Secrecy Precoder Design for k-User MIMO Interference Channels

Bing Fang[1(✉)] and Wei Shao[2]

[1] Army Command College of PLA, Nanjing, China
bingfang_ch@163.com
[2] Army Engineering University of PLA, Nanjing, China
swlxssz@126.com

Abstract. In this paper, we have studied the secrecy precoder design problem for a k-user multiple-input multiple-output (MIMO) interference channel (IFC), where an external eavesdropper intends to wiretap one of the legitimate wireless links. By adopting the "maxmin" fairness criteria, we define the secure precoding problem as an achievable secrecy-rate maximization problem, which is inherent nonconvex and pretty hard to deal with. To tackle the inherent complexity, we recast the original nonconvex problem into a difference-of-convex (DC) programming problem through a series of equivalent transformations. Based on these endeavors, a coordinated iterative precoding algorithm is designed to solve the achievable secrecy rate maximization problem within the framework of successive convex approximation (SCA) method. The basic idea of the proposed SCA method consists in recasting the DC-programming problem into a series of convexified subproblems, where the nonconvex parts of it are linearized to their first-order Taylor expansion. Moreover, in order to ensure the convergence of the proposed iterative algorithm, a regularization method based on the proximal point idea is also employed. Numerical simulations further show that our algorithm can achieve a satisfactory performance on the premise of ensuring convergence.

Keywords: MIMO precoding · Interference channel · Physical layer security · Successive convex approximation

1 Introduction

From a mathematical point of view, many real communication scenarios can be modeled as the interference channels (IFCs), where multiple uncoordinated communication links share the same radio spectrum at the same time. With multiple-input multiple-output (MIMO) having become a key technology for the

This work was supported by the State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System (CEMEE) Open Foundation of China (grant CEMEE2019Z0202B) and the Jiangsu Provincial Natural Science Foundation of China (grant BK20160080).

H. Gao et al. (Eds.): ChinaCom 2019, LNICST 312, pp. 564–575, 2020.
https://doi.org/10.1007/978-3-030-41114-5_42

fifth-generation mobile networks, i.e., 5G, the researches concerned on MIMO IFCs have gained considerable attention, refer to [1–4] and their references. On the other hand, there are also extensive interests in utilizing the extra benefits, i.e, the spatial degree-of-freedom (DoF), provided by MIMO technology to enhance the secrecy capabilities of pervasive wireless communication [5–7]. Naturally, it has become a critical issue to model and analyze physical layer security (PLS) performance for the MIMO IFCs [8,9].

In this work, we center on the design problem of secure precoding for a k-user MIMO IFC, where an external eavesdropper aims to wiretap one of the k legitimate wireless links. Here, we assume that the k legitimate transmitters simultaneously transmit independent messages to their corresponding receivers, while attempting to remain confidential to the external eavesdropper. In this setup, it is further assumed that all the transmitters, the receivers and the external eavesdropper are equipped with multiple antennas. Hence, our problem setup naturally constitutes a MIMO interference wiretap channel. By adopting the "maxmin" fairness criteria, the secrecy precoder design problem is defined as an achievable secrecy rate maximization problem, which subjects to individual transmit power budget allocated for each transmitter. However, the proposed problem is non-smooth and nonconvex and pretty hard to deal with.

To tackle the inherent complexity, we first resort to the epigraph optimization technique and equivalently relax the formulated problem to a smooth problem. Then, we recast the original nonconvex problem into a DC programming problem by a series of equivalent mathematical transformations. Based on these endeavors, a coordinated iterative precoding algorithm is designed to solve the achievable secrecy rate maximization problem within the framework of successive convex approximation (SCA) method [10,11]. The basic idea of the proposed SCA method is recasting the DC-programming problem into a sequence of convexified subproblems, where the nonconvex parts of it are linearized to their first-order Taylor expansion. Moreover, in order to ensure the convergence of the proposed iterative algorithm, a regularization method based on the proximal point thought is also employed here. Numerical simulations further show that our algorithm can achieve a satisfactory performance on the premise of ensuring convergence.

Notations: Bold uppercase letters denote matrices and bold lowercase letters denote vectors; $\mathbb{C}^{m\times n}$ defines the space of all $m \times n$ complex matrices; $\boldsymbol{A} \succeq 0$ means that the matrix $\boldsymbol{A}$ is positive semidefinite; Hermitian transpose of matrix $\boldsymbol{A}$ is represented as $\boldsymbol{A}^H$; inverse of matrix $\boldsymbol{A}$ is represented as $\boldsymbol{A}^{-1}$; determinant of matrix $\boldsymbol{A}$ is denoted as $|\boldsymbol{A}|$; trace of matrix $\boldsymbol{A}$ is denoted as $\mathrm{Tr}(\boldsymbol{A})$; and $\log(\cdot)$ denotes the natural logarithm.

2 System Model and Problem Formulation

This work studies the design problem of secure precoding for a k-user MIMO IFC. The system considered here is composed of k legitimate wireless links (Alice-to-Bob) and an external eavesdropper (Eve). As presented in Fig. 1, Alice, Bob, and Eve are all mounted with multiple antennas. We assume that each transmitter (Alice) aims to communicate confidential messages with its corresponding receiver (Bob), respectively, in the presence of an external eavesdropper (Eve), and further assume that Bob i only interests in the message sent by Alice i. However, Eve may have a general interest to wiretap the message transmitted by every one of the k transmitters. It is further assumed that all transmitters have N_t antennas, all receivers have N_r antennas, and Eve is enabled with N_e antennas.

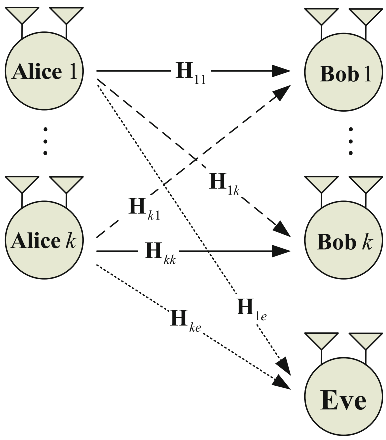

Fig. 1. System model of a k-user MIMO interference wiretap channel.

Here, it is assumed that a quasi-static frequency-flat fading communication environment for all wireless transmit links. The vector-valued signal received by Bob i is given as

$$\boldsymbol{y}_i = \sum_{j=1}^{k} \boldsymbol{H}_{ji}\boldsymbol{x}_j + \boldsymbol{n}_i, \forall i \in \mathcal{K}, \tag{1}$$

where $\boldsymbol{x}_j \in \mathbb{C}^{N_t \times 1}$ is the signal vector transmitted by Alice j, $\boldsymbol{H}_{ji} \in \mathbb{C}^{N_r \times N_t}$ denotes the complex channel matrix from Alice j to Bob i, $\boldsymbol{n}_i \in \mathbb{C}^{N_r \times 1}$ is additive Gaussian noise vector received by Bob i, and the user set $\mathcal{K}$ is defined as $\mathcal{K} = \{1, 2, \cdots, k\}$.

Then, the achievable data rate of the ith legitimate wireless link can be given in the following formula

$$R_i^b(\boldsymbol{Q}) = \log\left|\boldsymbol{I} + \boldsymbol{H}_{ii}^H \boldsymbol{Z}_i^{-1} \boldsymbol{H}_{ii}\boldsymbol{Q}_i\right|, \forall i \in \mathcal{K}, \tag{2}$$

where $\boldsymbol{Q}_i$ is the transmit covariance matrix, i.e., the precoding matrix, of Alice i, and $\boldsymbol{Q}$ denotes the profile of precoding matrix of all transmitters, which is framed as $\boldsymbol{Q} = \{\boldsymbol{Q}_i\}_{i=1}^k$. $\boldsymbol{Z}_i$ is the covariance matrix of the additive noise plus all interference received by Bob i, which is defined in the following formula

$$\boldsymbol{Z}_i = \sum_{j \neq i}^{k} \boldsymbol{H}_{ji}\boldsymbol{Q}_j\boldsymbol{H}_{ji}^H + \boldsymbol{N}_i, \forall i \in \mathcal{K}, \tag{3}$$

where $\boldsymbol{N}_i$ is the covariance matrix of additive noise vector received by Bob i.

On the other hand, the vector-valued signal received by Eve can be written in the following formula

$$\boldsymbol{y}_e = \sum_{j=1}^{k} \boldsymbol{H}_{je}\boldsymbol{x}_j + \boldsymbol{n}_e, \tag{4}$$

where $\boldsymbol{x}_j \in \mathbb{C}^{N_t \times 1}$ is the signal vector transmitted by Alice j, $\boldsymbol{H}_{je} \in \mathbb{C}^{N_e \times N_t}$ denotes the complex channel matrix from Alice j to Eve, and $\boldsymbol{n}_e \in \mathbb{C}^{N_e \times 1}$ is additive Gaussian noise vector received by Eve.

Then, the achievable data rate of the ith Alice-to-Eve wiretap link can be given as

$$R_i^e(\boldsymbol{Q}) = \log\left|\boldsymbol{I} + \boldsymbol{H}_{ie}^H\boldsymbol{N}_e^{-1}\boldsymbol{H}_{ie}\boldsymbol{Q}_i\right|, \forall i \in \mathcal{K}, \tag{5}$$

where $\boldsymbol{N}_e$ is the covariance matrix of the additive noise vector received by Eve. Note that, we consider a worst-case scenario here, that the external eavesdropper can remove all multiuser interference by using the successive interference cancelation (SIC) technique.

Therefore, the achievable secrecy data rate of the ith legitimate wireless link can be given as

$$R_i^s(\boldsymbol{Q}) = [R_i^b(\boldsymbol{Q}) - R_i^e(\boldsymbol{Q})]^+, \tag{6}$$

where $[\cdot]^+$ denotes the Euclidean projection onto $\mathbb{R}^+$. With the "maxmin" fairness criteria being adopted, the achievable secrecy rate maximization problem for the proposed MIMO IFC system can be formally formulated as

$$\begin{aligned} (\text{P1}): \ & \max_{\boldsymbol{Q}} \ \min_{i} \ R_i^s(\boldsymbol{Q}) \\ & s.t. \ \text{Tr}(\boldsymbol{Q}_i) \leq \text{P}_i, \boldsymbol{Q}_i \succeq 0, \forall i \in \mathcal{K}, \end{aligned} \tag{7}$$

where P_i denotes the maximum transmit power budget allocated for Alice i.

Note that, problem (P1) is non-smooth and of notoriously nonconvex complexity, which is pretty hard to solve directly. As shown in the next section, such a problem can be reformulated as a DC programming problem, through some equivalent mathematical transformation, which can be iteratively solved by employing the famous SCA method.

3 Coordinated Iterative Precoding Algorithm

In this section, a coordinated iterative precoding algorithm is designed within the framework of the SCA method. Moreover, a regularization method based on the proximal point idea is also pursued to ensure the convergence of the proposed algorithm.

3.1 Algorithm Design

By introducing a slack variable, i.e., $t > 0$, problem (P1) can be equivalently reformulated as the following epigraph optimization problem [12]

$$\begin{aligned} \text{(P2)}: \ & \max_{\boldsymbol{Q},t} t \\ & s.t. \ R_i^b(\boldsymbol{Q}) - R_i^e(\boldsymbol{Q}) \geq t, t > 0, \\ & \quad \mathrm{Tr}(\boldsymbol{Q}_i) \leq \mathrm{P}_i, \boldsymbol{Q}_i \succeq 0, \forall i \in \mathcal{K}. \end{aligned} \tag{8}$$

Note that, problem (P2) is exactly equivalent to problem (P1), the difference between (P1) and (P2) is only in the mathematical form. However, this simple transformation from (P1) to (P2) changes problem (P2) into a smooth problem and opens the way for further mathematical transformation.

To proceed, we further define the following two auxiliary functions

$$\begin{aligned} \phi_i(\boldsymbol{Q}) &= \log\left|\boldsymbol{H}_{ii}\boldsymbol{Q}_i\boldsymbol{H}_{ii}^H + \boldsymbol{Z}_i\right|, \\ \varphi_i(\boldsymbol{Q}) &= \log\left|\boldsymbol{I} + \boldsymbol{H}_{ie}^H\boldsymbol{N}_e^{-1}\boldsymbol{H}_{ie}\boldsymbol{Q}_i\right| + \log\left|\boldsymbol{Z}_i\right|. \end{aligned} \tag{9}$$

Note that, $\phi_i(\boldsymbol{Q})$ and $\varphi_i(\boldsymbol{Q})$ are both concave with respect to $\boldsymbol{Q}$. Then, problem (P2) can be equivalently reformulated in the following optimization problem

$$\begin{aligned} \text{(P3)}: \ & \max_{\boldsymbol{Q},t} t \\ & s.t. \ \phi_i(\boldsymbol{Q}) - \varphi_i(\boldsymbol{Q}) \geq t, t > 0, \forall i \in \mathcal{K}, \\ & \quad \mathrm{Tr}(\boldsymbol{Q}_i) \leq \mathrm{P}_i, \boldsymbol{Q}_i \succeq 0, \forall i \in \mathcal{K}. \end{aligned} \tag{10}$$

Thus, we have formulated a DC programming problem. And, the difficult in solving problem (P3) lies in the constraints $\phi_i(\boldsymbol{Q}) - \varphi_i(\boldsymbol{Q}) \geq t, t > 0, \forall i \in \mathcal{K}$.

According to the formula proposed in [13], the first-order differential of the concave function $\varphi_i(\boldsymbol{Q}), \forall i \in \mathcal{K}$ can be calculated as

$$d\varphi_i(\boldsymbol{Q}) = \sum_{j \neq i}^{k} \mathrm{Tr}(\boldsymbol{H}_{ji}^H\boldsymbol{Z}_i^{-1}\boldsymbol{H}_{ji}d\boldsymbol{Q}_j) + \mathrm{Tr}(\boldsymbol{H}_{ie}^H\boldsymbol{R}_{ie}^{-1}\boldsymbol{H}_{ie}d\boldsymbol{Q}_i). \tag{11}$$

Here, the intermediate parameter matrix $\boldsymbol{R}_{ie}$ is defined in the following formula

$$\boldsymbol{R}_{ie} = \boldsymbol{H}_{ie}\boldsymbol{Q}_i\boldsymbol{H}_{ie}^H + \boldsymbol{N}_e, \tag{12}$$

where $\boldsymbol{N}_e$ is the covariance matrix of additive noise vector received by Eve.

Then, with a given point $\boldsymbol{Q}^v$ which is feasible to problem (P3), the concave function $\varphi_i(\boldsymbol{Q}), \forall i \in \mathcal{K}$ can be locally linearized to

$$\varphi_i(\boldsymbol{Q}) \cong \varphi_i(\boldsymbol{Q}^v) + \sum_{j=1}^{k} \mathrm{Tr}[\boldsymbol{D}_{ij}(\boldsymbol{Q}_j - \boldsymbol{Q}_j^v)] \triangleq \overline{\varphi}_i(\boldsymbol{Q}), \tag{13}$$

Algorithm 1. Iterative precoding algorithm for solving problem (P1).

1: initially set k, $\boldsymbol{H}_i$, P_i, $\forall k \in \mathcal{K}$, $\boldsymbol{H}_e$, $\boldsymbol{Q}^v$, and $v = 0$.
2: **repeat**
3: compute $\boldsymbol{R}_e$ and $\boldsymbol{Z}_i, \forall i \in \mathcal{K}$ with $\boldsymbol{Q}^v$ according to formulae (12) and (3).
4: compute $\boldsymbol{D}_{ij}(\boldsymbol{Q}^v)$, $\forall i, j \in \mathcal{K}$ according to formula (14).
5: compute $\boldsymbol{Q}$ by solving problem (P4) with CVX solver
6: update $v = v + 1$, and $\boldsymbol{Q}^v = \boldsymbol{Q}$.
7: compute $R(\boldsymbol{Q}^v) = \min_i R_i^s(\boldsymbol{Q}^v)$, $\forall i \in \mathcal{K}$.
8: **until** the termination criteria are satisfied.
9: **return** $\boldsymbol{Q}^v$ and $R(\boldsymbol{Q}^v)$.

which is further denoted as $\overline{\varphi}_i(\boldsymbol{Q})$. Here, the intermediate parameter matrix $\boldsymbol{D}_{ij}$ can be computed as

$$\boldsymbol{D}_{ij} = \begin{cases} \boldsymbol{H}_{ie}^H \boldsymbol{R}_{ie}^{-1} \boldsymbol{H}_{ie}, \text{ if } j = i, \\ \boldsymbol{H}_{ji}^H \boldsymbol{Z}_i^{-1} \boldsymbol{H}_{ji}, \text{ if } j \neq i, \end{cases} \tag{14}$$

where the process parameter matrices $\boldsymbol{R}_e$ and $\boldsymbol{Z}_i, \forall i \in \mathcal{K}$ are all computed with $\boldsymbol{Q}^v$. Note that, the function $\overline{\varphi}_i(\boldsymbol{Q}), \forall i \in \mathcal{K}$ is a linear approximation of the concave function $\varphi_i(\boldsymbol{Q}), \forall i \in \mathcal{K}$. Thus, we always have the following inequality

$$\varphi_i(\boldsymbol{Q}) \leqslant \overline{\varphi}_i(\boldsymbol{Q}), \forall i \in \mathcal{K}, \tag{15}$$

due to the concavity of the function $\varphi_i(\boldsymbol{Q}), \forall i \in \mathcal{K}$.

Therefore, with the given point $\boldsymbol{Q}^v$, problem (P3) can be locally convexified to the following optimization problem

$$\begin{aligned} (\text{P4}): \quad & \max_{\boldsymbol{Q}, t} \; t \\ & s.t. \; \phi_i(\boldsymbol{Q}) - \overline{\varphi}_i(\boldsymbol{Q}) \geq t, t > 0, \forall i \in \mathcal{K}, \\ & \quad \mathrm{Tr}(\boldsymbol{Q}_i) \leq \mathrm{P}_i, \boldsymbol{Q}_i \succeq 0, \forall i \in \mathcal{K}. \end{aligned} \tag{16}$$

Note that, problem (P4) is convex and can be solved by a standard convex programming algorithm in polynomial time, e.g., with CVX solver [14]. Thus, a coordinated iterative precoding algorithm, proposed as *Algorithm 1*, can be framed based on the following dynamic: with a feasible solution $\boldsymbol{Q}^v$ obtained in the vth iteration, the next feasible solution $\boldsymbol{Q}^{v+1}$ can be obtained by solving problem (P4) in the $(v+1)$th iteration. Obviously, *Algorithm 1* is designed in a centralized fashion, and practical implement of it needs deep cooperation between all legitimate transmitters, which is the reason that it being named as "*coordinated iterative precoding algorithm*".

3.2 Convergence Analysis

Because problem (P1) is inherent nonconvex, the convergence property of *Algorithm 1* with local Linearization has to be analytically established, which is elaborated in the following theorem.

Theorem 1. *Suppose that problem (P4) is strictly convex with respect to* $\boldsymbol{Q}$*, then, starts from any feasible solution* $\boldsymbol{Q}^v$*, the running of* Algorithm 1 *must converge to a feasible solution to problem (P1) by solving problem (P4) in an iterative way.*

Proof. According to the concavity of auxiliary function $\varphi_i(\boldsymbol{Q}), \forall i \in \mathcal{K}$, the following inequality

$$\varphi_i(\boldsymbol{Q}) \leqslant \overline{\varphi}_i(\boldsymbol{Q}), \forall i \in \mathcal{K} \tag{17}$$

always holds. It is thus concluded that the following constraint condition of problem (P4) is always stricter than that of problem (P3)

$$\phi_i(\boldsymbol{Q}) - \overline{\varphi}_i(\boldsymbol{Q}) \geq t, \forall i \in \mathcal{K}. \tag{18}$$

Thus, we can draw a conclusion that any feasible solution of problem (P4) must be a feasible solution of problem (P3), because problem (P3) is exactly equivalent to problem (P1).

Let $\widetilde{R}_i^s(\boldsymbol{Q}|\boldsymbol{Q}^v)$ denote the objective function of problem (P4), which is the concave surrogate of $R_i^s(\boldsymbol{Q})$, i.e., the objective function of problem (P1). Then, consider the update dynamic of *Algorithm 1*

$$\boldsymbol{Q}^{v+1} = \arg\max_{\boldsymbol{Q}} \min_i \widetilde{R}_i^s(\boldsymbol{Q}|\boldsymbol{Q}^v). \tag{19}$$

Then, we can come to a conclusion that the following inequality always holds

$$\min_i \widetilde{R}_i^s(\boldsymbol{Q}^{v+1}) \geq \min_i R_i^s(\boldsymbol{Q}^v). \tag{20}$$

Note that, the above inequality results from the strict convexity of problem (P4), which is the preconditions of this theorem.

On the other hand, we can also have the following inequality according to the inequality in formula (17)

$$\min_i R_i^s(\boldsymbol{Q}^{v+1}) \geq \min_i \widetilde{R}_i^s(\boldsymbol{Q}^{v+1}). \tag{21}$$

Then, we can have the following inequality relationship by combining the formulae (20) and (21)

$$\min_i R_i^s(\boldsymbol{Q}^{v+1}) \geq \min_i R_i^s(\boldsymbol{Q}^v), \tag{22}$$

which means that the sequence $R(\boldsymbol{Q}^v)$ obtained by employing *Algorithm 1* is always monotonically non-decreasing.

Under limited transmit power constraints, we can come to a conclusion that the sequence $R(\boldsymbol{Q}^v)$ is always upper bounded, i.e.,

$$R(\boldsymbol{Q}^v) \leq \min_i R_i^s(\boldsymbol{Q}^*), \tag{23}$$

where $R(\boldsymbol{Q}^*)$ is the maximum value obtained under given transmit power budgets. Therefore, the convergence property of *Algorithm 1* is guaranteed, because a monotonically non-decreasing sequence that is upper bounded always converges.

Meanwhile, we can also draw a conclusion that there must exist a limit point of sequence $\boldsymbol{Q}^v$, which is generated by running *Algorithm 1*. Moreover, the limit point must constitute a stationary point of problem (P4). Because the stationary point of problem (P4) is also a maxima of problem (P1), the limit point of sequence $\boldsymbol{Q}^v$ must form a feasible solution to problem (P1).

Hence, it can be concluded that *Algorithm 1* will always converge to a feasible solution to problem (P1) under the precondition that problem (P4) is strictly convex over $\boldsymbol{Q}$.

According to Theorem 1, we can draw a conclusion that the convergence of *Algorithm 1* is centered on the precondition that problem (P4) is strict convex. However, such a precondition isn't always met, especially when some of the wireless channels of above-mentioned MIMO IFC systems are rank deficit. Therefore, we will resort to a regularization method in the next subsection, which is based on the proximal point thought, to ensure the strict convexity of problem (P4) and thus ensure the convergence of *Algorithm 1*.

3.3 Regularized Iterative Precoding Algorithm

The regularization method based on the proximal point thought consists in utilizing a quadratic term to penalize the constraints condition of problem (P4), and thus guarantee the strict convexity of it. Mathematically, the above idea can be formally written as the following convex problem

$$\begin{aligned} (\text{P5}):\ & \max_{\boldsymbol{Q},t}\ t \\ & s.t.\ \phi_i(\boldsymbol{Q}) - \widetilde{\varphi}_i(\boldsymbol{Q}) \geq t, t > 0, \forall i \in \mathcal{K}, \\ & \qquad \text{Tr}(\boldsymbol{Q}_i) \leq \text{P}_i, \boldsymbol{Q}_i \succeq 0, \forall i \in \mathcal{K}, \end{aligned} \tag{24}$$

where the surrogate function $\widetilde{\varphi}_i(\boldsymbol{Q})$ is introduced by using the quadratic regularization term. Specifically, the modified function is given as

$$\widetilde{\varphi}_i(\boldsymbol{Q}) = \overline{\varphi}_i(\boldsymbol{Q}) + \tau||\boldsymbol{Q} - \boldsymbol{Q}^v||_F^2, \tag{25}$$

where $\tau > 0$ is a small number used to constrain $\boldsymbol{Q}$ keeping "close" to $\boldsymbol{Q}^v$. The strict convexity of problem (P5) is thus guaranteed, because the Frobenius norm is always strict convex. Moreover, the strict convexity is obtained requiring no special restrictions on the proposed MIMO IFC system.

The regularized iterative precoding algorithm based on the idea of proximal point can also be presented in the framework of *Algorithm 1*, only problem (P4) being replaced with problem (P5). However, the regularized iterative precoding algorithm is hereafter named as *Algorithm 1*(P) to avoid some ambiguity. The convergence property of the resultant *Algorithm 1*(P) will be analyzed in the following theorem.

Theorem 2. *Because the strict convexity of problem (P5) is ensured by the regularization term,* Algorithm 1*(P) must converge to a feasible solution to problem (P1) by solving problem (P5) in an iterative way.*

Proof. Because problem (P5) is strict convex by adding a regularization term composed of Frobenius norm, the precondition of Theorem 1 is thus guaranteed. Then, according to analysis process of *Algorithm 1*, which is detailed in Theorem 1, we can draw a conclusion that the convergence property of *Algorithm 1*(P) is guaranteed.

Suppose that the sequence $\boldsymbol{Q}^v$ is generated by running *Algorithm 1*(P). Then, we can draw a conclusion from the analysis presented in Theorem 1, that the limit point of $\boldsymbol{Q}^v$ must be a stationary point of problem (P5). Meanwhile, we also have

$$\lim_{v \to \infty} ||\boldsymbol{Q}^{v+1} - \boldsymbol{Q}^v||_F^2 = 0, \tag{26}$$

which means that the limit point of sequence $\boldsymbol{Q}^v$ also constitutes a stationary point of problem (P4), sine regularization term is approaching to zero when $\boldsymbol{Q}^v$ approaching to the limit point. Thus, the limit point of sequence $\boldsymbol{Q}^v$, which is generated by running *Algorithm 1*(P), must be a feasible solution to problem (P1).

Therefore, we can draw a conclusion that *Algorithm 1*(P) must converge to a feasible solution to problem (P1).

According to Theorem 2, we can come to a conclusion that *Algorithm 1*(P) always converges to a feasible solution to problem (P1) with guaranteed convergence. However, a possibly slower convergence rate is the price to pay for the guaranteed convergence, which is common to the regularization method and will be further demonstrated by numerical simulations in the next section.

4 Numerical Simulations

In this section, the proposed algorithm is intensively investigated via numerical simulations.

The simulation condition is assumed that there are $k = 3$ Alice-to-Bob wireless links, and the transmit power budget of all transmitters are set to be equal, i.e.,

$$\mathrm{P}_i = \mathrm{P}, \forall i \in \mathcal{K}.$$

The elements of the channel matrices $\mathbf{H}_{ij}, \forall i, j \in \mathcal{K}$ are all set to be i.i.d. ZMCSCG random variables. And, the variances of these matrices' elements are further set to be

$$\sigma_{ij}^2 = 1, \text{if } i = j,$$
$$\sigma_{ij}^2 = 0.25, \text{other}.$$

The elements of the channel matrices $\mathbf{H}_{ie}, \forall i \in \mathcal{K}$ are also set to be i.i.d. ZMCSCG random variable, and the variances of these matrices' elements are given as

$$\sigma_{ie}^2 = 0.25, \forall i \in \mathcal{K}.$$

Moreover, the element of the additive noise $\mathbf{n}_i, \forall i \in \mathcal{K}$ and $\mathbf{n}_e$ are all set to be i.i.d. ZMCSCG random variables with unit variance.

The convergence property of *Algorithm 1*(P) is presented in Fig. 2, and the simulation result is obtained by setting P $= 1$ and $N_t = N_r = N_e = 2$. This figure shows that *Algorithm 1*(P) converges quite quickly, e.g., in no more than 6 iterations, to a common solution under different τ. It is also shown that the convergence rate is slightly slower when τ becomes larger, which is the price to pay for the ensuring convergence as detailed in Theorem 2.

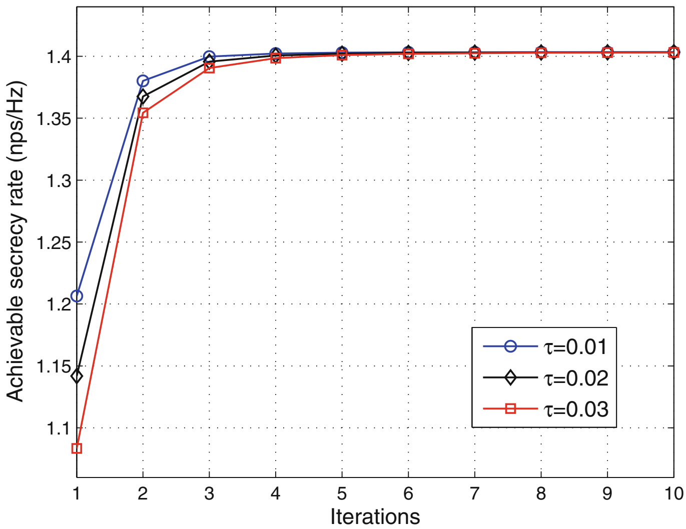

Fig. 2. The convergence property of *Algorithm 1*(P) under different τ.

The achievable secrecy rate achieved with *Algorithm 1*(P) is demonstrated in Fig. 3, which is achieved by setting $\tau = 0.01$ and $N_t = N_r = 2$. This figure shows that the achievable secrecy rate of the proposed MIMO IFC system increases with Alice's transmit power budget in a nonlinear way, and the performance is dramatically decreased when the power of Eve becomes stronger, i.e., when N_e becomes larger.

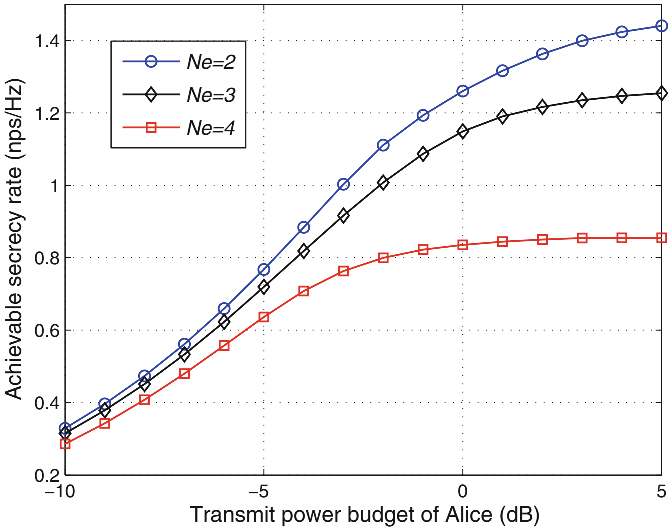

Fig. 3. The achievable secrecy rate versus Alice's transmit power budget P.

5 Conclusion

In this paper, we have studied the design problem of secure precoding for a k-user MIMO interference channel. By adopting the "maxmin" fairness criteria, the secure precoding problem is defined as an achievable secrecy rate maximization problem, which is nonconvex and non-smooth in nature. To tackle the inherent complexity, we recast the formulated problem into a DC programming problem by a series of equivalent mathematical transformations. Using the successive convex approximation method as a corner stone, a coordinated iterative precoding algorithm is developed by solving a sequence of convexified subproblems. In order to ensure the accuracy convergence of the proposed iterative algorithm, a regularization method based on the proximal point thought is also pursued. Numerical results further show that our algorithm can converge quickly to a feasible solution on the premise of ensuring convergence.

References

1. Razavi, S.M.: Beamformer design for MIMO interference broadcast channels with semidefinite programming. IEEE Trans. Signal Process. **66**(17), 4504–4515 (2018)
2. Jing, X., Mo, L., Liu, H., Zhang, C.: Linear space-time interference alignment for K-user MIMO interference channels. IEEE Access **6**, 3085–3095 (2018)
3. Shang, X., Poor, H.V.: Noisy-interference sum-rate capacity for vector Gaussian interference channels. IEEE Trans. Inf. Theory **59**(1), 132–153 (2013)
4. Larsson, E.G., Jorswieck, E.A.: Competition versus cooperation on the MISO interference channel. IEEE J. Sel. Areas Commun. **26**(7), 1059–1069 (2008)

5. Fan, Y., Wang, X., Liao, X.: On the secure degrees of freedom for two-user MIMO interference channel with a cooperative jammer. IEEE Trans. Commun. **67**(8), 5390–5402 (2019)
6. Siyari, P., Krunz, M., Nguyen, D.N.: Power games for secure communications in single-stream MIMO interference networks. IEEE Trans. Wireless Commun. **17**(9), 5759–5773 (2018)
7. Mukherjee, A., Fakoorian, S.A.A., Huang, J., Swindlehurst, A.L.: Principles of physical layer security in multiuser wireless networks: a survey. IEEE Commun. Surv. Tutor. **16**(3), 1550–1573 (2014)
8. Oggier, F., Hassibi, B.: The secrecy capacity of the MIMO wiretap channel. IEEE Trans. Inf. Theory **57**(8), 4961–4972 (2011)
9. Li, Q., Hong, M., Wai, H.-T., Liu, Y.-F., Ma, W.-K., Luo, Z.-Q.: Transmit solutions for MIMO wiretap channels using alternating optimization. IEEE J. Sel. Areas Commun. **31**(9), 2704–2717 (2013)
10. Zhang, Y., DallAnese, E., Giannakis, G.B.: Distributed optimal beamformers for cognitive radios robust to channel uncertainties. IEEE Trans. Signal Process. **60**(12), 6495–6508 (2012)
11. Alvarado, A., Scutari, G., Pang, J.-S.: A new decomposition method for multiuser DC-programming and its applications. IEEE Trans. Signal Process. **62**(11), 2984–2998 (2014)
12. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge University Press, Cambridge (2004)
13. Zhang, X.: Matrix Analysis and Applications. Tsinghua University Press, Beijing (2004)
14. CVX Research, Inc. CVX: Matlab software for disciplined convex programming, version 2.0, April 2011. http://cvxr.com/cvx