Power Allocation in MIMO Wiretap Channel with Statistical CSI and Finite-Alphabet Input

Sanjay Vishwakarma and A. Chockalingam
Department of ECE, Indian Institute of Science, Bangalore 560012

Abstract—In this paper, we consider the problem of power allocation in MIMO wiretap channel for secrecy in the presence of multiple eavesdroppers. Perfect knowledge of the destination channel state information (CSI) and only the statistical knowledge of the eavesdroppers CSI are assumed. We first consider the MIMO wiretap channel with Gaussian input. Using Jensen's inequality, we transform the secrecy rate max-min optimization problem to a single maximization problem. We use generalized singular value decomposition and transform the problem to a concave maximization problem which maximizes the sum secrecy rate of scalar wiretap channels subject to linear constraints on the transmit covariance matrix. We then consider the MIMO wiretap channel with finite-alphabet input. We show that the transmit covariance matrix obtained for the case of Gaussian input, when used in the MIMO wiretap channel with finite-alphabet input, can lead to zero secrecy rate at high transmit powers. We then propose a power allocation scheme with an additional power constraint which alleviates this secrecy rate loss problem, and gives non-zero secrecy rates at high transmit powers.

keywords: MIMO wiretap channel, physical layer security, secrecy rate, multiple eavesdroppers, statistical CSI, finite-alphabet input.

I. INTRODUCTION

Wireless transmissions are vulnerable to eavesdropping due to their broadcast nature. There is a growing demand to address the issue of providing security in wireless networks. Secrecy in wireless communication networks can be achieved using physical layer techniques, where the legitimate receiver gets the transmitted information correctly and the eavesdropper receives no or very little information. Achievable secrecy rates and secrecy capacity bounds for multiple antenna point-to-point wiretap channel has been studied in [1]–[4] and point-to-multipoint wiretap channel has been studied in [5]. In [1], [6], multiple-input single-output (MISO) wiretap channel is considered, and secrecy rate is computed assuming statistical information of the eavesdropper channel. In [7], [8], secrecy capacity of the multiple-input multiple-output (MIMO) wiretap channel has been computed assuming perfect channel state information (CSI) knowledge of the destination and the eavesdropper. These works consider secrecy rate when the input to the channel is Gaussian. In practice, the input to the channel will be from a finite alphabet set, e.g., M-ary alphabets. The effect of finite-alphabet input on the achievable secrecy rate for various channels has been studied in [9]–[12]. It has been shown that with finite-alphabet input, increasing the power beyond a maximum point is harmful as the secrecy rate curve dips continuously thereafter. In [13], design of optimum

linear transmit precoding for maximum secrecy rate over MIMO wiretap channel with finite-alphabet input and with perfect eavesdropper CSI assumption has been investigated.

In this paper, we consider the problem of power allocation in MIMO wiretap channel for secrecy in the presence of multiple eavesdroppers. Our approach to study this problem, which is adopted in this paper, is summarized as follows. First, we consider the MIMO wiretap channel with Gaussian input and knowledge of statistical CSI of the eavesdroppers. We transform the secrecy rate max-min optimization problem with Gaussian input into a single maximization problem using Jensen's inequality. Generalized singular value decomposition (GSVD) is used to transform the problem to a concave maximization problem which maximizes the sum secrecy rate of scalar wiretap channels subject to linear constraints on the transmit covariance matrix. We then consider the MIMO wiretap channel with finite-alphabet input and knowledge of statistical CSI of the eavesdroppers. It is found that when the transmit covariance matrix obtained for the case of Gaussian input is used in the MIMO wiretap channel with finite-alphabet input, the secrecy rate goes to zero at high transmit powers. Therefore, we propose a power allocation scheme with an additional power constraint to deal with this secrecy rate loss. The proposed scheme is shown to alleviate the secrecy rate loss problem and gives non-zero secrecy rates at high transmit powers.

Notations : Vectors are denoted by boldface lower case letters, and matrices are denoted by boldface upper case letters. $\boldsymbol{A} \in \mathbb{C}^{N_1 \times N_2}$ implies that $\boldsymbol{A}$ is a complex matrix of dimension $N_1 \times N_2$. $\boldsymbol{A} \succeq \boldsymbol{0}$ denotes that $\boldsymbol{A}$ is a positive semidefinite matrix. $\boldsymbol{I}$ denotes the identity matrix. Transpose and complex conjugate transpose operations are denoted with $[.]^T$ and $[.]^*$, respectively. $diag(\boldsymbol{a})$ denotes a diagonal matrix with elements of vector $\boldsymbol{a}$ on the diagonal of the matrix. $diag(\boldsymbol{A})$ denotes a vector formed with the diagonal entries of matrix $\boldsymbol{A}$. $\mathbb{E}[.]$ denotes expectation operation.

II. SYSTEM MODEL

Consider a MIMO wiretap channel which consists of a source S, an intended destination D, and J eavesdroppers $\{E_1, E_2, \cdots, E_J\}$. The system model is shown in Fig. 1. Source S has N_S transmit antennas, destination D has N_D receive antennas, and each eavesdropper E_j has N_{E_j} receive antennas. The communication between source S and destination D happens in n channel uses. The complex fading channel gain matrix between S to D is denoted by $\boldsymbol{H} \in \mathbb{C}^{N_D \times N_S}$.
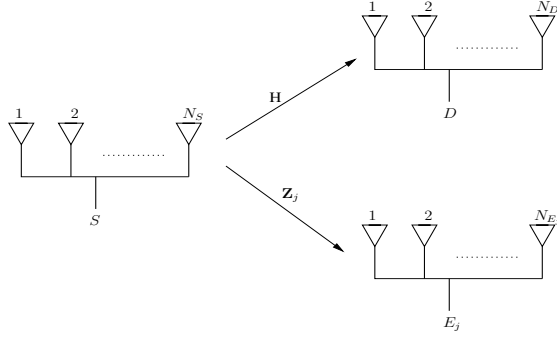
Fig. 1. System model.

Likewise, the channel gain matrix between S to E_j is denoted by $\boldsymbol{Z}_j \in \mathbb{C}^{N_{E_j} \times N_S}$. We assume that the channel gain matrix, $\boldsymbol{H}$, between S to D is known perfectly and remains static over the codeword transmit duration. We also assume that the channel gains of all E_js are unknown and undergo independent fast fading [1,6]. Channel gains of E_j are i.i.d. $\sim \mathcal{CN}(0, \sigma_{E_j}^2)$. Let P_0 denote the total available transmit power. The source S transmits message W which is equiprobable over $\{1, 2, \cdots, 2^{nR_s}\}$ with perfect secrecy with respect to all E_js [5]. Source maps each W to a codeword $\{\boldsymbol{x}_i\}_{i=1}^n$ of length n, where each $\boldsymbol{x}_i \in \mathbb{C}^{N_S \times 1}$ is i.i.d. ($\sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{Q})$) with $\mathbb{E}[\boldsymbol{x}_i] = \boldsymbol{0}$, $\mathbb{E}[\boldsymbol{x}_i \boldsymbol{x}_i^*] = \boldsymbol{Q}$, and $trace(\boldsymbol{Q}) \leq P_0$. Hereafter, we will use $\boldsymbol{x}$ to denote the symbols in the codeword $\{\boldsymbol{x}_i\}_{i=1}^n$. Let $\boldsymbol{y}_D \in \mathbb{C}^{N_D \times 1}$ and $\boldsymbol{y}_{E_j} \in \mathbb{C}^{N_{E_j} \times 1}$ denote the received signals at the destination D and the jth eavesdropper E_j, respectively. We then have

$$\boldsymbol{y}_D = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{\eta}_D, \tag{1}$$

$$\boldsymbol{y}_{E_j} = \boldsymbol{Z}_j \boldsymbol{x} + \boldsymbol{\eta}_{E_j}, \tag{2}$$

where $\boldsymbol{\eta}_D \sim \mathcal{CN}(\boldsymbol{0}, N_0 \boldsymbol{I})$ and $\boldsymbol{\eta}_{E_j} \sim \mathcal{CN}(\boldsymbol{0}, N_0 \boldsymbol{I})$ are the i.i.d. noise vectors at D and E_j, respectively.

III. MIMO Wiretap Channel with Gaussian Input

For a given $\boldsymbol{H}$, using (1), the information rate at the destination D is

$$I(\boldsymbol{x}; \boldsymbol{y}_D) = \log_2 \det\left(\boldsymbol{I} + \frac{\boldsymbol{H}\boldsymbol{Q}\boldsymbol{H}^*}{N_0}\right). \tag{3}$$

Similarly, for a given $\boldsymbol{Z}_j$, using (2), the information rate at the jth eavesdropper E_j, $\forall j = 1, 2, \cdots, J$, is

$$I(\boldsymbol{x}; \boldsymbol{y}_{E_j}) = \log_2 \det\left(\boldsymbol{I} + \frac{\boldsymbol{Z}_j \boldsymbol{Q} \boldsymbol{Z}_j^*}{N_0}\right). \tag{4}$$

Subject to the total power constraint P_0, using (3) and (4), the secrecy rate R_s for the MIMO wiretap channel is obtained by solving the following optimization problem:

$$R_s = \max_{\boldsymbol{Q}} \min_{j:1,2,\cdots,J} \left\{ \log_2 \det\left(\boldsymbol{I} + \frac{\boldsymbol{H}\boldsymbol{Q}\boldsymbol{H}^*}{N_0}\right) \right.$$
$$\left. - \mathbb{E}\left[\log_2 \det\left(\boldsymbol{I} + \frac{\boldsymbol{Z}_j \boldsymbol{Q} \boldsymbol{Z}_j^*}{N_0}\right)\right] \right\} \tag{5}$$

$$\geq \max_{\boldsymbol{Q}} \min_{j:1,2,\cdots,J} \left\{ \log_2 \det\left(\boldsymbol{I} + \frac{\boldsymbol{H}\boldsymbol{Q}\boldsymbol{H}^*}{N_0}\right) \right.$$

$$\left. - \log_2 \det\left(\boldsymbol{I} + \frac{N_{E_j} \sigma_{E_j}^2 \boldsymbol{Q}}{N_0}\right)\right\} \tag{6}$$

$$= \max_{\boldsymbol{Q}} \left\{ \log_2 \det\left(\boldsymbol{I} + \frac{\boldsymbol{H}\boldsymbol{Q}\boldsymbol{H}^*}{N_0}\right) \right.$$

$$\left. - \log_2 \det\left(\boldsymbol{I} + \frac{N_{E_{j_0}} \sigma_{E_{j_0}}^2 \boldsymbol{Q}}{N_0}\right)\right\} \tag{7}$$

$$= \max_{\boldsymbol{Q}} \left\{ \log_2 \det\left(\boldsymbol{I} + \frac{\boldsymbol{H}\boldsymbol{Q}\boldsymbol{H}^*}{N_0}\right) \right.$$

$$\left. - \log_2 \det\left(\boldsymbol{I} + \frac{\boldsymbol{Z}\boldsymbol{Q}\boldsymbol{Z}^*}{N_0}\right)\right\} \tag{8}$$

$$\text{s.t.} \quad \boldsymbol{Q} \succeq \boldsymbol{0}, \quad trace(\boldsymbol{Q}) \leq P_0, \tag{9}$$

where (6) is written using Jensen's inequality, j_0 in (7) corresponds to the eavesdropper with maximum $N_{E_{j_0}} \sigma_{E_{j_0}}^2$, and $\boldsymbol{Z}$ in (8) is $\sqrt{N_{E_{j_0}} \sigma_{E_{j_0}}^2} \boldsymbol{I}$. We intend to find the $\boldsymbol{Q}$ which maximizes the objective function in (8) subject to the constraints in (9). To do this, we take the GSVD [14] of $\boldsymbol{H}$ and $\boldsymbol{Z}$ as

$$\boldsymbol{H} = \boldsymbol{U}\boldsymbol{\Lambda}_H\left[\boldsymbol{\Phi}^*\boldsymbol{T}, \ \boldsymbol{0}\right]\boldsymbol{W}^* \tag{10}$$

$$\boldsymbol{Z} = \boldsymbol{V}\boldsymbol{\Lambda}_Z\left[\boldsymbol{\Phi}^*\boldsymbol{T}, \ \boldsymbol{0}\right]\boldsymbol{W}^*. \tag{11}$$

$\boldsymbol{U}$, $\boldsymbol{V}$, $\boldsymbol{\Phi}$, and $\boldsymbol{W}$ are unitary matrices of dimensions $N_D \times N_D$, $N_S \times N_S$, $k \times k$, and $N_S \times N_S$, respectively. $\boldsymbol{T}$ is an upper triangular matrix of size $k \times k$ and rank-k. $\boldsymbol{\Lambda}_H$ and $\boldsymbol{\Lambda}_Z$ are diagonal matrices of dimensions $N_D \times k$ and $N_S \times k$, respectively, and satisfy the condition

$$\boldsymbol{\Lambda}_H^T \boldsymbol{\Lambda}_H + \boldsymbol{\Lambda}_Z^T \boldsymbol{\Lambda}_Z = \boldsymbol{I}. \tag{12}$$

Substituting the GSVD of $\boldsymbol{H}$ and $\boldsymbol{Z}$ in (8), we write the problem as

$$\max_{\boldsymbol{Q}} \left\{ \right.$$
$$\log_2 \det\left(\boldsymbol{I} + \frac{\boldsymbol{U}\boldsymbol{\Lambda}_H\left[\boldsymbol{\Phi}^*\boldsymbol{T}, \ \boldsymbol{0}\right]\boldsymbol{W}^*\boldsymbol{Q}\boldsymbol{W}\left[\boldsymbol{\Phi}^*\boldsymbol{T}, \ \boldsymbol{0}\right]^*\boldsymbol{\Lambda}_H^T\boldsymbol{U}^*}{N_0}\right)$$

$$\left. - \log_2 \det\left(\boldsymbol{I} + \frac{\boldsymbol{V}\boldsymbol{\Lambda}_Z\left[\boldsymbol{\Phi}^*\boldsymbol{T}, \boldsymbol{0}\right]\boldsymbol{W}^*\boldsymbol{Q}\boldsymbol{W}\left[\boldsymbol{\Phi}^*\boldsymbol{T}, \boldsymbol{0}\right]^*\boldsymbol{\Lambda}_Z^T\boldsymbol{V}^*}{N_0}\right)\right\} \tag{13}$$

$$\text{s.t.} \quad \boldsymbol{Q} \succeq 0, \quad trace(\boldsymbol{Q}) \leq P_0. \tag{14}$$

We perform the following sequence of substitutions in (13):
1) $\boldsymbol{Q} = \boldsymbol{W}\boldsymbol{Q}_1\boldsymbol{W}^* \succeq \boldsymbol{0}$ and $\boldsymbol{Q}_1 \in \mathbb{C}^{N_S \times N_S}$,
2) $\boldsymbol{Q}_1 = [\boldsymbol{Q}_2, \boldsymbol{0}; \ \boldsymbol{0}, \boldsymbol{0}] \succeq \boldsymbol{0}$ and $\boldsymbol{Q}_2 \in \mathbb{C}^{k \times k}$,
3) $\boldsymbol{Q}_2 = (\boldsymbol{\Phi}^*\boldsymbol{T})^{-1}\boldsymbol{Q}_3\left((\boldsymbol{\Phi}^*\boldsymbol{T})^{-1}\right)^* \succeq \boldsymbol{0}$ and $\boldsymbol{Q}_3 \in \mathbb{C}^{k \times k}$.
With the above substitutions, (13) and (14) can be written in the following equivalent form:

$$\max_{\boldsymbol{Q}, \, \boldsymbol{Q}_1, \, \boldsymbol{Q}_2, \, \boldsymbol{Q}_3} \left\{ \log_2 \det\left(\boldsymbol{I} + \frac{\boldsymbol{\Lambda}_H\boldsymbol{Q}_3\boldsymbol{\Lambda}_H^T}{N_0}\right) \right.$$

$$\left. - \log_2 \det\left(\boldsymbol{I} + \frac{\boldsymbol{\Lambda}_Z\boldsymbol{Q}_3\boldsymbol{\Lambda}_Z^T}{N_0}\right)\right\} \tag{15}$$

$$\text{s.t.} \quad trace(\boldsymbol{Q}) \leq P_0, \quad \boldsymbol{Q} = \boldsymbol{W}\boldsymbol{Q}_1\boldsymbol{W}^*,$$
$$\boldsymbol{Q}_1 = [\boldsymbol{Q}_2, \boldsymbol{0}; \, \boldsymbol{0}, \boldsymbol{0}], \quad \boldsymbol{Q}_2 = (\boldsymbol{\Phi}^*\boldsymbol{T})^{-1}\boldsymbol{Q}_3\big((\boldsymbol{\Phi}^*\boldsymbol{T})^{-1}\big)^*,$$
$$\boldsymbol{Q}_3 \succeq \boldsymbol{0}. \quad (16)$$

Let there be r non-zero diagonal entries in $\boldsymbol{\Lambda}_H$. Since $\boldsymbol{\Lambda}_H$ is a diagonal matrix, the first term in the objective function in (15) will be maximized if $\boldsymbol{Q}_3$ is selected to be of the following form:

$$\boldsymbol{Q}_3 = [\boldsymbol{Q}_4, \boldsymbol{0}; \, \boldsymbol{0}, \boldsymbol{0}] \succeq \boldsymbol{0}, \quad (17)$$

where $\boldsymbol{Q}_4 \succeq \boldsymbol{0}$ and $\boldsymbol{Q}_4 \in \mathbb{C}^{r \times r}$. In order to simplify the analysis further, we assume that $\boldsymbol{Q}_4$ is a diagonal matrix with $\boldsymbol{Q}_4 = diag([q_1, q_2, \cdots, q_r]^T)$. Substituting (17) in (15) and (16), we can write

$$\max_{\substack{\boldsymbol{Q}, \, \boldsymbol{Q}_1, \, \boldsymbol{Q}_2, \, \boldsymbol{Q}_3, \, \boldsymbol{Q}_4, \\ q_1, q_2, \cdots, q_r}} \left\{ \log_2 \det \left(\boldsymbol{I} + \frac{\boldsymbol{\Lambda}_H^{r \times r}\boldsymbol{Q}_4\boldsymbol{\Lambda}_H^{r \times r \, T}}{N_0} \right) \right.$$
$$\left. - \log_2 \det \left(\boldsymbol{I} + \frac{\boldsymbol{\Lambda}_Z^{r \times r}\boldsymbol{Q}_4\boldsymbol{\Lambda}_Z^{r \times r \, T}}{N_0} \right) \right\} \quad (18)$$

$$\text{s.t.} \quad trace(\boldsymbol{Q}) \leq P_0, \quad \boldsymbol{Q} = \boldsymbol{W}\boldsymbol{Q}_1\boldsymbol{W}^*,$$
$$\boldsymbol{Q}_1 = [\boldsymbol{Q}_2, \boldsymbol{0}; \, \boldsymbol{0}, \boldsymbol{0}], \quad \boldsymbol{Q}_2 = (\boldsymbol{\Phi}^*\boldsymbol{T})^{-1}\boldsymbol{Q}_3\big((\boldsymbol{\Phi}^*\boldsymbol{T})^{-1}\big)^*,$$
$$\boldsymbol{Q}_3 = [\boldsymbol{Q}_4, \boldsymbol{0}; \, \boldsymbol{0}, \boldsymbol{0}], \quad \boldsymbol{Q}_4 = diag\big([q_1, \cdots, q_r]^T\big) \succeq \boldsymbol{0}, \quad (19)$$

where $\boldsymbol{\Lambda}_H^{r \times r} = diag([\lambda_1^H, \lambda_2^H, \cdots, \lambda_r^H]^T)$ and $\boldsymbol{\Lambda}_Z^{r \times r} = diag([\lambda_1^Z, \lambda_2^Z, \cdots, \lambda_r^Z]^T)$ are leading $r \times r$ diagonal matrices of $\boldsymbol{\Lambda}_H$ and $\boldsymbol{\Lambda}_Z$, respectively.

Rewrite the objective function in (18) in the following equivalent form:

$$\max_{\substack{\boldsymbol{Q}, \, \boldsymbol{Q}_1, \, \boldsymbol{Q}_2, \, \boldsymbol{Q}_3, \, \boldsymbol{Q}_4, \\ q_1, q_2, \cdots, q_r}} \sum_{i=1}^{r} \left\{ \log_2 \left(1 + \frac{(\lambda_i^H)^2 q_i}{N_0} \right) \right.$$
$$\left. - \log_2 \left(1 + \frac{(\lambda_i^Z)^2 q_i}{N_0} \right) \right\} \quad (20)$$

$$\text{s.t. all constraints in (19).}$$

We note that for $\lambda_i^H > \lambda_i^Z$, the function $\left\{ \log_2 \left(1 + \frac{(\lambda_i^H)^2 q_i}{N_0} \right) - \log_2 \left(1 + \frac{(\lambda_i^Z)^2 q_i}{N_0} \right) \right\}$ in (20) is positive, strictly increasing, and concave in the variable $q_i > 0$. Let $l \leq r$ be the number of λ_i^Hs which are strictly greater than λ_i^Zs. We keep the l terms in the summation in (20) for which $\lambda_i^H > \lambda_i^Z$ and remaining $r - l$ terms are discarded since they will not lead to positive secrecy rate. With this, the optimization problem (20) is written as follows:

$$\max_{\substack{\boldsymbol{Q}, \, \boldsymbol{Q}_1, \, \boldsymbol{Q}_2, \, \boldsymbol{Q}_3, \, \boldsymbol{Q}_4, \\ q_1, q_2, \cdots, q_l}} \sum_{i=1}^{l} \left\{ \log_2 \left(1 + \frac{(\lambda_i^H)^2 q_i}{N_0} \right) \right.$$
$$\left. - \log_2 \left(1 + \frac{(\lambda_i^Z)^2 q_i}{N_0} \right) \right\} \quad (21)$$

$$\text{s.t.} \quad trace(\boldsymbol{Q}) \leq P_0, \quad \boldsymbol{Q} = \boldsymbol{W}\boldsymbol{Q}_1\boldsymbol{W}^*,$$
$$\boldsymbol{Q}_1 = [\boldsymbol{Q}_2, \boldsymbol{0}; \, \boldsymbol{0}, \boldsymbol{0}], \quad \boldsymbol{Q}_2 = (\boldsymbol{\Phi}^*\boldsymbol{T})^{-1}\boldsymbol{Q}_3\big((\boldsymbol{\Phi}^*\boldsymbol{T})^{-1}\big)^*,$$
$$\boldsymbol{Q}_3 = [\boldsymbol{Q}_4, \boldsymbol{0}; \, \boldsymbol{0}, \boldsymbol{0}],$$
$$\boldsymbol{Q}_4 = diag([q_1, \cdots, q_l, 0, \cdots, 0]^T) \succeq \boldsymbol{0}. \quad (22)$$

The objective function in (21) is a sum of l concave functions and all the constraints in (22) are linear. The above optimization problem is a concave maximization problem and it can be solved using interior-point method. We denote the optimum values of $q_1, q_2, \cdots, q_l$ obtained from (21) as $q_1^g, q_2^g, \cdots, q_l^g$, respectively.

Remarks :

- A possible suboptimal approach to solve the optimization problem (21) will be to assign equal weights to all $q_1, q_2, \cdots, q_l$, i.e., $q_1 = q_2 = \cdots = q_l$, and solve the following optimization problem:

$$\max_{\substack{\boldsymbol{Q}, \, \boldsymbol{Q}_1, \, \boldsymbol{Q}_2, \, \boldsymbol{Q}_3, \, \boldsymbol{Q}_4, \\ q_1, q_2, \cdots, q_l}} \quad trace(\boldsymbol{Q})$$

$$\text{s.t.} \quad trace(\boldsymbol{Q}) \leq P_0, \quad \boldsymbol{Q} = \boldsymbol{W}\boldsymbol{Q}_1\boldsymbol{W}^*,$$
$$\boldsymbol{Q}_1 = [\boldsymbol{Q}_2, \boldsymbol{0}; \, \boldsymbol{0}, \boldsymbol{0}], \quad \boldsymbol{Q}_2 = (\boldsymbol{\Phi}^*\boldsymbol{T})^{-1}\boldsymbol{Q}_3\big((\boldsymbol{\Phi}^*\boldsymbol{T})^{-1}\big)^*,$$
$$\boldsymbol{Q}_3 = [\boldsymbol{Q}_4, \boldsymbol{0}; \, \boldsymbol{0}, \boldsymbol{0}],$$
$$\boldsymbol{Q}_4 = diag([q_1, \cdots, q_l, 0, \cdots, 0]^T) \succeq \boldsymbol{0},$$
$$q_1 = q_2 = \cdots = q_l.$$

- We note that the MIMO wiretap problem in (21) with the total available transmit power constraint, $trace(\boldsymbol{Q}) \leq P_0$, in (22) can also be extended to the scenario when there is an individual power constraint on $\boldsymbol{Q}$, i.e., $diag(\boldsymbol{Q}) \leq [P_1, P_2, \cdots, P_{N_S}]^T$, where $P_1, P_2, \cdots, P_{N_S}$ are the available transmit powers for antennas $1, 2, \cdots, N_s$, respectively.

IV. MIMO WIRETAP CHANNEL WITH FINITE-ALPHABET INPUT

The optimization problem (21) can be equivalently viewed as the sum secrecy rate of l scalar Gaussian wiretap channels with power constraints in (22). $\sqrt{\frac{(\lambda_i^H)^2 q_i}{N_0}}$ and $\sqrt{\frac{(\lambda_i^Z)^2 q_i}{N_0}}$ correspond to the destination and eavesdropper channel coefficients, respectively, associated with the ith Gaussian wiretap channel where $1 \leq i \leq l$ and noise $\sim \mathcal{CN}(0, 1)$. In this section, we consider the power allocation scheme for the above channel model when the input to each scalar wiretap channel is from a finite alphabet set $\mathbb{A} = \{a_1, a_2, \cdots, a_M\}$ of size M. We assume that symbols from the set $\mathbb{A}$ are drawn equiprobably and $\mathbb{E}\{|a|^2\} = 1$. With finite-alphabet input, we write the optimization problem (21) as follows:

$$\max_{\substack{\boldsymbol{Q}, \, \boldsymbol{Q}_1, \, \boldsymbol{Q}_2, \, \boldsymbol{Q}_3, \, \boldsymbol{Q}_4, \\ q_1, q_2, \cdots, q_l}} \sum_{i=1}^{l} \left\{ I\left(\frac{(\lambda_i^H)^2 q_i}{N_0} \right) - I\left(\frac{(\lambda_i^Z)^2 q_i}{N_0} \right) \right\} \quad (23)$$

$$\text{s.t. all constraints in (22).}$$

$I(.)$ in (23) is the mutual information function with finite-alphabet input and it is explicitly written as follows:

$$I(\rho) = \frac{1}{M} \sum_{i=1}^{M} \int p_n\big(z - \sqrt{\rho}a_i\big)$$
$$. \log_2 \frac{p_n(z - \sqrt{\rho}a_i)}{\frac{1}{M}\sum_{m=1}^{M} p_n(z - \sqrt{\rho}a_m)} dz, \quad (24)$$

where $p_n(\theta) = \frac{1}{\pi}e^{-|\theta|^2}$. Solving the optimization problem (23) for optimum $q_1, q_2, \cdots, q_l$ is hard. A suboptimal approach to find the secrecy rate with finite-alphabet input will be to use $q_1^g, q_2^g, \cdots, q_l^g$ directly in (23) obtained from (21) with Gaussian input. This suboptimal approach to find the secrecy rate with finite-alphabet input could be adverse and it could lead to reduced secrecy rate without transmit power control. In the Appendix, we show that the secrecy rate with finite-alphabet input for a Gaussian wiretap channel is a unimodal function in transmit power, i.e., there exists a unique transmit power at which the secrecy rate attains its maximum value.

Let $q_1^{ul}, q_2^{ul}, \cdots, q_l^{ul}$ be the upper limit for $q_1, q_2, \cdots, q_l$ obtained using the method proposed in the Appendix. Using these upper limits $q_1^{ul}, q_2^{ul}, \cdots, q_l^{ul}$, we rewrite the optimization problem (21) as follows:

$$\max_{\substack{\boldsymbol{Q},\ \boldsymbol{Q_1},\ \boldsymbol{Q_2},\ \boldsymbol{Q_3},\ \boldsymbol{Q_4}, \\ q_1, q_2, \cdots, q_l}} \sum_{i=1}^{l} \left\{ \log_2\left(1 + \frac{(\lambda_i^H)^2 q_i}{N_0}\right) \right.$$
$$\left. - \log_2\left(1 + \frac{(\lambda_i^Z)^2 q_i}{N_0}\right) \right\} \qquad (25)$$

$$\text{s.t.} \quad trace(\boldsymbol{Q}) \leq P_0, \quad \boldsymbol{Q} = \boldsymbol{W}\boldsymbol{Q_1}\boldsymbol{W}^*,$$
$$\boldsymbol{Q_1} = [\boldsymbol{Q_2}, \boldsymbol{0}; \ \boldsymbol{0}, \boldsymbol{0}], \quad \boldsymbol{Q_2} = (\boldsymbol{\Phi}^*\boldsymbol{T})^{-1}\boldsymbol{Q_3}\left((\boldsymbol{\Phi}^*\boldsymbol{T})^{-1}\right)^*,$$
$$\boldsymbol{Q_3} = [\boldsymbol{Q_4}, \boldsymbol{0}; \ \boldsymbol{0}, \boldsymbol{0}],$$
$$\boldsymbol{Q_4} = diag([q_1, q_2, \cdots, q_l, 0, \cdots, 0]^T) \succeq \boldsymbol{0},$$
$$[q_1, q_2, \cdots, q_l]^T \leq [q_1^{ul}, q_2^{ul}, \cdots, q_l^{ul}]^T. \quad (26)$$

We denote the optimum solution of (25) as $q_1^f, q_2^f, \cdots, q_l^f$. If $q_1^f, q_2^f, \cdots, q_l^f$ are used in (23) to compute the secrecy rate with finite-alphabet input, it will not lead to reduced secrecy rate due to the presence of additional constraint $[q_1, q_2, \cdots, q_l]^T \leq [q_1^{ul}, q_2^{ul}, \cdots, q_l^{ul}]^T$ in (26). We will see this in the numerical results presented in the next section.

V. RESULTS AND DISCUSSIONS

We computed the secrecy rate for MIMO wiretap channel with $N_S = N_D = N_{E_j} = 3$ (i.e., source, destination and eavesdroppers have 3 antennas each) by simulations. We take $N_0 = 1$, $\sigma_{E_{j_0}} = 0.5$, and

$$\boldsymbol{H} = \begin{bmatrix} 0.0799 - 0.1191i, & 1.9709 + 0.2753i, & -0.8066 + 0.8648i \\ 0.3111 - 0.1545i, & -0.8250 + 0.5312i, & -0.7731 - 0.9074i \\ 0.0719 + 0.3828i, & -1.3112 + 1.2574i, & -0.3066 - 1.6468i \end{bmatrix}.$$

We computed the secrecy rate for three different cases:

- *Case 1:* The secrecy rate is computed with Gaussian input.
- *Case 2:* The secrecy rate is computed with binary alphabet (BPSK) input but with no power control, i.e., the solution obtained directly from (21) is used to compute the finite-alphabet secrecy rate in (23).
- *Case 3:* The secrecy rate is computed with binary alphabet (BPSK) input but with power control, i.e., the solution obtained from (25) is used to compute the finite-alphabet secrecy rate in (23).
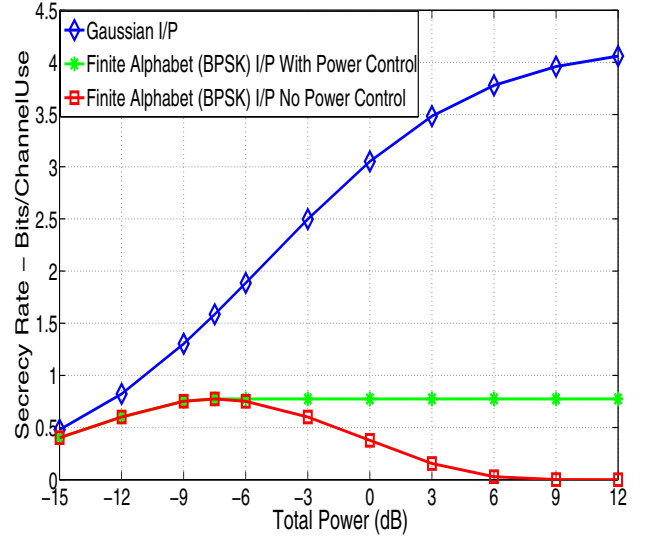

Fig. 2. Secrecy rate vs total power in MIMO wiretap channel with known destination CSI and unknown (statistical) eavesdroppers CSI. $N_S = N_D = N_{E_j} = 3$, $N_0 = 1$, $\sigma_{E_{j_0}} = 0.5$.

The computed secrecy rate results for the above three cases are shown in Fig. 2. From Fig. 2, it can be seen that, as expected, the secrecy rate for MIMO wiretap channel with Gaussian alphabet input (*Case 1*) increases with increase in P_0. The secrecy rate with BPSK input but with no power control (*Case 2*) first increases with increase in P_0 and then decreases to zero at high transmit powers. This is due to the fact that at high transmit powers with finite-alphabet input, the information rate at the eavesdroppers equals the information rate at the destination which causes the secrecy rate go to zero. However, when the power allocation scheme proposed in Section IV is used, the MIMO wiretap secrecy rate with BPSK input (*Case 3*) does not go to zero at high transmit powers (as was observed in Case 2). Instead, the secrecy rate increases with increasing transmit power and remains flat at some non-zero secrecy rate at high transmit powers. This is because of the presence of the additional power constraint $[q_1, q_2, \cdots, q_l]^T \leq [q_1^{ul}, q_2^{ul}, \cdots, q_l^{ul}]^T$, in (26).

VI. CONCLUSIONS

We studied the problem of power allocation for secrecy in MIMO wiretap channel with finite-alphabet input. Our work differed from past works in the following aspects: we assumed that only the statistical knowledge of the eavesdropper CSI is known, and we considered multiple eavesdroppers. To study the problem, we first considered the MIMO wiretap channel with Gaussian input, where we transformed the secrecy rate max-min optimization problem to a concave maximization problem which maximized the sum secrecy rate of l scalar wiretap channels subject to linear constraints on the transmit covariance matrix. When the transmit covariance matrix obtained in the Gaussian input setting is used in the finite-alphabet input setting, the secrecy rate decreased for increasing transmit powers leading to zero secrecy rate at high transmit

powers. To alleviate this secrecy rate loss, we proposed a power allocation scheme using an additional power constraint in the problem. The proposed power allocation scheme was shown to alleviate the secrecy rate loss problem and achieve flat non-zero secrecy rate at high transmit powers.

APPENDIX

In this appendix, we show that the secrecy rate with finite-alphabet input for a Gaussian wiretap channel is a unimodal function in transmit power, i.e., there exists a unique transmit power at which secrecy rate attains its maximum value. Let y_D and y_E be the received signals at the destination and eavesdropper, respectively, in a Gaussian wiretap channel, i.e.,

$$y_D = \sqrt{P}hx + \eta_D \tag{27}$$
$$y_E = \sqrt{P}zx + \eta_E, \tag{28}$$

where h and z are known channel coefficients for the destination and eavesdropper channels, respectively, x is the transmitted source symbol from a finite-alphabet set $\mathbb{A}$ as described in Section IV with $\mathbb{E}\{|x|^2\} = 1$, P is the power transmitted by the source, and η_D and η_E are the independent additive noise terms at the destination and eavesdropper $\sim \mathcal{CN}(0,1)$.

Using (27), the information rate at the destination, R_D^f, with finite-alphabet input is

$$R_D^f = I(|h|^2 P). \tag{29}$$

Similarly, using (28), the information rate at the eavesdropper, R_E^f, with finite-alphabet input is

$$R_E^f = I(|z|^2 P). \tag{30}$$

$I(.)$ in (29) and (30) is the mutual information function as defined in (24). The secrecy rate, R_s^f, with finite-alphabet input for the Gaussian wiretap channel is obtained as

$$R_s^f = R_D^f - R_E^f = I(|h|^2 P) - I(|z|^2 P). \tag{31}$$

With $P > 0$, R_s^f in (31) will be positive only when $|h| > |z|$. Therefore, w.l.o.g. we assume that $|h| > |z|$. Using Theorem 1 in [15] to find the derivatives of R_D^f and R_E^f w. r. t. P, respectively, we get

$$\frac{dR_D^f}{dP} = |h|^2 \text{MMSE}(|h|^2 P) \log_2 e \tag{32}$$

$$\frac{dR_E^f}{dP} = |z|^2 \text{MMSE}(|z|^2 P) \log_2 e. \tag{33}$$

Using (32) and (33), taking the derivative of R_s^f w.r.t. P and equating it to zero, we get

$$\frac{dR_s^f}{dP} = \left(|h|^2 \text{MMSE}(|h|^2 P) - |z|^2 \text{MMSE}(|z|^2 P)\right) \log_2 e$$
$$= 0. \tag{34}$$

We intend to seek the solution, $P = P_{opt}$, of (34). We show that, with finite alphabet, this solution is unique and secrecy rate, R_s^f, attains it's maximum value at $P = P_{opt}$.

For various M-ary alphabets, it is shown in [15,16] that 1) MMSE is a positive, strictly monotonic decreasing function in
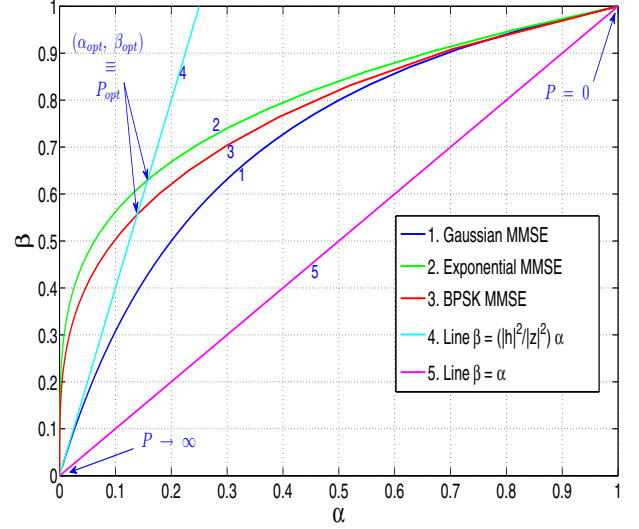

Fig. 3. Various MMSE β vs α curves with $|h|^2 = 2.0$ and $|z|^2 = 0.5$.

SNR and in the limit approaches zero as SNR tends to infinity, and 2) at high SNRs, MMSE decreases exponentially (Theorems 3 and 4 in [15]). Since MMSE is a strictly monotonic decreasing function, it's inverse, MMSE^{-1}, exists. Define

$$\alpha = \text{MMSE}(|h|^2 P) \implies P = \frac{1}{|h|^2} \text{MMSE}^{-1}(\alpha), \tag{35}$$

$$\text{and} \quad \beta = \text{MMSE}(|z|^2 P). \tag{36}$$

Using (35), we rewrite (36) in terms of α as

$$\beta = \text{MMSE}(|z|^2 P) = \text{MMSE}\left(\frac{|z|^2}{|h|^2} \text{MMSE}^{-1}(\alpha)\right). \tag{37}$$

It can be easily shown that β is a strictly monotonic increasing function in α. We plot β as a function of α for three different MMSE functions and two straight lines in Fig. 3. Point $(\alpha, \beta) = (0,0) \equiv O$ in the plot corresponds to $P \to \infty$. Similarly, point $(\alpha, \beta) = (1,1)$ corresponds to $P = 0$.

1) **Gaussian MMSE Function:** We take $\text{MMSE}(|h|^2 P) = \frac{1}{(1+|h|^2 P)} = \alpha$ and $\text{MMSE}(|z|^2 P) = \frac{1}{(1+|z|^2 P)} = \beta$. With this choice of MMSE functions, $\beta = \frac{1}{\left(1+\frac{|z|^2}{|h|^2}(\frac{1}{\alpha} - 1)\right)}$. The slope of this curve at the origin, $(0,0)$, is

$$\frac{d\beta}{d\alpha} \text{ at } (\alpha = 0) = \frac{\frac{d\beta}{dP}}{\frac{d\alpha}{dP}} \text{ as } (P \to \infty) = \frac{|h|^2}{|z|^2}.$$

This implies that $\beta = \left(\frac{|h|^2}{|z|^2}\right)\alpha$ is tangent to the Gaussian MMSE β vs α curve at the origin $(0,0)$.

2) **Exponential MMSE Function:** We take $\text{MMSE}(|h|^2 P) = \exp^{-(|h|^2 P)} = \alpha$, and $\text{MMSE}(|z|^2 P) = \exp^{-(|z|^2 P)} = \beta$. With this choice of MMSE functions, $\beta = \alpha^{\left(\frac{|z|^2}{|h|^2}\right)}$. The β axis, i.e., $\alpha = 0$, is tangent to the exponential MMSE β vs α curve at the origin $(0,0)$.

3) M-**ary MMSE Functions:** At high SNRs, MMSE for M-ary alphabets decreases exponentially (Theorems 3 and 4 in

[15]). This implies that the β axis, i.e., $\alpha = 0$, is tangent to the M-ary MMSE β vs α curve at the origin $(0,0)$.

4) **Straight Line:** $\beta = \left(\frac{|h|^2}{|z|^2}\right)\alpha$.

5) **Straight Line:** $\beta = \alpha$.

Since the β axis, i.e., $\alpha = 0$, is a tangent to exponential MMSE β vs α curve at the origin $(0,0)$, the exponential MMSE β vs α curve will always intersect with the $\beta = \left(\frac{|h|^2}{|z|^2}\right)\alpha$ line at a point other than $(0,0)$. This implies that for exponential MMSE function, there exists a $P = P_{opt}$ which makes (34) zero. Uniqueness of P_{opt} can be confirmed by substituting exponential MMSE function directly in (34). Also, since $|h| > |z| \geq 0$, R_s^f will attain it's maximum value at $P = P_{opt}$.

When the MMSE function is Gaussian, the Gaussian MMSE β vs α curve, $\beta = \frac{1}{\left(1 + \frac{|z|^2}{|h|^2}\left(\frac{1}{\alpha} - 1\right)\right)}$, does not intersect with $\beta = \left(\frac{|h|^2}{|z|^2}\right)\alpha$ line at any other point other than $(0,0)$. In fact, the $\beta = \left(\frac{|h|^2}{|z|^2}\right)\alpha$ line is tangent to the Gaussian MMSE β vs α curve at $(0,0)$. This implies that for Gaussian MMSE, there is no $P = P_{opt}$ which makes (34) zero. This fact can also be confirmed by substituting the Gaussian MMSE function directly in (34).

The MMSE function of M-ary alphabets at high SNRs decreases exponentially, which means β axis, i.e., $\alpha = 0$, is tangent to M-ary MMSE β vs α curve at the origin $(0,0)$. This implies that M-ary MMSE β vs α curve will always intersect with $\beta = \left(\frac{|h|^2}{|z|^2}\right)\alpha$ line at a point other than $(0,0)$. This shows that for M-ary MMSE function, there exists a $P = P_{opt}$ which makes (34) zero. To prove the uniqueness of P_{opt}, let $|h|^2 \text{MMSE}(|h|^2 P)$ and $|z|^2 \text{MMSE}(|z|^2 P)$ in (34) intersect for the first time at $P = P_{opt}$ from $P = 0$. Since $|h| > |z| \geq 0$, this implies that $|h|^2 \text{MMSE}(|h|^2 P) > |z|^2 \text{MMSE}(|z|^2 P)$ for all $P < P_{opt}$ and $|h|^2 \text{MMSE}(|h|^2 P) < |z|^2 \text{MMSE}(|z|^2 P)$ in some neighborhood of $P > P_{opt}$. Monotonicity of MMSE [16] implies that $|h|^2 \text{MMSE}(|h|^2 P)$ and $|z|^2 \text{MMSE}(|z|^2 P)$ will not intersect for any finite $P > P_{opt}$. This can be seen in Fig. 4 also. This proves the uniqueness of P_{opt}. The above analysis also implies that at $P = P_{opt}$ the secrecy rate R_s^f will attain its maximum value.

A. Numerical computation of P_{opt}

We can find P_{opt} of (34) for M-ary MMSE functions using gradient based method as follows.

Step 1 : Let P_{opt} lie in the interval $[P_{ll}, \ P_{ul}]$, $P_{ll} \geq 0$, $P_{ul} \leq P$. Let ϵ be a small positive number.

Step 2 : $P_{opt} = (P_{ll} + P_{ul})/2$. Compute $\frac{dR_s^f}{dP}$ using (34) at P_{opt}.

Step 3 : If $\frac{dR_s^f}{dP} \geq 0$, then $P_{ll} = P_{opt}$; else $P_{ul} = P_{opt}$.

Repeat **Step 2** and **Step 3** until $P_{ul} - P_{ll} \leq \delta$, where δ is a small positive number.

Fig. 4. BPSK MMSE vs P curves with $|h|^2 = 2.0$ and $|z|^2 = 0.5$.

REFERENCES

[1] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraint," *Proc. IEEE ISIT'2007*, June 2007.
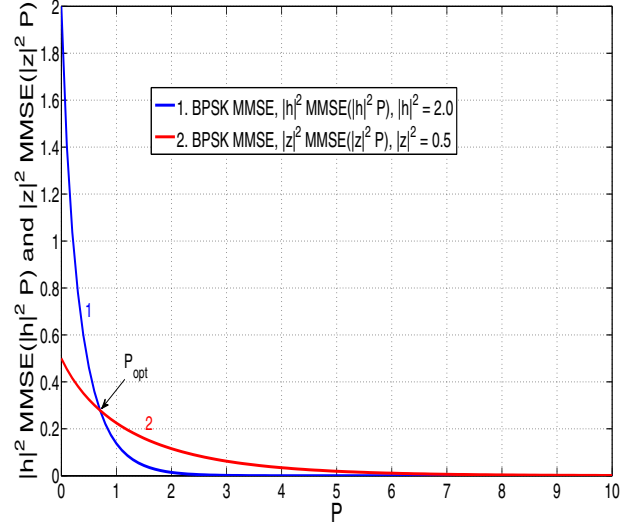
[2] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, July 2010.

[3] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *Proc. IEEE ISIT'2008*, July 2008.

[4] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, July 2010.

[5] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP Journ. on Wireless Commun. and Net.*, volume 2009, article ID 142374, 12 pages. doi:10.1155/2009/142374

[6] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176-1187, April 2011.

[7] J. Liu, Y. T. Hou, and H. D. Sherali "Optimal power allocation for achieving perfect secrecy capacity in MIMO wire-tap channels," *Proc. CISS'2009*, March 2009.

[8] S. A. A. Fakoorian and A. L. Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2620-2631, May 2013.

[9] M. R. D. Rodrigues, A. S. Baruch, and M. Bloch, "On Gaussian wiretap channels with M-PAM inputs," *2010 European Wireless Conference*, pp.774-781, April 2010.

[10] G. D. Raghava and B. S. Rajan, "Secrecy capacity of the Gaussian wire-tap channel with finite complex constellation input," Online: arXiv:1010.1163v1 [cs.IT] 6 Oct 2010.

[11] S. Bashar, Z. Ding, and C. Xiao, "On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input," *IEEE Commun. Letters*, vol. 15, no. 5, pp. 527-529, May 2011.

[12] S. Vishwakarma and A. Chockalingam, "Decode-and-forward relay beamforming for secrecy with finite-alphabet input," *IEEE Commun. Letters*, vol. 17, no. 5, pp. 912-915, May 2013.

[13] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite-alphabet signaling over MIMOME wiretap channels," *IEEE Trans. Veh. Tech.*, vol. 61, no. 6, pp. 2599-2612, July 2012.

[14] C. Paige and M. A. Saunders, "Towards a generalized singular value decomposition," *SIAM J. Numer. Anal.*, vol. 18, no. 3, pp. 398-405, June 1981.

[15] A. Lozano, A. M. Tulino, and S. Verdu, "Optimum power allocation for parallel Gaussian channels with arbitrary input distributions," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3033-3051, July 2006.

[16] D. Guo, Y. Wu, S. Shamai, and S. Verdu, "Estimation in Gaussian noise: properties of the minimum mean-square error," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2371-2385, April 2011.

[17] S. Boyd and L. Vandenberghe, *Convex optimization*, Cambridge Univ. Press, 2004.