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

Jie Yang, Xinsheng Ji, Feihu Wang, Kaizhi Huang, You Zhou

***Abstract*—Pilot spoofing attack brings challenges to the physical layer secure transmission. However, since the inherent characteristics of wireless environment have not changed, active eavesdropping can be detected based on prior information. Intelligent reflecting surface (IRS), with the real-time programmable characteristics for wireless environment, provides new possibilities for effective pilot spoofing. In this paper, the IRS is deployed near the legitimate users and the control strategy is embeded into the legitimate communication process under time-division duplex (TDD) mode to assist eavesdroppers to implement pilot spoofing. By designing different phase shifts at the IRS during the uplink phase and downlink phase, the channel reciprocity between uplink and downlink disappears, and thus secure beamforming vector is biased towards the eavesdropper. Furthermore, in order to obtain more information, the average secrecy rate minimization based on statistical channel state information is established by carefully designing the phase shifts. The formulated problem is non-trivial to solve. By using alternating optimization and Charnes-Cooper transformation technique, the original problem is transformed into convex form and a sub-optimal solution is achieved. Finally, simulation results show that our proposed scheme poses serious secure threat without any energy footprint especially for TDD systems.**

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

I. Introduction

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

However, there exist some shortcomings for this technology, which may be utilized by malicious users. As we know, accurate channel state information (CSI) is an essential prerequisite in designing SB vectors. Different from passive eavesdropper, which only wiretaps information, active eavesdropper can attack the channel training phase of legitimate links to improve wiretapping performance, which is a serious threat especially for time-division duplex (TDD) systems. In a TDD system, the process of obtaining downlink CSI is briefly descripted as follows: the legitimate receiver (LR) transmits pilot symbols to the legitimate transmitter (LT) during uplink training phase. Then, in order to reduce the interaction overhead, the estimated uplink channel is regarded as the downlink channel by exploiting reciprocity at a coherent time, and SB vector based on this CSI is designed and utilized to transmit the confidential message to the LR. If an eavesdropper attacks the uplink training phase by transmitting the same pre-designed training sequence as the LR, the estimated channel obtained at the LT is a weighted combination of the legitimate channel and the wiretap channel. Based on this faked CSI, the beam formed by the LT will be oriented towards both the LR and the eavesdropper, which results in severe signal leakage. In [2], the authors first propose this active eavesdropping method and name it as pilot spoofing attack (PSA). Then its severe consequences are analyzed. In [3], a PSA approach carried out by multiple eavesdroppers is investigated in a TDD system. And during the uplink channel training phase, multiple Eves collaboratively impair the channel acquisition of the legitimate link, aiming at maximizing the wiretapping signal-to-noise ratio in the subsequent downlink data transmission phase. Two different scenarios are investigated: one is that the BS is unaware of the PSA, and the other is that the BS attempts to detect the presence of the PSA. Moreover, the PSA detection scheme is also investigated. In [4], the authors formulats the PSA detection as a binary hypothesis testing problem, and the likelihood ratio based on the energy of the received signal is used as the detection statistic. In [5], under the same pilot allocation protocol, the authors respectively propose a random channel training scheme and a jamming-resistant scheme employing an unused pilot sequence to combat the pilot contamination attack and maintain secure communication. The reasons that these detection methods work rely on a key assumption: the received combination pilot signal contains the channel characteristics of eavesdroppers, which LT can use some methods to distinguish. Further, from the internal reasons, the conventional pilot spoofing attack does not really change the reciprocity of the uplink and downlink channels. To fundamentally avoid being detected by legitimate users, a novel attack method which can reconstruct the wireless communication environment in real time and change the reciprocity characteristics should be considered.

This work was supported in part by the National Natural Science Foundation of China under Grant 61801435 and Grant 61701538, and in part by China Postdoctoral Science Foundation 2019M663994.(Corresponding author: Kaizhi Huang);

J. Yang, X. Ji, F. Wang, K. Huang, Y. Zhou are with the School of Information Engineering University, Zhengzhou, 450002, China.(e-mails: yj_csu@126.com, jxs@ndsc.com.cn, fhw_wang@sina.com, huangkaizhi@tsinghua.org.cn, emailzhouyou@sina.com.

Meanwhile, Intelligent reflecting surface (IRS), which can reconstruct wireless propagation environment, has been viewed as an appealing technology for 6G networks [6]. IRS is a planar array consisting of masssive number of low-cost passive elements and each element can tune the reflection coefficients on the incident signal independently whereby the reflected signal can be enhanced or weakened at given users. Besides, the state switching time at each unit can be low to the order of microsecond (μs) [7], which is much smaller than the typical channel coherence time that is on the order of millisecond (ms), and thus IRS is well suited for mobile applications for time-varying channels. Therefore, IRS has been investigated in various applications such as coverage extension [8], physical layer security [9] [10], energy efficiency improvement [11], and so on. However, few literatures consider reverse application, where IRS is utilized for enhancing eavesdropping. In [12], the IRS is utilized as a jammer to sabotage the legitimate communication system without any energy footprint. While, these works just simply consider deploying the IRS around the LT or the LR, and tune the phase shifts according to instantaneous CSI.

Actually, due to the openness of the communication protocol, the control strategy of the IRS can be seamlessly embedded in the protocol and change the reciprocity of the uplink and downlink channels, which may bring new threat to legal communication. Moreover, with massive low-cost passive reflecting elements, more design parameters brought by IRS can be utilized to moderate link quality and the problem is usually intractable. To the best of our knowledge, by far there is few work that considers IRS-aided pilot spoofing scenario. Motived by above, a novel adverse application of IRS is investigated for enhancing eavesdropping performance. The control protocol of the IRS is designed to make LT misestimate the channel during uplink phase and the eavesdropper overhear signal more clearly during downlink phase. Consequently, this novel active attack can lead to information leakage without leaving any energy footprint, which is very difficult to detect and defend. Our main contributions are summarized as follows:

1) A novel pilot attack scheme in a three-node model with the aid of the IRS is proposed. In this model, the IRS is covertly deployed the LT and remotely controlled by the eavesdropper. During uplink phase and downlink phase, the phase shifts at the IRS are different, and thus the downlink CSI estimated by the LT is different from the actual downlink CSI, the designed SB vector will be shifted from LR. Furthermore, by carefully predesigning the phase shifts, more information can be leaked to the eavesdropper.
2) The average secrecy rate minimization problem based on statistical CSI is formulated and solved. Since instantaneous information is difficult to obtain for eavesdroppers, the average secrecy rate is considered as the performance metric and the optimization problem is established by jointly designing phase shifts at the uplink phase and downlink phase. First, the approximate expression of the problem is derived, then non-convex problem is efficiently solved by exploiting alternating optimization algorithm and Charnes-Cooper transformation method. Moreover, the computational complexity is analyzed.
3) Numerical results show the impact of parameters on system performance, such as the transmit power, the transmit antennas and the Rician factor. Compared with the existing pilot spoofing schemes, our proposed scheme can significantly degrade security performance. As the number of transmit antennas increases, security threat brought by IRS will not be weakened. If the eavesdropper belongs to a malicious user in the system, more serious security threat will be brought due to more accurate CSI. Moreover, when the number of low cost reflecting units increases, the secresecurity performance can be further cut down, which illustrates the advantages of the solution.

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

II. PROPOSAL AND ANALYSIS OF THE SCHEME

A. The proposal of the Scheme

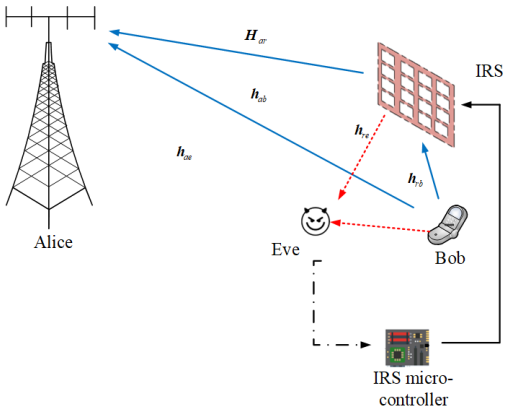
As depicted in Fig.1, we consider a three-node point-to-point communication model, where the transmitter Alice communicates with the receiver Bob under TDD mode, and the eavesdropper Eve tries to overhear the signal. Alice is equipped with M_a antennas, where $M_a > 1$, while Bob and Eve is equipped with single antenna, respectively. Meanwhile, one IRS is deployed near Alice and is controlled remotely by Eve through a private wireless channel. The IRS is composed of N reflecting units and $\Phi = \mathrm{diag}(\mathrm{e}^{\mathrm{j}\theta_1}, \mathrm{e}^{\mathrm{j}\theta_2}, \cdots \mathrm{e}^{\mathrm{j}\theta_\mathrm{N}})$ is denoted as the reflection coefficient matrix at the IRS, where $\theta_n \in [0, 2\pi]$ denotes the phase shift on the incident signal at its nth element. Suppose that there exist some low-power sensors integrated into the IRS and the reflected CSI can be probed by these sensors [13] [14]. Different from [2], where Eve sends jamming pilot sequence during the uplink pilot phase to induce Alice to obtain the false uplink CSI, in this model, Eve controls the IRS remotely to change its phase shifts several times in a coherent time to conduct pilot spoofing attack. The specific implementation process is shown in Fig.2.

1)Silent stage

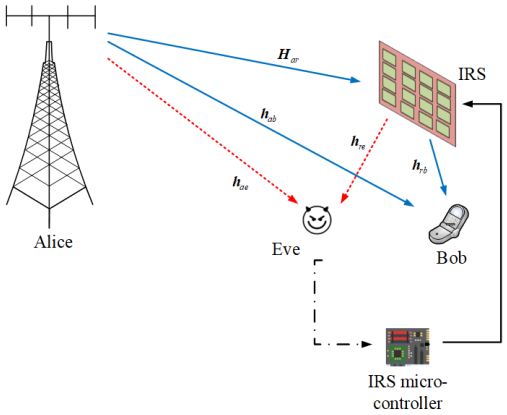
Alice and Bob communicate normally, while Eve keeps silent and only tries to establish synchronization with legitimate users. Although the received signal by Eve is too weak to decode information, timing synchronization is easy to be found by Eve after a long time capture due to the open communication protocol.

2)Eavesdropping stage

①Before Bob begins to send the uplink pilot, Eve turns on the IRS and sets the uplink phase shifts at the IRS. Then during the uplink pilot slot, Bob sends the pilot to Alice, and then Alice estimates the uplink CSI after receiving the pilot.



(a) uplink phase



(b) downlink phase

Fig. 1: IRS-assisted Pilot Spoofing Model

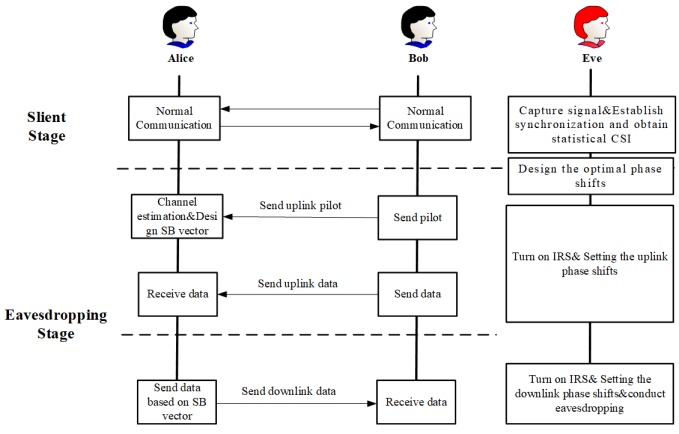


Fig. 2: Flow chart of pilot spoofing via IRS

In this case, the estimated CSI includes the direct path and the reflected path from Alice to Bob, as shown in Fig.1 (a). Then due to the channel reciprocity between the uplink and the downlink, Alice utilizes the uplink probed CSI as the downlink CSI, and designs the SB vector.

②In the uplink data slot, Bob sends uplink data to Alice. Alice performs channel equalization and information decoding. At this time, the phase shifts are maintained.

③Before Alice starts to send downlink data, Eve sets the downlink phase shifts at the IRS. In the downlink phase, Alice performs secure beamforming to send confidential signal, as shown in Fig.1(b), while Eve tries to overhear data.

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

B. The analysis of the Scheme

The physical layer secure transmission technology constructs endogenous security based on location-based wireless environment differences, while the proposed scheme utilizes the agility characteristics of IRS to reconfigure the wireless environment to combat physical layer security technique. Compared with the existing pilot spoofing methods, our scheme has the following advantages:

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

2) For traditional pilot spoofing methods, the pilot sent by the eavesdropper contains statistical CSI based on its location, and some detection methods are developed which can detect such an attack based on these prior information. For our proposed scheme, since the control strategy of the IRS is seamlessly embedded in the legitimate communication process, legitimate users working in TDD mode cannot perceive the difference between uplink channel and downlink channel, and the received pilot signal contains nothing about eavesdropper's location information, which makes existing detection methods invalid.

3) Additional energy consumption is required for sending pilot sequence, which is not conducive to the concealment of eavesdropping. While, due to the passive nature of the IRS, our solution does not require energy consumption except for its own state switching, which further increases the difficulty of detection.

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

III. Problem Formulation and Solved

A. Problem Formulation

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

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

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

With the probed CSI $\mathbf{h}_{abu}^H$, the downlink transmit SB vector is designed based on the MRT criterion and is given by

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

where P_t denotes the transmit power at Alice.

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

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

where $n_b \sim \mathcal{CN}(0, \sigma_0^2)$ is the additive Gaussian white noise (AWGN) at Bob. And the actual downlink CSI is given by:

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

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

$$\mathrm{SINR}_b = \frac{P_t\left|(\mathbf{h}_{ab}^H + \mathbf{h}_{rb}^H \Phi_2 \mathbf{H}_{ar})(\mathbf{h}_{ab} + \mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb})\right|^2}{\sigma^2 \left\|\mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb}\right\|_2^2} \tag{5}$$

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

Further, the received signal at Eve is expressed as

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

where n_e denotes the AWGN at Eve.

The corresponding SINR at Eve is derived as:

$$\mathrm{SINR}_e = \frac{P_t\left|(\mathbf{h}_{ae}^H + \mathbf{h}_{re}^H \Phi_2 \mathbf{H}_{ar})(\mathbf{h}_{ab} + \mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb})\right|^2}{\sigma^2 \left\|\mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb}\right\|_2^2} \tag{7}$$

Then the system secrecy rate is written as

$$R = [R_b - R_e]_+ = [\log_2(1+\mathrm{SINR}_b) - \log_2(1+\mathrm{SINR}_e)]_+ \tag{8}$$

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

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

$$\min_{\Phi_1,\Phi_2} R \tag{9a}$$

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

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

However, directly designing the reflection coefficient matrix based on instantaneous CSI in problem (9) seems impractical. There exist two reasons. One reason is that during the uplink phase, channel estimation has not conducted, and the eavesdropper cannot obtain instantaneous channel information in advance, thus the reflection coefficient matrix Φ_1 and Φ_2 cannot be designed. The other reason is that Eve eavesdrops on the communication channel passively, and it is relatively difficult to obtain the CSI of each channel in the system, especially for the channel from Alice to Bob. The methods to obtain the global instantaneous CSI are depicted in [15] [16], which need excessive ability requirements. While, after long-term observation, it is reasonable that statistical CSI of each channel can be obtained by Eve. Hence, average secrecy rate as a performance metric is considered and the orginal optimization problem can be transformed to minimize average secrecy rate, which is re-expressed as

$$\begin{aligned} &\min_{\Phi_1,\Phi_2} \mathbb{E}(R_b - R_e) \\ &= \mathbb{E}(\log_2(1+\mathrm{SINR}_b) - \log_2(1+\mathrm{SINR}_e) \\ &= \mathbb{E}\left\{\log_2\left(\frac{f_1(\Phi_1,\Phi_2)}{g_1(\Phi_1,\Phi_2)}\right)\right\} \end{aligned} \tag{10a}$$

$$\begin{aligned} f_1(\Phi_1,\Phi_2) = P_t&\left|(\mathbf{h}_{ab}^H + \mathbf{h}_{rb}^H \Phi_2 \mathbf{H}_{ar})(\mathbf{h}_{ab} + \mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb})\right|^2 \\ &+\sigma^2 \left\|\mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb}\right\|_2^2 \end{aligned} \tag{10b}$$

$$\begin{aligned} g_1(\Phi_1,\Phi_2) = P_t&\left|(\mathbf{h}_{ae}^H + \mathbf{h}_{re}^H \Phi_2 \mathbf{H}_{ar})(\mathbf{h}_{ab} + \mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb})\right|^2 \\ &+\sigma^2 \left\|\mathbf{H}_{ar}^H \Phi_1^H \mathbf{h}_{rb}\right\|_2^2 \end{aligned} \tag{10c}$$

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

Further, it is hard to obtain closed-form solution for problem (10). Fortunately, according to the theorem in [17], an approximate expression can be obtained

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

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

$$g_{ij}=\sqrt{\frac{\beta_{ij}}{1+\beta_{ij}}} g_{ij}^{\text{LOS}} + \sqrt{\frac{1}{1+\beta_{ij}}} g_{ij}^{\text{NLOS}} \tag{12}$$

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

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

$$\mathbf{h}_{ae} = \tilde{\mathbf{h}}_{ae} + \bar{\mathbf{h}}_{ae} \tag{13}$$

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

Similarly, for other channels, the corresponding LoS and NLoS components can be obtained. Note that since the IRS is deployed vertically high [18] and is deployed near Alice, less scattering environment from Alice to IRS is expected, namely $\mathbf{H}_{ar} = \bar{\mathbf{H}}_{ar} + \tilde{\mathbf{H}}_{ar} \approx \bar{\mathbf{H}}_{ar}$. Then (10b) and (10c) can be rewritten as (14) and (15).

After strict derivation, the expectation operation can be removed and the orginal problem can be rewritten as

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

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

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

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

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

Proof: See Appendix A.

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

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

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

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

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

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

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

B. Problem Solved

In this section, firstly, alternating optimization is utilized to separate the orginal problem into two sub-problems. Then, for each sub-problem, the Charnes-Cooper transformation [16] and SDR techniques are utilized to solve each sub-problem respectively.

1) Optimizing $\tilde{\mathbf{v}}_1$ for given $\tilde{\mathbf{v}}_2$: Let $\hat{\mathbf{V}}_1 = \tilde{\mathbf{v}}_1\tilde{\mathbf{v}}_1^H$, $\hat{\mathbf{V}}_2 = \tilde{\mathbf{v}}_2\tilde{\mathbf{v}}_2^H$, then we have $\text{Rank}(\tilde{\mathbf{V}}_1) = 1$, $\text{Rank}(\tilde{\mathbf{V}}_2) = 1$, and with the properties of matrix trace, (16b) and (16d) can be rewritten as

$$\begin{aligned}&f_2\left(\hat{\mathbf{V}}_1,\hat{\mathbf{V}}_2\right) = P_t\sigma_{ab}^2\text{Tr}(\hat{\mathbf{V}}_2\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H) + P_t\sigma_{ab}^2\text{Tr}(\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H)\\ &+P_t\text{Tr}(\hat{\mathbf{V}}_2\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H) + P_t\sigma_{rb}^2\text{Tr}(\hat{\mathbf{V}}_2\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ar}^H\bar{\mathbf{H}}_{ar}\bar{\mathbf{H}}_{ab}^H)\\ &+P_t\sigma_{rb}^2\text{Tr}(\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ar}^H\bar{\mathbf{H}}_{ar}\bar{\mathbf{H}}_{ab}^H) + \sigma^2\text{Tr}(\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H) + C_1\end{aligned} \tag{19}$$

$$\begin{aligned}&g_2\left(\hat{\mathbf{V}}_1,\hat{\mathbf{V}}_2\right) = P_t\sigma_{ab}^2\text{Tr}(\hat{\mathbf{V}}_2\bar{\mathbf{H}}_{ae}\bar{\mathbf{H}}_{ae}^H) + P_t\sigma_{ae}^2\text{Tr}(\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H)\\ &+P_t\text{Tr}(\hat{\mathbf{V}}_2\bar{\mathbf{H}}_{ae}\bar{\mathbf{H}}_{ab}^H\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ae}^H) + P_t\sigma_{rb}^2\text{Tr}(\hat{\mathbf{V}}_2\bar{\mathbf{H}}_{ae}\bar{\mathbf{H}}_{ar}^H\bar{\mathbf{H}}_{ar}\bar{\mathbf{H}}_{ae}^H)\\ &+P_t\sigma_{re}^2\text{Tr}(\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ar}^H\bar{\mathbf{H}}_{ar}\bar{\mathbf{H}}_{ab}^H) + \sigma^2\text{Tr}(\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H) + C_2\end{aligned} \tag{20}$$

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

$$\begin{aligned}&g_3\left(\hat{\mathbf{E}}_1,\hat{\mathbf{V}}_2\right) = s_1 \times g_2\left(\hat{\mathbf{V}}_1,\hat{\mathbf{V}}_2\right)\\ &= P_t\sigma_{ab}^2\text{Tr}(\hat{\mathbf{V}}_2\bar{\mathbf{H}}_{ae}\bar{\mathbf{H}}_{ae}^H) + P_t\sigma_{ae}^2\text{Tr}(\hat{\mathbf{E}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H)\\ &+P_t\text{Tr}(\hat{\mathbf{V}}_2\bar{\mathbf{H}}_{ae}\bar{\mathbf{H}}_{ab}^H\hat{\mathbf{E}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ae}^H) + P_t\sigma_{rb}^2\text{Tr}(\hat{\mathbf{V}}_2\bar{\mathbf{H}}_{ae}\bar{\mathbf{H}}_{ar}^H\bar{\mathbf{H}}_{ar}\bar{\mathbf{H}}_{ae}^H)\\ &+P_t\sigma_{re}^2\text{Tr}(\hat{\mathbf{E}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ar}^H\bar{\mathbf{H}}_{ar}\bar{\mathbf{H}}_{ab}^H) + \sigma^2\text{Tr}(\hat{\mathbf{E}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H) + s_1C_2\end{aligned} \tag{21}$$

$$f_1(\Phi_1,\Phi_2)=P_t\left|((\bar{\mathbf{h}}_{ab}^H+\tilde{\mathbf{h}}_{ab}^H)+(\bar{\mathbf{h}}_{rb}^H+\tilde{\mathbf{h}}_{rb}^H)\Phi_2\mathbf{H}_{ar}))((\bar{\mathbf{h}}_{ab}+\tilde{\mathbf{h}}_{ab})+\mathbf{H}_{ar}^H\Phi_1^H(\bar{\mathbf{h}}_{rb}+\tilde{\mathbf{h}}_{rb}))\right|^2+\sigma^2\left\|\mathbf{H}_{ar}^H\Phi_1^H(\bar{\mathbf{h}}_{rb}+\tilde{\mathbf{h}}_{rb})\right\|_2^2 \tag{14}$$

$$g_1(\Phi_1,\Phi_2)=P_t\left|((\bar{\mathbf{h}}_{ae}^H+\tilde{\mathbf{h}}_{ae}^H)+(\bar{\mathbf{h}}_{re}^H+\tilde{\mathbf{h}}_{re}^H)\Phi_2\mathbf{H}_{ar}))((\bar{\mathbf{h}}_{ab}+\tilde{\mathbf{h}}_{ab})+\mathbf{H}_{ar}^H\Phi_1^H(\bar{\mathbf{h}}_{rb}+\tilde{\mathbf{h}}_{rb}))\right|^2+\sigma^2\left\|\mathbf{H}_{ar}^H\Phi_1^H(\bar{\mathbf{h}}_{rb}+\tilde{\mathbf{h}}_{rb})\right\|_2^2 \tag{15}$$

$$\begin{aligned}&f_3\left(\hat{\mathbf{E}}_1,\hat{\mathbf{V}}_2\right)=s_1\times f_2\left(\hat{\mathbf{V}}_1,\hat{\mathbf{V}}_2\right)\\&=P_t\sigma_{ab}^2\mathrm{Tr}(\hat{\mathbf{V}}_2\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H)+P_t\sigma_{ab}^2\mathrm{Tr}(\hat{\mathbf{E}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H)\\&+P_t\mathrm{Tr}(\hat{\mathbf{V}}_2\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H\hat{\mathbf{E}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H)\\&+P_t\sigma_{rb}^2\mathrm{Tr}(\hat{\mathbf{V}}_2\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ar}^H\bar{\mathbf{H}}_{ar}\bar{\mathbf{H}}_{ab}^H)\\&+P_t\sigma_{rb}^2\mathrm{Tr}(\hat{\mathbf{E}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ar}^H\bar{\mathbf{H}}_{ar}\bar{\mathbf{H}}_{ab}^H)+\sigma^2\mathrm{Tr}(\hat{\mathbf{E}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H)+s_1C_1\end{aligned} \tag{22}$$

Then problem (18) is equivalently transformed as:

$$\min_{\hat{\mathbf{E}}_1}\ f_3\left(\hat{\mathbf{E}}_1,\hat{\mathbf{V}}_2\right) \tag{23a}$$

$$s.t.\quad g_3\left(\hat{\mathbf{E}}_1,\hat{\mathbf{V}}_2\right)=1 \tag{23b}$$

$$\hat{\mathbf{E}}_{1(n,n)}=s_1,\ n=1,2,\cdots(N+1) \tag{23c}$$

$$\mathrm{Rank}\left(\hat{\mathbf{E}}_1\right)=1 \tag{23d}$$

Note that problem (23) is non-convex due to the constraint (23d). Then, the Rank-1 constraint is firstly discarded and problem (23) is transformed to a convex semidefinite programming problem with linear constraints and can be efficiently solved via the CVX solver. Since the constraint of Rank-1 is relaxed in problem (23), it is necessary to verify whether the rank of the obtained solution satisfies Rank-1. If the obtained solution is not Rank-1, gaussian randomization is applied for recovering vector approximately [9].

2) Optimizing $\tilde{\mathbf{v}}_2$ for given $\tilde{\mathbf{v}}_1$: Similarly, slack variable $s_2>0$ is introduced, which satisfies $s_2\times g_2\left(\hat{\mathbf{V}}_1,\hat{\mathbf{V}}_2\right)=1$. And new matrix $\hat{\mathbf{E}}_2=s_2\hat{\mathbf{V}}_2$ is defined. Then new functions $g_4\left(\hat{\mathbf{V}}_1,\hat{\mathbf{E}}_2\right)$, $f_4\left(\hat{\mathbf{V}}_1,\hat{\mathbf{E}}_2\right)$ are constructed as follows

$$\begin{aligned}&g_4\left(\hat{\mathbf{V}}_1,\hat{\mathbf{E}}_2\right)=s_2\times g_2\left(\hat{\mathbf{V}}_1,\hat{\mathbf{V}}_2\right)\\&=P_t\sigma_{ab}^2\mathrm{Tr}(\hat{\mathbf{E}}_2\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ae}^H)+P_t\sigma_{rb}^2\mathrm{Tr}(\hat{\mathbf{E}}_2\bar{\mathbf{H}}_{ae}\bar{\mathbf{H}}_{ar}^H\bar{\mathbf{H}}_{ar}\bar{\mathbf{H}}_{ae}^H)\\&+P_t\mathrm{Tr}(\hat{\mathbf{E}}_2\bar{\mathbf{H}}_{ae}\bar{\mathbf{H}}_{ab}^H\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ae}^H)+P_t\sigma_{ae}^2\mathrm{Tr}(\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H)\\&+P_t\sigma_{re}^2\mathrm{Tr}(\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ar}^H\bar{\mathbf{H}}_{ar}\bar{\mathbf{H}}_{ab}^H)+\sigma^2\mathrm{Tr}(\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H)+s_2C_1\end{aligned} \tag{24}$$

$$\begin{aligned}&f_4\left(\hat{\mathbf{V}}_1,\hat{\mathbf{E}}_2\right)=s_2\times f_2\left(\hat{\mathbf{V}}_1,\hat{\mathbf{V}}_2\right)\\&=P_t\sigma_{ab}^2\mathrm{Tr}(\hat{\mathbf{E}}_2\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H)+P_t\sigma_{rb}^2\mathrm{Tr}(\hat{\mathbf{E}}_2\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ar}^H\bar{\mathbf{H}}_{ar}\bar{\mathbf{H}}_{ae}^H)\\&+P_t\mathrm{Tr}(\hat{\mathbf{E}}_2\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H)+P_t\sigma_{ab}^2\mathrm{Tr}(\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H)\\&+P_t\sigma_{rb}^2\mathrm{Tr}(\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ar}^H\bar{\mathbf{H}}_{ar}\bar{\mathbf{H}}_{ab}^H)+\sigma^2\mathrm{Tr}(\hat{\mathbf{V}}_1\bar{\mathbf{H}}_{ab}\bar{\mathbf{H}}_{ab}^H)+s_1C_1\end{aligned} \tag{25}$$

Then the orginal problem is equivalently transformed as:

$$\min_{\hat{\mathbf{E}}_2}\ f_4\left(\hat{\mathbf{V}}_1,\hat{\mathbf{E}}_2\right) \tag{26a}$$

$$s.t.g_4\left(\hat{\mathbf{V}}_1,\hat{\mathbf{E}}_2\right)=1 \tag{26b}$$

$$\hat{\mathbf{E}}_{2(n,n)}=s_2,\ n=1,2,\cdots(N+1) \tag{26c}$$

$$\mathrm{Rank}\left(\hat{\mathbf{E}}_2\right)=1 \tag{26d}$$

Similarly, by dropping Rank-1 constraint (26d), problem (26) can be efficiently solved via the CVX solver. And then Gaussian randomization method is utilized to recover $\tilde{\mathbf{v}}_2$.

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

Algorithm 1 proposed algorithm for solving problem (18)

1. Initialize the phase shifts of the IRS as $\tilde{\mathbf{v}}_1^{*(0)}=e^{j\bar{w}_1}\begin{bmatrix}\mathbf{v}_1^{(0)}\\1\end{bmatrix}$, $\tilde{\mathbf{v}}_2^{*(0)}=e^{j\bar{w}_2}\begin{bmatrix}\mathbf{v}_2^{(0)}\\1\end{bmatrix}$ with random values $\bar{w}_1,\bar{w}_2\in[0,2\pi]$, and set $l=1$;
2. Repeat
3. Solve (23) for given $\tilde{\mathbf{v}}_2^{(l-1)}$, and obtain the solution as $\tilde{\mathbf{v}}_1^{(l)}$.
4. Solve (26) for given $\tilde{\mathbf{v}}_1^{(l)}$, and obtain the solution as $\tilde{\mathbf{v}}_2^{(l)}$.
5. Update $l=l+1$.
6. Until the fractional decrease of the objective value is below the error ε or the iteration number meets $l=L$.

Convergence Analysis: For the lth alternating iteration, denote $R(\tilde{\mathbf{v}}_1^{(l)},\tilde{\mathbf{v}}_2^{(l)})$ as the objective function value, where $(\tilde{\mathbf{v}}_1^{(l)},\tilde{\mathbf{v}}_2^{(l)})$ is the feasible solution. Then for the $(l+1)$th iteration, $(\tilde{\mathbf{v}}_1^{(l+1)},\tilde{\mathbf{v}}_2^{(l)})$ is the feasible solution of problem (23), and $(\tilde{\mathbf{v}}_1^{(l+1)},\tilde{\mathbf{v}}_2^{(l+1)})$ is the feasible solution of problem (26). Then, we have

$$R(\tilde{\mathbf{v}}_1^{(l)},\tilde{\mathbf{v}}_2^{(l)})\overset{(a)}{\geq}R(\tilde{\mathbf{v}}_1^{(l+1)},\tilde{\mathbf{v}}_2^{(l)})\overset{(b)}{\geq}R(\tilde{\mathbf{v}}_1^{(l+1)},\tilde{\mathbf{v}}_2^{(l+1)}) \tag{27}$$

where inequality (a) holds due to the fact that problem (23) is solved optimally in step 3, equality (b) holds due to step 4. This indicates that the object value given in the $(l+1)$th iteration is not larger than that in the lth iteration. That is to say, after each iteration, the object value is non-increasing. Furthermore, along with the QoS constraint, the secrecy rate is lower bounded and thus it must converge after some iterations.

Complexity Analysis: The main complexity of Algorithm 2 lies on the Step 3, 4. For Step 3, the complexity for solving (23) using the interior-point method, which is denoted as $\mathcal{O}_1$, is determined by the number and size of variables (design variables and slack variables) and constraints (PSD constraints and slack constraints), which is summarized in Table I. Due to the same form between (23) and (26), the complexity of Step 4 is equal to that of Step 3. Furthermore, the major complexity of Algorithm 2 is given by $2I_{ao}\times\mathcal{O}_1$, where I_{ao} denotes the alternating iteration numbers.

TABLE I: Computational complexity analysis for the proposed algorithm

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

IV. NUMERICAL RESULTS

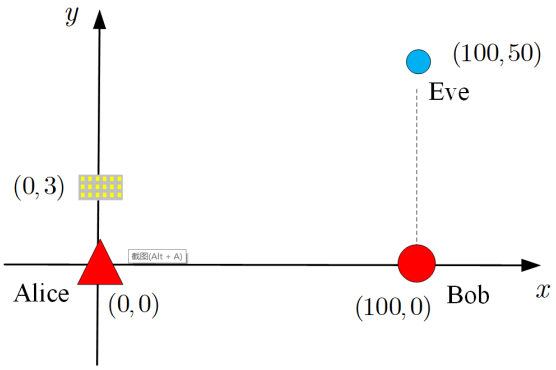


Fig. 3: Simulation Setup

In this section, we present numerical results to validate the performance of the proposed scheme. Simulation setups are shown in Fig. 2, where Alice, Bob, IRS, Eve are located at (0,0), (100,0), (0,3), (100,50) in meter (m), respectively. Considering that IRS is deployed vertically high [18], a less scattering environment is expected and thus we set $\beta_{ar} = \infty$, $c_{ar} = 2.5$, $c_{re} = c_{rb} = 3$, $\beta_{rb} = 10$, $\beta_{re} = 5$. The rest parameters are listed as follows: $c_{ae} = c_{ab} = 3$, $\beta_{ab} = 10$, $\sigma_0^2 = -80$dBm, $L_0 = -30$dB. The iterative threshold $\varepsilon = 0.001$, and the maximum iteration number L=15. The following simulation results are achieved by averaging over 500 randomly channel realizations.

Fig. 4 shows the convergence behavior of our proposed algorithm under different number of of reflecting elements N_{IRS} and transmitting antennas M_a, respectively. We can observe that with the increase of iteration numbers, the system secrecy rate gradually decreases. After about 8 iterations, the object values all reach stable values, which validates the convergence analysis given in Section III.C.

In order to evaluate the advantage brought by the IRS, we compare our proposed scheme (Active IRS) with the following three benchmark schemes:

Scheme 1: Without IRS. In this case, Eve passively wiretap information without the aid of the IRS.

Scheme 2: Jamming assisted pilot spoofing scheme (Pilot Jam). In this case, Eve sends jamming pilot when Bob sends the uplink pilot to Alice as shown in [2]. The jamming pilot power is set to 0.01 of the transmit power by Alice.

Scheme 3: Passive IRS. In this case, the phase shifts at the IRS keep constanst during the uplink phase and downlink phase. And the phase shifts is designed cooperating with Eve to minimize the secrecy rate. However, in this scheme, the probed CSI for Alice is not misleaded by the IRS, and it is the only selected attack strategy for FDD system.

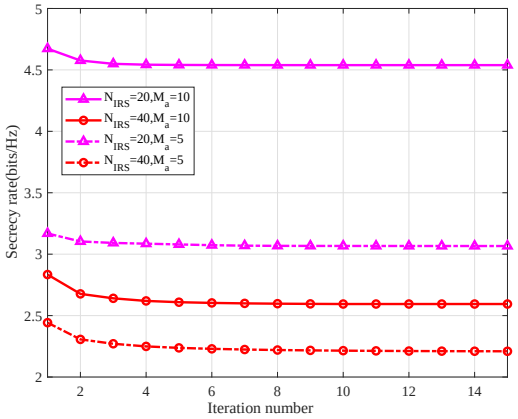


Fig. 4: Convergence behavior verus the iteration numbers of alternating optimization ($\beta_{ab} = 10$,$\beta_{ae} = 5$)

Fig. 5 shows the system secrecy rate verus different transmit power sent by Alice. As the transmit power increases, the secrecy rate increases gradually. Meanwhile, we can observe that, under the same condition, the proposed scheme is almost equal to Scheme 2 with Jamming and significantly outperforms the other two benchmark schemes. The reason that the scheme is superior to the scheme 1 and 3 can be concluded from problem (17). By carefully designing reflection coefficients, the misleaded beam sent by Alice can be intendly aligned to Eve during the uplink phase, and during the downlink phase, the received signal by Eve can be intendly enhanced. Moreover, compared with Scheme 2, no additional power is consumed by Eve.

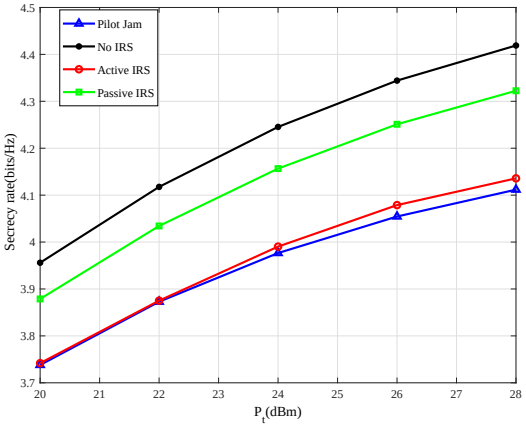


Fig. 5: the secrecy rate verus transmit power ($N_{\text{IRS}} = 20$,$M_a = 10$,$\beta_{ab} = 10$,$\beta_{ae} = 5$)

The performance gain verus the number of transmit antennas at Alice is plotted in Fig.6. It can be seen that as the number of transmit antennas increases, the system secrecy rate increases gradually. The reason is that with more transmit antennas, the beam can focus on legitimate users more accurately. Besides, we can observe that with the increase of the number of transmit antennas, the security rate difference between Scheme 3 and Scheme 1 under different reflecting elements decreases, which means that increasing transmitting antenna can reduce the security threat brought by Scheme 3. While, for our proposed scheme, the security rate difference under different reflecting elements keeps nearly unchanged, and for Scheme 2, the security rate difference becomes stronger, which means that due to pilot spoofing, more beam leakage although multiple antennas are utilized.

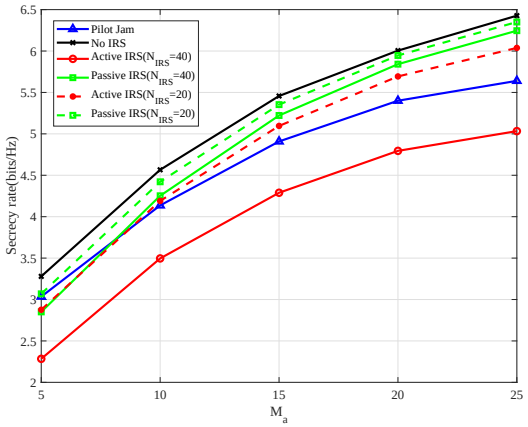


Fig. 6: the secrecy rate verus the number of transmit antennas at Alice ($N_{\mathrm{IRS}} = 20$,$\beta_{ab} = 10$, $\beta_{ae} = 5$)

In Fig.7, we shows the secrecy rate decrease ratio verus Rician factor β_{ae}, where the secrecy rate decrease ratio is defined as $\Delta R = (R_{noirs} - R_{active})/R_{noirs}$, and R_{noirs} and R_{active} denote the secrecy rate of Scheme 1 and proposed scheme under the same condition. It can be seen that as Rician factor β_{ae} increases, the secrecy rate decrease ratio ΔR of Scheme 3 and proposed scheme both increase gradually. The reason is that as Rician factor β_{ae} increases, LoS component becomes gradually dominant and statistical CSI is approximate to instantaneous CSI, then Eve can wiretap more information. Moreover, if Eve is a malicious internal user in the network, the Rician factor β_{ae} is strong and more damage to legitimate commnunication is brought by IRS. Besides, if Eve is an outside user in the network, less damage is brought and deploying multiple IRSs and tring to obtain more precise CSI may be potential solutions.

In Fig.8, we further show the performance gains verus the number of reflecting elements. It can be seen that as the number of reflection elements increases, the system secrecy rates of Scheme 3 and proposed scheme both decrease, and our proposed scheme decreases more quickly than Scheme 3. The reason is that IRS with larger elements can provide more adjustable dimension for inequality (18a). Moreover, from Fig. 5-8, we can observe that the secrecy rate of Scheme 3 is

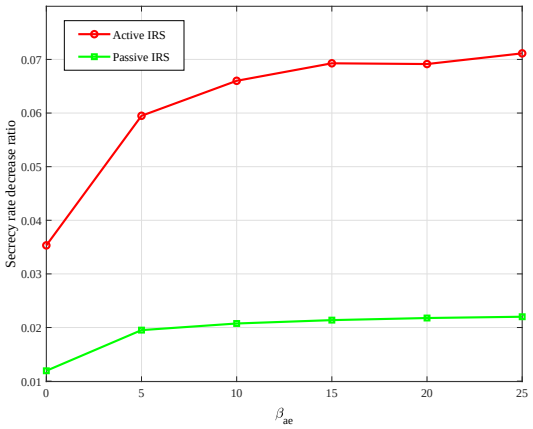


Fig. 7: the secrecy decrease ratio verus the Rician factorβ_{ae} ($N_{\mathrm{IRS}} = 20$, $\beta_{ab} = 10$)

significantly less than that of our proposed scheme, which indicates that our proposed scheme poses more damage to TDD system than FDD system and more attention should be paid to this attack. In fact, the number of reflecting elements can reach 100 or more at a low cost [19], which could bring more secure damage with less power.

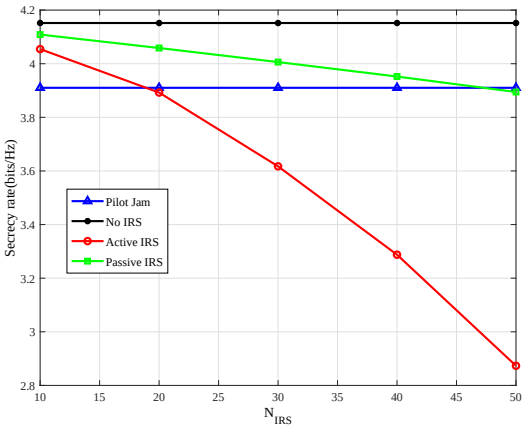


Fig. 8: the secrecy rate verus the number of reflecting elements ($M_a = 10$, $\beta_{ab} = 10$, $\beta_{ae} = 5$)

V. Conclusion And Future Work

In this paper, we have presented an investigation of IRS-assisted pilot spoofing scheme. Firstly, the control strategy of the IRS is proposed. By changing the phase shifts during uplink phase and downlink phase, the reciprocity between uplink and downlink disappears and the secure beamforming shifts, which leads to signal leakage. Then, the minimum average secrecy rate problem based on statistical CSI is established by carefully designing the phase shifts. With alternating optimization algorithm and Charnes-Cooper transformation technique, a near optimal solution is proposed. Finally, simulation results show that our scheme can seriously affect the security performance of the TDD systems without energy consumption. If

the IRS is not utilized by the internal users properly, it will bring serious threat. Therefore, it is worth paying attention to studying the effective countermeasures against pilot spoofing attack in future study.

APPENDIX A
PROOF OF PROPOSITION 1

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

$$\begin{aligned} &g_2(\Phi_1,\Phi_2)=\mathbb{E}(g_1(\Phi_1,\Phi_2))\\ &=\mathbb{E}(\sigma^2\left\|\mathbf{H}_{ar}^H\Phi_1^H\mathbf{h}_{rb}\right\|_2^2\\ &\quad+P_t\left|(\mathbf{h}_{a\mathbb{E}}^H+\mathbf{h}_{re}^H\Phi_2\mathbf{H}_{ar})(\mathbf{h}_{ab}+\mathbf{H}_{ar}^H\Phi_1^H\mathbf{h}_{rb})\right|^2) \end{aligned} \tag{28}$$

Let $q_1 = \left|(\mathbf{h}_{ae}^H+\mathbf{h}_{re}^H\mathbf{A})(\mathbf{h}_{ab}+\mathbf{B}^H\mathbf{h}_{rb})\right|^2$,$q_2 = \left\|\mathbf{B}^H(\bar{\mathbf{h}}_{rb}+\tilde{\mathbf{h}}_{rb})\right\|_2^2$, where $\mathbf{A}=\Phi_2\mathbf{H}_{ar}$, $\mathbf{B}=\Phi_1\mathbf{H}_{ar}$, then q_1 can be firstly expanded as

$$\begin{aligned} q_1&=\left|(\mathbf{h}_{ae}^H+\mathbf{h}_{re}^H\mathbf{A})(\mathbf{h}_{ab}+\mathbf{B}^H\mathbf{h}_{rb})\right|^2\\ &=\left|\mathbf{h}_{ae}^H\mathbf{h}_{ab}+\mathbf{h}_{ae}^H\mathbf{B}^H\mathbf{h}_{rb}+\mathbf{h}_{re}^H\mathbf{A}\mathbf{h}_{ab}+\mathbf{h}_{re}^H\mathbf{A}\mathbf{B}^H\mathbf{h}_{rb}\right|^2\\ &=\underbrace{\mathbf{h}_{ae}^H\mathbf{h}_{ab}\mathbf{h}_{ab}^H\mathbf{h}_{ae}}_{p_1}+\underbrace{\mathbf{h}_{ae}^H\mathbf{h}_{ab}\mathbf{h}_{rb}^H\mathbf{B}\mathbf{h}_{ae}}_{p_2}+\underbrace{\mathbf{h}_{ae}^H\mathbf{h}_{ab}\mathbf{h}_{ab}^H\mathbf{A}^H\mathbf{h}_{re}}_{p_3}\\ &\quad+\underbrace{\mathbf{h}_{ae}^H\mathbf{h}_{ab}\mathbf{h}_{rb}^H\mathbf{B}A^H\mathbf{h}_{re}}_{p_4}+\underbrace{\mathbf{h}_{ae}^H\mathbf{B}^H\mathbf{h}_{rb}\mathbf{h}_{ab}^H\mathbf{h}_{ae}}_{p_5}\\ &\quad+\underbrace{\mathbf{h}_{ae}^H\mathbf{B}^H\mathbf{h}_{rb}\mathbf{h}_{rb}^H\mathbf{B}\mathbf{h}_{ae}}_{p_6}+\underbrace{\mathbf{h}_{ae}^H\mathbf{B}^H\mathbf{h}_{rb}\mathbf{h}_{ab}^H\mathbf{A}^H\mathbf{h}_{re}}_{p_7}\\ &\quad+\underbrace{\mathbf{h}_{ae}^H\mathbf{B}^H\mathbf{h}_{rb}\mathbf{h}_{rb}^H\mathbf{B}A^H\mathbf{h}_{re}}_{p_8}+\underbrace{\mathbf{h}_{re}^H\mathbf{A}\mathbf{h}_{ab}\mathbf{h}_{ab}^H\mathbf{h}_{ae}}_{p_9}\\ &\quad+\underbrace{\mathbf{h}_{re}^H\mathbf{A}\mathbf{h}_{ab}\mathbf{h}_{rb}^H\mathbf{B}\mathbf{h}_{ae}}_{p_{10}}+\underbrace{\mathbf{h}_{re}^H\mathbf{A}\mathbf{h}_{ab}\mathbf{h}_{ab}^H\mathbf{A}^H\mathbf{h}_{re}}_{p_{11}}\\ &\quad+\underbrace{\mathbf{h}_{re}^H\mathbf{A}\mathbf{h}_{ab}\mathbf{h}_{rb}^H\mathbf{B}A^H\mathbf{h}_{re}}_{p_{12}}+\underbrace{\mathbf{h}_{re}^H\mathbf{A}\mathbf{B}^H\mathbf{h}_{rb}\mathbf{h}_{ab}^H\mathbf{h}_{ae}}_{p_{13}}\\ &\quad+\underbrace{\mathbf{h}_{re}^H\mathbf{A}\mathbf{B}^H\mathbf{h}_{rb}\mathbf{h}_{rb}^H\mathbf{B}\mathbf{h}_{ae}}_{p_{14}}+\underbrace{\mathbf{h}_{re}^H\mathbf{A}\mathbf{B}^H\mathbf{h}_{rb}\mathbf{h}_{ab}^H\mathbf{A}^H\mathbf{h}_{re}}_{p_{15}}\\ &\quad+\underbrace{\mathbf{h}_{re}^H\mathbf{A}\mathbf{B}^H\mathbf{h}_{rb}\mathbf{h}_{rb}^H\mathbf{B}A^H\mathbf{h}_{re}}_{p_{16}} \end{aligned} \tag{29}$$

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

$$\begin{aligned} &\mathbb{E}(p_{16})\\ &=\mathbb{E}\left\{(\bar{\mathbf{h}}_{re}^H+\tilde{\mathbf{h}}_{re}^H)\mathbf{A}\mathbf{B}^H(\bar{\mathbf{h}}_{rb}+\tilde{\mathbf{h}}_{rb})(\bar{\mathbf{h}}_{rb}^H+\tilde{\mathbf{h}}_{rb}^H)\mathbf{B}A^H(\bar{\mathbf{h}}_{re}+\tilde{\mathbf{h}}_{re})\right\}\\ &=\underbrace{\mathbb{E}\left(\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re}\right)}_{t_1}+\underbrace{\mathbb{E}\left(\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\tilde{\mathbf{h}}_{re}\right)}_{t_2}\\ &+\underbrace{\mathbb{E}\left(\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\tilde{\mathbf{h}}_{rb}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re}\right)}_{t_3}+\underbrace{\mathbb{E}\left(\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\tilde{\mathbf{h}}_{rb}^H\mathbf{B}A^H\tilde{\mathbf{h}}_{re}\right)}_{t_4}\\ &+\underbrace{\mathbb{E}\left(\tilde{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re}\right)}_{t_5}+\underbrace{\mathbb{E}\left(\tilde{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\tilde{\mathbf{h}}_{re}\right)}_{t_6}\\ &+\underbrace{\mathbb{E}\left(\tilde{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\tilde{\mathbf{h}}_{rb}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re}\right)}_{t_7}+\underbrace{\mathbb{E}\left(\tilde{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\tilde{\mathbf{h}}_{rb}^H\mathbf{B}A^H\tilde{\mathbf{h}}_{re}\right)}_{t_8}\\ &+\underbrace{\mathbb{E}\left(\tilde{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\tilde{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re}\right)}_{t_9}+\underbrace{\mathbb{E}\left(\tilde{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\tilde{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\tilde{\mathbf{h}}_{re}\right)}_{t_{10}}\\ &+\underbrace{\mathbb{E}\left(\tilde{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\tilde{\mathbf{h}}_{rb}\tilde{\mathbf{h}}_{rb}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re}\right)}_{t_{11}}+\underbrace{\mathbb{E}\left(\tilde{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\tilde{\mathbf{h}}_{rb}\tilde{\mathbf{h}}_{rb}^H\mathbf{B}A^H\tilde{\mathbf{h}}_{re}\right)}_{t_{12}}\\ &+\underbrace{\mathbb{E}\left(\tilde{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\tilde{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re}\right)}_{t_{13}}+\underbrace{\mathbb{E}\left(\tilde{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\tilde{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\tilde{\mathbf{h}}_{re}\right)}_{t_{14}}\\ &+\underbrace{\mathbb{E}\left(\tilde{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\tilde{\mathbf{h}}_{rb}\tilde{\mathbf{h}}_{rb}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re}\right)}_{t_{15}}+\underbrace{\mathbb{E}\left(\tilde{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\tilde{\mathbf{h}}_{rb}\tilde{\mathbf{h}}_{rb}^H\mathbf{B}A^H\tilde{\mathbf{h}}_{re}\right)}_{t_{16}} \end{aligned} \tag{30}$$

Then, for each item in (30), we calculate the expectation separately. First, we can have

$$\begin{aligned} \mathbb{E}(t_1)&=\mathbb{E}\left(\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re}\right)\\ &\overset{(a)}{=}\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re} \end{aligned} \tag{31}$$

$$\mathbb{E}(t_2)=\mathbb{E}\left(\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\tilde{\mathbf{h}}_{re}\right)\overset{(b)}{=}0 \tag{32}$$

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

$$\begin{aligned} &\mathbb{E}(t_3)=\mathbb{E}(t_4)=\mathbb{E}(t_5)=\mathbb{E}(t_6)\\ &=\mathbb{E}(t_8)=\mathbb{E}(t_9)=\mathbb{E}(t_{11})=\mathbb{E}(t_{13})\\ &=\mathbb{E}(t_{14})=\mathbb{E}(t_{15})=0 \end{aligned} \tag{33}$$

Then for t_7, we have

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

According to the properties of Gaussian distribution, we can derive

$$\mathbb{E}\left(\tilde{\mathbf{h}}_{rb}\tilde{\mathbf{h}}_{rb}^H\right)=\begin{pmatrix}\sigma_{rb}^2 & 0 & \cdots & 0\\ 0 & \sigma_{rb}^2 & & 0\\ \vdots & & \ddots & \vdots\\ 0 & \cdots & & \sigma_{rb}^2\end{pmatrix} \tag{35}$$

Then, we have

$$\mathbb{E}(t_7)=\sigma_{rb}^2\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re} \tag{36}$$

Similarly, t_{10} can be expressed as

$$\begin{aligned} \mathbb{E}(t_{10})&=\mathbb{E}\left(\tilde{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\tilde{\mathbf{h}}_{re}\right)\\ &=\sigma_{re}^2\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb} \end{aligned} \tag{37}$$

Similarly, t_{16} can be expressed as

$$\begin{aligned} \mathbb{E}(t_{16})&=\mathbb{E}(\tilde{\mathbf{h}}_{re}^HAB^H\tilde{\mathbf{h}}_{rb}\tilde{\mathbf{h}}_{rb}^HBA^H\tilde{\mathbf{h}}_{re})\\ &=\sigma_{re}^2\sigma_{rb}^2\mathrm{Tr}(AB^HBA^H)\\ &=\sigma_{re}^2\sigma_{rb}^2\mathrm{Tr}(\Phi_2\mathbf{H}_{ar}\mathbf{H}_{ar}^H\Phi_1^H\Phi_1\mathbf{H}_{ar}\mathbf{H}_{ar}^H\Phi_2^H)\\ &=\sigma_{re}^2\sigma_{rb}^2\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H\mathbf{H}_{ar}\mathbf{H}_{ar}^H) \end{aligned} \tag{38}$$

Further, all the subitem in p_{16} can be summed as follows

$$\begin{aligned}\mathbb{E}(p_{16}) &= \bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re} + \sigma_{rb}^2\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re}\\ &+\sigma_{re}^2\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb} + \sigma_{re}^2\sigma_{rb}^2\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H\mathbf{H}_{ar}\mathbf{H}_{ar}^H)\end{aligned} \tag{39}$$

Similarly, for each item in q_1, we can remove the expected operation and obtain the following result

$$\begin{aligned}\mathbb{E}(p_1) &= \bar{\mathbf{h}}_{ae}^H\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{ab}^H\bar{\mathbf{h}}_{ae} + \sigma_{ae}^2\bar{\mathbf{h}}_{ab}^H\bar{\mathbf{h}}_{ab} + \sigma_{ab}^2\bar{\mathbf{h}}_{ae}^H\bar{\mathbf{h}}_{ae}\\ &+M_a\sigma_{ae}^2\sigma_{ab}^2\\ \mathbb{E}(p_2) &= \bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}\bar{\mathbf{h}}_{ae} + \sigma_{ae}^2\bar{\mathbf{h}}_{rb}^H\mathbf{B}\bar{\mathbf{h}}_{ab}\\ \mathbb{E}(p_3) &= \bar{\mathbf{h}}_{ae}^H\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{ab}^H\mathbf{A}^H\bar{\mathbf{h}}_{re} + \sigma_{ab}^2\bar{\mathbf{h}}_{ae}^H\mathbf{A}^H\bar{\mathbf{h}}_{re}\\ \mathbb{E}(p_4) &= \bar{\mathbf{h}}_{ae}^H\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{rb}^H\mathbf{B}\mathbf{A}^H\bar{\mathbf{h}}_{re}\\ \mathbb{E}(p_5) &= \bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{ab}^H\bar{\mathbf{h}}_{ae} + \sigma_{ae}^2\bar{\mathbf{h}}_{ab}^H\mathbf{B}^H\bar{\mathbf{h}}_{rb}\\ \mathbb{E}(p_6) &= \bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}\bar{\mathbf{h}}_{ae} + \sigma_{ae}^2\bar{\mathbf{h}}_{rb}^H\mathbf{B}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\\ &+\sigma_{rb}^2\bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\mathbf{B}\bar{\mathbf{h}}_{ae} + \sigma_{ae}^2\sigma_{rb}^2\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H)\\ \mathbb{E}(p_7) &= \bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{ab}^H\mathbf{A}^H\bar{\mathbf{h}}_{re}\\ \mathbb{E}(p_8) &= \bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}\mathbf{A}^H\bar{\mathbf{h}}_{re} + \sigma_{rb}^2\bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\mathbf{B}\mathbf{A}^H\bar{\mathbf{h}}_{re}\\ \mathbb{E}(p_9) &= \bar{\mathbf{h}}_{re}^H\mathbf{A}\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{ab}^H\bar{\mathbf{h}}_{ae} + \sigma_{ab}^2\bar{\mathbf{h}}_{re}^H\mathbf{A}\bar{\mathbf{h}}_{ae}\\ \mathbb{E}(p_{10}) &= \bar{\mathbf{h}}_{re}^HA\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{rb}^HB\bar{\mathbf{h}}_{ae}\\ \mathbb{E}(p_{11}) &= \bar{\mathbf{h}}_{re}^H\mathbf{A}\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{ab}^H\mathbf{A}^H\bar{\mathbf{h}}_{re} + \sigma_{re}^2\mathbf{h}_{ab}^H\mathbf{A}^H\mathbf{A}\mathbf{h}_{ab}\\ &+\sigma_{ab}^2\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{A}^H\bar{\mathbf{h}}_{re} + \sigma_{ab}^2\sigma_{re}^2\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H)\\ \mathbb{E}(p_{12}) &= \bar{\mathbf{h}}_{re}^HA\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{rb}^HBA^H\bar{\mathbf{h}}_{re} + \sigma_{re}^2\bar{\mathbf{h}}_{rb}^HBA^HA\bar{\mathbf{h}}_{ab}\\ \mathbb{E}(p_{13}) &= \bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{ab}^H\bar{\mathbf{h}}_{ae}\\ \mathbb{E}(p_{14}) &= \bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^HB\bar{\mathbf{h}}_{ae} + \sigma_{rb}^2\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\mathbf{B}\bar{\mathbf{h}}_{ae}\\ \mathbb{E}(p_{15}) &= \bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{ab}^H\mathbf{A}^H\bar{\mathbf{h}}_{re} + \sigma_{re}^2\bar{\mathbf{h}}_{ab}^H\mathbf{A}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\end{aligned} \tag{40}$$

There are many items in (40). It is difficult to merge them directly. We combine some items according to certain association and get s_{11}, s_{12}, s_{13}, s_{14}, s_{15} as follows

$$\begin{aligned}s_{11} &= \bar{\mathbf{h}}_{ae}^H\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{ab}^H\bar{\mathbf{h}}_{ae} + \bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}\bar{\mathbf{h}}_{ae}\\ &+\bar{\mathbf{h}}_{ae}^H\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{ab}^H\mathbf{A}^H\bar{\mathbf{h}}_{re} + \bar{\mathbf{h}}_{ae}^H\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{rb}^H\mathbf{B}\mathbf{A}^H\bar{\mathbf{h}}_{re}\\ &+\bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{ab}^H\bar{\mathbf{h}}_{ae} + \bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}\bar{\mathbf{h}}_{ae}\\ &+\bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{ab}^H\mathbf{A}^H\bar{\mathbf{h}}_{re} + \bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}\mathbf{A}^H\bar{\mathbf{h}}_{re}\\ &+\bar{\mathbf{h}}_{re}^H\mathbf{A}\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{ab}^H\bar{\mathbf{h}}_{ae} + \bar{\mathbf{h}}_{re}^HA\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{rb}^HB\bar{\mathbf{h}}_{ae}\\ &+\bar{\mathbf{h}}_{re}^H\mathbf{A}\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{ab}^H\mathbf{A}^H\bar{\mathbf{h}}_{re} + \bar{\mathbf{h}}_{re}^HA\bar{\mathbf{h}}_{ab}\bar{\mathbf{h}}_{rb}^HBA^H\bar{\mathbf{h}}_{re}\\ &+\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{ab}^H\bar{\mathbf{h}}_{ae} + \bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}\bar{\mathbf{h}}_{ae}\\ &+\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{ab}^H\mathbf{A}^H\bar{\mathbf{h}}_{re} + \bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\bar{\mathbf{h}}_{rb}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re}\\ &= \left|(\bar{\mathbf{h}}_{ae}^H + \bar{\mathbf{h}}_{re}^H\mathbf{A})(\bar{\mathbf{h}}_{ab} + \mathbf{B}^H\bar{\mathbf{h}}_{rb})\right|^2\\ &= \left|(\bar{\mathbf{h}}_{ae}^H + \bar{\mathbf{h}}_{re}^H\Phi_2\mathbf{H}_{ar})(\bar{\mathbf{h}}_{ab} + \mathbf{H}_{ar}^H\Phi_1^H\bar{\mathbf{h}}_{rb})\right|^2\end{aligned} \tag{41}$$

$$\begin{aligned}s_{12} &= \sigma_{ae}^2\bar{\mathbf{h}}_{ab}^H\bar{\mathbf{h}}_{ab} + \sigma_{ae}^2\bar{\mathbf{h}}_{rb}^H\mathbf{B}\bar{\mathbf{h}}_{ab}\\ &+\sigma_{ae}^2\bar{\mathbf{h}}_{ab}^H\mathbf{B}^H\bar{\mathbf{h}}_{rb} + \sigma_{ae}^2\bar{\mathbf{h}}_{rb}^H\mathbf{B}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\\ &= \sigma_{ae}^2\left|(\bar{\mathbf{h}}_{rb}^H\mathbf{B} + \bar{\mathbf{h}}_{ab}^H)\right|^2\\ &= \sigma_{ae}^2\left|(\bar{\mathbf{h}}_{rb}^H\Phi_1\mathbf{H}_{ar} + \bar{\mathbf{h}}_{ab}^H)\right|^2\end{aligned} \tag{42}$$

$$\begin{aligned}s_{13} &= \sigma_{ab}^2\bar{\mathbf{h}}_{ae}^H\bar{\mathbf{h}}_{ae} + \sigma_{ab}^2\bar{\mathbf{h}}_{ae}^H\mathbf{A}^H\bar{\mathbf{h}}_{re}\\ &+\sigma_{ab}^2\bar{\mathbf{h}}_{re}^H\mathbf{A}\bar{\mathbf{h}}_{ae} + \sigma_{ab}^2\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{A}^H\bar{\mathbf{h}}_{re}\\ &= \sigma_{ab}^2\left|(\bar{\mathbf{h}}_{re}^H\mathbf{A} + \bar{\mathbf{h}}_{ae}^H)\right|^2\\ &= \sigma_{ab}^2\left|(\bar{\mathbf{h}}_{re}^H\Phi_2\mathbf{H}_{ar} + \bar{\mathbf{h}}_{ae}^H)\right|^2\end{aligned} \tag{43}$$

$$\begin{aligned}s_{14} &= \sigma_{rb}^2\bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\mathbf{B}\bar{\mathbf{h}}_{ae} + \sigma_{rb}^2\bar{\mathbf{h}}_{ae}^H\mathbf{B}^H\mathbf{B}\mathbf{A}^H\bar{\mathbf{h}}_{re}\\ &+\sigma_{rb}^2\bar{\mathbf{h}}_{ae}^H\mathbf{B}^HB\bar{\mathbf{h}}_{ae} + \sigma_{rb}^2\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\mathbf{B}\bar{\mathbf{h}}_{ae}\\ &+\sigma_{rb}^2\bar{\mathbf{h}}_{re}^H\mathbf{A}\mathbf{B}^H\mathbf{B}A^H\bar{\mathbf{h}}_{re}\\ &= \sigma_{rb}^2\left|(\bar{\mathbf{h}}_{re}^H\mathbf{A} + \bar{\mathbf{h}}_{ae}^H)\mathbf{B}^H\right|^2\\ &= \sigma_{rb}^2\left|(\bar{\mathbf{h}}_{re}^H\Phi_2\mathbf{H}_{ar} + \bar{\mathbf{h}}_{ae}^H)\mathbf{H}_{ar}^H\right|^2\end{aligned} \tag{44}$$

$$\begin{aligned}s_{15} &= \sigma_{re}^2\mathbf{h}_{ab}^H\mathbf{A}^H\mathbf{A}\mathbf{h}_{ab} + \sigma_{re}^2\bar{\mathbf{h}}_{rb}^H\mathbf{B}\mathbf{A}^H\mathbf{A}\bar{\mathbf{h}}_{ab}\\ &+\sigma_{re}^2\bar{\mathbf{h}}_{ab}^H\mathbf{A}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb} + \sigma_{re}^2\bar{\mathbf{h}}_{rb}^H\mathbf{B}\mathbf{A}^H\mathbf{A}\mathbf{B}^H\bar{\mathbf{h}}_{rb}\\ &= \sigma_{re}^2\left|(\bar{\mathbf{h}}_{rb}^H\mathbf{B} + \bar{\mathbf{h}}_{ab}^H)\mathbf{A}^H\right|^2\\ &= \sigma_{re}^2\left|(\bar{\mathbf{h}}_{rb}^H\Phi_1\mathbf{H}_{ar} + \bar{\mathbf{h}}_{ab}^H)\mathbf{H}_{ar}^H\right|^2\end{aligned} \tag{45}$$

Finally, the expectation of q_1 can be written as

$$\begin{aligned}\mathbb{E}(q_1) &= s_{11} + s_{12} + s_{13} + s_{14} + s_{15}\\ &+M_a\sigma_{ae}^2\sigma_{ab}^2 + \sigma_{ae}^2\sigma_{rb}^2\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H)\\ &+\sigma_{ab}^2\sigma_{re}^2\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H) + \sigma_{re}^2\sigma_{rb}^2\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H\mathbf{H}_{ar}\mathbf{H}_{ar}^H)\\ &= \left|(\bar{\mathbf{h}}_{ae}^H + \bar{\mathbf{h}}_{re}^H\Phi_2\mathbf{H}_{ar})(\bar{\mathbf{h}}_{ab} + \mathbf{H}_{ar}^H\Phi_1^H\bar{\mathbf{h}}_{rb})\right|^2\\ &+\sigma_{ae}^2\left|(\bar{\mathbf{h}}_{rb}^H\Phi_1\mathbf{H}_{ar} + \bar{\mathbf{h}}_{ab}^H)\right|^2 + \sigma_{ab}^2\left|(\bar{\mathbf{h}}_{re}^H\Phi_2\mathbf{H}_{ar} + \bar{\mathbf{h}}_{ae}^H)\right|^2\\ &+\sigma_{rb}^2\left|(\bar{\mathbf{h}}_{re}^H\Phi_2\mathbf{H}_{ar} + \bar{\mathbf{h}}_{ae}^H)\mathbf{H}_{ar}^H\right|^2 + \sigma_{re}^2\left|(\bar{\mathbf{h}}_{rb}^H\Phi_1\mathbf{H}_{ar} + \bar{\mathbf{h}}_{ab}^H)\mathbf{H}_{ar}^H\right|^2\\ &+M_a\sigma_{ae}^2\sigma_{ab}^2 + \sigma_{ae}^2\sigma_{rb}^2\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H) + \sigma_{ab}^2\sigma_{re}^2\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H)\\ &+\sigma_{re}^2\sigma_{rb}^2\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H\mathbf{H}_{ar}\mathbf{H}_{ar}^H)\end{aligned} \tag{46}$$

In the same way, the expectation of q_2 can be derived as

$$\begin{aligned}\mathbb{E}(q_2) &= \mathbb{E}\left(\left\|\mathbf{H}_{ar}^H\Phi_1^H(\bar{\mathbf{h}}_{rb} + \tilde{\mathbf{h}}_{rb})\right\|_2^2\right)\\ &= \left|(\bar{\mathbf{h}}_{rb}^H\mathbf{B} + \bar{\mathbf{h}}_{ab}^H)\right|^2 + \sigma_{rb}^2\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H) + M_a\sigma_{ab}^2\end{aligned} \tag{47}$$

Therefore, the expectation expression of the denominator $\mathbb{E}(g_1(\Phi_1, \Phi_2))$ can be obtained.

Since the form of the numerator is similar to that of denominator in (11), the expectation expression of the denominator can be derived as

$$\begin{aligned}&f_2(\Phi_1, \Phi_2)\\ &= \mathbb{E}(f_1(\Phi_1, \Phi_2))\\ &= P_t\left|(\bar{\mathbf{h}}_{ab}^H + \bar{\mathbf{h}}_{rb}^H\Phi_2\mathbf{H}_{ar})(\bar{\mathbf{h}}_{ab} + \mathbf{H}_{ar}^H\Phi_1^H\bar{\mathbf{h}}_{rb})\right|^2\\ &+P_t\sigma_{ab}^2\left|(\bar{\mathbf{h}}_{rb}^H\Phi_1\mathbf{H}_{ar} + \bar{\mathbf{h}}_{ab}^H)\right|^2 + P_t\sigma_{ab}^2\left|(\bar{\mathbf{h}}_{rb}^H\Phi_2\mathbf{H}_{ar} + \bar{\mathbf{h}}_{ab}^H)\right|^2\\ &+P_t\sigma_{rb}^2\left|(\bar{\mathbf{h}}_{rb}^H\Phi_2\mathbf{H}_{ar} + \bar{\mathbf{h}}_{ab}^H)\mathbf{H}_{ar}^H\right|^2 + \sigma^2\left|(\bar{\mathbf{h}}_{rb}^H\Phi_1\mathbf{H}_{ar} + \bar{\mathbf{h}}_{ab}^H)\right|^2\\ &+P_t\sigma_{rb}^2\left|(\bar{\mathbf{h}}_{rb}^H\Phi_1\mathbf{H}_{ar} + \bar{\mathbf{h}}_{ab}^H)\mathbf{H}_{ar}^H\right|^2 + \sigma^2\sigma_{rb}^2\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H)\\ &+M_a\sigma^2\sigma_{ab}^2 + P_tM_a\sigma_{ab}^4 + 2P_t\sigma_{ab}^2\sigma_{rb}^2\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H)\\ &+P_t\sigma_{rb}^4\mathrm{Tr}(\mathbf{H}_{ar}\mathbf{H}_{ar}^H\mathbf{H}_{ar}\mathbf{H}_{ar}^H)\end{aligned} \tag{48}$$

Thus, the proof is completed.

REFERENCES

[1] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. PP, pp. 1–1, 2018.

[2] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 903–907, 2012.

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

[4] 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 Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 932–940, 2015.

[5] X. Tian, M. Li, and Q. Liu, "Random-training-assisted pilot spoofing detection and security enhancement," *IEEE Access*, vol. 5, pp. 27 384–27 399, 2017.

[6] J. Zhao and Y. Liu, "A survey of intelligent reflecting surfaces (irss): Towards 6g wireless communication networks," *arXiv preprint arXiv:1907.04789*, 2019.

[7] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface aided wireless communications: A tutorial," *arXiv preprint arXiv:2007.02759*, 2020.

[8] H. Guo, Y.-C. Liang, J. Chen, and E. G. Larsson, "Weighted sum-rate maximization for intelligent reflecting surface enhanced wireless networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[9] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.

[10] L. Dong and H. M. Wang, "Secure mimo transmission via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 9, no. 6, pp. 787–790, 2020.

[11] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 4157–4170, 2019.

[12] B. Lyu, D. T. Hoang, S. Gong, D. Niyato, and D. I. Kim, "Irs-based wireless jamming attacks: When jammers can attack without power," *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1663–1667, 2020.

[13] A. Taha, M. Alrabeiah, and A. Alkhateeb, "Enabling large intelligent surfaces with compressive sensing and deep learning," *arXiv preprint arXiv:1904.10136*, 2019.

[14] A. Taha, Y. Zhang, F. B. Mismar, and A. Alkhateeb, "Deep reinforcement learning for intelligent reflecting surfaces: Towards standalone operation," *arXiv preprint arXiv:2002.11101*, 2020.

[15] J. Moon, S. H. Lee, H. Lee, and I. Lee, "Proactive eavesdropping with jamming and eavesdropping mode selection," *IEEE Transactions on Wireless Communications*, vol. 18, no. 7, pp. 3726–3738, 2019.

[16] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: Design and performance analysis," *IEEE Transactions on Wireless Communications*, vol. PP, no. 7, pp. 1–1, 2017.

[17] Q. Zhang, S. Jin, K.-K. Wong, H. Zhu, and M. Matthaiou, "Power scaling of uplink massive mimo systems with arbitrary-rank channel means," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 5, pp. 966–981, 2014.

[18] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Communications Letters*, pp. 1–1, 2020.

[19] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Communication Magazine*, vol. 58, no. 1, pp. 106–112, 2019.