EURASIP Journal on Advances in Signal Processing
a SpringerOpen Journal

RESEARCH Open Access

Distributed beamforming designs to improve physical layer security in wireless relay networks

Mujun Qian[1], Chen Liu[1*] and Youhua Fu[1,2]

Abstract

This paper investigates security-oriented beamforming designs in a relay network composed of a source-destination pair, multiple relays, and a passive eavesdropper. Unlike most of the earlier works, we assume that only statistical information of the relay-eavesdropper channels is known to the relays. We propose beamforming solutions for amplify-and-forward (AF) and decode-and-forward (DF) relay networks to improve secrecy capacity. In an AF network, the beamforming design is obtained by approximating a product of two correlated Rayleigh quotients to a single Rayleigh quotient using the Taylor series expansion. Our study reveals that in an AF network, the secrecy capacity does not always grow as the eavesdropper moves away from the relays or as total relay transmit power increases. Moreover, if the destination is nearer to the relays than the eavesdropper is, a suboptimal power is derived in closed form through monotonicity analysis of secrecy capacity. While in a DF network, secrecy capacity is a single Rayleigh quotient problem which can be easily solved. We also found that if the relay-eavesdropper distances are about the same, it is unnecessary to consider the eavesdropper in a DF network. Numerical results show that for either AF or DF relaying protocol, the proposed beamforming scheme provides higher secrecy capacity than traditional approaches.

Keywords: Physical layer security; Wireless relay networks; Cooperative beamforming; Amplify-and-forward; Decode-and-forward; Secrecy capacity

1. Introduction

Cooperative communications, in which multiple nodes help each other transmit messages, has been widely acknowledged as an effective way to improve system performance [1-3]. However, due to the broadcast property of radio transmission, wireless communication is vulnerable to eavesdropping which consequently makes security schemes of great importance as a promising approach to communicate confidential messages.

The traditional secure communication schemes rely on encryption techniques where secret keys are used. However, as the high-layer secure protocols have attracted growing attacks in recent years, the implementation of security schemes at physical layer becomes a hotspot. It was first proved by Wyner that it is possible to communicate perfectly at a non-zero rate without a secret key if the eavesdropper has a worse channel than the destination [4]. This work was extended to Gaussian channels in [5] and to fading channels in [6]. Recently, there has been considerable work on secure communication in wireless relay networks (WRNs) [7-15]. A widely acknowledged measurement of system security in WRNs is the maximal rate of secret information exchange between source and destination which is defined as secrecy capacity. A decode-and-forward (DF)-based cooperative beamforming scheme which completely nulls out source signal at eavesdropper(s) was proposed in [7], and this work was extended to the amplify-and-forward (AF) protocol and cooperative jamming in [8]. Hybrid beamforming and jamming was investigated in [9] where one relay was selected to cooperate and the other to make intentional interference in a DF network. Combined relay selection and cooperative beamforming schemes for DF networks were proposed in [10] where two best relays were selected to cooperate. The authors of [11,12] considered the scenario where the relay(s) could not be trusted in cooperative MIMO networks. Additionally, a new metric of system security is brought up in [13] as intercept probability and optimal relay selection schemes for AF and DF

* Correspondence: liuch@njupt.edu.cn
[1]The Key Lab of Broadband Wireless Communication and Sensor Network Technology (Ministry of Education), Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210003, China
Full list of author information is available at the end of the article

protocols based on the minimization of intercept probability were proposed.

In earlier works, it is widely assumed that the relays have access to instantaneous channel state information (CSI) of relay-eavesdropper (RE) channels [7,8,13-15]. This assumption is ideal but unpractical in a real-life wiretap attack since the malicious eavesdropper would not be willing to share its instantaneous CSI. Thus, security schemes using instantaneous CSI of the eavesdropper cannot be adopted anymore. However, the instantaneous CSI of relay-destination (RD) channels is available since the destination is positive. The statistical information of the RE channels is also available through long-term supervision of the eavesdropper's transmission [9]. It is worth mentioning that even if the relays do not have access to the perfect CSI of RD channels, they can still estimate these channels by training sequences and perform beamforming based on the estimated CSI [16].

Our focus is on secrecy capacity, and we are interested in maximizing it with appropriate weight designs of relays. The remainder of this paper is organized as follows. Section 2 introduces system model under AF and DF protocols using relay beamforming. The optimization problem in an AF network is addressed and solved in Section 3 along with some analyses of secrecy capacity. Section 4 provides the optimal beamforming design for a DF network along with a surprising finding that considering the eavesdropper sometimes may not be necessary. Numerical results are given in Section 5 to compare the performances of different designs, and Section 6 provides some concluding remarks.

2. System model

Consider a cooperative wireless network consisting of a source node S, a legitimate destination D, an eavesdropper E, and M relays R_i, $i = 1,\ldots, M$ as shown in Figure 1. Each node is equipped with single antenna working in half-duplex mode. Assume that there is no direct link between the source and the destination/eavesdropper, i.e., neither the destination nor the eavesdropper is in the coverage area of the source. For notational convenience, we denote the source-relay (SR) channels as f_i, the RD channels as g_i, and the RE channels as h_i. All the channels are modeled as independent and identically distributed (i.i.d.) Rayleigh fading channels, i.e., $f_i \sim \mathcal{CN}\left(0, \sigma_{f_i}^2\right)$, $g_i \sim \mathcal{CN}\left(0, \sigma_{g_i}^2\right)$, and $h_i \sim \mathcal{CN}\left(0, \sigma_{h_i}^2\right)$. Considering the path loss effect and setting the path loss exponent to 4 (for an urban environment), we have $\sigma_{f_i}^2 = d_{\mathrm{SR}_i}^{-4}$, $\sigma_{g_i}^2 = d_{\mathrm{R}_i\mathrm{D}}^{-4}$, and $\sigma_{h_i}^2 = d_{\mathrm{R}_i\mathrm{E}}^{-4}$, where d_{AB} is the distance between nodes A and B. We assume the relays to know instantaneous CSI of SR channels and RD channels, but only statistical information of RE channels. Without loss of generality, we also assume the additive noises to be i.i.d. and follow a $\mathcal{CN}(0, 1)$ distribution.

2.1 Amplify-and-forward

In an AF protocol, the source broadcasts $\sqrt{P_\mathrm{s}}s$ in the first hop where the information symbol s is selected from a codebook and is normalized as $\mathrm{E}|s|^2 = 1$, and P_s is the transmit power. The received signal at R_i is

$$r_i = f_i\sqrt{P_\mathrm{s}}s + v_i \tag{1}$$

where v_i is the additive noise at R_i.

In the second hop, each relay forwards a weighted version of the noisy signal it just received. More specifically, R_i normalizes r_i with a scaling factor $\rho_i = 1/\sqrt{1 + |f_i|^2 P_\mathrm{s}}$ and then transmits a weighted signal $t_i = w_i\rho_i r_i$. The transmit power of R_i is $P_i = |w_i|^2$. The received signal at the destination is

$$\begin{aligned} y_\mathrm{D} &= \sum_{i=}^{M} g_i t_i + v_\mathrm{D} \\ &= \sqrt{P_\mathrm{s}}\mathbf{w}^\mathrm{T}\boldsymbol{\rho}_{fg}s + \mathbf{w}^\mathrm{T}\mathrm{diag}\left\{\boldsymbol{\rho}_g\right\}\mathbf{v} + v_\mathrm{D} \end{aligned} \tag{2}$$

where $\mathbf{w} = (w_1, \ldots, w_M)^\mathrm{T}$, $\boldsymbol{\rho}_{fg} = (\rho_1 f_1 g_1, \ldots, \rho_M f_M g_M)^\mathrm{T}$, $\boldsymbol{\rho}_g = (\rho_1 g_1, \ldots, \rho_M g_M)^\mathrm{T}$, $\mathbf{v} = (v_1, \ldots, v_M)^\mathrm{T}$, and v_D represents additive white Gaussian noise (AWGN) at the destination. The total relay transmit power is $\mathbf{w}^\mathrm{H}\mathbf{w} = P$.

Meanwhile, the eavesdropper also gets a copy of s:

$$\begin{aligned} y_\mathrm{E} &= \sum_{i=1}^{M} h_i t_i + v_\mathrm{E} \\ &= \sqrt{P_\mathrm{s}}\mathbf{w}^\mathrm{T}\boldsymbol{\rho}_{fh}s + \mathbf{w}^\mathrm{T}\mathrm{diag}\{\boldsymbol{\rho}_h\}\mathbf{v} + v_\mathrm{E} \end{aligned} \tag{3}$$

where $\boldsymbol{\rho}_{fh} = (\rho_1 f_1 h_1, \ldots, \rho_M f_M h_M)^\mathrm{T}$, $\boldsymbol{\rho}_h = (\rho_1 h_1, \ldots, \rho_M h_M)^\mathrm{T}$, and v_E represents AWGN at the eavesdropper.

2.2 Decode-and-forward

In a DF protocol, the first hop is the same as in an AF protocol. While in the second hop, instead of simply amplifying the received signal, R_i decodes the message s and multiplies it with a weighted factor w_i to generate the transmit signal $t_i = w_i s$. The transmit power of R_i is still $P_i = |w_i|^2$. The received signals at the destination and the eavesdropper can be expressed, respectively, as

$$y_\mathrm{D} = \sum_{i=1}^{M} g_i t_i + v_\mathrm{D} = \mathbf{w}^\mathrm{T}\mathbf{g}s + v_\mathrm{D} \tag{4}$$

and

$$y_\mathrm{E} = \sum_{i=1}^{M} h_i t_i + v_\mathrm{E} = \mathbf{w}^\mathrm{T}\mathbf{h}s + v_\mathrm{E} \tag{5}$$

where $\mathbf{g} = (g_1, \ldots, g_M)^\mathrm{T}$ and $\mathbf{h} = (h_1, \ldots, h_M)^\mathrm{T}$.

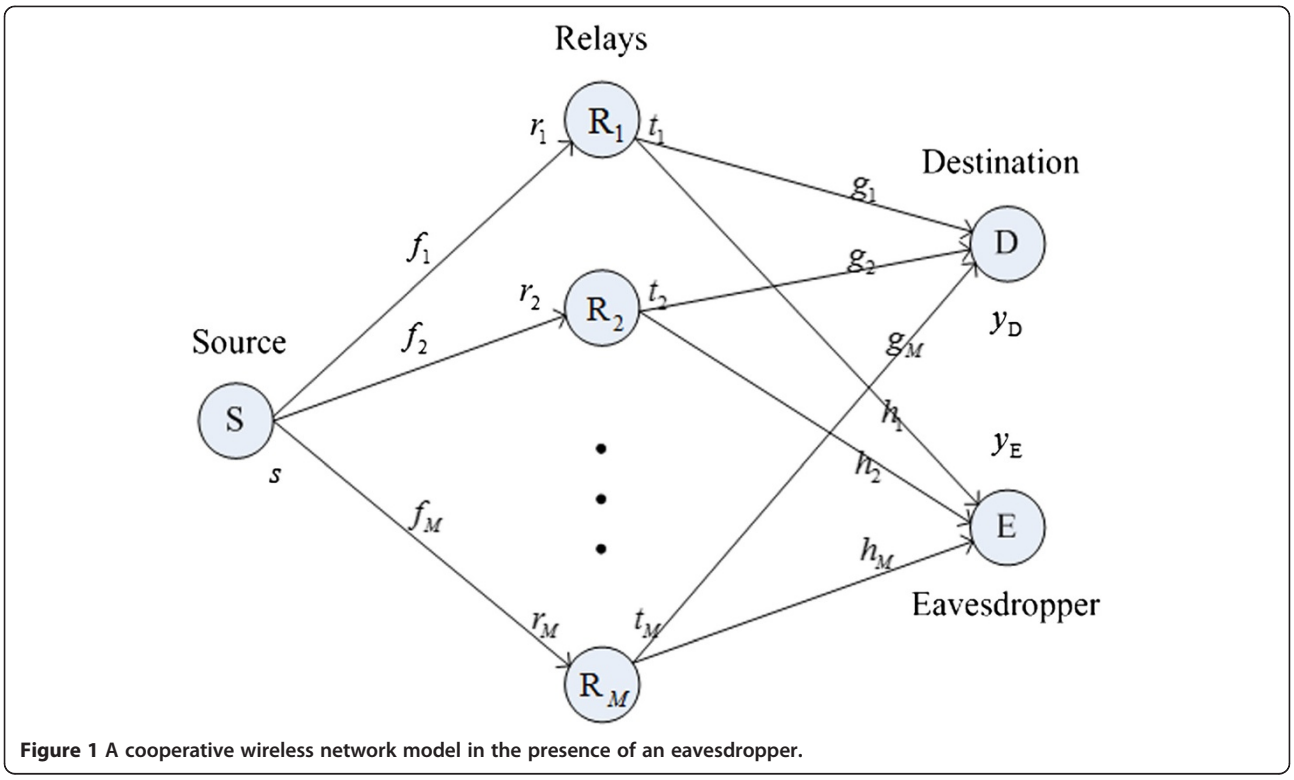

Figure 1 A cooperative wireless network model in the presence of an eavesdropper.

3. Distributed beamforming design for AF

In the following sections, we consider the security issue of the above relay network. The metric of interest is secrecy capacity which is defined as

$$C_{\mathrm{S}} = \max\{C_{\mathrm{D}} - C_{\mathrm{E}}, 0\} \tag{6}$$

where $C_{\mathrm{D}} = \frac{1}{2}\log_2(1+\gamma_{\mathrm{D}})$, $C_{\mathrm{E}} = \frac{1}{2}\log_2(1+\gamma_{\mathrm{E}})$, and γ_{D} and γ_{E} are received signal-to-noise ratios (SNRs) at the destination and the eavesdropper, respectively. We aim to improve C_{S} by exploiting appropriate beamforming designs. The following subsection describes the proposed beamforming design for an AF network.

3.1 Proposed design for AF (P-AF)

In distributed beamforming schemes, the relays compute the received SNRs at the destination and the eavesdropper from Equations 2 and 3, respectively, as

$$\gamma_{\mathrm{D}} = \frac{E_s\left(\sqrt{P_{\mathrm{s}}}\mathbf{w}^{\mathrm{T}}\boldsymbol{\rho}_{fg}s\right)^*\left(\sqrt{P_{\mathrm{s}}}\mathbf{w}^{\mathrm{T}}\boldsymbol{\rho}_{fg}s\right)}{\underset{\mathbf{v},\nu_{\mathrm{D}}}{E}\left(\mathbf{w}^{\mathrm{T}}\mathrm{diag}\left\{\boldsymbol{\rho}_g\right\}\mathbf{v}+\nu_{\mathrm{D}}\right)^*\left(\mathbf{w}^{\mathrm{T}}\mathrm{diag}\left\{\boldsymbol{\rho}_g\right\}\mathbf{v}+\nu_{\mathrm{D}}\right)} = \frac{P_{\mathrm{s}}\mathbf{w}^{\mathrm{H}}\boldsymbol{\rho}_{fg}\boldsymbol{\rho}_{fg}^{\mathrm{H}}\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}\boldsymbol{\Gamma}_g\mathbf{w}} \tag{7}$$

and

$$\gamma_{\mathrm{E}} = \frac{\underset{s,\mathbf{h}}{E}\left(\sqrt{P_{\mathrm{s}}}\mathbf{w}^{\mathrm{T}}\boldsymbol{\rho}_{fh}s\right)^*\left(\sqrt{P_{\mathrm{s}}}\mathbf{w}^{\mathrm{T}}\boldsymbol{\rho}_{fh}s\right)}{\underset{\mathbf{v},\nu_{\mathrm{E}}}{E}\left(\mathbf{w}^{\mathrm{T}}\mathrm{diag}\{\boldsymbol{\rho}_h\}\mathbf{v}+\nu_{\mathrm{E}}\right)^*\left(\mathbf{w}^{\mathrm{T}}\mathrm{diag}\{\boldsymbol{\rho}_h\}\mathbf{v}+\nu_{\mathrm{E}}\right)} = \frac{P_{\mathrm{s}}\mathbf{w}^{\mathrm{H}}\boldsymbol{\Gamma}_{fh}\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}\boldsymbol{\Gamma}_h\mathbf{w}} \tag{8}$$

where $\boldsymbol{\Gamma}_g = \mathrm{diag}(\rho_1^2|g_1|^2, \ldots, \rho_M^2|g_M|^2)$, $\boldsymbol{\Gamma}_{fh} = \mathrm{diag}(\rho_1{}^2|f_1|^2\sigma_{h_1}^2, \ldots, \rho_M{}^2|f_M|^2\sigma_{h_M}^2)$, and $\boldsymbol{\Gamma}_h = \mathrm{diag}\left(\rho_1{}^2\sigma_{h_1}^2, \ldots, \rho_M{}^2\sigma_{h_M}^2\right)$. Now we discuss how to design $\mathbf{w}$ to maximize C_{S}, and the proposed solution is denoted by $\mathbf{w}_{\mathrm{p}}^{\mathrm{AF}}$. It is obvious that maximizing C_{S} is equivalent to maximizing $\frac{1+\gamma_{\mathrm{D}}}{1+\gamma_{\mathrm{E}}}$. Hence, in what follows, the objective function will be $\frac{1+\gamma_{\mathrm{D}}}{1+\gamma_{\mathrm{E}}}$.

Substituting Equations 7 and 8 into $\frac{1+\gamma_{\mathrm{D}}}{1+\gamma_{\mathrm{E}}}$, we have

$$\mathbf{w}_{\mathrm{p}}^{\mathrm{AF}} = \arg\max_{\mathbf{w}^{\mathrm{H}}\mathbf{w}=P}\frac{1+\frac{P_{\mathrm{s}}\mathbf{w}^{\mathrm{H}}\boldsymbol{\rho}_{fg}\boldsymbol{\rho}_{fg}^{\mathrm{H}}\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}\boldsymbol{\Gamma}_g\mathbf{w}}}{1+\frac{P_{\mathrm{s}}\mathbf{w}^{\mathrm{H}}\boldsymbol{\Gamma}_{fh}\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}\boldsymbol{\Gamma}_h\mathbf{w}}} = \arg\max_{\mathbf{w}^{\mathrm{H}}\mathbf{w}=P}\frac{\mathbf{w}^{\mathrm{H}}\left(P_{\mathrm{s}}\boldsymbol{\rho}_{fg}\boldsymbol{\rho}_{fg}{}^{\mathrm{H}}+\boldsymbol{\Gamma}_g+P^{-1}\mathbf{I}\right)\mathbf{w}}{\mathbf{w}^{\mathrm{H}}\left(\mathbf{D}_h+P^{-1}\mathbf{I}\right)\mathbf{w}}\cdot\frac{\mathbf{w}^{\mathrm{H}}\left(\boldsymbol{\Gamma}_h+P^{-1}\mathbf{I}\right)\mathbf{w}}{\mathbf{w}^{\mathrm{H}}\left(\boldsymbol{\Gamma}_g+P^{-1}\mathbf{I}\right)\mathbf{w}} \tag{9}$$

where $\mathbf{D}_h = \mathrm{diag}\left\{\sigma_{h_1}^2, \ldots, \sigma_{h_M}^2\right\}$. This is a product of two correlated Rayleigh quotients [17] which is generally difficult to maximize. However, it would be much easier to

get a suboptimal solution if we approximate the objective function to a single Rayleigh quotient.

Rewrite the optimization problem as

$$\mathbf{w}_{\mathrm{p}}^{\mathrm{AF}} = \arg\max_{\mathbf{w}^{\mathrm{H}}\mathbf{w}=P} \frac{\mathbf{w}^{\mathrm{H}}\left(P_{\mathrm{s}}\boldsymbol{\rho}_{fg}\boldsymbol{\rho}_{fg}^{\mathrm{H}} + \boldsymbol{\Gamma}_g + P^{-1}\mathbf{I}\right)\mathbf{w}}{\frac{\mathbf{w}^{\mathrm{H}}\left(\mathbf{D}_h + P^{-1}\mathbf{I}\right)\mathbf{w}\cdot\mathbf{w}^{\mathrm{H}}\left(\boldsymbol{\Gamma}_g + P^{-1}\mathbf{I}\right)\mathbf{w}}{\mathbf{w}^{\mathrm{H}}\left(\boldsymbol{\Gamma}_h + P^{-1}\mathbf{I}\right)\mathbf{w}}}. \quad (10)$$

Denote the matrices $\mathbf{D}_h + P^{-1}\mathbf{I}$, $\boldsymbol{\Gamma}_g + P^{-1}\mathbf{I}$, and $\boldsymbol{\Gamma}_h + P^{-1}\mathbf{I}$ as $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$, respectively. For simplicity, we also let a_i, b_i, and c_i represent the ith diagonal entry of $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$, respectively, and define $\mathbf{p} = (P_1, \ldots, P_M)^{\mathrm{T}}$.

Since $P_i = |w_i|^2$, the denominator can be rewritten as $f(\mathbf{p}) = \sum_{i=1}^{M} a_i P_i \cdot \sum_{i=1}^{M} b_i P_i / \sum_{i=1}^{M} c_i P_i$. According to the Taylor series expansion $f(\mathbf{x}) = f(\mathbf{x}_0) + \sum_k \frac{\partial f(\mathbf{x}_0)}{\partial x_k}\left(x_k - x_{0,k}\right) + o\left(|\mathbf{x}-\mathbf{x}_0|\right)$,

$$f(\mathbf{p}) \approx f(\mathbf{p}_0) + \sum_{i=1}^{M} \frac{\partial f(\mathbf{p}_0)}{\partial P_i}\left(P_i - \frac{P}{M}\right) \quad (11)$$

if we expand $f(\mathbf{p})$ at $\mathbf{p}_0 = \left(\frac{P}{M}, \ldots, \frac{P}{M}\right)$. Since

$$f(\mathbf{p}) = \frac{\left(a_i P_i + \sum_{j=1, j\neq i}^{M} a_j P_j\right)\left(b_i P_i + \sum_{j=1, j\neq i}^{M} b_j P_j\right)}{c_i P_i + \sum_{j=1, j\neq i}^{M} c_j P_j}$$

$$= \frac{a_i b_i}{c_i} P_i + K_1 + \frac{K_2}{c_i P_i + \sum_{j=1, j\neq i}^{M} c_j P_j} \quad (12)$$

where $K_1 = \frac{a_i}{c_i}\sum_{j=1, j\neq i}^{M} b_j P_j + \frac{b_i}{c_i}\sum_{j=1, j\neq i}^{M} a_j P_j - \frac{a_i b_i}{c_i^2}\sum_{j=1, j\neq i}^{M} c_j P_j$ and $K_2 = \sum_{j=1, j\neq i}^{M} a_j P_j \cdot \sum_{j=1, j\neq i}^{M} b_j P_j - K_1 \sum_{j=1, j\neq i}^{M} c_j P_j$, we have $\frac{\partial f}{\partial P_i} \approx \frac{a_i b_i}{c_i}$. Substituting this partial derivative into (11), we further have $f(\mathbf{p}) \approx \sum_{i=1}^{M} \frac{a_i b_i}{c_i} P_i + K$ where $K = \frac{P}{M}\left(\frac{\mathrm{tr}(\mathbf{A})\,\mathrm{tr}(\mathbf{B})}{\mathrm{tr}(\mathbf{C})} - \mathrm{tr}\left(\mathbf{A}\mathbf{B}\mathbf{C}^{-1}\right)\right)$. It can be proved that K is negligible either with small P or large P if we make a commonly used assumption that the SR distances are about the same (see Appendix for details). Thus, we omit this part and rewrite $f(\mathbf{p})$ approximately as

$$f(\mathbf{p}) \approx \sum_{i=1}^{M} \frac{a_i b_i}{c_i} P_i = \mathbf{w}^{\mathrm{H}}\mathbf{A}\mathbf{B}\mathbf{C}^{-1}\mathbf{w} \quad (13)$$

So the optimization problem in (9) can be approximated to

$$\mathbf{w}_{\mathrm{p}}^{\mathrm{AF}} = \arg\max_{\mathbf{w}^{\mathrm{H}}\mathbf{w}=P} \frac{\mathbf{w}^{\mathrm{H}}\left(P_{\mathrm{s}}\boldsymbol{\rho}_{fg}\boldsymbol{\rho}_{fg}^{\mathrm{H}} + \boldsymbol{\Gamma}_g + P^{-1}\mathbf{I}\right)\mathbf{w}}{\mathbf{w}^{\mathrm{H}}\mathbf{A}\mathbf{B}\mathbf{C}^{-1}\mathbf{w}} \quad (14)$$

This is a single Rayleigh quotient problem. It has been reported in [17] that if $\mathbf{U}$ is Hermitian and $\mathbf{V}$ is positive definite Hermitian, for any non-zero column vector $\mathbf{x}$, we have $\frac{\mathbf{x}^{\mathrm{H}}\mathbf{U}\mathbf{x}}{\mathbf{x}^{\mathrm{H}}\mathbf{V}\mathbf{x}} \leq \lambda_{\max}\left(\mathbf{V}^{-1}\mathbf{U}\right)$ where $\lambda_{\max}(\mathbf{V}^{-1}\mathbf{U})$ is the largest eigenvalue of $\mathbf{V}^{-1}\mathbf{U}$. The equality holds if $\mathbf{x} = c\mathbf{u}_{\max}(\mathbf{V}^{-1}\mathbf{U})$ where c can be any non-zero constant and $\mathbf{u}_{\max}(\mathbf{V}^{-1}\mathbf{U})$ is the unit-norm eigenvector of $\mathbf{V}^{-1}\mathbf{U}$ corresponding to $\lambda_{\max}(\mathbf{V}^{-1}\mathbf{U})$. As a result, the optimal solution to (14) is

$$\mathbf{w}_{\mathrm{p}}^{\mathrm{AF}} = \sqrt{P}\mathbf{u}_{\lambda_{\max}}(\boldsymbol{\Phi}) \quad (15)$$

where $\boldsymbol{\Phi} = \mathbf{A}^{-1}\mathbf{B}^{-1}\mathbf{C}(P_{\mathrm{s}}\boldsymbol{\rho}_{fg}\boldsymbol{\rho}_{fg}^{\mathrm{H}} + \boldsymbol{\Gamma}_g + P^{-1}\mathbf{I})$.

To show the agreement of the approximated denominator and the exact denominator, we calculated them numerically, and the results are shown in Figure 2. The channel information we used are listed in Table 1 where $\mathbf{f} = (f_1, \ldots, f_M)^{\mathrm{T}}$, $\mathbf{g} = (g_1, \ldots, g_M)^{\mathrm{T}}$, and $\boldsymbol{\sigma}_h = \left(\sigma_{h_1}^2, \ldots, \sigma_{h_M}^2\right)^{\mathrm{T}}$. $\mathbf{f}$ and $\mathbf{g}$ are generated randomly.

For comparison purpose, we present two other beamforming designs. First, for the optimization of a product of two correlated Rayleigh quotient problems, a method was proposed recently in [8] to maximize the upper and lower bounds. Note that $\eta_{\min} \leq \frac{\mathbf{w}^{\mathrm{H}}\left(\boldsymbol{\Gamma}_h + P^{-1}\mathbf{I}\right)\mathbf{w}}{\mathbf{w}^{\mathrm{H}}\left(\boldsymbol{\Gamma}_g + P^{-1}\mathbf{I}\right)\mathbf{w}} \leq \eta_{\max}$ where $\eta_{\min} = \min_i \frac{\rho_i^2\sigma_{h_i}^2 + P^{-1}}{\rho_i^2|g_i|^2 + P^{-1}}$ and $\eta_{\max} = \max_i \frac{\rho_i^2\sigma_{h_i}^2 + P^{-1}}{\rho_i^2|g_i|^2 + P^{-1}} \cdot \frac{1+\gamma_{\mathrm{D}}}{1+\gamma_{\mathrm{E}}}$ is bounded as

$$\eta_{\min}\frac{\mathbf{w}^{\mathrm{H}}\left(P_{\mathrm{s}}\boldsymbol{\rho}_{fg}\boldsymbol{\rho}_{fg}^{\mathrm{H}} + \boldsymbol{\Gamma}_g + P^{-1}\mathbf{I}\right)\mathbf{w}}{\mathbf{w}^{\mathrm{H}}\left(\mathbf{D}_h + P^{-1}\mathbf{I}\right)\mathbf{w}} \leq \frac{1+\gamma_{\mathrm{D}}}{1+\gamma_{\mathrm{E}}} \leq \quad (16)$$

$$\eta_{\max}\frac{\mathbf{w}^{\mathrm{H}}\left(P_{\mathrm{s}}\boldsymbol{\rho}_{fg}\boldsymbol{\rho}_{fg}^{\mathrm{H}} + \boldsymbol{\Gamma}_g + P^{-1}\mathbf{I}\right)\mathbf{w}}{\mathbf{w}^{\mathrm{H}}\left(\mathbf{D}_h + P^{-1}\mathbf{I}\right)\mathbf{w}}.$$

As a result, the bounds maximization design for AF (B-AF) should be

$$\mathbf{w}_{\mathrm{b}}^{\mathrm{AF}} = \sqrt{P}\mathbf{u}_{\max}\left(\left(\mathbf{D}_h + P^{-1}\mathbf{I}\right)^{-1}\left(P_{\mathrm{s}}\boldsymbol{\rho}_{fg}\boldsymbol{\rho}_{fg}{}^{\mathrm{H}} + \boldsymbol{\Gamma}_g + P^{-1}\mathbf{I}\right)\right). \quad (17)$$

We also address the traditional design for AF (T-AF) where the eavesdropper is ignored and the goal is to maximize C_{D}. It can be easily proved that the optimal solution is $\mathbf{w}_{\mathrm{t}}^{\mathrm{AF}} = c^{\mathrm{AF}}\left(\boldsymbol{\Gamma}_g + P^{-1}\mathbf{I}\right)^{-1}\boldsymbol{\rho}_{fg}$ where c^{AF} is a constant chosen to satisfy $\left(\mathbf{w}_{\mathrm{t}}^{\mathrm{AF}}\right)^{\mathrm{H}}\mathbf{w}_{\mathrm{t}}^{\mathrm{AF}} = P$.

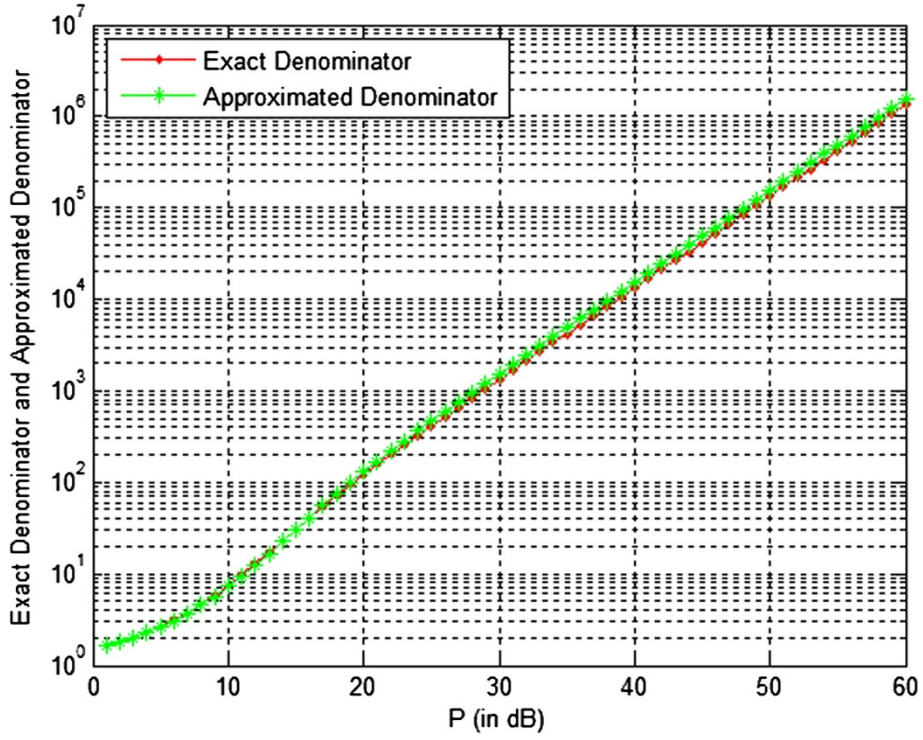

Figure 2 Comparison of the approximated denominator and the exact denominator.

3.2 Discussion about secrecy capacity in AF networks

It is natural to conjecture that secrecy capacity would grow as the eavesdropper moved away or as the total relay transmit power increased. However, we find that this conjecture is not always right.

For simplicity, we assume the distances between relays are much smaller than those between the relays and the source, so the path losses of the SR channels are almost the same. The same assumption is also made to the destination/eavesdropper. Denote the SR, RD, and RE distances as d_{SR}, d_{RD}, and d_{RE}, respectively, and the corresponding channel variances as σ_f^2, σ_g^2, and σ_h^2, respectively.

Proposition 1. *If the destination is much nearer to the relays than the eavesdropper is in an AF network, C_{S} does not always grow as the total relay transmit power increases, and a suboptimal value of the total relay transmit power is found as*

$$P_{\mathrm{subopt}} = d_{\mathrm{RD}}^2 d_{\mathrm{RE}}^2 \sqrt{1 + d_{\mathrm{SR}}^{-4} P_{\mathrm{s}}} \tag{18}$$

Proof. Recall that $\frac{1+\gamma_{\mathrm{D}}}{1+\gamma_{\mathrm{E}}} \approx \frac{\mathbf{w}^{\mathrm{H}}\left(P_{\mathrm{s}}\boldsymbol{\rho}_{fg}\boldsymbol{\rho}_{fg}^{\mathrm{H}}+\boldsymbol{\Gamma}_g+P^{-1}\mathbf{I}\right)\mathbf{w}}{\mathbf{w}^{\mathrm{H}}\mathbf{A}\mathbf{B}\mathbf{C}^{-1}\mathbf{w}}$. No matter how we design the beamforming vector $\mathbf{w}$, $\frac{\mathbf{w}^{\mathrm{H}}\left(P_{\mathrm{s}}\boldsymbol{\rho}_{fg}\boldsymbol{\rho}_{fg}^{\mathrm{H}}+\boldsymbol{\Gamma}_g+P^{-1}\mathbf{I}\right)\mathbf{w}}{\mathbf{w}^{\mathrm{H}}\mathbf{A}\mathbf{B}\mathbf{C}^{-1}\mathbf{w}}$ is bounded as

$$\lambda_{\min}(\boldsymbol{\Phi}) \le \frac{\mathbf{w}^{\mathrm{H}}\left(P_{\mathrm{s}}\boldsymbol{\rho}_{fg}\boldsymbol{\rho}_{fg}^{\mathrm{H}}+\boldsymbol{\Gamma}_g+P^{-1}\mathbf{I}\right)\mathbf{w}}{\mathbf{w}^{\mathrm{H}}\mathbf{A}\mathbf{B}\mathbf{C}^{-1}\mathbf{w}} \le \lambda_{\max}(\boldsymbol{\Phi}). \tag{19}$$

Due to the difficulty of calculating the eigenvalues of $\boldsymbol{\Phi}$, we replace the non-diagonal elements in $\boldsymbol{\Phi}$ with their mean value 0 and the ith diagonal element $\frac{\left(\rho_i^2\sigma_h^2P+1\right)\left(|g_i|^2P+1\right)}{\left(\sigma_h^2P+1\right)\left(\rho_i^2|g_i|^2P+1\right)}$ with $\lambda(P) = \frac{\left(\rho^2\sigma_h^2P+1\right)\left(\sigma_g^2P+1\right)}{\left(\sigma_h^2P+1\right)\left(\rho^2\sigma_g^2P+1\right)}$ where $\rho^2 = \frac{1}{1+\sigma_f^2P_{\mathrm{s}}}$. Thus, $\boldsymbol{\Phi}$ becomes $\lambda(P)\mathbf{I}$ after replacement.

Define $C_{\mathrm{S}}(P) = \frac{1}{2}\log_2\lambda(P)$. Now we investigate the monotonicity of $C_{\mathrm{S}}(P)$. The first-order derivatives of $C_{\mathrm{S}}(P)$ and $\lambda(P)$ can be computed, respectively, as

$$C_{\mathrm{S}}^{'}(P) = \frac{1}{2\ln 2}\cdot\frac{\lambda^{'}(P)}{\lambda(P)} \tag{20}$$

and

$$\lambda^{'}(P) = \frac{\left(\sigma_h^2-\sigma_g^2\right)(1-\rho^2)\left(\rho^2\sigma_h^2\sigma_g^2P^2-1\right)}{\left(\sigma_h^2P+1\right)^2\left(\rho^2\sigma_g^2P+1\right)^2}. \tag{21}$$

By setting $C_{\mathrm{S}}^{'}(P) = 0$, we obtain the positive stationary point of $C_{\mathrm{S}}(P)$ as described in (18).

If $d_{\mathrm{RE}} > d_{\mathrm{RD}}$ ($\sigma_h^2 < \sigma_g^2$), $\forall P \in (0, P_{\mathrm{subopt}})$, we have $C_{\mathrm{S}}^{'}(P) > 0$; $\forall P \in (P_{\mathrm{subopt}}, +\infty)$, we have $C_{\mathrm{S}}^{'}(P) < 0$. Hence, if the

Table 1 Channel coefficients used in Figure 2

Number	Channel coefficients realizations
$M = 6$	$\mathbf{f} = \begin{pmatrix} -0.4089 + 0.1458j \\ 0.0133 - 0.5438j \\ 0.7090 - 0.9965j \\ 0.5620 + 0.0720j \\ -0.0073 - 1.4754j \\ 0.8965 - 0.1606j \end{pmatrix}$ $\mathbf{g} = \begin{pmatrix} -0.4610 - 0.6694j \\ 0.6549 + 1.1034j \\ -0.0089 - 0.7161j \\ -0.2441 - 0.6272j \\ -0.5381 + 0.5625j \\ -0.7230 - 0.6100j \end{pmatrix}$ $\boldsymbol{\sigma}_h = \begin{pmatrix} 0.21 \\ 0.20 \\ 0.18 \\ 0.22 \\ 0.15 \\ 0.12 \end{pmatrix}$

destination is much nearer than the eavesdropper is, $C_S(P)$ is an increasing function over $(0, P_{subopt})$ and a decreasing function over $(P_{subopt}, +\infty)$, which means that $C_S(P_{subopt})$ is the maximum of $C_S(P)$.

This monotonicity of C_S and the accuracy of P_{subopt} under the case of $d_{RE} > d_{RD}$ will be verified in the next section. It needs to be pointed out that the above analysis is not for any certain design, so the optimal value of P for a certain design would be different from but around P_{subopt}. It also needs to be pointed out that the replacement of the channel coefficients in $\boldsymbol{\Phi}$ with their mean values may result in the loss of the security benefit that is supposed to be achieved by exploiting the perfect CSI of SR and RD channels. This loss does not affect the monotonicity of C_S greatly under the case of $d_{RE} > d_{RD}$ because the destination is much nearer and therefore much more advantageous in communication than the eavesdropper is. However, when $d_{RE} < d_{RD}$ (or $d_{RE} = d_{RD}$), such replacement becomes inappropriate, since the instantaneous CSI of f_i and g_i improves the system security significantly.

We can further compute the second-order derivatives of $C_S(P)$ and $\lambda(P)$, respectively, as

$$C_S''(P) = \frac{1}{2\ln 2} \cdot \frac{\lambda''(P)\lambda(P) - \left(\lambda'(P)\right)^2}{\lambda^2(P)} \tag{22}$$

and

$$\lambda''(P) = \frac{2\left(\sigma_h^2 - \sigma_g^2\right)(1-\rho^2)\left(-\rho^4\sigma_h^4\sigma_g^4P^3 + 3\rho^2\sigma_h^2\sigma_g^2P + \sigma_h^2 + \rho^2\sigma_g^2\right)}{\left(\sigma_h^2P + 1\right)^3\left(\rho^2\sigma_g^2P + 1\right)^3}. \tag{23}$$

It can be observed from (22) that the positivity of $C_S''(P)$ depends on the value of P. Thus, $C_S(P)$ is neither convex nor concave.

Remark 1. In an AF network, if the total relay transmit power is large, the AWGNs in the second hop are negligible compared to the forwarded versions of the AWGNs in the first hop. Thus, $\frac{1+\gamma_D}{1+\gamma_E}$ can be approximately written as

$$\frac{1+\gamma_D}{1+\gamma_E} \approx \frac{\mathbf{w}^H\left(P_s\boldsymbol{\rho}_{fg}\boldsymbol{\rho}_{fg}^H + \boldsymbol{\Gamma}_g\right)\mathbf{w}}{P} \cdot \frac{\mathbf{w}^H\mathrm{diag}\left(\rho_1^2, \ldots, \rho_M^2\right)\mathbf{w}}{\mathbf{w}^H\boldsymbol{\Gamma}_g\mathbf{w}}. \tag{24}$$

This equation does not involve σ_h^2, which implies C_S is a constant in this case wherever the eavesdropper is.

4. Distributed beamforming design for DF

This section focuses on the security-oriented beamforming design for DF protocol. Similar to the design for AF protocol, the mission is to find the optimal design under a total relay transmit power constraint to maximize secrecy capacity.

4.1 Proposed design for DF (P-DF)

From Equations 4 and 5, the received SNRs at the destination and the eavesdropper are obtained, respectively, as follows:

$$\gamma_D = \frac{\underset{s}{E}\left(\mathbf{w}^T\mathbf{g}s\right)^*\left(\mathbf{w}^T\mathbf{g}s\right)}{\underset{\nu_D}{E}\,\nu_D^*\nu_D} = \mathbf{w}^H\mathbf{g}\mathbf{g}^H\mathbf{w} \tag{25}$$

$$\gamma_E = \frac{\underset{s,\mathbf{h}}{E}\left(\mathbf{w}^T\mathbf{h}s\right)^*\left(\mathbf{w}^T\mathbf{h}s\right)}{\underset{\nu_E}{E}\,\nu_E{}^*\nu_E} = \mathbf{w}^H\mathbf{D}_h\mathbf{w}. \tag{26}$$

Let $\mathbf{w}_p^{DF}$ be the optimal solution of the proposed design, then

$$\begin{aligned} \mathbf{w}_p^{DF} &= \arg\max_{\mathbf{w}^H\mathbf{w}=P} \frac{1 + \mathbf{w}^H\mathbf{g}\mathbf{g}^H\mathbf{w}}{1 + \mathbf{w}^H\mathbf{D}_h\mathbf{w}} \\ &= \arg\max_{\mathbf{w}^H\mathbf{w}=P} \frac{\mathbf{w}^H(\mathbf{I} + P\mathbf{g}\mathbf{g}^H)\mathbf{w}}{\mathbf{w}^H(\mathbf{I} + P\mathbf{D}_h)\mathbf{w}} \\ &= \sqrt{P}\mathbf{u}_{\max}\left((\mathbf{I} + P\mathbf{D}_h)^{-1}\left(\mathbf{I} + P\mathbf{g}\mathbf{g}^H\right)\right). \end{aligned} \tag{27}$$

For comparison purpose, we also address the traditional design for DF (T-DF) and denote the solution by $\mathbf{w}_t^{DF}$. The optimization problem is formulated as $\mathbf{w}_t^{DF} = \arg\max_{\mathbf{w}^H\mathbf{w}=P} \mathbf{w}^H\mathbf{g}\mathbf{g}^H\mathbf{w}$, and the optimal solution is obviously $\mathbf{w}_t^{DF} = c^{DF}\mathbf{g}$ where c^{DF} is a constant chosen to satisfy the power constraint $\left(\mathbf{w}_t^{DF}\right)^H\mathbf{w}_t^{DF} = P$.

4.2 Discussion about secrecy capacity in DF networks

It is a natural thought that no matter under what channel assumption, secrecy capacity achieved by security-

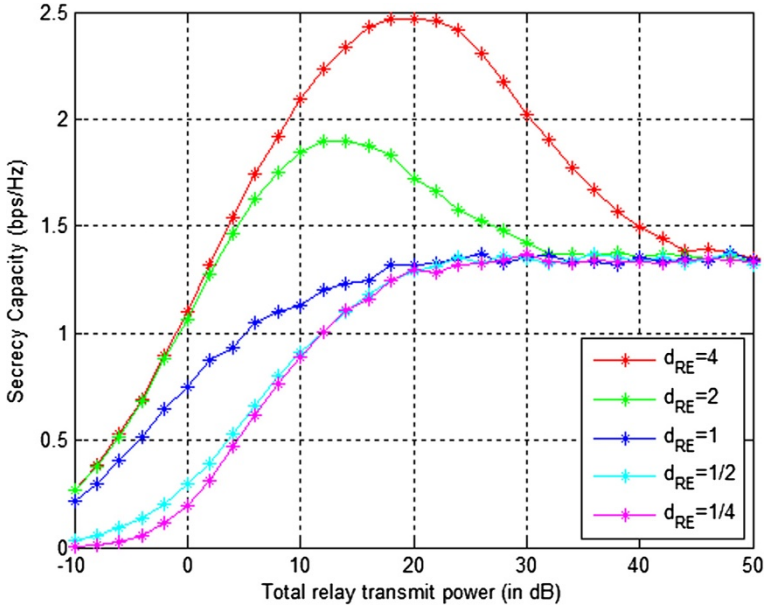

Figure 3 Secrecy capacity versus total relay transmit power using P-AF design.

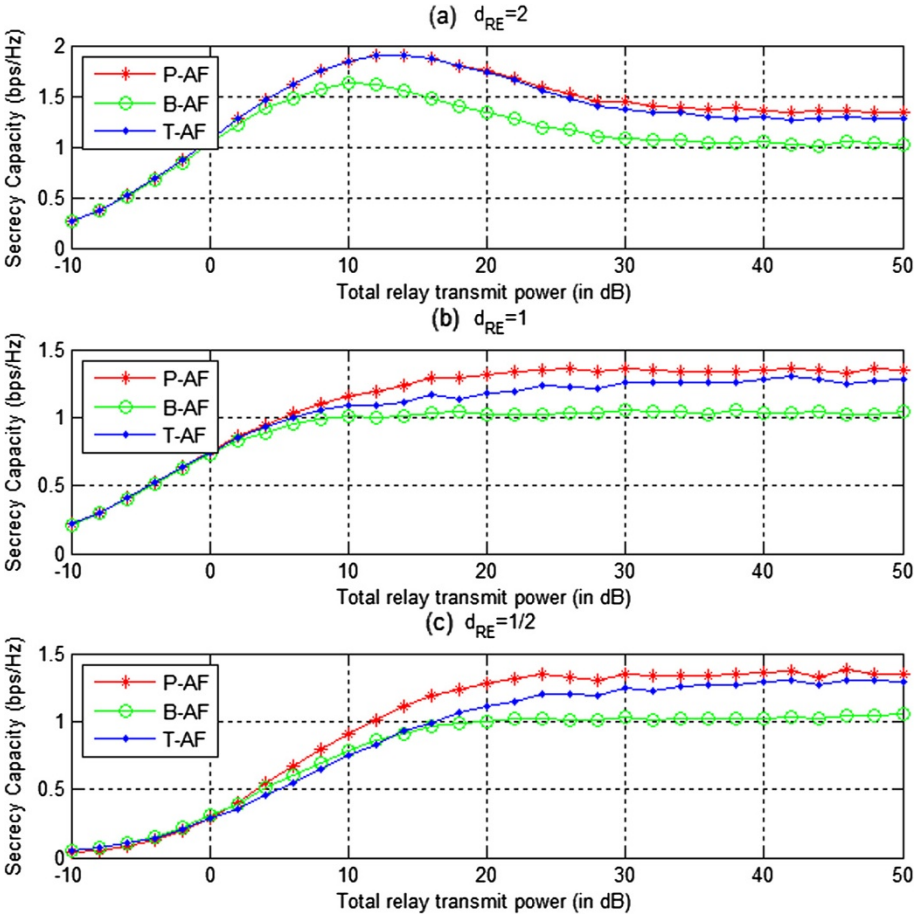

Figure 4 Secrecy capacity versus total relay transmit power using different AF designs.

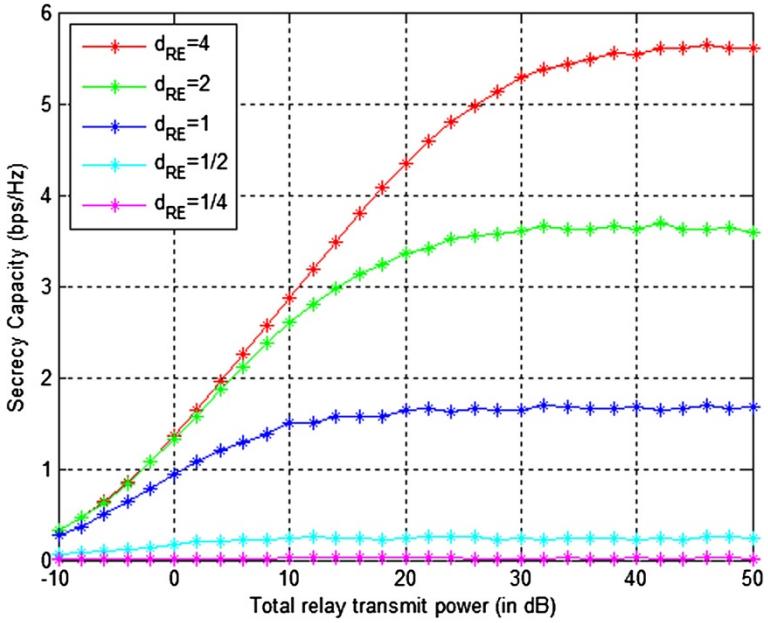

Figure 5 Secrecy capacity versus total relay transmit power using P-DF design.

oriented designs would be higher than that achieved by traditional designs. However, the fact is that these designs may have the same performance which means that sometimes we can just ignore the eavesdropper.

Remark 2. In a DF network, if the RE distances are about the same (which is widely assumed), it is unnecessary to consider the eavesdropper as the security-oriented design and the traditional design are indeed the same.

Noticing that in this scenario, we can write $\mathbf{D}_h$ as $\sigma_h^2\mathbf{I}$. Thus, one can rewrite (27) as $\mathbf{w}_{\mathrm{p}}^{\mathrm{DF}} = \sqrt{P}\mathbf{u}_{\max}\left(\frac{\mathbf{I}+P\mathbf{g}\mathbf{g}^{\mathrm{H}}}{1+P\sigma_h^2}\right) = \sqrt{P}\mathbf{u}_{\max}(\mathbf{I}+P\mathbf{g}\mathbf{g}^{\mathrm{H}})$. Since

$$\begin{aligned}(\mathbf{I}+P\mathbf{g}\mathbf{g}^{\mathrm{H}})\cdot\mathbf{u}_{\max}(P\mathbf{g}\mathbf{g}^{\mathrm{H}}) &= (1+\lambda_{\max}(P\mathbf{g}\mathbf{g}^{\mathrm{H}}))\cdot\mathbf{u}_{\max}(P\mathbf{g}\mathbf{g}^{\mathrm{H}}) \\ &= \lambda_{\max}(\mathbf{I}+P\mathbf{g}\mathbf{g}^{\mathrm{H}})\cdot\mathbf{u}_{\max}(P\mathbf{g}\mathbf{g}^{\mathrm{H}}),\end{aligned} \tag{28}$$

we have $\mathbf{u}_{\max}(\mathbf{I}+P\mathbf{g}\mathbf{g}^{\mathrm{H}}) = \mathbf{u}_{\max}(P\mathbf{g}\mathbf{g}^{\mathrm{H}})$. Thus, $\mathbf{w}_{\mathrm{p}}^{\mathrm{DF}} = c^{\mathrm{DF}}\mathbf{g}$ which is the same as $\mathbf{w}_{\mathrm{t}}^{\mathrm{DF}}$.

5. Numerical results

In this section, we investigate the performance of the above beamforming designs numerically. The simulation environment follows the model of Section 2. We perform Monte Carlo experiments consisting of 10,000 independent trials to obtain the average results.

Assume the number of relays is $M = 6$, and the source transmit power is $P_{\mathrm{s}} = 10$ dB. In order to show the influence of the RE distance in AF protocol, we fix the source at (0,0), the destination at (2,0), and the relays at (1,0) and move the eavesdropper from (1.25,0) to (5,0). We assume that the distances between relays are much smaller than SR/RD/RE distances. Therefore, the SR channels and RD channels follow a $\mathcal{CN}(0,1)$ distribution, and the RE distance d_{RE} varies from 0.25 to 4.

Figure 3 shows the relationship between average secrecy capacity and total relay transmit power with the eavesdropper in different locations using P-AF design. We can see that if the eavesdropper is nearer to the relays than the destination is, the relays should use the maximal power to transmit. However, if the destination is much nearer, there is an optimal value of total relay transmit power which is about 12 dB under the case of $d_{\mathrm{RE}} = 2$, while the theoretical value in (18) is $4\sqrt{1+10} \approx 11.23$ dB which is not very accurate but close. The reason is that P_{subopt} satisfies $d\left(\frac{1}{2}\log_2\lambda(P)\right)/dP = 0$ while the optimal power for P-AF design should satisfy $d\left(\frac{1}{2}\log_2\lambda_{\max}(\mathbf{\Phi})\right)/dP = 0$. However, it is difficult to express $\lambda_{\max}(\mathbf{\Phi})$ in terms of the total relay transmit power and the channel coefficients, not to mention to solve the latter equation analytically. It can also be seen that as the total relay transmit power increases, the secrecy capacity tends to keep constant no matter where the eavesdropper is.

Figure 4 compares different AF beamforming designs. It can be seen that the B-AF design shows a slight advantage over the T-AF design only when the total relay transmit power is small in the $d_{\mathrm{RE}} = 1/2$ case, while our proposed design always performs the best.

The relationship between average secrecy capacity and total relay transmit power with the eavesdropper

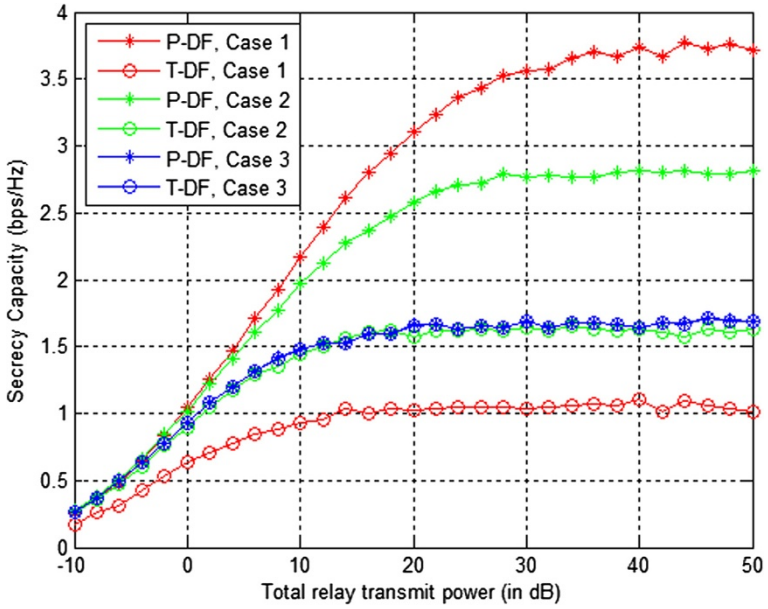

Figure 6 Secrecy capacity versus total relay transmit power under different DF designs.

in different locations using P-DF design is demonstrated in Figure 5. We still assume the RE distances to be the same. Results show that the secrecy capacity of a DF network grows as the total relay transmit power increases or as the eavesdropper moves away.

To verify Remark 2, we now examine the P-DF design and T-DF design under different variance assumptions of the RE channels.

$$\text{Case 1: } \boldsymbol{\sigma}_h = (1\,0 \quad 5 \quad 1 \quad 0.1 \quad 0.05 \quad 0.01)^{\mathrm{T}}$$
$$\text{Case 2: } \boldsymbol{\sigma}_h = (3 \quad 2 \quad 1 \quad 0.5 \quad 0.1 \quad 0.05)^{\mathrm{T}}$$
$$\text{Case 3: } \boldsymbol{\sigma}_h = (1.1 \quad 1.05 \quad 1 \quad 0.95 \quad 0.9 \quad 0.85)^{\mathrm{T}}$$

The average secrecy capacities of P-DF and T-DF designs under different RE channel assumptions are demonstrated in Figure 6. Our design outperforms the traditional design in case 1 and case 2. While in case 3, the two designs have the same performance. This indicates that the greater the RE channels differ from each other, the more superior the P-DF design is. If the RE distances are almost the same, the eavesdropper can be ignored.

6. Conclusions

In this paper, we focused on security-oriented distributed beamforming designs for relay networks in the presence of a passive eavesdropper. We provided two beamforming designs under a total relay transmit power constraint, one of which is for AF and the other is for DF. Each design is to maximize secrecy capacity by exploiting information of SR, RD, and RE channels. To derive the beamforming solution for AF requires approximating the optimization objective by using the Taylor series expansion, while the solution for DF is obtained much more easily. We also found that secrecy capacity does not always grow if the relays use more power to transmit or if the eavesdropper gets farther from the relays, and that taking the eavesdropper into consideration is not always necessary. Moreover, for AF, we derived a suboptimal value of the total relay transmit power if the destination is nearer than the eavesdropper is. Numerical results showed the efficiency of the proposed designs.

Appendix

Noticing that

$$K = \frac{1}{M}\left(\frac{\left(\sum_{i=1}^{M}\sigma_{h_i}^2 P + M\right)\left(\sum_{i=1}^{M}\rho_i^2 |g_i|^2 P + M\right)}{\sum_{i=1}^{M}\rho_i^2\sigma_{h_i}^2 P + M} - \sum_{i=1}^{M}\frac{\left(\sigma_{h_i}^2 P + 1\right)\left(\rho_i^2 |g_i|^2 P + 1\right)}{\rho_i^2\sigma_{h_i}^2 P + 1}\right), \tag{29}$$

we have $K \approx \frac{1}{M}\left(\frac{M^2}{M} - M\right) = 0$ with small P, and

$$K \approx \frac{P}{M}\left(\frac{\sum_{i=1}^{M}\sigma_{h_i}^2\sum_{i=1}^{M}\rho_i^2|g_i|^2}{\sum_{i=1}^{M}\rho_i^2\sigma_{h_i}^2} - \sum_{i=1}^{M}|g_i|^2\right) \tag{30}$$

with large P. If we make the assumption that the SR distances are all about the same, i.e., the $\sigma_{f_i}^2$'s are about the same (which is also assumed in [8]), and replace $|f_i|^2$ in the expression of ρ_i^2 with its mean value σ_f^2, we have

$$\frac{\sum_{i=1}^{M}\sigma_{h_i}^2\sum_{i=1}^{M}\rho_i^2|g_i|^2}{\sum_{i=1}^{M}\rho_i^2\sigma_{h_i}^2} \approx \sum_{i=1}^{M}|g_i|^2. \tag{31}$$

Thus, $K \approx 0$ with large P.

Competing interests
The authors declare that they have no competing interests.

Acknowledgements
This work is supported by the Natural Science Foundation of China under Grants 61372126 and 61302101, and the open research fund of National Mobile Communications Research Laboratory in Southeast University under Grant 2012D11.

Author details
[1]The Key Lab of Broadband Wireless Communication and Sensor Network Technology (Ministry of Education), Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210003, China. [2]National Mobile Communications Research Laboratory, Southeast University, Nanjing, Jiangsu 210096, China.

Received: 13 March 2014 Accepted: 8 April 2014
Published: 28 April 2014

References

1. A Sendonaris, E Erkip, B Aazhang, User cooperative diversity-part I: system description. IEEE Trans. Commun. **51**(11), 1927–1938 (2003)
2. A Sendonaris, E Erkip, B Aazhang, User cooperative diversity-part II: implementation aspects and performance analysis. IEEE Trans. Commun. **51**(11), 1939–1948 (2003)
3. JN Laneman, DNC Tse, Cooperative diversity in wireless networks: efficient protocols and outage behaviour. IEEE Trans. Inf. Theory **51**(12), 3062–3080 (2004)
4. AD Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
5. SK Leung-Yan-Cheong, ME Hellman, The Gaussian wiretap channels. IEEE Trans. Inf. Theory **24**(4), 451–456 (1978)
6. PK Gopala, L Lai, HE Gamal, On the secrecy capacity of fading channels. IEEE Trans. Inf. Theory **54**(10), 4687–4698 (2008)
7. L Dong, H Zhu, AP Petropulu, HV Poor, Secure wireless communication via cooperation, in *The 46-th Annual Allerton Conference on Communication, Control and Computing* (Urbana-Champaign, IL, USA, 23–26 September 2008), pp. 1132–1138
8. L Dong, Z Han, AP Petropulu, HV Poor, Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010)
9. I Krikidis, S Thompson, S McLaughlin, Relay selection for secure cooperative networks with jamming. IEEE Trans. Wirel. Commun. **8**(10), 5003–5011 (2009)
10. J Kim, A Ikhlef, R Schober, Combined relay selection and cooperative beamforming for physical layer Security. IEEE J. Commun. Netw. **14**(4), 364–373 (2012)
11. C Jeong, I-M Kim, DI Kim, Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system. IEEE Trans. Signal Process. **60**(1), 310–325 (2012)
12. X He, A Yener, End-to-end secure multi-hop communication with untrusted relays. IEEE Trans. Wirel. Commun. **12**(1), 1–11 (2013)
13. Y Zou, X Wang, W Shen, Optimal relay selection for physical-layer security in cooperative wireless networks. IEEE J. Select. Areas Commun. **31**(10), 2099–2111 (2013)
14. Y Yang, Q Li, J Ge, PC Ching, Cooperative secure beamforming for AF relay networks with multiple eavesdroppers. IEEE Signal Process. Lett. **20**(1), 35–38 (2013)
15. H-M Wang, M Luo, Q Yin, X-G Xia, Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks. IEEE Trans. Inf. Forensics Secur. **8**(12), 2007–2020 (2013)
16. Z Chen, H Li, G Cui, M Rangaswamy, Adaptive transmit and receive beamforming for interference mitigation. IEEE Signal Process. Lett. **21**(2), 235–239 (2014)
17. X Zhang, *Matrix Analysis and Applications* (Tsinghua University Press, Beijing, 2004), pp. 528–541

doi:10.1186/1687-6180-2014-56
Cite this article as: Qian *et al.*: Distributed beamforming designs to improve physical layer security in wireless relay networks. *EURASIP Journal on Advances in Signal Processing* 2014 **2014**:56.