Joint Precoding and Artificial Noise Design for MU-MIMO Wiretap Channels

Eunsung Choi, Graduate Student Member, IEEE, Mintaek Oh, Graduate Student Member, IEEE, Jinseok Choi, Member, IEEE, Jeonghun Park, Member, IEEE, Namyoon Lee, Senior Member, IEEE, and Naofal Al-Dhahir, Fellow, IEEE

Abstract—Secure precoding superimposed with artificial noise (AN) is a promising transmission technique to improve security by harnessing the superposition nature of the wireless medium. However, finding a jointly optimal precoding and AN structure is very challenging in downlink multi-user multiple-input multiple-output wiretap channels with multiple eavesdroppers. The major challenge in maximizing the secrecy rate arises from the non-convexity and non-smoothness of the rate function. Traditionally, an alternating optimization framework that identifies beamforming vectors and AN covariance matrix has been adopted; yet this alternating approach has limitations in maximizing the secrecy rate. In this paper, we put forth a novel secure precoding algorithm that jointly and simultaneously optimizes the beams and AN covariance matrix for maximizing the secrecy rate when a transmitter has either perfect or partial channel knowledge of eavesdroppers. To this end, we first establish an approximate secrecy rate in a smooth function. Then, we derive the first-order optimality condition in the form of the nonlinear eigenvalue problem (NEP). We present a computationally efficient algorithm to identify the principal eigenvector of the NEP as a suboptimal solution for secure precoding. Simulations demonstrate that the proposed methods improve secrecy rate significantly compared to the existing methods.

Index Terms—Physical layer security, secrecy rate, secure precoding, artificial noise (AN), joint and simultaneous optimization.

Manuscript received 30 June 2022; revised 29 October 2022; accepted 28 November 2022. Date of publication 7 December 2022; date of current version 17 March 2023. This work was supported in part by the National Research Foundation of Korea (NRF) grants funded by the Korea government (MSIT) (No. 2021R1C1C1004438 and (No. 2020R1C1C1013381) in part by the MSIT (Ministry of Science and ICT), Korea, under the Innovative Human Resource Development for Local Intellectualization support program (IITP-2022-00156361) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation). The work of Naofal Al-Dhahir was supported by Erik Jonsson Distinguished Professorship at UT-Dallas. The associate editor coordinating the review of this article and approving it for publication was W. Chen. (Corresponding author: Jinseok Choi.)

I. INTRODUCTION

AS THE amount of information delivered via wireless media grows rapidly, security in wireless communications has become an increasingly critical issue to protect confidential information from eavesdroppers. Cryptography has been used in traditional approaches to protect confidential information from eavesdropping [1]. Unfortunately, the key distribution and complicated encryption algorithms necessitate high implementation costs. Accordingly, systems with low-computing capability, for instance, internet-of-things (IoT) communication systems and sensor networks, are not capable of using the cryptography approach to prevent eavesdropping the signals transmitted by an access point (AP).

Compared to the cryptography approach, physical layer security has been flourishing due to its low computational complexity [2]. It has been demonstrated in [3] and [4] that a transmitter can reliably deliver confidential information to users with a positive rate while guaranteeing that an eavesdropper cannot decode the information if the wiretap channel quality is worse than the legitimate channel. Then, the secrecy rate is defined as this non-zero transmission rate. The importance of information security has become more significant with the rapidly increasing amount of transmitted information and highly diversified wireless applications. Accordingly, there have been many works to apply physical layer security for secrecy rate maximization in 6G applications. For instance, internet-of-things (IoT) systems, one of the primary 6G applications, are vulnerable to the wiretapping issue [5] and it is necessary to enhance security of the computation-limited IoT devices. Another possible application is a satellite communication scenario exposed to a risk of being attacked by terrestrial eavesdroppers [6], [7] which can be ground stations that were served by the same satellite. Lastly, wireless military communication links are highly recommended to apply both cryptography-based security and physical layer security as the protection of confidential information is significantly important [8]. In this sense, the low-complexity physical layer security communication algorithm can play a key role in guaranteeing wireless security in 6G communications. In physical layer security, there are two representative approaches which solve the secrecy rate maximization problem in multiple-input multiple-output (MIMO) systems: (i) secure precoding and (ii) artificial noise (AN) injection. In this paper, we investigate...
A secure precoding with AN design for physical layer security of downlink IoT networks and propose a joint optimization framework.

A. Prior Work

Starting with Wyner’s pioneering work [2], physical layer security has been studied in many scenarios including multiple access channels [3] and broadcast channels [4]. In particular, there have been extensive efforts to evaluate the secrecy rate of multiple antenna systems employing an information-theoretic approach. The secrecy rate was derived in [9] for single-input multiple-output (SIMO) channels in a slow fading environment. A single-antenna eavesdropper [10] and a multiple antennas eavesdropper [11] were also investigated to analyze the achievable secrecy rate in multiple-input single-output (MISO) channels. Furthermore, the secrecy rate was derived under a multiple-input multiple-output (MIMO) assumption in [12] and [13]. Specifically, the generalized singular-value decomposition was proposed in [12] to achieve the MIMO channels’ secrecy rate in the presence of a multi-antenna eavesdropper. Secure two-user MIMO broadcast channels were considered in [14], and secret dirty-paper coding (S-DPC) was proposed to achieve the secrecy rate region. In [15], it was also revealed that linear precoding can attain the same secrecy rate region as S-DPC. In [16], the achievable secrecy rates and linear precoding design in MIMO interference channels were investigated. In [17] and [18], the secrecy rate was investigated when multiple users and multiple eavesdroppers coexist.

There have been several prior works that proposed secure precoding method to maximize the secrecy rate. In [19], a secure beamforming approach was proposed to minimize the signal-to-interference-plus-noise-ratio (SINR) of eavesdroppers in a multi-user MIMO (MU-MIMO) system with a single eavesdropper overhearing information of a particular user. Assuming MIMO multi-eavesdropper (MIMOME) channels, robust beamforming methods were proposed in [20] and [21] where the channel state information (CSI) is imperfect. In [22], a successive convex approximation technique was introduced to relax the sum secrecy rate maximization problem. For wireless systems with multiple transmitter-receiver pairs and one eavesdropper, algorithms were proposed in [23] to maximize the secrecy rate and the secrecy energy efficiency. In [24], a secure antenna selection method was investigated to improve the secrecy performance without increasing computational complexity. To consider the secrecy rate and the secrecy energy efficiency together, massive MIMO systems [25], and simultaneous wireless information and power transfer systems [26] have been investigated. A comprehensive examination of physical layer security in multi-user systems was performed in [27]. In [28], the hybrid full- and half-duplex receiver deployment strategy was studied in a wireless ad hoc network with numerous legitimate transmitter-receiver pairs and eavesdroppers. Intelligent reflecting surface-aided communications [29] and cooperative jammer-assisted communications [30] were also investigated for maximizing secrecy rates as potential 6G communication systems.

The AN injection scheme is another representative approach for achieving secure communications in MIMO systems. In particular, AN design based on the null-space of the legitimate channel matrix is a well-known methodology for maximizing the sum secrecy rate [31], [32]. In [33], assuming that there is a single user and a single eavesdropper, the design of secure precoding and AN covariance was presented to maximize the secrecy rate. In [34], an AN-aided secrecy rate maximization method was proposed for the system with an intelligent reflecting surface. In [35], the secure precoder for the MISO scenario was found by solving the AN-aided secrecy rate maximization problem using the convex optimization toolbox, CVX. In [36], AN-aided transmit design for multi-user MISO systems was proposed to solve the secrecy rate region maximization problem. For the MIMO scenario, optimal transmit power allocation for precoder and AN was considered in [37]. The AN-aided scheme was also proposed in [25] where AN is injected into the downlink training signals to block the eavesdropper from obtaining CSIT of the correct wiretap link in the presence of a single-user and multiple eavesdroppers. The AN-aided secure beamforming approach for data transmission was investigated also for the single-user and multi-eavesdropper model in [38] and for the multi-group and multi-cast MU-MIMO model in [39]. Furthermore, the power ratio between the secure precoder and AN covariance matrix was optimized by using the alternating optimization approach. In [25] and [18], the secrecy rate maximization method was investigated with the secure precoder and fixed null-space AN by alternation-based power optimization. The power optimization between secure precoder and fixed null-space AN was performed by a one-dimensional line search for maximizing the secrecy rate in [35]. In [40], the proposed non-adaptive power allocation method was performed between a fixed zero-forcing (ZF) precoder and a fixed null-space AN. In [41], AN-aided secure communication design with the fixed ZF precoding method was researched by the proposed two-level optimization method.

Although physical layer security has been widely investigated, the existing secure precoding and AN injection approaches have the limited applicability for general downlink broadcasting wiretap channels as follows: (i) only a single legitimate user is assumed in the wiretap channel [33], [34], [35], [37], [38], (ii) only a single eavesdropper presents to overhear confidential messages [19], [25], [33], [34], [37], (iii) there are fixed pairs of an eavesdropper and legitimate user, i.e., each user has one designated eavesdropper [22], which is not a general wiretap channel where each eavesdropper is considered to overhear any legitimate user’s message, (iv) existing algorithms mostly require high computational complexity as in [25], [26], [35], [39], and [36], or (v) optimization of precoding and AN covariance is performed in an alternating manner [18], [25], [35], [40], [41], which is highly sub-optimal. Such limitations for physical layer security comes from the complicated nature of the optimization problem for AN-aided secure precoding; the sum rate maximization problem is a famous NP-hard problem even if there are only users in the network [42] and thus, solving a secure precoding problem for wiretap channels is more challenging. Furthermore, for the multiple eavesdropper case, the amount of information leakage is determined by the maximum rate of each wiretap channel [17] which causes the non-smoothness of the optimization problem. Finally, the design philosophies of
the precoder and AN covariance are disparate as the AN does not convey any information to legitimate users, which leads to alternation-based optimization for most AN-aided secure precoding methods. In this regard, it is necessary to develop a joint and simultaneous optimization framework of secure precoding and AN covariance design for general downlink broadcasting wiretap channels where multiple users and eavesdroppers coexist. Overcoming the aforementioned challenges, we propose a joint optimization framework without alternation for the system, i.e., joint and simultaneous optimization.

B. Contributions

In this paper, we propose a joint optimization framework for optimizing the secure precoder and AN covariance simultaneously in downlink systems where multiple legitimate users and multiple eavesdroppers coexist. In the considered system, a multi-antenna AP transmits confidential information symbols via linear precoding to single-antenna users. In addition, coexisting single-antenna eavesdroppers attempt to overhear the confidential information signals sent from the AP. In this setup, the AP employs both precoding and AN to maximize the sum secrecy rate. Here, we summarize our contributions.

- We adopt secrecy rate as our key performance measure. Using the secrecy rate, we formulate a sum secrecy rate maximization problem to jointly optimize (i) precoding matrix and (ii) an AN covariance matrix. There are key challenges in solving the formulated problem. First, the problem is non-convex and hence, finding the globally optimal solution is infeasible. Second, the sum secrecy rate is non-smooth since the secrecy rate is determined by the maximum wiretap channel rate of the eavesdroppers.

- To address these challenges, we first approximate the non-smooth objective function by a smooth form. Then, we reformulate the approximated problem into a tractable non-smooth objective function by a smooth form. Then, we propose a power iteration-based optimization algorithm to find the best stationary point. Accordingly, the proposed GPI-based optimization method jointly optimizes secure precoding, AN covariance, and the power ratio between the precoder and AN simultaneously.

- Through simulations, we validate the secrecy performance of the proposed joint and simultaneous optimization methods. We demonstrate that the proposed methods improve secrecy performance significantly in various system setups compared to the other baseline methods thanks to the joint optimization without alternation.

II. SYSTEM MODEL

In this section, we describe the considered downlink communication system. We focus on the scenario of multiple users in which an AP with $N$ antennas supports $K$ single-antenna users. In addition, $M$ single-antenna eavesdroppers coexist, attempting to overhear the private messages of the users. We let $K$ and $M$ denote the set of users and eavesdroppers, respectively. The AP precodes user symbols $s_k$, $k = 1, \ldots, K$, with a linear precoder $f_k$ and transmits the precoded signals along with an AN to enhance communication security as

$$x = Fs + \Phi z,$$

where $F = [f_1, \ldots, f_K] \in \mathbb{C}^{N \times K}$ is the precoding matrix, $s = [s_1, \ldots, s_K]^T$ is the vector of user symbols with $s \sim \mathcal{C}\mathcal{N}(0_{N \times 1}, P)$, and $\Phi z$ is the AN vector which follows $\Phi z \sim \mathcal{C}\mathcal{N}(0, P\Phi \Phi^H)$. Specifically, we utilize $J$ columns to design AN covariance matrix, i.e., $\Phi$ is a matrix of size $N \times J$. We assume $K \leq N$ and $J \leq N$ unless mentioned otherwise. Accordingly, the total transmit power constraint is given by

$$P \sum_{i=1}^K \|f_i\|^2 + P \sum_{j=1}^J \|\phi_j\|^2 \leq P,$$

where $\phi_j$ is the $j$-th column of $\Phi$ and $P$ is maximum transmit power constraint.

The legitimate channel vector from $k$-th user to the AP is denoted by $h_k \in \mathbb{C}^N$ for $k \in K$. The spatial covariance matrix $R_k \in \mathbb{C}^{N \times N}$ of the channel vector $h_k$ is defined as $R_k = E[h_k h_k^H]$. Similarly, the wiretap channel vector from the $m$-th eavesdropper to the AP is denoted by $g_m \in \mathbb{C}^N$ with the covariance of $R_m = E[g_m g_m^H]$. We first assume that perfect CSIT of the users and eavesdroppers are available at the AP. Then, we further consider the case of imperfect CSIT of eavesdroppers for a more practical scenario where only the channel covariance of eavesdroppers is available at the AP. The received signal at user $k$ is

$$y_k = h_k^H f_k s_k + \sum_{i=1, i \neq k}^K h_k^H f_i s_i + \sum_{j=1}^J h_k^H \phi_j z_j + n_k,$$

where $n_k \sim \mathcal{C}\mathcal{N}(0, \sigma^2_k)$ is additive white Gaussian noise (AWGN). Similarly, the received signal at eavesdropper $m$ is expressed as

$$y_m = \sum_{k=1}^K g_m^H h_k s_k + \sum_{j=1}^J g_m^H \phi_j z_j + n_m^e,$$

where $n_m^e \sim \mathcal{C}\mathcal{N}(0, \sigma^2_e)$ is the AWGN at the $m$-th eavesdropper.

In the following sections, we introduce a performance metrics and formulate a sum secrecy rate maximization problem. Then, we propose a novel optimization framework for joint and simultaneous precoding and AN covariance design.

III. PROBLEM FORMULATION

We assume that each user employs single user decoding treating the interference as noise. Consequently, the rate of user $k$ is given as

$$R_k = \log_2 \left(1 + \frac{|h_k^H f_k|^2}{\sum_{i=1, i \neq k}^K |h_i^H f_k|^2 + \sum_{j=1}^J |h_k^H \phi_j|^2 + \sigma^2/P} \right),$$

where $f_k$ is the $k$-th column of the precoding matrix $F$.
Similarly, the rate of the wiretap channel for the message $s_k$ achieved at eavesdropper $m$ is

$$R_{m,k}^e = \log_2 \left( 1 + \frac{|g_m^H f_k|^2 + \sum_{i=1, i \neq k}^K |g_m^H f_i|^2 + \sum_{j=1}^J |g_m^H \phi_j|^2 + \sigma_n^2}{P} \right).$$

(6)

The maximum wiretap channel rate determines the secrecy rate in the presence of multiple eavesdroppers [17], [24]. In this regard, we have $\max_{m \in \mathcal{M}} \{ R_{m,k}^e \}$ amount of rate loss from $R_k$ to transmit $s_k$ with guaranteed security, and the corresponding secrecy rate becomes

$$R_k = \log_2 \left( \bar{v}^H A_k \bar{v} \right).$$

(7)

Then, using the secrecy rate, we formulate a sum secrecy rate maximization problem as

$$\max_{\bar{F}, \bar{\Phi}} R_{\text{sum}} = \sum_{k=1}^K \left[ R_k - \max_{m \in \mathcal{M}} \{ R_{m,k}^e \} \right]^+ \quad \text{(8)}$$

subject to

$$\sum_{i=1}^K \| f_i \|^2 + \sum_{j=1}^J \| \phi_j \|^2 \leq 1, \quad \text{(9)}$$

where the constraint in (9) is the transmit power constraint.

We remark that to solve (8) a joint optimization of $\bar{F}$ and $\bar{\Phi}$ is necessary.

Unfortunately, the problem in (8) is significantly challenging due to non-smoothness and non-convexity. Even worse, the secure precoding vectors $f_k$ and the AN covariance vector $\phi_j$ are coupled which makes the optimization process intractable. In this regard, a null-space approach which fixes $\bar{\Phi}$ as the null-space projection matrix of the user channels was widely used [31], [32]. Furthermore, alternating power allocation strategies between the secure precoder and AN covariance matrix have been actively studied [18], [40]. Unlike such well-known optimization approaches, our key contribution is the joint optimization framework proposed in the next section that determines the secure precoder, AN covariance matrix, and power ratio between precoder and AN covariance matrix without any alternation.

### IV. Joint Optimization Framework

In this section, we solve the problem (8) by resolving the key challenges through approximation and reformulation of the problem, leading to a tractable form. Subsequently, we propose a joint and simultaneous optimization method for the secure precoding, AN covariance matrix design, and precoder-AN power allocation for the case of perfect CSIT. Then, we further extend the proposed framework to the case of imperfect CSIT of wiretap channels. We also introduce the application of the proposed framework to the null-space AN covariance design approach.

#### A. Joint and Simultaneous Optimization With Perfect CSIT

To cast the secrecy rate into a tractable form, we first define a joint optimization vector by stacking all the precoding vectors $f_k$ and AN covariance vectors $\phi_j$ as

$$\bar{v} = [f_1^T, \ldots, f_K^T, \phi_1^T, \ldots, \phi_J^T]^T \in \mathbb{C}^{N(K+J)}.$$  

(10)

We assume that the norm of (10) to be equal to one, i.e., $\| \bar{v} \| = 1$, which indicates transmission at maximum transmit power since it is the optimal transmission strategy in term of transmit power and rate. Using (10), we rewrite the legitimate channel rate $R_k$ in (5) as

$$R_k = \log_2 \left( \bar{v}^H A_k \bar{v} \right).$$

(11)
where
\[
\mathbf{A}_k = \text{blkdiag}(\mathbf{h}_k\mathbf{h}_k^H, \ldots, \mathbf{h}_k\mathbf{h}_k^H) + \mathbf{I}_{N(K+N)} \frac{\sigma^2}{P},
\]
and
\[
\mathbf{B}_k = \mathbf{A}_k - \text{blkdiag}(0, \ldots, \mathbf{h}_k\mathbf{h}_k^H, \ldots, 0).
\]

We note that \( \mathbf{A}_k \) and \( \mathbf{B}_k \) are block diagonal matrices with dimension of \( N(K + J) \times N(K + J) \). Similarly, we express the wiretap channel rate \( R_{m,k}^e \) in (6) as
\[
R_{m,k}^e = \log_2 \left( \frac{\mathbf{v}^H \mathbf{C}_{m,k} \mathbf{v}}{\mathbf{v}^H \mathbf{D}_{m,k} \mathbf{v}} \right),
\]
where
\[
\mathbf{C}_{m,k} = \text{blkdiag}(\mathbf{g}_m\mathbf{g}_m^H, \ldots, \mathbf{g}_m\mathbf{g}_m^H) + \mathbf{I}_{N(K+N)} \frac{\sigma^2}{P},
\]
and
\[
\mathbf{D}_{m,k} = \mathbf{C}_{m,k} - \text{blkdiag}(0, \ldots, \mathbf{g}_m\mathbf{g}_m^H, \ldots, 0).
\]

With (11) and (14), we reformulate the original problem (8) to
\[
\begin{align*}
\text{maximize} & \quad \sum_{k=1}^{K} \left\{ \log_2 \left( \frac{\mathbf{v}^H \mathbf{A}_k \mathbf{v}}{\mathbf{v}^H \mathbf{B}_k \mathbf{v}} \right) - \max_{m \in M} \log_2 \left( \frac{\mathbf{v}^H \mathbf{C}_{m,k} \mathbf{v}}{\mathbf{v}^H \mathbf{D}_{m,k} \mathbf{v}} \right) \right\} \\
\text{subject to:} & \quad \| \mathbf{v} \| = 1.
\end{align*}
\]

We remark that the reformulated problem in (17) is invariant up to the scaling of \( \mathbf{v} \), i.e., scaling of \( \mathbf{v} \) does not change the problem in (17). As a result, we can ignore the constraint of \( \| \mathbf{v} \| = 1 \) which has no effect on (17).

Next, we utilize the following LogSumExp function to approximate the non-smooth maximum function [43]:
\[
\max_{i=1, \ldots, N} \{ x_i \} \approx \alpha \log \left( \sum_{i=1}^{N} \exp \left( \frac{x_i}{\alpha} \right) \right), \quad \alpha > 0,
\]
where the approximation becomes tight as \( \alpha \to 0 \). Leveraging (18), we obtain the following approximation for the maximum wiretap channel rate:
\[
\max_{m \in M} \left\{ R_{m,k}^e \right\} \approx \alpha \log \left( \sum_{m=1}^{M} \exp \left( \frac{R_{m,k}^e}{\alpha} \right) \right).
\]

Applying (19) to (17), the sum secrecy rate \( R_{\text{sum}} \) is approximated as
\[
R_{\text{sum}} \approx \sum_{k=1}^{K} \left\{ \log_2 \left( \frac{\mathbf{v}^H \mathbf{A}_k \mathbf{v}}{\mathbf{v}^H \mathbf{B}_k \mathbf{v}} \right) - \alpha \log \left( \sum_{m=1}^{M} \exp \left( \frac{\mathbf{v}^H \mathbf{C}_{m,k} \mathbf{v}}{\mathbf{v}^H \mathbf{D}_{m,k} \mathbf{v}} \right) \right) \right\}.
\]

Finally, simplifying (20) further, the problem in (17) is reformulated as
\[
\begin{align*}
\text{maximize} & \quad \sum_{k=1}^{K} \left\{ \log_2 \left( \frac{\mathbf{v}^H \mathbf{A}_k \mathbf{v}}{\mathbf{v}^H \mathbf{B}_k \mathbf{v}} \right) - \alpha \log \left( \sum_{m=1}^{M} \left( \frac{\mathbf{v}^H \mathbf{C}_{m,k} \mathbf{v}}{\mathbf{v}^H \mathbf{D}_{m,k} \mathbf{v}} \right)^\beta \right) \right\},
\end{align*}
\]
where \( \beta = 1/(\alpha \log 2) \).

Now, we propose an optimization method that solves the problem in (21). To this end, we derive the first-order optimality condition of (21) in the following lemma:

Lemma 1: The first-order optimality condition of problem (21) is satisfied if the following condition holds:
\[
\mathbf{B}_k^{-1}(\bar{\mathbf{v}}) \mathbf{A}_k \mathbf{KKT}(\bar{\mathbf{v}}) \bar{\mathbf{v}} = \lambda(\bar{\mathbf{v}}) \bar{\mathbf{v}},
\]
where
\[
\lambda(\bar{\mathbf{v}}) = \lambda_{\text{num}}(\bar{\mathbf{v}})/\lambda_{\text{den}}(\bar{\mathbf{v}}),
\]
\[
\lambda_{\text{num}}(\bar{\mathbf{v}}) = \prod_{k=1}^{K} \left( \bar{\mathbf{v}}^H \mathbf{A}_k \bar{\mathbf{v}} \right),
\]
\[
\lambda_{\text{den}}(\bar{\mathbf{v}}) = \prod_{k=1}^{K} \left( \sum_{m=1}^{M} \left( \frac{\bar{\mathbf{v}}^H \mathbf{C}_{m,k} \bar{\mathbf{v}}}{\bar{\mathbf{v}}^H \mathbf{D}_{m,k} \bar{\mathbf{v}}} \right)^\alpha \right) \left( \bar{\mathbf{v}}^H \mathbf{B}_k \bar{\mathbf{v}} \right).
\]

Proof: See Appendix A.

The obtained first-order optimality condition in (22) can be interpreted as a general eigenvalue problem for the matrix \( \mathbf{B}_k^{-1}(\bar{\mathbf{v}}) \mathbf{A}_k \mathbf{KKT}(\bar{\mathbf{v}}) \). Accordingly, if \( \bar{\mathbf{v}} \) is a stationary point of the problem (21), it is an eigenvector of the matrix \( \mathbf{B}_k^{-1}(\bar{\mathbf{v}}) \mathbf{A}_k \mathbf{KKT}(\bar{\mathbf{v}}) \), where the corresponding eigenvalue is \( \lambda(\bar{\mathbf{v}}) \). We remark that the objective function in (21) is equivalent to \( \log_2 \lambda(\bar{\mathbf{v}}) \). This observation leads to the following fact: we need to find the leading eigenvector of \( \mathbf{B}_k^{-1}(\bar{\mathbf{v}}) \mathbf{A}_k \mathbf{KKT}(\bar{\mathbf{v}}) \) to maximize the objective function in (21), and then such a leading eigenvector is the best stationary point among all stationary points. We also remark that once finding the leading eigenvector, we simultaneously obtain the joint precoding and AN covariance solution with power allocation. The following proposition summarizes the insight:

Proposition 1: The best local optimal point for problem (21) is denoted by \( \bar{\mathbf{v}}^* \), where \( \bar{\mathbf{v}}^* \) is the leading eigenvector of \( \mathbf{B}_k^{-1}(\bar{\mathbf{v}}^*) \mathbf{A}_k \mathbf{KKT}(\bar{\mathbf{v}}^*) \) satisfying
\[
\mathbf{B}_k^{-1}(\bar{\mathbf{v}}^*) \mathbf{A}_k \mathbf{KKT}(\bar{\mathbf{v}}^*) \bar{\mathbf{v}}^* = \lambda^* \bar{\mathbf{v}}^*,
\]
and \( \lambda^* \) is the corresponding first (largest) eigenvalue.

To find the leading eigenvector, we adopt the generalized power iteration (GPI) method [42] which efficiently finds the vector in an iterative manner. In particular, during the \( t \)-th iteration, we update the vector in the current iteration as
\[
\bar{\mathbf{v}}_t \leftarrow \frac{\mathbf{B}_k^{-1}(\bar{\mathbf{v}}_{t-1}) \mathbf{A}_k \mathbf{KKT}(\bar{\mathbf{v}}_{t-1}) \bar{\mathbf{v}}_{t-1}}{\| \mathbf{B}_k^{-1}(\bar{\mathbf{v}}_{t-1}) \mathbf{A}_k \mathbf{KKT}(\bar{\mathbf{v}}_{t-1}) \bar{\mathbf{v}}_{t-1} \|}.
\]

Until the convergence criterion \( \| \bar{\mathbf{v}}_t - \bar{\mathbf{v}}_{t-1} \| < \epsilon_1 \) is met, we repeat (29). Algorithm 1 summarizes the GPI-based joint
and simultaneous precoding and AN covariance optimization method.

**Remark 1 (Multi-antenna user scenario):** The proposed algorithm can be naturally applied to a multi-antenna user scenario when receive beamforming at the users is fixed, considering the combined channels at the users as effective channel vectors. When the receive beamforming needs to be jointly optimized at every channel coherence time, a simple alternating approach can be used: compute the precoder and AN covariance matrix by using the proposed method with an initialized receive beamformer, then compute an MMSE receive beamformer with the obtained precoder and AN covariance, and repeat these steps until convergence. Since this is an alternating approach, we shall leave a joint and simultaneous optimization of precoding and AN covariance matrices and receive beamformer for the multi-antenna user case for future work.

### B. Joint and Simultaneous Optimization With Imperfect Wiretap CSIT

Now, we extend the proposed algorithm to the imperfect CSIT case of eavesdroppers in which only the channel covariances are known for wiretap channels at the AP. Since the perfect CSIT of the wiretap channel is not available at the AP, using the wiretap channel rate for each channel realization which is defined in (6) is no longer feasible. Consequently, we consider the wiretap channel rate as a perspective of an ergodic rate, i.e., we now use \( \mathbb{E}[R_{m,k}] \) instead of \( \bar{R}_{m,k} \) as our performance metric to utilize the wiretap channel covariance. Using the ergodic wiretap channel rate, we reformulate the optimization problem in (8) as

\[
\begin{align*}
\text{maximize} & \quad \sum_{k=1}^{K} \left[ R_k - \max_{m \in M} \left\{ \mathbb{E}[R_{m,k}] \right\} \right] \\
\text{subject to} & \quad \sum_{i=1}^{J} \| f_i \|^2 + \sum_{j=1}^{J} \| \phi_j \|^2 \leq 1.
\end{align*}
\]

To exploit the knowledge of the wiretap channel covariance, we need to properly handle \( \mathbb{E}[R_{m,k}] \). To this end, we approximate \( \mathbb{E}[R_{m,k}] \) as

\[
\mathbb{E}[R_{m,k}] = \mathbb{E} \left[ \log_2 \left( 1 + \frac{\left| g_{m,k}^H f_k \right|^2}{\sum_{i \neq k} \left| g_{m,ik}^H f_i \right|^2 + \sum_{j=1}^{J} \left| g_{m,j}^H \phi_j \right|^2 + \sigma_e^2 / P} \right) \right]
\]

(33)

\[
\approx \log_2 \left( 1 + \frac{\mathbb{E}[g_{m,k}^H f_k]}{\mathbb{E}[\sum_{i \neq k} |g_{m,ik}^H f_i|^2] + \mathbb{E}[\sum_{j=1}^{J} |g_{m,j}^H \phi_j|^2] + \sigma_e^2 / P} \right)
\]

(34)

\[
\approx \log_2 \left( 1 + \frac{f_{m,k}^H R_{m,k} f_k}{\sum_{i \neq k} f_{m,ik}^H R_{m,k} f_i + \sum_{j=1}^{J} \phi_j^H R_{m,k} \phi_j + \sigma_e^2 / P} \right)
\]

(35)

### Algorithm 1 Joint and Simultaneous GPI-Based Precoding (JS-GPIP)

1. initialize: \( \bar{v}_0 \)
2. Set the iteration count \( t = 1 \) and GPI threshold \( \epsilon_1 \).
3. while \( ||\bar{v}_t - \bar{v}_{t-1}|| > \epsilon_1 \) do
4. Create the matrices \( A_{\text{KKT}}(\bar{v}_{t-1}) \) and \( B_{\text{KKT}}(\bar{v}_{t-1}) \) by using (26) and (27), respectively.
5. Compute \( \bar{v}_t \leftarrow \frac{B_{\text{KKT}}(\bar{v}_{t-1})A_{\text{KKT}}(\bar{v}_{t-1})\bar{v}_{t-1}}{||B_{\text{KKT}}(\bar{v}_{t-1})A_{\text{KKT}}(\bar{v}_{t-1})\bar{v}_{t-1}||} \)
6. \( t \leftarrow t + 1 \).
7. \( \bar{v}^* \leftarrow \bar{v}_t \).
8. return \( \bar{v}^* \).

Now, following the similar steps as in Section IV-A, we derive the first-order optimality condition of the problem in (36). Let us define \( C_{m,k} \) and \( D_{m,k} \) as

\[
\begin{align*}
\bar{C}_{m,k} &= \text{blkdiag} \left( R_{m,k}^c, \ldots, R_{m,k}^c \right) + I_{N(K+J)} \frac{\sigma_e^2}{P}, \\
\bar{D}_{m,k} &= C_{m,k} - \text{blkdiag}(0, \ldots, R_{m,k}^c, \ldots, 0).
\end{align*}
\]

(36)

Then, the first order optimality condition in the form of the generalized eigenvalue problem is

**Lemma 2:** The first-order optimality condition of problem (36) is satisfied if the following condition holds:

\[
\begin{align*}
\bar{B}_{\text{KKT}}^{-1}(\bar{v}) \bar{A}_{\text{KKT}}(\bar{v}) \bar{v} &= \bar{\lambda}(\bar{v}) \bar{v},
\end{align*}
\]

(40)

where

\[
\bar{\lambda}(\bar{v}) = \lambda_{\text{num}}(\bar{v}) / \lambda_{\text{den}}(\bar{v}),
\]

(41)

\[
\lambda_{\text{den}}(\bar{v}) = \prod_{k=1}^{K} \left( \sum_{m=1}^{M} \left( \frac{\bar{v}^H \bar{C}_{m,k} \bar{v}}{\bar{v}^H \bar{D}_{m,k} \bar{v}} \right)^{\beta} \right)^{\alpha},
\]

(42)

\[
\bar{A}_{\text{KKT}}(\bar{v}) = \lambda_{\text{num}}(\bar{v}) \cdot \sum_{k=1}^{K} \left( \frac{1}{\log_2 \bar{v}^H \bar{A}_{k} \bar{v}} + \frac{\alpha \sum_{m} \beta \frac{\bar{v}^H \bar{C}_{m,k} \bar{v}}{\bar{v}^H \bar{D}_{m,k} \bar{v}}}{\sum_{m} \left( \frac{\bar{v}^H \bar{C}_{m,k} \bar{v}}{\bar{v}^H \bar{D}_{m,k} \bar{v}} \right)^{\beta}} \right),
\]

(43)

\[
\bar{B}_{\text{KKT}}(\bar{v}) = \bar{\lambda}_{\text{den}}(\bar{v}) \cdot \sum_{k=1}^{K} \left( \frac{1}{\log_2 \bar{v}^H \bar{B}_{k} \bar{v}} + \frac{\alpha \sum_{m} \beta \frac{\bar{v}^H \bar{C}_{m,k} \bar{v}}{\bar{v}^H \bar{D}_{m,k} \bar{v}}}{\sum_{m} \left( \frac{\bar{v}^H \bar{C}_{m,k} \bar{v}}{\bar{v}^H \bar{D}_{m,k} \bar{v}} \right)^{\beta}} \right),
\]

(44)

and \( A_k, B_k, \) and \( \lambda_{\text{num}}(\bar{v}) \) are defined in (12), (13), and (24), respectively.

Algorithm 1 can directly find the leading eigenvector of (40) by replacing \( A_{\text{KKT}} \) and \( B_{\text{KKT}} \) with \( A_k \) and \( B_k \), respectively. We call the algorithm as JS-GPIP (Cov) throughout this paper. Consequently, we can jointly and simultaneously design the secure precoder, AN covariance matrix, and precoder-AN.
power allocation when only the channel covariance is available for the wiretap channel.

Remark 2: (Secure GPI-based precoding) The proposed JS-GPI and JS-GPI (Cov) algorithms naturally reduce to a secure GPI-based precoding algorithm (S-GPI) without AN for the perfect wiretap CSIT and imperfect wiretap CSIT cases by enforcing $\Phi = 0$, i.e., $J = 0$, respectively.

C. Application to Null-Space Projection Approach

1) Alternating Approach: Although using null-space projection of AN covariance is not optimal, its design principle is greatly intuitive. In this regard, we also show the application of our framework to the null-space projection approach. We design $\Phi$ as the null-space of user channels, and $F$ as the proposed GPI-based secure precoder. Then we further need to perform power allocation between $\Phi$ and $F$ in an alternating manner. To this end, we employ a line search method by explicitly defining a power fraction factor $0 \leq \xi \leq 1$.

To begin with, we solve the optimization problem in (8) for the precoder with the given power fraction factor $\xi$ and AN covariance matrix that is designed as the null-space of the user channels. Let $\Phi = \sqrt{\xi} \Phi$ and $F = \sqrt{1 - \xi} F$, where $\Phi = [I - (H H^H)^{-1}]_{1:j}$ where $[\cdot]_{1:j}$ indicates using the first $J$ columns. Since we assume using maximum transmit power, we have the transmit power to be

$$\text{tr}((1 - \xi) \Phi F^H H) + \text{tr}(\xi \Phi F) = 1. \quad (45)$$

Equivalently, rewrite (45) as

$$\text{tr}\left(\frac{(1 - \xi)}{1 - \text{tr}(\xi \Phi F)} \Phi F^H H\right) = 1. \quad (46)$$

Now, we define $W$ as

$$W = \frac{1}{\sqrt{1 - \text{tr}(\xi \Phi F)}} F. \quad (47)$$

From (46) and (47), we have the power constraint to be $\text{tr}(W W^H) = 1$. Leveraging (47), we rewrite $R_k$ and $R_{m,k}$ as (48) and (49), as shown at the bottom of the page.

Similar to (19), we approximate the non-smooth maximum objective function by applying the LogSumExp function with $\bar{w} = \text{vec}(W)$. Then the problem (8) for given $\Phi$ is reformulated as

$$\max_{\bar{w}} \sum_{k=1}^{K} \left\{ \log_2 \left( \frac{w^H A^n_k \bar{w}}{w^H B^n_k \bar{w}} \right) - \alpha \log \left( \sum_{m=1}^{M} \frac{w^H C^n_{m,k} \bar{w}}{w^H D^n_{m,k} \bar{w}} \right) \right\}, \quad (50)$$

where

$$A^n_k = (1 - \text{tr}(\xi \Phi F)) \text{blkdiag}(h_k, h^H_k, \ldots, h_k, h^H_k)$$

$$B^n_k = (1 - \text{tr}(\xi \Phi F)) \text{blkdiag}(0, \ldots, h_k, h^H_k, \ldots, 0),$$

$$C^n_{m,k} = (1 - \text{tr}(\xi \Phi F)) \text{blkdiag}(g_m, g^H_m, \ldots, g_m, g^H_m)$$

$$D^n_{m,k} = (1 - \text{tr}(\xi \Phi F)) \text{blkdiag}(0, \ldots, g_m, g^H_m, \ldots, 0),$$

for $k = 1, \ldots, l$, and $m,k$ indicates using the $m$th block of $C^n_{m,k}$.

We also derive the first-order optimality condition of (50) in the following lemma:

Lemma 3: The first-order optimality condition of problem (50) is satisfied if the following condition holds:

$$B^{-1}_{\text{KKT}}(w) A_{\text{KKT}}(w) w = \lambda_{\text{num}}(w) \bar{w}, \quad (55)$$

where

$$\lambda_{\text{num}}(w) = \frac{\lambda_{\text{num}}(\bar{w})}{\lambda_{\text{den}}(w)}, \quad (56)$$

$$\lambda_{\text{den}}(w) = \prod_{k=1}^{K} \left( \frac{\bar{w}^H A^n_k \bar{w}}{\bar{w}^H D^n_{m,k} \bar{w}} \right)^{\alpha_k} \left( \frac{\bar{w}^H C^n_{m,k} \bar{w}}{\bar{w}^H D^n_{m,k} \bar{w}} \right)^{\beta_k}, \quad (57)$$

$$A_{\text{KKT}}(w) = \frac{\lambda_{\text{num}}(w)}{\lambda_{\text{den}}(w)}.$$
Subsequently, we can find the leading eigenvector of (55) by using the GPI method, and derive the precoder $F$ and AN pair with the highest performance. In this case, we initialize $K$ and $A$ by using (59), (60), and $\xi(0)$. We summarize the proposed joint GPI-based precoding with null-space AN approach (J-GPIP-NS) in Algorithm 2.

2) Low-Complexity (Non-Alternating) Approach: We note that J-GPIP-NS repeatedly computes GPI for each $\xi(i)$, which causes a high computational burden. To reduce computational complexity of J-GPIP-NS, we propose a low complexity version of the null-space projection based GPI method that computes the precoder by ignoring the AN and also compute the AN covariance matrix as the null-space projection matrix. Then, by defining a power fraction factor $\xi$ that offers the highest sum secrecy rate and use the corresponding pair of $F^*$ and $\Phi^*$. We summarize the proposed joint GPI-based precoding with null-space AN approach (J-GPIP-NS) in Algorithm 2.

Algorithm 2 Joint GPI-Based Precoding With Null-Space an (J-GPIP-NS)

1. initialize: $\bar{f}^{(0)} = \text{vec}(F^{(0)})$ and $\Phi = [I_N - (H(H^{H}H)^{-1})^{H}]_{1:1:J}$.
2. Set iteration counts $t = 1$ and $i = 1$, $\xi(0) = 0$, step size of power fraction factor $\Delta \xi$, and GPI threshold $\epsilon_2$.
3. while $\xi(i) \leq 1$ do
   4. Compute $\bar{\Phi}(i) = \sqrt{\xi(i)}\Phi$ and $\bar{w}(i) = \frac{1}{\sqrt{1-\text{tr}(\xi(i)\Phi\Phi^H)}}\bar{f}(i)$.
   5. while $\|\bar{w}(i) - \bar{w}(i-1)\| > \epsilon_2$ do
      6. Create the matrices $A_{KKT}^{\text{ns}}(\bar{w}(i))$ and $B_{KKT}^{\text{ns}}(\bar{w}(i))$ by using (59), (60), and $\xi(i)$.
      7. Compute $\bar{w}(i) \leftarrow \frac{B_{KKT}^{\text{ns}}(\bar{w}(i))A_{KKT}^{\text{ns}}(\bar{w}(i))\bar{w}(i)}{\|B_{KKT}^{\text{ns}}(\bar{w}(i))A_{KKT}^{\text{ns}}(\bar{w}(i))\bar{w}(i)\|}$.
      8. $t \leftarrow t + 1$.
   9. $\bar{f}(i) \leftarrow \bar{w}(i)\sqrt{1-\text{tr}(\xi(i)\Phi\Phi^H)}$.
   10. $\xi(i+1) \leftarrow \xi(i) + \Delta \xi$.
   11. $i \leftarrow i + 1$.
12. $[\bar{f}^*, \Phi^*] = \text{arg max}(\bar{f}(i), \Phi(i)) \sum_{k=1}^{K}\left[|R_k - \max_{m \in M}\{f_{m,k}\}|\right]$. return $F^*$ and $\Phi^*$.

Algorithm 3 J-GPIP-NS With Low Complexity

1. initialize: $f_0 = \text{vec}(F_0)$.
2. Set iteration counts $t = 1$ and $i = 1$, $\xi_L(0) = 0$, $\Delta \xi_L$, and $\epsilon_3$.
3. while $|\bar{f}_t - \bar{f}_{t-1}| > \epsilon_3$ do
   4. Create the matrices $A_{KKT}^{\text{ns}}(\bar{f}_t - \bar{f}_{t-1})$ and $B_{KKT}^{\text{ns}}(\bar{f}_t - \bar{f}_{t-1})$ by using (61) and (62).
   5. Compute $\bar{f}_t \leftarrow \frac{B_{KKT}^{\text{ns}}(\bar{f}_t - \bar{f}_{t-1})\bar{f}_t}{\|B_{KKT}^{\text{ns}}(\bar{f}_t - \bar{f}_{t-1})\|}$.
   6. $t \leftarrow t + 1$.
7. $\bar{f}^{(i)} = \frac{\sqrt{1 - \xi_L} \bar{f}_t}{\sqrt{1 - \xi_L}}$.
   8. $\Phi(i) = \sqrt{\xi_L} \Phi(i)$.
   9. $\xi_L \leftarrow \xi_L + \Delta \xi_L$.
   10. $i \leftarrow i + 1$.
11. $[\bar{f}^*, \Phi^*] = \text{arg max}(\bar{f}(i), \Phi(i)) \sum_{k=1}^{K}\left[|R_k - \max_{m \in M}\{f_{m,k}\}|\right]$. return $F^*$ and $\Phi^*$.

Algorithm 3 J-GPIP-NS With Low Complexity

The computational complexity of Algorithm 1 is dominated by the matrix inversion of $B_{KKT}(\bar{v})$. Generally, with Gauss–Jordan elimination, computational complexity for the inversion of a $N(K + J) \times N(K + J)$ is order of $O((N(K + J))^3)$. In our case, we can exploit the structure of $B_{KKT}(\bar{v})$ to reduce the complexity. In particular, since $B_{KKT}(\bar{v})$ is constructed based on a linear combination of block-diagonal and Hermitian matrices $B_k$ and $C_{m,k}$. $B_{KKT}(\bar{v})$ is also a block-diagonal and Hermitian matrix. Therefore, computing $B_{KKT}^{-1}(\bar{v})$ requires a total of $O\left(\frac{1}{2} \max(K, J)N^3\right)$ complexity [42]. Assuming that we have $T_1$ total iterations, the total complexity of Algorithm 1 is $O\left(\frac{1}{2}T_1 \max(K, J)N^3\right)$. Similarly, Algorithm 2 has a complexity of $O\left(\frac{1}{2}T_2 K N^3 L\right)$ when we assume that the power iteration per line search takes the similar number of iterations denoted as $T_2$ and consider $L$ to be the number of total line search with $NK \times NK$ block-diagonal Hermitian
matrix $B_{K	o T}^{ns}(\bar{w})$. With an assumption of $T_3$ iterations for the power iteration, Algorithm 3 has a total of $O\left(\frac{1}{3}T_3KN^3\right)$ complexity since the line searching method of Algorithm 3 does not increase the order of computational complexity. In particular, for $J \leq K$ and $T_1 \approx T_2 \approx T_3 = T$, JS-GPIP and J-GPIP-NS (Low) have the lowest complexity of $O\left(\frac{4}{3}TKN^3\right)$. Such a complexity order is same as a representative low-complexity framework in sum rate maximization (not secrecy rate), namely, the weighted minimum mean square error (MMSE) method [45]. In addition, the complexity order is also substantially small compared to the existing secure precoding methods. For instance, a two-stage optimization approach including solving a sequence of semi-definite programs (SDPs) was proposed with computational complexity order of $O\left(N^{6.5}\right)$ for a single confidential message and multicast message [36]. For visible light communications, a SDP-based algorithm was also developed for a single legitimate user and multiple eavesdroppers with computational complexity order of $O\left(N^{8.5}\right)$ [46]. As noted, the complexity of JS-GPIP is significantly lower than the state-of-the-art secure precoding algorithms.

V. NUMERICAL RESULTS

In this section, we evaluate the performance of the proposed algorithms under our secure precoding framework. In simulations, we employ the one-ring channel model in [47] for generating the small scale fading effects of the channels. Regarding the path-loss, we adopt the ITU-R model in [48] which models indoor non-line-of-sight path-loss environments. We use a distance power-loss coefficient as $3$ (equivalent to path-loss exponent of $3$), carrier frequency of $5$ GHz, $10$ MHz bandwidth (passband), $10 - 12$ dB lognormal shadowing variance, and $5$ dB noise figure are considered. We assume the noise power spectral density of legitimate users and eavesdroppers are the same as $-174$ dBm/Hz. Users are randomly generated around the AP with the maximum distance of $50$ m and minimum distance of $5$ m from the AP. Eavesdroppers are randomly distributed around random users with the maximum distance of $5$ m from the users to overhear the transmitted signal.

In the following cases, we evaluate the proposed algorithms and benchmarks, we evaluate the following cases:

- The proposed algorithms: JS-GPIP, JS-GPIP (Cov), J-GPIP-NS, J-GPIP-NS (Low), and S-GPIP. Recall that JS-GPIP (Cov) is the proposed JS-GPIP for the imperfect wiretap CSIT case and S-GPIP is the proposed JS-GPIP with $\Phi = 0$ as discussed in Remark 2.
- Benchmarks: (i) GPIP in [42], (ii) regularized zero-forcing (RZF), (iii) RZF with considering eavesdroppers in precoding design (RZF-EVE), and (iv) the applications of the benchmarks to the null-space AN projection approach: GPIP-NS, RZF-NS, RZF-EVE-NS, and maximum ratio transmission with null-space AN (MRT-NS).
- CVX-based methods (single user case): (i) CVX-based secrecy rate maximization (SRM-CVX) in [35] and (ii) CVX-based secrecy rate maximization with the successive convex approximation (SCA-CVX) in [49].

In particular, RZF-EVE-NS builds the $N \times K$ RZF precoder by including $K$ users and selecting $M_{\text{max}}$ eavesdroppers with the highest channel gains $\|g_m\|$ where $M_{\text{max}} = \min(N - K, M)$. The conventional linear precoders with NS extension adopt the line searching method to find the power ratio between precoder and null-space AN, which is similar to Algorithm 3.

We set $J = N$ throughout the simulations unless mentioned otherwise. We initialize the precoder of the proposed methods with ZF and the AN covariance matrix with the user channel null-space matrix.

A. Single-User Scenario

In Fig. 2, we evaluate the sum secrecy rate for (a) $N = 4$ AP antennas, $K = 1$ user, and $M = 3$ eavesdroppers with respect to transmit power $P$ and (b) $N = 4$ AP antennas, $K = 1$ user, and $P = 20$ dBm transmit power with respect to the number of eavesdroppers $M$. In Table II, we compare the average CPU time of the algorithms for the case of Fig. 2(a) measured at the workstation with i9-10900K CPU, RTX 3090 GPU, and 64GB RAM. We note that SRM-CVX uses a relaxation parameter. For fair comparison, we optimize both the relaxation parameter in SRM-CVX and the LogSumExp parameter $\alpha$ in our algorithms via online line searching. In particular, we employ the online line searching method only for Fig. 2.
TABLE II

AVERAGE MATLAB CPU TIME FOR $N = 4$, $K = 1$, $M = 3$

| Method          | CPU time (sec) | Comparison times |
|-----------------|----------------|------------------|
| JS-GPIP         | 0.0039         | 1                |
| J-GPIP-NS       | 1.1474         | 38.37            |
| SRM-CVX         | 2.1235         | 71.19            |
| SCA-CVX         | 27.8139        | 930.23           |

In the rest of the simulations, we use fixed empirical values of the LogSumExp relaxation parameter instead of the online line searching. As shown in Fig. 2(a) and Fig. 2(b), SCA-CVX, JS-GPIP, and SRM-CVX achieve similar sum secrecy rates. As the transmit power or the number of eavesdroppers increases, SCA-CVX provides marginal improvement from JS-GPIP. SCA-CVX, however, solves the sum secrecy rate maximization problem by using CVX for every iteration until it converges. Accordingly, SCA-CVX requires a very large computational burden and its average CPU time is $930.23 \times$ higher than that of the proposed JS-GPIP method as shown in Table II. In addition, SCA-CVX is applicable only for a single-user case. We also note that S-GPIP utilizes only the secure precoding method without AN, it achieves a lower secrecy performance compared to the AN-based methods such as JS-GPIP, J-GPIP-NS, SRM-CVX, SCA-CVX and MRT-NS. Therefore, Fig. 2 validates the performance and efficiency of JS-GPIP and demonstrates the benefit of using AN for physical layer security.

In Fig. 3, we plot the power ratio between the precoder and AN with respect to the transmit power for JS-GPIP and J-GPIP-NS obtained from the case in Fig. 2. The power ratio of the AN increases with the transmit power, and appears to converge in the high transmit power regime. As the transmit power increases, the users’ channel rate increases logarithmically which makes the performance gain marginal in the high transmit power regime. Therefore, JS-GPIP and J-GPIP-NS allocate more transmit power to the AN since focusing on the wiretap channel rate reduction is more efficient strategy once the precoder is allocated with enough power in the high transmit power regime. Although the J-GPIP-NS algorithm employs the line searching to optimize the power ratio, JS-GPIP and J-GPIP-NS illustrate similar behavior. In particular, JS-GPIP finds the precoder, the AN covariance matrix, and optimal power ratio simultaneously whereas the J-GPIP-NS attempts to find the power ratio by the line searching method for the fixed null-space AN. In this perspective, JS-GPIP finds a better solution to maximize the sum secrecy rate, thereby showing the higher rate than that of J-GPIP-NS. Furthermore, under the condition that the number of AP antennas and users are similar, the JS-GPIP algorithm allocates most of the transmit power to the precoder matrix since there are little spatial degrees-of-freedom to allocate power to the AN covariance matrix.

B. Multi-User Scenario

Unlike SRM-CVX and SCA-CVX which only work for a single-user case, the proposed algorithms work for a general number of users and eavesdroppers while maintaining its low computational complexity. In this regard, we further evaluate the proposed algorithms for multi-user cases. In Fig. 4, we evaluate the sum secrecy rate of the simulated algorithms with respect to the transmit power. We consider (a) $N = 8$
AP antennas, $K = 2$ users, and $M = 4$ eavesdroppers and (b) $N = 16$ AP antennas, $K = 2$ users, and $M = 4$ eavesdroppers. In comparison to the baseline methods, the proposed algorithms achieve the highest secrecy rate for both the cases of (a) and (b). Since JS-GPIP jointly optimizes both the precoder and AN covariance with perfect CSIT, it provides the highest rate. J-GPIP-NS which also uses perfect CSIT with alternating optimization of the precoder and AN covariance shows the second highest rate. JS-GPIP (Cov) follows J-GPIP-NS even with the partial wiretap CSIT followed by J-GPIP-NS (Low). Finally, S-GPIP shows the lowest rate among the proposed method even with perfect CSIT as it does not utilize the AN, yet achieving the higher rate than the benchmarks. In particular, the gap between the benchmarks and its NS extension demonstrates the efficiency of AN to improve secrecy rate performance. Accordingly, such a trend and performance order are intuitive and correspond to a general insight. In addition, the gap between GPIP and the proposed algorithms highlights the importance of the secure precoding approach.

In Fig. 5, we assess the sum secrecy rate of the proposed algorithms with the other baseline algorithms in terms of the number of AP antennas $N$. We consider the transmit power of $P = 20$ dBm, $K = 4$ users, and $M = 4$ eavesdroppers. In general, the algorithms exhibit similar performance order as in Fig. 4. In particular, the proposed JS-GPIP algorithm still achieves the highest secrecy rate. When the number of AP antennas is small, it is shown in Fig. 5 that GPIP-NS achieves a similar sum secrecy rate to that of JS-GPIP because there are not enough spatial degrees of freedom to nullify the leakage channels while keeping the user SINRs reasonable, and thus, focusing on maximizing sum rate becomes an effective approach in this regime. As the number of AP antennas increases, the performance gap between the baseline algorithms decreases; GPIP reduces to RZF with a large number of antennas as it does not consider secure precoding, which shows the importance of the joint secure optimization.

In Fig. 6, we evaluate the sum secrecy rate of the proposed algorithms with the other baseline algorithms in terms of the number of eavesdroppers $M$. We consider $N = 16$ AP antennas, $K = 4$ users, and $P = 20$ dBm transmit power. The proposed algorithms also achieve the highest secrecy rates. We note that the secrecy rate gap between AN-aided and non-AN-aided algorithms increases as the number of eavesdroppers increases. This behavior follows from the fact that the AN degrades the SINR of all eavesdroppers regardless of its number. Hence, the overall benefit of using AN becomes larger with the number of eavesdroppers. We also note that the rate of JS-GPIP (Cov) becomes similar to that of JS-GPIP, which indicates that with a large number of eavesdroppers, the covariance approximation becomes more accurate as mentioned in Lemma 1 in [44]. As a result, the proposed AN-aided joint secure precoding algorithms are considered to be a potential physical layer security algorithm as the number of eavesdroppers is expected to increase in the future wireless applications.

In Fig. 7, we assess the sum secrecy rate of the AN-aided algorithms in terms of $J$, i.e., the number of columns of $\Phi$, for $N = 16$ AP antennas, $K = 2$ users, and $M = 4$ eavesdroppers. Unlike the benchmarks, the proposed algorithm achieves their highest secrecy rates only with $J = 1$. This result indicates that the precoder of the proposed methods can well adapt to the AN for any dimension, thereby accomplishing high efficiency with only
$J = 1$ dimension. In other words, the proposed algorithms require small $J$ and thus, the total complexity of Algorithm 1 can reduce to $O \left( \frac{1}{3} TKN^3 \right)$ as discussed in Section IV-D.

In Fig. 8, we evaluate the convergence results in terms of the approximated objective function $L(\bar{v}) = \log_2 \lambda(\bar{v})$ in (69). Here, JS-GPIP converges within $T = 5$ iterations for $P \in \{0, 20, 40\}$ dBm transmit power and $T = 10$ iterations for $-20$ dBm transmit power. Therefore, with the small number of iteration $T$, the proposed algorithms reveal high potential in practical implementation. Overall, the proposed precoding and AN covariance design methods provide improvement in secrecy rate with low complexity, and wiretap channel covariance can be utilized and enough for achieving such an improvement.

We also compare the impact of $\alpha$ which affects the approximation accuracy. A sum secrecy rate versus a transmit power for $N = 8$ AP antennas, $K = 4$ users, $M = 4$ eavesdroppers, and $P \in \{-20, 0, 20, 40\}$ dBm transmit power.

Now, we evaluate the proposed algorithm with the PF policy for $N = 8$ AP antennas, $K \in \{2, 4\}$ users, and $M = 4$ eavesdroppers. In Fig. 9, we note that for $\alpha \in \{0.1, 0.5, 1\}$ the proposed algorithms achieve similar secrecy rate performance, which validates the effectiveness of the approximation and the robustness of the proposed algorithms to $\alpha$.

### C. Extension to Proportional Fairness

Regarding fairness over users, we can enforce long-term fairness with the proposed precoding method by employing the proportional fairness (PF) policy [50]. To adopt the PF policy, we reformulate the objective function as

$$
\sum_{k=1}^{K} [R_k(t) - R^*_{k}(t)]^+ / \mu_k(t),
$$

where $\mu_k(t)$ represents the average served secrecy rate for user $k$. We update $\mu_k(t)$ by a first-order autoregressive filter as [50]

$$
\mu_k(t + 1) = (1 - \delta)\mu_k(t) + \delta[R_k(t) - R^*_{k}(t)]^+
$$

where $\delta \in (0, 1)$ is a rate parameter of the filter. Subsequently, we introduce a threshold-based user selection by leveraging the relative transmit power of each user:

$$
||f^*_k||^2 / \max_i ||f^*_i||^2 < \tau,
$$

where $f^*_k$ denotes the optimized precoding vector of user $k$. By applying (68), users with relative transmit power less than $\tau$ are not scheduled. Thus, at each scheduling interval $t$, the AP keeps track of the average served secrecy rate $\mu_k(t)$ for every user $k$ and selects the user with the highest ratio of the current secrecy rate to the average served secrecy rate. In this manner, users can obtain a fair opportunity to be served, and the precoder and AN covariance matrix can be designed based on the weighted sum secrecy rate in (66) to incorporate the fairness issue. The proposed optimization method can be readily applied to the weighted sum secrecy problem in (66). Here, we omit the derivation as it can be directly derived by following the similar steps in the proof of Proposition 1. The overall steps of the proposed algorithm with the PF policy are summarized as

1) Perform Algorithm 1 by deriving $A_{KKT}$ and $B_{KKT}$ for the PF problem in (66).
2) Schedule users based on the power thresholding in (68).
3) Update $\mu_k(t)$ according (67) by using the result of Step 1 and Step 2.
4) Repeat Step 1 to Step 3.

Now, we evaluate the proposed algorithm with the PF policy (JS-GPIP-PF) through simulations. In our simulations, users are randomly generated around the AP with the maximum distance of $50m$ and minimum distance of $5m$ from the AP. Eavesdroppers are randomly distributed around random users with a maximum distance of $5m$ from the users to overhear the transmitted signal. Once we generate user locations for large-scale fading, we randomly change the small-scale fading of users to generate 1,000 different channels without changing the large-scale fading. We consider $N = 8$ AP antennas, $K = 8$ users and $M = 2$ eavesdroppers per user drop, $30$ dBm transmit power, $\tau = 0.1$, and $\delta = 0.2$. Fig. 10 shows the empirical cumulative distribution function (CDF) for the average secrecy rate of users for 50 user drops (50 large-scale fading realizations). JS-GPIP-PF shows a steeper curve than JS-GPIP, JS-GPIP (Cov), and GPI while achieving a higher rate than RZF and MRT. Therefore, the proposed algorithm with the PF policy achieves a better trade-off between the sum rate and fairness than the other methods.
satisfy smooth optimization problem. Then, we derived the first-order condition, we proposed the secure precoding method with null-space projection-algorithms that jointly and simultaneously identify both the beams and AN covariance matrix to maximize the sum secrecy rate when perfect or imperfect channel knowledge is available at the legitimate transmitter. As a byproduct, we also proposed a secure precoding method with null-space projection-based AN design. One key observation was that by jointly and simultaneously optimizing the precoder, AN covariance, and the precoder-AN power allocation, the proposed method achieved a higher secrecy rate performance than the existing methods with the need for only a small AN subspace and with fast convergence. Therefore, the proposed methods under the joint and simultaneous optimization framework can offer significantly improved security for future wireless applications. Potential future research directions include investigating the joint AN-aided secure beamforming by considering short-term fairness and expanding our investigation to a multi-antenna user scenario. Regarding different networks, considering the multi-beam satellite security scenario would be a promising future work by leveraging the channel property that is different from the terrestrial networks.

VI. CONCLUSION

In this paper, we presented a novel precoding algorithm that maximizes the sum secrecy rate for MU-MIMO wiretap channels with multiple eavesdroppers. Our key approach was to reformulate the non-convex and non-smooth secrecy rate maximization problem into a tractable non-convex and smooth optimization problem. Then, we derived the first-order optimality condition for the reformulated problem. Leveraging this first-order condition, we proposed the secure precoding algorithms that jointly and simultaneously identify both the beams and AN covariance matrix to maximize the sum secrecy rate when perfect or imperfect channel knowledge is available at the legitimate transmitter. As a byproduct, we also proposed a secure precoding method with null-space projection-based AN design. One key observation was that by jointly and simultaneously optimizing the precoder, AN covariance, and the precoder-AN power allocation, the proposed method achieved a higher secrecy rate performance than the existing methods with the need for only a small AN subspace and with fast convergence. Therefore, the proposed methods under the joint and simultaneous optimization framework can offer significantly improved security for future wireless applications. Potential future research directions include investigating the joint AN-aided secure beamforming by considering short-term fairness and expanding our investigation to a multi-antenna user scenario. Regarding different networks, considering the multi-beam satellite security scenario would be a promising future work by leveraging the channel property that is different from the terrestrial networks.

APPENDIX A PROOF OF LEMMA 1

The Lagrangian function of problem (17) is

\[ L(\bar{v}) = \sum_{k=1}^{K} \left\{ \log_2 \left( \frac{\bar{v}^H A_k \bar{v}}{\bar{v}^H B_k \bar{v}} \right) - \alpha \log \left( \sum_{m=1}^{M} \left( \frac{\bar{v}^H C_{m,k} \bar{v}}{\bar{v}^H D_{m,k} \bar{v}} \right)^\beta \right) \right\} \]

By the first-order KKT condition, a stationary point should satisfy \( \frac{\partial L(\bar{v})}{\partial \bar{v}} = 0 \). To find the condition, we take the partial derivatives of \( L(\bar{v}) \) with respect to \( \bar{v} \) and set it to zero. For simplicity, we let

\[ L_1(\bar{v}) = \sum_{k=1}^{K} \log_2 \left( \frac{\bar{v}^H A_k \bar{v}}{\bar{v}^H B_k \bar{v}} \right) \quad (70) \]

and

\[ L_2(\bar{v}) = -\sum_{k=1}^{K} \alpha \log \left( \sum_{m=1}^{M} \left( \frac{\bar{v}^H C_{m,k} \bar{v}}{\bar{v}^H D_{m,k} \bar{v}} \right)^\beta \right). \quad (71) \]

Then by using

\[ \frac{\partial}{\partial \bar{v}} \left( \frac{\bar{v}^H A_k \bar{v}}{\bar{v}^H B_k \bar{v}} \right) = \left( \frac{A_k \bar{v}}{\bar{v}^H B_k \bar{v}} \right) - \frac{B_k \bar{v}}{\bar{v}^H B_k \bar{v}}, \]

the partial derivative of \( L_1(\bar{v}) \) is obtained as

\[ \frac{\partial L_1(\bar{v})}{\partial \bar{v}} = \sum_{k=1}^{K} 1 \log_2 \left( \frac{A_k \bar{v}}{\bar{v}^H B_k \bar{v}} \right) - \frac{B_k \bar{v}}{\bar{v}^H B_k \bar{v}}. \quad (73) \]

Similarly, we calculate the partial derivative of \( L_2(\bar{v}) \) as

\[ \frac{\partial L_2(\bar{v})}{\partial \bar{v}} = \sum_{k=1}^{K} \alpha \sum_{m=1}^{M} \beta \left( \frac{C_{m,k} \bar{v}}{\bar{v}^H D_{m,k} \bar{v}} \right)^\beta \left( \frac{D_{m,k} \bar{v}}{\bar{v}^H B_k \bar{v}} \right) - \sum_{m=1}^{M} \left( \frac{C_{m,k} \bar{v}}{\bar{v}^H D_{m,k} \bar{v}} \right)^\beta \left( \frac{D_{m,k} \bar{v}}{\bar{v}^H B_k \bar{v}} \right). \]

Using (73) and (74) and rearrange the equations we obtain the following first order KKT condition:

\[ \sum_{k=1}^{K} \left( \frac{1}{\log_2 \left( \frac{A_k \bar{v}}{\bar{v}^H B_k \bar{v}} \right)} + \alpha \sum_{m=1}^{M} \beta \left( \frac{C_{m,k} \bar{v}}{\bar{v}^H D_{m,k} \bar{v}} \right)^\beta \left( \frac{D_{m,k} \bar{v}}{\bar{v}^H B_k \bar{v}} \right) \right) \bar{v} = \sum_{k=1}^{K} \left( \frac{1}{\log_2 \left( \frac{B_k \bar{v}}{\bar{v}^H B_k \bar{v}} \right)} + \alpha \sum_{m=1}^{M} \beta \left( \frac{C_{m,k} \bar{v}}{\bar{v}^H D_{m,k} \bar{v}} \right)^\beta \left( \frac{D_{m,k} \bar{v}}{\bar{v}^H B_k \bar{v}} \right) \right) \bar{v}. \]

Finally, we further rearrange (75) and derive

\[ A_{\text{KKT}}(\bar{v}) \bar{v} = \lambda(\bar{v}) B_{\text{KKT}}(\bar{v}) \bar{v}. \]

Since \( B_{\text{KKT}} \) is Hermitian, (76) can be cast to (22) in Lemma 1. This completes the proof.

REFERENCES

[1] J. L. Massey, “An introduction to contemporary cryptology,” Proc. IEEE, vol. 76, no. 5, pp. 533–549, May 1988.
[2] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, May 1975.
[3] Y. Liang and H. V. Poor, “Multiple-access channels with confidential messages,” IEEE Trans. Inf. Theory, vol. 54, no. 3, pp. 976–1002, Mar. 2008.
[4] A. Khisti, A. Tchamkerten, and G. W. Wornell, “Secure broadcasting over fading channels,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.
[5] S. A. Haider, M. N. Adil, and M. Zhao, “Optimization of secure wireless communications for IoT networks in the presence of eavesdroppers,” Comput. Commun., vol. 154, pp. 119–128, Mar. 2020.
[6] M. G. Schraml, R. T. Schwarz, and A. Knopp, “Multiuser MIMO concept for physical layer security in multibeam satellite systems,” IEEE Trans. Inf. Forensics Security, vol. 16, pp. 1670–1680, 2021.
Eunsung Choi (Graduate Student Member, IEEE) received the B.S. degree from the Department of Electrical Engineering, Ulsan National Institute of Science and Technology (UNIST), Ulsan, South Korea, in 2022, where he is currently pursuing the M.S. degree under supervision of Prof. Jinseok Choi. His main research interests include developing future wireless communication systems by applying information theory, optimization, and machine learning.

Mintaek Oh (Graduate Student Member, IEEE) received the B.S. degree from the Department of Electronics Engineering, Jeonbuk National University, Jeonju, South Korea, in 2021. He is currently pursuing the M.S. degree with the Department of Electrical Engineering, Ulsan National Institute of Science and Technology (UNIST), under supervision of Prof. Jinseok Choi. His research interests include developing advanced wireless communications, the Internet of Things communications, and machine learning.

Jinseok Choi (Member, IEEE) received the B.S. degree from the Department of Electrical and Electronic Engineering, Yonsei University, Seoul, South Korea, in 2014, and the M.S. and Ph.D. degrees in electrical and computer engineering from The University of Texas at Austin, Austin, TX, USA, in 2016 and 2019, respectively. He was a Student Member of the Wireless Networking and Communications Group (WNCG) and was working at the Embedded Signal Processing Laboratory under supervision of Prof. Brian L. Evans. He was a Senior System Engineer at Wireless Research and Development, Qualcomm Inc., San Diego, CA, USA. He is currently an Assistant Professor at the Ulsan National Institute of Science and Technology (UNIST). His research interests include developing and analyzing future wireless communication systems and to develop algorithms for intelligent devices that require ultra high-speed, high-reliability, and low-latency communications.

Jeonghun Park (Member, IEEE) received the B.S. and M.S. degrees in electrical and electronic engineering from Yonsei University, Seoul, South Korea, in 2010 and 2012, respectively, and the Ph.D. degree in electrical and computer engineering from The University of Texas at Austin, Austin, TX, USA, in 2017. He is currently working as an Assistant Professor with the School of Electronics Engineering, Kyungpook National University (KNU), Daegu, South Korea. Prior to joining KNU, he worked with Qualcomm Wireless Research and Development, San Diego, CA, USA. His main research interests include developing and analyzing future wireless communication systems using tools of optimization, information theory, and machine learning.

Naoyoshi Lee (Senior Member, IEEE) received the Ph.D. degree from The University of Texas at Austin in 2014. He was with the Communications and Network Research Group, Samsung Advanced Institute of Technology, South Korea, from 2008 to 2011, and also with the Wireless Communications Research, Intel Labs, Santa Clara, CA, USA, from 2015 to 2016. He is currently an Associate Professor at Korea University. His main research interests include communications, sensing, and machine learning. He was a recipient of the 2016 IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award, the 2020 IEEE Best YP Award (Outstanding Nominee), the 2021 IEEE-IEEE Joint Award for Young Engineer and Scientist, and the 2021 Headong Young Researcher Award. Since 2021, he has been an Associate Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COMMUNICATIONS, and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.

Naofal Al-Dhahir (Fellow, IEEE) received the Ph.D. degree from Stanford University. He was a Principal Member of Technical Staff at the GE Research Center and AT&T Shannon Laboratory from 1994 to 2003. He is currently an Erik Jonsson Distinguished Professor and the ECE Associate Head at UT-Dallas. He is a co-inventor of 43 issued patents and the coauthor of about 520 papers. He is an AAIA Fellow. He is a fellow of the U.S. National Academy of Inventors and a member of the European Academy of Sciences and Arts. He was a co-recipient of five IEEE best paper awards. He received the 2019 IEEE COMSOC SPCC Technical Recognition Award, the 2021 Qualcomm Faculty Award, and the 2022 IEEE COMSOC RCC Technical Recognition Award. He served as the Editor-in-Chief for IEEE TRANSACTIONS ON COMMUNICATIONS from January 2016 to December 2019.