Precoder Designs for MIMO Gaussian Multiple Access Wiretap Channels

Hoon Lee, Changick Song, Jihwan Moon, and Inkyu Lee, *Fellow, IEEE*

***Abstract*—This paper studies multiple-input multiple-output multiple access wiretap channels (MAC-WT) where an eavesdropper tries to tap the communication between multiple legitimate transmitters and a legitimate receiver. In this system, we propose precoder optimization methods at the transmitters in order to maximize the sum secrecy rate performance. Although this problem can be solved by the well-known difference of convex (DC) programming, we present a more efficient algorithm whose computational complexity is much lower than that of the conventional DC approach. By investigating the Karush-Kuhn-Tucker conditions, it is confirmed that the proposed low-complexity algorithm achieves the same performance as the conventional DC method. Our analysis also reveals that the proposed algorithm ensures global optimality for multiple-input single-output MAC-WT cases, while binary power control is optimal for single-input multiple-output scenarios. Simulation results demonstrate the efficacy of the proposed precoding methods.**

***Index Terms*—Multiple access wiretap channel (MAC-WT), MIMO systems, secrecy rate maximization.**

I. Introduction

In wireless communication systems, information signals are vulnerable to eavesdropping due to the broadcast nature of electromagnetic waves. To address such a security issue and achieve a higher level of secrecy, physical layer security designs have garnered a lot of interests [1]. For such designs, an important objective is to identify the secrecy capacity which is defined by the maximum achievable rate between legitimate transmitters and legitimate receivers without leaking any information to eavesdroppers.

Ever since the wiretap channels were introduced by Wyner [2], the research has evolved into more dynamic network topologies such as multiple-input multiple-output (MIMO) systems [3]–[5] and multi-user channels. In MIMO broadcast wiretap channels (BC-WT) where a single transmitter supports multiple legitimate receivers simultaneously, the secrecy capacity region was investigated in [6]. The authors in [7] examined the secrecy capacity region for the MIMO BC with confidential messages where each legitimate receiver is considered as a potential eavesdropper. Based on these theoretical results, [8] and [9] proposed linear precoding methods in the MIMO BC-WT for improving the secrecy rate performance. Recently, secure beamforming algorithms were proposed in heterogeneous downlink networks [10].

Also, multiple access wiretap channels (MAC-WT) have been studied in [11]–[18] where a single legitimate receiver receives signals from multiple legitimate transmitters. Unlike the BC systems, however, the secrecy capacity regions of the MAC-WT are still unknown even in a single antenna setup. In single-input single-output (SISO) MAC with an eavesdropper, it was shown in [11] that a secrecy rate region is achieved by Gaussian signalling at the transmitters with the superposition coding. In addition, the authors in [13] and [14] found an achievable rate-equivocation region for two-transmitter SISO MAC with confidential messages. The cognitive MAC with confidential messages were considered in [15] in which two transmitters send common information to a legitimate receiver while one transmitter also has confidential information. By extending these results, the secure degrees of freedom analysis was studied in SISO MAC-WT [16] and MIMO MAC-WT [17] [18], respectively. However, precoder designs for the Gaussian MIMO MAC-WT have not been addressed yet.

In this paper, we investigate an efficient precoder optimization method for the MIMO MAC-WT where multiple legitimate transmitters, a legitimate receiver, and an eavesdropper are equipped with multiple antennas. Such a scenario is important for improving the secrecy of mobile users. Assuming the superposition coding scheme [12] at the transmitters, we formulate a sum secrecy rate maximization problem which is generally non-convex. To solve the problem, we first present the well-known majorization minimization (MM) algorithm based on the difference of convex (DC) approach. Although this conventional MM algorithm provides good performance, its complexity becomes prohibitive when the number of the transmitters and the antennas get larger.

To tackle this issue, we propose a low complexity precoding algorithm for the sum secrecy rate maximization problem. By examining the Karuch-Kuhn-Tucker (KKT) conditions, it is mathematically verified that the proposed algorithm achieves the same performance as the MM algorithm. Also, we confirm that the proposed scheme requires much lower complexity and faster convergence rate compared to the MM algorithm. Furthermore, we show that the proposed low complexity algorithm provides the globally optimal point for multiple-input single-output (MISO) MAC-WT scenarios. Our analysis also reveals that binary power control becomes the optimal transmission strategy in single-input multiple-ouput (SIMO) MAC-WT. Finally, simulation results demonstrate that the superposition coding combined with the proposed precoding algorithms outperform conventional schemes.

II. System Model

In this section, we present a system model for MIMO MAC-WT in the presence of an eavesdropper as illustrated in Fig. 1. In this configuration, K legitimate transmitters, each of which is

Manuscript received October 31, 2016; revised January 18, 2017; accepted March 1, 2017. Date of publication March 6, 2017; date of current version September 15, 2017. This work was supported by the National Research Foundation (NRF) funded by the Ministry of Science, ICT and Future Planning of the Korean Government under Grant 2014R1A2A1A10049769. The work of C. Song was supported by the NRF Funded by the Ministry of Science, ICT, and Future Planning, Korean Government, under Grant NRF-2015R1C1A1A02036927. The review of this paper was coordinated by Dr. Z. Ding.

H. Lee, J. Moon, and I. Lee are with the School of Electrical Engineering, Korea University, Seoul 02841, South Korea (e-mail: ihun1@korea.ac.kr; anschino@korea.ac.kr; inkyu@korea.ac.kr).

C. Song is with the Department of Information and Communications Engineering, Korea National University of Transportation, Chungju 27469, South Korea (e-mail: c.song@ut.ac.kr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2017.2678601

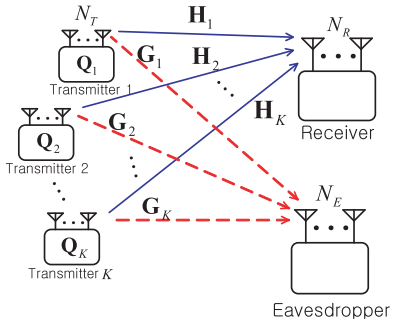

Fig. 1. Schematic diagrams for multi-user MIMO MAC-WT.

equipped with N_T antennas, want to secretly communicate with a legitimate receiver having N_R antennas, i.e., we consider uplink networks. At the same time, the eavesdropper with N_E antennas, which is assumed to have the same level of information and decoding capability as the legitimate receiver, tries to intercept the legitimate transmitters' messages.

Let us define $\mathbf{H}_i \in \mathbb{C}^{N_R \times N_T}$ and $\mathbf{G}_i \in \mathbb{C}^{N_E \times N_T}$ as the channel matrix from transmitter i to the receiver and the eavesdropper, respectively. The elements of the channel matrices $\{\mathbf{H}_i\}$ and $\{\mathbf{G}_i\}$ are independent and identically distributed complex zero mean Gaussian random variables with variance 1 and β, respectively, where β equals the channel gain between the legitimate transmitters and the eavesdropper. Then, the received signals at the receiver $\mathbf{y}_R \in \mathbb{C}^{N_R \times 1}$ and at the eavesdropper $\mathbf{y}_E \in \mathbb{C}^{N_E \times 1}$ are given by $\mathbf{y}_R = \sum_{i=1}^{K} \mathbf{H}_i \mathbf{x}_i + \mathbf{n}_R$ and $\mathbf{y}_E = \sum_{i=1}^{K} \mathbf{G}_i \mathbf{x}_i + \mathbf{n}_E$, where $\mathbf{x}_i \in \mathbb{C}^{N_T \times 1} \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_i)$ represents the transmitted signal at transmitter i with $\mathbf{Q}_i \in \mathbb{C}^{N_T \times N_T}$ being the transmit covariance matrix, and $\mathbf{n}_R \in \mathbb{C}^{N_R \times 1} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_R})$ and $\mathbf{n}_E \in \mathbb{C}^{N_E \times 1} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_E})$ indicate the complex Gaussian noise at the receiver and at the eavesdropper, respectively. Throughout this paper, it is assumed that the perfect knowledge for $\{\mathbf{H}_i\}$ and $\{\mathbf{G}_i\}$ is available at the legitimate receiver.[1]

In this paper, we aim to maximize the sum secrecy rate for the MIMO MAC-WT by jointly optimizing each transmitter's covariance matrix $\mathbf{Q}_i$ for $i = 1, \cdots, K$. When the superposition coding scheme is employed at the legitimate transmitters, the achievable sum secrecy rate maximization problem for the MIMO MAC-WT can be formulated as [11][2]

$$\max_{\{\mathbf{Q}_i\}} \log \left| \mathbf{I}_{N_R} + \sum_{i=1}^{K} \mathbf{H}_i \mathbf{Q}_i \mathbf{H}_i^H \right| - \log \left| \mathbf{I}_{N_E} + \sum_{i=1}^{K} \mathbf{G}_i \mathbf{Q}_i \mathbf{G}_i^H \right|$$
$$\text{s.t. } \mathbf{0} \preceq \mathbf{Q}_i \preceq \mathbf{S}_i, \ i = 1, \cdots, K, \tag{1}$$

[1]The eavesdropper's channel $\{\mathbf{G}_i\}$ can be estimated at the legitimate nodes utilizing the *torch* aided estimation methods in [19].

[2]Throughput this paper, we consider the collective secrecy constraint defined in [11] and [12] which guarantees the secrecy of any group of transmitters, and thus it is suitable for the multiple access nature.

TABLE I
ALGORITHM 1: MM ALGORITHM

Initialize $n = 0$ and $\mathbf{Q}_i^{(n)}$ for $i = 1, \cdots, K$.
Repeat
  Set $n \leftarrow n + 1$.
  Solve problem (3) by the interior point method.
Until $\{\mathbf{Q}_i^{(n)}\}$ converge

where $\mathbf{S}_i \in \mathbb{C}^{N_T \times N_T}$ accounts for a fixed positive semi-definite matrix. Here, the constraint $\mathbf{Q}_i \preceq \mathbf{S}_i$ stands for the input covariance matrix constraint [7], [20]–[22] which imposes a constraint on the shape of the transmit covariance matrix. Note that the input covariance matrix constraint is a general power constraint including the average power constraint and the per-antenna power constraint. Problem (1) is in general non-convex and thus it is difficult to obtain the optimal solution. In the following, we first introduce the conventional DC programming methods for solving (1) in Section III. Then, a low complexity algorithm will be proposed in Section IV. Also, the global optimality for problem (1) will be discussed.

III. Majorization Maximization Algorithm

In this section, we briefly describe the DC programming approach for problem (1). One can easily check that the objective function in (1) is the difference of two concave functions $f(\{\mathbf{Q}\}) \triangleq \log|\mathbf{I}_{N_R} + \sum_{i=1}^{K} \mathbf{H}_i \mathbf{Q}_i \mathbf{H}_i^H|$ and $g(\{\mathbf{Q}_i\}) \triangleq \log|\mathbf{I}_{N_E} + \sum_{i=1}^{K} \mathbf{G}_i \mathbf{Q}_i \mathbf{G}_i^H|$. Therefore, we can find a local optimal solution for the problem in (1) by employing the DC programming techniques, e.g., the MM algorithm [23]. At the n-th iteration in the MM algorithm, we first apply the first-order Taylor series approximation to the non-convex term $g(\{\mathbf{Q}_i\})$ in (1) as $g(\{\mathbf{Q}_i\}) \simeq \tilde{g}(\{\mathbf{Q}_i^{(n-1)}\}, \{\mathbf{Q}_i\})$, where $\tilde{g}(\{\mathbf{Q}_i^{(n-1)}\}, \{\mathbf{Q}_i\})$ is defined in (2) on the bottom of the page, and $\{\mathbf{Q}_i^{(n-1)}\}$ equals a solution from the MM algorithm at the $(n-1)$-th iteration.

Then, the covariance matrix $\{\mathbf{Q}_i^{(n)}\}$ at the n-th iteration can be obtained by solving the following problem:

$$\{\mathbf{Q}_i^{(n)}\} = \arg\max_{\{\mathbf{Q}_i\}} f(\{\mathbf{Q}_i\}) - \tilde{g}(\{\mathbf{Q}_i^{(n-1)}\}, \{\mathbf{Q}_i\})$$
$$\text{s.t. } \mathbf{0} \preceq \mathbf{Q}_i \preceq \mathbf{S}_i, \ i = 1, \cdots, K. \tag{3}$$

It is easy to check that problem (3) is convex, and thus the interior point method [24] can readily compute the globally optimal solution. The foregoing procedures are repeated until $\{\mathbf{Q}_i^{(n)}\}$ converges. The MM algorithm for the sum secrecy rate maximization problem (1) is summarized in Table I.

We can prove that Algorithm 1 converges to a stationary point of problem (1), i.e., a locally optimal solution can be obtained [23]. Also, note that the complexity of Algorithm 1 is dominated

$$\tilde{g}(\{\mathbf{Q}_i^{(n-1)}\}, \{\mathbf{Q}_i\}) \triangleq \text{tr}\left(\left(\mathbf{I}_{N_E} + \sum_{j=1}^{K} \mathbf{G}_j \mathbf{Q}_j^{(n-1)} \mathbf{G}_j^H \right)^{-1} \left(\sum_{i=1}^{K} \mathbf{G}_i (\mathbf{Q}_i - \mathbf{Q}_i^{(n-1)}) \mathbf{G}_i^H \right) \right) + \log \left| \mathbf{I}_{N_E} + \sum_{i=1}^{K} \mathbf{G}_i \mathbf{Q}_i^{(n-1)} \mathbf{G}_i^H \right|. \tag{2}$$

TABLE II
ALGORITHM 2: PROPOSED ALGORITHM

Initialize $\mathbf{Q}_i$ for $i = 1, \cdots, K$.
Repeat
 For $i = 1 : K$
  Set $\mathbf{Z}_R = \mathbf{I}_{N_R} + \sum_{j \neq i} \mathbf{H}_j \mathbf{Q}_j \mathbf{H}_j^H$ and $\mathbf{Z}_E = \mathbf{I}_{N_E} + \sum_{j \neq i} \mathbf{G}_j \mathbf{Q}_j \mathbf{G}_j^H$.
  Obtain $\mathbf{Q}_i = \underset{\mathbf{0} \preceq \mathbf{Q}_i \preceq \mathbf{S}_i}{\arg\max} \log\left|\mathbf{Z}_R + \mathbf{H}_i \mathbf{Q}_i \mathbf{H}_i^H\right| - \log\left|\mathbf{Z}_E + \mathbf{G}_i \mathbf{Q}_i \mathbf{G}_i^H\right|$.
 End
Until $\{\mathbf{Q}_i\}$ converge

by solving the convex problem in (3), whose complexity is given by $\mathcal{O}(K^2 N_T^7)$ [24]. Then, denoting L_{MM} as the number of iterations, the overall computational complexity of Algorithm 1 can be expressed as $\mathcal{O}(L_{MM} K^2 N_T^7)$.

IV. PROPOSED LOW COMPLEXITY ALGORITHM

In this section, we propose a low complexity algorithm for the sum secrecy rate maximization problem (1) that achieves the same local optimal performance with the MM algorithm in the previous section. Furthermore, the globally optimal solutions are provided for both MISO and SIMO scenarios as special cases. In order to efficiently solve problem (1), we first consider a single user MIMO wiretap scenario [20], whose secrecy rate maximization problem is written as

$$\max_{\mathbf{0} \preceq \mathbf{Q} \preceq \mathbf{S}} \log|\mathbf{Z}_R + \mathbf{H}\mathbf{Q}\mathbf{H}^H| - \log|\mathbf{Z}_E + \mathbf{G}\mathbf{Q}\mathbf{G}^H|, \quad (4)$$

where $\mathbf{Z}_R \in \mathbb{C}^{N_R \times N_R}$ and $\mathbf{Z}_E \in \mathbb{C}^{N_E \times N_E}$ are arbitrary noise covariance matrices at the legitimate receiver and the eavesdropper, respectively.

Then, the optimal solution $\mathbf{Q}^\star$ for (4) is given by [20]

$$\mathbf{Q}^\star = \mathbf{S}^{1/2} \mathbf{C}_1 (\mathbf{C}_1^H \mathbf{C}_1)^{-1} \mathbf{C}_1^H \mathbf{S}^{1/2}, \quad (5)$$

where $\mathbf{C}_1 \in \mathbb{C}^{N_T \times b}$ consists of the first b columns of $\mathbf{C} \in \mathbb{C}^{N_T \times N_T}$ which equals the generalized eigenvector matrix of a pencil $(\mathbf{S}^{1/2}\mathbf{H}^H \mathbf{Z}_R^{-1} \mathbf{H}\mathbf{S}^{1/2} + \mathbf{I}_{N_T}, \mathbf{S}^{1/2}\mathbf{G}^H \mathbf{Z}_E^{-1} \mathbf{G}\mathbf{S}^{1/2} + \mathbf{I}_{N_T})$. Here, b represents the number of generalized eigenvalues that are greater than 1.

By employing this single user solution, we propose an iterative process based on the block coordinate descent frameworks [25] which solves the multi-user MIMO MAC-WT problem in (1), and this is summarized in Table II. At each iteration, the covariance matrix $\mathbf{Q}_i$ is updated as a single user solution in (5) by fixing other $\mathbf{Q}_j$ for $j \neq i$. This procedure is repeated until all the covariance matrices converge.[3] In the following lemma, we prove the convergence behavior of Algorithm 2.

Lemma 1: Algorithm 2 converges to at least a locally optimal point of problem (1).

Proof: Before showing the convergence of the proposed algorithm, we first check the relationship between problems (1) and (4). It is worthwhile noting that despite the non-convexity of problem (1), we can prove that strong duality is satisfied [22]. Thus, the KKT conditions are necessary for the optimal covariance matrix $\mathbf{Q}_i^\star$ [24], which are written by

$$\mathbf{H}_i^H \left(\mathbf{I}_{N_R} + \sum_{j=1}^{K} \mathbf{H}_j \mathbf{Q}_j^\star \mathbf{H}_j^H\right)^{-1} \mathbf{H}_i + \mathbf{\Psi}_i^\star = \mathbf{G}_i^H \left(\mathbf{I}_{N_R} + \sum_{j=1}^{K} \mathbf{G}_j \mathbf{Q}_j^\star \mathbf{G}_j^H\right)^{-1} \mathbf{G}_i + \mathbf{\Phi}_i^\star, \ \forall i, \quad (6)$$

$$\mathbf{\Psi}_i^\star \mathbf{Q}_i^\star = \mathbf{0}, \ \mathbf{\Phi}_i^\star (\mathbf{S}_i - \mathbf{Q}_i^\star) = \mathbf{0}, \ \mathbf{\Psi}_i^\star \succeq \mathbf{0}, \ \mathbf{\Phi}_i^\star \succeq \mathbf{0}, \ \forall i \quad (7)$$

where $\mathbf{\Psi}_i^\star$ and $\mathbf{\Phi}_i^\star$ are the optimal dual variables associated with the constraints $\mathbf{Q}_i \succeq \mathbf{0}$ and $\mathbf{Q}_i \preceq \mathbf{S}_i$, respectively.

It can be shown that the KKT conditions in (6) and (7) for the multi-user MIMO MAC-WT become equivalent to those of the single user wiretap channel problem in (4) by setting the noise covariance matrices as

$$\mathbf{Z}_R = \mathbf{I}_{N_R} + \sum_{j \neq i} \mathbf{H}_j \mathbf{Q}_j^\star \mathbf{H}_j^H \text{ and } \mathbf{Z}_E = \mathbf{I}_{N_E} + \sum_{j \neq i} \mathbf{G}_j \mathbf{Q}_j^\star \mathbf{G}_j^H.$$

Therefore, for given $\{\mathbf{Q}_j^\star\}$ for $j \neq i$, the solution $\mathbf{Q}_i^\star$ of the multi-user problem (1) can be computed from (5).

Based on this result, we can provide the convergence behavior of Algorithm 2. At each iteration, Algorithm 2 updates the covariance matrix $\mathbf{Q}_i$ from (5), which satisfies the necessary KKT conditions. This implies that the objective function in (1) is non-decreasing with each iteration. Also, it is obvious that the objective function is upper bounded by a finite value, and thus the proposed algorithm converges to at least a local optimal point. This completes the proof. ■

We now discuss the complexity issue. The complexity of Algorithm 2 is dominated by the eigenvalue decomposition procedure for K matrices of size $N_T \times N_T$, which is given by $\mathcal{O}(K N_T^3)$ [26]. Therefore, the overall complexity of the proposed algorithm can be written by $\mathcal{O}(L_p K N_T^3)$, where L_p represents the number of iterations for the proposed algorithm, which is much lower than the complexity of the MM algorithm $\mathcal{O}(L_{MM} K^2 N_T^7)$ presented in Section III. Note that this complexity reduction is attributed to the closed-form expression for the covariance matrix solution (5). Also, from simulation results, we will show that the proposed algorithm converges faster than the MM algorithm, i.e., L_p is smaller than L_{MM}.

A. Global Optimal Solutions for MISO and SIMO Cases

In what follows, we address the globally optimality for the special cases of MISO and SIMO MAC-WT systems. Let us first consider the MISO MAC-WT where $N_R = N_E = 1$. As stated in Lemma 1, the proposed algorithm converges to a local optimal point in general. However, in the following theorem, we can state the global optimality of the proposed algorithm for MISO MAC-WT systems.

Theorem 1: When $N_R = N_E = 1$, Algorithm 2 converges to the globally optimal point.

[3] In practice, the covariance matrices can be computed at the legitimate receiver and then informed to the legitimate transmitters by employing the methods developed for the BC-WT [6].

Proof: For the MISO case, problem (1) can be recast to

$$\max_{\{\mathbf{Q}_i\}} \log\left(1+\sum_{i=1}^{K}\mathbf{h}_i\mathbf{Q}_i\mathbf{h}_i^H\right)-\log\left(1+\sum_{i=1}^{K}\mathbf{g}_i\mathbf{Q}_i\mathbf{g}_i^H\right)$$
$$\text{s.t. } \mathbf{0}\preceq\mathbf{Q}_i\preceq\mathbf{S}_i,\ i=1,\cdots,K, \tag{8}$$

where $\mathbf{h}_i\in\mathbb{C}^{1\times N_T}$ and $\mathbf{g}_i\in\mathbb{C}^{1\times N_T}$ stand for the channel row vectors from transmitter i to the legitimate receiver and the eavesdropper, respectively.

It is confirmed from Lemma 1 that the converged solution of Algorithm 2 is a local optimal for (8) in general, and satisfies the KKT conditions (6) and (7), which can be rewritten by

$$\frac{\mathbf{h}_i^H\mathbf{h}_i}{1+\sum_{j=1}^{K}\mathbf{h}_j\mathbf{Q}_j^\star\mathbf{h}_j^H}+\mathbf{\Psi}_i^\star=\frac{\mathbf{g}_i^H\mathbf{g}_i}{1+\sum_{j=1}^{K}\mathbf{g}_j\mathbf{Q}_j^\star\mathbf{g}_j^H}+\mathbf{\Phi}_i^\star,\ \forall i, \tag{9}$$

$$\mathbf{\Psi}_i^\star\mathbf{Q}_i^\star=\mathbf{0},\ \mathbf{\Phi}_i^\star(\mathbf{S}_i-\mathbf{Q}_i^\star)=\mathbf{0},\ \mathbf{\Psi}_i^\star\succeq\mathbf{0},\ \mathbf{\Phi}_i^\star\succeq\mathbf{0},\ \forall i. \tag{10}$$

In order to show the global optimality of Algorithm 2 in the MISO case, in the following, we will prove that the necessary conditions in (9) and (10) are indeed the necessary and sufficient conditions for problem (8).

To this end, we reformulate (8) as

$$\max_{\{\mathbf{Q}_i\}}\frac{1+\sum_{i=1}^{K}\mathbf{h}_i\mathbf{Q}_i\mathbf{h}_i^H}{1+\sum_{i=1}^{K}\mathbf{g}_i\mathbf{Q}_i\mathbf{g}_i^H},\ \text{s.t. } \mathbf{0}\preceq\mathbf{Q}_i\preceq\mathbf{S}_i,\ i=1,\cdots,K.$$

Since the above problem is concave fractional programming, the globally optimal solution can be found by the Dinkelbach method [27]. At each iteration of the Dinkelbach method, we solve the following convex semi-definite programming:

$$F(\lambda)\triangleq\max_{\{\mathbf{Q}_i\}}1-\lambda+\sum_{i=1}^{K}\text{tr}((\mathbf{h}_i^H\mathbf{h}_i-\lambda\mathbf{g}_i^H\mathbf{g}_i)\mathbf{Q}_i),$$
$$\text{s.t. } \mathbf{0}\preceq\mathbf{Q}_i\preceq\mathbf{S}_i,\ i=1,\cdots,K, \tag{11}$$

and the optimal $\lambda^\star$ is determined by a line search method such that $F(\lambda^\star)=0$.

Thus, the necessary and sufficient optimality conditions for the original problem (8) can be obtained as

$$\mathbf{h}_i^H\mathbf{h}_i+\mathbf{\Gamma}_i^\star=\lambda^\star\mathbf{g}_i^H\mathbf{g}_i+\mathbf{\Omega}_i^\star,\ \forall i, \tag{12}$$

$$\mathbf{\Gamma}_i^\star\mathbf{Q}_i^\star=\mathbf{0},\ \mathbf{\Omega}_i^\star(\mathbf{S}_i-\mathbf{Q}_i^\star)=\mathbf{0},\ \mathbf{\Gamma}_i^\star\succeq\mathbf{0},\ \mathbf{\Omega}_i^\star\succeq\mathbf{0},\ \forall i, \tag{13}$$

$$1-\lambda^\star+\sum_{i=1}^{K}\text{tr}((\mathbf{h}_j^H\mathbf{h}_j-\lambda^\star\mathbf{g}_j^H\mathbf{g}_j)\mathbf{Q}_j^\star)=0, \tag{14}$$

where $\mathbf{\Gamma}_i^\star$ and $\mathbf{\Omega}_i^\star$ are the optimal dual variables of problem (11) when $\lambda=\lambda^\star$, which correspond to the constraints $\mathbf{Q}_i\succeq\mathbf{0}$ and $\mathbf{Q}_i\preceq\mathbf{S}_i$, respectively. Note that (12) and (13) are the KKT conditions of the convex problem (11) that has zero duality gap [24], and (14) comes from the condition $F(\lambda^\star)=0$.

Now, we will show that the necessary optimality conditions (9) and (10) are indeed equivalent to the necessary and sufficient conditions (12)–(14). This reveals that the converged solution of Algorithm 2 always satisfies the necessary and sufficient optimality conditions, and thus it is the globally optimal solution for problem (1) when $N_R=N_E=1$. From (14), we have $\lambda^\star=\frac{1+\sum_{i=1}^{K}\mathbf{h}_j\mathbf{Q}_j^\star\mathbf{h}_j^H}{1+\sum_{i=1}^{K}\mathbf{g}_i\mathbf{Q}_i^\star\mathbf{g}_i^H}$. Substituting this into (12), (12)–(14) can be simplified as

$$\frac{\mathbf{h}_i^H\mathbf{h}_i}{\alpha}+\frac{\mathbf{\Gamma}_i^\star}{\alpha}=\frac{\mathbf{g}_i^H\mathbf{g}_i}{1+\sum_{j=1}^{K}\mathbf{g}_j\mathbf{Q}_j^\star\mathbf{g}_j^H}+\frac{\mathbf{\Omega}_i^\star}{\alpha},\ \forall i,\text{ and (13)}, \tag{15}$$

where $\alpha\triangleq1+\sum_{j=1}^{K}\mathbf{h}_j\mathbf{Q}_j^\star\mathbf{h}_j^H$.

In addition, combining (9) and (15), we obtain

$$\alpha\mathbf{\Psi}_i^\star=\alpha\mathbf{\Phi}_i^\star+\mathbf{\Gamma}_i^\star-\mathbf{\Omega}_i^\star. \tag{16}$$

Then, based on (10), (13), and (16), it is easily verified that the conditions (9) and (10) become equivalent to (12)–(14) if the dual variables $\mathbf{\Psi}_i^\star$ and $\mathbf{\Phi}_i^\star$ are respectively given by

$$\mathbf{\Psi}_i^\star=(\mathbf{\Gamma}_i^\star+\mathbf{N}_i)/\alpha\text{ and }\mathbf{\Phi}_i^\star=(\mathbf{\Omega}_i^\star+\mathbf{N}_i)/\alpha, \tag{17}$$

where $\mathbf{N}_i$ fulfills $\mathbf{N}_i\mathbf{Q}_i^\star=\mathbf{0}$ and $\mathbf{N}_i\mathbf{S}_i=\mathbf{0}$.

To prove the relationship in (17), we investigate the complementary slackness conditions $\mathbf{\Psi}_i^\star\mathbf{Q}_i^\star=\mathbf{0}$ and $\mathbf{\Gamma}_i^\star\mathbf{Q}_i^\star=\mathbf{0}$. By employing (16), the matrix $(\mathbf{\Psi}_i^\star-\mathbf{\Gamma}_i^\star)\mathbf{Q}_i^\star$ can be computed as

$$\begin{aligned}(\mathbf{\Psi}_i^\star-\mathbf{\Gamma}_i^\star)\mathbf{Q}_i^\star&=((1-\alpha)\mathbf{\Psi}_i^\star+\alpha\mathbf{\Phi}_i^\star-\mathbf{\Omega}_i^\star)\mathbf{Q}_i^\star\\&=(\alpha\mathbf{\Phi}_i^\star-\mathbf{\Omega}_i^\star)\mathbf{Q}_i^\star=(\alpha\mathbf{\Phi}_i^\star-\mathbf{\Omega}_i^\star)\mathbf{S}_i,\end{aligned} \tag{18}$$

where the equalities in (18) comes from (10) and (13). Due to the fact $\mathbf{\Psi}_i^\star\mathbf{Q}_i^\star=\mathbf{\Gamma}_i^\star\mathbf{Q}_i^\star=\mathbf{0}$, (18) must be a zero matrix for any given $\mathbf{S}_i\succeq\mathbf{0}$. For this reason, it follows $\alpha\mathbf{\Phi}_i^\star-\mathbf{\Omega}_i^\star=\mathbf{N}_i$, and combining this and (16) results in (17). Therefore, the necessary conditions (9) and (10) and the necessary and sufficient conditions (12)–(14) are the same.

Next, we consider another important special case of SIMO MAC-WT systems where each legitimate transmitter has a single antenna. In this case, the problem in (1) reduces to

$$\max_{\{0\le q_i\le s_i\}}\log\left|\mathbf{I}_{N_R}+\sum_{i=1}^{K}q_i\tilde{\mathbf{h}}_i\tilde{\mathbf{h}}_i^H\right|-\log\left|\mathbf{I}_{N_E}+\sum_{i=1}^{K}q_i\tilde{\mathbf{g}}_i\tilde{\mathbf{g}}_i^H\right| \tag{19}$$

where q_i is the transmit power of transmitter i, $\tilde{\mathbf{h}}_i\in\mathbb{C}^{N_R\times1}$ and $\tilde{\mathbf{g}}_i\in\mathbb{C}^{N_E\times1}$ stand for the channel column vectors from transmitter i to the legitimate receiver and the eavesdropper, respectively, and s_i accounts for the maximum power constraint at transmitter i. In the following theorem, we provide the globally optimal solution for problem (19).

Theorem 2: The optimal solution for (19) is obtained by either $q_i^\star=0$ or $q_i^\star=s_i$.

Proof: Let us define the objective function in (19) as $R(\{q_i\})$. We first show that $R(\{q_i\})$ is either increasing or non-increasing on each q_i. By differentiating $R(\{q_i\})$ with respect to q_i and applying some manipulations, it follows

$$\frac{\partial R(\{q_i\})}{\partial q_i}=\frac{\tilde{\mathbf{h}}_i^H\mathbf{A}_i^{-1}\tilde{\mathbf{h}}_i}{1+q_i\tilde{\mathbf{h}}_i^H\mathbf{A}_i^{-1}\tilde{\mathbf{h}}_i}-\frac{\tilde{\mathbf{g}}_i^H\mathbf{B}_i^{-1}\tilde{\mathbf{g}}_i}{1+q_i\tilde{\mathbf{g}}_i^H\mathbf{B}_i^{-1}\tilde{\mathbf{g}}_i}, \tag{20}$$

where $\mathbf{A}_i\triangleq\mathbf{I}_{N_R}+\sum_{j\neq i}q_j\tilde{\mathbf{h}}_j\tilde{\mathbf{h}}_j^H$ and $\mathbf{B}_i\triangleq\mathbf{I}_{N_E}+\sum_{j\neq i}q_j\tilde{\mathbf{g}}_j\tilde{\mathbf{g}}_j^H$. One can check that if $\tilde{\mathbf{h}}_i^H\mathbf{A}_i^{-1}\tilde{\mathbf{h}}_i>\tilde{\mathbf{g}}_i^H\mathbf{B}_i^{-1}\tilde{\mathbf{g}}_i$,

then the gradient in (20) becomes positive, which implies that $R(\{q_i\})$ is an increasing function on q_i. Otherwise, if $\tilde{\mathbf{h}}_i^H \mathbf{A}_i^{-1} \tilde{\mathbf{h}}_i \leq \tilde{\mathbf{g}}_i^H \mathbf{B}_i^{-1} \tilde{\mathbf{g}}_i$, we have $\frac{\partial R(\{q_i\})}{\partial q_i} \leq 0$. Therefore, with given $\{q_j\}$ for $j \neq i$, the objective function in (19) is either increasing or non-increasing for q_i.

Next, by contradiction, we will show that the optimal solution for problem (19) can be expressed as either $q_i^\star = 0$ or $q_i^\star = s_i$. Suppose that the optimal solution is obtained as $0 < q_i^\star < s_i$ for some i. Then, we can increase the objective function in (19) by setting $q_i^\star = s_i$ if $\tilde{\mathbf{h}}_i^H \hat{\mathbf{A}}_i^{-1} \tilde{\mathbf{h}}_i > \tilde{\mathbf{g}}_i^H \hat{\mathbf{B}}_i^{-1} \tilde{\mathbf{g}}_i$, where $\hat{\mathbf{A}}_i \triangleq \mathbf{I}_{N_R} + \sum_{j \neq i} q_j^\star \tilde{\mathbf{h}}_j \tilde{\mathbf{h}}_j^H$ and $\hat{\mathbf{B}}_i \triangleq \mathbf{I}_{N_E} + \sum_{j \neq i} q_j^\star \tilde{\mathbf{g}}_j \tilde{\mathbf{g}}_j^H$, since the objective function in (19) is an increasing function in this case. Also, when $\tilde{\mathbf{h}}_i^H \hat{\mathbf{A}}_i^{-1} \tilde{\mathbf{h}}_i \leq \tilde{\mathbf{g}}_i^H \hat{\mathbf{B}}_i^{-1} \tilde{\mathbf{g}}_i$, we can set the optimal q_i as $q_i^\star = 0$ without decreasing $R(\{q_i^\star\})$. This contradicts the assumption $0 < q_i^\star < s_i$, and thus the optimal solution for (19) is achieved by either $q_i^\star = 0$ or $q_i^\star = s_i$. This completes the proof. ■

Theorem 2 indicates that in the SIMO MAC-WT case, the optimal transmit power allocation strategy at the legitimate transmitters is binary power control. Note that Theorem 2 extends the results for the SISO MAC-WT systems considered in [11]. Based on this theorem, the optimal solution $q_i^\star$ for (19) can be found by searching over $2^K - 1$ candidates.

V. Simulation Results

In this section, we provide numerical results evaluating the performance of the proposed algorithms. In the simulations, we set the input covariance constraint matrices $\{\mathbf{S}_i\}$ as $\mathbf{S}_i = \mathbf{S}, \forall i$, where $\mathbf{S} \succeq \mathbf{0}$ is randomly generated such that $\mathrm{tr}(\mathbf{S}) = P$, i.e., we consider the average power constraint. Then, the signal-to-noise ratio (SNR) is defined as P. For convenience, we adopt the notation (N_T, N_R, N_E, K) to represent a K-user MAC-WT with N_T, N_R, and N_E being the number of antennas at legitimate transmitters, a legitimate receiver, and an eavesdropper, respectively.

Fig. 2 compares the convergence behavior of the MM algorithm and the proposed algorithm for SNR $= 10$ dB and $\beta = 1$. We can see that the proposed algorithm converges faster than the MM algorithm, while two algorithms exhibit the same average sum secrecy rate performance. This means that the proposed algorithm reduces both the computational complexity and the required number of iterations. In a $(4, 4, 4, 4)$ system, the proposed algorithm achieves about 92 % reduction in terms of the average running time.

Fig. 3 depicts the average sum secrecy rate performance as a function of SNR with $\beta = 2$ for various antenna configurations. Here, the naive precoding method chooses the covariance matrix as $\mathbf{Q}_i = \mathbf{S}_i$ which is optimal for $\mathbf{G}_i = \mathbf{0}$, i.e., when there is no eavesdropper. In addition, the TDMA scheme determines each legitimate transmitter's optimal covariance matrix from (5) and identifies the optimal transmit time duration by numerical line search as in [11]. It is observed that the naive precoding exhibits the worst performance in all cases. When the legitimate nodes have multiple antennas, the proposed algorithm outperforms the TDMA scheme, while two schemes have similar performance

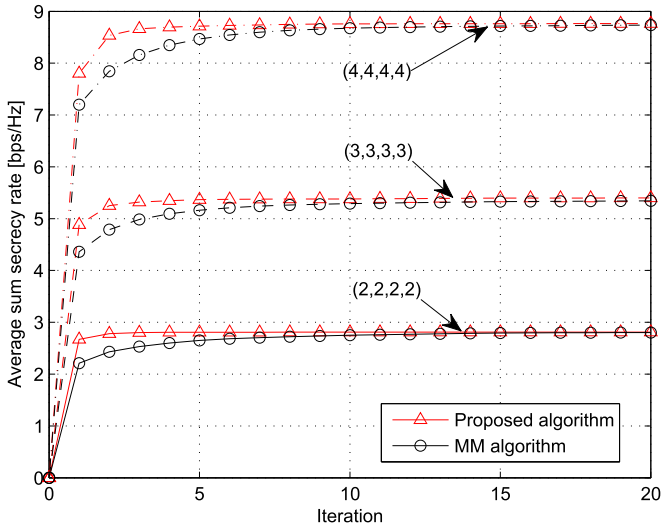

Fig. 2. Convergence behavior of the MM algorithm and the proposed scheme with SNR $= 10$ dB and $\beta = 1$.

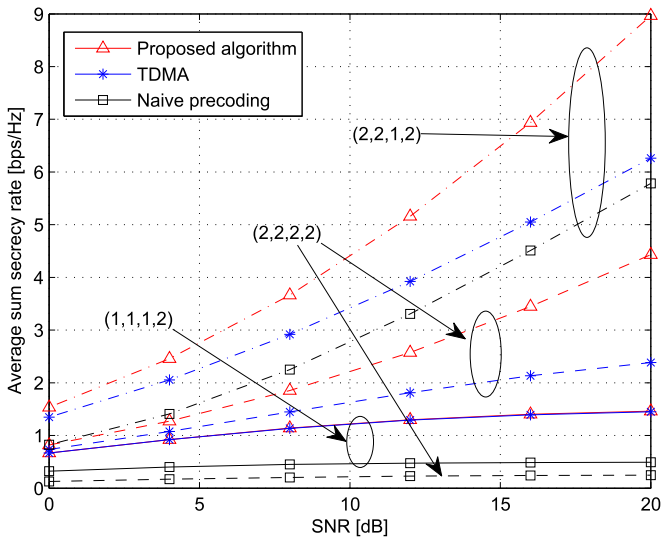

Fig. 3. Average sum secrecy rate performance as a function of SNR with $\beta = 2$.

in a SISO system $(1, 1, 1, 2)$ [11]. Also, as we can see from the curve of a $(2, 2, 2, 2)$ system, the proposed algorithm substantially improves the secrecy performance compared to the SISO MAC-WT even when the eavesdropper has multiple antennas. These observations indicate that unlike the SISO MAC-WT in [11], the proposed scheme is crucial in the MIMO MAC-WT for enhancing the sum secrecy rate performance.

In Fig. 4, we plot the average sum secrecy rate performance as a function of the number of antennas $N = N_T = N_R$ with $N_E = 3$, $K = 2$, and SNR $= 10$ dB. We can see that the performance gap between the proposed algorithm and the TDMA increases as the number of antennas grows. It is emphasized that a performance gain over the naive precoding for $\beta = 1$ and 2 equals 27% and 49% when $N = 7$, respectively. Therefore, we

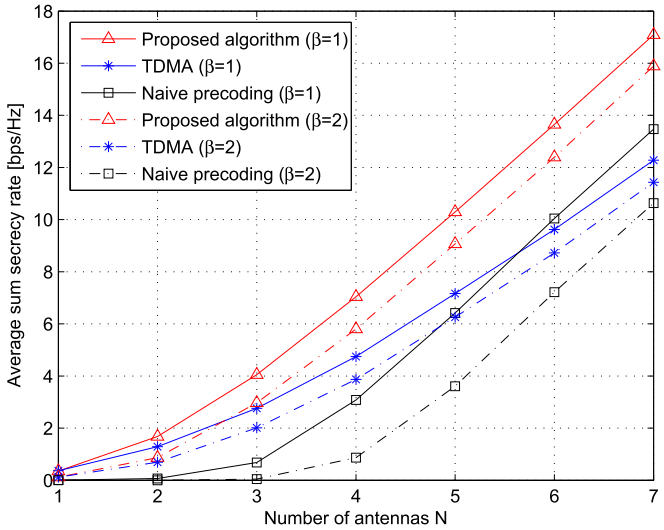

Fig. 4. Average sum secrecy rate performance as a function of the number of antennas with $N_E = 3$, $K = 2$, and SNR $= 10$ dB.

can conclude that the proposed precoding is more efficient when the channel gain (or path gain) of the eavesdropper is larger than that of the legitimate receiver.

VI. Conclusion

In this paper, we have studied low complexity precoding methods for MIMO MAC-WT which maximize the sum secrecy rate performance. By examining the KKT conditions, it has been shown that the proposed precoding scheme achieves the same performance as the conventional MM algorithm with much reduced complexity. We have also provided the global optimal solutions for MISO and SIMO MAC-WT cases. Simulation results have confirmed the effectiveness of the proposed precoding algorithm.

References

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, pp. 1550–1573, Mar. 2014.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[3] H. Lee, B. Lee, and I. Lee, "Iterative detection and decoding with an improved V-BLAST for MIMO-OFDM systems," *IEEE J. Sel. Areas Commun.*, vol. 24, pp. 504–513, Mar. 2006.

[4] K.-J. Lee, H. Sung, E. Park, and I. Lee, "Joint optimization for one and two-way MIMO AF multiple-relay systems," *IEEE Trans. Wireless Commun.*, vol. 9, no. 12, pp. 3671–3681, Dec. 2010.

[5] H. Sung, S.-H. Park, K.-J. Lee, and I. Lee, "Linear precoder designs for K-user interference channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 1, pp. 291–301, Jan. 2010.

[6] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[7] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[8] S. A. A. Fakkorian and A. L. Swindlehurst, "On the optimality of linear precoding for secrecy in the MIMO broadcast channel," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1701–1713, Sep. 2013.

[9] D. Park, "Weighted sum rate maximization of MIMO broadcast and interference channels with confidential messages," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 1742–1753, Mar. 2016.

[10] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[11] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[12] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 5747–5755, Dec. 2008.

[13] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 957–961.

[14] 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.

[15] R. Liu, Y. Liang, and H. V. Poor, "Fading cognitive multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4992–5005, Aug. 2011.

[16] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian multiple access wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 1337–1341.

[17] X. He, A. Khisti, and A. Yener, "MIMO multiple access channel with an arbitrarily varying eavesdropper: Secrecy degrees of freedom," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4733–4745, Aug. 2013.

[18] P. Mukherjee and S. Ulukus, "Secure degrees of freedom of the MIMO multiple access wiretap channel," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Nov. 2015, pp. 554–558.

[19] Y. Choi and D. Kim, "Performance analysis with and without torch node in secure communications," in *Proc. IEEE Int. Conf. Adv. Technol. Commun.*, Oct. 2015, pp. 84–87.

[20] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2009, pp. 2602–2606.

[21] H.-B. Kong, C. Song, H. Park, and I. Lee, "Shaping power constrained transceiver designs for MIMO AF relaying systems with direct link," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 294–304, Jan. 2015.

[22] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.

[23] M. Hong, Q. Li, and Y.-F. Liu, "Decomposition by successive convex approximation: A unifying approach for linear transceiver design in heterogeneous networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1377–1392, Feb. 2016.

[24] S. Boyd and L. Vanderberghe, *Convex Optimization*. Cambridge, UK: Cambridge Univ. Press, 2004.

[25] M. Hong, M. Razaviyayn, Z.-Q. Luo, and J.-S. Pang, "Unified algorithm framework for block-structured optimization involving big data: With applications in machine learning and signal processing," *IEEE Signal Process. Mag.*, vol. 33, no. 1, pp. 57–77, Jan. 2016.

[26] H. Sung, S.-R. Lee, and I. Lee, "Generalized channel inversion methods for multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 57, no. 11, pp. 3489–3499, Nov. 2009.

[27] W. Dinkelbach, "On nonlinear fractional programming," *Manage. Sci.*, vol. 13, pp. 493–498, Mar. 1967.