 1)$	$(N + 2)$

Fig. 3: Simulation Setup

at (0,0), (100,0), (0,3), (100,50) in meter (m), respectively. Considering that IRS is deployed vertically high [26], a less scattering environment is expected and thus we set $\beta_{ar} = \infty$, $c_{ar} = 2.5$, $c_{re} = c_{rb} = 3$, $\beta_{rb} = 10$, $\beta_{re} = 5$. The rest parameters are listed as follows: $c_{ae} = c_{ab} = 3$, $\beta_{ab} = 10$, $\sigma_n^2 = -80\text{dBm}$, $L_0 = -30\text{dB}$, $\varepsilon = 0.001$, and $L=15$. The following results are achieved by the average of simulating over 500 random channel realizations.

Fig. 4 shows the convergence behavior of our proposed algorithm under different number of reflecting elements N and transmit antennas M_a , respectively. With the increase of iteration number, the secrecy rate gradually decreases. After about 8 iterations, the object values all reach stable values, which validates the convergence analysis given in Section III.B.3.

Fig. 4: Convergence behavior versus the iteration number of alternating optimization ($\beta_{ae} = 5$)

In order to evaluate the advantage brought by the IRS, we compare our proposed scheme (Proposed IRS-PSA) with the following four benchmark schemes:

Scheme 1: Without IRS (No IRS). In this case, Eve passively wiretap information without the aid of the IRS.

Scheme 2: Jamming assisted pilot spoofing scheme (Jam-PSA). In this case, Eve sends the same pilot when Bob sends the uplink pilot to Alice as shown in [3], where the jamming pilot power is denoted by P_J .

Scheme 3: Passive IRS. In this case, compared to IRS-PSA scheme, the IRS is turned on during the downlink phase but turned off during the uplink phase. The downlink phase shifts are designed to minimize the average secrecy rate by solving problem (24) with $\tilde{\mathbf{v}}_1 = [0_{N \times 1}, 1]$.

Scheme 4: IRS-AL-PSA. As shown in [14], the beam of the IRS aligns with the channel Bob-IRS-Alice during the uplink phase, while aligns with the channel Alice-IRS-Eve during the downlink phase.

Fig. 5: The secrecy rate versus transmit power ($N = 60$, $M_a = 10$, $\beta_{ae} = 5$, $P_J = 0.15P_t$)

Fig. 5 shows the secrecy rate versus different transmit power by Alice. As the transmit power increases, the secrecy rates of five schemes all increase gradually. Meanwhile, under the same condition, the proposed scheme poses the most serious security threat. Compared to Scheme 4, the eavesdropping performance of the proposed scheme can be significantly enhanced with statistical CSI. Moreover, in order to achieve the same performance, the jamming power should be more than 0.15 times of the transmit power, while no extra energy is consumed with our proposed scheme. In addition, the performance of the scheme (Proposed IRS-PSA with P_t), where Eve can obtain P_t through some secret methods, is

given. We can see that the performance is close to that of our proposed algorithm, which verifies the approximation in formula (10).

The performance gains versus the number of transmit antennas M_a at Alice is plotted in Fig. 6. It can be seen that increasing M_a improves the system secrecy rate gradually. This is because with more transmit antennas, the beam can focus on legitimate users more accurately. However, as M_a increases, the security threats brought by pilot spoofing schemes still exist. It is worth noting that the secrecy rate difference between our proposed scheme and Scheme 1 under different N keeps nearly unchanged, and even further widens. This means that our proposed scheme poses a remarkable threat for massive MIMO system. Moreover, when M_a is small, the performance of our proposed scheme under $N = 60$ is better than that of Jam-PSA scheme, while when M_a increases to a certain extent, the contrary is the case. The reason is that for Jam-PSA scheme, the effect is adding a new channel on legitimate channel, but for IRS-aided scheme, the effect is tuning the phase of the original channel. Therefore, it is easy to know that the more the number of antennas, the greater the impact of the former scheme on security performance. When M_a is small, with larger N , the phase of the legitimate channel can be tuned in a wider range and IRS-aided scheme has a lower secrecy rate.

Fig. 6: The secrecy rate versus the number of transmit antennas at Alice ($P_t = 30\text{dBm}$, $P_J = 0.15P_t$, $\beta_{ae} = 5$)

In Fig. 7, we show the secrecy rate decrease ratio versus Rician factor β_{ae} . The secrecy rate decrease ratio is defined as $\Delta R = (R_1 - R_0)/R_0$, where R_0 denotes the secrecy rate of Scheme 1, R_1 denotes that of the proposed scheme or Scheme 3 under the same condition. It can be seen that as Rician factor β_{ae} increases, the secrecy rate decrease ratios ΔR of Scheme 3 and the proposed scheme both increase gradually. The reason lies in that as Rician factor β_{ae} increases, LoS component becomes dominant and statistical CSI is approximate to instantaneous CSI, and then Eve can wiretap more information. Therefore, if Eve is a malicious unscheduled user in the network [27] [28], which may be located close to BS,

there exists stronger LoS component and more damage to legitimate communication is brought by IRS. Moreover, if Eve is an outside user in the network, less damage is brought and deploying multiple IRSs and trying to obtain more precise CSI may be potential solutions.

Fig. 7: The secrecy decrease ratio versus the Rician factor β_{ae} ($P_t = 20\text{dBm}$, $N = 40$)

In Fig. 8, we further show the performance gains versus the number of reflecting elements N . It can be seen that as N increases, the secrecy rates of three IRS-aided schemes all decrease, and the proposed scheme decreases more quickly than the others. This is because IRS with larger elements can provide more adjustable dimension for inequality (18a). Moreover, from Fig. 8, we can see that deploying massive low-cost passive units can achieve the same performance as Jam-PSA scheme without energy consumption. It can be predicted that only by adjusting the phase shifts, the secrecy rate can approach zero. Furthermore, we also give the performance of IRS-aided secure transmission scheme (IRS-sec) [12]. Under the same condition, the security performance is significantly higher than that of the IRS-aided PSA schemes. Although the IRS is passive, when it is utilized for legitimate communication or information eavesdropping, the impact on security performance is obviously different and thus more attention should be paid to this novel attack.

V. CONCLUSION AND FUTURE WORK

In this paper, we have presented an investigation of IRS-assisted pilot spoofing scheme. Firstly, the control strategy of the IRS is proposed. By tuning the phase shifts during uplink phase and downlink phase, the reciprocity between uplink and downlink disappears and the downlink beam shifts, which leads to signal leakage. Then, the minimum average secrecy rate problem based on statistical CSI is established by properly designing the phase shifts. With alternating optimization algorithm and Charnes-Cooper transformation technique, a near optimal solution is proposed. Finally, simulation results show that our scheme can seriously degrade the downlink security performance for TDD systems without energy consumption. Therefore, it is worth paying attention to studying the effective countermeasures against this attack in future work.

$$\begin{aligned}
q_1 &= |\mathbf{h}_{ae}^H \mathbf{h}_{ab} + \mathbf{h}_{ae}^H \mathbf{B}^H \mathbf{h}_{rb} + \mathbf{h}_{re}^H \mathbf{A} \mathbf{h}_{ab} + \mathbf{h}_{re}^H \mathbf{A} \mathbf{B}^H \mathbf{h}_{rb}|^2 \\
&= \underbrace{\mathbf{h}_{ae}^H \mathbf{h}_{ab} \mathbf{h}_{ab}^H \mathbf{h}_{ae}}_{p_1} + \underbrace{\mathbf{h}_{ae}^H \mathbf{h}_{ab} \mathbf{h}_{rb}^H \mathbf{B} \mathbf{h}_{ae}}_{p_2} + \underbrace{\mathbf{h}_{ae}^H \mathbf{h}_{ab} \mathbf{h}_{ab}^H \mathbf{A}^H \mathbf{h}_{re}}_{p_3} \cdots + \underbrace{\mathbf{h}_{re}^H \mathbf{A} \mathbf{B}^H \mathbf{h}_{rb} \mathbf{h}_{ab}^H \mathbf{A}^H \mathbf{h}_{re}}_{p_{15}} + \underbrace{\mathbf{h}_{re}^H \mathbf{A} \mathbf{B}^H \mathbf{h}_{rb} \mathbf{h}_{rb}^H \mathbf{B}^H \mathbf{A} \mathbf{h}_{re}}_{p_{16}}
\end{aligned} \tag{27}$$

Fig. 8: The secrecy rate versus the number of reflecting elements ($P_t = 25\text{dBm}$, $M_a = 10$, $\beta_{ae} = 5$, $P_J = 0.1P_t$)

APPENDIX A PROOF OF PROPOSITION 1

In this appendix, the transformation of the expectation in (11) is proved here. Due to the similar form of the denominator $\mathbb{E}(g_1(\Phi_1, \Phi_2))$ and the numerator $\mathbb{E}(f_1(\Phi_1, \Phi_2))$, the denominator $\mathbb{E}(g_1(\Phi_1, \Phi_2))$ is firstly transformed.

$$\begin{aligned}
&\mathbb{E}(g_1(\Phi_1, \Phi_2)) \\
&= \mathbb{E}(|(\mathbf{h}_{ae}^H + \mathbf{h}_{re}^H \Phi_2 \bar{\mathbf{H}}_{ar})(\mathbf{h}_{ab} + \bar{\mathbf{H}}_{ar}^H \Phi_1^H \mathbf{h}_{rb})|^2) \tag{26}
\end{aligned}$$

Let $q_1 = |(\mathbf{h}_{ae}^H + \mathbf{h}_{re}^H \mathbf{A})(\mathbf{h}_{ab} + \mathbf{B}^H \mathbf{h}_{rb})|^2$, where $\mathbf{A} = \Phi_2 \bar{\mathbf{H}}_{ar}$, $\mathbf{B} = \Phi_1 \bar{\mathbf{H}}_{ar}$, then q_1 can be expanded as shown in (27).

Note that (27) is composed of 16 items, and we can transform each item one by one. In order to effectively illustrate the transformation process, we take the most complex item p_{16} as an example. Then each channel vector is expanded as the sum of the LoS component and NLoS component and p_{16} can be rewritten as

$$\begin{aligned}
&p_{16} \\
&= (\bar{\mathbf{h}}_{re}^H + \tilde{\mathbf{h}}_{re}^H) \mathbf{A} \mathbf{B}^H (\bar{\mathbf{h}}_{rb} + \tilde{\mathbf{h}}_{rb}) (\bar{\mathbf{h}}_{rb}^H + \tilde{\mathbf{h}}_{rb}^H) \mathbf{B} \mathbf{A}^H (\bar{\mathbf{h}}_{re} + \tilde{\mathbf{h}}_{re}) \\
&= \underbrace{(\bar{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{rb} \bar{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \bar{\mathbf{h}}_{re})}_{t_1} + \underbrace{(\bar{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \bar{\mathbf{h}}_{re})}_{t_2} \\
&+ \underbrace{(\bar{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \tilde{\mathbf{h}}_{rb} \bar{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \bar{\mathbf{h}}_{re})}_{t_3} + \underbrace{(\bar{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \tilde{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \bar{\mathbf{h}}_{re})}_{t_4} \\
&+ \underbrace{(\tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{rb} \bar{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re})}_{t_5} + \underbrace{(\tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re})}_{t_6} \\
&+ \underbrace{(\tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \tilde{\mathbf{h}}_{rb} \bar{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re})}_{t_7} + \underbrace{(\tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \tilde{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re})}_{t_8}
\end{aligned}$$

$$\begin{aligned}
&+ \underbrace{(\tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \tilde{\mathbf{h}}_{rb} \bar{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re})}_{t_9} + \underbrace{(\tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \tilde{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re})}_{t_{10}} \\
&+ \underbrace{(\bar{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \bar{\mathbf{h}}_{re})}_{t_{11}} + \underbrace{(\bar{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re})}_{t_{12}} \\
&+ \underbrace{(\tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{rb} \bar{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re})}_{t_{13}} + \underbrace{(\tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re})}_{t_{14}} \\
&+ \underbrace{(\bar{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \tilde{\mathbf{h}}_{rb} \bar{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \bar{\mathbf{h}}_{re})}_{t_{15}} + \underbrace{(\bar{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \tilde{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \bar{\mathbf{h}}_{re})}_{t_{16}}
\end{aligned} \tag{28}$$

Then, for each sub-item in (28), we calculate the expectation separately. First, we can have

$$\begin{aligned}
\mathbb{E}(t_1) &= \mathbb{E}(\bar{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{rb} \bar{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \bar{\mathbf{h}}_{re}) \\
&\stackrel{(a)}{=} \bar{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{rb} \bar{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \bar{\mathbf{h}}_{re} \tag{29}
\end{aligned}$$

$$\mathbb{E}(t_2) = \mathbb{E}(\bar{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \bar{\mathbf{h}}_{re}) \stackrel{(b)}{=} 0 \tag{30}$$

Equation (a) holds due to the fact that LoS component is constant, and equation (b) holds due to the fact that the last item $\tilde{\mathbf{h}}_{re}$ follows Gaussian distribution with zero mean, then it is easy to derive that t_2 also follows Gaussian distribution with zero mean. Similarly, we have:

$$\begin{aligned}
&\mathbb{E}(t_3) = \mathbb{E}(t_4) = \mathbb{E}(t_5) = \mathbb{E}(t_6) \\
&= \mathbb{E}(t_8) = \mathbb{E}(t_9) = \mathbb{E}(t_{11}) = \mathbb{E}(t_{13}) \\
&= \mathbb{E}(t_{14}) = \mathbb{E}(t_{15}) = 0
\end{aligned} \tag{31}$$

Then for t_7 , we have

$$\mathbb{E}(t_7) = \mathbb{E}(\tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{rb} \bar{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re}) \tag{32}$$

With the natures of Gaussian distribution, we can derive

$$\mathbb{E}(\tilde{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H) = \begin{pmatrix} \sigma_{rb}^2 & 0 & \cdots & 0 \\ 0 & \sigma_{rb}^2 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & & \sigma_{rb}^2 \end{pmatrix} \tag{33}$$

Then, we have

$$\mathbb{E}(t_7) = \sigma_{rb}^2 \bar{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \mathbf{B} \mathbf{A}^H \bar{\mathbf{h}}_{re} \tag{34}$$

Similarly, the expectation of t_{10} and t_{16} can be derived as, respectively

$$\begin{aligned}
\mathbb{E}(t_{10}) &= \mathbb{E}(\tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{rb} \bar{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re}) \\
&= \sigma_{re}^2 \bar{\mathbf{h}}_{re}^H \mathbf{B} \mathbf{A}^H \mathbf{A} \mathbf{B}^H \bar{\mathbf{h}}_{re}
\end{aligned} \tag{35}$$

$$\begin{aligned}
\mathbb{E}(t_{16}) &= \mathbb{E}(\tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \tilde{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re}) \\
&= \sigma_{re}^2 \sigma_{rb}^2 \text{Tr}(\mathbf{A} \mathbf{B}^H \mathbf{B} \mathbf{A}^H) \\
&= \sigma_{re}^2 \sigma_{rb}^2 \text{Tr}(\Phi_2 \mathbf{H}_{ar} \mathbf{H}_{ar}^H \Phi_1^H \Phi_1 \mathbf{H}_{ar} \mathbf{H}_{ar}^H \Phi_2^H) \\
&= \sigma_{re}^2 \sigma_{rb}^2 \text{Tr}(\mathbf{H}_{ar} \mathbf{H}_{ar}^H \mathbf{H}_{ar} \mathbf{H}_{ar}^H)
\end{aligned} \quad (36)$$

Further, all the sub-item in p_{16} can be summed as follows

$$\begin{aligned}
\mathbb{E}(p_{16}) &= \tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \tilde{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re} + \sigma_{rb}^2 \tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \mathbf{B} \mathbf{A}^H \tilde{\mathbf{h}}_{re} \\
&+ \sigma_{re}^2 \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \mathbf{A}^H \mathbf{A} \mathbf{B}^H \tilde{\mathbf{h}}_{rb} + \sigma_{re}^2 \sigma_{rb}^2 \text{Tr}(\mathbf{H}_{ar} \mathbf{H}_{ar}^H \mathbf{H}_{ar} \mathbf{H}_{ar}^H)
\end{aligned} \quad (37)$$

Next, for each item in q_1 , we can remove the expected operation with the same method as p_{16} . For example, $\mathbb{E}(p_1)$, $\mathbb{E}(p_2)$, $\mathbb{E}(p_3)$ and $\mathbb{E}(p_{15})$ in (27) can be derived as

$$\begin{aligned}
\mathbb{E}(p_1) &= \tilde{\mathbf{h}}_{ae}^H \tilde{\mathbf{h}}_{ab} \tilde{\mathbf{h}}_{ab}^H \tilde{\mathbf{h}}_{ae} + \sigma_{ae}^2 \tilde{\mathbf{h}}_{ab}^H \tilde{\mathbf{h}}_{ab} + \sigma_{ab}^2 \tilde{\mathbf{h}}_{ae}^H \tilde{\mathbf{h}}_{ae} \\
&+ M_a \sigma_{ae}^2 \sigma_{ab}^2 \\
\mathbb{E}(p_2) &= \tilde{\mathbf{h}}_{ae}^H \mathbf{B}^H \tilde{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \tilde{\mathbf{h}}_{ae} + \sigma_{ae}^2 \tilde{\mathbf{h}}_{rb}^H \mathbf{B} \tilde{\mathbf{h}}_{ab} \\
\mathbb{E}(p_3) &= \tilde{\mathbf{h}}_{ae}^H \tilde{\mathbf{h}}_{ab} \tilde{\mathbf{h}}_{ab}^H \mathbf{A}^H \tilde{\mathbf{h}}_{re} + \sigma_{ab}^2 \tilde{\mathbf{h}}_{ae}^H \mathbf{A}^H \tilde{\mathbf{h}}_{re} \\
\mathbb{E}(p_{15}) &= \tilde{\mathbf{h}}_{re}^H \mathbf{A} \mathbf{B}^H \tilde{\mathbf{h}}_{rb} \tilde{\mathbf{h}}_{ab}^H \mathbf{A}^H \tilde{\mathbf{h}}_{re} + \sigma_{re}^2 \tilde{\mathbf{h}}_{ab}^H \mathbf{A}^H \mathbf{A} \mathbf{B}^H \tilde{\mathbf{h}}_{rb}
\end{aligned} \quad (38)$$

The expectations of the rest items in (27) are not listed here for brief. Note that when directly adding up all the sub-items from p_1 to p_{16} , the result is very cumbersome. Fortunately, the summation of some associated sub-items can be transformed into the form of modulus square by polynomial merging, where the specific process is omitted for simplicity. Then by merging all sub-items, the expectation of q_1 can be given by

$$\begin{aligned}
\mathbb{E}(q_1) &= |(\tilde{\mathbf{h}}_{ae}^H + \tilde{\mathbf{h}}_{re}^H \Phi_2 \tilde{\mathbf{H}}_{ar})(\tilde{\mathbf{h}}_{ab} + \tilde{\mathbf{H}}_{ar}^H \Phi_1^H \tilde{\mathbf{h}}_{rb})|^2 \\
&+ \sigma_{ae}^2 |(\tilde{\mathbf{h}}_{rb}^H \Phi_1 \tilde{\mathbf{H}}_{ar} + \tilde{\mathbf{h}}_{ab}^H)|^2 + \sigma_{ab}^2 |(\tilde{\mathbf{h}}_{re}^H \Phi_2 \tilde{\mathbf{H}}_{ar} + \tilde{\mathbf{h}}_{ae}^H)|^2 \\
&+ \sigma_{rb}^2 |(\tilde{\mathbf{h}}_{re}^H \Phi_2 \tilde{\mathbf{H}}_{ar} + \tilde{\mathbf{h}}_{ae}^H) \mathbf{H}_{ar}^H|^2 + M_a \sigma_{ae}^2 \sigma_{ab}^2 \\
&+ \sigma_{ae}^2 \sigma_{rb}^2 \text{Tr}(\tilde{\mathbf{H}}_{ar} \tilde{\mathbf{H}}_{ar}^H) + \sigma_{re}^2 |(\tilde{\mathbf{h}}_{rb}^H \Phi_1 \tilde{\mathbf{H}}_{ar} + \tilde{\mathbf{h}}_{ab}^H) \tilde{\mathbf{H}}_{ar}^H|^2 \\
&+ \sigma_{ab}^2 \sigma_{re}^2 \text{Tr}(\tilde{\mathbf{H}}_{ar} \mathbf{H}_{ar}^H) + \sigma_{re}^2 \sigma_{rb}^2 \text{Tr}(\tilde{\mathbf{H}}_{ar} \tilde{\mathbf{H}}_{ar}^H \tilde{\mathbf{H}}_{ar} \tilde{\mathbf{H}}_{ar}^H)
\end{aligned} \quad (39)$$

Due to the similar form between the numerator and denominator in (11), the expectation of the numerator $\mathbb{E}(f_1(\Phi_1, \Phi_2))$ can be derived as shown in (16b) and (16c), which is omitted for brief.

Thus, the proof is completed.

REFERENCES

- [1] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, Oct 2019.
- [2] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "Phy-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10037–10047, Feb 2016.
- [3] X. Zhou, B. Maham, and A. Hjørungnes, "Pilot contamination for active eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 903–907, Mar 2012.
- [4] K. Huang, H. Wang, Y. Wu, and R. Schober, "Pilot spoofing attack by multiple eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 17, no. 10, pp. 6433–6447, Oct 2018.
- [5] B. Akgun, M. Krnz, and O. Ozan Koyluoglu, "Vulnerabilities of massive mimo systems to pilot contamination attacks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1251–1263, Oct 2019.
- [6] W. Wang, N. Cheng, K. C. Teh, X. Lin, W. Zhuang, and X. Shen, "On countermeasures of pilot spoofing attack in massive mimo systems: A double channel training based approach," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6697–6708, July 2019.
- [7] J. K. Tugnait, "Pilot spoofing attack detection and countermeasure," *IEEE Transactions on Communications*, vol. 66, no. 5, pp. 2093–2106, Jan 2018.
- [8] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, M. Di Renzo, and N. Al-Dhahir, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1546–1577, 2021.
- [9] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface aided wireless communications: A tutorial," *IEEE Transactions on Communications*, vol. 69, no. 5, pp. 3313–3351, May 2021.
- [10] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 4157–4170, Aug 2019.
- [11] W. Tang, J. Dai, M. Z. Chen, K. K. Wong, X. Li, X. Zhao, S. Jin, Q. Cheng, and T. J. Cui, "Mimo transmission through reconfigurable intelligent surface: System design, analysis, and implementation," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2683–2699, Nov 2020.
- [12] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, Oct 2019.
- [13] L. Dong and H. Wang, "Secure mimo transmission via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 9, no. 6, pp. 787–790, Nov 2020.
- [14] K. Huang and H. Wang, "Intelligent reflecting surface aided pilot contamination attack and its countermeasure," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 345–359, Jan 2021.
- [15] A. Taha, M. Alrabeiah, and A. Alkhateeb, "Enabling large intelligent surfaces with compressive sensing and deep learning," *IEEE Access*, vol. 9, pp. 44 304–44 321, 2021.
- [16] A. Taha, Y. Zhang, F. Mismar, and A. Alkhateeb, "Deep reinforcement learning for intelligent reflecting surfaces: Towards standalone operation," *IEEE 21st Int. Workshop Signal Process. Adv. Wireless Commun (SPAWC)*, pp. 1–5, 2020.
- [17] Q. Xiong, Y. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 932–940, May 2015.
- [18] J. Moon, S. H. Lee, H. Lee, and I. Lee, "Proactive eavesdropping with jamming and eavesdropping mode selection," *IEEE Transactions on Wireless Communications*, vol. 18, no. 7, pp. 3726–3738, Jul 2019.
- [19] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: Design and performance analysis," *IEEE Transactions on Wireless Communications*, vol. 16, no. 7, pp. 4585–4599, Jul 2017.
- [20] W. Xu, F. Gao, S. Jin, and A. Alkhateeb, "3d scene-based beam selection for mmwave communications," *IEEE Wireless Communications Letters*, vol. 9, no. 11, pp. 1850–1854, Nov 2020.
- [21] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, Oct 2009.
- [22] G. Chen, J. P. Coon, and M. D. Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1195–1206, May 2017.
- [23] Q. Zhang, S. Jin, K.-K. Wong, H. Zhu, and M. Matthaiou, "Power scaling of uplink massive mimo systems with arbitrary-rank channel means," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 5, pp. 966–981, Oct 2014.
- [24] Y. Han, W. Tang, S. Jin, C. Wen, and X. Ma, "Large intelligent surface-assisted wireless communication exploiting statistical csi," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 8238–8242, Aug 2019.
- [25] Q. Tao, J. Wang, and C. Zhong, "Performance analysis of intelligent reflecting surface aided communication systems," *IEEE Communications Letters*, vol. 24, no. 11, pp. 2464–2468, Nov 2020.
- [26] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Communications Letters*, vol. 9, no. 6, pp. 778–782, Jun 2020.
- [27] K. N. Le, "Performance analysis of secure communications over dual correlated rician fading channels," *IEEE Transactions on Communications*, vol. 66, no. 12, pp. 6659–6673, Dec 2018.

- [28] N. Yang, M. ElKashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in misome wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2170–2181, Apr 2016.