Transmitter Optimization in MISO Broadcast Channel with Common and Secret Messages

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

***Abstract*—In this paper, we consider transmitter optimization in multiple-input single-output (MISO) broadcast channel with common and secret messages. The secret message is intended for K users and it is transmitted with perfect secrecy with respect to J eavesdroppers which are also assumed to be legitimate users in the network. The common message is transmitted at a fixed rate R_0 and it is intended for all K users and J eavesdroppers. The source operates under a total power constraint. It also injects artificial noise to improve the secrecy rate. We obtain the optimum covariance matrices associated with the common message, secret message, and artificial noise, which maximize the achievable secrecy rate and simultaneously meet the fixed rate R_0 for the common message.**

keywords: Physical layer security, MISO, common and secret messages, secrecy rate, artificial noise, multiple eavesdroppers.

I. Introduction

The concept of achieving perfect secrecy using physical layer techniques was first introduced in [1] on a degraded wiretap channel. Later, this work was extended to more general broadcast channel and Gaussian channel in [2] and [3], respectively. Achieving secrecy using physical layer techniques as opposed to cryptographic techniques does not rely on the computational limitation of the eavesdroppers. Wireless networks can be easily eavesdropped due to the broadcast nature of the information transmission. With the growing applications on wireless networks, there is a growing demand for achieving secrecy on these networks. Secrecy in single and multi antenna point-to-point wireless links has been studied by several authors, e.g., [4]–[11]. In all the previous works, the secret message is intended only for a single multi-antenna user in the presence of single multi-antenna eavesdropper. In [12], the achievability of the secrecy rate is shown where the secret message from a multi-antenna source is indended for multiple multi-antenna users in the presence of multiple multi-antenna, non-colluding eavesdroppers.

In [2], simultaneous transmission of a private message to receiver 1 at rate R_1 and a common message to receivers 1 and 2 at rate R_0 for two discrete memoryless channels (DMC) with common input was considered. Recently, the work in [2] has been extended to multiple-input multiple-output (MIMO) broadcast channel with confidential and common messages in [13]–[15]. Motivated by the works in [2,12]–[15], in this paper, we consider transmitter optimization in multiple-input single-output (MISO) broadcast channel with common and secret messages. The secret message is intended for K users

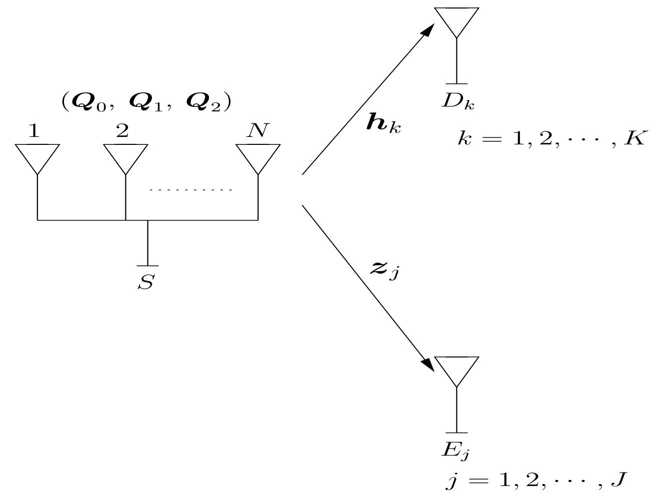

Fig. 1. System model for MISO broadcast channel with common and secret messages.

and it is transmitted with perfect secrecy with respect to J eavesdroppers which are also assumed to be legitimate users in the network. The common message is transmitted at a fixed rate R_0 and it is intended for all K users and J eavesdroppers. The source operates under a total power constraint. It also injects artificial noise to improve the secrecy rate. Under these settings, we obtain the optimum covariance matrices associated with the common message, secret message, and artificial noise, which maximize the achievable secrecy rate and simultaneously meet the fixed rate R_0 for the common message. We also note that the secrecy rate maximization in MISO channel without common message and in the presence of single eavesdropper has been considered in [16,17], and multiple eavesdroppers has been considered in [18] where the secret message is intended only for a single user (i.e., $K = 1$).

Notations : $\boldsymbol{A} \in \mathbb{C}^{N_1 \times N_2}$ implies that $\boldsymbol{A}$ is a complex matrix of dimension $N_1 \times N_2$. $\boldsymbol{A} \succeq \boldsymbol{0}$ and $\boldsymbol{A} \succ \boldsymbol{0}$ imply that $\boldsymbol{A}$ is a positive semidefinite matrix and positive definite matrix, respectively. Identity matrix is denoted by $\boldsymbol{I}$. Complex conjugate transpose operation is denoted by $[.]^{*}$. $\mathbb{E}[.]$ denotes the expectation operator, and $\|.\|$ denotes the 2-norm operator.

II. System Model

Consider a MISO broadcast channel as shown in Fig. 1 which consists of a source S having N transmit antennas, K users $\{D_1, D_2, \cdots, D_K\}$ each having single antenna, and J eavesdroppers $\{E_1, E_2, \cdots, E_J\}$ each having single antenna. The complex channel gain from S to D_k is denoted by $\boldsymbol{h}_k \in$

This work was supported in part by the Indo-French Centre for Applied Mathematics.

$\mathbb{C}^{1\times N}$, $1 \le k \le K$. Likewise, the complex channel gain from S to E_j is denoted by $\boldsymbol{z}_j \in \mathbb{C}^{1\times N}$, $1 \le j \le J$. We assume that eavesdroppers are non-colluding.

Let P_T denote the total transmit power budget in the system, i.e., the source S operates under total power constraint P_T. The communication between the source and the users and eavesdroppers happens in n channel uses. The source S transmits two independent messages W_0 and W_1, which are equiprobable over $\{1, 2, \cdots, 2^{nR_0}\}$ and $\{1, 2, \cdots, 2^{nR_1}\}$, respectively. W_0 is the common message to be conveyed to all D_ks and E_js at information rate R_0. W_1 is the secret message which has to be conveyed to all D_ks at some rate R_1 with perfect secrecy with respect to all E_js. For each W_0 drawn equiprobably from the set $\{1, 2, \cdots, 2^{nR_0}\}$, the source maps W_0 to a codeword $\{\boldsymbol{X}_i^0\}_{i=1}^n$ of length n, where each $\boldsymbol{X}_i^0 \in \mathbb{C}^{N\times 1}$, i.i.d. $\sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{Q}_0)$, $\mathbb{E}[\boldsymbol{X}_i^0] = \boldsymbol{0}$, and $\boldsymbol{Q}_0 = \mathbb{E}[\boldsymbol{X}_i^0 \boldsymbol{X}_i^{0*}]$. Similarly, for each W_1 drawn equiprobably from the set $\{1, 2, \cdots, 2^{nR_1}\}$, the source, using a stochastic encoder, maps W_1 to a codeword $\{\boldsymbol{X}_i^1\}_{i=1}^n$ of length n, where each $\boldsymbol{X}_i^1 \in \mathbb{C}^{N\times 1}$, i.i.d. $\sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{Q}_1)$, $\mathbb{E}[\boldsymbol{X}_i^1] = \boldsymbol{0}$, and $\boldsymbol{Q}_1 = \mathbb{E}[\boldsymbol{X}_i^1 \boldsymbol{X}_i^{1*}]$. The source also injects artificial noise sequence $\{\boldsymbol{X}_i^2\}_{i=1}^n$ of length n, where each $\boldsymbol{X}_i^2 \in \mathbb{C}^{N\times 1}$, i.i.d. $\sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{Q}_2)$, $\mathbb{E}[\boldsymbol{X}_i^2] = \boldsymbol{0}$, and $\boldsymbol{Q}_2 = \mathbb{E}[\boldsymbol{X}_i^2 \boldsymbol{X}_i^{2*}]$. In the ith channel use, $1 \le i \le n$, the source transmits the sum of the symbols which is $\boldsymbol{X}_i^0 + \boldsymbol{X}_i^1 + \boldsymbol{X}_i^2$. Since the source is power limited, this implies that

$$trace(\boldsymbol{Q}_0) + trace(\boldsymbol{Q}_1) + trace(\boldsymbol{Q}_2) \ \le \ P_T. \tag{1}$$

In the following, we will use $\boldsymbol{X}^0$, $\boldsymbol{X}^1$ and $\boldsymbol{X}^2$ to denote the symbols in the codewords $\{\boldsymbol{X}_i^0\}_{i=1}^n$ and $\{\boldsymbol{X}_i^1\}_{i=1}^n$, and the artificial noise sequence $\{\boldsymbol{X}_i^2\}_{i=1}^n$, respectively. We also assume that all the channel gains are known and remain static over the codeword transmit duration. Let y_{D_k} and y_{E_j} denote the received signals at D_k and E_j, respectively. We have

$$\begin{aligned} y_{D_k} &= \boldsymbol{h}_k(\boldsymbol{X}^0 + \boldsymbol{X}^1 + \boldsymbol{X}^2) + \eta_{D_k}, \ \forall k = 1, 2, \cdots, K, && (2)\\ y_{E_j} &= \boldsymbol{z}_j(\boldsymbol{X}^0 + \boldsymbol{X}^1 + \boldsymbol{X}^2) + \eta_{E_j}, \ \forall j = 1, 2, \cdots, J, && (3) \end{aligned}$$

where the ηs are the noise components, assumed to be i.i.d. $\sim \mathcal{CN}(0, N_0)$. Denoting the common and secret decoded messages at destination D_k by $\widehat{W}_0^{D_k}$ and $\widehat{W}_1^{D_k}$, respectively, and at eavesdropper E_j by $\widehat{W}_0^{E_j}$ and $\widehat{W}_1^{E_j}$, respectively, the reliability constraints at D_ks and E_js and the perfect secrecy constraints at E_js are as follows:

$$\begin{aligned} \Pr(\widehat{W}_0^{D_k} \ne W_0) &\le \epsilon_n, \ \forall k = 1, 2, \cdots, K,\\ \Pr(\widehat{W}_0^{E_j} \ne W_0) &\le \epsilon_n, \ \forall j = 1, 2, \cdots, J,\\ \Pr(\widehat{W}_1^{D_k} \ne W_1 \mid \widehat{W}_0^{D_k} = W_0) &\le \epsilon_n, \ \forall k = 1, 2, \cdots, K,\\ \frac{1}{n} I(W_1; \boldsymbol{y}_{E_j} \mid \widehat{W}_0^{E_j} = W_0) &\le \epsilon_n, \ \forall j = 1, 2, \cdots, J, \end{aligned}$$

where $\boldsymbol{y}_{E_j} = [y_{E_{j1}}, \ y_{E_{j2}}, \cdots, \ y_{E_{jn}}] \in \mathbb{C}^{1\times n}$ is the received signal at E_j in n channel uses, and $\epsilon_n \to 0$ as $n \to \infty$.

III. Transmitter optimization in MISO broadcast channel

Since the symbol $\boldsymbol{X}^0$ is transmitted at information rate R_0 irrespective of $\boldsymbol{X}^1$, treating $\boldsymbol{X}^1$ as noise in (2), D_ks will be able to decode $\boldsymbol{X}^0$ if $\forall k = 1, 2, \cdots, K$,

$$I(\boldsymbol{X}^0; y_{D_k}) \ = \ \log_2\Big(1 + \frac{\boldsymbol{h}_k \boldsymbol{Q}_0 \boldsymbol{h}_k^*}{N_0 + \boldsymbol{h}_k(\boldsymbol{Q}_1 + \boldsymbol{Q}_2)\boldsymbol{h}_k^*}\Big) \ \ge \ R_0. \tag{4}$$

Similarly, treating $\boldsymbol{X}^1$ as noise in (3), E_js will be able to decode $\boldsymbol{X}^0$ if $\forall j = 1, 2, \cdots, J$,

$$I(\boldsymbol{X}^0; y_{E_j}) \ = \ \log_2\Big(1 + \frac{\boldsymbol{z}_j \boldsymbol{Q}_0 \boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j(\boldsymbol{Q}_1 + \boldsymbol{Q}_2)\boldsymbol{z}_j^*}\Big) \ \ge \ R_0. \tag{5}$$

Using (2) and with the knowledge of the symbol $\boldsymbol{X}^0$, the information rate for $\boldsymbol{X}^1$ at D_k is

$$I(\boldsymbol{X}^1; y_{D_k} \mid \boldsymbol{X}^0) \ = \ \log_2\Big(1 + \frac{\boldsymbol{h}_k \boldsymbol{Q}_1 \boldsymbol{h}_k^*}{N_0 + \boldsymbol{h}_k \boldsymbol{Q}_2 \boldsymbol{h}_k^*}\Big). \tag{6}$$

Similarly, using (3) and with the knowledge of $\boldsymbol{X}^0$, the information rate for $\boldsymbol{X}^1$ at E_j is

$$I(\boldsymbol{X}^1; y_{E_j} \mid \boldsymbol{X}^0) \ = \ \log_2\Big(1 + \frac{\boldsymbol{z}_j \boldsymbol{Q}_1 \boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j \boldsymbol{Q}_2 \boldsymbol{z}_j^*}\Big). \tag{7}$$

A. Transmitter optimization - without artificial noise

In this subsection, we consider transmitter optimization in MISO broadcast channel when no artificial noise is injected by the source. Subject to the constraints in (1), (4) and (5), the achievable secrecy rate for $\boldsymbol{X}^1$ is obtained by solving the following optimization problem:

$$\begin{aligned} R_1 \ &= \ \max_{\boldsymbol{Q}_0,\ \boldsymbol{Q}_1} \ \min_{\substack{k=1,2,\cdots,K\\ j=1,2,\cdots,J}} \\ &\Big\{ I(\boldsymbol{X}^1; y_{D_k} \mid \boldsymbol{X}^0) - I(\boldsymbol{X}^1; y_{E_j} \mid \boldsymbol{X}^0) \Big\} && (8)\\ &= \max_{\boldsymbol{Q}_0,\ \boldsymbol{Q}_1} \ \min_{\substack{k=1,2,\cdots,K\\ j=1,2,\cdots,J}} \log_2\left(\frac{1 + \frac{\boldsymbol{h}_k \boldsymbol{Q}_1 \boldsymbol{h}_k^*}{N_0}}{1 + \frac{\boldsymbol{z}_j \boldsymbol{Q}_1 \boldsymbol{z}_j^*}{N_0}}\right) && (9)\\ &= \log_2 \max_{\boldsymbol{Q}_0,\ \boldsymbol{Q}_1} \ \min_{\substack{k=1,2,\cdots,K\\ j=1,2,\cdots,J}} \left(\frac{N_0 + \boldsymbol{h}_k \boldsymbol{Q}_1 \boldsymbol{h}_k^*}{N_0 + \boldsymbol{z}_j \boldsymbol{Q}_1 \boldsymbol{z}_j^*}\right) && (10)\\ \text{s.t.} \quad &\forall k = 1, 2, \cdots, K, \quad \forall j = 1, 2, \cdots, J,\\ &\log_2\Big(1 + \frac{\boldsymbol{h}_k \boldsymbol{Q}_0 \boldsymbol{h}_k^*}{N_0 + \boldsymbol{h}_k \boldsymbol{Q}_1 \boldsymbol{h}_k^*}\Big) \ \ge \ R_0, && (11)\\ &\log_2\Big(1 + \frac{\boldsymbol{z}_j \boldsymbol{Q}_0 \boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j \boldsymbol{Q}_1 \boldsymbol{z}_j^*}\Big) \ \ge \ R_0, && (12)\\ &\boldsymbol{Q}_0 \succeq \boldsymbol{0}, \quad \boldsymbol{Q}_1 \succeq \boldsymbol{0}, \quad trace(\boldsymbol{Q}_0) + trace(\boldsymbol{Q}_1) \ \le \ P_T. && (13) \end{aligned}$$

The constraints (11) and (12) are obtained from (4) and (5), respectively. The objective function in (8) is obtained from (6) and (7). We note that the achievability of the rate pair (R_1, R_0) can be seen by the repeated application of Lemma 1 in [12] as follows:

(a) *Achievability of the common message rate* R_0: Since the symbol $\boldsymbol{X}^1$ has been treated as noise in (4) and (5), the achievability of the common message rate R_0 follows from Lemma 1 in [12].

(b) *Achievability of the perfect secrecy rate* R_1: Having decoded the symbol $\boldsymbol{X}^0$ by all $(K + J)$ users, the achievability of the perfect secrecy rate R_1 for $\boldsymbol{X}^1$, which is intended only for K users, follows again from Lemma 1 in [12].

We now rewrite the optimization problem in (10) in the following equivalent form:

$$\max_{\boldsymbol{Q}_0,\ \boldsymbol{Q}_1} \min_{\substack{k=1,2,\cdots,K\\ j=1,2,\cdots,J}} \left(\frac{N_0 + \boldsymbol{h}_k\boldsymbol{Q}_1\boldsymbol{h}_k^*}{N_0 + \boldsymbol{z}_j\boldsymbol{Q}_1\boldsymbol{z}_j^*}\right) \tag{14}$$

$$\text{s.t.} \quad \forall k = 1,2,\cdots,K, \quad \forall j = 1,2,\cdots,J,$$
$$\left(1 + \frac{\boldsymbol{h}_k\boldsymbol{Q}_0\boldsymbol{h}_k^*}{N_0 + \boldsymbol{h}_k\boldsymbol{Q}_1\boldsymbol{h}_k^*}\right) \geq 2^{R_0},$$
$$\left(1 + \frac{\boldsymbol{z}_j\boldsymbol{Q}_0\boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j\boldsymbol{Q}_1\boldsymbol{z}_j^*}\right) \geq 2^{R_0},$$
$$\boldsymbol{Q}_0 \succeq \boldsymbol{0}, \quad \boldsymbol{Q}_1 \succeq \boldsymbol{0}, \quad trace(\boldsymbol{Q}_0) + trace(\boldsymbol{Q}_1) \leq P_T. \tag{15}$$

Further, we rewrite the innermost minimization in (14), namely,

$$\min_{\substack{k=1,2,\cdots,K\\ j=1,2,\cdots,J}} \left(\frac{N_0 + \boldsymbol{h}_k\boldsymbol{Q}_1\boldsymbol{h}_k^*}{N_0 + \boldsymbol{z}_j\boldsymbol{Q}_1\boldsymbol{z}_j^*}\right), \tag{16}$$

in the following equivalent maximization form:

$$\max_t \ t \tag{17}$$
$$\text{s.t.} \quad \forall k = 1,2,\cdots,K, \quad \forall j = 1,2,\cdots,J,$$
$$t\big(N_0 + \boldsymbol{z}_j\boldsymbol{Q}_1\boldsymbol{z}_j^*\big) - \big(N_0 + \boldsymbol{h}_k\boldsymbol{Q}_1\boldsymbol{h}_k^*\big) \leq 0. \tag{18}$$

Substituting the above maximization form in (14), we get the following single maximization form:

$$\max_{\boldsymbol{Q}_0,\ \boldsymbol{Q}_1,\ t} \ t \tag{19}$$
$$\text{s.t.} \quad \forall k = 1,2,\cdots,K, \quad \forall j = 1,2,\cdots,J,$$
$$t\big(N_0 + \boldsymbol{z}_j\boldsymbol{Q}_1\boldsymbol{z}_j^*\big) - \big(N_0 + \boldsymbol{h}_k\boldsymbol{Q}_1\boldsymbol{h}_k^*\big) \leq 0,$$
$$\big(2^{R_0} - 1\big)\big(N_0 + \boldsymbol{h}_k\boldsymbol{Q}_1\boldsymbol{h}_k^*\big) - \big(\boldsymbol{h}_k\boldsymbol{Q}_0\boldsymbol{h}_k^*\big) \leq 0,$$
$$\big(2^{R_0} - 1\big)\big(N_0 + \boldsymbol{z}_j\boldsymbol{Q}_1\boldsymbol{z}_j^*\big) - \big(\boldsymbol{z}_j\boldsymbol{Q}_0\boldsymbol{z}_j^*\big) \leq 0,$$
$$\boldsymbol{Q}_0 \succeq \boldsymbol{0}, \quad \boldsymbol{Q}_1 \succeq \boldsymbol{0}, \quad trace(\boldsymbol{Q}_0) + trace(\boldsymbol{Q}_1) \leq P_T. \tag{20}$$

For a given t, the above problem is formulated as the following semidefinite feasibility problem [19]:

$$\text{find} \quad \boldsymbol{Q}_0,\ \boldsymbol{Q}_1, \tag{21}$$

subject to the constraints in (20). The maximum value of t, denoted by t_{max}, can be obtained using bisection method as follows. Let t_{max} lie in the interval $[t_{ll}, t_{ul}]$. The value of t_{ll} can be taken as 1 (corresponding to the minimum secrecy rate of 0) and t_{ul} can be taken as $(1 + \min_{k=1,2,\cdots,K} \frac{P_T\|\boldsymbol{h}_k\|^2}{N_0})$, which corresponds to the minimum information capacity among D_ks when the entire power P_T is allotted to the source S. Check the feasibility of (20) at $t = (t_{ll}+t_{ul})/2$. If feasible, then $t_{ll} = t$, else $t_{ul} = t$. Repeat this until $t_{ul} - t_{ll} \leq \zeta$, where ζ is a small positive number. Using t_{max} in (10), the secrecy rate is given by

$$R_1 = \log_2 t_{max}. \tag{22}$$

Remark: We note that the maximum common message information rate, R_0^{max}, can be obtained as follows:

$$R_0^{max} = \max_{\boldsymbol{Q}_0} \min_{\substack{k=1,2,\cdots,K\\ j=1,2,\cdots,J}} \left\{I\big(\boldsymbol{X}^0;\ y_{D_k}\big),\ I\big(\boldsymbol{X}^0;\ y_{E_j}\big)\right\} \tag{23}$$
$$\text{s.t.} \quad \boldsymbol{Q}_0 \succeq \boldsymbol{0}, \quad trace(\boldsymbol{Q}_0) \leq P_T, \tag{24}$$

where $I\big(\boldsymbol{X}^0;\ y_{D_k}\big)$ and $I\big(\boldsymbol{X}^0;\ y_{E_j}\big)$ in (23) are obtained from (4) and (5), respectively, with $\boldsymbol{Q}_1 = \boldsymbol{Q}_2 = \boldsymbol{0}$. The above optimization problem can be easily solved using the method as proposed above to solve (10). Also, using the KKT conditions, it can be shown that R_0^{max} attains its maximum value when $trace(\boldsymbol{Q}_0) = P_T$, i.e., when all the available power is used. This implies that for $R_1 > 0$, $R_0 < R_0^{max}$.

B. Rank-1 approximation of $\boldsymbol{Q}_1$ and $\boldsymbol{Q}_0$ - without artificial noise

The optimal solutions $\boldsymbol{Q}_0$ and $\boldsymbol{Q}_1$ obtained from (19) may or may not have rank 1. This can be easily seen from the KKT conditions of the optimization problem (19). We show this in the Appendix A. For practical application, a rank-1 approximation of $\boldsymbol{Q}_0$ and $\boldsymbol{Q}_1$ can be done as follows. Let $\boldsymbol{\phi}^0 \in \mathbb{C}^{N\times 1}$ and $\boldsymbol{\phi}^1 \in \mathbb{C}^{N\times 1}$ be the unit norm eigen directions of $\boldsymbol{Q}_0$ and $\boldsymbol{Q}_1$ corresponding to the largest eigen values, respectively. We take $P_0\boldsymbol{\phi}^0\boldsymbol{\phi}^{0*}$ and $P_1\boldsymbol{\phi}^1\boldsymbol{\phi}^{1*}$ as the rank-1 approximation of $\boldsymbol{Q}_0$ and $\boldsymbol{Q}_1$, respectively, where $P_0 \geq 0$, $P_1 \geq 0$ and $P_0 + P_1 \leq P_T$. We substitute $\boldsymbol{Q}_0 = P_0\boldsymbol{\phi}^0\boldsymbol{\phi}^{0*}$ and $\boldsymbol{Q}_1 = P_1\boldsymbol{\phi}^1\boldsymbol{\phi}^{1*}$ in the optimization problem (19), which results in the following optimization problem:

$$\max_{P_0,\ P_1,\ t} \ t \tag{25}$$
$$\text{s.t.} \quad \forall k = 1,2,\cdots,K, \quad \forall j = 1,2,\cdots,J,$$
$$t\big(N_0 + P_1\boldsymbol{z}_j\boldsymbol{\phi}^1\boldsymbol{\phi}^{1*}\boldsymbol{z}_j^*\big) - \big(N_0 + P_1\boldsymbol{h}_k\boldsymbol{\phi}^1\boldsymbol{\phi}^{1*}\boldsymbol{h}_k^*\big) \leq 0,$$
$$\big(2^{R_0} - 1\big)\big(N_0 + P_1\boldsymbol{h}_k\boldsymbol{\phi}^1\boldsymbol{\phi}^{1*}\boldsymbol{h}_k^*\big) - \big(P_0\boldsymbol{h}_k\boldsymbol{\phi}^0\boldsymbol{\phi}^{0*}\boldsymbol{h}_k^*\big) \leq 0,$$
$$\big(2^{R_0} - 1\big)\big(N_0 + P_1\boldsymbol{z}_j\boldsymbol{\phi}^1\boldsymbol{\phi}^{1*}\boldsymbol{z}_j^*\big) - \big(P_0\boldsymbol{z}_j\boldsymbol{\phi}^0\boldsymbol{\phi}^{0*}\boldsymbol{z}_j^*\big) \leq 0,$$
$$P_0 \geq 0, \quad P_1 \geq 0, \quad P_0 + P_1 \leq P_T. \tag{26}$$

For a given t, the above problem is formulated as the following linear feasibility problem:

$$\text{find} \quad P_0,\ P_1, \tag{27}$$

subject to the constraints in (26). The maximum value of t can be obtained using the bisection method and the corresponding secrecy rate can be obtained using (22).

C. Transmitter optimization - with artificial noise

In this subsection, we consider transmitter optimization in MISO broadcast channel when artificial noise is injected by the source. Subject to the constraints in (1), (4) and (5), the achievable secrecy rate for $\boldsymbol{X}^1$ is obtained by solving the following optimization problem:

$$R_1 = \max_{\boldsymbol{Q}_0,\ \boldsymbol{Q}_1,\ \boldsymbol{Q}_2} \min_{\substack{k=1,2,\cdots,K\\ j=1,2,\cdots,J}}$$
$$\Big\{I\big(\boldsymbol{X}^1; y_{D_k} \mid \boldsymbol{X}^0\big) - I\big(\boldsymbol{X}^1; y_{E_j} \mid \boldsymbol{X}^0\big)\Big\} \tag{28}$$

$$= \max_{\boldsymbol{Q}_0,\ \boldsymbol{Q}_1,\ \boldsymbol{Q}_2} \min_{\substack{k=1,2,\cdots,K\\ j=1,2,\cdots,J}} \log_2 \left(\frac{1 + \frac{\boldsymbol{h}_k\boldsymbol{Q}_1\boldsymbol{h}_k^*}{N_0 + \boldsymbol{h}_k\boldsymbol{Q}_2\boldsymbol{h}_k^*}}{1 + \frac{\boldsymbol{z}_j\boldsymbol{Q}_1\boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j\boldsymbol{Q}_2\boldsymbol{z}_j^*}}\right) \tag{29}$$

$$= \log_2 \max_{\boldsymbol{Q}_0,\ \boldsymbol{Q}_1,\ \boldsymbol{Q}_2} \min_{\substack{k=1,2,\cdots,K\\ j=1,2,\cdots,J}}$$
$$\left(\frac{N_0 + \boldsymbol{h}_k(\boldsymbol{Q}_2 + \boldsymbol{Q}_1)\boldsymbol{h}_k^*}{N_0 + \boldsymbol{h}_k\boldsymbol{Q}_2\boldsymbol{h}_k^*}\right)\left(\frac{N_0 + \boldsymbol{z}_j\boldsymbol{Q}_2\boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j(\boldsymbol{Q}_2 + \boldsymbol{Q}_1)\boldsymbol{z}_j^*}\right) \tag{30}$$
$$\text{s.t.} \quad \forall k = 1,2,\cdots,K, \quad \forall j = 1,2,\cdots,J,$$
$$\log_2\left(1 + \frac{\boldsymbol{h}_k\boldsymbol{Q}_0\boldsymbol{h}_k^*}{N_0 + \boldsymbol{h}_k(\boldsymbol{Q}_2 + \boldsymbol{Q}_1)\boldsymbol{h}_k^*}\right) \geq R_0, \tag{31}$$
$$\log_2\left(1 + \frac{\boldsymbol{z}_j\boldsymbol{Q}_0\boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j(\boldsymbol{Q}_2 + \boldsymbol{Q}_1)\boldsymbol{z}_j^*}\right) \geq R_0, \tag{32}$$

$$\boldsymbol{Q}_0 \succeq \boldsymbol{0}, \quad \boldsymbol{Q}_1 \succeq \boldsymbol{0}, \quad \boldsymbol{Q}_2 \succeq \boldsymbol{0},$$
$$trace(\boldsymbol{Q}_0) + trace(\boldsymbol{Q}_1) + trace(\boldsymbol{Q}_2) \ \leq \ P_T, \tag{33}$$

where the constraints (31) and (32) are obtained from (4) and (5), respectively, and the objective function in (28) is obtained from (6) and (7). We rewrite the optimization problem in (30) in the following equivalent form:

$$\max_{\boldsymbol{Q}_0,\ \boldsymbol{Q}_1,\ \boldsymbol{Q}_2} \ \min_{\substack{k=1,2,\cdots,K \\ j=1,2,\cdots,J}} \Big(\frac{N_0 + \boldsymbol{h}_k(\boldsymbol{Q}_2+\boldsymbol{Q}_1)\boldsymbol{h}_k^*}{N_0 + \boldsymbol{h}_k\boldsymbol{Q}_2\boldsymbol{h}_k^*}\Big) \Big(\frac{N_0 + \boldsymbol{z}_j\boldsymbol{Q}_2\boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j(\boldsymbol{Q}_2+\boldsymbol{Q}_1)\boldsymbol{z}_j^*}\Big) \tag{34}$$

$$\text{s.t.} \quad \forall k \ = \ 1,2,\cdots,K, \quad \forall j \ = \ 1,2,\cdots,J,$$
$$\Big(1 + \frac{\boldsymbol{h}_k\boldsymbol{Q}_0\boldsymbol{h}_k^*}{N_0 + \boldsymbol{h}_k(\boldsymbol{Q}_2+\boldsymbol{Q}_1)\boldsymbol{h}_k^*}\Big) \ \geq \ 2^{R_0},$$
$$\Big(1 + \frac{\boldsymbol{z}_j\boldsymbol{Q}_0\boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j(\boldsymbol{Q}_2+\boldsymbol{Q}_1)\boldsymbol{z}_j^*}\Big) \ \geq \ 2^{R_0},$$
$$\boldsymbol{Q}_0 \succeq \boldsymbol{0}, \quad \boldsymbol{Q}_1 \succeq \boldsymbol{0}, \quad \boldsymbol{Q}_2 \succeq \boldsymbol{0},$$
$$trace(\boldsymbol{Q}_0) + trace(\boldsymbol{Q}_1) + trace(\boldsymbol{Q}_2) \ \leq \ P_T. \tag{35}$$

Further, we rewrite the innermost minimization in (34), namely,

$$\min_{\substack{k=1,2,\cdots,K \\ j=1,2,\cdots,J}} \ \Big(\frac{N_0 + \boldsymbol{h}_k(\boldsymbol{Q}_2+\boldsymbol{Q}_1)\boldsymbol{h}_k^*}{N_0 + \boldsymbol{h}_k\boldsymbol{Q}_2\boldsymbol{h}_k^*}\Big) \Big(\frac{N_0 + \boldsymbol{z}_j\boldsymbol{Q}_2\boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j(\boldsymbol{Q}_2+\boldsymbol{Q}_1)\boldsymbol{z}_j^*}\Big), \tag{36}$$

in the following equivalent maximization form:

$$\max_{u,\ v} \quad uv \tag{37}$$
$$\text{s.t.} \quad \forall k \ = \ 1,2,\cdots,K, \quad \forall j \ = \ 1,2,\cdots,J,$$
$$u \ \geq 0, \quad v \ \geq 0,$$
$$u\big(N_0 + \boldsymbol{h}_k\boldsymbol{Q}_2\boldsymbol{h}_k^*\big) - \Big(N_0 + \boldsymbol{h}_k(\boldsymbol{Q}_2+\boldsymbol{Q}_1)\boldsymbol{h}_k^*\Big) \ \leq \ 0,$$
$$v\Big(N_0 + \boldsymbol{z}_j(\boldsymbol{Q}_2+\boldsymbol{Q}_1)\boldsymbol{z}_j^*\Big) - \big(N_0 + \boldsymbol{z}_j\boldsymbol{Q}_2\boldsymbol{z}_j^*\big) \ \leq \ 0. \tag{38}$$

Substituting the above maximization form in (34), we get the following single maximization form:

$$\max_{\boldsymbol{Q}_0,\ \boldsymbol{Q}_1,\ \boldsymbol{Q}_2,\ u,\ v} \quad uv \tag{39}$$
$$\text{s.t.} \quad \forall k \ = \ 1,2,\cdots,K, \quad \forall j \ = \ 1,2,\cdots,J,$$
$$u \ \geq 0, \quad v \ \geq 0,$$
$$\big(2^{R_0}-1\big)\Big(N_0 + \boldsymbol{h}_k(\boldsymbol{Q}_2+\boldsymbol{Q}_1)\boldsymbol{h}_k^*\Big) - \big(\boldsymbol{h}_k\boldsymbol{Q}_0\boldsymbol{h}_k^*\big) \leq 0,$$
$$\big(2^{R_0}-1\big)\Big(N_0 + \boldsymbol{z}_j(\boldsymbol{Q}_2+\boldsymbol{Q}_1)\boldsymbol{z}_j^*\Big) - \big(\boldsymbol{z}_j\boldsymbol{Q}_0\boldsymbol{z}_j^*\big) \leq 0,$$
$$u\big(N_0 + \boldsymbol{h}_k\boldsymbol{Q}_2\boldsymbol{h}_k^*\big) - \Big(N_0 + \boldsymbol{h}_k(\boldsymbol{Q}_2+\boldsymbol{Q}_1)\boldsymbol{h}_k^*\Big) \leq 0,$$
$$v\Big(N_0 + \boldsymbol{z}_j(\boldsymbol{Q}_2+\boldsymbol{Q}_1)\boldsymbol{z}_j^*\Big) - \big(N_0 + \boldsymbol{z}_j\boldsymbol{Q}_2\boldsymbol{z}_j^*\big) \leq 0,$$
$$\boldsymbol{Q}_0 \succeq \boldsymbol{0}, \quad \boldsymbol{Q}_1 \succeq \boldsymbol{0}, \quad \boldsymbol{Q}_2 \succeq \boldsymbol{0},$$
$$trace(\boldsymbol{Q}_0) + trace(\boldsymbol{Q}_1) + trace(\boldsymbol{Q}_2) \ \leq \ P_T. \tag{40}$$

From the constraints in (40), it is obvious that the upper bound for u can be taken as $\big(1 + \min_{k=1,2,\cdots,K} \frac{P_T\|\boldsymbol{h}_k\|^2}{N_0}\big)$ and we denote it by u_{max}. Similarly, the upper bound for v can be taken as 1 and we denote it by v_{max}. We denote the optimum value of the optimization problem (39) by $u_{opt}v_{opt}$. For positive secrecy rate, $u_{max} \geq u_{opt} > 1$, $v_{max} \geq v_{opt} > 0$ and $u_{opt}v_{opt} > 1$. We obtain $u_{opt}v_{opt}$ sequentially by increasing u from 1 towards u_{max} in discrete steps of size $\triangle_u = (u_{max}-1)/M$, where M is a large positive integer, and finding the maximum v such that the constraints in (40) are feasible and the product uv is maximum. The algorithm to obtain $u_{opt}v_{opt}$ is as follows.

1. **for** $(i \ = \ 1 \ : \ 1 \ : \ M)$
2. **begin**
3. $u_i \ = \ 1 + (i \ast \ \triangle_u)$
4. $v_i \ = \ \max_{\substack{\boldsymbol{Q}_0,\ \boldsymbol{Q}_1,\ \boldsymbol{Q}_2,\ v, \\ u=u_i}} \ v$ s.t. all constraints in (40).
5. **if** $(i = 1)$ **then** $u_{opt} = u_i, \ v_{opt} = v_i$
6. **elseif** $(u_{opt}v_{opt} \ \leq \ u_iv_i)$ **then** $u_{opt} = u_i, \ v_{opt} = v_i$
7. **else** $u_{opt} = u_{opt}, \ v_{opt} = v_{opt}$
8. **endif**
9. **end for loop**

The constrained maximization problem in the for loop can be solved using the bisection method by checking the feasibility of the constraints in (40) at $u = u_i$ and v in the interval $[0, v_{max}]$. Having obtained $u_{opt}v_{opt}$, the secrecy rate is given by

$$R_1 = \log_2 u_{opt}v_{opt}. \tag{41}$$

We can take the rank-1 approximation of $\boldsymbol{Q}_1$ and $\boldsymbol{Q}_0$ as discussed in subsection III-B, i.e., by substituting $\boldsymbol{Q}_0 = P_0\boldsymbol{\phi}^0\boldsymbol{\phi}^{0*}$ and $\boldsymbol{Q}_1 = P_1\boldsymbol{\phi}^1\boldsymbol{\phi}^{1*}$ in the optimization problem (39) and solving for $P_0, \ P_1, \ \boldsymbol{Q}_2, \ u$ and v. An analysis of the rank for this system can be carried out along the same line as that in Appendix A.

IV. Results and Discussions

We present the numerical results and discussions in this section. We obtained the secrecy rate results through simulations for $N = 2$, $K = 2$ and $J = 1, 2, 3$ eavesdroppers. The following complex channel gains are taken in the simulations: $\boldsymbol{h}_1 = [0.7647 - 0.8345i, 0.9672 - 0.3692i]$, $\boldsymbol{h}_2 = [2.1455 + 0.4291i, 1.4245 - 1.1555i]$, $\boldsymbol{z}_1 = [-0.3473 + 0.2551i, 0.6134 - 0.0568i]$, $\boldsymbol{z}_2 = [0.5298 + 0.8579i, -1.2671 - 0.0428i]$, $\boldsymbol{z}_3 = [-0.2776 + 0.4551i, 0.4310 + 0.7209i]$.

Figure 2 shows the secrecy rate plots for MISO broadcast channel as a function of total transmit power (P_T) when no artificial noise is injected. The secrecy rates are plotted for the cases of with and without W_0. For the case with W_0, the information rate of W_0 is fixed at $R_0 = 1$. From Fig. 2, we observe that, for a given number of eavesdroppers, the secrecy rate degrades when W_0 is present. Also, the secrecy rate degrades for increasing number of eavesdroppers. Figure 3 shows the R_1 vs R_0 tradeoff, where R_1 is plotted as a function of R_0 for $K = 2$, $J = 1, 2, 3$ at a fixed total power of $P_T = 12$ dB and no artificial noise. It can be seen that as R_0 is increased, secrecy rate decreases. This is because the available transmit power for W_1 decreases as R_0 is increased. The point 3.16 on the R_0 axis where the secrecy rate drops to zero corresponds to R_0^{max}. Figure 4 shows the secrecy rate plots for MISO broadcast channel as a function of total

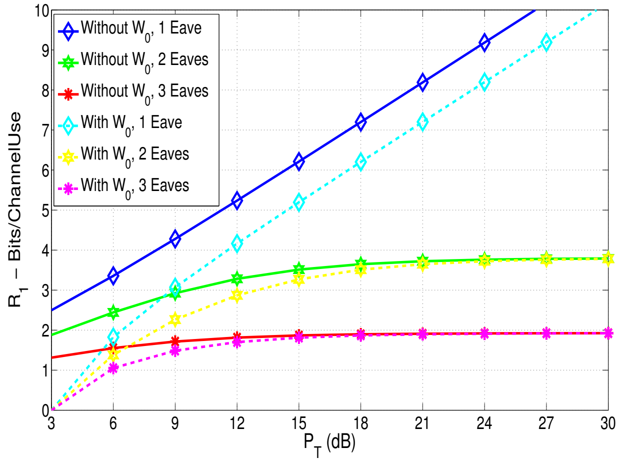

Fig. 2. Secrecy rate vs total power (P_T) in MISO broadcast channel with/without W_0 for $N = 2$, $K = 2$, $J = 1, 2, 3$, no artificial noise, and $R_0 = 1$.

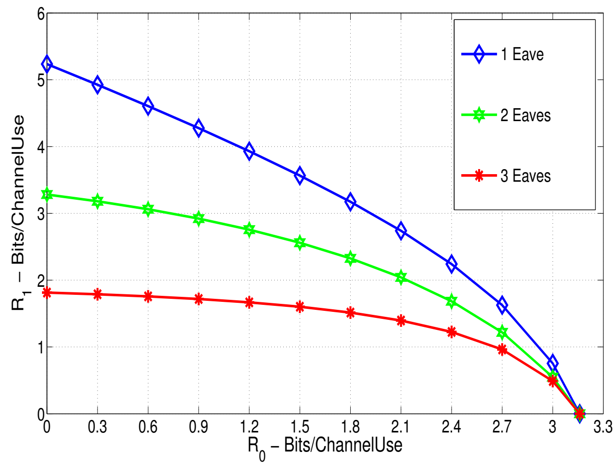

Fig. 3. R_1 vs R_0 in MISO broadcast channel for $N = 2$, $K = 2$, $J = 1, 2, 3$, $P_T = 12$ dB, and no artificial noise.

transmit power (P_T) when artificial noise is injected. Similarly, Fig. 5 shows the R_1 vs R_0 tradeoff with artificial noise, where R_1 is plotted as a function of R_0 for $K = 2$, $J = 1, 2, 3$ at a fixed total power of $P_T = 12$ dB. We observe a significant improvement in secrecy rate as compared to Fig. 2 and Fig. 3 when $J = 2$ or 3 eavesdroppers are present. When only one eavesdropper is present, artificial noise does not help in improving the secrecy rate. This is due to the null signal beamforming by the source at the eavesdropper which is only possible when $J < N$. Also, for the above channel conditions, we observe that the solutions $\boldsymbol{Q}_0$ and $\boldsymbol{Q}_1$ obtained by solving the optimization problems (19) and (39) have rank 1.

V. Conclusions

We investigated transmitter optimization problem in MISO broadcast channel with common and secret messages. The source operates under a total power constraint. It also injects artificial noise to improve the secrecy rate. We obtained the optimum covariance matrices associated with the common

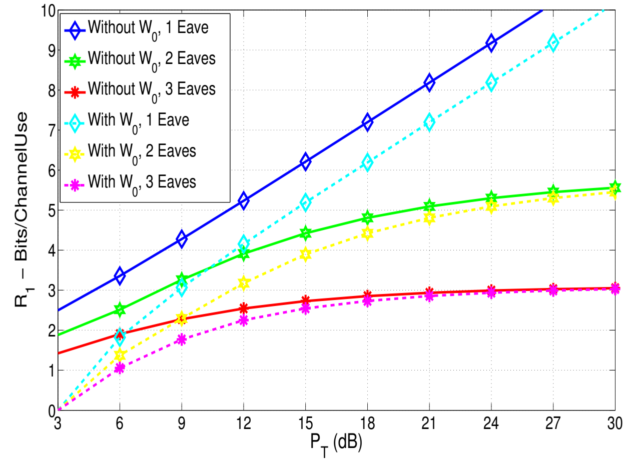

Fig. 4. Secrecy rate vs total power (P_T) in MISO broadcast channel with/without W_0 for $N = 2$, $K = 2$, $J = 1, 2, 3$, with artificial noise, and $R_0 = 1$.

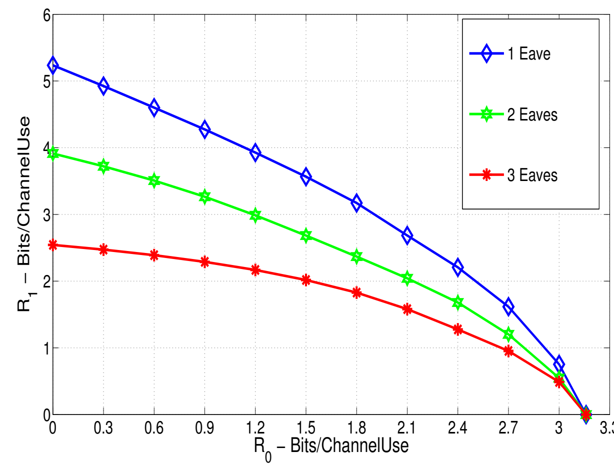

Fig. 5. R_1 vs R_0 in MISO broadcast channel for $N = 2$, $K = 2$, $J = 1, 2, 3$, $P_T = 12$ dB, and with artificial noise.

message, secret message, and artificial noise, which maximized the achievable secrecy rate and simultaneously met the fixed rate R_0 for the common message.

Appendix A

In this appendix, we analyze the rank of the solutions $\boldsymbol{Q}_0$ and $\boldsymbol{Q}_1$ which are obtained by solving the optimization problem (19). We take the Lagrangian of the objective function $-t$ subject to the constraints in (20) as follows [19]:

$$
\begin{aligned}
\ell(t,\ \boldsymbol{Q}_0,\ \boldsymbol{Q}_1,\ \lambda,\ \boldsymbol{\Lambda}_0,\ \boldsymbol{\Lambda}_1,\ \mu_{kj},\ \nu_k,\ \xi_j) \ &= \ -t \\
&+\lambda\Big(trace(\boldsymbol{Q}_0) + trace(\boldsymbol{Q}_1) - P_T\Big) \\
&-trace(\boldsymbol{\Lambda}_0\boldsymbol{Q}_0) - trace(\boldsymbol{\Lambda}_1\boldsymbol{Q}_1) \\
+\sum_{k=1}^{K}\sum_{j=1}^{J}\mu_{kj}\Big(t\big(N_0 + \boldsymbol{z}_j\boldsymbol{Q}_1\boldsymbol{z}_j^*\big) &- \big(N_0 + \boldsymbol{h}_k\boldsymbol{Q}_1\boldsymbol{h}_k^*\big)\Big) \\
+\sum_{k=1}^{K}\nu_k\Big(\big(2^{R_0}-1\big)\big(N_0 + \boldsymbol{h}_k\boldsymbol{Q}_1\boldsymbol{h}_k^*\big) &- \big(\boldsymbol{h}_k\boldsymbol{Q}_0\boldsymbol{h}_k^*\big)\Big)
\end{aligned}
$$

$$+\sum_{j=1}^{J}\xi_j\Big(\big(2^{R_0}-1\big)\big(N_0+\boldsymbol{z}_j\boldsymbol{Q}_1\boldsymbol{z}_j^*\big)-\big(\boldsymbol{z}_j\boldsymbol{Q}_0\boldsymbol{z}_j^*\big)\Big), \qquad (42)$$

where $\lambda \geq 0,\ \boldsymbol{\Lambda}_0 \succeq \mathbf{0},\ \boldsymbol{\Lambda}_1 \succeq \mathbf{0},\ \mu_{kj} \geq 0,\ \nu_k \geq 0,\ \xi_j \geq 0$ are the Lagrangian multipliers. The KKT conditions of (42) are as follows:

$(a.)$ all the constraints in (20),

$(b.)$ $\lambda\Big(trace(\boldsymbol{Q}_0)+trace(\boldsymbol{Q}_1)-P_T\Big)=0$,

$(c.)$ $trace(\boldsymbol{\Lambda}_0\boldsymbol{Q}_0)=0$. Since $\boldsymbol{\Lambda}_0 \succeq \mathbf{0}$ and $Q_0 \succeq \mathbf{0} \Longrightarrow \boldsymbol{\Lambda}_0\boldsymbol{Q}_0=\mathbf{0}$,

$(d.)$ $trace(\boldsymbol{\Lambda}_1\boldsymbol{Q}_1)=0$. Since $\boldsymbol{\Lambda}_1 \succeq \mathbf{0}$ and $Q_1 \succeq \mathbf{0} \Longrightarrow \boldsymbol{\Lambda}_1\boldsymbol{Q}_1=\mathbf{0}$,

$(e.)$ $\forall k=1,2,\cdots,K$, and $\forall j=1,2,\cdots,J$, $\mu_{kj}\Big(t\big(N_0+\boldsymbol{z}_j\boldsymbol{Q}_1\boldsymbol{z}_j^*\big)-\big(N_0+\boldsymbol{h}_k\boldsymbol{Q}_1\boldsymbol{h}_k^*\big)\Big)=0$,

$(f.)$ $\forall k=1,2,\cdots,K$, $\nu_k\Big(\big(2^{R_0}-1\big)\big(N_0+\boldsymbol{h}_k\boldsymbol{Q}_1\boldsymbol{h}_k^*\big)-\big(\boldsymbol{h}_k\boldsymbol{Q}_0\boldsymbol{h}_k^*\big)\Big)=0$,

$(g.)$ $\forall j=1,2,\cdots,J$, $\xi_j\Big(\big(2^{R_0}-1\big)\big(N_0+\boldsymbol{z}_j\boldsymbol{Q}_1\boldsymbol{z}_j^*\big)-\big(\boldsymbol{z}_j\boldsymbol{Q}_0\boldsymbol{z}_j^*\big)\Big)=0$,

$(h.)$ $\frac{\partial\ell}{\partial t}=0 \Longrightarrow \sum_{k=1}^{K}\sum_{j=1}^{J}\mu_{kj}\big(N_0+\boldsymbol{z}_j\boldsymbol{Q}_1\boldsymbol{z}_j^*\big)=1$. This implies that not all μ_{kj}s can be zero simultaneously.

$(i.)$ $\frac{\partial\ell}{\partial\boldsymbol{Q}_0}=\mathbf{0} \Longrightarrow \boldsymbol{\Lambda}_0=\lambda\boldsymbol{I}-\sum_{k=1}^{K}\nu_k\big(\boldsymbol{h}_k^*\boldsymbol{h}_k\big)-\sum_{j=1}^{J}\xi_j\big(\boldsymbol{z}_j^*\boldsymbol{z}_j\big)$,

$(j.)$ $\frac{\partial\ell}{\partial\boldsymbol{Q}_1}=\mathbf{0} \Longrightarrow \boldsymbol{\Lambda}_1=\lambda\boldsymbol{I}+\sum_{k=1}^{K}\sum_{j=1}^{J}\mu_{kj}\Big(t\big(\boldsymbol{z}_j^*\boldsymbol{z}_j\big)-\big(\boldsymbol{h}_k^*\boldsymbol{h}_k\big)\Big)+\big(2^{R_0}-1\big)\sum_{k=1}^{K}\nu_k\big(\boldsymbol{h}_k^*\boldsymbol{h}_k\big)+\big(2^{R_0}-1\big)\sum_{j=1}^{J}\xi_j\big(\boldsymbol{z}_j^*\boldsymbol{z}_j\big)$.

The KKT condtitions (c) and (d) imply that $trace(\boldsymbol{\Lambda}_0\boldsymbol{Q}_0)+trace(\boldsymbol{\Lambda}_1\boldsymbol{Q}_1)=0$. The KKT condtitions (i), (j), (b), (e), (f) and (g) further imply that

$$\lambda P_T+\sum_{k=1}^{K}\sum_{j=1}^{J}\mu_{kj}(1-t)N_0-\sum_{k=1}^{K}\nu_k\big(2^{R_0}-1\big)N_0 -\sum_{j=1}^{J}\xi_j\big(2^{R_0}-1\big)N_0 \;=\; 0.$$

For $R_1>0$, $t>1$. This implies that the above expression will be satisfied when $\lambda>0$. With $\lambda>0$, the KKT condition (b) implies that $trace(\boldsymbol{Q}_0)+trace(\boldsymbol{Q}_1)=P_T$, i.e., entire power is used for the transmission.

Assuming $\lambda>0$, we rewrite the KKT condition (j) in the following form:

$$\boldsymbol{\Lambda}_1+\sum_{k=1}^{K}\sum_{j=1}^{J}\mu_{kj}\big(\boldsymbol{h}_k^*\boldsymbol{h}_k\big) \;=\; \lambda\boldsymbol{I}+\sum_{k=1}^{K}\sum_{j=1}^{J}\mu_{kj}t\big(\boldsymbol{z}_j^*\boldsymbol{z}_j\big) + \big(2^{R_0}-1\big)\sum_{k=1}^{K}\nu_k\big(\boldsymbol{h}_k^*\boldsymbol{h}_k\big) \;+\; \big(2^{R_0}-1\big)\sum_{j=1}^{J}\xi_j\big(\boldsymbol{z}_j^*\boldsymbol{z}_j\big) \;\succ\; \mathbf{0}.$$

The above expression implies that $rank(\boldsymbol{\Lambda}_1) \geq N - rank\Big(\sum_{k=1}^{K}\sum_{j=1}^{J}\mu_{kj}\big(\boldsymbol{h}_k^*\boldsymbol{h}_k\big)\Big)$. The KKT condition (d) implies that $rank(\boldsymbol{Q}_1) \leq rank\Big(\sum_{k=1}^{K}\sum_{j=1}^{J}\mu_{kj}\big(\boldsymbol{h}_k^*\boldsymbol{h}_k\big)\Big)$. If $rank\Big(\sum_{k=1}^{K}\sum_{j=1}^{J}\mu_{kj}\big(\boldsymbol{h}_k^*\boldsymbol{h}_k\big)\Big)=1$ then $rank(\boldsymbol{Q}_1)=1$ (assuming $\boldsymbol{Q}_1 \neq \mathbf{0}$). For the special case when $K=1$, rank of $\boldsymbol{Q}_1$ will be 1 (assuming $\boldsymbol{Q}_1 \neq \mathbf{0}$). For $K>1$, the rank of $\boldsymbol{Q}_1$ may or may not be 1.

In order to determine the rank of $\boldsymbol{Q}_0$, we rewrite the KKT condition (i) in the following form:

$$\boldsymbol{\Lambda}_0+\sum_{k=1}^{K}\nu_k\big(\boldsymbol{h}_k^*\boldsymbol{h}_k\big)+\sum_{j=1}^{J}\xi_j\big(\boldsymbol{z}_j^*\boldsymbol{z}_j\big)=\lambda\boldsymbol{I}\succ\mathbf{0}.$$

The above expression implies that $rank(\boldsymbol{\Lambda}_0) \geq N - rank\Big(\sum_{k=1}^{K}\nu_k\big(\boldsymbol{h}_k^*\boldsymbol{h}_k\big)+\sum_{j=1}^{J}\xi_j\big(\boldsymbol{z}_j^*\boldsymbol{z}_j\big)\Big)$. Further, the KKT condition (c) implies that $rank(\boldsymbol{Q}_0) \leq rank\Big(\sum_{k=1}^{K}\nu_k\big(\boldsymbol{h}_k^*\boldsymbol{h}_k\big)+\sum_{j=1}^{J}\xi_j\big(\boldsymbol{z}_j^*\boldsymbol{z}_j\big)\Big)$. This implies that the rank of $\boldsymbol{Q}_0$ may or may not be 1.

REFERENCES

[1] A. Wyner, "The wire-tap channel," Bell. Syst Tech. J, vol. 54, no. 8, pp. 1355-1387, Jan. 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 339-348, May 1978.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 451-456, Jul. 1978.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, NOW Publishers, vol. 5, no. 4-5, 2009.

[5] Z. Li, R. Yates, and W. Trappe, "Secure Communication with a Fading Eavesdropper Channel," *Proc. IEEE ISIT'2007*, June 2007.

[6] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraint," *Proc. IEEE ISIT'2007*, June 2007.

[7] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

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

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

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

[11] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-II: The MIMOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[12] 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

[13] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5477-5487, Nov. 2010.

[14] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages," *IEEE Trans. Inform. Theory*, vol. 58, no. 9, pp. 5669-5680, Sep. 2012.

[15] R. Liu, T. Liu, and H. V. Poor, "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 59, no. 3, pp. 1346-1359, Mar. 2013.

[16] 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.

[17] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696-1707, April 2012.

[18] Q. Li and W. K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Sig. Proc.*, vol. 61, no. 10, pp. 2704-2717, Mar 2013.

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