Covert Pilot Spoofing Attack via Active Reconfigurable Intelligent Surface

Covert Pilot Spoofing Attack via Active Reconfigurable Intelligent Surface

Junshan Luo, Zhengfei Qu, Boxiang He, Shilian Wang, Giorgio Taricco, *Fellow, IEEE*, and Chau Yuen, *Fellow, IEEE*

***Abstract*—The active reconfigurable intelligent surface (RIS) offers a promising solution to overcome the double-fading attenuation inherent in passive RIS-aided systems. However, this capability can be exploited by adversaries to launch potent pilot spoofing attack (PSA). In this paper, we propose a novel active RIS-aided covert PSA scheme for time-division duplex systems, where a passive eavesdropper manipulates the channel state information (CSI) estimation at the legitimate transceiver during the uplink stage and steers downlink data towards itself during the downlink stage. Crucially, without requiring perfect instantaneous CSI, a practical challenge for eavesdroppers, we maximize the average eavesdropping signal-to-noise ratio (SNR) by jointly designing the RIS reflection coefficients for both stages. To ensure covertness, we integrate an anti-energy ratio detection (ERD) mechanism that constrains the detection probability below a predefined threshold. The resulting non-convex optimization problem is solved via an efficient alternating optimization algorithm combined with penalty methods, handling the rank-1 constraints and statistical CSI uncertainties. Simulations demonstrate that the proposed scheme achieves up to 26 dB SNR gain over passive RIS-aided PSA and reduces ERD detection probability compared to traditional PSA. This work reveals the dual-edged nature of the active RIS: while enhancing security, it introduces new attack schemes demanding advanced countermeasures.**

***Index Terms*—Active reconfigurable intelligent surface, energy ratio detection, pilot spoofing attack.**

I. Introduction

The evolution from the first to the fifth generation mobile networks has set the stage for sixth-generation (6G) systems, slated for deployment by 2030. A cornerstone of 6G is enhanced physical layer security (PLS), a critical advancement given the escalating sophistication of wireless attacks [1], [2]. While emerging technologies like massive multiple-input multiple-output (MIMO) beamforming and fluid antennas have fortified conventional encryption, they simultaneously introduce novel vulnerabilities that adversaries can exploit [3], [4]. Understanding these attack schemes, particularly those subverting core PLS mechanisms, is paramount for securing next-generation networks.

PLS has emerged as a vital complement to cryptographic protocols, eliminating key distribution overhead while providing information-theoretic safeguards [5]. Its efficacy in multi-antenna systems, however, hinges critically on precise channel state information (CSI) acquisition. In time-division duplex (TDD) systems, CSI estimation typically leverages channel reciprocity through reverse pilot training [6]. This dependency creates a fundamental vulnerability: publicly known pilot sequences enable adversaries to launch pilot spoofing attack (PSA). By transmitting identical pilots during uplink training, attackers distort CSI estimation at legitimate transceivers and subsequently intercept confidential beams intended for legitimate receivers.

PSA in the TDD systems was first introduced in [7]. Specifically, during the uplink training stage, as the legitimate receiver transmits the pilots to the legitimate transmitter, an eavesdropper concurrently transmits identical pilots to induce inaccuracies in CSI estimation at the legitimate transceivers. This manipulation subsequently leads to increased signal leakage to the eavesdropper during the downlink transmission stage. Furthermore, prior studies [8]–[11] have extensively demonstrated the susceptibility of TDD systems to PSA. For instance, simulations in [8] revealed that the maximum achievable secure degrees of freedom (DoF) diminishes to zero under PSA. In [9], researchers proposed a coordinated PSA framework, wherein multiple eavesdroppers collaboratively distort the CSI estimation process, to maximize the eavesdropping signal-to-noise ratio (SNR) in the downlink stage. The authors of [10] extended this cooperative PSA approach to a multi-user MIMO system, significantly reducing the achievable downlink sum-rate of legitimate users. Additionally, results from [11] indicated that the PSA can degrade the throughput of massive MIMO systems by more than 50%.

To detect and counter PSA, numerous studies have been developed, primarily categorized into two approaches: randomness-based methods [12]–[14] and statistical feature-based methods [15]. Specifically, in [12], an uncoordinated frequency shift scheme was proposed, introducing multiple random frequency offsets into pilot sequences. The work in [13] designed a detection mechanism by leveraging phase noise from non-ideal local oscillators. [14] developed a se-

This work was supported in part by the the National Natural Science Foundation of China under Grants 62501612, in part by China Postdoctoral Science Foundation under Grant BX20240471, 2025M774418, and in part by Ministry of Education, Singapore, under MOE Tier 2 (Award number T2EP50124-0032). *(Corresponding authors: Zhengfei Qu and Boxiang He.)*

Junshan Luo is with the Sixty-Third Research Institute, National University of Defense Technology, Nanjing 210007, China, and also with the College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China (e-mail: ljsnudt@foxmail.com).

Zhengfei Qu, Boxiang He and Shilian Wang are with the College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China (e-mail: quzhengfei2023@163.com; wangsl@nudt.edu.cn; boxianghe1@bjtu.edu.cn).

Giorgio Taricco is with the Department of Electronics and Telecommunications (DET), Politecnico di Torino, Turin 10129, Italy (e-mail: taricco@polito.it).

Chau Yuen is with the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore 639798 (e-mail: chau.yuen@ntu.edu.sg).

cure framework based on random channel training, wherein legitimate users randomly select one orthogonal pilot sequence from a predefined set. [15] proposed an energy ratio detection (ERD) method, which exploits disparities in received signal power levels at legitimate transceivers. Among these countermeasures, ERD has been proven particularly effective against traditional PSA schemes. Its detection capability stems from the fundamental reliance of TDD systems on channel reciprocity.

Reconfigurable intelligent surface (RIS) is a promising technique that allows flexible electromagnetic waves manipulation, recognized by the world economic forum as one of the top ten emerging technologies globally. RIS is a planar array consisting of a massive number of low-cost reflecting elements which can tune the reflection coefficient on the incident signal independently [16]. This capability allows targeted enhancement or suppression of reflected signals at specific receivers [17], [18]. Crucially, RIS elements support real-time reconfiguration, with state-switching times as low as tens of microseconds [19], orders of magnitude faster than typical channel coherence times, typically milliseconds.

The dual-faced nature of RIS introduces both security enhancements and vulnerabilities. On the one hand, RIS enables advanced PLS techniques [20]–[23], leveraging dynamically tuned reflection coefficients to protect legitimate transmissions against eavesdropping. On the other hand, malicious communication parties exploit RIS to launch novel PSA in TDD systems [24]–[27]. Specifically, RIS can execute these attacks without prior knowledge of pilot sequences [24] by strategically altering reflection coefficients across uplink/downlink stages. Recent research demonstrates three threat paradigms. In [25], the authors designed reflection coefficients using statistical channel information to minimize secrecy rates, degrading downlink security performance. The work in [26] minimized legitimate data rates under attack detection probability constraints. Employing rapidly modulated coefficients to disrupt both channel estimation at base stations (BS) and downlink signal transmission, the user throughput was remarkably reduced [27].

Conventional RIS-aided PSA schemes predominantly employ passive reflecting elements. Nevertheless, passive RIS faces fundamental limitations due to double-fading (or multiplicative fading) constraints [28]. The double-fading effect refers to the signal attenuation experienced in passive RIS systems due to the product of path losses on both transmitter-RIS and RIS-receiver links [29]. This multiplicative fading constraint significantly limits the effectiveness of passive RIS in practical deployment scenarios [30]. These surfaces merely reflect incident signals passively, necessitating substantial numbers of reflecting elements and meticulous deployment arrangements to achieve effective attacks [31]. Increasing passive RIS elements enhances attack efficacy at the cost of drastically increased computational complexity in associated algorithms. Moreover, such RIS deployments exhibit optimal effectiveness only when physically proximate to legitimate transceivers [32], a condition often impractical in real-world attack scenarios.

To overcome the limitations of passive RIS, active RIS employ reflecting elements integrated with power amplifiers, enabling simultaneous control of reflection phase and signal amplification through an external power supply [33]. Recent experimental studies confirm the technical feasibility of such amplification levels, with active RIS prototypes demonstrating gains exceeding 25 dB in [34] and array-level average gains up to 34.1 dB in [30] in realistic deployment scenarios. This architecture delivers two critical advancements. Firstly, active RIS strengthens signal strength and quality in challenging environments, e.g., weak-signal regions or long-distance transmissions [35], substantially mitigating multiplicative fading constraints inherent in passive designs. Secondly, by eliminating complex radio frequency chains, active RIS achieves lightweight signal amplification [36], thereby reducing capital expenditure, system complexity, and power consumption. Crucially, active RIS elevates attack efficacy with minimal increase in reflecting elements, providing malicious communication parties with a resource-efficient attack vector.

The active RIS-aided PSA scheme possesses an inherent advantage in circumventing conventional security measures. By reflecting pilots transmitted between legitimate transceivers without requiring explicit knowledge of pilot sequences, it inherently neutralizes secure approaches based on dynamic pilot alteration[1]. This capability arises because the randomness-based countermeasures, including those relying on random frequency shift, phase noise, or orthogonal pilots, are designed under a critical assumption: they require the attacker to first decipher the pilot's explicit content. The RIS-based attack inherently bypasses this prerequisite of deciphering and replication, which is a fundamental step. However, the RIS-aided PSA method suffers from detection vulnerability to ERD mechanisms, where thermal noise generated by active RIS amplifiers must be incorporated into ERD models. Consequently, ensuring attack efficacy while maintaining controllable detection probability becomes paramount.

To address this, we propose a novel covert PSA scheme leveraging active RIS to systematically evade ERD. In our scheme, we aim to enhance eavesdropping SNR by disrupting channel reciprocity while maintaining covertness. While minimizing the legitimate receiver's secrecy capacity is a prevalent method for enhancing eavesdropping performance, it may require reducing the legitimate achievable capacity. Such capacity degradation inherently increases the risk of exposing the PSA under ERD. Furthermore, jointly optimizing RIS coefficients for both uplink spoofing and downlink eavesdropping under imperfect CSI would introduce complex non-convex coupling in secrecy capacity formulations. The proposed SNR metric enables tractable optimization via alternating optimization (AO) while maintaining attack efficacy. Our main contributions are summarized as follows:

- *Novel covert attack model with active RIS*: we propose the first active RIS-aided covert PSA framework that overcomes the double-fading effect of passive RIS. By dynamically tuning reflection coefficients across uplink

[1]The proposed PSA scheme does not require explicit pilot sequence knowledge but relies on pilot length τ, which can be obtained from public standards or estimated via pilot length estimation-based approaches [37].

and downlink stages, it steers confidential signals towards Eve with far fewer elements, significantly enhancing the eavesdropping efficacy.
- *Covertness guarantee against ERD:* to address the vulnerability under ERD, we embed an explicit anti-ERD constraint into the covert attack optimization problem. This enables precisely controlled detection probability while maintaining high eavesdropping SNR, achieving a critical trade-off unexplored in prior art.
- *Efficient algorithm under statistical CSI:* for practical passive eavesdroppers lacking instantaneous CSI, we develop an AO framework integrating penalty-based rank-1 handling and Fenchel duality transformation. It efficiently solves the non-convex joint design problem with low complexity, and converges fast without requiring instantaneous CSI.

The remainder of this paper is organized as follows: Section II proposes and analyzes the PSA system with the aid of the active RIS as well as the CSI assumptions. Section III illustrates the mechanism of ERD, and establishes the optimization problem of the covert attack model. Section IV presents the joint reflection optimization methodology. Section V provides the simulation results. Section VI gives the conclusion.

Notations: x, $\boldsymbol{x}$, and $\boldsymbol{X}$ represent a scalar, a vector, a matrix, respectively. The Euclidean norm of a vector $\boldsymbol{x}$ is expressed as $\|\boldsymbol{x}\|$. $|\boldsymbol{x}|^2$ denotes that the vector of component-wise squared magnitudes. $|x|$ represents the absolute value of a scalar x. Matrix entries are indexed by $\boldsymbol{X}_{(m,n)}$, corresponding to the element at the m-th row and n-th column. $|\boldsymbol{X}|$ and $\|\boldsymbol{X}\|_{\mathrm{F}}$ denote the determinant and the Frobenius norm of $\boldsymbol{X}$, respectively. $\mathrm{Tr}\,(\boldsymbol{X})$ and $\mathrm{rank}\,(\boldsymbol{X})$ represent trace and rank of matrix $\boldsymbol{X}$, respectively. $\boldsymbol{X}^*$, $\boldsymbol{X}^{\mathrm{T}}$, and $\boldsymbol{X}^\dagger$ denote conjugate, transpose, and conjugate transpose of the matrix $\boldsymbol{X}$, respectively. $\boldsymbol{X} \succeq 0$ specifies that $\boldsymbol{X}$ is a positive semi-definite matrix. $\boldsymbol{I}_N$ denotes an identity matrix of dimension $N \times N$. $\boldsymbol{0}_M$ denotes the M-dimensional all-zero vector. $\mathbb{C}^N$ denotes the space of complex column vectors of length N. $\mathbb{C}^{M\times N}$ describes the space containing all complex matrices of dimension $M \times N$. $\mathcal{I}_N = \{1, 2, \ldots, N\}$ is defined as the index set. $\mathcal{CN}(\boldsymbol{0}, \boldsymbol{\Gamma})$ denotes the circularly symmetric complex Gaussian (CSCG) distribution with zero mean and covariance being matrix $\boldsymbol{\Gamma}$. $\mathrm{vec}(\boldsymbol{X})$ denotes the vectorization operation that converts matrix $\boldsymbol{X}$ into a column vector by stacking its columns. $\mathbb{E}\,[x]$ represents the expectation of the random variable x.

II. System Model

This section formulates the system framework for the active RIS-aided PSA scheme. The operational process comprises two sequential stages: an uplink pilot spoofing stage followed by a downlink eavesdropping stage. We subsequently specify critical CSI assumptions governing this framework.

A. System Description

We consider an active RIS-aided PSA scheme in the TDD system shown in Fig. 1, including a transmitter (Alice) equipped with N antennas, a legitimate receiver (Bob) with single antenna, an active RIS with M elements, and an eavesdropper (Eve) with single antenna. As shown in Fig. 2, during the uplink training stage, Bob transmits the pilots to Alice, in order to assist Alice in estimating the CSI between them. The active RIS, controlled by Eve via a separate communication link, reflects the pilots with the goal of misleading Alice's CSI estimation. In the downlink data transmission stage, Eve seeks to wiretap the confidential information transmitted from Alice to Bob, with the assistance of the active RIS. The reflecting coefficients of the active RIS can be configured asymmetrically across these two stages and are meticulously designed to redirect the downlink signals toward Eve[2]

B. Uplink Pilot Spoofing Stage

Specifically, during the uplink training stage, Bob transmits the pilots $\boldsymbol{x}_{\mathrm{p}} = [x_{\mathrm{p},1}, \cdots, x_{\mathrm{p},\tau}]^{\mathrm{T}} \in \mathbb{C}^\tau$ to Alice for CSI estimation, where τ is the length of the pilots, satisfying $\boldsymbol{x}_{\mathrm{p}}^\dagger \boldsymbol{x}_{\mathrm{p}} = 1$. At the same time, Eve turns on the active RIS and attempts to interfere with the CSI estimation. Denote the reflection coefficient matrix of the active RIS as $\boldsymbol{P}_{\mathrm{up}} = \mathrm{diag}\left[\beta_1 e^{j\theta_1}, \cdots, \beta_M e^{j\theta_M}\right] \in \mathbb{C}^{M\times M}$, where $\beta_i \in [0, \beta_{\max}]$ and θ_i represent the amplification factor and the phase shift of the ith reflection element, respectively, and $\beta_{\max} > 1$ is the maximum allowable power gain factor, $i \in \mathcal{I}_M$.

Assuming that Alice has prior knowledge of the pilots, the estimated CSI of Alice is given by

$$\hat{\boldsymbol{h}} = \boldsymbol{h} + \tilde{\boldsymbol{\epsilon}} \tag{1}$$

where $\boldsymbol{h} = \boldsymbol{h}_{\mathrm{B}} + \boldsymbol{H}_{\mathrm{A}} \boldsymbol{P}_{\mathrm{up}} \boldsymbol{h}_{\mathrm{R}}$; $\tilde{\boldsymbol{\epsilon}} \sim \mathcal{CN}(\boldsymbol{0}, \frac{\tilde{\sigma}_{\mathrm{AR}}^2}{P_{\mathrm{T}}} \boldsymbol{I}_N)$; $\tilde{\sigma}_{\mathrm{AR}}^2 = \sigma_{\mathrm{R1}}^2 \boldsymbol{H}_{\mathrm{A}} \boldsymbol{P}_{\mathrm{up}} \boldsymbol{P}_{\mathrm{up}}^\dagger \boldsymbol{H}_{\mathrm{A}}^\dagger + \sigma_{\mathrm{A}}^2 \boldsymbol{I}_N$; $\boldsymbol{h}_{\mathrm{B}} \in \mathbb{C}^N$, $\boldsymbol{H}_{\mathrm{A}} \in \mathbb{C}^{N\times M}$ and $\boldsymbol{h}_{\mathrm{R}} \in \mathbb{C}^M$ denote the channels from Bob to Alice, from RIS to Alice, and from Bob to RIS, respectively; $\mathrm{vec}(\boldsymbol{Z}_{\mathrm{R1}}) \sim \mathcal{CN}\left(\boldsymbol{0}_{M\tau}, \sigma_{\mathrm{R1}}^2 \boldsymbol{I}_{M\tau}\right)$ is the thermal noise generated by the amplifiers with σ_{R1}^2 being the noise power; $\mathrm{vec}(\boldsymbol{N}_{\mathrm{A}}) \sim \mathcal{CN}\left(\boldsymbol{0}_{N\tau}, \sigma_{\mathrm{A}}^2 \boldsymbol{I}_{N\tau}\right)$ is the noise matrix at Alice, following CSCG distribution with σ_{A}^2 being the noise power; P_{T} is the transmit power of Bob. The estimated cascaded CSI includes the component of the direct channel from Bob to Alice and the component of the reflection channel induced by the active RIS.

C. Downlink Eavesdropping Stage

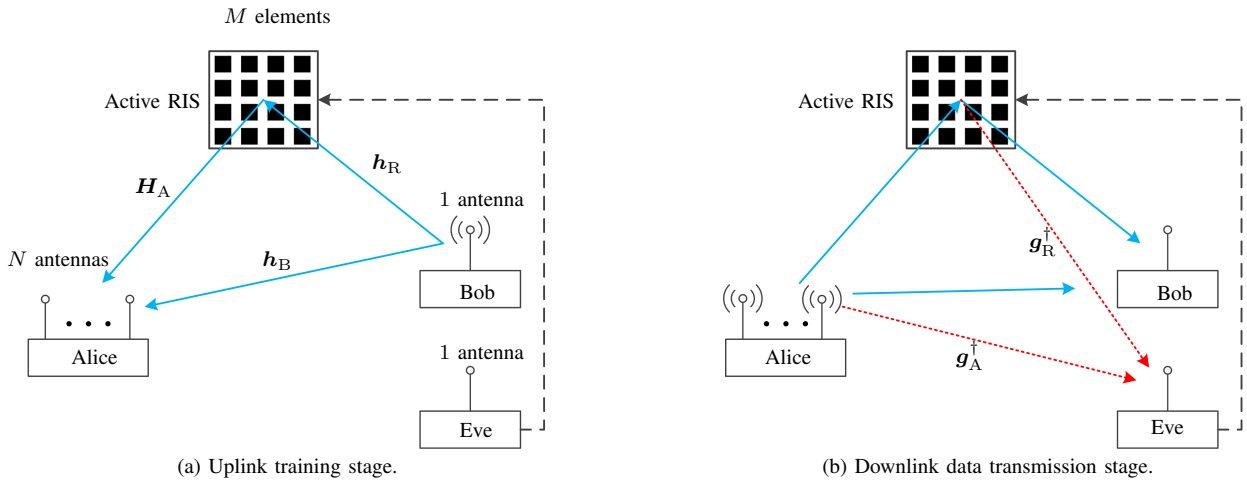
During the downlink data transmission stage, we assume that Alice utilizes the maximum ratio transmission (MRT) technique to convey secret messages to Bob based on the estimated CSI[3]. The beamforming vector of Alice, $\boldsymbol{w} \in \mathbb{C}^N$, can be expressed as

$$\boldsymbol{w} = \frac{\hat{\boldsymbol{h}}}{\|\hat{\boldsymbol{h}}\|}. \tag{2}$$

In this stage, Eve wiretaps the signals transmitted from Alice to Bob with the aid of the active RIS. The reflection

[2]The RIS can distinguish between uplink and downlink stages through power detection methods or authentication-based detection methods like Sni5Gect, which can sniff communication traffic during pre-authentication phases to determine transmission directions [38].

[3]Notice that the presence of single-antenna terminal implies that MRT is theoretically the best option for information transmission.



(a) Uplink training stage. (b) Downlink data transmission stage.

Fig. 1. The active RIS-aided PSA model where Eve launches the attack during the uplink training stage and eavesdrops the signal transmitted from Alice to Bob during the downlink data transmission stage with the assistance of an active RIS.

coefficient matrix of the active RIS is set to $\boldsymbol{P}_{\mathrm{down}} = \mathrm{diag}\left[\gamma_1 e^{j\phi_1}, \cdots, \gamma_M e^{j\phi_M}\right] \in \mathbb{C}^{M\times M}$, where γ_l and ϕ_l denote the amplification factor and the phase shift of the lth reflection element, respectively, and $\gamma_l \in [0, \beta_{\max}]$, $l \in \mathcal{I}_M$. The received signal at Eve is given by

$$y_{\mathrm{E}} = \sqrt{P_{\mathrm{S}}}\left(\boldsymbol{g}_{\mathrm{A}}^{\dagger} + \boldsymbol{g}_{\mathrm{R}}^{\dagger}\boldsymbol{P}_{\mathrm{down}}\boldsymbol{H}_{\mathrm{A}}^{\dagger}\right)\boldsymbol{w}s + \boldsymbol{g}_{\mathrm{R}}^{\dagger}\boldsymbol{P}_{\mathrm{down}}\boldsymbol{z}_{\mathrm{R2}} + n_{\mathrm{E}} \quad (3)$$

where $\boldsymbol{g}_{\mathrm{A}} \in \mathbb{C}^N$ and $\boldsymbol{g}_{\mathrm{R}} \in \mathbb{C}^M$ denote the channels from Alice to Eve and from Eve to RIS, respectively; P_{S} is the transmit power of Alice; $\boldsymbol{z}_{\mathrm{R2}} \sim \mathcal{CN}\left(0, \sigma_{\mathrm{R2}}^2 \boldsymbol{I}_M\right) \in \mathbb{C}^M$ is the thermal noise of the active RIS during the downlink stage; $n_{\mathrm{E}} \sim \mathcal{CN}\left(0, \sigma_{\mathrm{E}}^2\right)$ denotes the AWGN at Eve and σ_{E}^2 is the noise power.

Remark 1: As shown in (28), our proposed scheme is different from the traditional RIS-aided downlink eavesdropping scheme due to the exploitation of the uplink stage.

D. CSI Assumptions

The successful execution of the proposed active RIS-aided PSA scheme relies on the knowledge of certain CSI at Eve and/or the RIS. The design of the reflection matrices $\boldsymbol{P}_{\mathrm{up}}$ and $\boldsymbol{P}_{\mathrm{down}}$ requires information related to the channels $\boldsymbol{H}_{\mathrm{A}}$, $\boldsymbol{h}_{\mathrm{R}}$, $\boldsymbol{g}_{\mathrm{A}}$, $\boldsymbol{g}_{\mathrm{R}}$, and $\boldsymbol{h}_{\mathrm{B}}$. However, as passive entities, Eve and the RIS cannot directly acquire instantaneous CSI via conventional pilot training. Our work adopts the statistical CSI error model [39]–[42], aligned with current RIS-related channel estimation methods and position-based channel estimation methods. Specifically, we consider the following practical and conservative approaches to estimate the related channels:

a) RIS-related Channel Estimation Techniques: The feasibility of acquiring necessary channel information is supported by well-established RIS channel estimation methods in the literature. (i) Direct estimation employs active sensing elements integrated into the RIS to separately resolve individual channel links, i.e., transmitter-RIS channel and RIS-receiver channels [43]; (ii) Cascaded estimation efficiently obtains the composite transmitter-RIS-receiver channel as a whole, reducing estimation complexity [44]; and (iii) Compressed sensing leverages the inherent sparsity of wireless channels to drastically lower the pilot overhead, making covert estimation feasible for a passive eavesdropper [38]. Collectively, these methods provide a technical foundation for the channel knowledge assumed in our work. During the uplink training stage, the RIS can passively observe the signals transmitted by Bob to estimate $\boldsymbol{h}_{\mathrm{R}}$ with the help of active channel elements on it. And it is common to estimate $\boldsymbol{g}_{\mathrm{R}}$ by transmitting pilots from Eve to RIS.

b) Position-based CSI Estimation Techniques: The channels, particularly at high frequencies, exhibit a sparse structure and are mainly determined by the geometric configuration of the user, base station, and the environment (including the RIS). This sparsity can be exploited for efficient channel parameter estimation using compressive sensing (CS) methods. Furthermore, geometric information, such as user location, can be translated into partial CSI or its statistical properties. Numerous existing studies on position-based channel estimation methods lay the foundation for the channel configuration in our work [45]–[47]. Machine learning techniques can model the end-to-end channel as a function of user equipment location. Since user locations can be known statistically, this positional uncertainty should be correspondingly accounted for in the CSI uncertainty model [45]. The work in [46] demonstrates that user position and trajectory information can inform the angular structure of the sparse mmWave channel, enabling efficient compressive channel estimation. The work in [47] establishes that real-time user position can pinpoint the specific region of dominant channel components in the delay-Doppler domain, guiding a targeted compressed sensing channel estimation strategy. Eve and the active RIS are assumed to possess long-term statistical information, e.g., path loss, spatial correlation matrices, Rician factors of the relevant channels. This information can be obtained through long-term observation of the legitimate transmissions without requiring perfect instantaneous channel estimation during the attack phase. Based on this information, it becomes possible to estimate the legitimate channels $\boldsymbol{H}_{\mathrm{A}}$, $\boldsymbol{g}_{\mathrm{A}}$, and $\boldsymbol{h}_{\mathrm{B}}$ with error according to the legitimate transceivers location.

c) Control Link Collaboration: A low-rate, out-of-band control link exists between Eve and the RIS. This link allows Eve

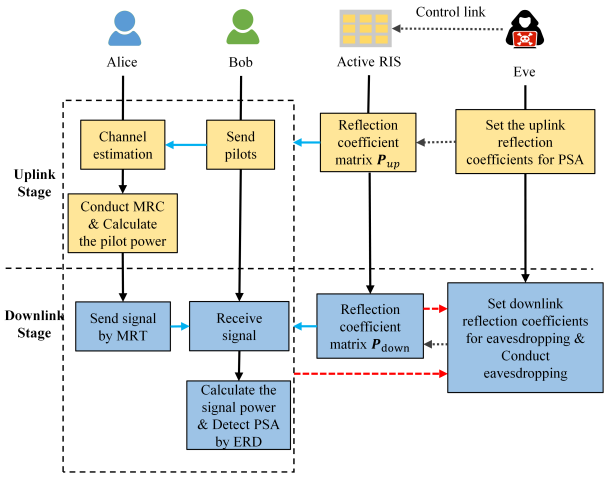


Fig. 2. The flowchart of the proposed active RIS-aided PSA system.

to share necessary information, e.g., coarse channel estimates, received signal quality feedback, and coordinate the reflection coefficients $\boldsymbol{P}_{\rm up}$ and $\boldsymbol{P}_{\rm down}$ based on the available statistical or partially observed information. Given the difficulty of acquiring perfect instantaneous CSI, our optimization problem aims to maximize the average eavesdropping SNR over the statistical distributions of the channels. This formulation is robust to the uncertainty in instantaneous CSI and relies only on the statistical knowledge or coarse estimates[4].

The power consumption budget at the active RIS can be expressed as

$$\mathbb{E}\left(P_{\rm T}\|\boldsymbol{P}_{\rm up}(\boldsymbol{h}_{\rm R}+\Delta\boldsymbol{h}_{\rm R})\|^2+\|\boldsymbol{P}_{\rm up}\|_{\rm F}^2\sigma_{\rm R1}^2\right)\le P_{\rm RIS} \tag{4}$$

$$\mathbb{E}\left(P_{\rm S}\|\boldsymbol{P}_{\rm down}(\boldsymbol{H}_{\rm A}+\Delta\boldsymbol{H}_{\rm A})^\dagger\boldsymbol{w}\|^2+\|\boldsymbol{P}_{\rm down}\|_{\rm F}^2\sigma_{\rm R2}^2\right)\le P_{\rm RIS} \tag{5}$$

where $\Delta\boldsymbol{h}_{\rm R}\sim\mathcal{CN}(\boldsymbol{0},\overline{\sigma}_{\rm R}^2)$ and $vec(\Delta\boldsymbol{H}_{\rm A})\sim\mathcal{CN}(\boldsymbol{0},\overline{\sigma}_{\rm A}^2)$ are the estimation errors. After some calculations, the expectations can be equivalently reformulated as

$$P_{\rm T}\|\boldsymbol{P}_{\rm up}\boldsymbol{h}_{\rm R}\|^2+\|\boldsymbol{P}_{\rm up}\|_{\rm F}^2(\sigma_{\rm R1}^2+P_{\rm T}\overline{\sigma}_{\rm R}^2)\le P_{\rm RIS} \tag{6}$$

$$P_{\rm S}\|\boldsymbol{P}_{\rm down}\boldsymbol{H}_{\rm A}^\dagger\boldsymbol{w}\|^2+\|\boldsymbol{P}_{\rm down}\|_{\rm F}^2\left(P_{\rm S}\overline{\sigma}_{\rm A}^2+\sigma_{\rm R2}^2\right)\le P_{\rm RIS}. \tag{7}$$

III. The Proposed Attack Optimization Framework

In this section, we first introduce the basic detection principle of the ERD for RIS-aided PSA scheme. Then we formulate the average eavesdropping SNR maximization problem subject to a detection probability constraint for covertness guarantee.

A. Energy Ratio Detection

The main idea of ERD is to check the received power level differences at Alice and Bob respectively by sending signals to each other [15]. As shown in Fig. 2, the two stages of the ERD in TDD systems are specified as follows: Bob first sends pilots to Alice and then Alice calculates the received power level. Then, Alice transmits information containing the value of the power level to Bob, from which Bob can obtain his own received power level and recover Alice's power level. By comparing the two power levels, Bob can identify the existence of the PSA.

Without loss of generality, we assume the ERD is employed by the legitimate transceivers. The detection of the active RIS-aided PSA is formulated as a binary hypothesis test problem, where the null hypothesis $\mathcal{H}_0$ describes that the system is free from PSA, and the alternative hypothesis $\mathcal{H}_1$ indicates the system is under the risk of PSA as illustrated in section II. Specifically, the received signals at Alice under these hypotheses can be respectively expressed as

$$\mathcal{H}_0:\boldsymbol{Y}_{\rm A}=\sqrt{P_{\rm T}}\boldsymbol{h}_{\rm B}\boldsymbol{x}_{\rm p}^\dagger+\boldsymbol{N}_{\rm A} \tag{8}$$

$$\mathcal{H}_1:\boldsymbol{Y}_{\rm A}=\sqrt{P_{\rm T}}(\boldsymbol{h}_{\rm B}+\boldsymbol{H}_{\rm A}\boldsymbol{P}_{\rm up}\boldsymbol{h}_{\rm R})\boldsymbol{x}_{\rm p}^\dagger+\boldsymbol{H}_{\rm A}\boldsymbol{P}_{\rm up}\boldsymbol{Z}_{\rm R1}+\boldsymbol{N}_{\rm A} \tag{9}$$

We assume that Alice employs the maximum ratio combining (MRC) to combine the received pilots, which yields

$$\mathcal{H}_0:\tilde{\boldsymbol{y}}_{\rm A}^{\rm T}=\sqrt{P_{\rm T}}\frac{(\boldsymbol{h}_{\rm B}+\boldsymbol{\epsilon})^\dagger}{\|\boldsymbol{h}_{\rm B}+\boldsymbol{\epsilon}\|}\boldsymbol{h}_{\rm B}\boldsymbol{x}_{\rm p}^\dagger+\boldsymbol{n}_{\rm A} \tag{10}$$

$$\mathcal{H}_1:\tilde{\boldsymbol{y}}_{\rm A}^{\rm T}=\frac{\sqrt{P_{\rm T}}(\boldsymbol{h}_{\rm B}+\boldsymbol{H}_{\rm A}\boldsymbol{P}_{\rm up}\boldsymbol{h}_{\rm R}+\tilde{\boldsymbol{\epsilon}})^\dagger(\boldsymbol{h}_{\rm B}+\boldsymbol{H}_{\rm A}\boldsymbol{P}_{\rm up}\boldsymbol{h}_{\rm R})}{\|\boldsymbol{h}_{\rm B}+\boldsymbol{H}_{\rm A}\boldsymbol{P}_{\rm up}\boldsymbol{h}_{\rm R}+\tilde{\boldsymbol{\epsilon}}\|}\boldsymbol{x}_{\rm p}^\dagger+\tilde{\boldsymbol{n}}_{\rm A} \tag{11}$$

where $\tilde{\boldsymbol{n}}_{\rm A}\triangleq\frac{(\boldsymbol{h}_{\rm B}+\boldsymbol{H}_{\rm A}\boldsymbol{P}_{\rm up}\boldsymbol{h}_{\rm R}+\tilde{\boldsymbol{\epsilon}})^\dagger}{\|\boldsymbol{h}_{\rm B}+\boldsymbol{H}_{\rm A}\boldsymbol{P}_{\rm up}\boldsymbol{h}_{\rm R}+\tilde{\boldsymbol{\epsilon}}\|}(\boldsymbol{H}_{\rm A}\boldsymbol{P}_{\rm up}\boldsymbol{Z}_{\rm R1}+\boldsymbol{N}_{\rm A})$ is the effective noise under $\mathcal{H}_1$, and $\boldsymbol{\epsilon}\sim\mathcal{CN}(\boldsymbol{0},\frac{\sigma_{\rm A}^2}{P_{\rm T}\tau}\boldsymbol{I}_N)$. Thus the average received power at Alice in the uplink training stage, denoted by Q_1, is

$$Q_1=\frac{1}{\tau}\|\tilde{\boldsymbol{y}}_{\rm A}\|^2. \tag{12}$$

In the downlink stage, Alice modulates the power level Q_1 into the data signal $\boldsymbol{x}_{\rm q}=[x_{{\rm q},1},\cdots,x_{{\rm q},K}]^{\rm T}\in\mathbb{C}^K$. In the kth time slot, $k\in\mathcal{I}_K$, Alice uses the MRT technique to send the signal $x_{{\rm q},k}$ and the received signal at Bob is

$$\mathcal{H}_0:y_{{\rm B},k}=\sqrt{P_{\rm S}}\boldsymbol{h}_{\rm B}^\dagger\boldsymbol{w}x_{{\rm q},k}+n_{{\rm B},k} \tag{13}$$

$$\mathcal{H}_1:y_{{\rm B},k}=\sqrt{P_{\rm S}}\left(\boldsymbol{h}_{\rm B}^\dagger+\boldsymbol{h}_{\rm R}^\dagger\boldsymbol{P}_{\rm down}\boldsymbol{H}_{\rm A}^\dagger\right)\boldsymbol{w}x_{{\rm q},k}+\boldsymbol{h}_{\rm R}^\dagger\boldsymbol{P}_{\rm down}\boldsymbol{z}_{\rm R2}+n_{{\rm B},k} \tag{14}$$

where $n_{{\rm B},k}\sim\mathcal{CN}(0,\sigma_{\rm B}^2)$ is the CSCG noise in the kth time slot, and the beamforming vector can be expressed as

$$\mathcal{H}_0:\boldsymbol{w}=\frac{\boldsymbol{h}_{\rm B}+\boldsymbol{\epsilon}}{\|\boldsymbol{h}_{\rm B}+\boldsymbol{\epsilon}\|} \tag{15}$$

$$\mathcal{H}_1:\boldsymbol{w}=\frac{\boldsymbol{h}_{\rm B}+\boldsymbol{H}_{\rm A}\boldsymbol{P}_{\rm up}\boldsymbol{h}_{\rm R}+\tilde{\boldsymbol{\epsilon}}}{\|\boldsymbol{h}_{\rm B}+\boldsymbol{H}_{\rm A}\boldsymbol{P}_{\rm up}\boldsymbol{h}_{\rm R}+\tilde{\boldsymbol{\epsilon}}\|} \tag{16}$$

respectively. During K transmission slots, the average received power at Bob is

$$Q_2=\frac{1}{K}\sum_{k=1}^{K}|y_{{\rm B},k}|^2. \tag{17}$$

According to the central limit theorem (CLT), Q_1 and Q_2 can be approximated by a Gaussian distributed random variable if τ and K are sufficiently large, i.e.,

$$Q_1\sim\mathcal{N}(\mu_1,\sigma_1^2) \tag{18}$$

[4]It is acknowledged that the precise acquisition of instantaneous $\boldsymbol{g}_{\rm A}$ and $\boldsymbol{h}_{\rm B}$ by a passive eavesdropper is challenging in practice. The performance evaluated in Section V is based on the availability of statistical CSI and the passive observation mechanisms described above.

$$Q_2 \sim \mathcal{N}(\mu_2, \sigma_2^2) \tag{19}$$

with μ_k and σ_k^2 being the expectation and variance, respectively, $k \in \{1, 2\}$. The expectations can be respectively expressed as

$$\mu_1 = \begin{cases} \left| \frac{\hat{\boldsymbol{h}}^\dagger}{\|\hat{\boldsymbol{h}}\|} \boldsymbol{h}_{\mathrm{B}} \right|^2 P_{\mathrm{T}} + \sigma_{\mathrm{A}}^2 \to \mathcal{H}_0 \\ \left| \frac{\hat{\boldsymbol{h}}^\dagger}{\|\hat{\boldsymbol{h}}\|} \left(\boldsymbol{h}_{\mathrm{B}} + \boldsymbol{H}_{\mathrm{A}} \boldsymbol{P}_{\mathrm{up}} \boldsymbol{h}_{\mathrm{R}} \right) \right|^2 P_{\mathrm{T}} + \tilde{\sigma}_{\mathrm{A}}^2 \to \mathcal{H}_1 \end{cases} \tag{20}$$

$$\mu_2 = \begin{cases} \left| \boldsymbol{h}_{\mathrm{B}}^\dagger \frac{\hat{\boldsymbol{h}}}{\|\hat{\boldsymbol{h}}\|} \right|^2 P_{\mathrm{S}} + \sigma_{\mathrm{B}}^2 \to \mathcal{H}_0 \\ \left| \left(\boldsymbol{h}_{\mathrm{B}}^\dagger + \boldsymbol{h}_{\mathrm{R}}^\dagger \boldsymbol{P}_{\mathrm{down}} \boldsymbol{H}_{\mathrm{A}}^\dagger \right) \frac{\hat{\boldsymbol{h}}}{\|\hat{\boldsymbol{h}}\|} \right|^2 P_{\mathrm{S}} + \tilde{\sigma}_{\mathrm{B}}^2 \to \mathcal{H}_1 \end{cases} \tag{21}$$

where the channel estimates $\hat{\boldsymbol{h}}$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ follow (8) and (9), respectively; $\tilde{\sigma}_{\mathrm{A}}^2 = \sigma_{\mathrm{R}}^2 \|\boldsymbol{h}^\dagger \boldsymbol{H}_{\mathrm{A}} \boldsymbol{P}_{\mathrm{up}}\|^2 / \|\boldsymbol{h}\|^2 + \sigma_{\mathrm{A}}^2$; $\tilde{\sigma}_{\mathrm{B}}^2 = \sigma_{\mathrm{R2}}^2 \|\boldsymbol{h}_{\mathrm{R}}^\dagger \boldsymbol{P}_{\mathrm{down}}\|^2 + \sigma_{\mathrm{B}}^2$. The variances can be expressed as $\sigma_1^2 = \frac{1}{\tau}\mu_1^2$ and $\sigma_2^2 = \frac{1}{K}\mu_2^2$, respectively.

Proof. See appendix. □

To illustrate the principle of ERD conveniently, we set $P_{\mathrm{S}} = P_{\mathrm{T}}$ and $\sigma_{\mathrm{A}}^2 = \sigma_{\mathrm{B}}^2$ without loss of generality. If there is no PSA, then we have $\mu_1 = \mu_2$ and $\sigma_1^2 = \sigma_2^2$ under $\mathcal{H}_0$. Otherwise, if PSA exists and we generally set $\boldsymbol{P}_{\mathrm{down}} \neq \boldsymbol{P}_{\mathrm{up}}$, the downlink channel is not reciprocal with the uplink channel, i.e., $\boldsymbol{h}_{\mathrm{B}} + \boldsymbol{H}_{\mathrm{A}} \boldsymbol{P}_{\mathrm{down}}^\dagger \boldsymbol{h}_{\mathrm{R}} \neq \boldsymbol{h}_{\mathrm{B}} + \boldsymbol{H}_{\mathrm{A}} \boldsymbol{P}_{\mathrm{up}} \boldsymbol{h}_{\mathrm{R}}$, hence the inequality $\mu_1 \neq \mu_2$ holds. By setting the test statistic as $T = \frac{Q_2}{Q_1}$, Bob can detect the existence of RIS-aided PSA.

Remark 2: If we set $\boldsymbol{P}_{\mathrm{down}} = \boldsymbol{P}_{\mathrm{up}}^\dagger$, it is difficult to detect the PSA by ERD, as the conclusions $\mu_1 = \mu_2$ and $\sigma_1^2 = \sigma_2^2$ still hold. Our proposed scheme is demonstrated to have better performance than this setting in Section V.

Theorem 1: Based on the CLT, Q_1 can be seen as stationary $Q_1 \to \mu_1$ for sufficiently large τ. According to [48], the distributions of T under $\mathcal{H}_0$ and $\mathcal{H}_1$ are

$$\mathcal{H}_0 : T \sim \mathcal{N}(\mu_{1,0}, \sigma_{1,0}^2) \tag{22}$$

$$\mathcal{H}_1 : T \sim \mathcal{N}(\mu_{1,1}, \sigma_{1,1}^2) \tag{23}$$

where $\mu_{1,0} = 1$, $\sigma_{1,0}^2 = \frac{1}{\tau}$, $\mu_{1,1} = \frac{\mu_2}{\mu_1}$, and $\sigma_{1,1}^2 = \frac{\mu_2^2}{K\mu_1^2}$.

The test statistic T is a common Gaussian random variable following (22) under $\mathcal{H}_0$ and (23) under $\mathcal{H}_1$. Then a simple expression of the detection threshold $\tilde{\gamma}$ can be derived based on a given probability of false alarm. We get

$$\mathbb{P}_{\mathrm{D}} = \Phi\left(\frac{\tilde{\gamma} - \mu_{1,1}}{\sigma_{1,1}} \right) = \Phi\left(\sqrt{K} \left(\frac{\mu_1}{\mu_2} \tilde{\gamma} - 1 \right) \right) \tag{24}$$

Then the threshold can be derived as

$$\tilde{\gamma} = \frac{\Phi^{-1}(\mathbb{P}_{\mathrm{D}})}{\sqrt{K}} + 1. \tag{25}$$

We could obtain the probability of detection $\mathbb{P}_{\mathrm{D}}$ as

$$\mathbb{P}_{\mathrm{D}} = \Phi\left(\frac{\tilde{\gamma} - \mu_{1,1}}{\sigma_{1,1}} \right) = \Phi\left((\sqrt{K} + \Phi^{-1}(\mathbb{P}_{\mathrm{F}})) \frac{\mu_1}{\mu_2} - \sqrt{K} \right) \tag{26}$$

Building upon the ERD mechanism described above, we will develop a joint optimization framework to achieve a balance between eavesdropping capability and covertness, with the core objective of maximizing the average eavesdropping SNR under ERD constraints

B. Covert Attack Optimization Problem

The proposed active RIS-aided PSA scheme jointly necessitates the design of the uplink and downlink reflection coefficients. The objective is to maximize the eavesdropping SNR of Eve subject to the active RIS power budget and the given ERD detection probability. The eavesdropping SNR of Eve can be expressed as

$$\rho = \log_{10} \frac{P_{\mathrm{S}} \left| \left(\boldsymbol{g}_{\mathrm{A}}^\dagger + \boldsymbol{g}_{\mathrm{R}}^\dagger \boldsymbol{P}_{\mathrm{down}} \boldsymbol{H}_{\mathrm{A}}^\dagger + \boldsymbol{\varepsilon}^\dagger \right) \left(\boldsymbol{h}_{\mathrm{B}} + \boldsymbol{H}_{\mathrm{A}} \boldsymbol{P}_{\mathrm{up}} \boldsymbol{h}_{\mathrm{R}} + \tilde{\boldsymbol{\epsilon}} \right) \right|^2}{\left(\|\boldsymbol{g}_{\mathrm{R}}^\dagger \boldsymbol{P}_{\mathrm{down}}\|^2 \sigma_{\mathrm{R2}}^2 + \sigma_{\mathrm{E}}^2 \right) \|\boldsymbol{h}_{\mathrm{B}} + \boldsymbol{H}_{\mathrm{A}} \boldsymbol{P}_{\mathrm{up}} \boldsymbol{h}_{\mathrm{R}} + \tilde{\boldsymbol{\epsilon}}\|^2} \tag{27}$$

where $\boldsymbol{\varepsilon} \sim \mathcal{CN}\left(0, \tilde{\sigma}_{\mathrm{A}}^2 \boldsymbol{I}_N\right) \in \mathbb{C}^N$ is the channel estimation error of the channel $\boldsymbol{g}_{\mathrm{A}}^\dagger$, and $\tilde{\sigma}_{\mathrm{A}}^2$ is the variance of the error. The average eavesdropping SNR in dB can be rewritten as

$$\mathbb{E}\{\rho\} = \mathbb{E}\left(\log_{10} \frac{f_{\mathrm{A}}\left(\boldsymbol{P}_{\mathrm{up}}, \boldsymbol{P}_{\mathrm{down}} \right)}{f_{\mathrm{B}}\left(\boldsymbol{P}_{\mathrm{up}}, \boldsymbol{P}_{\mathrm{down}} \right)} \right) \tag{28}$$

where

$$\begin{aligned} & f_{\mathrm{A}}\left(\boldsymbol{P}_{\mathrm{up}}, \boldsymbol{P}_{\mathrm{down}} \right) \\ & = P_{\mathrm{S}} |(\boldsymbol{g}_{\mathrm{A}}^\dagger + \boldsymbol{g}_{\mathrm{R}}^\dagger \boldsymbol{P}_{\mathrm{down}} \boldsymbol{H}_{\mathrm{A}}^\dagger + \boldsymbol{\varepsilon}^\dagger)(\boldsymbol{h}_{\mathrm{B}} + \boldsymbol{H}_{\mathrm{A}} \boldsymbol{P}_{\mathrm{up}} \boldsymbol{h}_{\mathrm{R}} + \tilde{\boldsymbol{\epsilon}})|^2 \end{aligned} \tag{29}$$

$$\begin{aligned} & f_{\mathrm{B}}\left(\boldsymbol{P}_{\mathrm{up}}, \boldsymbol{P}_{\mathrm{down}} \right) \\ & = (\|\boldsymbol{g}_{\mathrm{R}}^\dagger \boldsymbol{P}_{\mathrm{down}}\|^2 \sigma_{\mathrm{R2}}^2 + \sigma_{\mathrm{E}}^2) \|\boldsymbol{h}_{\mathrm{B}} + \boldsymbol{H}_{\mathrm{A}} \boldsymbol{P}_{\mathrm{up}} \boldsymbol{h}_{\mathrm{R}} + \tilde{\boldsymbol{\epsilon}}\|^2. \end{aligned} \tag{30}$$

The problem of maximizing the average eavesdropping SNR can be formulated as

$$\max_{\boldsymbol{P}_{\mathrm{up}}, \boldsymbol{P}_{\mathrm{down}}} \quad \mathbb{E}\{\rho\} \tag{31a}$$

$$\text{s.t.} \quad (6), (7)$$

$$0 \leq \gamma_i \leq \beta_{\max}, 0 \leq \beta_l \leq \beta_{\max}, \forall i, l \in \mathcal{I}_M \tag{31b}$$

$$\theta_i \in [0, 2\pi), \phi_l \in [0, 2\pi), \forall i, l \in \mathcal{I}_M \tag{31c}$$

$$\mathbb{P}_{\mathrm{D}} \leq \tilde{\gamma} \tag{31d}$$

where P_{RIS} is the power budget at the active RIS; (6) and (7) are the total power consumption budget at the active RIS during the uplink stage and downlink stage, respectively; (31b) specifies the range of the amplification factors; (31c) constrains the feasible sets of the phase shifts; (31d) guarantees that the detection probability is below the threshold $\tilde{\gamma}$. The difficulty of solving the problem (31) lies in the non-convex fractional structure of the objective function, the coupled variables, and the nonconvexity of the ERD constraints.

IV. The Proposed Joint Reflection Optimization Algorithm

In this section, we first transform the problem (31) into a tractable one. Then we propose an iterative algorithm based on Fenchel conjugate-based lemma and external penalty function.

A. Optimal $\boldsymbol{P}_{\rm up}$ for Fixed $\boldsymbol{P}_{\rm down}$

Due to the monotonicity of the logarithmic function and the theorem in [49], the objective function in problem (31) can be approximated as

$$\begin{aligned}&\max_{\boldsymbol{P}_{\rm up},\boldsymbol{P}_{\rm down}} \mathbb{E}\left\{\log\left(\frac{f_{\rm A}\left(\boldsymbol{P}_{\rm up},\boldsymbol{P}_{\rm down}\right)}{f_{\rm B}\left(\boldsymbol{P}_{\rm up},\boldsymbol{P}_{\rm down}\right)}\right)\right\}\\ &\approx \max_{\boldsymbol{P}_{\rm up},\boldsymbol{P}_{\rm down}} \log\left(\frac{\mathbb{E}\left\{f_{\rm A}\left(\boldsymbol{P}_{\rm up},\boldsymbol{P}_{\rm down}\right)\right\}}{\mathbb{E}\left\{f_{\rm B}\left(\boldsymbol{P}_{\rm up},\boldsymbol{P}_{\rm down}\right)\right\}}\right).\end{aligned} \tag{32}$$

We first optimize the reflection coefficient matrix $\boldsymbol{P}_{\rm up}$ with fixed $\boldsymbol{P}_{\rm down}$. Denote $\boldsymbol{V}_{\rm up}=\left[\begin{array}{c}\boldsymbol{p}_{\rm up}\\1\end{array}\right][\boldsymbol{p}_{\rm up}^{\dagger}\ 1]$, where $\boldsymbol{p}_{\rm up}=[\boldsymbol{P}_{{\rm up},(1,1)},\boldsymbol{P}_{{\rm up},(2,2)},\cdots,\boldsymbol{P}_{{\rm up},(M,M)}]^{\rm T}$, $\forall i\in\mathcal{I}_M$. Problem (31) can be reformulated as

$$\max_{\boldsymbol{V}_{\rm up}}\quad \log(\mathrm{Tr}(\boldsymbol{R}_{\rm B1}\boldsymbol{V}_{\rm up}))-\log(\mathrm{Tr}(\boldsymbol{R}_{\rm B2}\boldsymbol{V}_{\rm up}))+C_1 \tag{33a}$$

$$\text{s.t.}\quad \mathrm{Tr}(\boldsymbol{R}_{\rm B3}\boldsymbol{V}_{\rm up})\le P_{\rm RIS} \tag{33b}$$

$$\boldsymbol{V}_{{\rm up},(i,i)}\le\beta_{\max}^2,\boldsymbol{V}_{{\rm up},(M+1,M+1)}=1,\forall i\in\mathcal{I}_M \tag{33c}$$

$$\boldsymbol{V}_{\rm up}\succeq 0 \tag{33d}$$

$$\mathrm{rank}\{\boldsymbol{V}_{\rm up}\}=1 \tag{33e}$$

$$\text{(31d)}$$

where the notations are written as

$$C_1=\log\left(P_{\rm S}\right)-\log\left(\left\|\boldsymbol{g}_{\rm R}^{\dagger}\boldsymbol{P}_{\rm down}\right\|^2\sigma_{\rm R2}^2+\sigma_{\rm E}^2\right) \tag{34}$$

$$\boldsymbol{R}_{\rm B1}=\left[\begin{array}{cc}\boldsymbol{h}_{\rm B2}\boldsymbol{h}_{\rm B2}^{\dagger}+\tilde{\sigma}_{\rm A}^2\boldsymbol{H}_{\rm R}^{\dagger}\boldsymbol{H}_{\rm R} & h_{\rm B1}\boldsymbol{h}_{\rm B2}+\tilde{\sigma}_{\rm A}^2\boldsymbol{H}_{\rm R}^{\dagger}\boldsymbol{h}_{\rm B}\\ h_{\rm B1}^{\dagger}\boldsymbol{h}_{\rm B2}^{\dagger}+\tilde{\sigma}_{\rm A}^2\boldsymbol{h}_{\rm B}^{\dagger}\boldsymbol{H}_{\rm R} & C_2\end{array}\right] \tag{35}$$

$$h_{\rm B1}=\left(\boldsymbol{g}_{\rm A}^{\dagger}+\boldsymbol{g}_{\rm R}^{\dagger}\boldsymbol{P}_{\rm down}\boldsymbol{H}_{\rm A}^{\dagger}\right)\boldsymbol{h}_{\rm B} \tag{36}$$

$$\boldsymbol{H}_{\rm R}=\boldsymbol{H}_{\rm A}\mathrm{diag}(\boldsymbol{h}_{\rm R}) \tag{37}$$

$$\boldsymbol{h}_{\rm B2}^{\dagger}=\left(\boldsymbol{g}_{\rm A}^{\dagger}+\boldsymbol{g}_{\rm R}^{\dagger}\boldsymbol{P}_{\rm down}\boldsymbol{H}_{\rm A}^{\dagger}\right)\boldsymbol{H}_{\rm A}\mathrm{diag}\left(\boldsymbol{h}_{\rm R}\right) \tag{38}$$

$$C_2=|h_{\rm B1}|^2+\tilde{\sigma}_{\rm A}^2\|\boldsymbol{h}_{\rm B}\|^2+\tilde{\sigma}_{\rm AR}^2\|\boldsymbol{g}_{\rm A}^{\dagger}+\boldsymbol{g}_{\rm R}^{\dagger}\boldsymbol{P}_{\rm down}\boldsymbol{H}_{\rm A}^{\dagger}\|^2 \tag{39}$$

$$\boldsymbol{R}_{\rm B2}=\left[\begin{array}{cc}\boldsymbol{H}_{\rm R}^{\dagger}\boldsymbol{H}_{\rm R} & \boldsymbol{H}_{\rm R}^{\dagger}\boldsymbol{h}_{\rm B}\\ \boldsymbol{h}_{\rm B}^{\dagger}\boldsymbol{H}_{\rm R} & \boldsymbol{h}_{\rm B}^{\dagger}\boldsymbol{h}_{\rm B}+N\tilde{\sigma}_{\rm AR}^2\end{array}\right] \tag{40}$$

$$\boldsymbol{R}_{\rm B3}=\left[\begin{array}{cc}P_{\rm T}\mathrm{diag}(|\boldsymbol{h}_{\rm R}|^2)+(\sigma_{\rm R1}^2+P_{\rm T}\overline{\sigma}_{\rm R}^2)I_M & \boldsymbol{0}_M\\ \boldsymbol{0}_M^{\rm T} & 0\end{array}\right] \tag{41}$$

As for the detection probability constraint (31d), it can be rewritten as the equivalent form as follows

$$\frac{\mu_1}{\mu_2}\le 1+\delta \tag{42}$$

where $\delta=\frac{\Phi^{-1}(\tilde{\gamma})+\sqrt{K}}{\Phi^{-1}(\mathbb{P}_F)+\sqrt{K}}$ can be seen as the threshold of the difference between the uplink stage and downlink stage. Constraint (42) then can be rewritten as

$$\begin{aligned}&\|\boldsymbol{h}\|^2P_{\rm T}+\tilde{\sigma}_{\rm A}^2\\ &\le(1+\delta)\left(\frac{P_{\rm S}\left|\left(\boldsymbol{h}_{\rm B}^{\dagger}+\boldsymbol{h}_{\rm R}^{\dagger}\boldsymbol{P}_{\rm down}\boldsymbol{H}_{\rm A}^{\dagger}\right)\boldsymbol{h}\right|^2}{\|\boldsymbol{h}\|^2}+\tilde{\sigma}_{\rm B}^2\right)\end{aligned} \tag{43}$$

The noise part $\tilde{\sigma}_{\rm A}^2$ in the left term can be omitted without changing the inequality sign. After some trivial transformations, it can be transformed into a standard quadratic constraint as follows

$$[\mathrm{Tr}(\boldsymbol{R}_{\rm B2}\boldsymbol{V}_{\rm up})]^2-(1+\delta)[\mathrm{Tr}\left(\boldsymbol{R}_{\rm B4}\boldsymbol{V}_{\rm up}\right)+\frac{\tilde{\sigma}_{\rm B}}{P_{\rm T}}\mathrm{Tr}(\boldsymbol{R}_{\rm B2}\boldsymbol{V}_{\rm up})]\le 0 \tag{44}$$

where $\boldsymbol{R}_{\rm B4}=\left[\begin{array}{cc}\boldsymbol{h}_{\rm B2}\boldsymbol{h}_{\rm B2}^{\dagger} & h_{\rm B3}\boldsymbol{h}_{\rm B2}\\ h_{\rm B3}^{\dagger}\boldsymbol{h}_{\rm B2}^{\dagger} & h_{\rm B3}^{\dagger}h_{\rm B3}\end{array}\right]$, $\boldsymbol{h}_{\rm B2}^{\dagger}=\left(\boldsymbol{h}_{\rm B}^{\dagger}+\boldsymbol{h}_{\rm R}^{\dagger}\boldsymbol{P}_{\rm down}\boldsymbol{H}_{\rm A}^{\dagger}\right)\boldsymbol{H}_{\rm A}\,\mathrm{diag}(\boldsymbol{h}_{\rm B})$, and $h_{\rm B3}=\left(\boldsymbol{h}_{\rm B}^{\dagger}+\boldsymbol{h}_{\rm R}^{\dagger}\boldsymbol{P}_{\rm down}\boldsymbol{H}_{\rm A}^{\dagger}\right)\boldsymbol{h}_{\rm B}$.

Hence, the equivalent quadratic form is a convex constraint. Problem (33) remains a non-convex optimization due to the rank-1 constraint and the non-convex objective function. In the following, we present a Fenchel conjugate-based lemma to transform the objective function into a tractable one.

Lemma 1: Let $\boldsymbol{X}\in\mathbb{C}^{n\times n}$ be any complex positive definite matrix. For the function $\tilde{f}(\boldsymbol{S})=-\mathrm{Tr}(\boldsymbol{S}\boldsymbol{X})+\log|\boldsymbol{S}|+n$, the following equation

$$\max_{\boldsymbol{S}\in\mathbb{C}^{n\times n},\boldsymbol{S}\succ 0}\tilde{f}(\boldsymbol{S})=\log|\boldsymbol{X}^{-1}| \tag{45}$$

is satisfied, and the optimal solution is $\boldsymbol{S}^{\rm opt}=\boldsymbol{X}^{-1}$ [50].

Lemma 1 is obtained via Fenchel conjugate arguments in [51]. Applying Lemma 1, we transform the original problem into th following form

$$\begin{aligned}\max_{\boldsymbol{V}_{\rm up}}\quad &\log\left(\mathrm{Tr}\left(\boldsymbol{R}_{\rm B1}\boldsymbol{V}_{\rm up}\right)\right)+\max_{s_1\in\mathbb{C},s_1>0}\tilde{f}\left(s_1\right)\\ \text{s.t.}\quad &\text{(33b)}-\text{(33e)},\text{(44)}\end{aligned} \tag{46}$$

where $\tilde{f}\left(s_1\right)=-\mathrm{Tr}\left(s_1\mathrm{Tr}\left(\boldsymbol{R}_{\rm B2}\boldsymbol{V}_{\rm up}\right)\right)+\log|s_1|+1$.

To address the rank-1 constraint (33e), the standard Gaussian randomization method is conventionally used to obtain an approximate solution, which, however, cannot guarantee an optimal solution. To overcome the shortcoming, we use the following equivalent form

$$\mathrm{Tr}\left(\boldsymbol{V}_{\rm up}\right)-\lambda_{\max}\left(\boldsymbol{V}_{\rm up}\right)\le 0 \tag{47}$$

where $\lambda_{\max}\left(\boldsymbol{V}_{\rm up}\right)$ is the maximal eigenvalue of the matrix $\boldsymbol{V}_{\rm up}$. For any positive semidefinite matrix $\boldsymbol{V}_{\rm up}$, we have $\mathrm{Tr}\left(\boldsymbol{V}_{\rm up}\right)\ge\lambda_{\max}\left(\boldsymbol{V}_{\rm up}\right)$. Hence, (47) is equivalent to $\mathrm{Tr}\left(\boldsymbol{V}_{\rm up}\right)=\lambda_{\max}\left(\boldsymbol{V}_{\rm up}\right)$, meaning that

$$\boldsymbol{V}_{\rm up}=\lambda_{\max}\left(\boldsymbol{V}_{\rm up}\right)\boldsymbol{v}_{\rm up,max}\boldsymbol{v}_{\rm up,max}^{\dagger} \tag{48}$$

where $\boldsymbol{v}_{\rm up,max}$ is the unit eigenvector of $\boldsymbol{V}_{\rm up}$ corresponding to the maximal eigenvalue $\lambda_{\max}\left(\boldsymbol{V}_{\rm up}\right)$. The rank-1 constraint can be guaranteed by (47) in all cases.

To address the issue above, we adopt the external penalty method. Specifically, we first introduce the penalty weighting coefficient ξ_1 to enlarge the size of the feasible solution set spanned by constraint. Then we add the new goal into the objective function based on the external penalty method. Then the problem (46) can be equivalently rewritten as

$$\begin{aligned}\max_{\boldsymbol{V}_{\rm up},s_1>0}\quad &\log\left(\mathrm{Tr}\left(\boldsymbol{R}_{\rm B1}\boldsymbol{V}_{\rm up}\right)\right)+\tilde{f}\left(s_1\right)-\xi_1P(\boldsymbol{V}_{\rm up})\\ \text{s.t.}\quad &\text{(33b)}-\text{(33d)},\text{(44)}.\end{aligned} \tag{49}$$

where $P(\boldsymbol{V}_{\rm up})=\mathrm{Tr}\left(\boldsymbol{V}_{\rm up}\right)-\lambda_{\max}\left(\boldsymbol{V}_{\rm up}\right)$ and ξ_1 is the penalty weighting coefficient. When ξ_1 is large enough, $\mathrm{Tr}\left(\boldsymbol{V}_{\rm up}\right)\approx\lambda_{\max}\left(\boldsymbol{V}_{\rm up}\right)$ holds. However, the spectral function $\lambda_{\max}\left(\boldsymbol{V}_{\rm up}\right)$ is a non-smooth function, which is not differentiable. The sub-gradient version of the maximal eigenvalue function can be adopted to solve this problem, which is $\partial\lambda_{\max}\left(\boldsymbol{V}_{\rm up}\right)=\boldsymbol{v}_{\rm up,max}\boldsymbol{v}_{\rm up,max}^{\dagger}$. Then, we can obtain

$$\lambda_{\max}(\boldsymbol{X})-\lambda_{\max}\left(\boldsymbol{V}_{\rm up}\right)\ge\left\langle\boldsymbol{v}_{\rm up,max}\boldsymbol{v}_{\rm up,max}^{\dagger},\boldsymbol{X}-\boldsymbol{V}_{\rm up}\right\rangle \tag{50}$$

for $\forall \boldsymbol{X} \succeq \mathbf{0}$, where $\langle \boldsymbol{A}, \boldsymbol{B} \rangle = \mathrm{Tr}\left(\boldsymbol{A}^\dagger \boldsymbol{B}\right)$. Let $\boldsymbol{v}_{\mathrm{up,max}}^{(n)}$ be the unit eigenvector of $\boldsymbol{V}_{\mathrm{up}}^{(n)}$ corresponding to the largest eigenvalue at the nth iteration. We denote that $\psi(\boldsymbol{V}_{\mathrm{up}}) = \mathrm{Tr}\left(\boldsymbol{V}_{\mathrm{up}}\right) - \langle \boldsymbol{v}_{\mathrm{up,max}}^{(n)} \boldsymbol{v}_{\mathrm{up,max}}^{(n)\dagger}, \boldsymbol{V}_{\mathrm{up}} \rangle$, which is an affine function with respect to (w.r.t) $\boldsymbol{V}_{\mathrm{up}}$. Hence, by initializing $\boldsymbol{V}_{\mathrm{up}}^{(n)}$ within the feasible domain, we can achieve the optimal solution to problem (49) by solving the following equivalent problem

$$\begin{aligned} \max_{\boldsymbol{V}_{\mathrm{up}}, s_1 > 0} \quad & \log\left(\mathrm{Tr}\left(\boldsymbol{R}_{\mathrm{B1}} \boldsymbol{V}_{\mathrm{up}}\right)\right) + \tilde{f}\left(s_1\right) - \xi_1 \psi(\boldsymbol{V}_{\mathrm{up}}) \quad (51) \\ \text{s.t.} \quad & (33\text{b}) - (33\text{d}), (44). \end{aligned}$$

Then problem (51) is concave w.r.t either $\boldsymbol{V}_{\mathrm{up}}$ or s_1 when fixing the other variable. In the nth iteration, we alternatively solve the following two problems

$$\boldsymbol{V}_{\mathrm{up}}^{(n+1)} = \underset{\boldsymbol{V}_{\mathrm{up}} \in \mathcal{C}_{\mathrm{up}}}{\arg\max} \log\left(\mathrm{Tr}\left(\boldsymbol{R}_{\mathrm{B1}} \boldsymbol{V}_{\mathrm{up}}\right)\right) + \tilde{f}\left(s_1\right) - \xi_1 \psi(\boldsymbol{V}_{\mathrm{up}}) \quad (52)$$

$$s_1^{(n+1)} = \underset{s_1 > 0}{\arg\max}\, \tilde{f}\left(s_1\right) \quad (53)$$

where $\mathcal{C}_{\mathrm{up}} = \left\{ \boldsymbol{V}_{\mathrm{up}} \,\middle|\, \text{Constraints (33b)–(33d) and (44) hold} \right\}$. The problem (53) has a semi-closed form optimal solution

$$s_1^{(n+1)} = \mathrm{Tr}\Big(\boldsymbol{R}_{\mathrm{B2}} \boldsymbol{V}_{\mathrm{up}}^{(n)}\Big)^{-1}. \quad (54)$$

Problem (52) is a concave semidefinite programming (SDP) problem and thus can be optimally solved by using the interior-point method to obtain $\boldsymbol{V}_{\mathrm{up}}^{(n+1)}$. Then $\boldsymbol{v}_{\mathrm{up}}^{(n+1)}$ can be obtained from the eigenvalue decomposition (EVD) of the solution $\boldsymbol{V}_{\mathrm{up}}^{(n+1)}$ in the $(n+1)$th iteration.

B. Optimal $\boldsymbol{P}_{\mathrm{down}}$ for Fixed $\boldsymbol{P}_{\mathrm{up}}$

By letting $\boldsymbol{V}_{\mathrm{down}} = \begin{bmatrix} \boldsymbol{v}_{\mathrm{down}} \\ 1 \end{bmatrix} [\boldsymbol{v}_{\mathrm{down}}^\dagger \; 1]$, where $\boldsymbol{v}_{\mathrm{down}} = [\boldsymbol{P}_{\mathrm{down},(1,1)}, \boldsymbol{P}_{\mathrm{down},(2,2)}, \cdots, \boldsymbol{P}_{\mathrm{down},(M,M)}]^{\mathrm{T}}$, $\forall l \in \mathcal{I}_M$, problem (32) can be reformulated as

$$\begin{aligned} \max_{\boldsymbol{V}_{\mathrm{down}}} \quad & \log\left(\mathrm{Tr}\left(\boldsymbol{R}_{\mathrm{E1}} \boldsymbol{V}_{\mathrm{down}}\right)\right) - \log\left(\mathrm{Tr}\left(\boldsymbol{R}_{\mathrm{E2}} \boldsymbol{V}_{\mathrm{down}}\right)\right) \quad (55\text{a}) \\ \text{s.t.} \quad & (31\text{d}) \\ & \mathrm{Tr}\left(\boldsymbol{R}_{\mathrm{E3}} \boldsymbol{V}_{\mathrm{down}}\right) \le P_{\mathrm{RIS}} \quad (55\text{b}) \\ & \boldsymbol{V}_{\mathrm{down},(l,l)} \le \beta_{\max}^2, \boldsymbol{V}_{\mathrm{down},(M+1,M+1)} = 1, \forall l \in \mathcal{I}_M \quad (55\text{c}) \\ & \boldsymbol{V}_{\mathrm{down}} \succeq 0 \quad (55\text{d}) \\ & \mathrm{rank}\{\boldsymbol{V}_{\mathrm{down}}\} = 1 \quad (55\text{e}) \end{aligned}$$

where $\boldsymbol{R}_{\mathrm{E1}} = \begin{bmatrix} \boldsymbol{H}_{\mathrm{E2}} \boldsymbol{H}_{\mathrm{E1}}^* \boldsymbol{H}_{\mathrm{E2}}^\dagger & \boldsymbol{H}_{\mathrm{E2}} \boldsymbol{H}_{\mathrm{E1}}^* \boldsymbol{g}_{\mathrm{A}}^* \\ \boldsymbol{g}_{\mathrm{A}}^{\mathrm{T}} \boldsymbol{H}_{\mathrm{E1}}^* \boldsymbol{H}_{\mathrm{E2}}^\dagger & \boldsymbol{g}_{\mathrm{A}}^{\mathrm{T}} \boldsymbol{H}_{\mathrm{E1}}^* \boldsymbol{g}_{\mathrm{A}}^* \end{bmatrix}$, $\boldsymbol{H}_{\mathrm{E1}} = \boldsymbol{h}\boldsymbol{h}^\dagger + \frac{\tilde{\sigma}_{\mathrm{AR}}^2}{\tau} \boldsymbol{I}_N$; $\boldsymbol{H}_{\mathrm{E2}} = \mathrm{diag}(\boldsymbol{g}_{\mathrm{R}}^{\mathrm{T}}) \boldsymbol{H}_{\mathrm{A}}^{\mathrm{T}}$, $\boldsymbol{R}_{\mathrm{E2}} = \begin{bmatrix} \boldsymbol{g}_{\mathrm{R}} \boldsymbol{g}_{\mathrm{R}}^\dagger & \mathbf{0}_M \\ \mathbf{0}_M^{\mathrm{T}} & \sigma_{\mathrm{E}}^2 \end{bmatrix}$, and $\boldsymbol{R}_{\mathrm{E3}} = \begin{bmatrix} P_{\mathrm{S}} \mathrm{diag}(|\boldsymbol{w}^\dagger \boldsymbol{H}_{\mathrm{A}}|^2) + (\sigma_{\mathrm{R2}}^2 + P_{\mathrm{S}} \overline{\sigma}_{\mathrm{A}}^2) \boldsymbol{I}_M & \mathbf{0}_M \\ \mathbf{0}_M^{\mathrm{T}} & 0 \end{bmatrix}$.

As for the detection constraint (31d), it can be transformed into the following equivalent form

$$\frac{1}{P_{\mathrm{S}}} \left(\frac{\|\boldsymbol{h}\|^2 P_{\mathrm{T}} + \tilde{\sigma}_{\mathrm{A}}^2}{1+\delta} - \tilde{\sigma}_{\mathrm{B}}^2 \right) \|\boldsymbol{h}\|^2 \le \mathrm{Tr}\left(\boldsymbol{R}_{\mathrm{E4}} \boldsymbol{V}_{\mathrm{down}}\right) \quad (56)$$

where $\boldsymbol{R}_{\mathrm{E4}} = \begin{bmatrix} \boldsymbol{h}_{\mathrm{E1}} \boldsymbol{h}_{\mathrm{E1}}^\dagger & \boldsymbol{h}_{\mathrm{E1}} \boldsymbol{h}_{\mathrm{B}}^\dagger \boldsymbol{h} \\ \boldsymbol{h}^\dagger \boldsymbol{h}_{\mathrm{B}} \boldsymbol{h}_{\mathrm{E1}}^\dagger & |\boldsymbol{h}_{\mathrm{B}}^\dagger \boldsymbol{h}|^2 \end{bmatrix}$ and $\boldsymbol{h}_{\mathrm{E1}}^\dagger = \boldsymbol{h}_{\mathrm{R}}^\dagger \mathrm{diag}(\boldsymbol{H}_{\mathrm{A}}^\dagger \boldsymbol{h})$. By reapplying Lemma 1 and employing the external penalty function method to separately handle the objective function and the rank-1 constraint as IV. A, problem (55) can be equivalently reformulated as

$$\begin{aligned} \max_{\boldsymbol{V}_{\mathrm{down}}, s_2} \quad & \log\left(\mathrm{Tr}\left(\boldsymbol{R}_{\mathrm{E1}} \boldsymbol{V}_{\mathrm{down}}\right)\right) + \tilde{f}(s_2) - \xi_2 \psi(\boldsymbol{V}_{\mathrm{down}}) \quad (57) \\ \text{s.t.} \quad & (55\text{b}) - (55\text{d}), (56) \end{aligned}$$

where $\psi(\boldsymbol{V}_{\mathrm{down}}) = \mathrm{Tr}(\boldsymbol{V}_{\mathrm{down}}) - \langle \boldsymbol{v}_{\mathrm{down,max}}^{(n)} \boldsymbol{v}_{\mathrm{down,max}}^{(n)\dagger}, \boldsymbol{V}_{\mathrm{down}} \rangle$; $\tilde{f}\left(s_2\right) = -\mathrm{Tr}\left(s_2 \left(\mathrm{Tr}\left(\boldsymbol{R}_{\mathrm{E2}} \boldsymbol{V}_{\mathrm{down}}\right)\right)\right) + \log|s_2| + 1$; $\boldsymbol{v}_{\mathrm{down,max}}^{(n)}$ is the unit eigenvector of $\boldsymbol{V}_{\mathrm{down}}^{(n)}$ corresponding to the largest eigenvalue at the nth iteration; ξ_2 is the penalty weighting coefficient. Problem (57) can be equivalently transformed into a concave form, which can be solved by alternatively solving the following two problems

$$\begin{aligned} & \boldsymbol{V}_{\mathrm{down}}^{(n+1)} \\ & = \underset{\boldsymbol{V}_{\mathrm{down}} \in \mathcal{C}_{\mathrm{down}}}{\arg\max}\; \log(\mathrm{Tr}\left(\boldsymbol{R}_{\mathrm{E1}} \boldsymbol{V}_{\mathrm{down}}\right)) + \tilde{f}\left(s_2\right) - \xi_2 \psi(\boldsymbol{V}_{\mathrm{down}}) \quad (58) \\ & s_2^{(n+1)} = \underset{s_2 > 0}{\arg\max}\, \tilde{f}\left(s_2\right) \quad (59) \end{aligned}$$

where $\mathcal{C}_{\mathrm{down}} = \{\boldsymbol{V}_{\mathrm{down}} | \text{Constraints (55b)} - (55\text{d}), (56) \text{ hold.}\}$. The penalty weighting coefficient ξ_2 gradually increases to satisfy the rank-1 constraint. The semi-closed optimal solution to problem (59) is

$$s_2^{(n+1)} = \mathrm{Tr}\Big(\boldsymbol{R}_{\mathrm{E2}} \boldsymbol{V}_{\mathrm{down}}^{(n)}\Big)^{-1} \quad (60)$$

C. Overall Algorithm

Due to the application of the external penalty function approach, the choices of ξ_ℓ, $\boldsymbol{V}_\jmath^{(0)}$ are very crucial for the efficiency of the proposed iterative procedure, $\ell \in \{1, 2\}$, $\jmath \in \{\mathrm{up}, \mathrm{down}\}$. Thus, we summarize the proposed AO algorithm together with the external penalty function in two phases as described in Algorithm I. The initialization phase is to obtain the value of penalty weighting coefficient ξ_ℓ and feasible initialization $\boldsymbol{V}_\jmath^{(0)}$. The optimization phase is to find the optimal solutions of the reflection coefficient matrices $\boldsymbol{V}_\jmath^{(n)}$. The notation $\mathbb{E}\{\rho\}^{(n)}$ represents the objective value at nth iteration with given $\boldsymbol{V}_\jmath^{(n)}$. We then discuss the convergence and complexity of the proposed algorithm.

1) Convergence: Let $\phi(\boldsymbol{V}_{\mathrm{up}}^{(n)})$ represent the objective value of problem (51) at nth iteration. It can be proven that the objective value of (52) under $\boldsymbol{V}_{\mathrm{up}}^{(n+1)}$ is greater than that under $\boldsymbol{V}_{\mathrm{up}}^{(n)}$ as

$$\begin{aligned} & \phi(\boldsymbol{V}_{\mathrm{up}}^{(n+1)}) \\ & = \log(\mathrm{Tr}(\boldsymbol{R}_{\mathrm{B1}} \boldsymbol{V}_{\mathrm{up}}^{(n+1)})) - \mathrm{Tr}(s_1 \mathrm{Tr}(\boldsymbol{R}_{\mathrm{B2}} \boldsymbol{V}_{\mathrm{up}}^{(n+1)})) + \log|s_1| \\ & \quad - \xi_1(\mathrm{Tr}(\boldsymbol{V}_{\mathrm{up}}^{(n+1)}) - \lambda_{\max}(\boldsymbol{V}_{\mathrm{up}}^{(n+1)})) \quad (61\text{a}) \\ & \ge \log(\mathrm{Tr}(\boldsymbol{R}_{\mathrm{B1}} \boldsymbol{V}_{\mathrm{up}}^{(n+1)})) - \mathrm{Tr}(s_1 \mathrm{Tr}(\boldsymbol{R}_{\mathrm{B2}} \boldsymbol{V}_{\mathrm{up}}^{(n+1)})) + \log|s_1| \\ & \quad - \xi_1 \Big[\mathrm{Tr}(\boldsymbol{V}_{\mathrm{up}}^{(n+1)}) - \lambda_{\max}(\boldsymbol{V}_{\mathrm{up}}^{(n)}) \\ & \quad - \langle \boldsymbol{v}_{\mathrm{up,max}}^{(n)} \boldsymbol{v}_{\mathrm{up,max}}^{(n)\dagger}, \boldsymbol{V}_{\mathrm{up}}^{(n+1)} - \boldsymbol{V}_{\mathrm{up}}^{(n)} \rangle \Big] \quad (61\text{b}) \\ & \ge \log(\mathrm{Tr}(\boldsymbol{R}_{\mathrm{B1}} \boldsymbol{V}_{\mathrm{up}}^{(n)})) - \mathrm{Tr}(s_1 \mathrm{Tr}(\boldsymbol{R}_{\mathrm{B2}} \boldsymbol{V}_{\mathrm{up}}^{(n)})) + \log|s_1| \\ & \quad - \xi_1(\mathrm{Tr}(\boldsymbol{V}_{\mathrm{up}}^{(n)}) - \lambda_{\max}(\boldsymbol{V}_{\mathrm{up}}^{(n)})) \quad (61\text{c}) \end{aligned}$$

Algorithm I Proposed AO Algorithm for optimizing the reflection coefficient matrices

1: **Input:** Set $\boldsymbol{V}_{\mathrm{up}}^{(0)}$ and $\boldsymbol{V}_{\mathrm{down}}^{(0)}$, ξ_ℓ in feasible domain, iteration index $n=0$, the threshold δ, tolerance ε_0 and ε_ℓ.
2: **Initialization stage:**
3: While $\left|\mathrm{Tr}\left(\boldsymbol{V}_\jmath^{(n)}\right)-\lambda_{\max}\left(\boldsymbol{V}_\jmath^{(n)}\right)\right| \geq \varepsilon_\ell$, $\{\ell,\jmath\} \in \{\{1,\mathrm{up}\},\{2,\mathrm{down}\}\}$ do
4: Solve (52) and (53) separately to obtain the optimal $\boldsymbol{V}_{\mathrm{up}}^{(n+1)}$;
5: Solve (58) and (59) separately to obtain the optimal $\boldsymbol{V}_{\mathrm{down}}^{(n+1)}$;
6: If $\left\|\boldsymbol{V}_\jmath^{(n+1)}-\boldsymbol{V}_\jmath^{(n)}\right\|_{\mathrm{F}} \leq \varepsilon_0$ then
7: Set $\xi_\ell := 2\xi_\ell$;
8: else
9: Set $n=n+1$;
10: end if
11: end while
12: **Output:** ξ_ℓ, $\boldsymbol{V}_{\mathrm{up}}^{(0)} := \boldsymbol{V}_{\mathrm{up}}^{(n+1)}$ and $\boldsymbol{V}_{\mathrm{down}}^{(0)} := \boldsymbol{V}_{\mathrm{down}}^{(n+1)}$.
13: **Optimization stage:**
14: Set $n=0$;
15: While $|\mathbb{E}\{\rho\}^{(n+1)}-\mathbb{E}\{\rho\}^{(n)}| \geq \varepsilon_0$ do
16: Calculate $\mathbb{E}\{\rho\}^{(n)}$ with given $\boldsymbol{V}_{\mathrm{up}}^{(n)}$, $\boldsymbol{V}_{\mathrm{down}}^{(n)}$;
17: Calculate optimal $s_1^{(n+1)\mathrm{opt}}$ with given $\boldsymbol{V}_{\mathrm{up}}^{(n)}$, $\boldsymbol{V}_{\mathrm{down}}^{(n)}$ through (54);
18: Solve (52) over known $s_1^{(n+1)\mathrm{opt}}$, output optimal $\boldsymbol{V}_{\mathrm{up}}^{(n+1)}$;
19: Calculate optimal $s_2^{(n+1)\mathrm{opt}}$ with given $\boldsymbol{V}_{\mathrm{up}}^{(n)}$, $\boldsymbol{V}_{\mathrm{down}}^{(n)}$ through (60);
20: Solve (58) over known $s_2^{(n+1)\mathrm{opt}}$, output optimal $\boldsymbol{V}_{\mathrm{down}}^{(n+1)}$;
21: Calculate $\mathbb{E}\{\rho\}^{(n+1)}$ with given $\boldsymbol{V}_{\mathrm{up}}^{(n+1)}$, $\boldsymbol{V}_{\mathrm{down}}^{(n+1)}$;
22: Update iteration index $n=n+1$.
23: end while
24: Using EVD to obtain $\boldsymbol{v}_\jmath^{(n+1)}$ from $\boldsymbol{V}_\jmath^{(n+1)}$.
25: **Output:** Calculate the optimal average eavesdropping SNR at Eve.

$$= \phi(\boldsymbol{V}_{\mathrm{up}}^{(n)})$$

The inequality (61b) holds, which can be demonstrated by substituting $\boldsymbol{X}$ with $\boldsymbol{V}_{\mathrm{up}}^{(n+1)}$ in the inequality (50). For $\boldsymbol{V}_{\mathrm{down}}$, following the same reasoning as inequality (61), it can be proven that the objective value of (58) under $\boldsymbol{V}_{\mathrm{down}}^{(n+1)}$ is greater than that under $\boldsymbol{V}_{\mathrm{down}}^{(n)}$. The effectiveness of the iterative procedure has been proven. From an arbitrary feasible initial point, the optimization stage in Algorithm I always yields the optimal solutions in lines 17∼20, which indicates that the average eavesdropping SNR is non-decreasing after each iteration and can converge to a locally optimal solution after finite iterations.

2) Complexity: The main computational load in lines 18 and 20 is the RIS reflection coefficient matrices product. For two matrices $\boldsymbol{A} \in {}^{D_1\times D_2}$ and $\boldsymbol{B} \in {}^{D_2\times D_3}$, the complexity of their product $\boldsymbol{AB}$ is $\mathcal{O}(D_1D_2D_3)$. Thus, the per-iteration complexity of line 18 and 20 is $\mathcal{O}\left((M+1)^3\right)$. In the convex optimization process, the complexity using the interior point method can be expressed as $\mathcal{O}\left((M+1)^{3.5}\log(1/\varepsilon)\right)$, in which ε is the target accuracy.

TABLE I
SIMULATION SETUP

Parameter	Value
The bandwidth B	20 MHz
The noise power density N_0	-173 dBm/Hz
The reference path loss C_0	-30 dBm
The penalty weighting coefficients ξ_1, ξ_2	10 , 10
The tolerances in the algorithm ε_0, ε_1, ε_2	10^{-3}, 10^{-5}, 10^{-5}
The thermal noise power at active RIS σ_{R1}^2, σ_{R2}^2	-80 dBm, -80 dBm
The Rician factors κ_{AB}, κ_{AR}, κ_{RB}, κ_{AE}, and κ_{RE}	10, 10, 10, 1, 1
The path loss exponents α_{AB}, α_{RB}, α_{AE}, α_{RE}, α_{AR}	2, 2, 3.5, 3.5 2.8
The power budget at the active RIS P_{RIS}	10 dBW

V. NUMERICAL RESULTS

A. Simulation Setup and Parameters

In this section, numerical results are provided to investigate the performance of the proposed active RIS-aided covert PSA system. As shown in Fig. 3, Alice, Bob, Eve and the active RIS are located at (0,0), (100,100), (x_{Eve},0), and ($x_{\mathrm{RIS}}, y_{\mathrm{RIS}}$) in meter ($m$), respectively. We consider a typical quasi-static Rician fading environment in an urban area. Considering that Bob is an air user and active RIS is more likely to be deployed on the surface of tall buildings, we set the link between Alice and its nearby RIS $\boldsymbol{H}_{\mathrm{A}}$, air-gound links $\boldsymbol{h}_{\mathrm{B}}$ and $\boldsymbol{h}_{\mathrm{R}}$ as the LoS-dominant channel with high Rician factors, denoted as κ_{AR}, κ_{AB}, and κ_{RB}, and the path loss exponents are denoted as α_{AR}, α_{AB}, and α_{RB}, respectively. The channel between Eve and Alice $\boldsymbol{g}_{\mathrm{A}}$ and the channel between RIS and Eve $\boldsymbol{g}_{\mathrm{R}}$ are set as the Rician channel with low Rician factors, denoted as κ_{AE} and κ_{RE}, and the path loss exponents are denoted as α_{AE} and α_{RE}, respectively. The setting of the system and channel parameters are listed in Table I. The large-scale path loss is $\delta = C_0 - 10\alpha\log_{10}(d)$ dB, where α is path loss exponent, d is the distance between the transmitter and the receiver, and C_0 is the path loss at the reference distance of 1m. All the results plotted are averaged over 1000 channel realizations.

In our simulations, the channel matrices $\boldsymbol{H}_{\mathrm{A}}$, $\boldsymbol{h}_{\mathrm{R}}$, $\boldsymbol{g}_{\mathrm{R}}$ are assumed to be estimated by the active RIS via passive uplink observation. The direct channels $\boldsymbol{g}_{\mathrm{A}}$ and $\boldsymbol{h}_{\mathrm{B}}$ are known only through their statistical properties, i.e., path loss, Rician K-factor, etc. The RIS-Eve control link is assumed to enable perfect sharing of this information.

To evaluate the advantage brought by our proposed scheme, we compare it with the following seven benchmark schemes.

- **Scheme 1: No RIS.** Eve passively wiretaps the information without the aid of the RIS.
- **Scheme 2: Active/Passive RIS-aided downlink eavesdropping scheme (Active/Passive-downlink).** Active/Passive RIS is turned on during the downlink stage and designed to maximizing the eavesdropping SNR, but turned off during the uplink stage [52], [53].

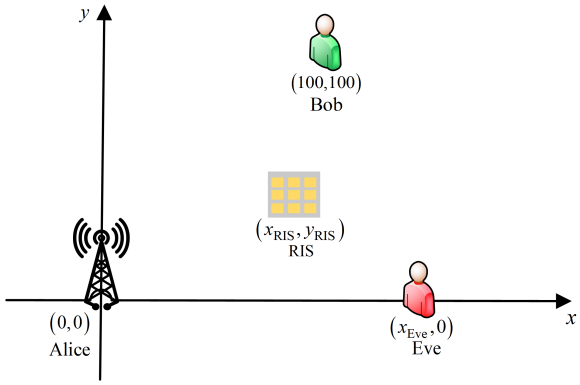


Fig. 3. Simulation setup.

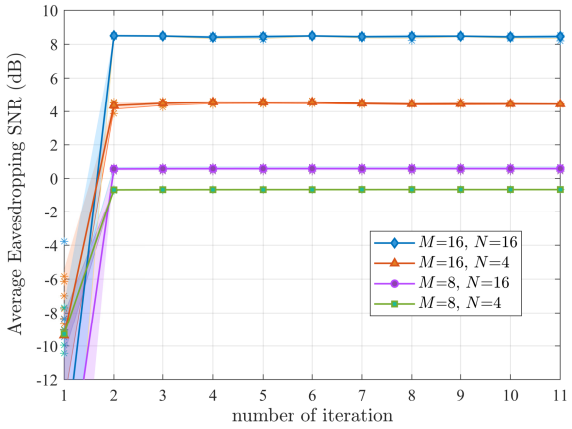


Fig. 4. Convergence shadow error plot of our proposed algorithm under different settings of M and N, given $P_{\text{S}} = P_{\text{T}} = 20$ dBW, $\beta^2_{\max} = 30$ dB, $\delta = 0.2$, $x_{\text{RIS}} = 0$ m, $y_{\text{RIS}} = 5$ m, and x_{Eve}=120 m.

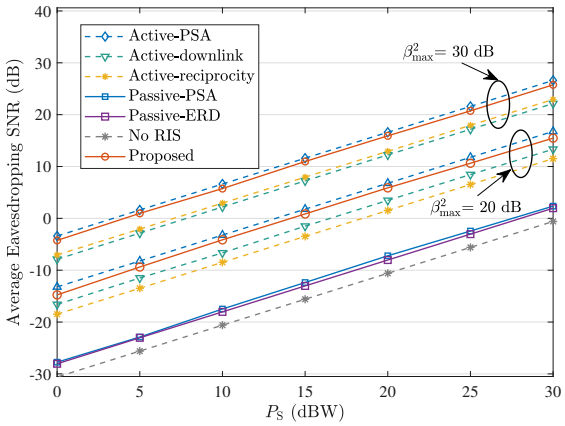


Fig. 5. The average eavesdropping SNR at Eve versus the transmit power of Alice P_{S} under different schemes, given $N = 4$, $M = 64$, $\delta = 0.2$, $x_{\text{RIS}} = 0$ m, $y_{\text{RIS}} = 5$ m, and $x_{\text{Eve}} = 120$ m.

- **Scheme 3: Active/Passive RIS-aided PSA scheme maintaining channel reciprocity (Active/Passive-reciprocity).** In this case, active/passive RIS is turned on and the reflection coefficient matrices satisfy $\boldsymbol{P}_{\text{up}} = \boldsymbol{P}^{\dagger}_{\text{down}}$. Hence, the uplink and downlink stages maintain channel reciprocity [54].
- **Scheme 4: Passive RIS-aided PSA scheme with the ERD limitation (Passive-ERD).** In this case, passive RIS is turned on with different reflection coefficients during the downlink and uplink stages, and its phase shifts are optimized by our proposed method with $\beta_{\max} = 1$.
- **Scheme 5: Active/Passive RIS-aided PSA without ERD limitation (Active/Passive-PSA).** In this case, active/passive RIS is turned on with different reflection coefficients during the uplink and downlink stages, which are optimized without any limitation on ERD detection probability. The passive-PSA scheme follows from [25].
- **Scheme 6: Traditional PSA scheme (Trad-PSA).** In this case, Eve sends the same pilots when Bob transmits the uplink pilots to Alice [55], where the jamming pilots power at Eve is denoted by P_{J}.
- **Scheme 7: Active/Passive RIS-aided PSA scheme with random reflection coefficients (Active/Passive-random).** In this case, the reflection coefficients of active/passive RIS are randomly generated within the feasible domain during the uplink and downlink stages.

From the simulations, we summarize the key findings as the following seven observations.

B. Convergence and Comparison with Benchmark Schemes

Observation 1: *The proposed optimization framework demonstrates rapid and stable convergence across diverse system configurations (cf. Fig. 4).*

The convergence behavior is shown in Fig. 4 to demonstrate the effectiveness of the simulations in the optimization phase, following the selection of the penalty weighting coefficients in the initialization stage. Fig. 4 shows the shaded error graph of our proposed algorithm, where the scattered points represent the average eavesdropping SNR values achieved by our proposed scheme of 10 simulation trials, the solid line represents the mean of them, and the shadow represents the continuous standard deviation region. Within three iterations, the mean of the average eavesdropping SNR values stabilizes and the shadow area narrows for different configurations of the number of reflecting elements M and antennas at Alice N. This performance verifies the algorithm's convergence.

Observation 2: *Conventional passive RIS-aided attacks suffer from severe performance degradation due to multiplicative fading effects (cf. Fig. 5).*

Fig. 5 shows the average eavesdropping SNR achieved by the proposed algorithm as well as the benchmark schemes versus different values of Alice's transmit power P_{S}. Following recent active RIS prototypes [30], [34], the maximum allowable power gain factor $\beta^2_{\max}$ is set to 20 dB or 30 dB. When the active RIS-aided PSA scheme is implemented without anti-ERD mechanism, the achievable eavesdropping SNR is the highest. Compared with this scheme, the performance loss of our proposed scheme is less than 1.5 dB even at the worst performance. It is observed that due to the multiplicative fading effect [34], the eavesdropping SNR achieved by the passive RIS-aided PSA schemes (with/without anti-ERD con-

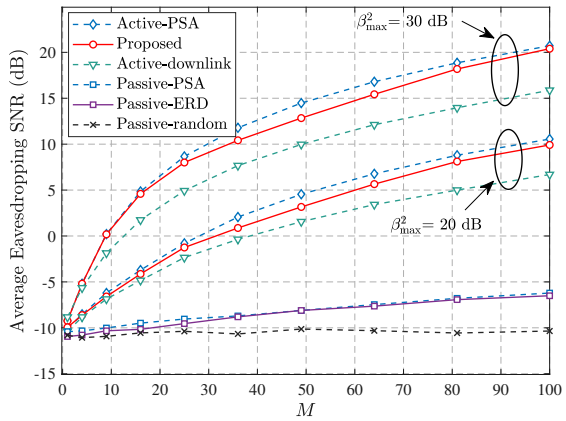


Fig. 6. Eavesdropping SNR at Eve versus the number of reflecting elements achieved by different schemes, given $N = 4$, $P_{\mathrm{T}} = P_{\mathrm{S}} = 20$ dBW, $P_{\mathrm{RIS}} = 10$ dBW, $\delta = 0.2$, $x_{\mathrm{RIS}} = 0$ m, $y_{\mathrm{RIS}} = 5$ m, and $x_{\mathrm{Eve}} = 120$ m.

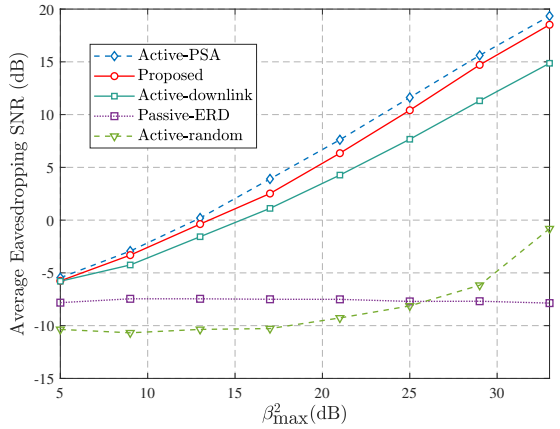


Fig. 7. Eavesdropping SNR at Eve versus the amplification factor $\beta^2_{\max}$ under different schemes, given $N = 4$, $M = 64$, $\delta = 0.2$, $x_{\mathrm{RIS}} = 0$ m, $y_{\mathrm{RIS}} = 5$ m, and $x_{\mathrm{Eve}} = 120$ m.

sideration) increases by only about 2.5 dB compared with the traditional PSA scheme. The proposed active RIS-aided covert PSA scheme achieves much better eavesdropping performance (i.e., about 16 dB gain when $\beta^2_{\max} = 20$ dB, and about 26 dB gain when $\beta^2_{\max} = 30$ dB). Compared with the active RIS-aided downlink eavesdropping scheme and active RIS-aided PSA scheme maintaining channel reciprocity, the gain of our proposed scheme remains over 2 dB, because neither scheme fully exploits the uplink stage of the TDD system.

C. Impact of System Parameters

Observation 3: *Increasing the number of the active RIS reflecting elements boosts the eavesdropping SNR (cf. Fig. 6).*

Fig. 6 illustrates the average eavesdropping SNR performance versus different number of reflecting elements M under different schemes given fixed P_{S}, P_{T} and P_{RIS}. It is noted that the average eavesdropping SNR achieved by both active and passive RIS-aided PSA schemes increases with M due to the increased DoF. However, our proposed scheme given the assigned allowable power gain factor has significantly better eavesdropping performance than the schemes with passive RIS and random reflection coefficients. Specifically, the average eavesdropping SNR achieved by passive RIS-aided PSA schemes only increases by about 4.4 dB when M varies from 1 to 100, which is less than 19.9 dB achieved by the proposed scheme when $\beta^2_{\max} = 20$ dB and 29.6 dB when $\beta^2_{\max} = 30$ dB. Even when $M = 100$, the passive RIS only helps to boost the SNR to about -6.6 dB, which is close to but still less than –6.5 dB achieved by the proposed scheme when $\beta^2_{\max} = 20$ dB and $M = 10$. On the other hand, we note that the average eavesdropping SNR loss of our proposed scheme compared with the active RIS-aided PSA shceme is only 0.6 dB, while the average gain compared to the active RIS-aided downlink eavesdropping scheme is up to 2 dB.

Observation 4: *The signal amplification capability enables substantial eavesdropping enhancement (cf. Fig. 7).*

Fig. 7 shows the average eavesdropping SNR versus the maximum allowable power gain factor $\beta^2_{\max}$ of reflecting

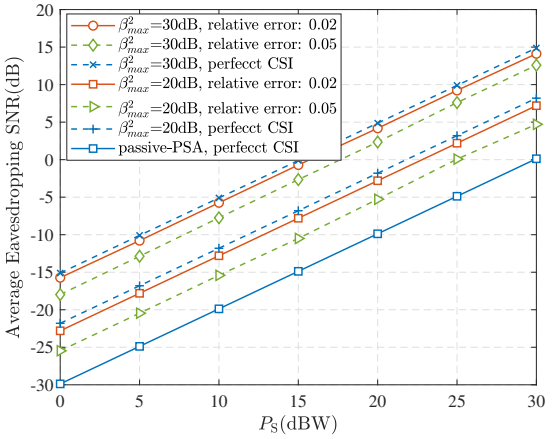


Fig. 8. Eavesdropping SNR versus relative channel estimation error variance under different RIS configurations, given $N = 4$, $M = 16$, $\delta = 0.2$, and $\beta^2_{\max} = 20/30$ dB.

elements. Notably, the SNR performance gap between our proposed scheme and the active RIS-aided PSA scheme without ERD limitation does not increase sharply. In comparison with both the active RIS-aided downlink eavesdropping scheme and passive RIS-aided PSA scheme with ERD constraint, the SNR gain of the proposed scheme continues to grow along with the increase in $\beta^2_{\max}$. Specifically, when $\beta^2_{\max}$= 33 dB, our scheme achieves SNR improvements of up to 1.9 dB and 13 dB relative to these two benchmarks, respectively. The active RIS-aided PSA scheme with random reflection coefficients exhibits even worse performance than the passive RIS-aided PSA schemes when the value of $\beta^2_{\max}$ is not very high.

Observation 5: *The proposed scheme demonstrates robustness against channel estimation errors, maintaining a consistent eavesdropping performance advantage over passive RIS-assisted PSA even under imperfect CSI conditions (cf. Fig. 8).*

As shown in Fig. 8, the proposed active RIS-assisted PSA scheme maintains a significant SNR advantage over its

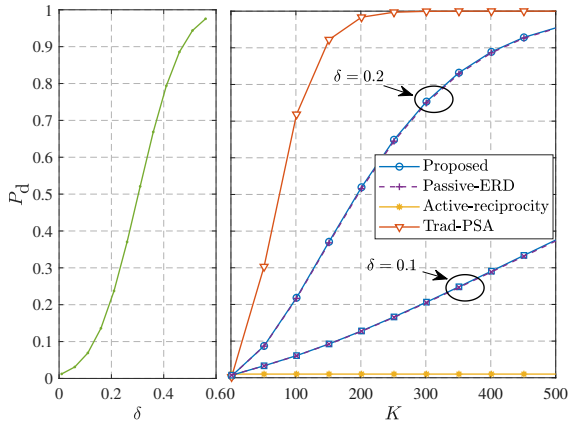


Fig. 9. The relationship between the probability of detection $P_{\rm d}$ and δ. $P_{\rm d}$ versus different number of received signal samples at Bob K under different schemes, given $N = 4$, $M = 64$, $P_{\rm T} = P_{\rm S} = 20$ dBW, $P_{\rm J} = 42$ dBW, $P_{\rm F} = 10$ dBW, $\beta^2_{\max} = 30$ dB, $\mathbb{P}_{\rm D}$ =0.01, $x_{\rm RIS} = 0$ m, $y_{\rm RIS} = 5$ m, and $x_{\rm Eve} = 120$ m.

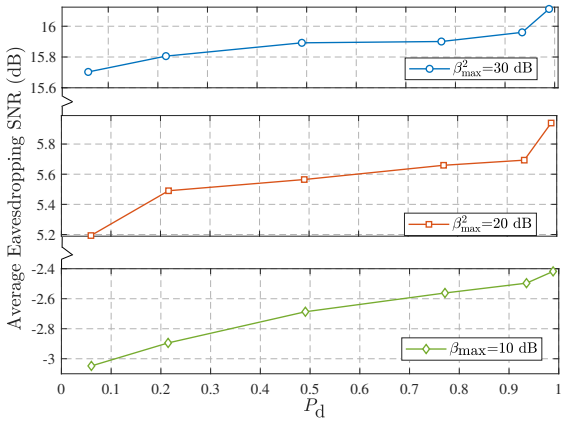


Fig. 10. Eavesdropping SNR at Eve under the different probability of detection achieved by our proposed scheme, given $\mathbb{P}_{\rm D}$ =0.01, $P_{\rm T} = P_{\rm S} = 20$ dBW, $N = 4$, $M = 64$, $\delta = 0.2$, $x_{\rm RIS} = 0$ m, $y_{\rm RIS} = 5$ m, and $x_{\rm Eve} = 120$ m.

passive counterpart across different levels of relative channel estimation errors, which is defined as the amplitude ratio of the channel estimation error and the estimated CSI. Notably, even with a relative channel estimation error variance of 0.05, the active RIS still achieves approximately 5 dB average eavesdropping SNR gain compared to the passive RIS scheme operating under perfect CSI condition. This robustness can be attributed to the active RIS's ability to compensate for channel imperfections through its amplification capability, whereas the passive RIS lacks such compensation mechanism. The results validate that the proposed scheme can effectively operate in practical scenarios where perfect CSI acquisition is challenging, though careful channel estimation remains important to maximize eavesdropping performance.

D. Covertness and Detection Analysis

Observation 6: *The proposed scheme can achieve high eavesdropping performance with low degrees of freedom and power budget (cf. Fig. 9).*

The relationship between the probability of detection $P_{\rm d}$ and δ is plotted in Fig. 9 based on the analysis in Section III. A. Fig. 9 shows the probability of detection $P_{\rm d}$ versus different numbers of received signal samples at Bob under different schemes. When Eve employs different schemes to maintain the same SNR level, it incurs different costs. Our proposed scheme requires 9 elements to achieve 0 dB eavesdropping SNR, while the passive RIS-aided PSA scheme with ERD constraint requires 324 elements to achieve 0 dB. The large-scale hardware requirements of passive RIS make it impractical for covert eavesdropping scenarios. Contrary to intuition, passive RIS has no obvious advantage over active RIS in resisting ERD. It should be emphasized that although the great performance gain brought by active RIS is at the cost of extra power consumption, only a minuscule fraction of the total power budget at the active RIS $P_{\rm RIS}$ is utilized for amplification. Because the power constraints are inactive and the allowable power gain factor constraint is active, resulting that when $P_{\rm RIS} = 10$ dBW and $\beta^2_{\max} = 30$ dB, the total power used for signal amplification at active RIS is only about 1 dBW. The power budget brings a high performance gain with low detection probability. These results fully indicate that using active RIS for PSA can significantly reduces the number of more reflecting elements to achieve a better performance gain compared with passive RIS-aided cases. As for the active/passive RIS-aided PSA schemes maintaining channel reciprocity, they can achieve the lowest detection probability, which is difficult for ERD to detect but undermines the purpose of pilot spoofing attacks and has a performance loss in eavesdropping SNR. And the traditional PSA scheme demands 42 dBW jamming power at Eve to launch a PSA to achieve an eavesdropping SNR of only -4.9 dB, and the probability of detection exceeds 70% when $K = 100$, which turns out to be a solution with more effort and less gain.

Observation 7: *The proposed scheme can achieve a relatively low probability of being detected by ERD at the cost of marginally reduced eavesdropping performance (cf. Fig. 10).*

Since the optimal performance for minimizing detection probability and maximizing eavesdropping SNR cannot be achieved simultaneously, a trade-off is necessary. As shown in Fig. 10, there exists a positive correlation between the achievable average eavesdropping SNR and the detection probability. This implies that if Eve pursues optimal eavesdropping performance, it will carry a high risk of being detected by Bob. Once it is detected, the eavesdropping activity may be exposed and Alice can apply several beamforming methods to counteract PSA, which may have a more negative impact on Eve's eavesdropping activity. Fortunately, in our case, the SNR loss to achieve lower detection probability is relatively minor, as shown in Fig. 10. Specifically, the detection probability can be as low as 0.06 at the expense of a SNR loss of less than 0.8 dB in Fig. 10, when $\delta = 0.01$. This small performance sacrifice proves worthwhile to enhance covertness.

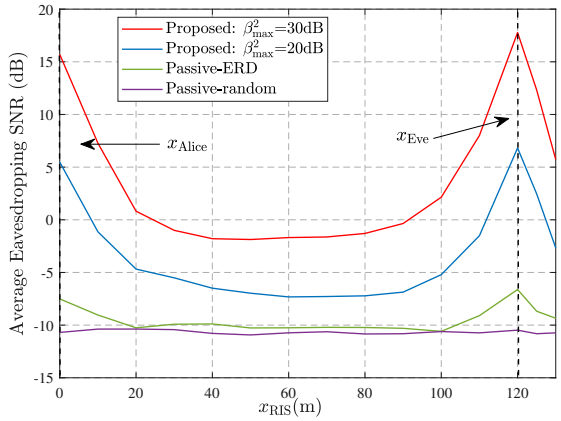


Fig. 11. Eavesdropping SNR at Eve versus the location of the RIS, where RIS is located at $(x_{\text{RIS}}, 5)$, given $N = 4$, $M = 64$, $\delta = 0.2$ and x_{Eve}=120 m.

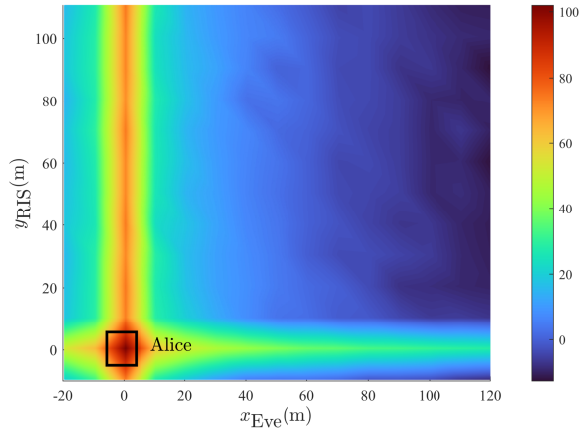


Fig. 12. Eavesdropping SNR at Eve versus the horizontal distance between Eve and Alice x_{Eve} and the vertical distance between RIS and Eve y_{RIS}, given $N = 4$, $M = 64$, $\delta = 0.2$, and $x_{\text{Eve}} = 120$ m.

E. Deployment Flexibility and Practical Insights

Observation 8: *The proposed scheme can enhance deployment flexibility to some extent while maintaining a certain eavesdropping SNR level (cf. Fig. 11).*

In Fig. 11, the average eavesdropping SNR of the RIS-aided PSA systems versus the horizontal distance between RIS and Alice is illustrated. The height of the RIS y_{RIS} is fixed at 5 m, and the RIS is deployed at different horizontal positions. For both the proposed scheme and the passive RIS-aided PSA scheme with ERD limitation, when the RIS is deployed near Eve, the systems achieve the highest SNR performance. And the SNR gain of the former compared to the latter is approximately 9.5 dB under the condition $\beta^2_{\max}$ = 20 dB, and this gain rises to 20 dB, when $\beta^2_{\max}$ = 30 dB. When the RIS is deployed close to Alice, these systems will obtain the second highest eavesdropping SNR. Notably, the lowest SNR achieved by the proposed scheme exceeds the maximum SNR attained by the passive one. This indicates that the active RIS offers greater flexibility for effective PSA implementation.

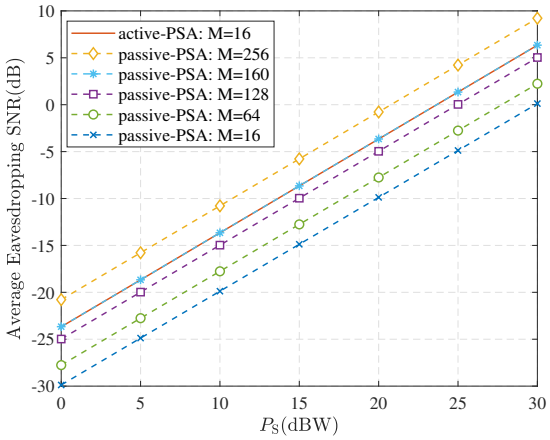


Fig. 13. Eavesdropping performance comparison between the active RIS (with fixed $M = 16$) and passive RIS with different numbers of elements.

Observation 9: *The deployment of RIS in the proposed scheme near Eve can achieve optimal eavesdropping performance, which consistent with practical condition (cf. Fig. 12).*

We deploy the active RIS above Eve as suggested by the results in Fig. 11, and it can move with Eve along the vertical direction. Fig. 12 illustrates the average eavesdropping SNR at Eve versus the horizontal distance between Eve and Alice x_{Eve} and the vertical distance between the RIS and Eve y_{RIS}. The highest eavesdropping SNR is achieved when $y_{\text{RIS}} = 0$ and $x_{\text{Eve}} = x_{\text{Alice}}$. The former condition is easy to achieve because the RIS can be controlled by Eve, whereas the latter is hard to realize as Alice is the adversary. Considering the need for deployment concealment, when Eve positions the RIS away from Alice, the closer the RIS is to Eve in the vertical direction, the higher the eavesdropping SNR is. When the height of RIS exceeds 10 m, the SNR drops rapidly to a low level. Hence, it is better to deploy the RIS close to Eve, and Eve is better to move closer to Alice in the actual eavesdropping scenario.

Observation 10: *The proposed scheme achieves a remarkable equivalent array gain compared with passive RIS, offering a substantial reduction in physical size for comparable performance, which is a decisive advantage for practical deployments (cf. Fig. 13).*

To provide deeper insight into the impact of the active RIS's additional power budget, we compare the proposed scheme (with fixed $M = 16$) against passive RIS schemes with different numbers of elements ($M = 16, 64, 128, 160, 256, 400$) in Fig. 13. The simulations demonstrate that even with 8 times more passive elements ($M = 128$), the passive RIS's eavesdropping performance remains approximately 1.3 dB worse than that of the active RIS when $\beta^2_{\max} = 20$ dB. It requires about ten times the number of elements ($M = 160$) for the passive RIS to achieve a comparable eavesdropping performance. This quantifies an equivalent array gain of approximately 10 times for the active RIS with 10 dBW power budget. This gain translates into a critical practical advantage: the proposed scheme can achieve target performance with a physical size that is only one-tenth of that required by

a passive RIS. Given that the increase in the number of passive RIS elements implies a significant expansion in the required area, the active RIS effectively translates its power consumption into a substantial reduction in physical size and a dramatic improvement in deployment flexibility, making it highly suitable for covert eavesdropping applications.

VI. Conclusion

This paper established an active RIS-aided covert PSA scheme. It demonstrated that an active RIS can be exploited to launch a powerful and covert PSA, breaching the security of TDD wireless systems. The main findings are summarized as follows. First, the amplification capability of the active RIS provides a substantial eavesdropping advantage, achieving extra SNR gains over passive RIS-based attacks. Second, the simulations reveal and quantify a key trade-off between eavesdropping performance and covertness. The proposed joint optimization framework effectively balances this trade-off, delivering high SNR while maintaining a low detection probability under energy ratio detection. Third, the active RIS exhibits superior deployment flexibility, achieving performance comparable to a passive RIS with ten times more elements, significantly reducing aperture size for the attacker. Furthermore, the sensitivity analysis confirms the robustness of the proposed scheme to imperfect CSI, as the inherent amplification of the active RIS provides resilience to estimation uncertainty. Overall, this study highlights that while the active RIS is promising for enhancing communication performance, it also introduces a new class of stealthy and efficient security threats, underscoring the urgent need for practical defense strategies and attack-aware system designs.

Appendix

Lemma 1 [56]: if $x \sim \mathcal{N}\left(\mu_x, \sigma_x^2\right)$ and $y \sim \mathcal{N}\left(\mu_y, \sigma_y^2\right)$ are two independent Gaussian random variables, the probability density function of $t = \frac{x}{y}$ is

$$f(t) = \frac{b(t)c(t)}{\sqrt{2\pi}\sigma_x\sigma_y a^3(t)}\left[2\Phi\left(\frac{b(t)}{a(t)}\right) - 1\right] + \frac{1}{a^2(t)\pi\sigma_x\sigma_y} e^{-\frac{1}{2}\left(\frac{\mu_x^2}{\sigma_x^2} + \frac{\mu_y^2}{\sigma_y^2}\right)} \tag{62}$$

where $a(t) = \sqrt{\frac{t^2}{\sigma_x^2} + \frac{1}{\sigma_y^2}}$, $b(t) = \frac{\mu_x}{\sigma_x^2}t + \frac{\mu_y}{\sigma_y^2}$, and $c(t) = \exp\left\{\frac{1}{2}\left[\frac{b^2(t)}{a^2(t)} - \left(\frac{\mu_x^2}{\sigma_x^2} + \frac{\mu_y^2}{\sigma_y^2}\right)\right]\right\}$. We set the test statistic as $T = \frac{Q_2}{Q_1}$, where $Q_1 \sim \mathcal{N}(\mu_1, \sigma_1^2)$ and $Q_2 \sim \mathcal{N}(\mu_2, \sigma_2^2)$. Under $\mathcal{H}_0$, we have $\mu_1 = \mu_2$, $\frac{b(T)}{a(T)} = \frac{KT+\tau}{\sqrt{KT^2+\tau}}$, $\sigma_1\sigma_2\, a^2(T) = \sqrt{\tau K}\left(KT^2 + \tau\right)$, and $c(T) = \exp\left\{\frac{1}{2}\left[\frac{b^2(T)}{a^2(T)} - \tau - K\right]\right\}$.

For sufficient τ and K, the test statistic T under $\mathcal{H}_0$ can be approximated as a random variable with the PDF of $f_0(T)$, which is not related to legitimate channel or illegitimate channel but dependent on the numbers of samples τ and K. The PDF under $\mathcal{H}_0$ can be expressed as

$$f_0(T) = \frac{\left(KT+\tau\right)\sqrt{\tau K}}{\sqrt{2\pi}\left(KT^2+\tau\right)^{\frac{3}{2}}} e^{\frac{1}{2}\left[\frac{(KT+\tau)^2}{KT^2+\tau} - \tau - K\right]} \times \left[2\Phi\left(\frac{KT+\tau}{\sqrt{KT^2+\tau}}\right) - 1\right] + \frac{\sqrt{\tau K}}{\pi\left(KT^2+\tau\right)} e^{-\frac{1}{2}(\tau+K)} \tag{63}$$

where $\Phi(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} e^{-u^2/2} du$.

Under $\mathcal{H}_1$, the PDF of T can be expressed as

$$f_1(T) = \frac{\sqrt{\tau K}\, b(T)c(T)}{\sqrt{2\pi}\mu_1\mu_2 a^3(T)}\left[2\Phi\left(\frac{b(T)}{a(T)}\right) - 1\right] + \frac{\sqrt{\tau K}}{a^2(T)\pi\mu_1\mu_2} e^{-\frac{1}{2}(\tau+K)} \tag{64}$$

where $a(T) = \sqrt{\frac{KT^2}{\mu_2^2} + \frac{\tau}{\mu_1^2}}$, $b(T) = \frac{KT}{\mu_2} + \frac{\tau}{\mu_1}$, and $c(T) = \exp\left\{\frac{1}{2}\left[\frac{b^2(T)}{a^2(T)} - \tau - K\right]\right\}$.

The probability of false alarm $\mathbb{P}_{\mathrm{F}}$ can be illustrated as

$$\mathbb{P}_{\mathrm{F}} = Pr(T < \tilde{\gamma} | H_0) = \int_{-\infty}^{\tilde{\gamma}} f_0(x) dx. \tag{65}$$

Given a target of $\mathbb{P}_{\mathrm{F}}$, we can calculate a corresponding detection threshold γ. Then the probability of detection $\mathbb{P}_{\mathrm{D}}$ can be written as

$$\mathbb{P}_{\mathrm{D}} = Pr(T < \tilde{\gamma} | H_1) = \int_{-\infty}^{\tilde{\gamma}} f_1(x) dx. \tag{66}$$

We assume that the sample numbers at Alice τ is very large, i.e., $\tau \to \infty$. The estimation error $\tilde{\boldsymbol{\epsilon}}$ becomes very small and negligible, i.e., $\tilde{\boldsymbol{\epsilon}} \to 0$. Hence, the expectations can be respectively expressed as

$$\mu_1 = \begin{cases} \left|\frac{\hat{\boldsymbol{h}}^\dagger}{\|\hat{\boldsymbol{h}}\|}\boldsymbol{h}_{\mathrm{B}}\right|^2 P_{\mathrm{T}} + \sigma_{\mathrm{A}}^2 \to \mathcal{H}_0 \\ \left|\frac{\hat{\boldsymbol{h}}^\dagger}{\|\hat{\boldsymbol{h}}\|}\left(\boldsymbol{h}_{\mathrm{B}} + \boldsymbol{H}_{\mathrm{A}}\boldsymbol{P}_{\mathrm{up}}\boldsymbol{h}_{\mathrm{R}}\right)\right|^2 P_{\mathrm{T}} + \tilde{\sigma}_{\mathrm{A}}^2 \to \mathcal{H}_1 \end{cases} \tag{67}$$

$$\mu_2 = \begin{cases} \left|\boldsymbol{h}_{\mathrm{B}}^\dagger \frac{\hat{\boldsymbol{h}}}{\|\hat{\boldsymbol{h}}\|}\right|^2 P_{\mathrm{S}} + \sigma_{\mathrm{B}}^2 \to \mathcal{H}_0 \\ \left|\left(\boldsymbol{h}_{\mathrm{B}}^\dagger + \boldsymbol{h}_{\mathrm{R}}^\dagger \boldsymbol{P}_{\mathrm{down}} \boldsymbol{H}_{\mathrm{A}}^\dagger\right)\frac{\hat{\boldsymbol{h}}}{\|\hat{\boldsymbol{h}}\|}\right|^2 P_{\mathrm{S}} + \tilde{\sigma}_{\mathrm{B}}^2 \to \mathcal{H}_1 \end{cases} \tag{68}$$

According to the central limit theorem (CLT), Q_1 and Q_2 can be approximated by a Gaussian distributed random variable if τ and K are sufficiently large, i.e.,

$$Q_1 \sim \mathcal{N}(\mu_1, \sigma_1^2) \tag{69}$$

$$Q_2 \sim \mathcal{N}(\mu_2, \sigma_2^2) \tag{70}$$

with μ_k and σ_k^2 being the expectation and variance, respectively, $k \in \{1, 2\}$.

References

[1] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas, J. S. Thompson, E. G. Larsson, M. D. Renzo, W. Tong, P. Zhu, X. Shen, H. V. Poor, and L. Hanzo, "On the road to 6g: Visions, requirements, key technologies, and testbeds," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 905–974, Secondquarter 2023.

[2] B. He, Z. Chen, J. Luo, C. Liu, S. Wang, F. Wang, and T. Q. Quek, "Towards secure semantic transmission in the era of genai: A diffusion-based framework," *arXiv preprint arXiv:2505.05724*, 2025.

[3] C. Wang, Z. Li, K.-K. Wong, R. Murch, C.-B. Chae, and S. Jin, "Ai-empowered fluid antenna systems: Opportunities, challenges, and future directions," *IEEE Wireless Commun.*, Oct. 2024.

[4] Y. Guo, J. Luo, F. Wang, H. Ding, S. Wang, and Z. Xu, "Dual-end fluid antennas for robust anti-jamming in low-altitude air-ground communications," *arXiv preprint arXiv:2509.02260*, 2025.

[5] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6g: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, Fourthquarter 2021.

[6] B. He, X. Zhou, and T. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *ZTE Commun.*, vol. 11, no. 3, pp. 11–19, Sep. 2013.

[7] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[8] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Physical-layer security in tdd massive mimo," *IEEE Trans. Inf. Theory*, vol. 64, no. 11, pp. 7359–7380, Nov. 2018.

[9] K.-W. Huang, H.-M. Wang, Y. Wu, and R. Schober, "Pilot spoofing attack by multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6433–6447, Oct. 2018.

[10] H.-M. Wang and S.-D. Wang, "Cooperative pilot spoofing in mu-mimo systems," *IEEE Wireless Commun. Lett.*, vol. 9, no. 11, pp. 1956–1960, Nov. 2020.

[11] B. Akgun, M. Krunz, and O. O. Koyluoglu, "Vulnerabilities of massive mimo systems to pilot contamination attacks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1251–1263, May 2019.

[12] W. Zhang, H. Lin, and R. Zhang, "Detection of pilot contamination attack based on uncoordinated frequency shifts," *IEEE Trans. Commun.*, vol. 66, no. 6, pp. 2658–2670, Jun. 2018.

[13] F. Choudhury, A. Ikhlef, and M. Debbah, "Dnn-based detection of pilot spoofing attacks in massive mimo networks with phase noise," in *Proc. IEEE Middle East Conf. Commun. Netw. (MECOM)*, May 2024, pp. 235–240.

[14] H.-M. Wang, K.-W. Huang, and T. A. Tsiftsis, "Multiple antennas secure transmission under pilot spoofing and jamming attack," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 860–876, Jun. 2018.

[15] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.

[16] C. Pan, H. Ren, K. Wang, J. F. Kolb, M. Elkashlan, M. Chen, M. D. Renzo, Y. Hao, J. Wang, A. L. Swindlehurst, X. You, and L. Hanzo, "Reconfigurable intelligent surfaces for 6g systems: Principles, applications, and research directions," *IEEE Commun. Mag.*, vol. 59, no. 6, pp. 14–20, Jun. 2021.

[17] J. Luo, S. Wang, and B. He, "Large-scale aerial reconfigurable intelligent surface-aided robust anti-jamming transmission," *arXiv preprint arXiv:2509.10280*, 2025.

[18] F. Naeem, M. Ali, G. Kaddoum, C. Huang, and C. Yuen, "Security and privacy for reconfigurable intelligent surface in 6g: A review of prospective applications and challenges," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 1196–1217, Jun. 2023.

[19] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, M. D. Renzo, and N. Al-Dhahir, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1546–1577, Thirdquarter 2021.

[20] J. Luo, F. Wang, and S. Wang, "Secure two-way transmission via autonomous reconfigurable intelligent surface," *IEEE Wireless Commun. Lett.*, vol. 12, no. 2, pp. 262–266, Feb. 2023.

[21] W. Hao, J. Li, G. Sun, C. Huang, M. Zeng, O. A. Dobre, and C. Yuen, "Robust security energy efficiency optimization for ris-aided cell-free networks with multiple eavesdroppers," *IEEE Trans. Commun.*, vol. 72, no. 12, pp. 7401–7416, Dec. 2024.

[22] H. Niu, X. Lei, J. An, L. Zhang, and C. Yuen, "On the efficient design of stacked intelligent metasurfaces for secure siso transmission," *IEEE Trans. Inf. Forensics Security*, vol. 20, pp. 60–70, Jan. 2025.

[23] J. Luo, F. Wang, S. Wang, H. Wang, and D. Wang, "Reconfigurable intelligent surface: Reflection design against passive eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 20, no. 5, pp. 3350–3364, May 2021.

[24] K.-W. Huang and H.-M. Wang, "Intelligent reflecting surface aided pilot contamination attack and its countermeasure," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 345–359, Jan. 2021.

[25] J. Yang, X. Ji, F. Wang, K. Huang, and L. Guo, "A novel pilot spoofing scheme via intelligent reflecting surface based on statistical csi," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12 847–12 857, Dec. 2021.

[26] S. S. Acharjee and A. Chattopadhyay, "Controller manipulation attack on reconfigurable intelligent surface aided wireless communication," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2022, pp. 1247–1252.

[27] K.-W. Huang, H.-M. Wang, and L. Yang, "Smart jamming using reconfigurable intelligent surface: Asymptotic analysis and optimization," *IEEE Trans. Wireless Commun.*, vol. 23, no. 1, pp. 637–651, Jan. 2024.

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

[29] M. H. Khoshafa, T. M. N. Ngatched, M. H. Ahmed, and A. R. Ndjiongue, "Active reconfigurable intelligent surfaces-aided wireless communication system," *IEEE Commun. Lett.*, vol. 25, no. 11, pp. 3699–3703, Nov. 2021.

[30] G. S. Bhatia, Y. Corre, T. Tenoux, and M. D. Renzo, "Exploring ris coverage enhancement in factories: From ray-based modeling to use-case analysis," in *Proc. 18th Eur. Conf. Antennas Propag. (EuCAP)*, Mar. 2024, pp. 1–5.

[31] H. Niu, Y. Xiao, X. Lei, L. Dan, W. Xiang, and C. Yuen, "Reconfigurable intelligent surface-assisted passive beamforming attack," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 8236–8247, Jan. 2024.

[32] J. Dang, Z. Zhang, and L. Wu, "Joint beamforming for intelligent reflecting surface aided wireless communication using statistical csi," *China Commun.*, vol. 17, no. 8, pp. 147–157, Aug. 2020.

[33] R. Song, H. Yin, Z. Wang, T. Yang, and X. Ren, "Modeling, design, and verification of an active transmissive ris," *IEEE Trans. Antennas Propag.*, vol. 72, no. 12, pp. 9239–9250, Dec. 2024.

[34] Z. Zhang, L. Dai, X. Chen, C. Liu, F. Yang, R. Schober, and H. V. Poor, "Active ris vs. passive ris: Which will prevail in 6g?" *IEEE Trans. Commun.*, vol. 71, no. 3, pp. 1707–1725, Mar. 2023.

[35] K. Liu, Z. Zhang, L. Dai, S. Xu, and F. Yang, "Active reconfigurable intelligent surface: Fully-connected or sub-connected?" *IEEE Commun. Lett.*, vol. 26, no. 1, pp. 167–171, Jan. 2022.

[36] P. Liu, Y. Li, W. Cheng, X. Dong, and L. Dong, "Active intelligent reflecting surface aided rsma for millimeter-wave hybrid antenna array," *IEEE Trans. Commun.*, vol. 71, no. 9, pp. 5287–5302, Sep. 2023.

[37] Z. Qu, J. Luo, S. Wang, W. Zhang, and A. Zhou, "Generalized code index modulation based on chaotic sequence for anti-interception," in *2023 IEEE 23rd International Conference on Communication Technology (ICCT)*, 2023, pp. 1297–1301.

[38] S. Luo, M. E. Garbelini, S. Chattopadhyay, and J. Zhou, "Sni5gect: a practical approach to inject anrchy into 5g nr," in *Proc. 34th USENIX Conf. Security Symp.*, ser. SEC '25, Aug. 2025.

[39] J. Yang, H. Lee, and J. Choi, "Robust transmission design for active ris-aided systems," *IEEE Trans. Veh. Technol.*, vol. 74, no. 7, pp. 11 591–11 596, Jul. 2025.

[40] Y. Omid, S. M. Shahabi, C. Pan, Y. Deng, and A. Nallanathan, "Low-complexity robust beamforming design for irs-aided miso systems with imperfect channels," *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1697–1701, May 2021.

[41] S. Hong, C. Pan, H. Ren, K. Wang, K. K. Chai, and A. Nallanathan, "Robust transmission design for intelligent reflecting surface-aided secure communication systems with imperfect cascaded csi," *IEEE Trans. Wireless Commun.*, vol. 20, no. 4, pp. 2487–2501, Apr. 2021.

[42] A. Bansal, N. Agrawal, K. Singh, C.-P. Li, and S. Mumtaz, "Ris selection scheme for uav-based multi-ris-aided multiuser downlink network with imperfect and outdated csi," *IEEE Trans. Commun.*, vol. 71, no. 8, pp. 4650–4664, Aug. 2023.

[43] A. Taha, M. Alrabeiah, and A. Alkhateeb, "Enabling large intelligent surfaces with compressive sensing and deep learning," *arXiv preprint arXiv:1904.10136*, Apr. 2019. [Online]. Available: https://arxiv.org/abs/1904.10136

[44] S. Zhang and R. Zhang, "Capacity characterization for intelligent reflecting surface aided mimo communication," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1823–1838, Aug. 2020.

[45] A. Taha, M. Alrabeiah, and A. Alkhateeb, "Enabling large intelligent surfaces with compressive sensing and deep learning," *arXiv preprint arXiv:1904.10136*, Apr. 2019. [Online]. Available: https://arxiv.org/abs/1904.10136

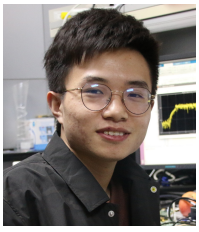
[46] J. Rodriguez-Fernandez, N. Gonzalez-Prelcic, and R. W. Heath, "Position-aided compressive channel estimation and tracking for millimeter wave multi-user mimo air-to-air communications," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Kansas City, MO, USA, May 2018, pp. 1–6.

[47] X. Ren, W. Chen, and M. Tao, "Position-based compressed channel estimation and pilot design for high-mobility ofdm systems," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1918–1929, May 2015.

[48] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.
[49] 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 J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 966–981, Oct. 2014.
[50] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for mimo wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.
[51] J. Borwein and A. Lewis, *Convex Analysis and Nonlinear Optimization: Theory and Examples*, 2nd ed. Springer, Jan. 2006.
[52] Z. Chu, W. Hao, P. Xiao, and J. Shi, "Intelligent reflecting surface aided multi-antenna secure transmission," *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 108–112, Jan. 2020.
[53] L. Dong, H.-M. Wang, and J. Bai, "Active reconfigurable intelligent surface aided secure transmission," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 2181–2186, Feb. 2022.
[54] W. Tang, X. Chen, M. Z. Chen, J. Y. Dai, Y. Han, S. Jin, Q. Cheng, G. Y. Li, and T. J. Cui, "On channel reciprocity in reconfigurable intelligent surface assisted wireless networks," *IEEE Wireless Commun.*, vol. 28, no. 6, pp. 94–101, Dec. 2021.
[55] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.
[56] D. V. Hinkley, "On the ratio of two correlated normal random variables," *Biometrika*, vol. 56, no. 3, pp. 635–639, Dec. 1969.

Junshan Luo received the B.Sc., the M.Sc., and the Ph.D. degrees in information and communications engineering from the National University of Defense Technology, Changsha, China, in 2014, 2016, and 2021, respectively. He is currently an Associate Professor with the College of Electronic Science and Technology, National University of Defense Technology, China. His current research interests are in reconfigurable intelligent surface, fluid antenna, anti-jamming communications, and physical layer security. He was a recipient of the Exemplary Reviewer for IEEE COMMUNICATIONS LETTERS in 2020 and 2021.

Zhengfei Qu received the B.Sc. degree in communications engineering from the National University of Defense Technology, Changsha, China, in 2022, where she is pursuing the Ph.D. degree in information and communications engineering with the College of Electronic Science and Technology. She is currently a Visiting Ph.D. student with Politecnico di Torino, Turin, Italy. Her current research interests are in reconfigurable intelligent surface, physical layer security, and signal processing for wireless communications.



Boxiang He received the B.Eng. and Ph.D. degrees from the School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China, in 2018 and 2024, respectively.,He was a visiting student with the Singapore University of Technology and Design, Singapore, from 2023 to 2024. He is currently a Research Fellow with the College of Electronic Science and Technology, National University of Defense Technology, Changsha, China. His current research interests include signal identification, physical-layer security, and signal processing.

Shilian Wang received his B.S. degree and Ph.D. degree in information and communication engineering from National University of Defense Technology, in 1998 and 2004, respectively. Since 2004, he has been with the School of Electronic Science at National University of Defense Technology, as a lecturer, an associate professor and a professor. From 2008 to 2009, he was a visiting scholar with the Department of Electronic and Electrical Engineering at Columbia University (CU), New York. His research interests are in wireless communications and signal processing, specifically in the spread spectrum and the low-probability of interception communications.

Giorgio Taricco (Fellow, IEEE) received the Laurea degree (cum laude) in ingegneria elettronica from Politecnico di Torino, Italy, in 1985. He was a Researcher with Italian Telecom Laboratories (CSELT), from 1985 to 1987, where he was involved in the design process of the GSM mobile telephony standard (channel coding). Since 1991, he has been with the Department of Electronics and Telecommunications (DET), Politecnico di Torino, as an Assistant Professor, where he has been a Full Professor since 2010. In 1996, he was a Research Fellow with ESA/ESTEC, The Netherlands. He has coauthored more than 200 papers published in international journals and international conferences, several book chapters, and three international patents. His research interests include information theory, error-control coding, multiuser detection, space-time coding, MIMO communications, cognitive radio networks, sensor networks, the IoT satellite networks, and MIMO relay channels. He was a co-recipient of the Best Paper Awards from the WPMC 2001 Conference and the Journal of Communications and Networks (Special Issue on Coding and Signal Processing for MIMO Systems), in 2003. He was on the ISI highly cited researcher list in the category of computer science, from 2008 to 2013. He has participated in several committees of IEEE conferences (as a treasurer). He has been an Associate Editor of the IEEE Communications Letters, the IEEE Transactions on Information Theory, and the Journal on Communications and Networks. He was also a Senior Associate Editor of the IEEE Wireless Communications Letters. He is currently an Associate Editor of Entropy.

Chau Yuen (S02-M06-SM12-F21) received the B.Eng. and Ph.D. degrees from Nanyang Technological University, Singapore, in 2000 and 2004, respectively. He was a Post-Doctoral Fellow with Lucent Technologies Bell Labs, Murray Hill, in 2005. From 2006 to 2010, he was with the Institute for Infocomm Research, Singapore. From 2010 to 2023, he was with the Engineering Product Development Pillar, Singapore University of Technology and Design. Since 2023, he has been with the School of Electrical and Electronic Engineering, Nanyang Technological University. Currently he is Provost's Chair in Wireless Communications, Assistant Dean in Graduate College, and Cluster Director for Sustainable Built Environment at ER@IN.

Dr. Yuen received IEEE Communications Society Leonard G. Abraham Prize (2024), IEEE Communications Society Best Tutorial Paper Award (2024), IEEE Communications Society Fred W. Ellersick Prize (2023), IEEE Marconi Prize Paper Award in Wireless Communications (2021), IEEE APB Outstanding Paper Award (2023), and EURASIP Best Paper Award for JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING (2021). He is listed as Top 2% Scientists by Stanford University, and also a Highly Cited Researcher by Clarivate Web of Science from 2022.