Decode-and-Forward Relay Beamforming for Secrecy with Finite-Alphabet Input

Sanjay Vishwakarma and A. Chockalingam

***Abstract*—In this letter, we compute the secrecy rate of decode-and-forward (DF) relay beamforming with *finite input alphabet of size* M. Source and relays operate under a total power constraint. First, we observe that the secrecy rate with finite-alphabet input can go to zero as the total power increases, when we use the source power and the relay weights obtained assuming Gaussian input. This is because the capacity of an eavesdropper can approach the finite-alphabet capacity of $\frac{1}{2}\log_2 M$ with increasing total power, due to the inability to completely null in the direction of the eavesdropper. We then propose a transmit power control scheme where the optimum source power and relay weights are obtained by carrying out transmit power (source power plus relay power) control on DF with Gaussian input using semi-definite programming, and then obtaining the corresponding source power and relay weights which maximize the secrecy rate for DF with finite-alphabet input. The proposed power control scheme is shown to achieve increasing secrecy rates with increasing total power with a saturation behavior at high total powers.**

***Index Terms*—Cooperative relay beamforming, physical layer security, multiple eavesdroppers, finite-alphabet input, semi-definite programming.**

I. Introduction

PROVIDING security through physical layer mechanisms, where the intended receiver gets the information reliably while the eavesdroppers get no information, is an active area of recent research [1]. Recently, achievable secrecy rates in cooperative relaying schemes, using amplify-and-forward (AF) and decode-and-forward (DF) protocols, have been investigated [2], [3], [4]. In these works, the input alphabet is assumed to be Gaussian. However, finite-alphabet inputs (e.g., M-ary alphabets) will be used in practice. The effect of finite-alphabet inputs on the achievable secrecy rates has been studied in [5]- [9]. It has been shown that for a chosen constellation, increasing the power beyond a maximum point is harmful as the secrecy capacity curve dips continuously thereafter [5], [6]. Subsequently, in [7], a similar secrecy rate loss behavior at high transmit powers has been reported for multiple-input single-output (MISO) channels. It has been further shown that power control and jamming can restore the achieved secrecy rate to close to $\log_2 M$ at high transmit powers. In [8], design of optimum linear transmit precoding for maximum secrecy rate over multiple-input multiple-output (MIMO) wiretap channels with finite-alphabet input has been investigated. It has been shown that substantial improvement in secrecy rate can be achieved using the proposed design compared to the secrecy rate achieved by the design using Gaussian input assumption. Our contribution in this letter is that we study the effect of finite-alphabet input on the secrecy rate of cooperative relay beamforming, which has not been reported so far. In particular, we consider decode-and-forward (DF) relaying protocol with an input alphabet of size M. First, as in the previous studies [5], [6], [7], [9], we observe that the secrecy rate in DF beamforming also can go to zero with increasing total power, when Gaussian input optimized source power and relay weights are used with finite-alphabet input. This is because the information rate of an eavesdropper can approach $\frac{1}{2}\log_2 M$ with increasing total power, due to the inability to completely null in the direction of the eavesdropper. To alleviate this issue, we propose a transmit power control scheme where the optimum source power and relay weights are obtained by carrying out transmit power (source power plus relay power) control on DF with Gaussian input alphabet using semi-definite programming, and then obtaining the corresponding source power and relay weights which maximize the secrecy rate for DF with finite-alphabet input.

Manuscript received January 11, 2013. The associate editor coordinating the review of this letter and approving it for publication was R. Souza.

This work was supported in part by a gift from The Cisco University Research Program, a corporate advised fund of Silicon Valley Community Foundation.

The authors are with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore 560012, India (e-mail: {sanjay, achockal}@ece.iisc.ernet.in).

Digital Object Identifier 10.1109/LCOMM.2013.040213.130082

II. System Model

Consider the cooperative relay beamforming system model shown in Fig. 1, which consists of a source node S, N relay nodes $\{R_1, R_2, \cdots, R_N\}$, an intended destination node D, and J eavesdropper nodes $\{E_1, E_2, \cdots, E_J\}$, where J can be greater than N (i.e., more eavesdroppers than relays). In addition to the links from relays to destination node and relays to eavesdropper nodes, we assume direct links from source to destination node and source to eavesdropper nodes. The complex fading channel gains between source to relays are denoted by $\{\gamma_1^*, \gamma_2^*, \cdots, \gamma_N^*\}$. Likewise, the channel gains between relays to destination and relays to the jth eavesdropper are denoted by $\{\alpha_1^*, \alpha_2^*, \cdots, \alpha_N^*\}$ and $\{\beta_{1j}^*, \beta_{2j}^*, \cdots, \beta_{Nj}^*\}$, respectively, where $j = 1, 2, \cdots, J$. The channel gains on the direct links from source to destination and source to jth eavesdropper are denoted by α_0^* and β_{0j}^*, respectively. The channel gains are assumed to be i.i.d. complex Gaussian with zero mean and variances $\sigma^2_{\gamma_i^*}$, $\sigma^2_{\alpha_0^*}$, $\sigma^2_{\alpha_i^*}$, $\sigma^2_{\beta_{0j}^*}$, and $\sigma^2_{\beta_{ij}^*}$. As in previous studies [2], global channel state information (CSI) is assumed. This assumption can be justified when evesdroppers are legitimate users in the network [4].

Let P_0 denote the total transmit power budget in the system (i.e., source power plus relays power). We consider cooperative beamforming using decode-and-forward (DF) protocol. Previous studies on the secrecy rate of such relaying systems

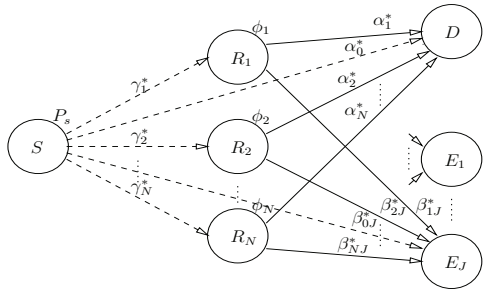


Fig. 1. System model of relay beamforming with multiple eavesdroppers.

have assumed codewords from Gaussian alphabet [2], [3], [4]. Unlike these previous studies, here we consider that the input codewords are from a finite alphabet of size M.

The source S transmits data in the first hop of transmission. Let x be the symbol transmitted from the source S with $\mathbb{E}\{|x|^2\} = 1$. In the second hop of transmission, relays which successfully decode this symbol retransmit it to the destination D. Without loss of generality, let all N relays decode the symbol successfully which aid the communication from S to D. Let P_s denote the power transmitted by the source in the first hop of transmission, and let $\{\phi_1, \phi_2, \cdots, \phi_N\}$ denote the complex weights applied on the transmitted signals at the N relays in the second hop of transmission.

Let y_{R_i} $(i = 1, 2, \cdots, N)$, y_{D_1} and $y_{E_{1j}}$ $(j = 1, 2, \cdots, J)$ denote the received signals at the ith relay, destination D and jth eavesdropper E_j, respectively, in the first hop of transmission. In the second hop of transmission, the received signals at the destination and jth eavesdropper are denoted by y_{D_2} and $y_{E_{2j}}$, respectively. We have

$$y_{D_1} = \sqrt{P_s}\alpha_0^* x + \eta_{D_1}, \quad y_{R_i} = \sqrt{P_s}\gamma_i^* x + \eta_{R_i}, \tag{1}$$

$$y_{E_{1j}} = \sqrt{P_s}\beta_{0j}^* x + \eta_{E_{1j}}, \quad y_{E_{2j}} = \boldsymbol{\beta}_j^\dagger \boldsymbol{\phi} x + \eta_{E_{2j}}, \tag{2}$$

$$y_{D_2} = \boldsymbol{\alpha}^\dagger \boldsymbol{\phi} x + \eta_{D_2}, \tag{3}$$

where $\boldsymbol{\phi} = [\phi_1, \phi_2, \cdots, \phi_N]^T, \boldsymbol{\alpha}^* = [\alpha_1^*, \alpha_2^*, \cdots, \alpha_N^*]^T, \boldsymbol{\beta}_j^* = [\beta_{1j}^*, \beta_{2j}^*, \cdots, \beta_{Nj}^*]^T$ and $[.]^T, (.)^*, [.]^\dagger$ denote transpose, conjugate, conjugate transpose operations, respectively. The noise components, η's, are assumed to be i.i.d. $\mathcal{CN}(0, N_0)$. We rewrite (1) and (3) in the following vector form:

$$\boldsymbol{y}_D = [y_{D_1}\ y_{D_2}]^T = [\sqrt{P_s}\alpha_0^* \quad \boldsymbol{\alpha}^\dagger \boldsymbol{\phi}]^T x + [\eta_{D_1}\ \eta_{D_2}]^T. \tag{4}$$

Taking the inner product of $\frac{[\sqrt{P_s}\alpha_0^* \quad \boldsymbol{\alpha}^\dagger \boldsymbol{\phi}]^T}{\sqrt{N_0(P_s\alpha_0^*\alpha_0 + \boldsymbol{\phi}^\dagger \boldsymbol{\alpha}\boldsymbol{\alpha}^\dagger \boldsymbol{\phi})}}$ with $\boldsymbol{y}_D$, (4) is transformed to the following scalar equation which is a sufficient statistics for detecting x at the destination D:

$$y_D = \sqrt{\frac{P_s\alpha_0^*\alpha_0 + \boldsymbol{\phi}^\dagger \boldsymbol{\alpha}\boldsymbol{\alpha}^\dagger \boldsymbol{\phi}}{N_0}} x + \eta_D, \tag{5}$$

where η_D is $\mathcal{CN}(0, 1)$. Similarly, we rewrite (2) in the following scalar form:

$$y_{E_j} = \sqrt{\frac{P_s\beta_{0j}^*\beta_{0j} + \boldsymbol{\phi}^\dagger \boldsymbol{\beta}_j \boldsymbol{\beta}_j^\dagger \boldsymbol{\phi}}{N_0}} x + \eta_{E_j}, \tag{6}$$

where η_{E_j} is $\mathcal{CN}(0, 1)$.

III. Secrecy Rate with Finite-Alphabet Input

First, consider that the source symbol x is from complex Gaussian alphabet. Let R_D^g, $R_{E_j}^g$, and $R_{R_i}^g$ denote the information rates at the destination D, jth eavesdropper E_j, and ith relay, respectively, with Gaussian input. Using (5), the expression for the information rate at the destination D is

$$R_D^g = \frac{1}{2}\log_2\big(1 + \frac{P_s\alpha_0^*\alpha_0 + \boldsymbol{\phi}^\dagger \boldsymbol{\alpha}\boldsymbol{\alpha}^\dagger \boldsymbol{\phi}}{N_0}\big). \tag{7}$$

Similarly, using (6), the expression for the information rate at the jth eavesdropper E_j $(j = 1, 2 \cdots, J)$ is

$$R_{E_j}^g = \frac{1}{2}\log_2\big(1 + \frac{P_s\beta_{0j}^*\beta_{0j} + \boldsymbol{\phi}^\dagger \boldsymbol{\beta}_j \boldsymbol{\beta}_j^\dagger \boldsymbol{\phi}}{N_0}\big). \tag{8}$$

Using (1), the information rate at the ith relay is given by

$$R_{R_i}^g = \frac{1}{2}\log_2\big(1 + \frac{P_s\gamma_i^*\gamma_i}{N_0}\big), \quad i = 1, 2 \cdots, N. \tag{9}$$

The factor $\frac{1}{2}$ appears in (7), (8) and (9) because of the two hops. Subject to the total power constraint and the information rate constraint to correctly decode the source symbol by the relays, the achievable secrecy rate R_s^g for DF is obtained by solving the following optimization problem [2]:

$$R_s^g = \max_{P_s, \boldsymbol{\phi}} \min_{j:1,2,\cdots,J} (R_D^g - R_{E_j}^g)$$

$$= \max_{P_s, \boldsymbol{\phi}} \min_{j:1,2,\cdots,J} \frac{1}{2}\log_2\big(\frac{N_0 + P_s\alpha_0^*\alpha_0 + \boldsymbol{\phi}^\dagger \boldsymbol{\alpha}\boldsymbol{\alpha}^\dagger \boldsymbol{\phi}}{N_0 + P_s\beta_{0j}^*\beta_{0j} + \boldsymbol{\phi}^\dagger \boldsymbol{\beta}_j \boldsymbol{\beta}_j^\dagger \boldsymbol{\phi}}\big) \tag{10}$$

$$\text{s.t. } P_s \geq 0,\ P_s + \boldsymbol{\phi}^\dagger \boldsymbol{\phi} \leq P_0,\ R_{R_i}^g \geq R_D^g,\ \forall i = 1, 2 \cdots, N, \tag{11}$$

where the constraints in (11) include power constraints and rate constraints for the relays to decode the transmitted symbol. Defining $\boldsymbol{\Phi} \triangleq \boldsymbol{\phi}\boldsymbol{\phi}^\dagger$, the kth relay's transmit power is given by the kth diagonal element of $\boldsymbol{\Phi}$. Further, defining $r \triangleq (N_0 + P_s\alpha_0^*\alpha_0 + \boldsymbol{\alpha}^\dagger \boldsymbol{\Phi}\boldsymbol{\alpha})$ and $s_j \triangleq (N_0 + P_s\beta_{0j}^*\beta_{0j} + \boldsymbol{\beta}_j^\dagger \boldsymbol{\Phi}\boldsymbol{\beta}_j)$, we can write (10) and (11) in the following equivalent form:

$$R_s^g = \max_{P_s, \boldsymbol{\Phi}} \min_{j:1,2,\cdots,J} \frac{1}{2}\log_2\frac{r}{s_j} = \frac{1}{2}\log_2\big(\max_{P_s, \boldsymbol{\Phi}} \min_{j:1,2,\cdots,J} \frac{r}{s_j}\big) \tag{12}$$

$$\text{s.t. } \boldsymbol{\Phi} \succeq 0,\ rank(\boldsymbol{\Phi}) = 1,\ P_s \geq 0,\ P_s + trace(\boldsymbol{\Phi}) \leq P_0,$$

$$\frac{1}{2}\log_2\big(1 + \frac{P_s\gamma_i^*\gamma_i}{N_0}\big) \geq \frac{1}{2}\log_2\big(1 + \frac{P_s\alpha_0^*\alpha_0 + \boldsymbol{\alpha}^\dagger \boldsymbol{\Phi}\boldsymbol{\alpha}}{N_0}\big),$$

$$\forall i = 1, 2, \cdots, N, \tag{13}$$

where (13) is by using (9) and (7) in (11). Further, relaxing the rank constraint on $\boldsymbol{\Phi}$ [10] and dropping the logarithms, the optimization problem (12) to compute the secrecy rate expression can be written in the following optimization form:

$$\max_{P_s, \boldsymbol{\Phi}} \min_{j:1,2,\cdots,J} \frac{r}{s_j} \tag{14}$$

$$\text{s.t. } \boldsymbol{\Phi} \succeq 0,\ P_s \geq 0,\ P_s + trace(\boldsymbol{\Phi}) \leq P_0,$$

$$N_0 + P_s\gamma_i^*\gamma_i \ \geq\ r,\ \forall i = 1, 2, \cdots, N. \tag{15}$$

The innermost minimization $\min_{j:1,\cdots,J} \frac{r}{s_j}$ is equivalent to $\max_t\ t$ such that $r - ts_j \geq 0, \forall j = 1, 2, \cdots, J$. So, we write (14) and (15) in the following single maximization form [3]:

$$\max_{P_s,\ \boldsymbol{\Phi}} \max_t\ t \ =\ \max_{P_s,\ \boldsymbol{\Phi},\ t}\ t \tag{16}$$

$$\text{s.t. } \boldsymbol{\Phi} \succeq 0,\ P_s \geq 0,\ P_s + trace(\boldsymbol{\Phi}) \leq P_0,$$

$$N_0 + P_s\gamma_i^*\gamma_i \ \geq\ r,\ \forall i = 1, 2, \cdots, N,$$

$$r - ts_j \ \geq 0,\ \forall j = 1, 2 \cdots, J. \tag{17}$$

For a given t, the above problem is formulated as the following semi-definite feasibility problem:

$$\text{find} \quad P_s,\ \boldsymbol{\Phi} \tag{18}$$

subject to the constraints in (17). The maximum value of t, denoted by t_{max}, can be obtained using bisection method as follows. Let t_{max} lie in the interval $[t_{ll},\ t_{ul}]$. Check the feasibility of (17) 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 (12), the secrecy rate is given by $R_s^g = \frac{1}{2}\log_2 t_{max}$. As in [10], we numerically verified that the solution of the optimization problem (16) is rank-1, i.e., $rank(\mathbf{\Phi}) = 1$. We take $\boldsymbol{\phi}$ in the largest eigen direction of relay weight matrix $\mathbf{\Phi}$ and denote it by $\boldsymbol{\phi}^g$. Let P_s^g denote the optimum source power. P_s^g and $\boldsymbol{\phi}^g$ will be used in the computation of the secrecy rate with finite-alphabet input, which is described next.

Consider the secrecy rate expression for DF when the source symbol x is from a finite alphabet of size M. Let $\mathbb{A} = \{a_1, a_2, \cdots, a_M\}$ denote the alphabet. We assume that all elements in $\mathbb{A}$ are equiprobable. Now, define $I(\rho) \stackrel{\triangle}{=}$

$$\frac{1}{2}\frac{1}{M}\sum_{l=1}^{M}\int p_n(y-\sqrt{\rho}a_l)\log_2\frac{p_n(y-\sqrt{\rho}a_l)}{\frac{1}{M}\sum_{m=1}^{M}p_n(y-\sqrt{\rho}a_m)}dy, \quad (19)$$

where $p_n(\theta) = \frac{1}{\pi}e^{-|\theta|^2}$. Using (5) and (19), the expression for the information rate at D with finite-alphabet input is

$$R_D^f = I\Big(\frac{P_s\alpha_0^*\alpha_0 + \boldsymbol{\phi}^\dagger\boldsymbol{\alpha}\boldsymbol{\alpha}^\dagger\boldsymbol{\phi}}{N_0}\Big). \quad (20)$$

Similarly, using (6) and (19), the information rate at the jth eavesdropper E_j is given by

$$R_{E_j}^f = I\Big(\frac{P_s\beta_{0j}^*\beta_{0j} + \boldsymbol{\phi}^\dagger\boldsymbol{\beta}_j\boldsymbol{\beta}_j^\dagger\boldsymbol{\phi}}{N_0}\Big). \quad (21)$$

Using (1) and (19), the information rate at the ith relay is given by

$$R_{R_i}^f = I\Big(\frac{P_s\gamma_i^*\gamma_i}{N_0}\Big). \quad (22)$$

Using (20), (21) and (22), we write the secrecy rate expression as

$$R_s^f = \max_{P_s,\boldsymbol{\phi}} \min_{j:1,2,\cdots,J} (R_D^f - R_{E_j}^f) \quad (23)$$

$$\text{s.t. } P_s \geq 0,\ P_s + \boldsymbol{\phi}^\dagger\boldsymbol{\phi} \leq P_0,\ R_{R_i}^f \geq R_D^f,\ \forall i = 1, 2, \cdots, N. \quad (24)$$

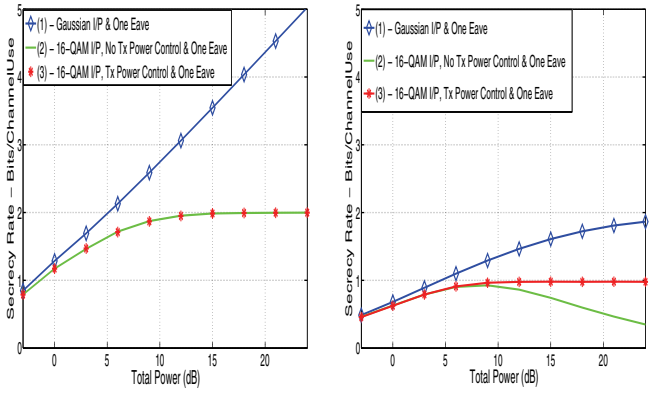
Solving the above problem for optimum source power P_s and $\boldsymbol{\phi}$ for a given total power P_0 is hard. One option would be to use the P_s^g and $\boldsymbol{\phi}^g$ obtained from (16). But, if P_s^g and $\boldsymbol{\phi}^g$ obtained from (16) are used directly in (23) without transmit power control for a given total power P_0, it could be adverse and lead to reduced secrecy rate as has been pointed out for the case of MISO in [7]. For the case of DF relay beamforming, we find the optimum transmit power P_{opt} (source power plus relay power) and the corresponding P_s^g and $\boldsymbol{\phi}^g$ such that the secrecy rate with finite-alphabet input in (23) is maximized for a given total power P_0. In the appendix, we prove that R_s^f is a unimodal function of the total power P_0 when P_s^g and $\boldsymbol{\phi}^g$ are used to find R_s^f. Therefore, we can use the gradient based method given below to find P_{opt} and the corresponding P_s^g and $\boldsymbol{\phi}^g$.

Step 1 : Let P_{opt} lie in the interval $[P_{ll},\ P_{ul}]$, $P_{ll} \geq 0$, $P_{ul} \leq P_0$. Let ϵ be a small positive number.

Step 2 : $P_{opt} = (P_{ll} + P_{ul})/2$. Solve (16) for $P_s^g(-\epsilon)$ and $\boldsymbol{\phi}^g(-\epsilon)$ at total power $P_{opt} - \epsilon$. Solve (16) for $P_s^g(+\epsilon)$ and $\boldsymbol{\phi}^g(+\epsilon)$ at total power $P_{opt} + \epsilon$.

Step 3 : Compute secrecy rate with finite-alphabet input in (23) at $P_s^g(-\epsilon)$, $\boldsymbol{\phi}^g(-\epsilon)$ and $P_s^g(+\epsilon)$, $\boldsymbol{\phi}^g(+\epsilon)$, and denote them by $R_s^f(-\epsilon)$ and $R_s^f(+\epsilon)$, respectively. If $R_s^f(-\epsilon) \leq R_s^f(+\epsilon)$, 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.



(a) No direct link. (b) With direct link.

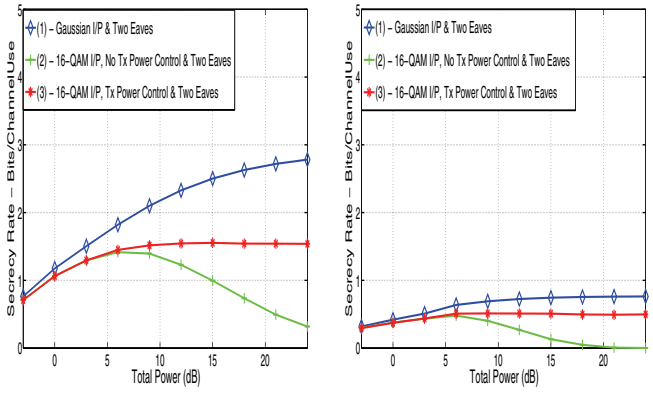
Fig. 2. Secrecy rate versus total power in DF relay beamforming with two relays ($N = 2$) and one eavesdropper ($J = 1$).

We note that (29) can also be used in **Step 2** and **Step 3**, i.e., compute (29) at $P_{opt} = (P_{ll} + P_{ul})/2$ and check the sign of (29) to find the new P_{ll} and P_{ul}. Alternatively, instead of using the gradient based algorithm described above, Golden section search (a technique for finding the extremum of a strictly unimodal function) can be used.

IV. Results and Discussions

We numerically evaluated the secrecy rate for DF relay beamforming for two relays ($N = 2$), varying number of eavesdroppers ($J = 1, 2$), 16-QAM ($M = 16$) and $N_0 = 1$. The following system parameters are used with and without direct links to destination and eavesdroppers: $\sigma_{\gamma_1^*} = \sigma_{\gamma_2^*} = 4$, $\sigma_{\alpha_1^*} = \sigma_{\alpha_2^*} = 4$, $\sigma_{\beta_{11}^*} = \sigma_{\beta_{21}^*} = 1$, $\sigma_{\beta_{12}^*} = \sigma_{\beta_{22}^*} = 2$. With direct links, $\sigma_{\alpha_0^*} = 2, \sigma_{\beta_{01}^*} = 0.5, \sigma_{\beta_{02}^*} = 1$. With no direct links, $\sigma_{\alpha_0^*} = \sigma_{\beta_{0j}^*} = 0, j = 1, 2$. These parameter settings correspond to the case where the relays-to-destination links are stronger than the relays-to-eavesdroppers links. Source-to-destination link is stronger than the source-to-eavesdroppers links, when direct links are present. We plot the secrecy rate versus total power P_0 with and without direct links for 1 and 2 eavesdroppers in Figs. 2 and 3, respectively. In each figure, secrecy rates for three different cases - denoted by (1), (2) and (3) in the legends - are plotted. In case (1), secrecy rates with Gaussian input are plotted. In case (2), secrecy rates with 16-QAM input using Gaussian optimized source power and relay beamforming vectors (without transmit power control) are plotted. In case (3), secrecy rates with 16-QAM using the source power and relay beamforming vectors obtained using the proposed transmit power control scheme are plotted.

From Fig. 2(a), we can observe that the secrecy rates with 16-QAM input without and with transmit power control are the same. This is because with 2 relays and 1 eavesdropper, complete nulling is achieved at the eavesdropper, resulting in zero information rate at the eavesdropper. Therefore, the secrecy rate follows the information rate at the destination, which increases with increasing total power, approaching the finite-alphabet capacity of $\frac{1}{2}\log_2 M = 2$ bits/channel use. However, such complete nulling may not be possible when the number of eavesdroppers are more than or equal to the number of relays, resulting in non-zero information rates at



(a) No direct link. (b) With direct link.

Fig. 3. Secrecy rate versus total power in DF relay beamforming with two relays ($N = 2$) and two eavesdroppers ($J = 2$).

the eavesdroppers that grow with the total power. Also, the information rate at the eavesdroppers will grow with total power if direct links between the source and eavesdroppers exist, resulting in reducing secrecy rate with increasing total power. This behavior is observed in 2(b). Figures 3(a) and 3(b) illustrate the effect of such non-zero information rate at the eavesdroppers on the secrecy rate when $J \geq N$ (for $N = 2$, $J = 2$). In Figs. 3(a) and 3(b), it can be observed that the secrecy rate without transmit power control (i.e., case (2)) increases with total power up to some point and then starts decreasing and goes to zero. This is due to the inability to completely null at the eavesdroppers, and, in addition, due to the presence of direct links to the eavesdroppers (in case of 3(b)). So, the information rates at both D and E_j's grow and approach the finite alphabet channel capacity of $\frac{1}{2}\log_2 M$. On the other hand, the proposed transmit power control scheme (i.e., case (3)) is able to avoid the secrecy rate decrease with increase in total power. With the proposed transmit power control, the secrecy rate increases with total power with a saturating behavior at high total power. Finally, we note that the secrecy rate can be increased by using the remaining available power for jamming purposes. Also, finite-alphabet secrecy rates with partial/imperfect CSI can be investigated as future extension to this work.

APPENDIX

We first show that for a given total power P_0, the Gaussian secrecy rate R_s^g in (10) attains its maximum when $P_s + \boldsymbol{\phi}^\dagger\boldsymbol{\phi} = P_0$, i.e., when entire total power is used. We write (10) and its constraints (11) in terms of a $N+1$ length vector $\boldsymbol{\psi}$ as

$$R_s^g = \max_{\boldsymbol{\psi}} \min_{j:1,2,\cdots,J} (R_D^g - R_{E_j}^g) =$$

$$\max_{\boldsymbol{\psi}} \min_{j:1,2,\cdots,J} \frac{1}{2}\log_2\left(1+\frac{\boldsymbol{\psi}^\dagger\mathbf{A}\boldsymbol{\psi}}{N_0}\right) - \frac{1}{2}\log_2\left(1+\frac{\boldsymbol{\psi}^\dagger\mathbf{B}_j\boldsymbol{\psi}}{N_0}\right) \quad (25)$$

$$\text{s.t.} \quad \boldsymbol{\psi}^\dagger\boldsymbol{\psi} \leq P_0,\ R_{R_i}^g - R_D^g = \frac{1}{2}\log_2\left(1+\frac{\boldsymbol{\psi}^\dagger\mathbf{C}_i\boldsymbol{\psi}}{N_0}\right)$$

$$-\frac{1}{2}\log_2\left(1+\frac{\boldsymbol{\psi}^\dagger\mathbf{A}\boldsymbol{\psi}}{N_0}\right) \geq 0,\ \forall i = 1,2\cdots,N, \quad (26)$$

where $\boldsymbol{\psi} = [\phi_0,\ \boldsymbol{\phi}]^T$, $P_s = \phi_0^*\phi_0$, and $\mathbf{A}$, $\mathbf{B}_j$ and $\mathbf{C}_i$ are $(N+1)\times(N+1)$ matrices given by $\mathbf{A} = [\alpha_0^*\alpha_0,\ \mathbf{0};\ \mathbf{0},\ \boldsymbol{\alpha}\boldsymbol{\alpha}^\dagger] \succeq 0$, $\mathbf{B}_j = [\beta_{0j}^*\beta_{0j},\ \mathbf{0};\ \mathbf{0},\ \boldsymbol{\beta}_j\boldsymbol{\beta}_j^\dagger] \succeq 0$, $\mathbf{C}_i = [\gamma_i^*\gamma_i,\ \mathbf{0};\ \mathbf{0},\ \mathbf{0}] \succeq 0$. Let the solution of the above optimization problem be $\boldsymbol{\psi}^g = \sqrt{P}\boldsymbol{\psi}_u^g$, where $\boldsymbol{\psi}_u^g$ is a unit-norm vector in the direction of $\boldsymbol{\psi}^g$, and let $R_s^g > 0$. From the power constraint, $\boldsymbol{\psi}^{g\dagger}\boldsymbol{\psi}^g = P\boldsymbol{\psi}_u^{g\dagger}\boldsymbol{\psi}_u^g = P \leq P_0$. Since $\frac{d(R_D^g - R_{E_j}^g)}{dP} > 0$ at $\boldsymbol{\psi} = \sqrt{P}\boldsymbol{\psi}_u^g$, $\forall j = 1,2,\cdots,J$, and $\frac{d(R_{R_i}^g - R_D^g)}{dP} \geq 0$ at $\boldsymbol{\psi} = \sqrt{P}\boldsymbol{\psi}_u^g$, $\forall i = 1,2,\cdots,N$, this implies that the secrecy rate maximum occurs at $P = P_0$. We next show that secrecy rate with finite-alphabet input using P_s^g and $\boldsymbol{\phi}^g$ has unique maximum in P_0. From the above result and (5), (6), the SNRs at the destination D and at the jth eavesdropper E_j are given, respectively, by

$$\frac{P_s^g\alpha_0^*\alpha_0 + \boldsymbol{\phi}^{g\dagger}\boldsymbol{\alpha}\boldsymbol{\alpha}^\dagger\boldsymbol{\phi}^g}{N_0} = \frac{\boldsymbol{\psi}_u^{g\dagger}\mathbf{A}\boldsymbol{\psi}_u^g}{N_0}P_0 \triangleq \rho_D P_0, \quad (27)$$

$$\frac{P_s^g\beta_{0j}^*\beta_{0j} + \boldsymbol{\phi}^{g\dagger}\boldsymbol{\beta}_j\boldsymbol{\beta}_j^\dagger\boldsymbol{\phi}^g}{N_0} = \frac{\boldsymbol{\psi}_u^{g\dagger}\mathbf{B}_j\boldsymbol{\psi}_u^g}{N_0}P_0 \triangleq \rho_{E_j}P_0. \quad (28)$$

Using (27), (28) and Theorem 1 in [11] to find the difference of the derivatives of R_D^f and $R_{E_j}^f$ w. r. t. P_0, we get

$$\frac{d(R_D^f - R_{E_j}^f)}{dP_0} = \frac{\left(\rho_D \text{MMSE}(\rho_D P_0) - \rho_{E_j}\text{MMSE}(\rho_{E_j}P_0)\right)\log_2 e}{2}. \quad (29)$$

For various M-ary alphabets, it is shown in [11] that a) MMSE is a strictly monotonic decreasing function in SNR, and b) at high SNRs, MMSE decreases exponentially (Theorems 3 and 4 in [11]). With the above facts and $\rho_D > \rho_{E_j} > 0$, the difference of the derivatives in (29) will be zero at a unique point, $P_{opt,j}$. Since $\rho_D > \rho_{E_j} > 0$, $P_{opt,j}$ will be the point at which $(R_D^f - R_{E_j}^f)$ will be maximum. Finite alphabet secrecy rate, R_s^f, will be maximum at $P_{opt} = P_{opt,j_0}$ where $j = j_0$ corresponds to the eavesdropper index for which maximum of $(R_D^f - R_{E_j}^f)$ is minimum.

REFERENCES

[1] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Commun. and Inf. Theory*, vol. 5, no. 4–5, 2009.

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

[3] S. Vishwakarma and A. Chockalingam, "Decode-and-forward relay beamforming for secrecy with imperfect CSI and multiple eavesdroppers," in *Proc. 2012 IEEE SPAWC*.

[4] G. Zheng, J. Li, K.-K. Wong, A. P. Petropulu, and B. Ottersten, "Using simple relays to improve physical-layer security," in *Proc. 2012 IEEE ICCC: Signal Proc. for Commun.*, pp. 377–381.

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

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

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

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

[9] F. Renna, N. Laurenti, and H. V. Poor, "Achievable secrecy rates for wiretap OFDM with QAM constellations," *2011 SECURENETS*.

[10] 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, Apr. 2012.

[11] 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, Jul. 2006.