Constant Modulus Beamforming for Large-Scale MISOME Wiretap Channel

Qiang Li, Chao Li and Jingran Lin
School of Communication and Information Engineering,
University of Electronic Science and Technology of China, P. R. China,
Chengdu, 611731
Email: lq@uestc.edu.cn

***Abstract*—The multi-input single-output multi-eavesdropper (MISOME) wiretap channel is one of the generic wiretap channels in physical layer security. In Khisti and Wornell's classical work [1], the optimal secure beamformer for MISOME has been derived under the total power constraint. In this work, we revisit the MISOME wiretap channel and focus on the large-scale transmit antenna regime and the constant modulus beamformer design. The former is motivated by the significant spectral efficiency gains provided by massive antennas, and the latter is due to the consideration of cheap hardware implementation of constant modulus beamforming. However, from an optimization point of view, the secrecy beamforming with constant modulus constraints is challenging, more specifically, NP-hard. In light of this, we propose two methods to tackle it, namely the semidefinite relaxation (SDR) method and the ADMM-Dinkelbach method. Simulation results demonstrate that the ADMM-Dinkelbach method outperforms the SDR method, and can attain nearly optimal secrecy performance for the large-scale antenna scenario.**

I. Introduction

The multi-input single-output multi-eavesdropper wiretap channel, coined MISOME for short, is one of the generic wiretap channels studied in physical-layer security. In the classical work [1], Khisti and Wornell proved that transmit beamforming is optimal for achieving the secrecy capacity of MISOME. Transmit beamforming is a simple, yet effective way of conveying information. Recent studies show that with massive transmit antennas transmit beamforming can provide substantial spectral efficiency gains, and attain nearly optimal performances [2]–[4]. Despite the effectiveness of large-scale array beamforming, the increase of the number of transmit antennas would also scale up hardware costs, as each antenna usually requires a dedicated RF chain. In light of this, the works [5]–[9] studied constant envelope/modulus precoding for massive MIMO by fixing the amplitude and changing only the phase of the transmit signal at each antenna. The main advantage of the constant modulus precoding is that it can be easily implemented with a single RF chain by using phase shifters and a cheap variable gain amplifier [8].

In this work, we revisit the secure beamforming problem for the MISOME wiretap channel, with a focus on the large-scale transmit antenna regime and constant modulus beamforming (CMB). It is well known that under the total transmit power constraint, the optimal secure beamforming for the MISOME wiretap channel is obtained as the principle generalized eigenvector associated with the legitimate channel and the eavesdropping one [1]. However, under the CMB requirement the principle generalized eigenvector is generally no longer optimal or even feasible; it is thus needed to take CMB constraints explicitly into the secure beamforming design.

In view of this, we formulate a secure CMB problem for secrecy capacity maximization of the MISOME wiretap channel. Owing to the CMB constraints, the secrecy capacity maximization problem is generally NP-hard. To tackle it, two approximate methods are proposed. The first one is based on the semidefinite relaxation (SDR), which has been widely used for beamformer designs in the literature [10]–[13] with satisfactory performance. However, for large-scale transmit antennas, SDR-based approach may suffer from high computational complexity, owing to lifting the variable dimension. To circumvent the dimensionality problem, we further propose a low-complexity nonconvex alternating direction method of multipliers (ADMM)-based Dinkelbach approach [14], which works directly over the vector variable space. The ADMM-Dinkelbach method iteratively solves a sequence of nonconvex subproblems via nonconvex ADMM. Inspired by [15], we show that the nonconvex ADMM converges to a Karush-Kuhn-Tucker (KKT) point of the subproblem. The preliminary simulation results demonstrate that the ADMM-Dinkelbach method outperforms the SDR method in both secrecy performance and computational complexity.

II. System Model and Problem Statement

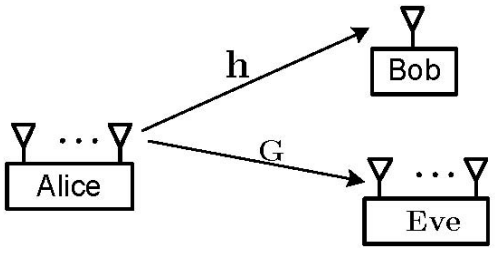


Fig. 1. The MISOME wiretap channel model.

Consider the generic MISOME wiretap channel in Figure 1, where a transmitter, named Alice, employs a large-scale antenna array to send information to a single-antenna receiver, named Bob, and a multiantenna eavesdropper, named Eve,

ISBN 978-0-9928626-7-1 © EURASIP 2017

overhears the transmission. Assuming that transmit beamforming is applied at Alice, the transmit signal may be expressed as

$$\boldsymbol{x}(t) = \boldsymbol{w}s(t), \tag{1}$$

where $s(t) \in \mathbb{C}$ is coded confidential information with unit power, and $\boldsymbol{w} \in \mathbb{C}^N$ is the transmit beamformer with constant modulus, i.e.,

$$|w_i| = \sqrt{P}, \quad \forall i = 1, \ldots, N. \tag{2}$$

where $P > 0$ represents the per-antenna transmit power. The received signal at Bob and Eve are given by

$$y_b(t) = \boldsymbol{h}^H \boldsymbol{x}(t) + n_b(t) \in \mathbb{C} \tag{3}$$

and

$$\boldsymbol{y}_e(t) = \boldsymbol{G}^H \boldsymbol{x}(t) + \boldsymbol{n}_e(t) \in \mathbb{C}^M, \tag{4}$$

respectively (resp.), where M is the number of antennas at Eve, $n_b(t) \sim \mathcal{CN}(0, 1)$ and $\boldsymbol{n}_e(t) \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{I})$ are additive Gaussian noise; $\boldsymbol{h} \in \mathbb{C}^N$ and $\boldsymbol{G} \in \mathbb{C}^{N \times M}$ denote the channels from Alice to Bob and to Eve, resp.

According to (1)-(4), the secrecy capacity of the MISOME is expressed as [1]:

$$R_s(\boldsymbol{w}) = \left[\log(1 + |\boldsymbol{h}^H \boldsymbol{w}|^2) - \log(1 + \|\boldsymbol{G}^H \boldsymbol{w}\|^2)\right]^+ \tag{5}$$

where $[\cdot]^+ = \max\{0, \cdot\}$. Now, our goal is to maximize the secrecy capacity $R_s(\boldsymbol{w})$ by optimizing the beamformer $\boldsymbol{w}$ under the constant modulus constraints, viz.,

$$\max_{\boldsymbol{w} \in \mathbb{C}^N} \ R_s(\boldsymbol{w}) \tag{6a}$$

$$\text{s.t. } |w_i| = \sqrt{P}, \ i = 1, \ldots, N. \tag{6b}$$

It is well known that Problem (6) has a closed-form optimal solution (i.e., the principle generalized eigenvector of $\boldsymbol{h}$ and $\boldsymbol{G}$), when the total power constraint is imposed [1]. However, under the constant modulus constraint, problem (6) becomes very difficult to solve. In particular, the following result identifies the complexity of solving problem (6).

Proposition 1. *Problem* (6) *is NP-hard in general.*

Proof. We need the following lemma, which is established in the proof of Proposition 3.3 in [16]:

Lemma 1. *Consider the following problem*

$$\begin{aligned} \min_{\boldsymbol{w} \in \mathbb{C}^N} \ & \boldsymbol{w}^H \boldsymbol{Q} \boldsymbol{w} \\ \text{s.t. } & |w_i| = 1, \ i = 1, \ldots, N. \end{aligned} \tag{7}$$

for some $\boldsymbol{Q} \succeq \boldsymbol{0}$. Then, problem (7) *is NP-hard in general.*

Let us show that problem (6) includes problem (7) as a special case, thereby establishing NP-hardness of problem (6). It is easy to see that problem (6) is equivalent to

$$\min_{\boldsymbol{w} \in \mathbb{C}^N} \ \frac{1 + \|\boldsymbol{G}^H \boldsymbol{w}\|^2}{1 + |\boldsymbol{h}^H \boldsymbol{w}|^2} \tag{8a}$$

$$\text{s.t. } |w_i| = \sqrt{P}, \ i = 1, \ldots, N. \tag{8b}$$

Let us consider a special case of problem (8) via setting $\boldsymbol{h} = [1, 0, \ldots, 0]$ and $P = 1$. Then, we have $|\boldsymbol{h}^H \boldsymbol{w}|^2 = |w_1|^2 = 1$ for any feasible $\boldsymbol{w}$, and thus problem (8) can be further simplified as

$$\min_{\boldsymbol{w} \in \mathbb{C}^N} \ \boldsymbol{w}^H (\boldsymbol{G}\boldsymbol{G}^H) \boldsymbol{w} \tag{9a}$$

$$\text{s.t. } |w_i| = 1, \ i = 1, \ldots, N, \tag{9b}$$

which is exactly the same as problem (7) by setting $\boldsymbol{Q} = \boldsymbol{G}\boldsymbol{G}^H \succeq \boldsymbol{0}$. ∎

In light of Proposition 1, in the following sections we focus on finding some high-quality approximate solutions for problem (6).

III. An SDR Approach to Problem (6)

Notice that in (8), the magnitude of w_i can be normalized to one by multiplying the channels with $\sqrt{P}$. Therefore, problem (8) can be reexpressed as

$$\min_{\boldsymbol{w} \in \mathbb{C}^N} \ \frac{\boldsymbol{w}^H (\frac{1}{N}\boldsymbol{I} + P\boldsymbol{G}\boldsymbol{G}^H) \boldsymbol{w}}{\boldsymbol{w}^H (\frac{1}{N}\boldsymbol{I} + P\boldsymbol{h}\boldsymbol{h}^H) \boldsymbol{w}} \tag{10a}$$

$$\text{s.t. } |w_i| = 1, \ i = 1, \ldots, N. \tag{10b}$$

By denoting $\boldsymbol{W} = \boldsymbol{w}\boldsymbol{w}^H$ and dropping the rank-one constraint on $\boldsymbol{W}$, we get an SDR of (10), viz.,

$$\min_{\boldsymbol{W} \in \mathbb{H}^N} \ \frac{\mathrm{Tr}(\boldsymbol{W}(\frac{1}{N}\boldsymbol{I} + P\boldsymbol{G}\boldsymbol{G}^H))}{\mathrm{Tr}(\boldsymbol{W}(\frac{1}{N}\boldsymbol{I} + P\boldsymbol{h}\boldsymbol{h}^H))} \tag{11a}$$

$$\text{s.t. } W_{ii} = 1, \ i = 1, \ldots, N, \tag{11b}$$

$$\boldsymbol{W} \succeq \boldsymbol{0}. \tag{11c}$$

Problem (11) can be rewritten as an SDP by applying the Charnes-Cooper transformation [13]. In particular, by making a change of variable $\boldsymbol{W} = \tilde{\boldsymbol{W}}/\zeta$ for some $\zeta \geq 0$, problem (11) can be equivalently written as

$$\min_{\tilde{\boldsymbol{W}} \in \mathbb{H}^N, \zeta} \ \mathrm{Tr}(\tilde{\boldsymbol{W}}(\frac{1}{N}\boldsymbol{I} + P\boldsymbol{G}\boldsymbol{G}^H)) \tag{12a}$$

$$\text{s.t. } \mathrm{Tr}\big(\tilde{\boldsymbol{W}}(\frac{1}{N}\boldsymbol{I} + P\boldsymbol{h}\boldsymbol{h}^H)\big) = 1, \tag{12b}$$

$$\tilde{W}_{ii} = \zeta, \ i = 1, \ldots, N, \tag{12c}$$

$$\tilde{\boldsymbol{W}} \succeq \boldsymbol{0}, \quad \zeta \geq 0, \tag{12d}$$

which is an SDP and can be solved to global optimality with general purposed conic solvers. In general, the SDR is not tight, i.e., the solution of problem (12) may not be of rank one. In such a case, eigenvalue decomposition and projection are needed to extract a feasible solution for problem (6). Algorithm 1 summarizes the SDR-based approach to (6).

IV. An ADMM-Dinkelbach Approach to (6)

As mentioned in Introduction, for large-scale antenna scenario the SDR method may suffer from the curse of dimensionality. Nevertheless, the SDR method is still meaningful as it may serve as a benchmark. In this section, we propose another low-complexity algorithm for problem (6), which can better explore the problem structure.

ISBN 978-0-9928626-7-1 © EURASIP 2017

Algorithm 1 An SDR Approach to Problem (6)

1: Solve problem (12) to obtain $(\tilde{\boldsymbol{W}}^\star, \zeta^\star)$ and let $\boldsymbol{W}^\star = \tilde{\boldsymbol{W}}^\star/\zeta^\star$
2: **if** $\mathrm{rank}(\boldsymbol{W}^\star) \leq 1$ **then**
3: Perform eigendecomposition $\boldsymbol{W}^\star = \boldsymbol{w}^\star(\boldsymbol{w}^\star)^H$ and output $\sqrt{P}\boldsymbol{w}^\star$ as an optimal solution of (6).
4: **else**
Let $\boldsymbol{v}$ be the principle eigenvector of $\boldsymbol{W}^\star$ and output $\boldsymbol{w} = \sqrt{P}\exp(j\angle \boldsymbol{v})$ as an approximate solution of (6).
5: **end if**

To proceed, notice that the objective in (10) is a ratio of quadratic functions. A classical way to handle this fractional objective is the Dinkelbach method [14], which translates the fractional program into a sequence of quadratic programs. Algorithm 2 summarizes the main procedure of the Dinkelbach method for problem (10). According to the classical convergence result of the Dinkelbach method [14], Algorithm 2 converges to an optimal solution of (10) whenever problem (13) is optimally solved throughout the iterations. Unfortunately, problem (13) can be as hard as the original problem (10). As a compromise, we propose to apply ADMM method to approximately solve (13), which is detailed in the remaining part of this section.

Algorithm 2 A Dinkelbach Approach to Problem (10)

1: Initialize a feasible $\boldsymbol{w}$ for (10)
2: **repeat**
3: $\eta \leftarrow \frac{\boldsymbol{w}^H(\frac{1}{N}\boldsymbol{I}+P\boldsymbol{G}\boldsymbol{G}^H)\boldsymbol{w}}{\boldsymbol{w}^H(\frac{1}{N}\boldsymbol{I}+P\boldsymbol{h}\boldsymbol{h}^H)\boldsymbol{w}}$
4:
$$\boldsymbol{w} \leftarrow \arg\min_{\boldsymbol{w}\in\mathbb{C}^N} \boldsymbol{w}^H(\boldsymbol{G}\boldsymbol{G}^H - \eta\boldsymbol{h}\boldsymbol{h}^H)\boldsymbol{w} \quad \text{s.t. } |w_i| = 1,\ i = 1,\ldots,N. \tag{13}$$
5: **until** some stopping criterion is satisfied
6: **Output** $\boldsymbol{w}$.

Notice that under the unit modulus constraints the objective of problem (13) can be turned into convex by adding some sufficiently large constant. Therefore, problem (13) can be equivalently written as

$$\min_{\boldsymbol{w}\in\mathbb{C}^N} \frac{1}{2}\boldsymbol{w}^H\boldsymbol{A}\boldsymbol{w} \quad \text{s.t. } |w_i| = 1,\ i = 1,\ldots,N, \tag{14}$$

where $\boldsymbol{A} \triangleq \boldsymbol{G}\boldsymbol{G}^H - \eta\boldsymbol{h}\boldsymbol{h}^H - \lambda_{\min}(\boldsymbol{G}\boldsymbol{G}^H - \eta\boldsymbol{h}\boldsymbol{h}^H)\boldsymbol{I} \succeq \boldsymbol{0}$. To fit problem (14) into the ADMM framework, let us rewrite problem (14) as

$$\min_{\boldsymbol{w},\boldsymbol{x}\in\mathbb{C}^N} \frac{1}{2}\boldsymbol{w}^H\boldsymbol{A}\boldsymbol{w} \quad \text{s.t. } |x_i| = 1,\ i = 1,\ldots,N,\ \boldsymbol{x} = \boldsymbol{w}. \tag{15}$$

Its augmented Lagrangian reads

$$\mathcal{L}(\boldsymbol{x},\boldsymbol{w},\boldsymbol{\nu}) = \frac{1}{2}\boldsymbol{w}^H\boldsymbol{A}\boldsymbol{w} + \mathrm{Re}\{\boldsymbol{\nu}^H(\boldsymbol{x}-\boldsymbol{w})\} + \frac{\rho}{2}\|\boldsymbol{x}-\boldsymbol{w}\|^2$$

where $\rho > 0$ and $\boldsymbol{\nu} \in \mathbb{C}^N$ is Lagrangian multiplier associated with the second equality constraint. Let $(\boldsymbol{x}^0, \boldsymbol{w}^0, \boldsymbol{\nu}^0)$ be the initialized primal-dual variables. The ADMM method for (13) consists of the following three steps:

$$\begin{cases} \boldsymbol{x}^{k+1} = \arg\min_{|\boldsymbol{x}|=1} \mathcal{L}(\boldsymbol{x}, \boldsymbol{w}^k, \boldsymbol{\nu}^k), & (16)\\ \boldsymbol{w}^{k+1} = \arg\min_{\boldsymbol{w}} \mathcal{L}(\boldsymbol{x}^{k+1}, \boldsymbol{w}, \boldsymbol{\nu}^k), & (17)\\ \boldsymbol{\nu}^{k+1} = \boldsymbol{\nu}^k + \rho(\boldsymbol{x}^{k+1} - \boldsymbol{w}^{k+1}) & (18)\end{cases}$$

for $k = 0, 1, \ldots$. The subproblem (16) is equivalent to

$$\max_{|\boldsymbol{x}|=1} \|\boldsymbol{x} - (\boldsymbol{w}^k - \rho^{-1}\boldsymbol{\nu}^k)\|^2,$$

which has a closed-form solution

$$(\boldsymbol{x}^{k+1})_i = \begin{cases} \frac{(\boldsymbol{w}^k - \rho^{-1}\boldsymbol{\nu}^k)_i}{|(\boldsymbol{w}^k - \rho^{-1}\boldsymbol{\nu}^k)_i|}, & \text{if } (\boldsymbol{w}^k - \rho^{-1}\boldsymbol{\nu}^k)_i \neq 0 \\ (\boldsymbol{x}^k)_i, & \text{otherwise} \end{cases} \tag{19}$$

The subproblem (17) is an unconstrained least-squares problem. Take the first-order derivative and set it to zero to get

$$\boldsymbol{A}\boldsymbol{w}^{k+1} - \boldsymbol{\nu}^k - \rho(\boldsymbol{x}^{k+1} - \boldsymbol{w}^{k+1}) = \boldsymbol{0} \tag{20}$$

Rearranging the above terms yields

$$\boldsymbol{w}^{k+1} = (\rho\boldsymbol{I} + \boldsymbol{A})^{-1}(\rho\boldsymbol{x}^{k+1} + \boldsymbol{\nu}^k). \tag{21}$$

Also, it follows from (18) and (20) that

$$\boldsymbol{\nu}^{k+1} = \boldsymbol{A}\boldsymbol{w}^{k+1}, \quad \forall\ k. \tag{22}$$

Algorithm 3 summarizes the main steps of ADMM for (13).

Algorithm 3 A Nonconvex ADMM Approach to (13)

1: Initialize with a feasible primal-dual point $(\boldsymbol{x}^0, \boldsymbol{w}^0, \boldsymbol{\nu}^0)$, choose $\rho > 0$ and set $k = 0$
2: **repeat**
3: Compute $\boldsymbol{x}^{k+1}$ by (19);
4: Compute $\boldsymbol{w}^{k+1}$ by (21);
5: Compute $\boldsymbol{\nu}^{k+1}$ by (22);
6: $k \leftarrow k + 1$
7: **until** some stopping criterion is satisfied
8: **Output** $(\boldsymbol{x}^k, \boldsymbol{w}^k, \boldsymbol{\nu}^k)$.

Since problem (13) is a nonconvex problem, Algorithm 3 in general has no convergence guarantee. Nevertheless, with some appropriately chosen parameter ρ, we establish the following convergence for Algorithm 3.

Proposition 2. *Suppose* $\rho > \max\{\sqrt{2\lambda_{\max}(\boldsymbol{A})}, \lambda_{\max}(\boldsymbol{A})\}$. *Then, every limit point generated by Algorithm 3 is a KKT point of problem* (14).

Proof. The proof follows from [15] with some modification in order to address the nonconvex unit modulus constraints. Owing to the page limit, herein we provide a sketched proof.

First of all, we show sufficient decrease of the augmented Lagrangian function $\mathcal{L}(\boldsymbol{x}^k, \boldsymbol{w}^k, \boldsymbol{\nu}^k)$ after one cycle of the primal-dual update in (16)-(18), i.e.,

$$\mathcal{L}(\boldsymbol{x}^k, \boldsymbol{w}^k, \boldsymbol{\nu}^k) - \mathcal{L}(\boldsymbol{x}^{k+1}, \boldsymbol{w}^{k+1}, \boldsymbol{\nu}^{k+1}) \geq \tilde{\theta}\|\boldsymbol{w}^{k+1} - \boldsymbol{w}^k\|^2, \tag{23}$$

ISBN 978-0-9928626-7-1 © EURASIP 2017

where $\tilde{\theta} \triangleq \frac{\rho}{2} - \rho^{-1}\lambda_{\max}(\boldsymbol{A}) > 0$ due to $\rho > \sqrt{2\lambda_{\max}(\boldsymbol{A})}$.

Secondly, we show that $\mathcal{L}(\boldsymbol{x}^k, \boldsymbol{w}^k, \boldsymbol{\nu}^k)$ is lower bounded below, i.e.,

$$\mathcal{L}(\boldsymbol{x}^k, \boldsymbol{w}^k, \boldsymbol{\nu}^k) \geq 0, \ \forall \ k. \tag{24}$$

Thirdly, by (23) and (24), we can establish the following limit:

$$\lim_{k\to\infty} \{\boldsymbol{w}^{k+1} - \boldsymbol{w}^k\} = \boldsymbol{0} \tag{25}$$

which together with (22) and (18) implies

$$\lim_{k\to\infty} \{\boldsymbol{\nu}^{k+1} - \boldsymbol{\nu}^k\} = \boldsymbol{0}, \quad \lim_{k\to\infty} \{\boldsymbol{x}^{k+1} - \boldsymbol{w}^{k+1}\} = \boldsymbol{0}. \tag{26}$$

Let $\boldsymbol{w}^{k_j}$ be any converging subsequence of $\boldsymbol{w}^k$ with the limit point $\bar{\boldsymbol{w}}$. Then it follows from (25), (26) and (22) that

$$\lim_{k_j\to\infty} \boldsymbol{w}^{k_j+1} = \lim_{k_j\to\infty} \boldsymbol{w}^{k_j} = \bar{\boldsymbol{w}} \tag{27a}$$

$$\lim_{k_j\to\infty} \boldsymbol{x}^{k_j+1} = \lim_{k_j\to\infty} \boldsymbol{w}^{k_j+1} = \bar{\boldsymbol{w}} \tag{27b}$$

$$\lim_{k_j\to\infty} \boldsymbol{\nu}^{k_j} = \lim_{k_j\to\infty} \boldsymbol{\nu}^{k_j+1} = \lim_{k_j\to\infty} \boldsymbol{A}\boldsymbol{w}^{k_j+1} = \boldsymbol{A}\bar{\boldsymbol{w}} \tag{27c}$$

In particular, (27b) implies that

$$|\bar{w}_i| = 1, \quad i = 1, \ldots, N. \tag{28}$$

Moreover, since $\boldsymbol{x}^{k+1}$ is a minimizer of $\mathcal{L}(\boldsymbol{x}, \boldsymbol{w}^k, \boldsymbol{\nu}^k)$ w.r.t. $\boldsymbol{x}$, we have

$$\mathcal{L}(\boldsymbol{x}, \boldsymbol{w}^k, \boldsymbol{\nu}^k) \geq \mathcal{L}(\boldsymbol{x}^{k+1}, \boldsymbol{w}^k, \boldsymbol{\nu}^k), \tag{29}$$

for all feasible $\boldsymbol{x}$. Taking limit along the subsequence k_j in the above inequality yields

$$\begin{aligned} &\lim_{k_j\to\infty} \mathcal{L}(\boldsymbol{x}, \boldsymbol{w}^{k_j}, \boldsymbol{\nu}^{k_j}) \\ =&\mathcal{L}(\boldsymbol{x}, \bar{\boldsymbol{w}}, \boldsymbol{A}\bar{\boldsymbol{w}}) \\ \geq &\lim_{k_j\to\infty} \mathcal{L}(\boldsymbol{x}^{k_j+1}, \boldsymbol{w}^{k_j}, \boldsymbol{\nu}^{k_j}) \\ =&\mathcal{L}(\bar{\boldsymbol{w}}, \bar{\boldsymbol{w}}, \boldsymbol{A}\bar{\boldsymbol{w}}) \end{aligned} \tag{30}$$

for all feasible $\boldsymbol{x}$. That is, $\bar{\boldsymbol{w}}$ is an optimal solution of $\mathcal{L}(\boldsymbol{x}, \bar{\boldsymbol{w}}, \boldsymbol{A}\bar{\boldsymbol{w}})$; thus satisfying the following first-order optimality condition:

$$\boldsymbol{A}\bar{\boldsymbol{w}} + \boldsymbol{\zeta} \odot \bar{\boldsymbol{w}} = \boldsymbol{0} \tag{31}$$

where $\boldsymbol{\zeta} \in \mathbb{R}^N$ is the dual variable associated with the unit modulus constraints, and $\odot$ denotes elementwise product. It is easy to verify that Eqn. (31) and (28) form the KKT conditions of problem (14). ■

V. Simulation Results

We use Monte-Carlo simulations to verify the effectiveness of our design. The following simulation settings are used, unless otherwise specified: The number of receive antenna at Eve is $M = 20$. For the ADMM-Dinkelbach method, the inner ADMM algorithm sets ρ according to Proposition 2, and stops when $\|\boldsymbol{x}^k - \boldsymbol{w}^k\|_2 / \|\boldsymbol{x}^k\|_2 \leq 10^{-5}$, while the outer Dinkelbach iteration is executed until the successive difference of η is smaller than 10^{-2} or a maximum number of 50 iterations achieves. All the channels are randomly generated with i.i.d. standard complex Gaussian distribution. All the results were averaged over 1,000 random channel realizations.

In the first example, we study the average secrecy rate performance of different designs when increasing the total transmit power $P_{\text{total}} = NP$ from 0dB to 14dB. Fig. 2(a) shows the results for $N = 20$ and $M = 20$. In the legend, "Dinkelbach CM BF" and "SDR CM BF" correspond to the proposed constant modulus beamforming designs in Sec. III and IV, respectively; "Generalized eigenvector CM BF" represents the secrecy rate obtained by naively projecting the generalized eigenvector beamformer in [1] onto the circle. Since the optimal rate of problem (6) is generally not known, we instead consider a secrecy rate upper bound calculated from the SDR solution $\boldsymbol{W}^\star$ in (11), which is labeled as "Rate upper bound". From Fig. 2(a) we see that with the increase of the total power, the secrecy rates of Dinkelbach method and the SDR method both increase, and the former is slightly better than the latter. On the other hand, the secrecy rate of generalized eigenvector beamforming tends to decrease, because the generalized eigenvector beamforming is optimized under the total power constraint; after projection, there is no performance guarantee for the generalized eigenvector beamforming. To test the performance of the designs under large-scale antenna settings, we further increase N to 50 and 100, and keep $M = 20$. The result is shown in Fig. 2(b) and (c), resp. From the figures, we see that the performance of Dinkelbach method is far better than the SDR method, and the former is very close to the rate upper bound, which implies that the Dinkelbach method actually can find a nearly optimal solution for problem (6) under the considered setting.

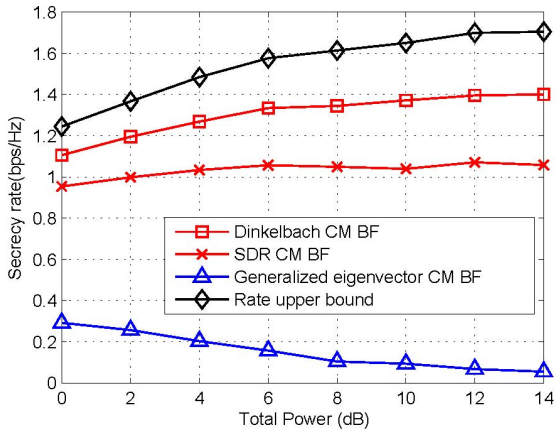
To further demonstrate the superior performance of the Dinkelbach method, we record the running times of the Dinkelbach method and the SDR method for the first 20 randomly generated channel realizations under the setting of Fig. 2(b). The result is shown in Fig. 3. From the figure, we see that the Dinkelbach method runs much faster than the SDR method. This is mainly attributed to the efficient closed-form updates of the ADMM.

VI. Conclusion

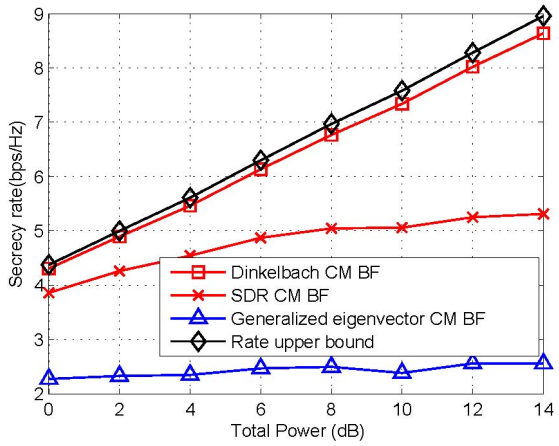
We have considered a constant modulus secrecy beamforming design for the MISOME wiretap channel. Due to constant modulus constraints, the resultant secrecy rate maximization (SRM) problem is no longer tractable. To tackle this SRM problem, two different methods have been proposed. One is based on the widely used SDR technique, and the other is the ADMM-based Dinkelbach method. Numerical results demonstrate that the Dinkelbach method is superior to the SDR method in both the rate performance and the running time. Moreover, for the tested large-scale antenna settings, the Dinkelbach method is able to approach the optimal secrecy rate.

VII. Acknowledgement

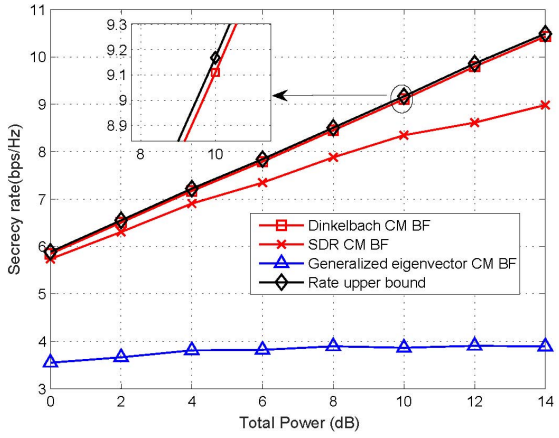
This work was supported in part by the National Natural Science Foundation of China under Grants 61401073,



(a)



(b)



(c)

Fig. 2. Total transmit power vs. secrecy rate (a) $N = 20$, (b) $N = 50$, and (c) $N = 100$.

61531009, 61671120, and in part by the Fundamental Research Funds for the Central Universities under Grants ZYGX2016J011 and ZYGX2016J007.

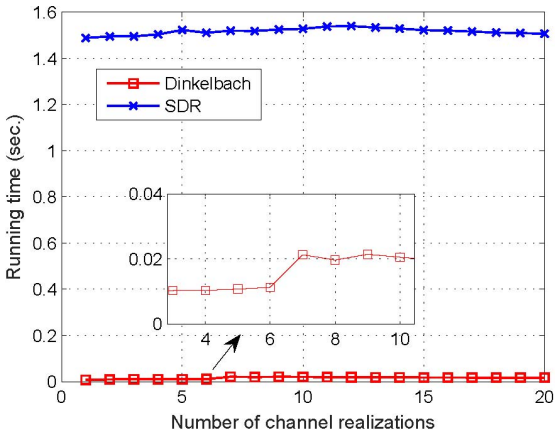


Fig. 3. Running time vs. number of channel realizations ($N = 50, M = 20, P_{\text{total}} = 6\,\text{dB}$).

REFERENCES

[1] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[2] T. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.

[3] T. L. Marzetta, "Massive MIMO: An introduction," *Bell Labs Tech. J*, vol. 20, pp. 11–22, 2015.

[4] E. Bjornson, E. G. Larsson, and T. L. Marzetta, "Massive MIMO: Ten myths and one critical question," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 114–123, Feb. 2016.

[5] S. K. Mohammed and E. G. Larsson, "Per-antenna constant envelope precoding for large multi-user MIMO systems," *IEEE Trans. Commun.*, vol. 61, no. 3, pp. 1059–1071, Mar. 2013.

[6] J. Pan and W.-K. Ma, "Constant envelope precoding for single-user large-scale MISO channels: Efficient precoding and optimal designs," *IEEE Journal Sel. Top. Sig. Process.*, vol. 8, no. 5, pp. 982–995, Oct. 2014.

[7] J.-C. Chen, C.-K. Wen, and K.-K. Wong, "Improved constant envelope multiuser precoding for massive MIMO systems," *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1311–1314, Aug. 2014.

[8] S. Zhang, R. Zhang, and T. J. Lim, "MISO multicasting with constant envelope precoding," *IEEE Wireless Commun. Lett.*, vol. 5, no. 6, pp. 1311–1314, Dec. 2016.

[9] M. Kazemi, H. Aghaeinia, and T. M. Duman, "Discrete-phase constant envelope precoding for massive MIMO systems," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2011–2021, May 2017.

[10] Q. Li, W.-K. Ma, and D. Han, "Sum secrecy rate maximization for full-duplex two-way relay networks using Alamouti-based rank-two beamforming," *IEEE Journal Sel. Top. Sig. Process.*, vol. 10, no. 8, pp. 1359–1374, Dec. 2016.

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

[12] Y. Huang and D. P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *IEEE Trans. Signal Process.*, vol. 58, no. 2, pp. 664–678, Feb. 2010.

[13] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[14] W. Dinkelbach, "On nonlinear fractional programming," *Management Science*, vol. 13, no. 7, pp. 492–498, 1967.

[15] M. Hong, Z.-Q. Luo, and M. Razaviyayn, "Convergence analysis of alternating direction method of multipliers for a family of nonconvex problems," *SIAM J. Opt.*, vol. 26, no. 1, pp. 337–364, 2016.

[16] S. Zhang and Y. Huang, "Complex quadratic optimization and semidefinite programming," *SIAM J. Opt.*, vol. 16, no. 3, pp. 871–890, 2006.

ISBN 978-0-9928626-7-1 © EURASIP 2017