Artificial-Noise-Aided Secure MIMO Wireless Communications via Intelligent Reflecting Surface

Sheng Hong, Cunhua Pan, Hong Ren, Kezhi Wang, and Arumugam Nallanathan, *Fellow, IEEE*

***Abstract*—This paper considers an artificial noise (AN)-aided secure MIMO wireless communication system. To enhance the system security performance, the advanced intelligent reflecting surface (IRS) is invoked, and the base station (BS), legitimate information receiver (IR) and eavesdropper (Eve) are equipped with multiple antennas. With the aim for maximizing the secrecy rate (SR), the transmit precoding (TPC) matrix at the BS, covariance matrix of AN and phase shifts at the IRS are jointly optimized subject to constrains of transmit power limit and unit modulus of IRS phase shifts. Then, the secrecy rate maximization (SRM) problem is formulated, which is a non-convex problem with multiple coupled variables. To tackle it, we propose to utilize the block coordinate descent (BCD) algorithm to alternately update the variables while keeping SR non-decreasing. Specifically, the optimal TPC matrix and AN covariance matrix are derived by Lagrangian multiplier method, and the optimal phase shifts are obtained by Majorization-Minimization (MM) algorithm. Since all variables can be calculated in closed form, the proposed algorithm is very efficient. We also extend the SRM problem to the more general multiple-IRs scenario and propose a BCD algorithm to solve it. Simulation results validate the effectiveness of system security enhancement via an IRS.**

***Index Terms*—Intelligent Reflecting Surface (IRS), Reconfigurable Intelligent Surfaces, Secure Communication, Physical Layer Security, Artificial Noise (AN), MIMO.**

I. Introduction

THE next-generation (i.e, 6G) communication is expected to be a sustainable green, cost-effective and secure communication system [1]. In particular, secure communication is crucially important in 6G communication networks since communication environment becomes increasingly complicated and the security of private information is imperative. The information security using crytographic encryption (in the network layer) is a conventional secure communication technique, which suffers from the vulnerabilities, such as secret key distribution, protection and management [2]. Unlike this network layer security approach, the physical layer security can guarantee good security performance bypassing the relevant manipulations on the secret key, thus is more attractive for the academia and industry [3]. There are various physical-layer secrecy scenarios. The first one is the classical physical-layer secrecy setting where there is one legitimate information receiver (IR) and one eavesdropper (Eve) operating over a single-input-single-output (SISO) channel (i.e., the so-called three-terminal SISO Gaussian wiretap channel) [4]. The second one considers the physical-layer secrecy with an IR and Eve operating over a multiple-input-single-output (MISO) channel, which is called as three-terminal MISO Gaussian wiretap channel. The third one is a renewed and timely scenario with one IR and one Eve operating over a multiple-input-multiple-output (MIMO) channel, which is named as three-terminal MIMO Gaussian wiretap channel [5], [6] and is the focus of this paper. A novel idea in physical-layer security is to transmit artificial noise (AN) from the base station (BS) to contaminate the Eve's received signal [7]. For AN-aided secure systems, while most of the existing AN-aided design papers focused on the MISO wiretap channel and null-space AN [5], [8], designing the transmit precoding (TPC) matrix together with AN covariance matrix for the MIMO wiretap channel is more challenging [9].

In general, the achieved secrecy rate (SR) is limited by the channel difference between the BS-IR link and the BS-Eve link. The AN-aided method can further improve the SR, but it consumes the transmit power destined for the legitimate IR. When the transmit power is confined, the performance bottleneck always exists for the AN-aided secure communication. To conquer the dilemma, the recently proposed intelligent reflecting surface (IRS) technique can be exploited. Since higher SR can be achieved by enhancing the channel quality in the BS-IR link and degrading the channel condition in the BS-Eve link, the IRS can serve as a powerful complement to AN-aided secure communication due to its capability of reconfiguring the wireless propagation environment.

This work was supported by the National Natural Science Foundation of China (61661032), the Young Natural Science Foundation of Jiangxi Province (20181BAB202002), the China Postdoctoral Science Foundation (2017M622102), the Foundation from China Scholarship Council (201906825071), and the EPSRC grant EP/R006466/1. *(Correspondence author: Cunhua Pan.)*

S. Hong is with Information Engineering School of Nanchang University, Nanchang 330031, China. (email: shenghong@ncu.edu.cn). C. Pan, H. Ren, and A. Nallanathan are with the School of Electronic Engineering and Computer Science at Queen Mary University of London, London E1 4NS, U.K. (e-mail:{c.pan, h.ren, a.nallanathan}@qmul.ac.uk). K. Wang is with Department of Computer and Information Sciences, Northumbria University, UK. (email: kezhi.wang@northumbria.ac.uk)

The IRS technique has been regarded as a revolutionary technique to control and reconfigure the wireless environment [10], [11]. An IRS comprises an array of reflecting elements, which can reflect the incident electromagnetic (EM) wave passively, and the complex reflection coefficients contain the phase shift and amplitude. In practical applications, the phase shifts of the reflection coefficients are discrete due to the manufacturing cost [12]. However, most of the existing contributions on IRS aided wireless communications are based on the assumption of continuous phase shifts [13], [14]. To investigate the potential effect of IRS on the secure communication, we also assume continuous phase shifts to simplify the problem. We evaluate its impact on the system performance in the simulation section. Theoretically, the reflection amplitude of each IRS element can be adjusted for different purposes [10]. However, considering the hardware cost, the reflection amplitude is usually assumed to be 1 for simplicity. By smartly tuning the phase shifts with a preprogrammed controller, the direct signals from the BS and the reflected signals from the IRS can be combined constructively or destructively according to different requirements. Due to the light weight and compact size, the IRS can be integrated into the traditional communication systems with minor modifications [15]. Nowadays, the IRS has been introduced into various wireless communication systems, including the single-user case [16], the multiuser case [13], [17], [18], the mobile edge computing [19], the wireless information and power transfer design [20], and the physical layer security design [21]–[24].

The IRS is promising to strengthen the system security of wireless communication. In [21], [23], the authors investigated the problem of maximizing the achievable SR in a secure MISO communication system aided by IRS, where the TPC matrix at the BS and the phase shifts at the IRS were optimized by an alternate optimization (AO) strategy. To handle the nonconvex unit modulus constraint, the semidefinite relaxation (SDR) [25], majorization-minimization (MM) [13], [26], complex circle manifold (CCM) [27] techniques were proposed to optimize phase shifts. An IRS-assisted MISO secure communication with a single IR and a single Eve was also considered in [22], but it was limited to a special scenario, where the Eve has a stronger channel than the IR, and the two channels from BS to Eve and IR are highly correlated. Under this assumption, the transmit beamforming and the IRS reflection beamforming are jointly optimized to improve the SR. Similarly, a secure IRS-assisted downlink MISO broadcast system was considered in [24], and it assumes that multiple legitimate IRs and multiple Eves are in the same directions to the BS, which implies that the IR channels are highly correlated with the Eve channels. The authors in [28] considered the transmission design for an IRS-aided secure MISO communication with a single IR and a single Eve, in which the system energy consumption is minimized under two assumptions that the channels of access point (AP)-IRS links are rank-one and full-rank. The physical layer security in a simultaneous wireless information and power transfer (SWIPT) system was considered with the aid of IRS [29]. However, there are a paucity of contributions considering the IRS-assisted secure communication with AN. A secure MISO communication system aided by the transmit jamming and AN was considered in [30], where a large number of Eves exist, and the AN beamforming vector and jamming vector were optimized to reap the additional degrees of freedom (DoF) brought by the IRS. The authors in [31] investigated the resource allocation problem in an IRS-assisted MISO communication by jointly optimizing the beamforming vectors, the phase shifts of the IRS, and AN covariance matrix for secrecy rate maximization (SRM), but the direct BS-IRs links and direct BS-Eves links are assumed to be blocked.

Although a few papers have studied the security enhancement for an AN-aided system through the IRS, the existing papers related to this topic either only studied the MISO scenario or assumed special conditions to the channels. The investigation on the MIMO scenario with general channel settings is absent in the existing literature. Hence, we investigate this problem in this paper by employing an IRS in an AN-aided MIMO communication system for the physical layer security enhancement. Specifically, by carefully designing the phase shifts of the IRS, the reflected signals are combined with the direct signals constructively for enhancing the data rate at the IR and destructively for decreasing the rate at the Eve. As a result, the TPC matrix and AN covariance matrix at the BS can be designed flexibly with a higher DoF than the case without IRS. In this work, the TPC matrix, AN covariance matrix and the phase shift matrix are jointly optimized. Since these optimization variables are highly coupled, an efficient algorithm based on the block coordinate descent (BCD) and MM techniques for solving the problem is proposed.

We summarize our main contributions as follows:

1) This is the first research on exploiting an IRS to enhance security in AN-aided MIMO communication systems. Specifically, an SRM problem is formulated by jointly optimizing the TPC matrix and AN covariance matrix at the BS, together with the phase shifts of the IRS subject to maximum transmit power limit and the unit modulus constraint of the phase shifts. The objective function (OF) of this problem is the difference of two Shannon capacity expressions, thus is not jointly concave over the three highly-coupled variables. To handle it, the popular minimum mean-square error (MMSE) algorithm is used to reformulate the SRM problem.

2) The BCD algorithm is exploited to optimize the variables alternately. Firstly, given the phase shifts of IRS, the optimal TPC matrix and AN covariance matrix are obtained in semi-closed form by utilizing the Lagrangian multiplier method. Then, given the TPC matrix and AN covariance matrix, the optimization problem for IRS phase shifts is transformed by sophisticated matrix manipulations into a quadratic program problem subject to unit modulus constraints. To solve it, the MM algorithm is utilized, where the phase shifts are derived in closed form iteratively. Based on the BCD-MM algorithm, the original formulated SRM problem can be solved efficiently.
3) The SRM problem is also extended to the more general scenario of multiple legitimate IRs. A new BCD algorithm is proposed to solve it, where the optimal TPC matrix and AN covariance matrix are obtained by solving a quadratically constrained quadratic program (QCQP) problem, and the unit modulus constraint is handled by the penalty convex-concave procedure (CCP) method [32].
4) The simulation results confirm that on the one hand, the IRS can greatly enhance the security of an AN-aided MIMO communication system; on the other hand, the phase shifts of IRS should be properly optimized. Simulation results also show that a larger IRS element number is beneficial to the security performance, and the properly-selected IRS location is important to reap the full potential of IRS.

This paper is organized as follows. Section II provides the signal model of an AN-aided MIMO communication system assisted by an IRS, and the SRM problem formulation. The SRM problem is reformulated in Section III, where the BCD-MM algorithm is proposed to optimize the TPC matrix, AN covariance matrix and phase shifts of IRS. Section IV extends the SRM problem to a more general scenario of multiple IRs. In Section V, numerical simulations are given to validate the algorithm efficiency and security enhancement. Section VI concludes this paper.

Notations: Throughout this paper, boldface lower case, boldface upper case and regular letters are used to denote vectors, matrices, and scalars respectively. $\mathbf{X} \odot \mathbf{Y}$ is the Hadamard product of $\mathbf{X}$ and $\mathbf{Y}$. $\mathrm{Tr}(\mathbf{X})$ and $|\mathbf{X}|$ denote the trace and determinant of $\mathbf{X}$, respectively. $\mathbb{C}^{M\times N}$ denotes the space of $M \times N$ complex matrices. $\mathrm{Re}\{\cdot\}$ and $\arg\{\cdot\}$ denote the real part of a complex value and the extraction of phase information, respectively. $\mathrm{diag}\{\cdot\}$ is the operator for diagonalization. $\mathcal{CN}(\boldsymbol{\mu}, \mathbf{Z})$ represents a circularly symmetric complex gaussian (CSCG) random vector with mean $\boldsymbol{\mu}$ and covariance matrix $\mathbf{Z}$. $(\cdot)^{\mathrm{T}}$, $(\cdot)^{\mathrm{H}}$ and $(\cdot)^{*}$ denote the transpose, Hermitian and conjugate operators, respectively. $(\cdot)^{\star}$ stands for the optimal value, and $(\cdot)^{\dagger}$ means the pseudo-inverse. $[\cdot]^{+}$ is the projection onto the non-negative number, i.e, if $y = [x]^{+}$, then $y = \max\{0, \mathrm{x}\}$.

II. Signal Model and Problem Formulation

A. Signal Model

We consider an IRS-aided communication network shown in Fig. 1 that consists of a BS, a legitimate IR and an Eve, all of which are equipped with multiple antennas. The number of transmit antennas at the BS is $N_T \geq 2$, and the numbers of receive antennas at the legitimate IR and Eve are $N_I \geq 2$ and $N_E \geq 2$, respectively. To ensure secure transmission from the BS to the IR, the AN is sent from the BS to interfere the Eve to achieve the strong security. The BS employs the TPC matrix to transmit

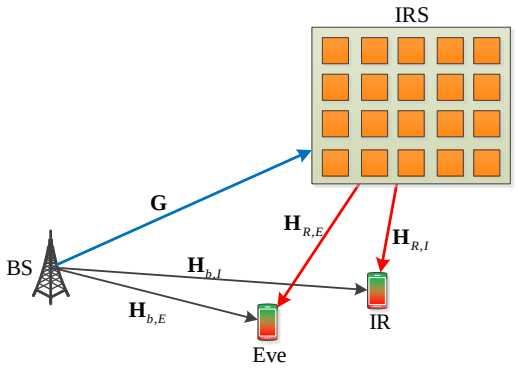

Fig. 1. An AN-aided MIMO secure communication system with IRS.

data streams with AN, and the transmitted signal can be modeled as

$$\mathbf{x} = \mathbf{V}\mathbf{s} + \mathbf{n}, \tag{1}$$

where $\mathbf{V} \in \mathbb{C}^{N_T \times d}$ is the TPC matrix; the number of data streams is $d \leq \min(N_T, N_I)$; the transmitted data towards the IR is $\mathbf{s} \sim \mathcal{CN}(0, \mathbf{I}_d)$; and $\mathbf{n} \in \mathcal{CN}(\mathbf{0}, \mathbf{Z})$ represents the AN random vector with zero mean and covariance matrix $\mathbf{Z}$.

Assuming that the wireless signals are propagated in a non-dispersive and narrow-band way, we model the equivalent channels of the BS-IRS link, the BS-IR link, the BS-Eve link, the IRS-IR link, the IRS-Eve link by the matrices $\mathbf{G} \in \mathbb{C}^{M\times N_T}$, $\mathbf{H}_{b,I} \in \mathbb{C}^{N_I\times N_T}$, $\mathbf{H}_{b,E} \in \mathbb{C}^{N_E\times N_T}$, $\mathbf{H}_{R,I} \in \mathbb{C}^{N_I\times M}$, $\mathbf{H}_{R,E} \in \mathbb{C}^{N_E\times M}$, respectively. The phase shift coefficients of IRS are collected in a diagonal matrix defined by $\boldsymbol{\Phi} = \mathrm{diag}\{\phi_1, \cdots, \phi_m, \cdots, \phi_M\}$ and $\phi_m = e^{j\theta_m}$, where $\theta_m \in [0, 2\pi]$ denotes the phase shift of the m-th reflection element. The multi-path signals that have been reflected by multiple times are considered to

be absorbed and diffracted, then the signal received at the legitimate IR is given by

$$\mathbf{y}_I = (\mathbf{H}_{b,I} + \mathbf{H}_{R,I}\mathbf{\Phi}\mathbf{G})\mathbf{x} + \mathbf{n}_I, \tag{2}$$

where $\mathbf{n}_I$ is the random noise vector at IR obeying the distribution $\mathbf{n}_I \sim \mathcal{CN}(\mathbf{0}, \sigma_I^2\mathbf{I}_{N_I})$. The signal received at the Eve is

$$\mathbf{y}_E = (\mathbf{H}_{b,E} + \mathbf{H}_{R,E}\mathbf{\Phi}\mathbf{G})\mathbf{x} + \mathbf{n}_E, \tag{3}$$

where $\mathbf{n}_E$ is the Eve's noise vector following the distribution $\mathbf{n}_E \sim \mathcal{CN}(\mathbf{0}, \sigma_E^2\mathbf{I}_{N_E})$.

Assume that the BS has acquired the prior information of all the channel state information (CSI). Then the BS is responsible for optimizing the IRS phase shifts and sending them back to the IRS controller through a separate low-rate communication link such as wireless links [10], [12] or wired lines [33]. The assumption of perfect CSI knowledge is idealistic, since the CSI estimation for IRS networks is challenging. However, the algorithms developed allow us to derive the relevant performance upper bounds for realistic scenarios in the presence of realistic CSI errors. Recently, we have investigated the design of robust and secure transmission in IRS-aided MISO wireless communication systems in [34] by considering the statistical CSI error model associated with the cascaded channels for the eavesdropper. Its extension to the MIMO scenario will be studied in our future work.

Upon substituting $\mathbf{x}$ into (2), $\mathbf{y}_I$ can be rewritten as

$$\mathbf{y}_I = \hat{\mathbf{H}}_I(\mathbf{V}\mathbf{s} + \mathbf{n}) + \mathbf{n}_I = \hat{\mathbf{H}}_I\mathbf{V}\mathbf{s} + \hat{\mathbf{H}}_I\mathbf{n} + \mathbf{n}_I, \tag{4}$$

where $\hat{\mathbf{H}}_I \triangleq \mathbf{H}_{b,I} + \mathbf{H}_{R,I}\mathbf{\Phi}\mathbf{G}$ is defined as the equivalent channel spanning from the BS to the legitimate IR. Then, the data rate (bit/s/Hz) achieved by the legitimate IR is given by

$$R_I(\mathbf{V}, \mathbf{\Phi}, \mathbf{Z}) = \log\left|\mathbf{I} + \hat{\mathbf{H}}_I\mathbf{V}\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{J}_I^{-1}\right|, \tag{5}$$

where $\mathbf{J}_I$ is the interference-plus-noise covariance matrix given by $\mathbf{J}_I \triangleq \hat{\mathbf{H}}_I\mathbf{Z}\hat{\mathbf{H}}_I^H + \sigma_I^2\mathbf{I}_{N_I}$.

Upon substituting $\mathbf{x}$ into (3), $\mathbf{y}_E$ can be rewritten as

$$\mathbf{y}_E = \hat{\mathbf{H}}_E(\mathbf{V}\mathbf{s} + \mathbf{n}) + \mathbf{n}_E = \hat{\mathbf{H}}_E\mathbf{V}\mathbf{s} + \hat{\mathbf{H}}_E\mathbf{n} + \mathbf{n}_E, \tag{6}$$

where $\hat{\mathbf{H}}_E \triangleq \mathbf{H}_{b,E} + \mathbf{H}_{R,E}\mathbf{\Phi}\mathbf{G}$ is defined as the equivalent channel spanning from the BS to the Eve. Then, the data rate (bit/s/Hz) achieved by the Eve is given by

$$R_E(\mathbf{V}, \mathbf{\Phi}, \mathbf{Z}) = \log\left|\mathbf{I} + \hat{\mathbf{H}}_E\mathbf{V}\mathbf{V}^H\hat{\mathbf{H}}_E^H\mathbf{J}_E^{-1}\right|, \tag{7}$$

where $\mathbf{J}_E$ is the interference-plus-noise covariance matrix given by $\mathbf{J}_E \triangleq \hat{\mathbf{H}}_E\mathbf{Z}\hat{\mathbf{H}}_E^H + \sigma_E^2\mathbf{I}_{N_E}$. The achievable secrecy rate is given by

$$\begin{aligned}\mathrm{C}_{AN}(\mathbf{V}, \mathbf{\Phi}, \mathbf{Z}) &= [R_I(\mathbf{V}, \mathbf{\Phi}, \mathbf{Z}) - R_E(\mathbf{V}, \mathbf{\Phi}, \mathbf{Z})]^+ \\ &= \log\left|\mathbf{I} + \hat{\mathbf{H}}_I\mathbf{V}\mathbf{V}^H\hat{\mathbf{H}}_I^H(\hat{\mathbf{H}}_I\mathbf{Z}\hat{\mathbf{H}}_I^H + \sigma_I^2\mathbf{I}_{N_I})^{-1}\right| \\ &\quad - \log\left|\mathbf{I} + \hat{\mathbf{H}}_E\mathbf{V}\mathbf{V}^H\hat{\mathbf{H}}_E^H(\hat{\mathbf{H}}_E\mathbf{Z}\hat{\mathbf{H}}_E^H + \sigma_E^2\mathbf{I}_{N_E})^{-1}\right|. \end{aligned} \tag{8}$$

B. Problem Formulation

In this paper, we aim to maximize the SR by jointly optimizing the TPC matrix $\mathbf{V}$ at the BS, the AN covariance matrix $\mathbf{Z}$ at the BS, and the phase shift matrix $\mathbf{\Phi}$ at the IRS subject to the constraints of the maximum transmit power and unit modulus of phase shifts. Hence, we formulate the SRM problem as

$$\max_{\mathbf{V},\mathbf{\Phi},\mathbf{Z}} \quad \mathrm{C}_{AN}(\mathbf{V}, \mathbf{\Phi}, \mathbf{Z}) \tag{9a}$$
$$\text{s.t.} \quad \mathrm{Tr}(\mathbf{V}\mathbf{V}^H + \mathbf{Z}) \le P_T, \tag{9b}$$
$$\mathbf{Z} \succeq 0, \tag{9c}$$
$$|\phi_m| = 1, m = 1, \cdots, M, \tag{9d}$$

where P_T is the maximum transmit power limit. The optimal value of SR in (9) is always non-negative, which can be proved by using contradiction. Assume that the optimal value of SR is negative, then we can simply set the TPC matrix $\mathbf{V}$ to zero matrix, and the resulted SR will be equal to zero, which is larger than a negative SR.

By variable substitution $\mathbf{Z} = \mathbf{V}_E\mathbf{V}_E^H$, where $\mathbf{V}_E \in \mathbb{C}^{N_T \times N_T}$, Problem (9) is equivalent to

$$\max_{\mathbf{V},\mathbf{V}_E,\mathbf{\Phi}} \quad \mathrm{C}_{AN}(\mathbf{V}, \mathbf{V}_E, \mathbf{\Phi}) \tag{10a}$$
$$\text{s.t.} \quad \mathrm{Tr}(\mathbf{V}\mathbf{V}^H + \mathbf{V}_E\mathbf{V}_E^H) \le P_T, \tag{10b}$$
$$|\phi_m| = 1, m = 1, \cdots, M, \tag{10c}$$

where the OF of (10a) is obtained by substituting $\mathbf{Z} = \mathbf{V}_E\mathbf{V}_E{}^H$ into (8). In (10a), the expression of OF is difficult to tackle, and the variables of $\mathbf{V}$, $\mathbf{V}_E$ and $\mathbf{\Phi}$ are coupled with each other, which make Problem (10) difficult to solve. In addition, the unit modulus constraint imposed on the phase shifts in (10c) aggravates the difficulty. In the following, we provide a low-complexity algorithm to solve this problem.

III. A Low-Complexity Algorithm of BCD-MM

Firstly, the OF of Problem (10) is reformulated into a more tractable expression equivalently. Then, the BCD-MM method is proposed for optimizing the TPC matrix $\mathbf{V}$, $\mathbf{V}_E$, and the phase shift matrix $\mathbf{\Phi}$ alternately.

A. Reformulation of the Original Problem

Firstly, the achievable SR $\mathrm{C}_{AN}(\mathbf{V},\mathbf{V}_E,\mathbf{\Phi})$ in (8) can be further simplified as

$$\begin{aligned}
&\mathrm{C}_{AN}(\mathbf{V},\mathbf{V}_{\mathrm{E}},\mathbf{\Phi})\\
&=\log\left|\mathbf{I}_{N_I}+\hat{\mathbf{H}}_I\mathbf{V}\mathbf{V}^H\hat{\mathbf{H}}_I^H(\hat{\mathbf{H}}_I\mathbf{Z}\hat{\mathbf{H}}_I^H+\sigma_I^2\mathbf{I}_{N_I})^{-1}\right|\\
&\quad+\log\left|\hat{\mathbf{H}}_E\mathbf{Z}\hat{\mathbf{H}}_E^H+\sigma_E^2\mathbf{I}_{N_E}\right|\\
&\quad-\log\left|\hat{\mathbf{H}}_E\mathbf{Z}\hat{\mathbf{H}}_E^H+\sigma_E^2\mathbf{I}_{N_E}+\hat{\mathbf{H}}_E\mathbf{V}\mathbf{V}^H\hat{\mathbf{H}}_E^H\right|\\
&=\underbrace{\log\left|\mathbf{I}_{N_I}+\hat{\mathbf{H}}_I\mathbf{V}\mathbf{V}^H\hat{\mathbf{H}}_I^H(\hat{\mathbf{H}}_I\mathbf{V}_E\mathbf{V}_E^H\hat{\mathbf{H}}_I^H+\sigma_I^2\mathbf{I}_{N_I})^{-1}\right|}_{f_1}\\
&\quad+\underbrace{\log\left|\mathbf{I}_{N_E}+\hat{\mathbf{H}}_E\mathbf{V}_E\mathbf{V}_E^H\hat{\mathbf{H}}_E^H(\sigma_E^2\mathbf{I}_{N_E})^{-1}\right|}_{f_2}\\
&\quad\underbrace{-\log\left|\mathbf{I}_{N_E}+\sigma_E^{-2}\hat{\mathbf{H}}_E(\mathbf{V}\mathbf{V}^H+\mathbf{V}_E\mathbf{V}_E^H)\hat{\mathbf{H}}_E^H\right|}_{f_3}. \quad (11)
\end{aligned}$$

The f_1 can be reformulated by exploiting the relationship between the data rate and the mean-square error (MSE) for the optimal decoding matrix. Specifically, the linear decoding matrix $\mathbf{U}_I\in\mathbb{C}^{N_T\times d}$ is applied to estimate the signal vector $\hat{\mathbf{s}}$, and the MSE matrix of estimation is given by

$$\begin{aligned}
&\mathbf{E}_I(\mathbf{U}_I,\mathbf{V},\mathbf{V}_E)\triangleq\mathbb{E}_{\mathbf{s},\mathbf{n},\mathbf{n}_I}\left[(\hat{\mathbf{s}}-\mathbf{s})(\hat{\mathbf{s}}-\mathbf{s})^H\right]\\
&=(\mathbf{U}_I{}^H\hat{\mathbf{H}}_I\mathbf{V}-\mathbf{I}_d)(\mathbf{U}_I{}^H\hat{\mathbf{H}}_I\mathbf{V}-\mathbf{I}_d)^H\\
&\quad+\mathbf{U}_I{}^H(\hat{\mathbf{H}}_I\mathbf{V}_E\mathbf{V}_E{}^H\hat{\mathbf{H}}_I^H+\sigma_I^2\mathbf{I}_{N_I})\mathbf{U}_I. \quad (12)
\end{aligned}$$

By introducing an auxiliary matrix $\mathbf{W}_I\succeq 0$, $\mathbf{W}_I\in\mathbb{C}^{d\times d}$ and using Lemma 4.1 in [35], we have

$$\begin{aligned}
f_1&=\max_{\mathbf{U}_I,\mathbf{W}_I\succeq 0}h_1(\mathbf{U}_I,\mathbf{V},\mathbf{V}_E,\mathbf{W}_I)\\
&\triangleq\max_{\mathbf{U}_I,\mathbf{W}_I\succeq 0}\log|\mathbf{W}_I|-\mathrm{Tr}(\mathbf{W}_I\mathbf{E}_I(\mathbf{U}_I,\mathbf{V},\mathbf{V}_E))+d. \quad (13)
\end{aligned}$$

$h_1(\mathbf{U}_I,\mathbf{V},\mathbf{V}_E,\mathbf{W}_I)$ is concave with respect to (w.r.t.) each matrix of the matrices $\mathbf{U}_I$,$\mathbf{V}$,$\mathbf{V}_E$,$\mathbf{W}_I$ by fixing the other matrices. According to Lemma 4.1 in [35], the optimal $\mathbf{U}_I^\star$, $\mathbf{W}_I^\star$ to achieve the maximum value of $h_1(\mathbf{U}_I,\mathbf{V},\mathbf{V}_E,\mathbf{W}_I)$ are given by

$$\begin{aligned}
\mathbf{U}_I^\star&=\arg\max_{\mathbf{U}_I}h_1(\mathbf{U}_I,\mathbf{V},\mathbf{V}_E,\mathbf{W}_I)\\
&=(\hat{\mathbf{H}}_I\mathbf{V}_E\mathbf{V}_E^H\hat{\mathbf{H}}_I^H+\sigma_I^2\mathbf{I}_{N_I}+\hat{\mathbf{H}}_I\mathbf{V}\mathbf{V}^H\hat{\mathbf{H}}_I^H)^{-1}\hat{\mathbf{H}}_I\mathbf{V}, \quad (14a)\\
\mathbf{W}_I^\star&=\arg\max_{\mathbf{W}_I\succeq 0}h_1(\mathbf{U}_I,\mathbf{V},\mathbf{V}_E,\mathbf{W}_I)\\
&=[\mathbf{E}_I(\mathbf{U}_I^\star,\mathbf{V},\mathbf{V}_E)]^{-1}\\
&=[(\mathbf{U}_I^{\star H}\hat{\mathbf{H}}_I\mathbf{V}-\mathbf{I}_d)(\mathbf{U}_I^{\star H}\hat{\mathbf{H}}_I\mathbf{V}-\mathbf{I}_d)^H\\
&\quad+\mathbf{U}_I^{\star H}(\hat{\mathbf{H}}_I\mathbf{V}_E\mathbf{V}_E^H\hat{\mathbf{H}}_I^H+\sigma_I^2\mathbf{I}_{N_I})\mathbf{U}_I^\star]^{-1}. \quad (14b)
\end{aligned}$$

Similarly, by introducing the auxiliary variables $\mathbf{W}_E\succeq 0$, $\mathbf{W}_E\in\mathbb{C}^{N_T\times N_T}$, $\mathbf{U}_E\in\mathbb{C}^{N_E\times N_T}$, and exploiting Lemma 4.1 in [35], we have

$$\begin{aligned}
f_2&=\max_{\mathbf{U}_E,\mathbf{W}_E\succeq 0}h_2(\mathbf{U}_E,\mathbf{V}_E,\mathbf{W}_E)\\
&\triangleq\max_{\mathbf{U}_E,\mathbf{W}_E\succeq 0}\log|\mathbf{W}_E|-\mathrm{Tr}(\mathbf{W}_E\mathbf{E}_E(\mathbf{U}_E,\mathbf{V}_E))+N_t. \quad (15)
\end{aligned}$$

$h_2(\mathbf{U}_E,\mathbf{V}_E,\mathbf{W}_E)$ is concave w.r.t each matrix of the matrices $\mathbf{U}_E$,$\mathbf{V}_E$,$\mathbf{W}_E$ when the other matrices are fixed. According to Lemma 4.1 in [35], the optimal $\mathbf{U}_E^\star$, $\mathbf{W}_E^\star$ to achieve the maximum value of $h_2(\mathbf{U}_E,\mathbf{V}_E,\mathbf{W}_E)$ are given by

$$\begin{aligned}
\mathbf{U}_E^\star&=\arg\max_{\mathbf{U}_E}h_2(\mathbf{U}_E,\mathbf{V}_E,\mathbf{W}_E)\\
&=(\sigma_E^2\mathbf{I}_{N_E}+\hat{\mathbf{H}}_E\mathbf{V}_E\mathbf{V}_E^H\hat{\mathbf{H}}_E^H)^{-1}\hat{\mathbf{H}}_E\mathbf{V}_E, \quad (16a)\\
\mathbf{W}_E^\star&=\arg\max_{\mathbf{W}_E\succeq 0}h_2(\mathbf{U}_E,\mathbf{V}_E,\mathbf{W}_E)=[\mathbf{E}_E(\mathbf{U}_E^\star,\mathbf{V}_E)]^{-1}\\
&=[(\mathbf{U}_E{}^{\star H}\hat{\mathbf{H}}_E\mathbf{V}_E-\mathbf{I}_{N_T})(\mathbf{U}_E^{\star H}\hat{\mathbf{H}}_E\mathbf{V}_E-\mathbf{I}_{N_T})^H\\
&\quad+\mathbf{U}_E^{\star H}(\sigma_E^2\mathbf{I}_{N_E})\mathbf{U}_E^\star]^{-1}. \quad (16b)
\end{aligned}$$

By using Lemma 1 in [9], we have

$$\begin{aligned}
f_3&=\max_{\mathbf{W}_X\succeq 0}h_3(\mathbf{V},\mathbf{V}_E,\mathbf{W}_X)\\
&=\max_{\mathbf{W}_X\succeq 0}\log|\mathbf{W}_X|-\mathrm{Tr}(\mathbf{W}_X\mathbf{E}_X(\mathbf{V},\mathbf{V}_E))+N_E, \quad (17)
\end{aligned}$$

where $\mathbf{W}_X\succeq 0$, $\mathbf{W}_X\in\mathbb{C}^{N_E\times N_E}$ is the introduced auxiliary matrix variable, and

$$\mathbf{E}_X(\mathbf{V},\mathbf{V}_E)\triangleq\mathbf{I}_{N_E}+\sigma_E^{-2}\hat{\mathbf{H}}_E(\mathbf{V}\mathbf{V}^H+\mathbf{V}_E\mathbf{V}_E^H)\hat{\mathbf{H}}_E^H. \quad (18)$$

$h_3(\mathbf{V},\mathbf{V}_E,\mathbf{W}_X)$ is concave w.r.t each matrix of $\mathbf{V},\mathbf{V}_E,\mathbf{W}_X$ when the other matrices are fixed. The optimal $\mathbf{W}_X^\star$ to achieve the maximum value of $h_3(\mathbf{V},\mathbf{V}_E,\mathbf{W}_X)$ is given by

$$\begin{aligned}
\mathbf{W}_X^\star&=\arg\max_{\mathbf{W}_X\succeq 0}h_3(\mathbf{V},\mathbf{V}_E,\mathbf{W}_X)\\
&=[\mathbf{E}_X(\mathbf{V},\mathbf{V}_E)]^{-1}. \quad (19)
\end{aligned}$$

By substituting (13), (15), (17) into (11), we have

$$\mathrm{C}_{AN}(\mathbf{V},\mathbf{V}_E,\mathbf{\Phi})=\max_{\mathbf{U}_I,\mathbf{W}_I\succeq 0,\mathbf{U}_E,\mathbf{W}_E\succeq 0,\mathbf{W}_X\succeq 0}\mathrm{C}_{AN}^l(\mathbf{T}), \quad (20)$$

where $\mathbf{T}=[\mathbf{U}_I,\mathbf{W}_I,\mathbf{U}_E,\mathbf{W}_E,\mathbf{W}_X,\mathbf{V},\mathbf{V}_E,\mathbf{\Phi}]$ and

$$\begin{aligned}
\mathrm{C}_{AN}^l(\mathbf{T})&\triangleq h_1(\mathbf{U}_I,\mathbf{V},\mathbf{V}_E,\mathbf{W}_I)+h_2(\mathbf{U}_E,\mathbf{V}_E,\mathbf{W}_E)\\
&\quad+h_3(\mathbf{V},\mathbf{V}_E,\mathbf{W}_X). \quad (21)
\end{aligned}$$

Obviously, $\mathrm{C}_{AN}^l(\mathbf{T})$ is a concave function for each of the matrices $\mathbf{U}_I$,$\mathbf{W}_I$,$\mathbf{U}_E$,$\mathbf{W}_E$,$\mathbf{W}_X$,$\mathbf{V}$,$\mathbf{V}_E$,$\mathbf{\Phi}$ when the other matrices are fixed. By substituting (20) into Problem (10), we have the following equivalent problem:

$$\begin{aligned}
&\max_{\mathbf{U}_I,\mathbf{W}_I\succeq 0,\mathbf{U}_E,\mathbf{W}_E\succeq 0,\mathbf{W}_X\succeq 0,\mathbf{V},\mathbf{V}_E,\mathbf{\Phi}} \quad \mathrm{C}_{AN}^l(\mathbf{T}) \quad (22a)\\
&\text{s.t.}\quad \mathrm{Tr}(\mathbf{V}\mathbf{V}^H+\mathbf{V}_E\mathbf{V}_E{}^H)\le P_T, \quad (22b)\\
&\qquad |\phi_m|=1, m=1,\cdots,M. \quad (22c)
\end{aligned}$$

To solve Problem (22), we apply the BCD method, each iteration of which consists of the following two sub-iterations. Firstly, given $\mathbf{V}, \mathbf{V}_E, \mathbf{\Phi}$, update $\mathbf{U}_I, \mathbf{W}_I, \mathbf{U}_E, \mathbf{W}_E, \mathbf{W}_X$ by using (14a), (14b), (16a), (16b), (19) respectively. Secondly, given $\mathbf{U}_I, \mathbf{W}_I, \mathbf{U}_E, \mathbf{W}_E, \mathbf{W}_X$, update $\mathbf{V}, \mathbf{V}_E, \mathbf{\Phi}$ by solving the following subproblem:

$$\begin{aligned}\min_{\mathbf{V},\mathbf{V}_E,\mathbf{\Phi}} \{&-\mathrm{Tr}(\mathbf{W}_I\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I) - \mathrm{Tr}(\mathbf{W}_I\mathbf{U}_I^H\hat{\mathbf{H}}_I\mathbf{V})\\ &+\mathrm{Tr}(\mathbf{V}^H\mathbf{H}_V\mathbf{V}) - \mathrm{Tr}(\mathbf{W}_E\mathbf{V}_E^H\hat{\mathbf{H}}_E^H\mathbf{U}_E)\\ &-\mathrm{Tr}(\mathbf{W}_E\mathbf{U}_E^H\hat{\mathbf{H}}_E\mathbf{V}_E) + \mathrm{Tr}(\mathbf{V}_E^H\mathbf{H}_{VE}\mathbf{V}_E)\} \quad (23a)\\ \text{s.t.}\quad &\mathrm{Tr}(\mathbf{V}\mathbf{V}^H + \mathbf{V}_E\mathbf{V}_E^H) \le P_T, \quad (23b)\\ &|\phi_m| = 1, m = 1, \cdots, M, \quad (23c)\end{aligned}$$

where

$$\mathbf{H}_V = \hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I^H\hat{\mathbf{H}}_I + \sigma_E^{-2}\hat{\mathbf{H}}_E^H\mathbf{W}_X\hat{\mathbf{H}}_E, \quad (24a)$$

$$\mathbf{H}_{VE} = \hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I^H\hat{\mathbf{H}}_I + \hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E\mathbf{U}_E^H\hat{\mathbf{H}}_E + \sigma_E^{-2}\hat{\mathbf{H}}_E^H\mathbf{W}_X\hat{\mathbf{H}}_E. \quad (24b)$$

Problem (23) is obtained from Problem (22) by taking the $\mathbf{U}_I, \mathbf{W}_I, \mathbf{U}_E, \mathbf{W}_E, \mathbf{W}_X$ as constant values, and the specific derivations are given in Appendix A.

Now, we devote to solve Problem (23) equivalently instead of Problem (10), and the matrices $\mathbf{V}$, $\mathbf{V}_E$, and phase shift matrix $\mathbf{\Phi}$ will be optimized.

B. Optimizing the Matrices $\mathbf{V}$ *and* $\mathbf{V}_E$

In this subsection, the TPC matrix $\mathbf{V}$ and matrix $\mathbf{V}_E$ are optimized by fixing $\mathbf{\Phi}$. Specifically, the unit modulus constraint on the phase shifts $\mathbf{\Phi}$ is removed, and the updated optimization problem from Problem (23) is given by

$$\begin{aligned}\min_{\mathbf{V},\mathbf{V}_E} \{&-\mathrm{Tr}(\mathbf{W}_I\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I) - \mathrm{Tr}(\mathbf{W}_I\mathbf{U}_I^H\hat{\mathbf{H}}_I\mathbf{V})\\ &+\mathrm{Tr}(\mathbf{V}^H\mathbf{H}_V\mathbf{V}) - \mathrm{Tr}(\mathbf{W}_E\mathbf{V}_E^H\hat{\mathbf{H}}_E^H\mathbf{U}_E)\\ &-\mathrm{Tr}(\mathbf{W}_E\mathbf{U}_E^H\hat{\mathbf{H}}_E\mathbf{V}_E) + \mathrm{Tr}(\mathbf{V}_E^H\mathbf{H}_{VE}\mathbf{V}_E)\} \quad (25a)\\ \text{s.t.}\quad &\mathrm{Tr}(\mathbf{V}\mathbf{V}^H + \mathbf{V}_E\mathbf{V}_E^H) \le P_T. \quad (25b)\end{aligned}$$

The above problem is a convex QCQP problem, and the standard optimization packages, such as CVX [36] can be exploited to solve it. However, the computational burden is heavy. To reduce the complexity, the semi-closed forms of expressions of the optimal TPC matrix and AN covariance matrix are provided by applying the Lagrangian multiplier method.

Since Problem (25) is a convex problem, the Slater's condition is satisfied, where the duality gap between Problem (25) and its dual problem is zero. Thus, Problem (25) can be solved by addressing its dual problem if the dual problem is easier. For this purpose, by introducing Lagrange multiplier λ to combine the the constraint and OF of Problem (25), the Lagrangian function of Problem (25) is obtained as

$$\begin{aligned}\mathcal{L}(\mathbf{V}, \mathbf{V}_E, \lambda) \triangleq &-\mathrm{Tr}(\mathbf{W}_I\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I) - \mathrm{Tr}(\mathbf{W}_I\mathbf{U}_I^H\hat{\mathbf{H}}_I\mathbf{V})\\ &+\mathrm{Tr}(\mathbf{V}^H\mathbf{H}_V\mathbf{V}) - \mathrm{Tr}(\mathbf{W}_E\mathbf{V}_E^H\hat{\mathbf{H}}_E^H\mathbf{U}_E)\\ &- \mathrm{Tr}(\mathbf{W}_E\mathbf{U}_E^H\hat{\mathbf{H}}_E\mathbf{V}_E) + \mathrm{Tr}\left(\mathbf{V}_E^H\mathbf{H}_{VE}\mathbf{V}_E\right)\\ &+ \lambda[\mathrm{Tr}\left(\mathbf{V}\mathbf{V}^H + \mathbf{V}_E\mathbf{V}_E^H\right) - P_T]\\ = &-\mathrm{Tr}(\mathbf{W}_I\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I) - \mathrm{Tr}(\mathbf{W}_I\mathbf{U}_I^H\hat{\mathbf{H}}_I\mathbf{V}) - \lambda P_T\\ &- \mathrm{Tr}(\mathbf{W}_E\mathbf{V}_E^H\hat{\mathbf{H}}_E^H\mathbf{U}_E) - \mathrm{Tr}(\mathbf{W}_E\mathbf{U}_E^H\hat{\mathbf{H}}_E\mathbf{V}_E)\\ &+\mathrm{Tr}\left[\mathbf{V}^H(\mathbf{H}_V + \lambda\mathbf{I})\mathbf{V}\right] + \mathrm{Tr}\left[\mathbf{V}_E^H(\mathbf{H}_{VE} + \lambda\mathbf{I})\mathbf{V}_E\right]. \quad (26)\end{aligned}$$

Then the dual problem of Problem (25) is

$$\begin{aligned}\max_{\lambda} \quad & h(\lambda) \quad (27a)\\ \text{s.t.} \quad & \lambda \ge 0, \quad (27b)\end{aligned}$$

where $h(\lambda)$ is the dual function given by

$$h(\lambda) \triangleq \min_{\mathbf{V},\mathbf{V}_E} \mathcal{L}(\mathbf{V}, \mathbf{V}_E, \lambda). \quad (28)$$

Note that Problem (28) is a convex quadratic optimization problem with no constraint, which can be solved in closed form. The optimal solution $\mathbf{V}^\star, \mathbf{V}^\star{}_E$ for Problem (28) is

$$[\mathbf{V}^\star, \mathbf{V}^\star{}_E] = \arg\min_{\mathbf{V},\mathbf{V}_E} \mathcal{L}(\mathbf{V}, \mathbf{V}_E, \lambda). \quad (29)$$

By setting the first-order derivative of $\mathcal{L}(\mathbf{V}, \mathbf{V}_E, \lambda)$ w.r.t. $\mathbf{V}$ to zero matrix, we can obtain the optimal solution of $\mathbf{V}$ as follows:

$$\frac{\partial\mathcal{L}(\mathbf{V}, \mathbf{V}_E, \lambda)}{\partial\mathbf{V}} = \mathbf{0}, \quad (30a)$$

$$\frac{\partial\mathcal{L}(\mathbf{V}, \mathbf{V}_E, \lambda)}{\partial\mathbf{V}_E} = \mathbf{0}. \quad (30b)$$

The left hand side of (30a) can be expanded as

$$\frac{\partial\mathcal{L}(\mathbf{V}, \mathbf{V}_E, \lambda)}{\partial\mathbf{V}} = 2(\mathbf{H}_V + \lambda\mathbf{I})\mathbf{V} - 2(\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I). \quad (31)$$

The equation (30a) becomes

$$(\mathbf{H}_V + \lambda\mathbf{I})\mathbf{V} = (\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I). \quad (32)$$

Then the optimal solution $\mathbf{V}^\star$ for Problem (29) is

$$\begin{aligned}\mathbf{V}^\star &= (\mathbf{H}_V + \lambda\mathbf{I})^\dagger(\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I)\\ &\triangleq \mathbf{\Theta}_V(\lambda)(\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I). \quad (33)\end{aligned}$$

Similarly, we solve Problem (29) by setting the first-order derivative of $\mathcal{L}(\mathbf{V}, \mathbf{V}_E, \lambda)$ w.r.t. $\mathbf{V}_E$ to zero matrix, which becomes

$$2(\mathbf{H}_{VE} + \lambda\mathbf{I})\mathbf{V}_E - 2\hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E^H = \mathbf{0}. \quad (34)$$

Then the optimal solution $\mathbf{V}_E^\star$ for Problem (29) is

$$\begin{aligned}\mathbf{V}_E^\star &= (\mathbf{H}_{VE} + \lambda\mathbf{I})^\dagger(\hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E^H)\\ &\triangleq \mathbf{\Theta}_{VE}(\lambda)(\hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E^H). \quad (35)\end{aligned}$$

Once the optimal solution $\lambda^\star$ for Problem (27) is found, the final optimal $\mathbf{V}^\star, \mathbf{V}_E^\star$ can be obtained. The value of $\lambda^\star$ should be chosen in order to guarantee the complementary slackness condition as follows:

$$\lambda[\mathrm{Tr}(\mathbf{V}^\star\mathbf{V}^{\star H}+\mathbf{V}_E^\star\mathbf{V}_E^{\star H}) - P_T] = 0. \tag{36}$$

We define $P(\lambda) \triangleq \mathrm{Tr}(\mathbf{V}^\star\mathbf{V}^{\star H}+\mathbf{V}_E^\star\mathbf{V}_E^{\star H})$, then $P(\lambda)$ becomes

$$\begin{aligned} P(\lambda) = &\mathrm{Tr}\left(\mathbf{\Theta}_V^n(\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I^H)(\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I^H)^H\right) \\ &+ \mathrm{Tr}\left(\mathbf{\Theta}_{VE}^n(\hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E^H)(\hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E^H)^H\right), \end{aligned} \tag{37}$$

where

$$\mathbf{\Theta}_V^n = (\mathbf{H}_V + \lambda\mathbf{I})^{\dagger H}(\mathbf{H}_V + \lambda\mathbf{I})^\dagger, \tag{38a}$$

$$\mathbf{\Theta}_{VE}^n = (\mathbf{H}_{VE} + \lambda\mathbf{I})^{\dagger H}(\mathbf{H}_{VE} + \lambda\mathbf{I})^\dagger. \tag{38b}$$

To find the optimal $\lambda^\star \geq 0$, we first check whether $\lambda = 0$ is the optimal solution or not. If

$$P(0)=\mathrm{Tr}\big(\mathbf{V}^{\star H}(0)\mathbf{V}^\star(0)\big)+\mathrm{Tr}\big(\mathbf{V}_E^{\star H}(0)\mathbf{V}_E{}^\star(0)\big)\leq P_T, \tag{39}$$

then the optimal solutions are given by $\mathbf{V}^\star = \mathbf{V}(0)$ and $\mathbf{V}_E^\star = \mathbf{V}_E(0)$. Otherwise, the optimal $\lambda^\star > 0$ is the solution of the equation $P(\lambda) = 0$.

It is readily to verify that $\mathbf{H}_V$ and $\mathbf{H}_{VE}$ are positive semidefinite matrices. Let us define the rank of $\mathbf{H}_V$ and $\mathbf{H}_{VE}$ as $r_V = \mathrm{rank}(\mathbf{H}_V) \leq N_T$ and $r_{VE} = \mathrm{rank}(\mathbf{H}_{VE}) \leq N_T$ respectively. By decomposing $\mathbf{H}_V$ and $\mathbf{H}_{VE}$ by using the singular value decomposition (SVD), we have

$$\mathbf{H}_V = [\mathbf{P}_{V,1}, \mathbf{P}_{V,2}]\,\mathbf{\Sigma}_V[\mathbf{P}_{V,1}, \mathbf{P}_{V,2}]^{\mathrm{H}}, \tag{40a}$$

$$\mathbf{H}_{VE} = [\mathbf{P}_{VE,1}, \mathbf{P}_{VE,2}]\,\mathbf{\Sigma}_{VE}[\mathbf{P}_{VE,1}, \mathbf{P}_{VE,2}]^{\mathrm{H}}, \tag{40b}$$

where $\mathbf{P}_{V,1}$ comprises the first r_V singular vectors associated with the r_V positive eigenvalues of $\mathbf{H}_V$, and $\mathbf{P}_{V,2}$ includes the last $N_T - r_V$ singular vectors associated with the $N_T - r_V$ zero-valued eigenvalues of $\mathbf{H}_V$, $\mathbf{\Sigma}_V = \mathrm{diag}\left\{\mathbf{\Sigma}_{V,1}, \mathbf{0}_{(N_T-r_V)\times(N_T-r_V)}\right\}$ with $\mathbf{\Sigma}_{V,1}$ representing the diagonal submatrix collecting the first r_V positive eigenvalues. Similarly, the first r_{VE} singular vectors corresponding to the r_{VE} positive eigenvalues of $\mathbf{H}_{VE}$ are contained in $\mathbf{P}_{VE,1}$, while the last $N_T - r_{VE}$ singular vectors corresponding to the $N_T - r_{VE}$ zero-valued eigenvalues of $\mathbf{H}_{VE}$ are held in $\mathbf{P}_{VE,2}$. $\mathbf{\Sigma}_{VE} = \mathrm{diag}\left\{\mathbf{\Sigma}_{VE,1}, \mathbf{0}_{(N_T-r_{VE})\times(N_T-r_{VE})}\right\}$ is a diagonal matrix with $\mathbf{\Sigma}_{VE,1}$ representing the diagonal submatrix gathering the first r_{VE} positive eigenvalues. By defining $\mathbf{P}_V \triangleq [\mathbf{P}_{V,1}, \mathbf{P}_{V,2}]$ and $\mathbf{P}_{VE} \triangleq [\mathbf{P}_{VE,1}, \mathbf{P}_{VE,2}]$, and substituting (40) into (38a) and (38b), $P(\lambda)$ becomes

$$\begin{aligned} P(\lambda) &= \mathrm{Tr}([(\mathbf{\Sigma}_V+\lambda\mathbf{I})^{-2}]\mathbf{Z}_V)+\mathrm{Tr}([(\mathbf{\Sigma}_{VE}+\lambda\mathbf{I})^{-2}]\mathbf{Z}_{VE}) \\ &= \sum_{i=1}^{r_V}\left[\frac{[\mathbf{Z}_V]_{i,i}}{\left([\Sigma_V]_{i,i}+\lambda\right)^2}\right] + \sum_{i=1}^{r_{VE}}\left[\frac{[\mathbf{Z}_{VE}]_{i,i}}{\left([\Sigma_{VE}]_{i,i}+\lambda\right)^2}\right] \\ &\quad + \sum_{i=r_V+1}^{N_T}\left[\frac{[\mathbf{Z}_V]_{i,i}}{(\lambda)^2}\right] + \sum_{i=r_{VE}+1}^{N_T}\left[\frac{[\mathbf{Z}_{VE}]_{i,i}}{(\lambda)^2}\right], \end{aligned} \tag{41}$$

where $\mathbf{Z}_V = \mathbf{P}_V^H(\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I^H)(\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I^H)^H\mathbf{P}_V$ and $\mathbf{Z}_{VE} = \mathbf{P}_{VE}^H(\hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E^H)(\hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E^H)^H\mathbf{P}_{VE}$. $[\mathbf{Z}_V]_{i,i}$, $[\mathbf{Z}_{VE}]_{i,i}$, $[\Sigma_V]_{i,i}$, and $[\Sigma_{VE}]_{i,i}$ represent the ith diagonal element of matrices $\mathbf{Z}_V$, $\mathbf{Z}_{VE}$, Σ_V, and Σ_{VE}, respectively. The first line of (41) is obtained by substituting (40) into the expression of $P(\lambda)$ in (37). It can be verified from the last line of (41) that $P(\lambda)$ is a monotonically decreasing function.

Then, the optimal $\lambda^\star$ can be obtained by solving the following equation,

$$\begin{aligned} &\sum_{i=1}^{r_V}\left[\frac{[\mathbf{Z}_V]_{i,i}}{\left([\Sigma_V]_{i,i}+\lambda\right)^2}\right] + \sum_{i=1}^{r_{VE}}\left[\frac{[\mathbf{Z}_{VE}]_{i,i}}{\left([\Sigma_{VE}]_{i,i}+\lambda\right)^2}\right] \\ &+ \sum_{i=r_V+1}^{N_T}\left[\frac{[\mathbf{Z}_V]_{i,i}}{(\lambda)^2}\right] + \sum_{i=r_{VE}+1}^{N_T}\left[\frac{[\mathbf{Z}_{VE}]_{i,i}}{(\lambda)^2}\right] = P_T. \end{aligned} \tag{42}$$

To solve it, the bisection search method is utilized. Since $P(\infty) = 0$, the solution to (42) must exist. The lower bound of $\lambda^\star$ is a positive value approaching zero, while the upper bound of $\lambda^\star$ is

$$\lambda^\star < \sqrt{\frac{\sum_{i=1}^{N_T}[\mathbf{Z}_V]_{i,i} + \sum_{i=1}^{N_T}[\mathbf{Z}_{VE}]_{i,i}}{P_T}} \triangleq \lambda^{\mathrm{ub}}. \tag{43}$$

which can be proved as

$$\begin{aligned} P(\lambda^{\mathrm{ub}}) &= \sum_{i=1}^{r_V}\frac{[\mathbf{Z}_V]_{i,i}}{\left([\Sigma_V]_{i,i}+\lambda^{\mathrm{ub}}\right)^2} + \sum_{i=1}^{r_{VE}}\frac{[\mathbf{Z}_{VE}]_{i,i}}{\left([\Sigma_{VE}]_{i,i}+\lambda^{\mathrm{ub}}\right)^2} \\ &\quad + \sum_{i=r_V+1}^{N_T}\left[\frac{[\mathbf{Z}_V]_{i,i}}{(\lambda^{\mathrm{ub}})^2}\right] + \sum_{i=r_{VE}+1}^{N_T}\left[\frac{[\mathbf{Z}_{VE}]_{i,i}}{(\lambda^{\mathrm{ub}})^2}\right] \\ &< \sum_{i=1}^{N_T}\frac{[\mathbf{Z}_V]_{i,i}}{(\lambda^{\mathrm{ub}})^2} + \sum_{i=1}^{N_T}\frac{[\mathbf{Z}_{VE}]_{i,i}}{(\lambda^{\mathrm{ub}})^2} = P_T. \end{aligned} \tag{44}$$

When the optimal $\lambda^\star$ is found, the optimal matrices $\mathbf{V}^\star$ and $\mathbf{V}_E^\star$ can be obtained by substituting $\lambda^\star$ into (33) and (35).

C. Optimizing the Phase Shifts $\mathbf{\Phi}$

In this subsection, the phase shift matrix $\mathbf{\Phi}$ is optimized by fixing $\mathbf{V}$ and $\mathbf{V}_E$. The transmit power constraint in Problem (23) is only related with $\mathbf{V}$ and $\mathbf{V}_E$, thus is

removed. Then, the optimization problem for $\mathbf{\Phi}$ reduced from Problem (23) is formulated as

$$\begin{aligned}\min_{\mathbf{\Phi}}\ & g_0(\mathbf{\Phi}) \triangleq -\mathrm{Tr}(\mathbf{W}_I\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I)-\mathrm{Tr}(\mathbf{W}_I{\mathbf{U}_I}^H\hat{\mathbf{H}}_I\mathbf{V})\\ &+\mathrm{Tr}(\mathbf{V}^H\mathbf{H}_V\mathbf{V})-\mathrm{Tr}(\mathbf{W}_E{\mathbf{V}_E}^H\hat{\mathbf{H}}_E^H\mathbf{U}_E)\\ &-\mathrm{Tr}(\mathbf{W}_E{\mathbf{U}_E}^H\hat{\mathbf{H}}_E\mathbf{V}_E)+\mathrm{Tr}({\mathbf{V}_E}^H\mathbf{H}_{VE}\mathbf{V}_E) \quad (45a)\\ \text{s.t.}\quad & |\phi_m|=1, m=1,\cdots,M. \quad (45b)\end{aligned}$$

By the aid of complex mathematical manipulations, which are given in details in Appendix B, Problem (45) can be transformed into a form that can facilitate the MM algorithm. Based on the derivations in Appendix B, the OF $g_0(\mathbf{\Phi})$ can be equivalently transformed into

$$\begin{aligned}g_0(\mathbf{\Phi}) =&\mathrm{Tr}\left(\mathbf{\Phi}^H\mathbf{D}^H\right)+\mathrm{Tr}\left(\mathbf{\Phi}\mathbf{D}\right)+\mathrm{Tr}\left[\mathbf{\Phi}^H\mathbf{B}_{VE}\mathbf{\Phi}\mathbf{C}_{VE}\right]\\ &+\mathrm{Tr}\left(\mathbf{\Phi}^H\mathbf{B}_V\mathbf{\Phi}\mathbf{C}_V\right)+C_t, \quad (46)\end{aligned}$$

where C_t, $\mathbf{D}$, $\mathbf{C}_{VE}$, $\mathbf{C}_V$, $\mathbf{B}_{VE}$ and $\mathbf{B}_V$ are constants for $\mathbf{\Phi}$, and are given in Appendix B.

By exploiting the matrix properties in [37, Eq. (1.10.6)], the trace operators can be removed, and the third and fourth terms in (46) become as

$$\mathrm{Tr}\left(\mathbf{\Phi}^{\mathrm{H}}\mathbf{B}_{VE}\mathbf{\Phi}\mathbf{C}_{VE}\right)=\boldsymbol{\phi}^{\mathrm{H}}\left(\mathbf{B}_{VE}\odot\mathbf{C}_{VE}^{\mathrm{T}}\right)\boldsymbol{\phi}, \quad (47a)$$

$$\mathrm{Tr}\left(\mathbf{\Phi}^{\mathrm{H}}\mathbf{B}_V\mathbf{\Phi}\mathbf{C}_V\right)=\boldsymbol{\phi}^{\mathrm{H}}\left(\mathbf{B}_V\odot\mathbf{C}_V^{\mathrm{T}}\right)\boldsymbol{\phi}, \quad (47b)$$

where $\boldsymbol{\phi}\triangleq[\phi_1,\cdots,\phi_m,\cdots,\phi_M]^{\mathrm{T}}$ is a vector holding the diagonal elements of $\mathbf{\Phi}$.

Similarly, the trace operators can be removed for the first and second terms in (46), which become as

$$\mathrm{Tr}\left(\mathbf{\Phi}^{\mathrm{H}}\mathbf{D}^{\mathrm{H}}\right)=\mathbf{d}^{\mathrm{H}}(\boldsymbol{\phi}^*),\mathrm{Tr}\left(\mathbf{\Phi}\mathbf{D}\right)=\boldsymbol{\phi}^{\mathrm{T}}\mathbf{d}, \quad (48)$$

where $\mathbf{d}=\left[[\mathbf{D}]_{1,1},\cdots,[\mathbf{D}]_{M,M}\right]^{\mathrm{T}}$ is a vector gathering the diagonal elements of matrix $\mathbf{D}$.

Hence, Problem (45) can be rewritten as

$$\begin{aligned}\min_{\boldsymbol{\phi}}\quad & \boldsymbol{\phi}^{\mathrm{H}}\mathbf{\Xi}\boldsymbol{\phi}+\boldsymbol{\phi}^{\mathrm{T}}\mathbf{d}+\mathbf{d}^{\mathrm{H}}(\boldsymbol{\phi}^*) \quad (49a)\\ \text{s.t.}\quad & |\phi_m|=1, m=1,\cdots,M, \quad (49b)\end{aligned}$$

where $\mathbf{\Xi}=\mathbf{B}_{VE}\odot\mathbf{C}_{VE}^{\mathrm{T}}+\mathbf{B}_V\odot\mathbf{C}_V^{\mathrm{T}}$. It can be observed that $\mathbf{B}_{VE}$, $\mathbf{C}_{VE}^{\mathrm{T}}$, $\mathbf{B}_V$ and $\mathbf{C}_V^{\mathrm{T}}$ are semidefinite matrices. The Hadamard products of $\mathbf{B}_{VE}\odot\mathbf{C}_{VE}^{\mathrm{T}}$ and $\mathbf{B}_V\odot\mathbf{C}_V^{\mathrm{T}}$ are also semidefinite matrices according to the Property (9) on Page 104 of [37]. Then, $\mathbf{\Xi}$ is a semidefinite matrix, because it is a sum of two semidefinite matrices, both of which are Hadamard products of two semidefinite matrices. Problem (49) is equivalent to

$$\begin{aligned}\min_{\boldsymbol{\phi}}\quad & f(\boldsymbol{\phi})\triangleq\boldsymbol{\phi}^{\mathrm{H}}\mathbf{\Xi}\boldsymbol{\phi}+2\mathrm{Re}\left\{\boldsymbol{\phi}^{\mathrm{H}}(\mathbf{d}^*)\right\} \quad (50a)\\ \text{s.t.}\quad & |\phi_m|=1, m=1,\cdots,M. \quad (50b)\end{aligned}$$

Problem (50) can be solved by the SDR method [17] by transforming the unimodulus constraint into a rank-one constraint, however, the rank-one solution cannot always be obtained and the computational complexity is high for the SDR method. Thus, we propose to solve Problem (50) efficiently by the MM algorithm as [15], where the closed-form solution can be obtained in each iteration. Details are omitted for simplicity.

D. Overall Algorithm to Solve Problem (10)

To sum up, the detailed execution of the overall BCD-MM algorithm proposed for solving Problem (10) is provided in Algorithm 1. The MM algorithm is exploited for solving the optimal phase shifts $\mathbf{\Phi}^{(n+1)}$ of Problem (50) in Step 5. The iteration process in MM algorithm ensures that the OF value of Problem (50) decreases monotonically. Moreover, the BCD algorithm also guarantees that the OF value of Problem (23) monotonically decreases in each step and each iteration of Algorithm 1. Since the OF value in (23a) has a lower bound with the power limit, the convergence of Algorithm 1 is guaranteed.

Algorithm 1 BCD-MM Algorithm

1: Parameter Setting. Set the maximum number of iterations $n_{\max}$ and the first iterative number $n=1$; Give the error tolerance ε.
2: Variables Initialization. Initialize the variables $\mathbf{V}^{(1)}$, $\mathbf{V}_E^{(1)}$ and $\mathbf{\Phi}^{(1)}$ in the feasible region; Compute the OF value of Problem (10) as $\mathrm{OF}(\mathbf{V}^{(1)},\mathbf{V}_E^{(1)},\mathbf{\Phi}^{(1)})$;
3: Auxiliary Variables Calculation. Given $\mathbf{V}^{(n)},\mathbf{V}_E^{(n)}$, $\mathbf{\Phi}^{(n)}$, compute the optimal matrices $\mathbf{U}_I^{(n)},\mathbf{W}_I^{(n)},\mathbf{U}_E^{(n)},\mathbf{W}_E^{(n)},\mathbf{W}_X^{(n)}$ according to (14a), (14b), (16a), (16b), (19) respectively;
4: Matrices Optimization. Given $\mathbf{U}_I^{(n)},\mathbf{W}_I^{(n)},\mathbf{U}_E^{(n)},\mathbf{W}_E^{(n)},\mathbf{W}_X^{(n)}$, solve the optimal TPC matrix $\mathbf{V}^{(n+1)}$ and equivalent AN covariance matrix $\mathbf{V}_E^{(n+1)}$ of Problem (29) with the Lagrangian multiplier method;
5: Phase Shifts Optimization. Given $\mathbf{U}_I^{(n)},\mathbf{W}_I^{(n)},\mathbf{U}_E^{(n)},\mathbf{W}_E^{(n)},\mathbf{W}_X^{(n)}$ and $\mathbf{V}^{(n+1)},\mathbf{V}_E^{(n+1)}$, solve the optimal phase shifts $\mathbf{\Phi}^{(n+1)}$ of Problem (50) with the MM algorithm;
6: Termination Check. If $n\geq n_{\max}$ or

$$\frac{\left|\mathrm{OF}(\mathbf{V}^{(n+1)},\mathbf{V}_E^{(n+1)},\mathbf{\Phi}^{(n+1)})-\mathrm{OF}(\mathbf{V}^{(n)},\mathbf{V}_E^{(n)},\mathbf{\Phi}^{(n)})\right|}{\mathrm{OF}(\mathbf{V}^{(n+1)},\mathbf{V}_E^{(n+1)},\mathbf{\Phi}^{(n+1)})}<\varepsilon,$$

terminate. Otherwise, update $n\leftarrow n+1$ and jump to step 2.

Based on the algorithm description, the complexity analysis of the proposed BCD-MM algorithm is performed. In Step 3, computing the decoding matrices $\mathbf{U}_I^{(n)}$ and $\mathbf{U}_E^{(n)}$ incurs the complexity of $\mathcal{O}(N_I^3)+\mathcal{O}(N_E^3)$, while calculating the auxiliary matrices $\mathbf{W}_I^{(n)}$, $\mathbf{W}_E^{(n)}$, and $\mathbf{W}_X^{(n)}$ requires the complexity of $\mathcal{O}(d^3)+\mathcal{O}(N_T^3)+\mathcal{O}(N_E^3)$. The complexity of calculating the TPC matrix $\mathbf{V}^{(n+1)}$

and AN covariance matrix $\mathbf{V}_E^{(n+1)}$ in Step 4 can be analyzed according to the specific process of Lagrangian multiplier method based on the fact that the complexity of computing product the $\mathbf{XY}$ of complex matrices $\mathbf{X} \in \mathbb{C}^{m\times n}$ and $\mathbf{Y} \in \mathbb{C}^{n\times p}$ is $\mathcal{O}(mnp)$. By assuming that $N_T > N_I(\text{or } N_E) > d$, the complexity of computing the matrices $\{\mathbf{H}_V, \mathbf{H}_{VE}\}$ in (24a) and (24b) is $\mathcal{O}(N_T^3) + \mathcal{O}(2N_T^2 d) + \mathcal{O}(2N_T^2 N_E)$; while the complexity of calculating $\mathbf{V}^*$, $\mathbf{V}_E^*$ in (33) and (35) is $\mathcal{O}(2N_T^3)$. The SVD decomposition of $\{\mathbf{H}_V, \mathbf{H}_{VE}\}$ requires the computational complexity of $\mathcal{O}(2N_T^3)$, while calculating $\{\mathbf{Z}_V\}$ and $\{\mathbf{Z}_{VE}\}$ requires the complexity of $\mathcal{O}(N_T^2 N_I)+\mathcal{O}(2N_T^3)$. The complexity of finding the Lagrangian multipliers $\{\lambda\}$ is negligible. Thus, the overall complexity for $\mathbf{V}^{(n+1)}$, $\mathbf{V}_E^{(n+1)}$ is about $\mathcal{O}(\max\{2N_T^3, 2N_T^2 N_E\})$. In step 5, obtaining the optimal $\mathbf{\Phi}^{(n+1)}$ by the MM algorithm entails a complexity of $C_{MM} = \mathcal{O}(M^3 + T_{MM}M^2)$, where T_{MM} is the iteration number for convergence. Based on the complexity required in Step 3, 4 and 5, the overall complexity $C_{\text{BCD}-\text{MM}}$ of the BCD-MM algorithm can be evaluated by

$$C_{\text{BCD}-\text{MM}} = \mathcal{O}(\max\{2N_T^3, 2N_T^2 N_E, C_{MM}\}). \quad (51)$$

IV. Extensions to the Multiple-IRs Scenario

Consider a multicast extension where there are $L \geq 2$ legitimate IRs, and they all intend to receive the same message. The signal model for the MIMO multi-IR wiretap channel scenario is

$$\mathbf{y}_{I,l} = \hat{\mathbf{H}}_{I,l}(\mathbf{V}\mathbf{s} + \mathbf{n}) + \mathbf{n}_{I,l}, l = 1, \cdots, L, \quad (52)$$

where $\hat{\mathbf{H}}_{I,l} \triangleq \mathbf{H}_{b,I,l} + \mathbf{H}_{R,I,l}\mathbf{\Phi}\mathbf{G}$. The subscript l indicates the lth IR, and the other notations are the same as in (4) and (6). Then, the achievable SR is given by [38]

$$R_s(\mathbf{V},\mathbf{V}_E,\mathbf{\Phi}) = \min_{l=1,\cdots,L}\{R_{I,l}(\mathbf{V},\mathbf{\Phi},\mathbf{Z}) - R_E(\mathbf{V},\mathbf{\Phi},\mathbf{Z})\}, \quad (53)$$

where

$$R_{I,l}(\mathbf{V},\mathbf{\Phi},\mathbf{Z}) = \log\left|\mathbf{I} + \hat{\mathbf{H}}_{I,l}\mathbf{V}\mathbf{V}^H\hat{\mathbf{H}}_{I,l}^H\mathbf{J}_{I,l}^{-1}\right|, \quad (54a)$$

$$\mathbf{J}_{I,l} \triangleq \hat{\mathbf{H}}_{I,l}\mathbf{Z}\hat{\mathbf{H}}_{I,l}^H + \sigma_{I,l}^2\mathbf{I}_{N_I}. \quad (54b)$$

The AN-aided SRM problem for the multicast multiple IRs scenario is formulated as

$$\max_{\mathbf{V},\mathbf{V}_E,\mathbf{\Phi}} \quad R_s(\mathbf{V},\mathbf{V}_E,\mathbf{\Phi}) \quad (55a)$$

$$\text{s.t.} \quad \text{Tr}(\mathbf{V}\mathbf{V}^H + \mathbf{V}_E\mathbf{V}_E^H) \leq P_T, \quad (55b)$$

$$|\phi_m| = 1, m = 1, \cdots, M. \quad (55c)$$

The OF of Problem (55) can be rewritten in (56b). The lower bound to the first term of (56b) can be found as

$$\min_{l=1,\cdots,L}\{\max_{\mathbf{U}_{I,l},\mathbf{W}_{I,l}\succeq 0} h_{1,l}(\mathbf{U}_{I,l},\mathbf{V},\mathbf{V}_E,\mathbf{W}_{I,l})\} \geq \max_{\{\mathbf{U}_{I,l},\mathbf{W}_{I,l}\succeq 0\}_{l=1}^L}\{\min_{l=1,\cdots,L} h_{1,l}(\mathbf{U}_{I,l},\mathbf{V},\mathbf{V}_E,\mathbf{W}_{I,l})\}, \quad (57)$$

where the inequality holds due to the fact that $\min_x \max_y f(x,y) \geq \max_y \min_x f(x,y)$ for any function $f(x,y)$. Here by exchanging the positions of $\max_{\{\mathbf{U}_{I,l},\mathbf{W}_{I,l}\succeq 0\}_{l=1}^L}$ and $\min_{l=1,\cdots,L}$ in (57), we can find a lower bound to $R_s(\mathbf{V},\mathbf{V}_E,\mathbf{\Phi})$ as

$$f_{ms}(\mathbf{S},\Phi) \triangleq \max_{\mathbf{S}}\{\min_{l=1,\cdots,L} h_{1,l}(\mathbf{U}_{I,l},\mathbf{V},\mathbf{V}_E,\mathbf{W}_{I,l}) + h_2(\mathbf{U}_E,\mathbf{V}_E,\mathbf{W}_E) + h_3(\mathbf{V},\mathbf{V}_E,\mathbf{W}_X)\}. \quad (58)$$

where $\mathbf{S} = [\mathbf{V},\mathbf{V}_E,\{\mathbf{U}_{I,l},\mathbf{W}_{I,l} \succeq 0\}_{l=1}^L,\mathbf{U}_E,\mathbf{W}_E \succeq 0,\mathbf{W}_X \succeq 0]$. We simplify Problem (55) by maximizing a lower bound to its original objective as follows,

$$\max_{\mathbf{\Phi},\mathbf{S}} \quad f_{ms}(\mathbf{S},\Phi) \quad (59a)$$

$$\text{s.t.} \quad \text{Tr}(\mathbf{V}\mathbf{V}^H + \mathbf{V}_E\mathbf{V}_E^H) \leq P_T, \quad (59b)$$

$$|\phi_m| = 1, m = 1, \cdots, M. \quad (59c)$$

The detailed derivations for solving Problem (59) can be found in our full journal version in [39], where a BCD-QCQP-CCP algorithm is proposed.

V. Simulation Results

In this section, numerical simulations are carried out to evaluate the beneficial impacts of the IRS on the AN-aided MIMO secure communication system. We focus on the scenario of the standard three-terminal MIMO Guassian wiretap channel shown in Fig. 2. The distance from the BS to the IRS is $d_{BR} = 50$ m. We assume that the line connecting the IR and Eve is parallel to the line connecting the BS and the IRS, and that the vertical distance between them is $d_v = 2$ m.

The large-scale path loss is modeled as $\text{PL} = \text{PL}_0 - 10\alpha\log_{10}\left(\frac{d}{d_0}\right)$, where PL_0 is the path loss at the reference distance $d_0 = 1$ m, α is the path loss exponent, d is the link distance. In our simulations, we set $\text{PL}_0 = -30$ dB. The operating frequency is $f_0 = 2$ GHz. The path loss exponents of the links from BS to Eve, from BS to IR, from IRS to Eve and from IRS to IR are $\alpha_{\text{BE}} = 3.5$, $\alpha_{\text{BI}} = 3.5$, $\alpha_{\text{RE}} = 2.5$ and $\alpha_{\text{RI}} = 2.5$, respectively. The path-loss exponent of the link from BS to IRS is set to be $\alpha_{\text{BR}} = 2.2$, which means that the IRS is well-located, and the path loss is negligible in this link.

For the direct channels from the BSs to the Eve and IR, the small-scale fading is assumed to be Rayleigh fading due to extensive scatters. However, for the IRS-related channels, the small-scale fading is assumed to be Rician fading. Specifically, the small-scale channel can be modeled as

$$\tilde{\mathbf{H}} = \left(\sqrt{\frac{\beta}{1+\beta}}\tilde{\mathbf{H}}^{LOS} + \sqrt{\frac{1}{1+\beta}}\tilde{\mathbf{H}}^{NLOS}\right), \quad (60)$$

$$R_s(\mathbf{V},\mathbf{V}_E,\mathbf{\Phi}) = \min_{l=1,\cdots,L}\{\underbrace{\log\left|\mathbf{I}_{N_I}+\hat{\mathbf{H}}_{I,l}\mathbf{V}\mathbf{V}^H\hat{\mathbf{H}}_{I,l}^H(\hat{\mathbf{H}}_{I,l}\mathbf{V}_E\mathbf{V}_E^H\hat{\mathbf{H}}_{I,l}^H+\sigma_{I,l}^2\mathbf{I}_{N_I})^{-1}\right|}_{f_{1,l}}\}$$

$$+\underbrace{\log\left|\mathbf{I}_{N_E}+\hat{\mathbf{H}}_E\mathbf{V}_E\mathbf{V}_E^H\hat{\mathbf{H}}_E^H(\sigma_E^2\mathbf{I}_{N_E})^{-1}\right|}_{f_2}\underbrace{-\log\left|\mathbf{I}_{N_E}+\sigma_E^{-2}\hat{\mathbf{H}}_E(\mathbf{V}\mathbf{V}^H+\mathbf{V}_E\mathbf{V}_E^H)\hat{\mathbf{H}}_E^H\right|}_{f_3}, \quad (56a)$$

$$=\min_{l=1,\cdots,L}\{\max_{\mathbf{U}_{I,l},\mathbf{W}_{I,l}\succeq 0} h_{1,l}(\mathbf{U}_{I,l},\mathbf{V},\mathbf{V}_E,\mathbf{W}_{I,l})\}+\max_{\mathbf{U}_E,\mathbf{W}_E\succeq 0} h_2(\mathbf{U}_E,\mathbf{V}_E,\mathbf{W}_E)+\max_{\mathbf{W}_X\succeq 0} h_3(\mathbf{V},\mathbf{V}_E,\mathbf{W}_X). \quad (56b)$$

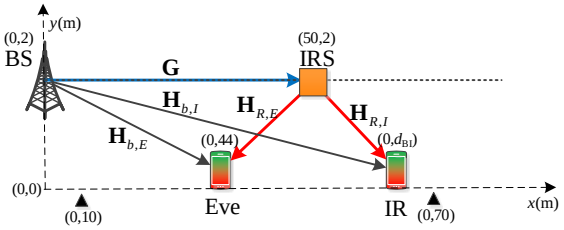

Fig. 2. The three-terminal MIMO communication scenario in simulation.

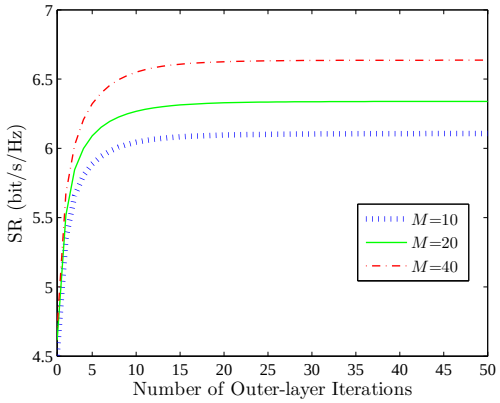

Fig. 3. Convergence behaviour of the BCD algorithm.

where β is the Rican factor, $\tilde{\mathbf{H}}^{LOS}$ denotes the deterministic line of sight (LoS) component of the IRS-related channel, and $\tilde{\mathbf{H}}^{NLOS}$ denotes the non-LoS (NLoS) component of the IRS-related channel, which is modeled as Rayleigh fading. By assuming the antennas at the BS, IRS, Eve and IR are arranged in a uniform linear array (ULA), the $\tilde{\mathbf{H}}^{LOS}$ can be modeled as $\tilde{\mathbf{H}}^{LOS}=\mathbf{a}_r\mathbf{a}_t^H$, where $\mathbf{a}_t$ and $\mathbf{a}_r$ are the steering vectors of the transmit and receive arrays, respectively. The $\mathbf{a}_t$ and $\mathbf{a}_r$ are defined as,

$$\mathbf{a}_t=\left[1,\exp(j2\pi\frac{d_t}{\lambda}\sin\varphi_t),\cdots,\exp(j2\pi\frac{d_t}{\lambda}(N_t-1)\sin\varphi_t)\right]^T, \quad (61a)$$

$$\mathbf{a}_r=\left[1,\exp(j2\pi\frac{d_r}{\lambda}\sin\varphi_r),\cdots,\exp(j2\pi\frac{d_r}{\lambda}(N_r-1)\sin\varphi_r)\right]^T. \quad (61b)$$

In (61), λ is the wavelength; d_t and d_r are the element intervals of the transmit and receive array; φ_t and φ_r are the angle of departure and the angle of arrival; N_t and N_r are the number of antennas/elements at the transmitter and receiver, respectively. We set $\frac{d_t}{\lambda}=\frac{d_r}{\lambda}=0.5$, and $\varphi_t=\tan^{-1}(\frac{y_r-y_t}{x_r-x_t})$, $\varphi_r=\pi-\varphi_t$, where (x_t,y_t) is the location of the transmitter, and (x_r,y_r) is the location of the receiver.

If not specified, the simulation parameters are set as follows. The IR's noise power and the Eve's noise power are $\sigma_I^2=-75$ dBm and $\sigma_E^2=-75$ dBm. The numbers of BS antennas, IR antennas, and Eve antennas are $N_T=4$, $N_I=2$, and $N_E=2$ respectively. There are $d=2$ data streams and $M=50$ IRS reflection elements. The transmit power limit is $P_T=15$ dBm, and the error tolerance is $\varepsilon=10^{-6}$. The horizontal distance between the BS and the Eve is $d_{BE}=44$ m. The horizontal distance between the BS and the IR is selected from $d_{BI}=[10\text{ m},70\text{ m}]$. The following results are obtained by averaging over 200 independent channel generations.

A. Convergence Analysis

The convergence performance of the proposed BCD-MM algorithm is investigated. The iterations of the BCD algorithm are termed as outer-layer iterations, while the iterations of the MM algorithm are termed as the inner-layer iterations. Fig. 3 shows three examples of convergence behaviour for $M=10$, 20 and 40. In Fig. 3, the SR increases with the iteration number, and finally reaches a stable value. It is shown that the algorithm converges quickly, almost within 20 iterations, which demonstrates the efficiency of the proposed algorithm. Moreover, a larger converged SR value is reached with a larger M, which means that better security performance can be obtained by using more IRS elements. However, more IRS elements bring a heavier computation burden, which is demonstrated in Fig. 3 in the form of a slower convergence speed with more phase shifts.

Specifically, we evaluate the convergence performance of the MM algorithm used for solving the optimal IRS phase shifts. The inner-layer iterative process of the MM algorithm in the first iteration of the BCD algorithm is shown in Fig. 4. The SR value increases as the iteration

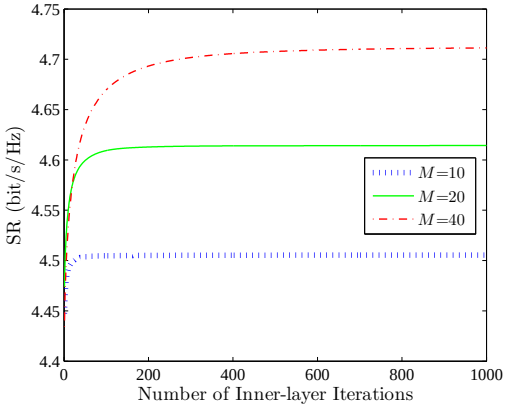

Fig. 4. Convergence behaviour of the MM algorithm.

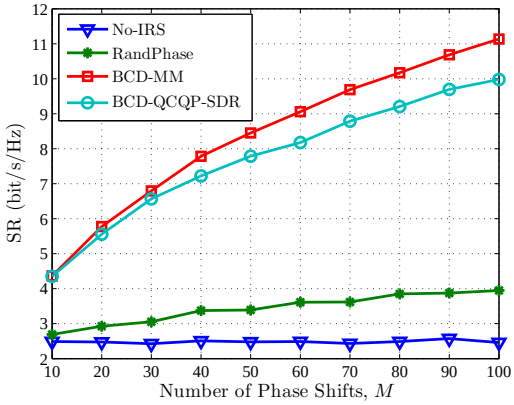

Fig. 5. Achievable SR versus the number of phase shifts M.

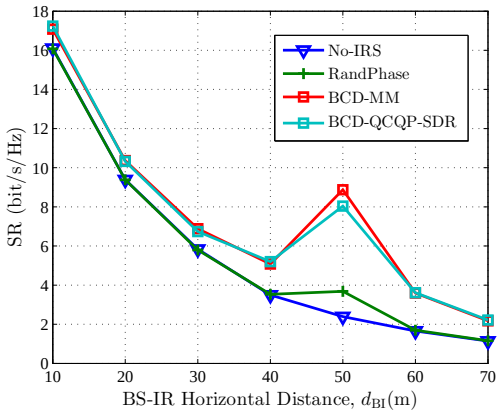

Fig. 6. Achievable SR versus the location of the IR.

number increases, and finally converges to a stable value. According with the convergency performance in the out-layer iteration, similar conclusions can be drawn for the inner-layer iteration, which is that a higher converged SR value can be obtained with more phase shifts but at the cost of a lower convergence speed. The reason for the lower convergence speed with larger M value is that more optimization variables are introduced, which requires a higher computational complexity.

B. Performance Evaluation

In this subsection, we compare the performance of our proposed algorithm with the following three schemes:

1) **RandPhase**: The phase shifts of the IRS are randomly selected from $[0, 2\pi]$. In this scheme, the MM algorithm is skipped, and only the TPC matrix and AN covariance matrix are optimized.
2) **No-IRS**: Without the IRS, the channel matrices of IRS related links become zero matrices, which are $\mathbf{H}_{R,I} = \mathbf{0}$, $\mathbf{H}_{R,E} = \mathbf{0}$ and $\mathbf{G} = \mathbf{0}$. This scheme leads to a conventional AN-aided communication system, and only the TPC matrix and AN covariance matrix need to be optimized.
3) **BCD-QCQP-SDR**: The BCD algorithm is utilized. However, the TPC matrix and the AN covariance matrix is optimized by tackling Problem (25) as a QCQP problem, which is solved by the general CVX solvers, e.g. Sedumi or Mosek. The phase shifts of IRS are optimized by solving Problem (50) with the SDR technique.

1) Impact of the Number of Phase Shifts: The averaged SR performance of four schemes with various values of M is shown in Fig. 5, which demonstrates that the proposed BCD-MM algorithm is significantly superior to the other three schemes. We observe that the SR achieved by the BCD-MM scheme obviously increases with M, while the RandPhase scheme only shows a slight improvement as M increases, and the No-IRS scheme has very low SRs that is independent of M. Larger the value of M of IRS is, more significant performance gain the proposed algorithm can obtain. For example, when M is small as $M = 10$, the SR gain of the BCD-MM over the No-IRS is only 1.3 bit/s/Hz, while this SR gain becomes 9.5 bit/s/Hz when M increases to $M = 100$. The performance gain for the proposed algorithm comes from two aspects. On the one hand, a higher array gain can be obtained by increasing M, since more signal power can be received at the IRS with a larger M. On the other hand, a higher reflecting beamforming gain can be obtained by increasing M, which means that the sum of coherently adding the reflected signals at the IRS increases with M by appropriately designing the phase shifts. However, only the array gain can be exploited by the RandPhase scheme, thus the SRs increase slowly, and remain at much lower values than that of the proposed algorithm. These results further confirm that more security improvements can be achieved by using a large IRS with more reflecting elements and optimizing the phase shifts properly, however increasing the number of elements may lead to a computational complexity. In comparison to the BCD-QCQP-SDR algorithm, the proposed BCD-MM algorithm can achieve higher SRs, and the SR performance gap increases with M.

2) Impact of the relative location of IRS: Fig. 6 illustrates the achieved SRs for four schemes with various BS-

IR horizontal distance d_{BI}, where the BS-Eve distance is fixed to be $d_{BE} = 44$ m. It is observed that the proposed BCD-MM algorithm is the best among the four schemes for obtaining the highest SR value. When the IR moves far away from the BS, the SRs decrease for the four schemes, however, the SRs achieved for the RandPhase, the proposed BCD-MM algorithm and the BCD-QCQP-SDR algorithm increase greatly when the IR approaches the IRS. The achieved SRs at different BS-IR distances of the RandPhase scheme and the no-IRS scheme are almost the same, except for $d_{BI} \in [40\text{m}, 50\text{m}]$, in which the IRS brings a prominent security enhancement when IR becomes close to it even with random IRS phase shifts. Similarly, the proposed BCD-MM algorithm and the BCD-QCQP-SDR algorithm can achieve almost the same SRs, except for $d_{BI} \in [40\text{m}, 50\text{m}]$, in which the IR is close to the IRS, and the proposed BCD-MM algorithm is superior to the BCD-QCQP-SDR algorithm. For other BS-IR distances where the IR is far from the IRS, the SRs of RandPhase scheme are similar with those of the No-IRS scheme due to the not fully explored potential of IRS. By optimizing the phase shifts of IRS, the SRs are enhanced at different BS-IRS distances. And the SR gain of the proposed BCD-MM algorithm over the RandPhase scheme increases when the IR moves close to the IRS ($d_{BI} \in [40\text{m}, 50\text{m}]$). This means that as long as the IRS is deployed close to the IR, significant security enhancement can be achieved by deploying an IRS in an AN-aided MIMO communication system.

3) Impact of the Number of Data Streams: Compared with the MISO scenario, a significant advantage of the MIMO scenario is that multiple data streams can be transmitted to the users simultaneously. To evaluate the impact of the number of data streams on the SR, the average SRs versus the transmit power limit for various numbers of data streams are given in Fig. 7. The number of transmit antennas is $N_T = 4$. The path loss exponents are $\alpha_{\text{BR}} = 2.2$, $\alpha_{\text{BE}} = 3.5$, $\alpha_{\text{BI}} = 2.5$, $\alpha_{\text{RE}} = 3.5$ and $\alpha_{\text{RI}} = 2.5$ respectively. The Rician factor is $\beta = 3$. The number of phase shifts is $M = 50$.

As shown in Fig. 7, the SR increases with the transmit power limit and larger number of data streams result in a higher SR. When the transmit power limit is low, marginal performance gains are achieved by increasing the number of data streams d. When the transmit power limit is high, significant performance gains can be achieved by increasing the number of data streams d. This means that a greater number of data streams ensure the higher SR, and the performance gain increases with the transmit power limit. For the case of $d = 1$, the SR performance of $N_I = N_E = 4$ and $N_I = N_E = 1$ is compared. It is revealed that the SR obtained by four receive antennas is higher than that obtained by one single receive antenna when the transmit power limit is relatively low. With the increase of transmit power limit, the SR performance gain brought by multiple receive antennas decreases. When the transmit power limit is high enough, the SR performance is saturated, and the SR performance of the multiple receive antennas and single receive antenna becomes the same.

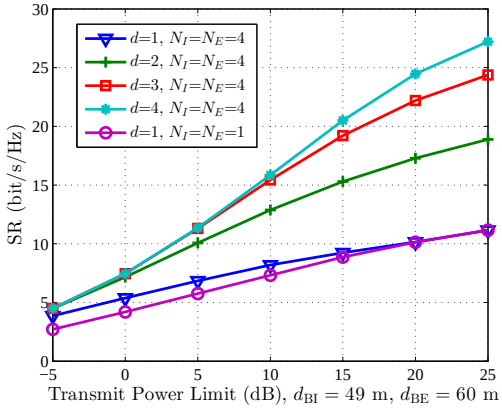

Fig. 7. Achievable SR versus the transmit power limit for various numbers of data streams.

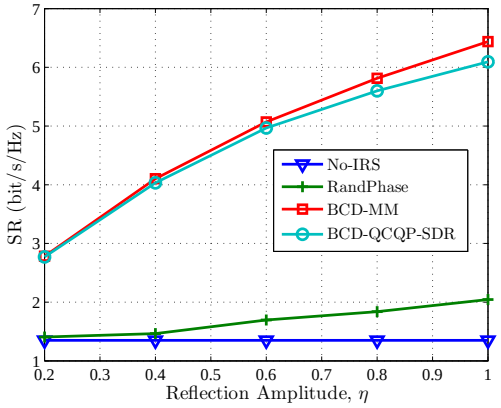

Fig. 8. Achievable SR versus the reflection amplitude η.

4) Impact of the Reflection Amplitude: Due to the manufactural and hardware impairments, the signals reflected by the IRS may be attenuated. Then, in Fig. 8, we study the impact of the reflection amplitude on the security performance. The transmit power limit is 10 dBm. We assume that the reflection amplitudes of all the IRS elements are the same as η, and that the phase shift matrix of the IRS is rewritten as $\mathbf{\Phi} = \eta\text{diag}\{\phi_1, \cdots, \phi_m, \cdots, \phi_M\}$. As expected, the SR achieved by the IRS-aided scheme increases with η due to reduced power loss. As η increases, the superiority of the proposed BCD-MM algorithm over the other algorithms becomes more obvious. The reflection amplitude has a great impact on the security performance. Specifically, when η increases from 0.2 to 1, the SR increases over 3.6 bit/s/Hz for the proposed BCD-MM algorithm.

5) Impact of the Discrete Phase Shifts: In practice, it is difficult to realize continuous phase shifts at the reflecting

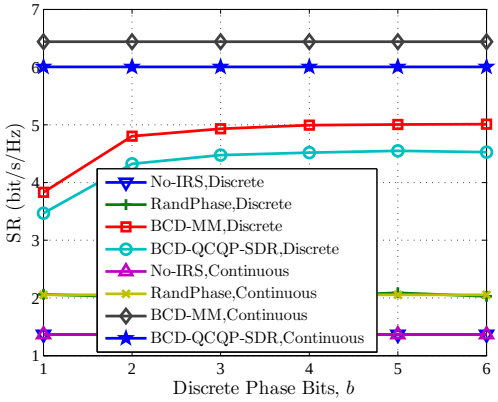

Fig. 9. Achievable SR versus the discrete phase bits b.

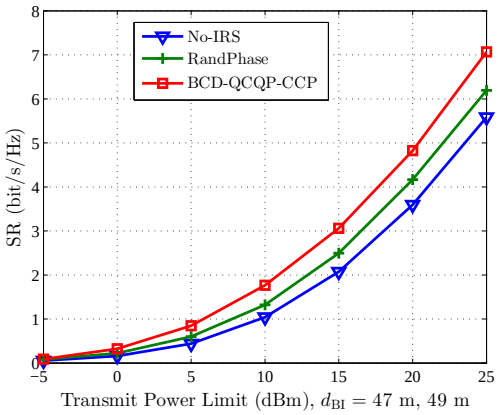

Fig. 10. Achievable SR versus the transmit power limit for multiple IRs.

elements of the IRS due to the high manufacturing cost. It is more cost-effective to implement only discrete phase shifts with a small number of control bits for each element, e.g., 1-bit for two-level (0 or π) phase shifts. Let b denote the number of bits used to discretize the phase shift. We first obtain the continuous phase shifts by the proposed algorithm and compared schemes, and then discretizing them into phase shifts with b-bits solution by the numerical method in [40]. Thus, the impact of b on the security performance is investigated in Fig. 9. The transmit power limit is 10 dBm. It is shown that the SR with continuous phase shifts of the IRS is higher than those with discrete phase shifts. The limited discrete phase shifts inevitably cause SR performance degradation. The SR of the IRS with discrete phase shifts increases with the number of control bits b, and becomes saturated when $b \geq 4$, which means that the SR loss is inevitable even when the number of control bits b is high. For the proposed BCD-MM algorithm, the maximum SR gap between the continuous phase shifts and the discrete phase shifts is 1.4 bit/s/Hz.

6) Multiple IRs Scenario: Finally, we consider the multiple IRs scenario to investigate the security enhancement brought by the IRS on the AN-aided MIMO communication systems. The horizontal distances between the BS and the two IRs are selected as $d_{BI,1} = 47$m and $d_{BI,2} = 49$m. Considering the heavy computational burden, the number of elements at the IRS is assumed to be $M = 20$. The proposed BCD-QCQP-CCP algorithm is utilized to perform the joint optimization of the TPC matrix, AN covariance matrix and the phase shifts of the IRS. The achieved SRs for the proposed algorithm, the random IRS scheme and the No-IRS scheme are shown in Fig. 10. By comparing with the Random IRS scheme and the No-IRS scheme, the proposed BCD-QCQP-CCP algorithm can optimize the phase shifts of the IRS, and thus achieves higher SRs. The SR gain increases with the power limit P_T.

VI. Conclusions

In this paper, we propose to enhance the security performance of AN-aided MIMO secure communication systems by exploiting an IRS. To exploit the IRS efficiently, we formulate an SRM problem by jointly optimizing the TPC matrix at the BS, the covariance matrix of AN and phase shifts at the IRS with the constraints of transmit power limit and unit-modulus of phase shifts. To solve this non-convex problem, we propose a BCD-MM algorithm, where the optimal TPC matrix and AN covariance matrix are obtained in semi-closed form by using the Lagrange multiplier method, and the phase shifts at the IRS are obtained in closed form by an efficient MM algorithm. Various simulations validated that significant security gains can be achieved by the IRS. Furthermore, useful engineering design guidelines for choosing and deploying the IRS are provided.

Appendix A
Derivation of Problem (23)

By substituting $h_1(\mathbf{U}_I, \mathbf{V}, \mathbf{V}_E, \mathbf{W}_I)$ of (13), $h_2(\mathbf{U}_E, \mathbf{V}_E, \mathbf{W}_E)$ of (15) and $h_3(\mathbf{V}, \mathbf{V}_E, \mathbf{W}_X)$ of (17) into (21), we have

$$\begin{aligned} \mathrm{C}_{AN}^{l}(\mathbf{T}) &= \log|\mathbf{W}_I| - \mathrm{Tr}(\mathbf{W}_I\mathbf{E}_I(\mathbf{U}_I,\mathbf{V},\mathbf{V}_E)) \\ &+ \log|\mathbf{W}_E| - \mathrm{Tr}(\mathbf{W}_E\mathbf{E}_E(\mathbf{U}_E,\mathbf{V}_E)) + \log|\mathbf{W}_X| \\ &- \mathrm{Tr}(\mathbf{W}_X\mathbf{E}_X(\mathbf{V},\mathbf{V}_E)) + d + N_t + N_E \\ &= C_{g_0} - \underbrace{\mathrm{Tr}(\mathbf{W}_I\mathbf{E}_I(\mathbf{U}_I,\mathbf{V},\mathbf{V}_E))}_{g_1} \\ &- \underbrace{\mathrm{Tr}(\mathbf{W}_E\mathbf{E}_E(\mathbf{U}_E,\mathbf{V}_E))}_{g_2} - \underbrace{\mathrm{Tr}(\mathbf{W}_X\mathbf{E}_X(\mathbf{V},\mathbf{V}_E))}_{g_3}, \end{aligned} \tag{62}$$

where $C_{g_0} \triangleq \log|\mathbf{W}_I| + \log|\mathbf{W}_E| + \log|\mathbf{W}_X| + d + N_t + N_E$. C_{g_0} contains the constant terms independent of $\mathbf{V}, \mathbf{V}_E, \mathbf{\Phi}$. By substituting matrix functions $\mathbf{E}_I$, $\mathbf{E}_E$ and $\mathbf{E}_X$ into (62), we expand g_1, g_2, and g_3 respectively as follows.

(1) g_1 can be reformulated as

$$g_1 = \mathrm{Tr}(\mathbf{W}_I[(\mathbf{I}-\mathbf{U}_I{}^H\hat{\mathbf{H}}_I\mathbf{V})(\mathbf{I}-\mathbf{U}_I{}^H\hat{\mathbf{H}}_I\mathbf{V})^H + \mathbf{U}_I{}^H(\hat{\mathbf{H}}_I\mathbf{V}_E\mathbf{V}_E{}^H\hat{\mathbf{H}}_I^H+\sigma_I^2\mathbf{I}_{N_I})\mathbf{U}_I]). \quad (63)$$

By gathering the constant terms related with $\mathbf{W}_I, \mathbf{U}_I$ in C_{g_1}, g_1 can be simplified as

$$g_1 = -\mathrm{Tr}(\mathbf{W}_I\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I) - \mathrm{Tr}(\mathbf{W}_I\mathbf{U}_I{}^H\hat{\mathbf{H}}_I\mathbf{V}) + \mathrm{Tr}(\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I{}^H\hat{\mathbf{H}}_I\mathbf{V}) + \mathrm{Tr}(\mathbf{V}_E{}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I{}^H\hat{\mathbf{H}}_I\mathbf{V}_E) + C_{g_1}, \quad (64)$$

where $C_{g_1} \triangleq \mathrm{Tr}(\mathbf{W}_I + \sigma_I^2\mathbf{W}_I\mathbf{U}_I{}^H\mathbf{U}_I)$.

(2) g_2 can be reformulated as

$$g_2 = \mathrm{Tr}(\mathbf{W}_E[(\mathbf{I}-\mathbf{U}_E{}^H\hat{\mathbf{H}}_E\mathbf{V}_E)(\mathbf{I}-\mathbf{U}_E{}^H\hat{\mathbf{H}}_E\mathbf{V}_E)^H + \sigma_E^2\mathbf{U}_E{}^H\mathbf{U}_E]). \quad (65)$$

By gathering the constant terms related with $\mathbf{W}_E, \mathbf{U}_E$ in C_{g_2}, g_2 can be simplified as

$$g_2 = -\mathrm{Tr}(\mathbf{W}_E\mathbf{V}_E{}^H\hat{\mathbf{H}}_E^H\mathbf{U}_E) - \mathrm{Tr}(\mathbf{W}_E\mathbf{U}_E{}^H\hat{\mathbf{H}}_E\mathbf{V}_E) + \mathrm{Tr}(\mathbf{V}_E{}^H\hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E\mathbf{U}_E{}^H\hat{\mathbf{H}}_E\mathbf{V}_E) + C_{g_2}, \quad (66)$$

where $C_{g_2} \triangleq \mathrm{Tr}(\mathbf{W}_E + \sigma_E^2\mathbf{W}_E\mathbf{U}_E{}^H\mathbf{U}_E)$.

(3) g_3 can be reformulated as

$$g_3 = \mathrm{Tr}(\mathbf{W}_X(\mathbf{I}_{N_E} + \sigma_E^{-2}\hat{\mathbf{H}}_E(\mathbf{V}\mathbf{V}^H + \mathbf{V}_E\mathbf{V}_E{}^H)\hat{\mathbf{H}}_E^H)). \quad (67)$$

By gathering the constant terms related with $\mathbf{W}_X$ in C_{g_3}, g_3 can be simplified as

$$g_3 = \sigma_E^{-2}\mathrm{Tr}(\mathbf{V}^H\hat{\mathbf{H}}_E^H\mathbf{W}_X\hat{\mathbf{H}}_E\mathbf{V}) + \sigma_E^{-2}\mathrm{Tr}(\mathbf{V}_E{}^H\hat{\mathbf{H}}_E^H\mathbf{W}_X\hat{\mathbf{H}}_E\mathbf{V}_E) + C_{g_3}, \quad (68)$$

where $C_{g_3} \triangleq \mathrm{Tr}(\mathbf{W}_X)$.

By substituting (64), (66) and (68) into (62), we have

$$\begin{aligned}\mathrm{C}_{AN}^l(\mathbf{T}) &= \mathrm{Tr}(\mathbf{W}_I\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I) + \mathrm{Tr}(\mathbf{W}_I\mathbf{U}_I{}^H\hat{\mathbf{H}}_I\mathbf{V}) \\ &- \mathrm{Tr}(\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I{}^H\hat{\mathbf{H}}_I\mathbf{V}) + \mathrm{Tr}(\mathbf{W}_E\mathbf{V}_E{}^H\hat{\mathbf{H}}_E^H\mathbf{U}_E) \\ &- \mathrm{Tr}(\mathbf{V}_E{}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I{}^H\hat{\mathbf{H}}_I\mathbf{V}_E) + \mathrm{Tr}(\mathbf{W}_E\mathbf{U}_E{}^H\hat{\mathbf{H}}_E\mathbf{V}_E) \\ &- \mathrm{Tr}(\mathbf{V}_E{}^H\hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E\mathbf{U}_E{}^H\hat{\mathbf{H}}_E\mathbf{V}_E) \\ &- \sigma_E^{-2}\mathrm{Tr}(\mathbf{V}^H\hat{\mathbf{H}}_E^H\mathbf{W}_X\hat{\mathbf{H}}_E\mathbf{V}) \\ &- \sigma_E^{-2}\mathrm{Tr}(\mathbf{V}_E{}^H\hat{\mathbf{H}}_E^H\mathbf{W}_X\hat{\mathbf{H}}_E\mathbf{V}_E) + C_g, \end{aligned} \quad (69)$$

where $C_g \triangleq C_{g_0} - C_{g_1} - C_{g_2} - C_{g_3}$.

Equation (69) can be rewritten more compactly as

$$\begin{aligned}\mathrm{C}_{AN}^l(\mathbf{T}) &= C_g + \mathrm{Tr}(\mathbf{W}_I\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I) + \mathrm{Tr}(\mathbf{W}_I\mathbf{U}_I{}^H\hat{\mathbf{H}}_I\mathbf{V}) \\ &- \mathrm{Tr}(\mathbf{V}^H\mathbf{H}_V\mathbf{V}) + \mathrm{Tr}(\mathbf{W}_E\mathbf{V}_E{}^H\hat{\mathbf{H}}_E^H\mathbf{U}_E) \\ &+ \mathrm{Tr}(\mathbf{W}_E\mathbf{U}_E{}^H\hat{\mathbf{H}}_E\mathbf{V}_E) - \mathrm{Tr}(\mathbf{V}_E{}^H\mathbf{H}_{VE}\mathbf{V}_E). \end{aligned} \quad (70)$$

where

$$\mathbf{H}_V = \hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I{}^H\hat{\mathbf{H}}_I + \sigma_E^{-2}\hat{\mathbf{H}}_E^H\mathbf{W}_X\hat{\mathbf{H}}_E. \quad (71a)$$

$$\mathbf{H}_{VE} = \hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I{}^H\hat{\mathbf{H}}_I + \hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E\mathbf{U}_E{}^H\hat{\mathbf{H}}_E + \sigma_E^{-2}\hat{\mathbf{H}}_E^H\mathbf{W}_X\hat{\mathbf{H}}_E. \quad (71b)$$

By substituting (70) into Problem (22), and removing the constant term C_g, we arrive at Problem (23).

APPENDIX B
DERIVATION OF THE NEW OF FORM IN (46)

The objective function of Problem (45) is

$$\begin{aligned}g_0(\mathbf{V},\mathbf{V}_E,\mathbf{\Phi}) &= -\mathrm{Tr}(\mathbf{W}_I\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I) \\ &- \mathrm{Tr}(\mathbf{W}_I\mathbf{U}_I{}^H\hat{\mathbf{H}}_I\mathbf{V}) + \mathrm{Tr}(\mathbf{V}^H\mathbf{H}_V\mathbf{V}) \\ &- \mathrm{Tr}(\mathbf{W}_E\mathbf{V}_E{}^H\hat{\mathbf{H}}_E^H\mathbf{U}_E) - \mathrm{Tr}(\mathbf{W}_E\mathbf{U}_E{}^H\hat{\mathbf{H}}_E\mathbf{V}_E) \\ &+ \mathrm{Tr}(\mathbf{V}_E{}^H\mathbf{H}_{VE}\mathbf{V}_E). \end{aligned} \quad (72)$$

The third term of (72) is

$$\begin{aligned}&\mathrm{Tr}\left(\mathbf{V}^H\mathbf{H}_V\mathbf{V}\right) \\ &= \mathrm{Tr}\left[\mathbf{V}^H\left(\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I^H\hat{\mathbf{H}}_I + \sigma_E^{-2}\hat{\mathbf{H}}_E^H\mathbf{W}_X\hat{\mathbf{H}}_E\right)\mathbf{V}\right] \\ &= \mathrm{Tr}\left[\hat{\mathbf{H}}_I\mathbf{V}\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I^H\right] \\ &\quad + \sigma_E^{-2}\mathrm{Tr}\left[\hat{\mathbf{H}}_E\mathbf{V}\mathbf{V}^H\hat{\mathbf{H}}_E^H\mathbf{W}_X\right]. \end{aligned} \quad (73)$$

The sixth term of (72) is

$$\begin{aligned}&\mathrm{Tr}\left(\mathbf{V}_E^H\mathbf{H}_{VE}\mathbf{V}_E\right) = \mathrm{Tr}[\mathbf{V}_E^H(\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I^H\hat{\mathbf{H}}_I \\ &+ \hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E\mathbf{U}_E^H\hat{\mathbf{H}}_E + \sigma_E^{-2}\hat{\mathbf{H}}_E^H\mathbf{W}_X\hat{\mathbf{H}}_E)\mathbf{V}_E] \\ &= \mathrm{Tr}\left[\hat{\mathbf{H}}_I\mathbf{V}_E\mathbf{V}_E^H\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I^H\right] \\ &\quad + \mathrm{Tr}\left[\hat{\mathbf{H}}_E\mathbf{V}_E\mathbf{V}_E^H\hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E\mathbf{U}_E^H\right] \\ &\quad + \sigma_E^{-2}\mathrm{Tr}\left[\hat{\mathbf{H}}_E\mathbf{V}_E\mathbf{V}_E^H\hat{\mathbf{H}}_E^H\mathbf{W}_X\right]. \end{aligned} \quad (74)$$

The summation of Equation (73) and Equation (74) is

$$\begin{aligned}&\mathrm{Tr}\left(\mathbf{V}^H\mathbf{H}_V\mathbf{V}\right) + \mathrm{Tr}\left(\mathbf{V}_E^H\mathbf{H}_{VE}\mathbf{V}_E\right) \\ &= \mathrm{Tr}\left[\hat{\mathbf{H}}_I\left(\mathbf{V}\mathbf{V}^H + \mathbf{V}_E\mathbf{V}_E^H\right)\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I^H\right] \\ &\quad + \sigma_E^{-2}\mathrm{Tr}\left[\hat{\mathbf{H}}_E\left(\mathbf{V}\mathbf{V}^H + \mathbf{V}_E\mathbf{V}_E^H\right)\hat{\mathbf{H}}_E^H\mathbf{W}_X\right] \\ &\quad + \mathrm{Tr}\left[\hat{\mathbf{H}}_E\mathbf{V}_E\mathbf{V}_E^H\hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E\mathbf{U}_E^H\right]. \end{aligned} \quad (75)$$

By defining $\mathbf{V}_X = \left(\mathbf{V}\mathbf{V}^H + \mathbf{V}_E\mathbf{V}_E^H\right)$ and $\mathbf{M}_I = \mathbf{U}_I\mathbf{W}_I\mathbf{U}_I^H$, the first part of (75) can be derived as

$$\begin{aligned}&\mathrm{Tr}\left[\hat{\mathbf{H}}_I\left(\mathbf{V}\mathbf{V}^H + \mathbf{V}_E\mathbf{V}_E^H\right)\hat{\mathbf{H}}_I^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I^H\right] \\ &= \mathrm{Tr}\left[\hat{\mathbf{H}}_I\mathbf{V}_X\hat{\mathbf{H}}_I^H\mathbf{M}_I\right] \\ &= \mathrm{Tr}\left[\left(\mathbf{H}_{b,I} + \mathbf{H}_{R,I}\mathbf{\Phi}\mathbf{G}\right)\mathbf{V}_X\left(\mathbf{H}_{b,I}^H + \mathbf{G}^H\mathbf{\Phi}^H\mathbf{H}_{R,I}^H\right)\mathbf{M}_I\right] \\ &= \mathrm{Tr}[\mathbf{H}_{b,I}\mathbf{V}_X\mathbf{H}_{b,I}^H\mathbf{M}_I + \mathbf{H}_{b,I}\mathbf{V}_X\mathbf{G}^H\mathbf{\Phi}^H\mathbf{H}_{R,I}^H\mathbf{M}_I \\ &+ \mathbf{H}_{R,I}\mathbf{\Phi}\mathbf{G}\mathbf{V}_X\mathbf{H}_{b,I}^H\mathbf{M}_I + \mathbf{H}_{R,I}\mathbf{\Phi}\mathbf{G}\mathbf{V}_X\mathbf{G}^H\mathbf{\Phi}^H\mathbf{H}_{R,I}^H\mathbf{M}_I]. \end{aligned} \quad (76)$$

Based on the derivation in (76), it is obvious that the second part of (75) can be derived as

$$\begin{aligned}&\sigma_E^{-2}\mathrm{Tr}\left[\hat{\mathbf{H}}_E\left(\mathbf{V}\mathbf{V}^H+\mathbf{V}_E\mathbf{V}_E^H\right)\hat{\mathbf{H}}_E^H\mathbf{W}_X\right]\\&=\sigma_E^{-2}\mathrm{Tr}[\mathbf{H}_{b,E}\mathbf{V}_X\mathbf{H}_{b,E}^H\mathbf{W}_X\\&+\mathbf{H}_{b,E}\mathbf{V}_X\mathbf{G}^H\mathbf{\Phi}^H\mathbf{H}_{R,E}^H\mathbf{W}_X+\mathbf{H}_{R,E}\mathbf{\Phi}\mathbf{G}\mathbf{V}_X\mathbf{H}_{b,E}^H\mathbf{W}_X\\&+\mathbf{H}_{R,E}\mathbf{\Phi}\mathbf{G}\mathbf{V}_X\mathbf{G}^H\mathbf{\Phi}^H\mathbf{H}_{R,E}^H\mathbf{W}_X].\end{aligned}\tag{77}$$

Based on the derivation in (76) and by defining $\mathbf{M}_E=\mathbf{U}_E\mathbf{W}_E\mathbf{U}_E^H$, it is obvious that the third part of (75) can be derived as

$$\begin{aligned}&\mathrm{Tr}\left[\hat{\mathbf{H}}_E\mathbf{V}_E\mathbf{V}_E^H\hat{\mathbf{H}}_E^H\mathbf{U}_E\mathbf{W}_E\mathbf{U}_E^H\right]\\&=\mathrm{Tr}\left[\hat{\mathbf{H}}_E\left(\mathbf{V}_E\mathbf{V}_E^H\right)\hat{\mathbf{H}}_E^H\mathbf{M}_E\right]\\&=\mathrm{Tr}[\mathbf{H}_{b,E}\mathbf{V}_E\mathbf{V}_E^H\mathbf{H}_{b,E}^H\mathbf{M}_E+\mathbf{H}_{b,E}\mathbf{V}_E\mathbf{V}_E^H\mathbf{G}^H\mathbf{\Phi}^H\mathbf{H}_{R,E}^H\mathbf{M}_E\\&+\mathbf{H}_{R,E}\mathbf{\Phi}\mathbf{G}\mathbf{V}_E\mathbf{V}_E^H\mathbf{H}_{b,E}^H\mathbf{M}_E\\&+\mathbf{H}_{R,E}\mathbf{\Phi}\mathbf{G}\mathbf{V}_E\mathbf{V}_E^H\mathbf{G}^H\mathbf{\Phi}^H\mathbf{H}_{R,E}^H\mathbf{M}_E].\end{aligned}\tag{78}$$

By adding (76), (77) and (78), and gathering constant terms independent of $\mathbf{\Phi}$, (75) becomes

$$\begin{aligned}&\mathrm{Tr}\left(\mathbf{V}^H\mathbf{H}_V\mathbf{V}\right)+\mathrm{Tr}\left(\mathbf{V}_E^H\mathbf{H}_{VE}\mathbf{V}_E\right)\\&=\mathrm{Tr}[\mathbf{\Phi}^H(\mathbf{H}_{R,I}^H\mathbf{M}_I\mathbf{H}_{b,I}\mathbf{V}_X\mathbf{G}^H+\sigma_E^{-2}\mathbf{H}_{R,E}^H\mathbf{W}_X\mathbf{H}_{b,E}\mathbf{V}_X\mathbf{G}^H\\&+\mathbf{H}_{R,E}^H\mathbf{M}_E\mathbf{H}_{b,E}\mathbf{V}_E\mathbf{V}_E^H\mathbf{G}^H)]+\mathrm{Tr}[\mathbf{\Phi}(\mathbf{G}\mathbf{V}_X\mathbf{H}_{b,I}^H\mathbf{M}_I\mathbf{H}_{R,I}\\&+\sigma_E^{-2}\mathbf{G}\mathbf{V}_X\mathbf{H}_{b,E}^H\mathbf{W}_X\mathbf{H}_{R,E}+\mathbf{G}\mathbf{V}_E\mathbf{V}_E^H\mathbf{H}_{b,E}^H\mathbf{M}_E\mathbf{H}_{R,E})]\\&+\mathrm{Tr}\left[\mathbf{\Phi}\mathbf{G}\mathbf{V}_X\mathbf{G}^H\mathbf{\Phi}^H\left(\mathbf{H}_{R,I}^H\mathbf{M}_I\mathbf{H}_{R,I}+\sigma_E^{-2}\mathbf{H}_{R,E}^H\mathbf{W}_X\mathbf{H}_{R,E}\right)\right]\\&+\mathrm{Tr}\left[\mathbf{\Phi}\mathbf{G}\mathbf{V}_E\mathbf{V}_E^H\mathbf{G}^H\mathbf{\Phi}^H\mathbf{H}_{R,E}^H\mathbf{M}_E\mathbf{H}_{R,E}\right]+C_{t_1},\end{aligned}\tag{79}$$

where

$$\begin{aligned}C_{t_1}=&\mathrm{Tr}\left[\mathbf{H}_{b,I}\mathbf{V}_X\mathbf{H}_{b,I}^H\mathbf{M}_I\right]+\sigma_E^{-2}\mathrm{Tr}\left[\mathbf{H}_{b,E}\mathbf{V}_X\mathbf{H}_{b,E}^H\mathbf{W}_X\right]\\&+\mathrm{Tr}\left[\mathbf{H}_{b,E}\mathbf{V}_E\mathbf{V}_E^H\mathbf{H}_{b,E}^H\mathbf{M}_E\right].\end{aligned}\tag{80}$$

The first term of $g_0(\mathbf{V},\mathbf{V}_E,\mathbf{\Phi})$ is derived as

$$\begin{aligned}\mathrm{Tr}\left(\mathbf{W}_I\mathbf{V}^H\hat{\mathbf{H}}_I^H\mathbf{U}_I\right)=&\underbrace{\mathrm{Tr}\left[\mathbf{U}_I\mathbf{W}_I^H\mathbf{V}^H\mathbf{H}_{b,I}^H\right]}_{C_{t_2}\,(\text{constant for }\mathbf{\Phi})}\\&+\mathrm{Tr}\left[\mathbf{H}_{R,I}^H\mathbf{U}_I\mathbf{W}_I^H\mathbf{V}^H\mathbf{G}^H\mathbf{\Phi}^H\right].\end{aligned}\tag{81}$$

The second term of $g_0(\mathbf{V},\mathbf{V}_E,\mathbf{\Phi})$ is derived as

$$\begin{aligned}\mathrm{Tr}\left(\mathbf{W}_I\mathbf{U}_I^H\hat{\mathbf{H}}_I\mathbf{V}\right)=&\underbrace{\mathrm{Tr}\left[\mathbf{H}_{b,I}\mathbf{V}\mathbf{W}_I\mathbf{U}_I^H\right]}_{C_{t_3}\,(\text{constant for }\mathbf{\Phi})}\\&+\mathrm{Tr}\left[\mathbf{\Phi}\mathbf{G}\mathbf{V}\mathbf{W}_I\mathbf{U}_I^H\mathbf{H}_{R,I}\right].\end{aligned}\tag{82}$$

The fourth term of $g_0(\mathbf{V},\mathbf{V}_E,\mathbf{\Phi})$ is derived as

$$\begin{aligned}\mathrm{Tr}\left(\mathbf{W}_E\mathbf{V}_E^H\hat{\mathbf{H}}_E^H\mathbf{U}_E\right)=&\underbrace{\mathrm{Tr}\left[\mathbf{U}_E\mathbf{W}_E^H\mathbf{V}_E^H\mathbf{H}_{b,E}^H\right]}_{C_{t_4}\,(\text{constant for }\mathbf{\Phi})}\\&+\mathrm{Tr}\left[\mathbf{H}_{R,E}^H\mathbf{U}_E\mathbf{W}_E^H\mathbf{V}_E^H\mathbf{G}^H\mathbf{\Phi}^H\right].\end{aligned}\tag{83}$$

The fifth term of $g_0(\mathbf{V},\mathbf{V}_E,\mathbf{\Phi})$ is derived as

$$\begin{aligned}\mathrm{Tr}\left(\mathbf{W}_E\mathbf{U}_E^H\hat{\mathbf{H}}_E\mathbf{V}_E\right)=&\underbrace{\mathrm{Tr}\left[\mathbf{H}_{b,E}\mathbf{V}_E\mathbf{W}_E\mathbf{U}_E^H\right]}_{C_{t_5}\,(\text{constant for }\mathbf{\Phi})}\\&+\mathrm{Tr}\left[\mathbf{\Phi}\mathbf{G}\mathbf{V}_E\mathbf{W}_E\mathbf{U}_E^H\mathbf{H}_{R,E}\right].\end{aligned}\tag{84}$$

By including the first term in (81), the second term in (82), the fourth term in (83), the fifth term in (84), and the sum of the third and six terms in (79) of $g_0(\mathbf{V},\mathbf{V}_E,\mathbf{\Phi})$ and gathering constant terms independent of $\mathbf{\Phi}$, we have $g_0(\mathbf{\Phi})$ in (85), where $C_t=C_{t_1}+C_{t_2}+C_{t_3}+C_{t_4}+C_{t_5}$.

Then $g_0(\mathbf{\Phi})$ becomes

$$\begin{aligned}g_0(\mathbf{\Phi})=&\mathrm{Tr}\left(\mathbf{\Phi}^H\mathbf{D}^H\right)+\mathrm{Tr}\left(\mathbf{\Phi}\mathbf{D}\right)+\mathrm{Tr}\left[\mathbf{\Phi}\mathbf{C}_{VE}\mathbf{\Phi}^H\mathbf{B}_{VE}\right]\\&+\mathrm{Tr}\left(\mathbf{\Phi}\mathbf{C}_V\mathbf{\Phi}^H\mathbf{B}_V\right)+C_t\\=&\mathrm{Tr}\left(\mathbf{\Phi}^H\mathbf{D}^H\right)+\mathrm{Tr}\left(\mathbf{\Phi}\mathbf{D}\right)+\mathrm{Tr}\left[\mathbf{\Phi}^H\mathbf{B}_{VE}\mathbf{\Phi}\mathbf{C}_{VE}\right]\\&+\mathrm{Tr}\left(\mathbf{\Phi}^H\mathbf{B}_V\mathbf{\Phi}\mathbf{C}_V\right)+C_t,\end{aligned}\tag{86}$$

where

$$\begin{aligned}\mathbf{D}=&\mathbf{G}\mathbf{V}_X\mathbf{H}_{b,I}^H\mathbf{M}_I\mathbf{H}_{R,I}+\sigma_E^{-2}\mathbf{G}\mathbf{V}_X\mathbf{H}_{b,E}^H\mathbf{W}_X\mathbf{H}_{R,E}\\&+\mathbf{G}\mathbf{V}_E\mathbf{V}_E^H\mathbf{H}_{b,E}^H\mathbf{M}_E\mathbf{H}_{R,E}-\mathbf{G}\mathbf{V}\mathbf{W}_I\mathbf{U}_I^H\mathbf{H}_{R,I}\\&-\mathbf{G}\mathbf{V}_E\mathbf{W}_E\mathbf{U}_E^H\mathbf{H}_{R,E},\end{aligned}\tag{87a}$$

$$\mathbf{C}_{VE}=\mathbf{G}\mathbf{V}_E\mathbf{V}_E^H\mathbf{G}^H,\tag{87b}$$

$$\mathbf{C}_V=\mathbf{G}\mathbf{V}\mathbf{V}^H\mathbf{G}^H,\tag{87c}$$

$$\begin{aligned}\mathbf{B}_{VE}=&(\mathbf{H}_{R,I}^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I^H\mathbf{H}_{R,I}+\sigma_E^{-2}\mathbf{H}_{R,E}^H\mathbf{W}_X\mathbf{H}_{R,E}\\&+\mathbf{H}_{R,E}^H\mathbf{U}_E\mathbf{W}_E\mathbf{U}_E^H\mathbf{H}_{R,E}),\end{aligned}\tag{87d}$$

$$\mathbf{B}_V=\left(\mathbf{H}_{R,I}^H\mathbf{U}_I\mathbf{W}_I\mathbf{U}_I^H\mathbf{H}_{R,I}+\sigma_E^{-2}\mathbf{H}_{R,E}^H\mathbf{W}_X\mathbf{H}_{R,E}\right).\tag{87e}$$

REFERENCES

[1] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE network*, vol. 34, no. 3, pp. 134–142, 2019.

[2] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, 2010.

[3] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, 2018.

[4] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennaspart II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.

[8] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, 2010.

$$
\begin{aligned}
g_0(\mathbf{\Phi}) &= -\text{Equation (81)} - \text{Equation (82)} - \text{Equation (83)} - \text{Equation (84)} + \text{Equation (79)} \\
&= \mathrm{Tr}\left[\mathbf{\Phi}^H \begin{pmatrix} \mathbf{H}_{R,I}^H \mathbf{M}_I \mathbf{H}_{b,I} \mathbf{V}_X \mathbf{G}^H + \sigma_E^{-2} \mathbf{H}_{R,E}^H \mathbf{W}_X \mathbf{H}_{b,E} \mathbf{V}_X \mathbf{G}^H + \mathbf{H}_{R,E}^H \mathbf{M}_E \mathbf{H}_{b,E} \mathbf{V}_E \mathbf{V}_E^H \mathbf{G}^H \\ -\mathbf{H}_{R,I}^H \mathbf{U}_I \mathbf{W}_I^H \mathbf{V}^H \mathbf{G}^H - \mathbf{H}_{R,E}^H \mathbf{U}_E \mathbf{W}_E^H \mathbf{V}_E^H \mathbf{G}^H \end{pmatrix}\right] \\
&\quad + \mathrm{Tr}\left[\mathbf{\Phi} \begin{pmatrix} \mathbf{G}\mathbf{V}_X \mathbf{H}_{b,I}^H \mathbf{M}_I \mathbf{H}_{R,I} + \sigma_E^{-2} \mathbf{G}\mathbf{V}_X \mathbf{H}_{b,E}^H \mathbf{W}_X \mathbf{H}_{R,E} + \mathbf{G}\mathbf{V}_E \mathbf{V}_E^H \mathbf{H}_{b,E}^H \mathbf{M}_E \mathbf{H}_{R,E} \\ -\mathbf{G}\mathbf{V}\mathbf{W}_I \mathbf{U}_I^H \mathbf{H}_{R,I} - \mathbf{G}\mathbf{V}_E \mathbf{W}_E \mathbf{U}_E^H \mathbf{H}_{R,E} \end{pmatrix}\right] \\
&\quad + \mathrm{Tr}\left[\mathbf{\Phi}\mathbf{G}\mathbf{V}_E \mathbf{V}_E^H \mathbf{G}^H \mathbf{\Phi}^H \left(\mathbf{H}_{R,I}^H \mathbf{M}_I \mathbf{H}_{R,I} + \sigma_E^{-2} \mathbf{H}_{R,E}^H \mathbf{W}_X \mathbf{H}_{R,E} + \mathbf{H}_{R,E}^H \mathbf{M}_E \mathbf{H}_{R,E}\right)\right] \\
&\quad + \mathrm{Tr}\left[\mathbf{\Phi}\mathbf{G}\mathbf{V}\mathbf{V}^H \mathbf{G}^H \mathbf{\Phi}^H \left(\mathbf{H}_{R,I}^H \mathbf{M}_I \mathbf{H}_{R,I} + \sigma_E^{-2} \mathbf{H}_{R,E}^H \mathbf{W}_X \mathbf{H}_{R,E}\right)\right] + C_t \\
&= \mathrm{Tr}\left[\mathbf{\Phi}^H \begin{pmatrix} \mathbf{H}_{R,I}^H \mathbf{M}_I \mathbf{H}_{b,I} \mathbf{V}_X \mathbf{G}^H + \sigma_E^{-2} \mathbf{H}_{R,E}^H \mathbf{W}_X \mathbf{H}_{b,E} \mathbf{V}_X \mathbf{G}^H + \mathbf{H}_{R,E}^H \mathbf{M}_E \mathbf{H}_{b,E} \mathbf{V}_E \mathbf{V}_E^H \mathbf{G}^H \\ -\mathbf{H}_{R,I}^H \mathbf{U}_I \mathbf{W}_I^H \mathbf{V}^H \mathbf{G}^H - \mathbf{H}_{R,E}^H \mathbf{U}_E \mathbf{W}_E^H \mathbf{V}_E^H \mathbf{G}^H \end{pmatrix}\right] \\
&\quad + \mathrm{Tr}\left[\mathbf{\Phi} \begin{pmatrix} \mathbf{G}\mathbf{V}_X \mathbf{H}_{b,I}^H \mathbf{M}_I \mathbf{H}_{R,I} + \sigma_E^{-2} \mathbf{G}\mathbf{V}_X \mathbf{H}_{b,E}^H \mathbf{W}_X \mathbf{H}_{R,E} + \mathbf{G}\mathbf{V}_E \mathbf{V}_E^H \mathbf{H}_{b,E}^H \mathbf{M}_E \mathbf{H}_{R,E} \\ -\mathbf{G}\mathbf{V}\mathbf{W}_I \mathbf{U}_I^H \mathbf{H}_{R,I} - \mathbf{G}\mathbf{V}_E \mathbf{W}_E \mathbf{U}_E^H \mathbf{H}_{R,E} \end{pmatrix}\right] \\
&\quad + \mathrm{Tr}\left[\mathbf{\Phi}\mathbf{G}\mathbf{V}_E \mathbf{V}_E^H \mathbf{G}^H \mathbf{\Phi}^H \left(\mathbf{H}_{R,I}^H \mathbf{U}_I \mathbf{W}_I \mathbf{U}_I^H \mathbf{H}_{R,I} + \sigma_E^{-2} \mathbf{H}_{R,E}^H \mathbf{W}_X \mathbf{H}_{R,E} + \mathbf{H}_{R,E}^H \mathbf{U}_E \mathbf{W}_E \mathbf{U}_E^H \mathbf{H}_{R,E}\right)\right] \\
&\quad + \mathrm{Tr}\left[\mathbf{\Phi}\mathbf{G}\mathbf{V}\mathbf{V}^H \mathbf{G}^H \mathbf{\Phi}^H \left(\mathbf{H}_{R,I}^H \mathbf{U}_I \mathbf{W}_I \mathbf{U}_I^H \mathbf{H}_{R,I} + \sigma_E^{-2} \mathbf{H}_{R,E}^H \mathbf{W}_X \mathbf{H}_{R,E}\right)\right] + C_t, \qquad (85)
\end{aligned}
$$

[9] 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, 2013.

[10] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, 2020.

[11] C. Huang, S. Hu, G. C. Alexandropoulos, A. Zappone, C. Yuen, R. Zhang, M. Di Renzo, and M. Debbah, "Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends," *IEEE Wireless Communications*, 2020.

[12] Q. Wu and R. Zhang, "Beamforming optimization for wireless network aided by intelligent reflecting surface with discrete phase shifts," *IEEE Transactions on Communications*, vol. 68, no. 3, pp. 1838–1851, 2020.

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

[14] C. Huang, R. Mo, and C. Yuen, "Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 8, pp. 1839–1850, 2020.

[15] C. Pan, H. Ren, K. Wang, W. Xu, M. Elkashlan, A. Nallanathan, and L. Hanzo, "Multicell MIMO communications relying on intelligent reflecting surfaces," *IEEE Transactions on Wireless Communications*, 2020.

[16] X. Yu, D. Xu, and R. Schober, "MISO wireless communication systems via intelligent reflecting surfaces," in *2019 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE, 2019, pp. 735–740.

[17] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, 2019.

[18] G. Zhou, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Intelligent reflecting surface aided multigroup multicast MISO communication systems," *IEEE Transactions on Signal Processing*, 2020.

[19] T. Bai, C. Pan, Y. Deng, M. Elkashlan, and A. Nallanathan, "Latency minimization for intelligent reflecting surface aided mobile edge computing." [Online]. Available: https://arxiv.org/abs/1910.07990

[20] C. Pan, H. Ren, K. Wang, M. Elkashlan, A. Nallanathan, J. Wang, and L. Hanzo, "Intelligent reflecting surface aided MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Journal on Selected Areas in Communications*, 2020.

[21] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.

[22] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, 2019.

[23] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1488–1492, 2019.

[24] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82 599–82 612, 2019.

[25] Z. Luo, W. Ma, A. M. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems and applications," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, 2010.

[26] Y. Sun, P. Babu, and D. P. Palomar, "Majorization-minimization algorithms in signal processing, communications, and machine learning," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 794–816, 2016.

[27] P. A. Absil, R. Mahony, and R. Sepulchre, *Optimization algorithms on matrix manifolds*. Princeton University Press, 2009.

[28] B. Feng, Y. Wu, and M. Zheng, "Secure transmission strategy for intelligent reflecting surface enhanced wireless system," in *2019 11th International Conference on Wireless Communications and Signal Processing (WCSP)*. IEEE, 2019, pp. 1–6.

[29] W. Shi, X. Zhou, L. Jia, Y. Wu, F. Shu, and J. Wang, "Enhanced secure wireless information and power transfer via intelligent reflecting surface." [Online]. Available: https://arxiv.org/abs/1911.01001

[30] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication via joint beamforming and jamming." [Online]. Available: https://arxiv.org/abs/1907.12839

[31] D. Xu, X. Yu, Y. Sun, D. W. K. Ng, and R. Schober, "Resource allocation for secure IRS-assisted multiuser MISO systems," in *2019 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2019, pp. 1–6.

[32] G. Zhou, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "A framework of robust transmission design for IRS-aided MISO communications with imperfect cascaded channels," *IEEE Transactions on Signal Processing*, pp. 1–1, 2020.

[33] X. Tan, Z. Sun, J. M. Jornet, and D. Pados, "Increasing indoor spectrum sharing capacity using smart reflect-array," in *2016 IEEE International Conference on Communications (ICC)*. IEEE, 2016, pp. 1–6.

[34] 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." [Online]. Available: https://arxiv.org/abs/2004.11580v2

[35] Q. Shi, W. Xu, J. Wu, E. Song, and Y. Wang, "Secure beamforming for MIMO broadcasting with wireless information and power

transfer," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2841–2853, 2015.
[36] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," 2014.
[37] X. D. Zhang, *Matrix analysis and applications*. Cambridge University Press, 2017.
[38] Y. Liang, H. V. Poor *et al.*, "Information theoretic security," *Foundations and Trends in communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.
[39] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface." [Online]. Available: https://arxiv.org/abs/2002.07063
[40] C. Huang, G. C. Alexandropoulos, A. Zappone, M. Debbah, and C. Yuen, "Energy efficient multi-user MISO communication using low resolution large intelligent surfaces," in *2018 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2018, pp. 1–6.

Sheng Hong received the B.S. degree in communication engineering from South-Central University For Nationalities, Wuhan, China, in 2009, and the Ph.D. degrees in radio physics from Wuhan University, Wuhan, China, in 2015. She has been a faculty member in Nanchang University since 2015. From 2019 to 2020, she was a Visiting Researcher with the School of Electronic Engineering and Computer Science, Queen Mary University of London, U.K. Her research interests lie in the areas of intelligent reflection surface (IRS), physical lay security, wireless communication and signal processing.

Cunhua Pan received the B.S. and Ph.D. degrees from the School of Information Science and Engineering, Southeast University, Nanjing, China, in 2010 and 2015, respectively. From 2015 to 2016, he was a Research Associate at the University of Kent, U.K. He held a post-doctoral position at Queen Mary University of London, U.K., from 2016 and 2019, where he is currently a Lecturer.

His research interests mainly include intelligent reflection surface (IRS), machine learning, UAV, Internet of Things, and mobile edge computing. He serves as a TPC member for numerous conferences, such as ICC and GLOBECOM, and the Student Travel Grant Chair for ICC 2019. He also serves as an Editor of IEEE Wireless Communication Letters and IEEE ACCESS.

Hong Ren received the B.S. degree in electrical engineering from Southwest Jiaotong University, Chengdu, China, in 2011, and the M.S. and Ph.D. degrees in Electrical Engineering from Southeast University, Nanjing, China, in 2014 and 2018, respectively. From 2016 to 2018, she was a Visiting Student with the School of Electronics and Computer Science, University of Southampton, U.K. She is currently a Post-Doctoral Scholar with the School of Electronic Engineering and Computer Science, Queen Mary University of London, U.K. Her research interests lie in the areas of communication and signal processing, including green communication systems, cooperative transmission, and cross layer transmission optimization.

Kezhi Wang received his B.E. and M.E. degrees in School of Automation from Chongqing University, China, in 2008 and 2011, respectively. He received his Ph.D. degree in Engineering from the University of Warwick, U.K. in 2015. He was a Senior Research Officer in University of Essex, U.K. Currently he is a Senior Lecturer with Department of Computer and Information Sciences at Northumbria University, U.K. His research interests include wireless communications and machine learning.

Arumugam Nallanathan (S'97-M'00-SM'05-F'17) is Professor of Wireless Communications and Head of the Communication Systems Research (CSR) group in the School of Electronic Engineering and Computer Science at Queen Mary University of London since September 2017. He was with the Department of Informatics at Kings College London from December 2007 to August 2017, where he was Professor of Wireless Communications from April 2013 to August 2017 and a Visiting Professor from September 2017. He was an Assistant Professor in the Department of Electrical and Computer Engineering, National University of Singapore from August 2000 to December 2007. His research interests include Artificial Intelligence for Wireless Systems, Beyond 5G Wireless Networks, Internet of Things (IoT) and Molecular Communications. He published nearly 500 technical papers in scientific journals and international conferences. He is a co-recipient of the Best Paper Awards presented at the IEEE International Conference on Communications 2016 (ICC'2016) , IEEE Global Communications Conference 2017 (GLOBECOM'2017) and IEEE Vehicular Technology Conference 2018 (VTC'2018). He is an IEEE Distinguished Lecturer. He has been selected as a Web of Science Highly Cited Researcher in 2016.

He is an Editor for IEEE Transactions on Communications and Senior Editor for IEEE Wireless Communications Letters. He was an Editor for IEEE Transactions on Wireless Communications (2006-2011), IEEE Transactions on Vehicular Technology (2006-2017) and IEEE Signal Processing Letters. He served as the Chair for the Signal Processing and Communication Electronics Technical Committee of IEEE Communications Society and Technical Program Chair and member of Technical Program Committees in numerous IEEE conferences. He received the IEEE Communications Society SPCE outstanding service award 2012 and IEEE Communications Society RCC outstanding service award 2014.