OPTIMIZATION OF TRANSMIT SIGNALS TO INTERFERE AN EAVESDROPPER WITH MULTIPLE ANTENNAS

Shuichi Ohno, Yuji Wakasa, and Shui Qiang Yan*

Hiroshima University, 1-4-1 Kagamiyama, Higashi-Hiroshima, 739-8527, JAPAN
*Yamaguchi University, 2-16-1 Tokiwadai, Ube 755-8611, JAPAN

ABSTRACT

Wireless communications are susceptible to eavesdropping. To interfere the eavesdropper having multiple antennas, secret information signals and interference signals that are transmitted from multiple antennas are designed. It is shown that our design can be cast into a semidefinite program, which can be numerically solved efficiently. Simulation results are provided to demonstrate the efficiency of the proposed design.

Index Terms— security, physical-layer secrecy, eavesdropping, beamforming, convex optimization

1. INTRODUCTION

Wireless communications have become indispensable for our daily life but are susceptible to eavesdropping, since they can be overheard by receivers within a certain range in nature. Cryptography is commonly used to provide information security. However, secret key distribution necessary for the encryption remains vulnerable to eavesdropping. In this context, physical-layer secrecy, which may not have to rely on encryption, is attractive.

Physical-layer secrecy is not so new, as it can be dated back to the seminal work [1] in 1975. If the channel state information (CSI) of the eavesdropper is known, theoretically, secrecy is guaranteed if the communication rate between the transmitter and the legitimate receiver is lower than the so-called secrecy capacity, which is the maximum rate at which the transmitter can send secret information to the legitimate receiver without the secret information being decoded by the eavesdropper.

Recently, multiple-input and multiple-output (MIMO) systems, have become available and are utilized to achieve high performance. For multiple antenna systems, many efficient transmit and/or receive antenna beamforming techniques have been developed (see [2] and the references therein). Accordingly, the importance of physical-layer secrecy has been re-acknowledged, since physical-layer secrecy can be enhanced by using multiple antenna systems.

Secrecy capacity has been investigated in [3] for systems where the transmitter equipped with multiple antennas sends secret information signals as well as interference signals to interfere the eavesdropper using eavesdropper's CSI. In theory, physical-layer secrecy is improved by using cooperative relays [4] and separate transmitter that sends an interference signal [5]. Physical-layer secrecy has been characterized in [6] also, when the transmitter does not know locations and CSIs of eavesdroppers. Although physical-layer secrecy has been well studied in terms of information theory, its realization has not yet been established.

If eavesdroppers are not passive but active, then the transmitter may be able to obtain their CSI. One candidate to realize physical-layer secrecy when eavesdroppers' CSIs are available at the transmitter is the system in which the transmitter can degrade the quality of the received signals of eavesdroppers by sending interference signals, while keeping the quality of the received signals of the legitimate receiver.

In [7], designs of the signals transmitted from multiple antennas are proposed: The signal-to-interference-and-noise-ratios (SINR) of eavesdroppers are constrained to be low enough for decoding the secret information, while the SINR of the legitimate receiver is kept sufficiently large for decoding or is maximized under the transmit power constraint. Since the designs cannot be cast into convex optimization problems, semidefinite relaxation (SDR) techniques have been developed. Moreover, [7] studies the case when multiple eavesdroppers cooperate to form a joint receive beamforming to improve their SINR, which can be mathematically equivalent to the case when one eavesdropper having multiple receive antennas forms an optimal receive beamforming. In this paper, we deal with the latter case and propose a design method for the signals to be transmitted.

In addition to the minimum SINR constraint on the legitimate receiver, we set the maximum allowable SINR of the signal beamformed by the eavesdropper as in [7]. Unlike [7], we do not impose any SINR constraints on each receive antenna but impose additional constraints on the transmit beamformer and interference signals. This enables us to formulate our design problem as a convex optimization problem, which can be solved efficiently by numerical method. Simulation results are provided to demonstrate that our proposed design attains the two SINR constraints with lower transmit power than the design in [7].

2. SYSTEM MODEL AND PROBLEM STATEMENT

Let us consider a digital communication from a transmitter having N_t transmit antennas to a legitimate receiver having one receive antenna over quasi-static flat fading channels. Let $\boldsymbol{x}(t)$ be the transmitted signal vector at time t whose nth entry is the signal transmitted from the nth transmit antenna. The signal $y_b(t)$ of the legitimate receiver is modeled as

$$y_b(t) = \boldsymbol{h}^{\mathcal{H}}\boldsymbol{x}(t) + n(t) \tag{1}$$

where $\boldsymbol{h}$ is an $N_t \times 1$ channel vector, whose nth entry is the complex conjugate of the channel coefficient from the nth transmit antenna to the receiver, $()^{\mathcal{H}}$ stands for the complex conjugate transpose of a matrix or a vector, and $n(t)$ denotes an additive noise, which is assumed to be independent and identically distributed (i.i.d.) complex circular Gaussian with zero mean and variance σ_n^2.

Suppose that there is an eavesdropper having M receive antennas. The signal at the mth receive antenna can be expressed as

$$y_{e,m}(t) = \boldsymbol{g}_m^{\mathcal{H}}\boldsymbol{x}(t) + v_m(t), \quad m = 1, \ldots, M \tag{2}$$

where $\boldsymbol{g}_m$ is an $N_t \times 1$ channel vector, whose nth entry is the complex conjugate of the channel coefficient from the nth transmit antenna to the mth receive antenna of the eavesdropper, and the additive noise $v_m(t)$ at the mth receive antenna is i.i.d. complex circular Gaussian with zero mean and non-zero variance $\sigma_{v,m}^2 > 0$. We assume that $M < N_t$ and that $\{v_m(t)\}_{m=1}^M$ are independent of each other and of $n(t)$.

Following the convention, we call the transmitter, the legitimate receiver, and the eavesdropper, as Alice, Bob, and Eve, respectively.

Let the secret information data that Alice wants to inform only to Bob be $s(t)$, which is assumed to have zero mean and unit variance. Suppose Eve tries to eavesdrop $s(t)$ from the received signal vector defined as

$$\boldsymbol{y}_e(t) = [y_{e,1}(t), \ldots, y_{e,M}(t)]^T \tag{3}$$

by using receive beamforming. It should be remarked that the same model can be obtained if there are multiple eavesdroppers that collude by using their M received signals, for example, if there exist M eavesdroppers, each of which has only one receive antenna, but can utilize all $\{y_{e,m}(t)\}_{m=1}^M$ by exchanging their received signals.

To improve the signal-to-interference-and-noise-ratio (SINR) at Bob, Alice utilizes transmit beamforming. At the same time, to interfere the eavesdropping, Alice sends the interference signal $z_n(t)$ from its nth transmit antenna. This is so-called artificial noise (AN) aided (transmit) beamforming, whose transmitted signal vector is expressed as

$$\boldsymbol{x}(t) = \boldsymbol{w}s(t) + \boldsymbol{z}(t) \tag{4}$$

where the nth entry of $\boldsymbol{w}$ denotes the weight at the nth transmit antenna and the interference noise vector $\boldsymbol{z}(t)$ is given by

$$\boldsymbol{z}(t) = [z_1(t), \ldots, z_{N_t}(t)]^T. \tag{5}$$

We assume that $\boldsymbol{z}(t)$ is i.i.d. circular Gaussian with zero mean and covariance matrix $\boldsymbol{\Sigma}$ which is positive semidefinite.

From (1) and (4), the SINR at Bob is found to be

$$\mathrm{SINR}_b(\boldsymbol{w}, \boldsymbol{\Sigma}) = \frac{|\boldsymbol{w}^{\mathcal{H}}\boldsymbol{h}|^2}{\boldsymbol{h}^{\mathcal{H}}\boldsymbol{\Sigma}\boldsymbol{h} + \sigma_n^2}. \tag{6}$$

On the other hand, if Eve utilizes the maximum SINR receive beamforming vector, then from (3) and (4), the SINR at Eve is expressed as

$$\mathrm{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma}) = \max_{\boldsymbol{r} \neq \boldsymbol{0}} \frac{\boldsymbol{r}^{\mathcal{H}}\boldsymbol{G}^{\mathcal{H}}\boldsymbol{w}\boldsymbol{w}^{\mathcal{H}}\boldsymbol{G}\boldsymbol{r}}{\boldsymbol{r}^{\mathcal{H}}(\boldsymbol{G}^{\mathcal{H}}\boldsymbol{\Sigma}\boldsymbol{G} + \boldsymbol{D}^2)\boldsymbol{r}} \tag{7}$$

where $\boldsymbol{r}$ denotes the receive beamforming weight at the antennas of Eve,

$$\boldsymbol{G} = [\boldsymbol{g}_1, \ldots, \boldsymbol{g}_M] \tag{8}$$

and

$$\boldsymbol{D}^2 = \mathrm{diag}(\sigma_{v,1}^2, \ldots, \sigma_{v,M}^2). \tag{9}$$

Our problem is to design the transmit beamforming vector $\boldsymbol{w}$ and the covariance $\boldsymbol{\Sigma}$ of the interference signal vector when $\boldsymbol{G}$ is available at the transmitter. More specifically, we would like to design $\boldsymbol{w}$ and $\boldsymbol{\Sigma}$ that minimizes the transmit power subject to the constraints that the SINR of Bob is larger or equal to the threshold γ_b and that the SINR of Eve is smaller or equal to γ_{ce}. Mathematically, our problem can be described as a minimization (optimization) problem:

$$\min_{\boldsymbol{w}, \boldsymbol{\Sigma}} \left(||\boldsymbol{w}||^2 + \mathrm{trace}\, \boldsymbol{\Sigma} \right) \tag{10}$$

subject to

$$\mathrm{SINR}_b(\boldsymbol{w}, \boldsymbol{\Sigma}) \geq \gamma_b \tag{11}$$

$$\mathrm{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma}) \leq \gamma_{ce}. \tag{12}$$

A similar problem has been studied in [7], where each SINR of Eve's receive antenna is constrained to be less than or equal to a threshold γ_e, such that

$$\mathrm{SINR}_{e,m}(\boldsymbol{w}, \boldsymbol{\Sigma}) = \frac{\boldsymbol{g}_m^{\mathcal{H}}\boldsymbol{w}\boldsymbol{w}^{\mathcal{H}}\boldsymbol{g}_m}{\boldsymbol{g}_m^{\mathcal{H}}\boldsymbol{\Sigma}\boldsymbol{g}_m + \sigma_{v,m}^2} \leq \gamma_e, \quad m = 1, \ldots, M. \tag{13}$$

Since the problem in [7] is NP-hard and cannot be cast into a convex optimization problem, a semidefinite relaxation (SDR) technique has been developed to obtain the solution.

However, since $\mathrm{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma})$ is the upper bound of SINR attained by eavesdropping, that is,

$$\mathrm{SINR}_{e,m}(\boldsymbol{w}, \boldsymbol{\Sigma}) \leq \mathrm{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma}), \quad \forall m \in [1, M], \tag{14}$$

then we do not require the constraints (13) in our design. This enables us to develop an efficient algorithm based on semidefinite program [8] as shown in the following section.

3. CONVEX OPTIMIZATION TO DESIGN SIGNALS TO BE TRANSMITTED FROM ALICE

Without loss of generality, we assume that $\boldsymbol{G}$ has full column rank. We also assume that $\boldsymbol{h}$ is not in the column space of $\boldsymbol{G}$.

Since $\text{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma})$ is not degraded by sending interference signal vectors orthogonal to the column space of $\boldsymbol{G}$, a possible candidate for the interference signal vector is given by

$$\boldsymbol{z}(t) = \boldsymbol{G}(\boldsymbol{G}^{\mathcal{H}}\boldsymbol{G})^{-1}\tilde{\boldsymbol{z}}(t) \tag{15}$$

where $E\{\tilde{\boldsymbol{z}}(t)\} = \boldsymbol{0}$ and

$$E\{\tilde{\boldsymbol{z}}(t)\tilde{\boldsymbol{z}}^{\mathcal{H}}(t)\} = \tilde{\boldsymbol{\Sigma}} \succeq 0 \tag{16}$$

in which $E\{\cdot\}$ stands for the expectation operator and $\boldsymbol{A} \succeq \boldsymbol{B}$ means that $\boldsymbol{A} - \boldsymbol{B}$ is positive semidefinite.

To avoid degrading Bob's SINR and to improve Bob's SINR, we would like to impose

$$\boldsymbol{h}^{\mathcal{H}}\boldsymbol{z}(t) = 0, \ \ \forall t. \tag{17}$$

Eq. (17) can be accomplished by using

$$\boldsymbol{z}(t) = \boldsymbol{Q}_h\boldsymbol{G}(\boldsymbol{G}^{\mathcal{H}}\boldsymbol{Q}_h\boldsymbol{G})^{-1}\tilde{\boldsymbol{z}}(t) \tag{18}$$

in place of (15), where $\boldsymbol{Q}_h$ is a projection matrix defined as

$$\boldsymbol{Q}_h = \boldsymbol{I} - \frac{1}{||\boldsymbol{h}||^2}\boldsymbol{h}\boldsymbol{h}^{\mathcal{H}}. \tag{19}$$

It is easy to see from (18) that

$$\boldsymbol{\Sigma} = \boldsymbol{Q}_h\boldsymbol{G}(\boldsymbol{G}^{\mathcal{H}}\boldsymbol{Q}_h\boldsymbol{G})^{-1}\tilde{\boldsymbol{\Sigma}}(\boldsymbol{G}^{\mathcal{H}}\boldsymbol{Q}_h\boldsymbol{G})^{-1}\boldsymbol{G}^{\mathcal{H}}\boldsymbol{Q}_h. \tag{20}$$

If we define a matrix $\boldsymbol{B}$ as $\boldsymbol{B} = \boldsymbol{G}^{\mathcal{H}}\boldsymbol{\Sigma}\boldsymbol{G} + \boldsymbol{D}^2$, then it follows from (20) that

$$\boldsymbol{B} = \tilde{\boldsymbol{\Sigma}} + \boldsymbol{D}^2. \tag{21}$$

Since from our assumptions, $\boldsymbol{B}$ is positive definite, we can define $\boldsymbol{B}^{\frac{1}{2}}$. If we put

$$\boldsymbol{u} = \boldsymbol{B}^{\frac{1}{2}}\boldsymbol{r} \tag{22}$$

then $\text{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma})$ can be re-expressed as

$$\text{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma}) = \max_{\boldsymbol{u}\neq\boldsymbol{0}} \frac{|\boldsymbol{u}^{\mathcal{H}}\boldsymbol{B}^{-\frac{1}{2}}\boldsymbol{G}^{\mathcal{H}}\boldsymbol{w}|^2}{\boldsymbol{u}^{\mathcal{H}}\boldsymbol{u}}. \tag{23}$$

Thus, $\text{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma})$ is given by

$$\text{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma}) = \boldsymbol{w}^{\mathcal{H}}\boldsymbol{G}\boldsymbol{B}^{-1}\boldsymbol{G}^{\mathcal{H}}\boldsymbol{w} \tag{24}$$

with $\boldsymbol{u} = \boldsymbol{B}^{-\frac{1}{2}}\boldsymbol{G}^{\mathcal{H}}\boldsymbol{w}$

By defining an auxiliary vector

$$\tilde{\boldsymbol{w}} = \boldsymbol{G}^{\mathcal{H}}\boldsymbol{w} \tag{25}$$

the constraint $\text{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma}) = \boldsymbol{w}^{\mathcal{H}}\boldsymbol{G}\boldsymbol{B}^{-1}\boldsymbol{G}^{\mathcal{H}}\boldsymbol{w} \leq \gamma_{ce}$ can be rewritten by using Schur's complement [9, p.472] as

$$\begin{pmatrix} \tilde{\boldsymbol{\Sigma}} + \boldsymbol{D}^2 & \tilde{\boldsymbol{w}} \\ \tilde{\boldsymbol{w}}^{\mathcal{H}} & \gamma_{ce} \end{pmatrix} \succeq 0 \tag{26}$$

which is convex in $\tilde{\boldsymbol{\Sigma}}$ and $\tilde{\boldsymbol{w}}$.

It follows from (17) that the Bob's SINR is given by

$$\text{SINR}_b(\boldsymbol{w}, \boldsymbol{\Sigma}) = \frac{|\boldsymbol{w}^{\mathcal{H}}\boldsymbol{h}|^2}{\sigma_n^2}. \tag{27}$$

If we impose an additional convex constraint such as

$$\Im\{\boldsymbol{w}^{\mathcal{H}}\boldsymbol{h}\} = 0, \tag{28}$$

then the constraint (11) can be re-expressed as

$$\Re\{\boldsymbol{w}^{\mathcal{H}}\boldsymbol{h}\} \geq \sqrt{\gamma_b}\sigma_n, \tag{29}$$

where $\Im\{\cdot\}$ and $\Re\{\cdot\}$ denote the imaginary and the real part of a complex value.

From (20), the objective function can be expressed as

$$f(\boldsymbol{w}, \tilde{\boldsymbol{\Sigma}}) = ||\boldsymbol{w}||^2 + \text{trace}\left[(\boldsymbol{G}^{\mathcal{H}}\boldsymbol{Q}_h\boldsymbol{G})^{-1}\tilde{\boldsymbol{\Sigma}}\right] \tag{30}$$

which is also convex in $\boldsymbol{w}$ and $\tilde{\boldsymbol{\Sigma}}$. [8] In summary, under (17) and (28), the problem reduces to a convex optimization problem:

$$\min_{\boldsymbol{w}, \tilde{\boldsymbol{\Sigma}}} f(\boldsymbol{w}, \tilde{\boldsymbol{\Sigma}}) \tag{31}$$

subject to the convex constraints (16), (25), (26), (28) and (29), which can be posed as a semidefinite program and can be numerically solved efficiently by using existing semidefinite programming solvers.

4. SIMULATION RESULTS

The proposed design is compared with the SDR design developed in [7] by numerical simulations.

First of all, we would like to clarify the difference between our optimization problem and the corresponding SDR problem in [7]. The objective function in [7] is the same with our objective function given by (10). However, our problem has the constraints resulted from (28) and (17) that the SDR problem does not have, while the SDR problem has the constraints given by (13) that our problem does not have. As proved in [7, Prop.1], solving the SDR problem with the instantaneous channel $\boldsymbol{h}$ leads to the exact solution theoretically. However, the rank one approximation is necessary when the problem is solved numerically. For fair comparison, we compute the minimum of the transmit power of the SDR problem with the same γ_{ce} as the proposed design. This means that the threshold $\gamma_{e,m}$, defined by Eq. (25) in [7], of the SDR problem is set to be γ_{ce}/M.

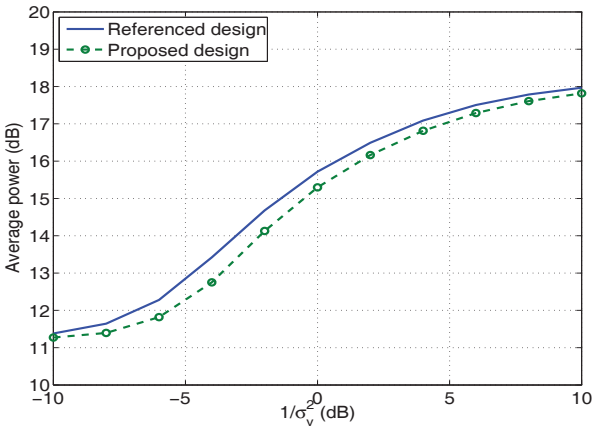

Fig. 1. Average transmit power by the proposed design (with ○) and the referenced SDR design for $N_t = 4$, $M = 3$, $\gamma_b = 10$dB, and $\gamma_{ce} = 5$dB.

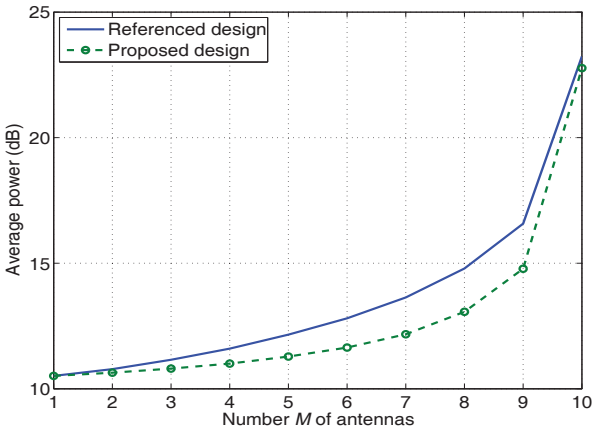

Fig. 2. Average transmit power by the proposed design (with ○) and the referenced SDR design for $N_t = 11$, $\gamma_b = 10$dB, $\gamma_{ce} = 5$dB and $1/\sigma_v^2 = 10$ dB.

The channels $\boldsymbol{h}$ and $\{\boldsymbol{g}_m\}_{m=1}^M$ are randomly generated such that they are i.i.d. complex Gaussian with zero mean and covariance matrix $\boldsymbol{I}_{N_t}/N_t$, where $\boldsymbol{I}_{N_t}$ is an identity matrix of size $N_t \times N_t$. Bob's noise power is $\sigma_n^2 = 0$ dB, while Eve's noise power at each receive antenna is $\sigma_{v,m}^2 = \sigma_v^2$ for each $m \in [1, M]$. CVX [10], a package for specifying and solving convex programs, is utilized to numerically solve the optimization problems. The results are averaged over 10^3 channel realizations.

Fig. 1 compares the average transmit power obtained by the proposed design (with ○) with the average transmit power by the referenced SDR design for different noise power $1/\sigma_v^2$ at Eve, where $N_t = 4$, $M = 3$, $\gamma_b = 10$dB, and $\gamma_{ce} = 5$dB. As can be seen, our design attains smaller average transmit power than the SDR design, that is, our design exhibits better performance than the SDR design.

For a fixed number $N_t = 11$ of Alice's transmit antennas, Fig. 2 depicts the average transmit power for different number M of Eve's receive antennas at $\gamma_b = 10$dB, $\gamma_{ce} = 5$dB, and $1/\sigma_v^2 = 10$ dB. Since the thresholds $\gamma_b = 10$dB and $\gamma_{ce} = 5$dB are fixed, Alice has to consume more transmit power as increasing the number of Eve's receive antennas, as observed in Fig. 2. There could not be found significant differences between the two designs for $M = 1, 2, 10$. Except for them, our design clearly outperforms the SDR design in this example.

5. REFERENCES

[1] A.D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, Oct. 1975.

[2] A. B. Gershman, N. D. Sidiropoulos, S. Shahbazpanahi, M. Bengtsson, and B. Ottersten, "Convex optimization-based beamforming: From receive to transmit and network designs," *IEEE Signal Processing Magazine*, vol. 27, no. 3, pp. 62 –75, 2010.

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

[4] L. Dong, Z. Han, A.P. Petropulu, and H.V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. on Signal Processing*, vol. 58, no. 3, pp. 1875 –1888, Mar. 2010.

[5] X. Tang, R. Liu, P. Spasojević, and H.V. Poor, "Interference assisted secret communication," *IEEE Trans. on Information Theory*, vol. 57, no. 5, pp. 3153 –3167, May 2011.

[6] M. Ghogho and A. Swami, "Characterizing physical-layer secrecy with unknown eavesdropper locations and channels," in *Proc. ICASSP 2011*, May 2011, pp. 3432 –3435.

[7] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. on Signal Processing*, vol. 59, no. 3, pp. 1202 –1216, Mar. 2011.

[8] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.

[9] R. A. Horn and C. R. Johnson, *Matrix analysis*, Cambridge university press, 1990.

[10] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 1.21," `http://cvxr.com/cvx`, Apr. 2011.