Sum Secrecy Rate in Multicarrier DF Relay Beamforming

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

***Abstract*—In this paper, we study sum secrecy rate in multicarrier decode-and-forward relay beamforming. We obtain the optimal source power and relay weights on each subcarrier which maximize the sum secrecy rate. For a given total power on a given subcarrier k, P_0^k, we reformulate the optimization problem by relaxing the rank-1 constraint on the complex positive semidefinite relay weight matrix, and solve using semidefinite programming. We analytically prove that the solution to the relaxed optimization problem is indeed rank 1. We show that the subcarrier secrecy rate, $R_s(P_0^k)$, is a concave function in total power P_0^k if $R_s(P_0^k) > 0$ for any $P_0^k > 0$. Numerical results show that the sum secrecy rate with optimal power allocation across subcarriers is more than the sum secrecy rate with equal power allocation. We also propose a low complexity suboptimal power allocation scheme which outperforms equal power allocation scheme.**

keywords: *Cooperative relaying, physical layer security, sum secrecy rate, multicarrier, multiple eavesdroppers, semi-definite programming.*

I. Introduction

Wireless networks are vulnerable to eavesdropping because of the broadcast nature of wireless channels. Secure wireless communication in the presence of eavesdroppers is a topic of current interest. Traditional methods handle security using encryption methods at the application layer. An alternate approach is physical layer security, which aims to provide security through physical layer mechanisms by which the intended receiver gets the information reliably while the eavesdroppers get no information [1]–[4]. Achievable secrecy rates and secrecy capacity bounds in single and multiple antenna point-to-point wireless wiretap channels have been studied in [5]–[10], and point-to-multipoint wiretap channel has been studied in [11]. There is growing interest in secure wireless communications via cooperative relaying. Cooperative relays can act as distributed antennas, and therefore can help to improve secrecy rate using relay beamforming [12]–[16].

Several works on secrecy using cooperative relays consider single carrier schemes. Little work has been done on secrecy in multicarrier schemes in general, and in multicarrier schemes with cooperative relaying in particular. For example, [17] considers achievable secrecy rates in a wiretap OFDM channel with no relaying. Efficient bit-loading strategies with QAM input to minimize the secrecy rate loss with respect to the Gaussian input have been proposed. In [18], a multicarrier scheme for secrecy with decode-and-forward (DF) relaying has been studied. The model in [18] used one relay and one eavesdropper on each subcarrier. The source and the relay operated under a total power constraint. Optimum source and relay powers over the subcarriers were obtained by maximizing the sum secrecy rate. A more general scenario will be to consider multiple relays with multiple eavesdroppers on each subcarrier, and to optimally allocate power between source and relays over the subcarriers so that the sum secrecy rate is maximized under a total power constraint. A direct extension of the approach in [18] to multiple relays and multiple eavesdroppers is not straightforward. In this paper, we solve the optimum power allocation problem for multiple relays and multiple eavesdroppers by taking a different approach, where for a given total power on a given subcarrier k, denoted by P_0^k, we reformulate the optimization problem by relaxing the rank-1 constraint on the complex positive semidefinite relay weight matrix, and solve using semidefinite programming. We analytically prove that the solution to the relaxed optimization problem is indeed rank 1. We show that the subcarrier secrecy rate, $R_s(P_0^k)$, is a concave function in total power P_0^k if $R_s(P_0^k) > 0$ for any $P_0^k > 0$. The sum secrecy rate with the optimal power allocation across subcarriers is shown to be more than the sum secrecy rate with equal power allocation. In addition, a low complexity suboptimal power allocation scheme which outperforms equal power allocation scheme is also proposed.

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 $\boldsymbol{A} \succ \boldsymbol{0}$ denote that $\boldsymbol{A}$ is a positive semidefinite matrix and positive definite matrix, respectively. $\boldsymbol{I}$ denotes the identity matrix. Transpose and complex conjugate transpose operations are denoted by $[.]^T$ and $[.]^*$, respectively. $|.|$ denotes absolute value.

II. System Model

Consider a multicarrier decode-and-forward cooperative relaying scheme with M subcarriers. The system model is 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_k eavesdropper nodes $\{E_1^k, E_2^k, \cdots, E_{J_k}^k\}$ on the kth subcarrier ($1 \leq k \leq M$), where J_k 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. For the kth subcarrier, the complex channel gains between source to relays are denoted by $\boldsymbol{\gamma}^k = [\gamma_1^k, \gamma_2^k, \cdots, \gamma_N^k] \in \mathbb{C}^{1 \times N}$. Likewise, the channel gains between relays to destination and relays to the jth eavesdropper on the kth subcarrier are denoted by $\boldsymbol{\alpha}^k = [\alpha_1^k, \alpha_2^k, \cdots, \alpha_N^k] \in \mathbb{C}^{1 \times N}$, and $\boldsymbol{\beta}_j^k = [\beta_{1j}^k, \beta_{2j}^k, \cdots, \beta_{Nj}^k] \in \mathbb{C}^{1 \times N}$, respectively, where $j = 1, 2, \cdots, J_k$. The channel gains on the direct links from source to destination and source to jth eavesdropper on the kth subcarrier are denoted by α_0^k

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

and β_{0j}^k, respectively. We assume that the eavesdroppers do not collude [11].

Let P_0 denote the total transmit power budget in the system (i.e., source power plus relays power) and let P_0^k denote the total available power on the kth subcarrier. The communication between source S and destination D happens in two hops. Each hop is divided into n channel uses. In the first hop of transmission on the kth subcarrier, S transmits message W^k which is equiprobable over $\{1, 2, \cdots, 2^{2nR_s(P_0^k)}\}$. W^k needs to be conveyed to the destination at perfect secrecy rate $R_s(P_0^k)$. For each W^k drawn equiprobably over the set $\{1, 2, \cdots, 2^{2nR_s(P_0^k)}\}$, S, using a stochastic encoder, maps W^k to a codeword $\{X_m^k\}_{m=1}^n$ of length n, where each symbol, X_m^k, in the codeword is i.i.d. $\sim \mathcal{CN}(0,1)$. Let P_s^k denote the source transmit power on the kth subcarrier. In the mth $(1 \leq m \leq n)$ channel use, source transmits the weighted symbol $\sqrt{P_s^k} X_m^k$. In the following, we will use X^k to denote the symbols in the codeword $\{X_m^k\}_{m=1}^n$ on the kth subcarrier. We also assume that all the channel gains are known and remain static over the codeword transmit duration.

In the second hop of transmission on the kth subcarrier, relays retransmit the decoded symbol X^k to the destination D. Let $\boldsymbol{\phi}^k = [\phi_1^k, \phi_2^k, \cdots, \phi_N^k]^T \in \mathbb{C}^{N\times 1}$ denote the complex weights applied by the relays on the transmit symbol X^k. The ith $(1 \leq i \leq N)$ relay transmits the weighted symbol $\phi_i^k X^k$.

Let $y_{R_i}^k$, $y_{D_1}^k$ and $y_{E_{1j}}^k$ denote the received signals at the ith relay, destination D and jth eavesdropper E_j^k, respectively on the kth subcarrier, in the first hop of transmission. In the second hop of transmission on the kth subcarrier, the received signals at the destination and jth eavesdropper are denoted by $y_{D_2}^k$ and $y_{E_{2j}}^k$, respectively. We have

$$y_{R_i}^k = \sqrt{P_s^k}\gamma_i^k X^k + \eta_{R_i}^k, \quad \forall i = 1, 2, \cdots, N, \qquad (1)$$

$$y_{D_1}^k = \sqrt{P_s^k}\alpha_0^k X^k + \eta_{D_1}^k, \qquad (2)$$

$$y_{E_{1j}}^k = \sqrt{P_s^k}\beta_{0j}^k X^k + \eta_{E_{1j}}^k, \qquad j = 1, 2, \cdots, J_k, \qquad (3)$$

$$y_{D_2}^k = \boldsymbol{\alpha}^k \boldsymbol{\phi}^k X^k + \eta_{D_2}^k, \qquad (4)$$

$$y_{E_{2j}}^k = \boldsymbol{\beta}_j^k \boldsymbol{\phi}^k X^k + \eta_{E_{2j}}^k, \qquad j = 1, 2, \cdots, J_k. \qquad (5)$$

The noise components, η's, are assumed to be i.i.d. $\mathcal{CN}(0, N_0)$. We rewrite (2), (4) and (3), (5) in the following vector forms:

$$\begin{aligned} \boldsymbol{y}_D^k &= [y_{D_1}^k,\ y_{D_2}^k]^T \\ &= [\sqrt{P_s^k}\alpha_0^k, \quad \boldsymbol{\alpha}^k\boldsymbol{\phi}^k]^T X^k + [\eta_{D_1}^k,\ \eta_{D_2}^k]^T, \qquad (6) \\ \boldsymbol{y}_{E_j}^k &= [y_{E_{1j}}^k,\ y_{E_{2j}}^k]^T \\ &= [\sqrt{P_s^k}\beta_{0j}^k, \quad \boldsymbol{\beta}_j^k\boldsymbol{\phi}^k]^T X^k + [\eta_{E_{1j}}^k,\ \eta_{E_{2j}}^k]^T. \qquad (7) \end{aligned}$$

III. Sum Secrecy Rate in Multicarrier DF Relay Beamforming

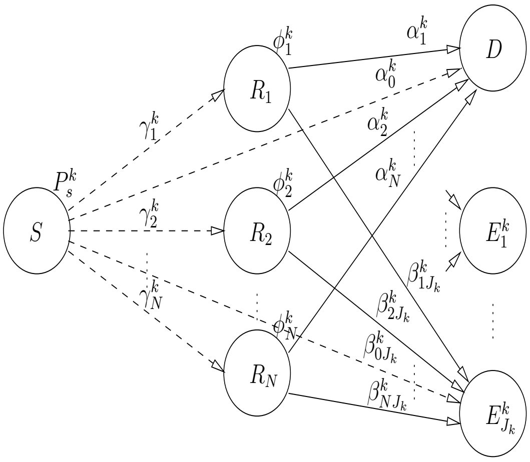

Fig. 1. System model.

Using (1), (6) and (7), the information rates at the ith relay, destination D and jth eavesdropper E_j^k, respectively, on the kth subcarrier are

$$R_{R_i}^k \triangleq \frac{1}{2} I\big(X^k; y_{R_i}^k\big) = \frac{1}{2}\log_2\Big(1 + \frac{P_s^k|\gamma_i^k|^2}{N_0}\Big), \qquad (8)$$

$$\begin{aligned} R_D^k &\triangleq \frac{1}{2} I\big(X^k; \boldsymbol{y}_D^k\big) \\ &= \frac{1}{2}\log_2\Big(1 + \frac{P_s^k|\alpha_0^k|^2 + \boldsymbol{\alpha}^k\boldsymbol{\phi}^k\boldsymbol{\phi}^{k*}\boldsymbol{\alpha}^{k*}}{N_0}\Big), \qquad (9) \end{aligned}$$

$$\begin{aligned} R_{E_j}^k &\triangleq \frac{1}{2} I\big(X^k; \boldsymbol{y}_{E_j}^k\big) \\ &= \frac{1}{2}\log_2\Big(1 + \frac{P_s^k|\beta_{0j}^k|^2 + \boldsymbol{\beta}_j^k\boldsymbol{\phi}^k\boldsymbol{\phi}^{k*}\boldsymbol{\beta}_j^{k*}}{N_0}\Big). (10) \end{aligned}$$

The factor $\frac{1}{2}$ appears in (8), (9) and (10) 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 on the kth subcarrier, the achievable secrecy rate on the kth subcarrier $R_s(P_0^k)$ for DF is obtained by solving the following optimization problem [11,13]:

$$\begin{aligned} R_s(P_0^k) &= \max_{P_s^k,\ \boldsymbol{\phi}^k}\ \min_{j:1,2,\cdots,J_k} \{R_D^k - R_{E_j}^k\}^+ \\ &= \max_{P_s^k,\boldsymbol{\phi}^k}\ \min_{j:1,2,\cdots,J_k} \frac{1}{2}\log_2\Big(\frac{N_0 + P_s^k|\alpha_0^k|^2 + \boldsymbol{\alpha}^k\boldsymbol{\phi}^k\boldsymbol{\phi}^{k*}\boldsymbol{\alpha}^{k*}}{N_0 + P_s^k|\beta_{0j}^k|^2 + \boldsymbol{\beta}_j^k\boldsymbol{\phi}^k\boldsymbol{\phi}^{k*}\boldsymbol{\beta}_j^{k*}}\Big) \\ &= \frac{1}{2}\log_2 \max_{P_s^k,\boldsymbol{\phi}^k}\ \min_{j:1,2,\cdots,J_k} \Big(\frac{N_0 + P_s^k|\alpha_0^k|^2 + \boldsymbol{\alpha}^k\boldsymbol{\phi}^k\boldsymbol{\phi}^{k*}\boldsymbol{\alpha}^{k*}}{N_0 + P_s^k|\beta_{0j}^k|^2 + \boldsymbol{\beta}_j^k\boldsymbol{\phi}^k\boldsymbol{\phi}^{k*}\boldsymbol{\beta}_j^{k*}}\Big) \qquad (11) \end{aligned}$$

$$\begin{aligned} \text{s.t.} \quad P_s^k &\geq 0, \quad P_s^k + \boldsymbol{\phi}^{k*}\boldsymbol{\phi}^k \leq P_0^k, \\ R_{R_i}^k &\geq R_D^k, \quad \forall i = 1, 2 \cdots, N, \qquad (12) \end{aligned}$$

where $\{a\}^+ = \max(a, 0)$, and w.l.o.g we drop this notation assuming that secrecy rate is a non-negative number. Defining $\boldsymbol{\Phi}^k \triangleq \boldsymbol{\phi}^k\boldsymbol{\phi}^{k*}$, the ith relay's transmit power on the kth subcarrier is given by the ith diagonal element of $\boldsymbol{\Phi}^k$. We can write the above secrecy rate expression in the following equivalent optimization form:

$$R_s(P_0^k) \;=\; \frac{1}{2}\log_2 \max_{P_s^k,\ \mathbf{\Phi}^k} \min_{j:1,2,\cdots,J_k} \frac{r^k}{s_j^k} \tag{13}$$

$$\text{s.t.} \quad \mathbf{\Phi}^k \succeq 0, \quad rank(\mathbf{\Phi}^k) = 1, \quad P_s^k \geq 0,$$
$$P_s^k + trace(\mathbf{\Phi}^k) \leq P_0^k, \quad \frac{1}{2}\log_2\Big(1 + \frac{P_s^k|\gamma_i^k|^2}{N_0}\Big) \quad \geq$$
$$\frac{1}{2}\log_2\Big(1 + \frac{P_s^k|\alpha_0^k|^2 + \boldsymbol{\alpha}^k\mathbf{\Phi}^k\boldsymbol{\alpha}^{k*}}{N_0}\Big), \quad \forall i = 1, 2\cdots, N, \tag{14}$$

where

$$r^k \;=\; (N_0 + P_s^k|\alpha_0^k|^2 + \boldsymbol{\alpha}^k\mathbf{\Phi}^k\boldsymbol{\alpha}^{k*}),$$
$$s_j^k \;=\; (N_0 + P_s^k|\beta_{0j}^k|^2 + \boldsymbol{\beta}_j^k\mathbf{\Phi}^k\boldsymbol{\beta}_j^{k*}).$$

Further, relaxing the rank constraint on $\mathbf{\Phi}^k$ and dropping the logarithms, the optimization problem (13) to compute the secrecy rate expression can be written in the following optimization form:

$$\max_{P_s^k,\ \mathbf{\Phi}^k} \min_{j:1,2,\cdots,J_k} \frac{r^k}{s_j^k} \tag{15}$$

$$\text{s.t.} \quad \mathbf{\Phi}^k \succeq 0, \quad P_s^k \geq 0, \quad P_s^k + trace(\mathbf{\Phi}^k) \leq P_0^k,$$
$$N_0 + P_s^k|\gamma_i^k|^2 \;\geq\; r^k, \quad \forall i = 1, 2, \cdots, N. \tag{16}$$

The innermost minimization $\min\limits_{j:1,\cdots,J_k} \frac{r^k}{s_j^k}$ is equivalent to $\max\limits_{t^k}\ t^k$ such that $r^k - t^k s_j^k \geq 0,\ \forall j = 1, 2, \cdots, J_k$. So, we write (15) and (16) in the following single maximization form:

$$\max_{P_s^k,\ \mathbf{\Phi}^k} \max_{t^k} t^k \;=\; \max_{P_s^k,\ \mathbf{\Phi}^k,\ t^k} t^k \tag{17}$$

$$\text{s.t.} \quad \mathbf{\Phi}^k \succeq 0, \quad P_s^k \geq 0, \quad P_s^k + trace(\mathbf{\Phi}^k) \leq P_0^k,$$
$$N_0 + P_s^k|\gamma_i^k|^2 \;\geq\; r^k, \quad \forall i = 1, 2, \cdots, N,$$
$$r^k - t^k s_j^k \;\geq 0, \quad \forall j = 1, 2\cdots, J_k. \tag{18}$$

We prove that $rank(\mathbf{\Phi}^k) = 1$ in the Appendix. We also numerically confirm that $rank(\mathbf{\Phi}^k) = 1$. This implies that optimization problems (13), (15) and (17) are equivalent. For a given t^k, the above problem is formulated as the following semi-definite feasibility problem:

$$\text{find} \quad P_s^k,\ \mathbf{\Phi}^k \tag{19}$$

subject to the constraints in (18). The maximum value of t^k, denoted by t_{max}^k, can be obtained using bisection method as follows. Let t_{max}^k lie in the interval $[t_{ll}^k,\ t_{ul}^k]$. The value of t_{ll}^k can be taken as 1 (corresponding to the minimum secrecy rate of 0) and t_{ul}^k can be taken as $\min\limits_{i:1,2,\cdots,N} (1 + \frac{P_0^k|\gamma_i^k|^2}{N_0})$, which corresponds to the minimum information rate to the relays when the total available power P_0^k is allotted to the source. Check the feasibility of (18) at $t^k = (t_{ll}^k + t_{ul}^k)/2$. If feasible, then $t_{ll}^k = t^k$, else $t_{ul}^k = t^k$. Repeat this until $t_{ul}^k - t_{ll}^k \leq \zeta$, where ζ is a small positive number. Using t_{max}^k in (13), the secrecy rate is given by

$$R_s(P_0^k) = \frac{1}{2}\log_2 t_{max}^k. \tag{20}$$

We now show the concavity of $R_s(P_0^k)$ as a function of P_0^k. First, we show that for a given total power P_0^k in the interval $(0,\ P_0]$, $R_s(P_0^k)$ attains its maximum when $P_s^k + \boldsymbol{\phi}^{k*}\boldsymbol{\phi}^k = P_0^k$, i.e., when entire total power is used. We write (11) and its constraints (12) in terms of a new vector $\boldsymbol{\psi}^k \in \mathbb{C}^{(N+1)\times 1}$ as

$$R_s(P_0^k) \;=\; \max_{\boldsymbol{\psi}^k} \min_{j:1,2,\cdots,J_k} (R_D^k - R_{E_j}^k)$$
$$=\; \max_{\boldsymbol{\psi}^k} \min_{j:1,\cdots,J_k} \frac{1}{2}\Big\{\log_2\Big(1 + \frac{\boldsymbol{\psi}^{k*}\mathbf{A}^k\boldsymbol{\psi}^k}{N_0}\Big)$$
$$-\log_2\Big(1 + \frac{\boldsymbol{\psi}^{k*}\mathbf{B}_j^k\boldsymbol{\psi}^k}{N_0}\Big)\Big\} \tag{21}$$

$$\text{s.t.} \quad \boldsymbol{\psi}^{k*}\boldsymbol{\psi}^k \;\leq\; P_0^k,$$
$$R_{R_i}^k - R_D^k \;=\; \frac{1}{2}\log_2\Big(1 + \frac{\boldsymbol{\psi}^{k*}\mathbf{C}_i^k\boldsymbol{\psi}^k}{N_0}\Big) -$$
$$\frac{1}{2}\log_2\Big(1 + \frac{\boldsymbol{\psi}^{k*}\mathbf{A}^k\boldsymbol{\psi}^k}{N_0}\Big) \;\geq\; 0, \ \forall i = 1, 2\cdots, N, \tag{22}$$

where $\boldsymbol{\psi}^k = [\sqrt{P_s^k},\ \boldsymbol{\phi}^{kT}]^T$, and $\mathbf{A}^k$, $\mathbf{B}_j^k$ and $\mathbf{C}_i^k$ are $(N+1)\times(N+1)$ matrices given by

$$\mathbf{A}^k \;=\; [\alpha_0^{k*}\alpha_0^k,\ \mathbf{0};\ \mathbf{0},\ \boldsymbol{\alpha}^{k*}\boldsymbol{\alpha}^k] \;\succeq\; \mathbf{0},$$
$$\mathbf{B}_j^k \;=\; [\beta_{0j}^{k*}\beta_{0j}^k,\ \mathbf{0};\ \mathbf{0},\ \boldsymbol{\beta}_j^{k*}\boldsymbol{\beta}_j^k] \;\succeq\; \mathbf{0},$$
$$\mathbf{C}_i^k \;=\; [\gamma_i^{k*}\gamma_i^k,\ \mathbf{0};\ \mathbf{0},\ \mathbf{0}] \;\succeq\; \mathbf{0}.$$

Let the solution of the above optimization problem be feasible with $R_s(P_0^k) > 0$, and $\boldsymbol{\psi}^k = \sqrt{P^k}\boldsymbol{\psi}_u^k$, where $\boldsymbol{\psi}_u^k$ is a unit-norm vector in the direction of $\boldsymbol{\psi}^k$. From the power constraint, $\boldsymbol{\psi}^{k*}\boldsymbol{\psi}^k = P^k\boldsymbol{\psi}_u^{k*}\boldsymbol{\psi}_u^k = P^k \leq P_0^k$. Since $\frac{d(R_D^k - R_{E_j}^k)}{dP^k} > 0$ at $\boldsymbol{\psi}^k = \sqrt{P^k}\boldsymbol{\psi}_u^k$, $\forall j = 1, 2, \cdots, J_k$, and $\frac{d(R_{R_i}^k - R_D^k)}{dP^k} \geq 0$ at $\boldsymbol{\psi}^k = \sqrt{P^k}\boldsymbol{\psi}_u^k$, $\forall i = 1, 2, \cdots, N$, this implies that the secrecy rate maximum occurs at $P^k = P_0^k$. Hence, $R_s(P_0^k)$ is a monotonically increasing function in P_0^k over the interval $[0,\ P_0]$. Also, $\frac{d^2(R_D^k - R_{E_j}^k)}{d{P_0^k}^2} < 0$ at $\boldsymbol{\psi}^k = \sqrt{P_0^k}\boldsymbol{\psi}_u^k$, $\forall j = 1, 2, \cdots, J_k$. This further implies that $R_s(P_0^k)$ is concave in P_0^k over the interval $[0,\ P_0]$.

Let L $(\leqslant M)$ be the number of subcarriers having respective $R_s(P_0^k) > 0$ for any $P_0^k > 0$. This can be verified by solving (17) for each subcarrier with some fixed $P_0^k > 0$ e.g. $P_0^k = P_0 > 0$. We also obtain the unit norm vector $\boldsymbol{\psi}_u^k = \frac{1}{\sqrt{P_0^k}}[\sqrt{P_s^k},\ \boldsymbol{\phi}^{kT}]^T$ for each subcarrier by solving (17) with some fixed $P_0^k > 0$ e.g. $P_0^k = P_0 > 0$. With this, all L subcarriers $R_s(P_0^k)$ will be concave functions in their respective P_0^k which follows from the previous discussion. We discard remaining $M - L$ subcarriers because they will not lead to any positive secrecy rate. We obtain the maximum sum secrecy rate by solving the following optimization problem:

$$\text{Sum Secrecy Rate} = \max_{P_0^1,\ P_0^2,\cdots,P_0^L} \sum_{k=1}^{L} R_s(P_0^k) \tag{23}$$

$$= \max_{P_0^1,\ P_0^2,\cdots,P_0^L} \sum_{k=1}^{L} \frac{1}{2}\Big\{ \log_2\Big(1+\frac{P_0^k \boldsymbol{\psi}_u^{k*}\mathbf{A}^k\boldsymbol{\psi}_u^k}{N_0}\Big) - \log_2\Big(1+\frac{P_0^k \boldsymbol{\psi}_u^{k*}\mathbf{B}_{j_0}^k\boldsymbol{\psi}_u^k}{N_0}\Big)\Big\} \tag{24}$$

$$\text{s.t.} \quad \forall k = 1,2,\cdots,L, \quad 0 \ \leq\ P_0^k \ \leq\ P_0, \qquad \sum_{k=1}^{L} P_0^k \ \leq\ P_0, \tag{25}$$

where $j_0 = \arg\max_{j:1,2,\cdots,J_k} \ \boldsymbol{\psi}_u^{k*}\mathbf{B}_j^k\boldsymbol{\psi}_u^k$, i.e., the eavesdropper index having maximum information rate on the kth subcarrier. The objective function in (23) and its equivalent (24) is a sum of L concave functions, and all the constraints in (25) are linear. This implies that the optimization problem (24) is a convex optimization problem, or, to be more specific, a concave maximization problem. For a convex optimization problem, the first order necessary conditions (KKT) are also sufficient. This implies that a local maximum of the above optimization problem will also be a global maximum. We note that the existing convex optimization tools can not be used to solve (24). However, the optimal solution of (24) can be obtained using interior-point method. As discussed above, optimality of the solution is guaranteed due to the fact that (24) is a concave maximization problem.

A. Low complexity suboptimum power allocation

We will compare the sum secrecy rate achieved by the above optimum power allocation (OPA) scheme with that of equal power allocation (EPA) scheme, where the total power P_0 is distributed equally among all the M subcarriers in the system. We refer to the later scheme as 'EPA scheme 1'. Another scheme is to distribute the total power P_0 equally among the L subcarriers which have non-zero secrecy rate for any $P_0^k > 0$. We refer to this scheme as 'EPA scheme 2'. EPA schemes 1 and 2 are low complexity suboptimum schemes. Since EPA scheme 2 does not waste its power on zero secrecy rate subchannels, it is expected to achieve higher sum secrecy rate than EPA scheme 1.

IV. Results and Discussions

We evaluated the sum secrecy rates of the OPA scheme, EPA scheme 1 and EPA scheme 2 for a system with $N = 2$ relays, $M = 4$ subcarriers, and $J = 3$ eavesdroppers on each subcarrier. We consider the following channel gains for all subcarriers:

$\big[\boldsymbol{\gamma}^{1T},\ \boldsymbol{\gamma}^{2T},\ \boldsymbol{\gamma}^{3T},\ \boldsymbol{\gamma}^{4T}\big] = \big[-0.9483 - 0.4119i,\ -1.1554 + 0.1758i,\ 0.2077 + 0.2217i,\ -0.7993 + 0.3741i;\ 0.3391 - 0.6338i,\ -1.0201 - 1.0534i,\ -0.0993 - 1.4320i,\ -0.2069 + 0.2429i\big]$,

$[\alpha_0^1,\ \alpha_0^2,\ \alpha_0^3,\ \alpha_0^4] = [0.2681 + 0.0181i,\ -0.2446 - 0.7506i,\ 0.2405 + 0.1007i,\ -0.3792 - 0.2593i]$,

$[\beta_{01}^1,\ \beta_{01}^2,\ \beta_{01}^3,\ \beta_{01}^4] = [-0.0547 - 0.0076i,\ 0.0107 + 0.0717i,\ -0.0238 - 0.0336i,\ 0.0686 + 0.0049i]$,

$[\beta_{02}^1,\ \beta_{02}^2,\ \beta_{02}^3,\ \beta_{02}^4] = [0.0282 - 0.0970i,\ 0.0789 - 0.0485i,\ 0.0439 + 0.0235i,\ -0.0203 - 0.0705i]$,

$[\beta_{03}^1,\ \beta_{03}^2,\ \beta_{03}^3,\ \beta_{03}^4] = [0.0206 + 0.0287i,\ 0.0783 + 0.0860i,\ 0.0173 + 0.1024i,\ 0.0117 - 0.0725i]$,

$[\boldsymbol{\alpha}^{1T},\ \boldsymbol{\alpha}^{2T},\ \boldsymbol{\alpha}^{3T},\ \boldsymbol{\alpha}^{4T}] = [0.0453 + 0.0374i,\ -0.1867 + 1.0868i,\ 0.6052 + 0.7846i,\ 0.5741 + 0.2726i;\ 0.0164 - 0.0112i,\ 1.7645 - 1.1383i,\ -0.6017 - 0.7847i,\ 0.4951 + 0.6825i]$,

$[\boldsymbol{\beta}_1^{1T},\ \boldsymbol{\beta}_1^{2T},\ \boldsymbol{\beta}_1^{3T},\ \boldsymbol{\beta}_1^{4T}] = [0.0579 + 0.0392i,\ -0.0655 + 0.0044i,\ -0.0568 + 0.0141i,\ -0.0637 + 0.1471i;\ 0.0026 - 0.0294i,\ -0.0079 + 0.0323i,\ -0.1177 + 0.0182i,\ 0.0416 - 0.1610i]$,

$[\boldsymbol{\beta}_2^{1T},\ \boldsymbol{\beta}_2^{2T},\ \boldsymbol{\beta}_2^{3T},\ \boldsymbol{\beta}_2^{4T}] = [0.0240 + 0.0935i,\ 0.0468 + 0.0931i,\ 0.0628 - 0.1011i,\ 0.0600 - 0.0357i;\ 0.0205 - 0.0045i,\ -0.0411 + 0.0161i,\ 0.0122 - 0.0106i,\ 0.0681 - 0.1223i]$,

$[\boldsymbol{\beta}_3^{1T},\ \boldsymbol{\beta}_3^{2T},\ \boldsymbol{\beta}_3^{3T},\ \boldsymbol{\beta}_3^{4T}] = [-0.0295 + 0.0204i,\ 0.0510 + 0.0570i,\ 0.0624 + 0.0085i,\ -0.0103 + 0.0404i;\ -0.0435 + 0.0824i,\ 0.0240 - 0.0959i,\ 0.0201 - 0.0157i,\ -0.0063 - 0.0212i]$.

The secrecy rates achieved on subcarriers 1, 2, 3, and 4 as a function of total power under various power allocation schemes are plotted in Fig. 2, Fig. 3, Fig. 4, and Fig. 5, respectively. The sum secrecy rates achieved in the system as a function of total power under various power allocation schemes are plotted in Fig. 6. As expected, OPA scheme achieves the highest sum secrecy rate among all the three schemes. EPA scheme 1, though less complex, achieves much less sum secrecy rate. EPA scheme 2, while being less complex than OPA scheme, achieves better sum secrecy rate than EPA scheme 1 and closer to sum secrecy rate of OPA scheme. As pointed out, EPA scheme 2 achieves higher sum secrecy rate than EPA scheme 1 because it does not use its power on zero secrecy rate subcarriers. At high transmit powers, the performance difference between the three schemes tend to diminish.

V. Conclusions

We considered the sum secrecy rate in multicarrier decode-and-forward relay beamforming. We transformed the sum secrecy rate maximization problem to an equivalent concave maximization problem which can be easily solved using

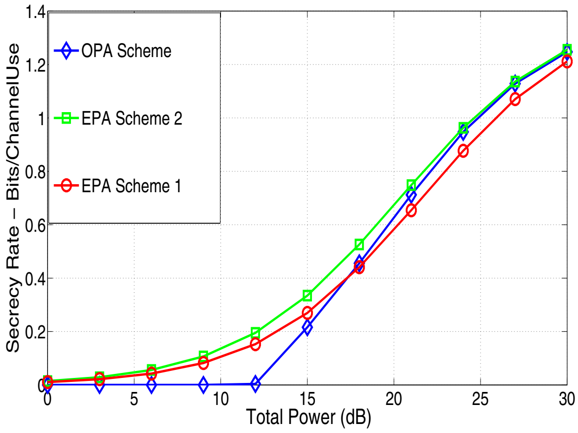

Fig. 2. Subcarrier 1 secrecy rate in DF multicarrier relay beamforming with $N = 2,\ M = 4,\ J = 3$.

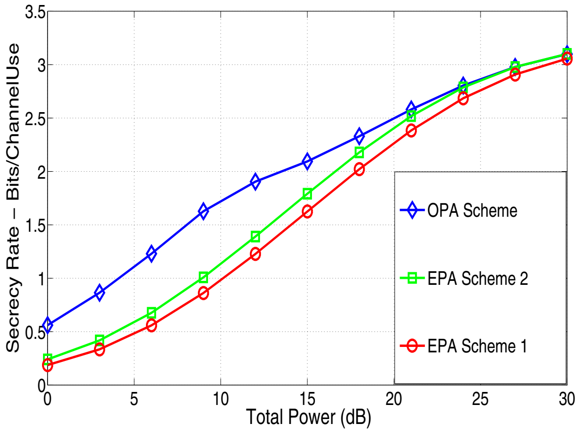

Fig. 3. Subcarrier 2 secrecy rate in DF multicarrier relay beamforming with $N = 2,\ M = 4,\ J = 3$.

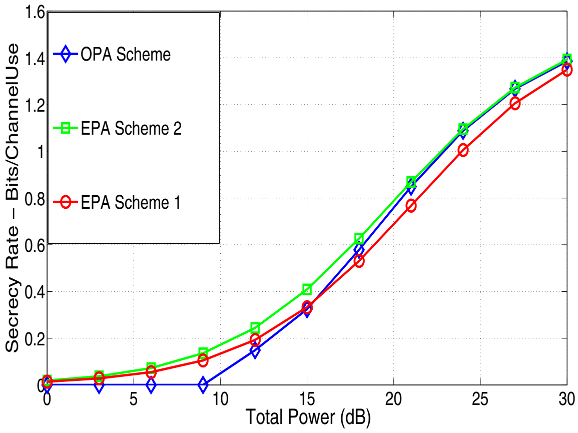

Fig. 4. Subcarrier 3 secrecy rate in DF multicarrier relay beamforming with $N = 2,\ M = 4,\ J = 3$.

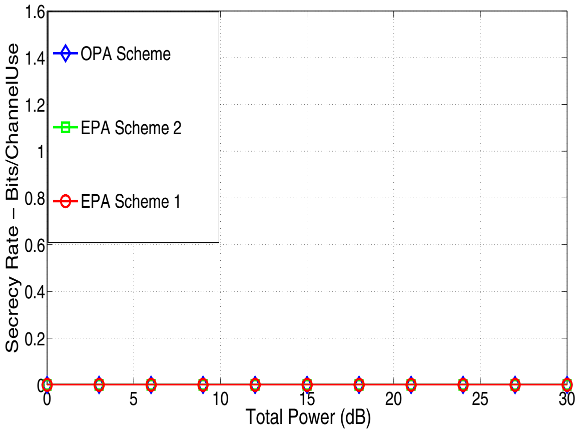

Fig. 5. Subcarrier 4 secrecy rate in DF multicarrier relay beamforming with $N = 2,\ M = 4,\ J = 3$.

interior-point method. We obtained the optimal source power and relay weights on each subcarrier which maximized the sum secrecy rate. Numerical results showed that the sum secrecy rate with optimal power allocation across subcarriers was more than the sum secrecy rate with equal power allocation. We also proposed a low complexity suboptimal power allocation scheme which outperformed equal power allocation scheme.

Appendix

In this appendix, we prove that the solution of the optimization problem (17) has rank 1, i.e., $rank(\mathbf{\Phi}^k) = 1$. We take the Lagrangian of the objective function $-t^k$ with constraints in (18) as follows [19]:

$$\ell(t^k,\ P_s^k,\ \mathbf{\Phi}^k,\ \lambda_s^k,\ \mathbf{\Lambda}^k,\ \lambda_0^k,\ \mu_j^k,\ \nu_i^k) = -t^k - \lambda_s^k P_s^k - trace(\mathbf{\Lambda}^k\mathbf{\Phi}^k) + \lambda_0^k(P_s^k + trace(\mathbf{\Phi}^k) - P_0^k) + \sum_{j=1}^{J_k}\mu_j^k(t^k s_j^k - r^k) + \sum_{i=1}^{N}\nu_i^k(r^k - N_0 - P_s^k|\gamma_i^k|^2), \quad (26)$$

where $\lambda_s^k \geq 0,\ \mathbf{\Lambda}^k \succeq \mathbf{0},\ \lambda_0^k \geq 0,\ \mu_j^k \geq 0,\ \nu_i^k \geq 0$ are Lagrangian multipliers. The KKT conditions for (26) are as follows:

(a) all constraints in (18),

(b) $\lambda_s^k P_s^k = 0$. For positive secrecy rate, $P_s^k > 0 \implies \lambda_s^k = 0$,

(c) $trace(\mathbf{\Lambda}^k\mathbf{\Phi}^k) = 0$. Since $\mathbf{\Lambda}^k \succeq \mathbf{0}$ and $\mathbf{\Phi}^k \succeq \mathbf{0} \implies \mathbf{\Lambda}^k\mathbf{\Phi}^k = \mathbf{0}$,

(d) $\lambda_0^k(P_s^k + trace(\mathbf{\Phi}^k) - P_0^k) = 0$,

(e) $\forall j = 1, 2, \cdots, J_k, \quad \mu_j^k(t^k s_j^k - r^k) = 0$,

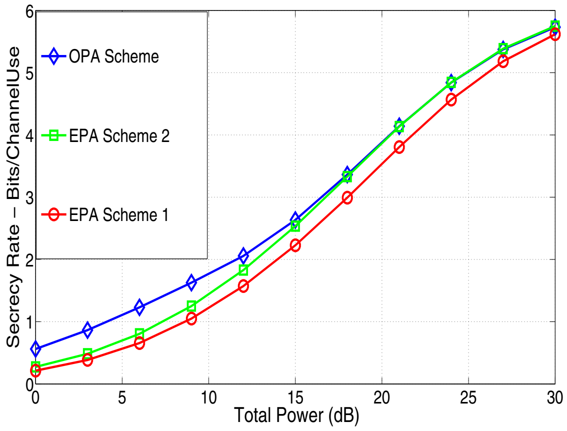

Fig. 6. Sum secrecy rate in DF multicarrier relay beamforming with $N = 2,\ M = 4,\ J = 3$.

(f) $\forall i = 1, 2, \cdots, N, \quad \nu_i^k(r^k - N_0 - P_s^k|\gamma_i^k|^2) = 0,$

(g) $\frac{\partial \ell}{\partial t^k} = 0 \implies \sum_{j=1}^{J_k} \mu_j^k s_j^k = 1 \implies$ not all μ_j^k's can be zero simultaneously,

(h) $\frac{\partial \ell}{\partial P_s^k} = 0 \implies \lambda_0^k + \sum_{j=1}^{J_k} \mu_j^k (t^k|\beta_{0j}^k|^2 - |\alpha_0^k|^2) + \sum_{i=1}^{N} \nu_i^k(|\alpha_0^k|^2 - |\gamma_i^k|^2) = 0,$

(i) $\frac{\partial \ell}{\partial \boldsymbol{\Phi}^k} = \mathbf{0} \implies \boldsymbol{\Lambda}^k = \lambda_0^k \boldsymbol{I} + \sum_{j=1}^{J_k} \mu_j^k (t^k \boldsymbol{\beta}_j^{k*} \boldsymbol{\beta}_j^k - \boldsymbol{\alpha}^{k*}\boldsymbol{\alpha}^k) + \sum_{i=1}^{N} \nu_i^k (\boldsymbol{\alpha}^{k*}\boldsymbol{\alpha}^k) \succeq \mathbf{0}.$

The KKT conditions (i) and (h) in the above imply that

$$\lambda_0^k P_s^k \ + \ \sum_{j=1}^{J_k} \mu_j^k (t^k |\beta_{0j}^k|^2 - |\alpha_0^k|^2) P_s^k \ + \ \sum_{i=1}^{N} \nu_i^k (|\alpha_0^k|^2 - |\gamma_i^k|^2) P_s^k \ + \ \lambda_0^k trace(\boldsymbol{\Phi}^k) \ + \ \sum_{j=1}^{J_k} \mu_j^k (t^k \boldsymbol{\beta}_j^k \boldsymbol{\Phi}^k \boldsymbol{\beta}_j^{k*} - \boldsymbol{\alpha}^k \boldsymbol{\Phi}^k \boldsymbol{\alpha}^{k*}) \ + \ \sum_{i=1}^{N} \nu_i^k (\boldsymbol{\alpha}^k \boldsymbol{\Phi}^k \boldsymbol{\alpha}^{k*}) \ = \ 0,$$

which, in turn, implies that

$$\lambda_0^k P_s^k \ + \ \lambda_0^k trace(\boldsymbol{\Phi}^k) \ = \ \sum_{j=1}^{J_k} \mu_j^k N_0 (t^k - 1).$$

With $t^k > 1$ for positive secrecy rate, the above expression implies that $\lambda_0^k > 0$. With $\lambda_0^k > 0$, KKT condition (d) implies that $P_s^k + trace(\boldsymbol{\Phi}^k) \ = \ P_0^k$, i.e., entire power is used for the transmission. This further implies that the subcarrier secrecy rate, $R_s(P_0^k)$, is a strictly increasing function in P_0^k. Further, rewriting the KKT condition (i) in the following form

$$\boldsymbol{\Lambda}^k \ + \ \sum_{j=1}^{J_k} \mu_j^k (\boldsymbol{\alpha}^{k*}\boldsymbol{\alpha}^k) \ = \ \lambda_0^k \boldsymbol{I} \ + \ \sum_{j=1}^{J_k} \mu_j^k (t^k \boldsymbol{\beta}_j^{k*} \boldsymbol{\beta}_j^k) \ + \ \sum_{i=1}^{N} \nu_i^k (\boldsymbol{\alpha}^{k*}\boldsymbol{\alpha}^k),$$

which is $\succ \mathbf{0}$ since $\lambda_0^k > 0$ for positive secrecy rate. This implies that $\boldsymbol{\Lambda}^k + \sum_{j=1}^{J_k} \mu_j^k (\boldsymbol{\alpha}^{k*}\boldsymbol{\alpha}^k)$ is a full rank positive definite matrix. This further implies that $rank(\boldsymbol{\Lambda}^k) \geq N - 1$ because $\sum_{j=1}^{J_k} \mu_j^k (\boldsymbol{\alpha}^{k*}\boldsymbol{\alpha}^k)$ is a rank 1 matrix. The KKT condition (c) also implies that $rank(\boldsymbol{\Lambda}^k) \neq N$ (assuming $\boldsymbol{\Phi}^k \neq \mathbf{0}$). This means that $rank(\boldsymbol{\Lambda}^k) = N - 1$. This and KKT condition (c) (assuming $\boldsymbol{\Phi}^k \neq \mathbf{0}$) imply $rank(\boldsymbol{\Phi}^k) = 1$.

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*, Jun. 2007.

[6] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraint," *Proc. IEEE ISIT'2007*, Jun. 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] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *Proc. IEEE ISIT'2008*, Jul. 2008.

[9] 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.

[10] 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.

[11] 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.

[12] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory.*, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.

[13] 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.

[14] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," *Proc. IEEE ICC'2010*, May 2010.

[15] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical-layer security," *Proc. CISS'2010*, Mar. 2010.

[16] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985-4997, Oct. 2011.

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

[18] C. Jeong and I. M. Kim, "Optimal power allocation for secure multi-carrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428-5442, Nov. 2011.

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

[20] J. Sturm, "Using SeDuMi 1.03: A MATLAB toolbox for optimization over symmetric ones," *Opt. Methods and Software*, vol. 11-12, pp. 625-653, 1999. Special issue on Interior Point Methods (CD supplement with software).

[21] J. Lofberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," *Proc. CACSD Conf.*, Taipei, 2004. [Online] Available: http://control.ee.ethz.ch/ joloef/yalmip.php.