Beamforming Design of Decode-and-Forward Cooperation for Improving Wireless Physical Layer Security

Hui MA, Piming MA

School of Information Science and Engineering, Shandong University, China

maphoenix@126.com, mapiming@sdu.edu.cn

***Abstract*—Physical-layer-based security aims at ensuring the reliability of communication and preventing eavesdropping by taking advantage of the physical layer's characteristics rather than the data encryption in upper layer. Cooperation is a way to achieve this goal with many benefits for wireless communication. In particular, the cooperation scheme called decode-and-forward (DF) is discussed in this paper and our objective is to design the beamforming weight of each cooperating node which is one antenna equipped for maximum achievable secrecy rate. Considering that individual power constraint is more reasonable than total power constraint and to set noise power levels at the destination and the eavesdropper different is more practical than the same, we get the whole optimization problem which is unconvex. With the help of perfect global channel state information (CSI), the problem is solved through a way where convex optimization and one-dimensional search are combined together. And strict proofs are presented for this method. Then zero-forcing (ZF) based simplification and extension to cope with multi-antenna case are discussed. Numerical results show that the proposed design can significantly improve the security performance of wireless systems.**

***Index Terms*—physical layer security, maximum achievable secrecy rate, cooperating relays, beamforming, convex analysis.**

I. INTRODUCTION

SECURE data transmission plays an important role in wireless communication system. However, the open nature of wireless communication makes it vulnerable to wiretapping. At physical layer, this problem was first studied by Wyner [1] from an information-theoretic perspective. Wyner demonstrated that secure communication is possible without relying on private (secret) keys if the source-eavesdropper channel is a degraded version of the main (source-destination) channel, even though the eavesdropper has unlimited computation ability and know the coding/decoding scheme. He used a concept 'secrecy rate' to describe a rate at which information can be transmitted reliably in the main channel and can not be wiretapped by the eavesdropper, and defined 'secrecy capacity' as the maximal achievable secrecy rate. Then, Wyner's result was generalized to the Gaussian channel [2].In [3] secure communications over broadcast channels were studied by I. Csiszár and J. Körner. In recent years, considerable efforts have been made to extending this line of work to the fading channel like [4] ,[5].

To overcome the problem that the traditional single antenna system based PHY layer security approaches are infeasible when Wyner's condition is not met [1], [2], some recent works have been proposed to make up for this weakness by using multiple antenna technique e.g., multiple-input multiple-output (MIMO) [6-10], single-input multiple-output (SIMO) [11] and multiple-input single-output (MISO) [12-13].

Additionally, another more flexible and practical approach is relaying cooperation where the source to destination transmission is helped by relays. Totally, there are three cooperative schemes which can be used to provide security, i.e. decode-and-forward (DF), amplify-and-forward (AF) and cooperative jamming (CJ). And in particular, the security performance of DF based cooperation system has attracted much attention in recent years [14-17].

In [14] and [15], a DF based cooperative protocol was considered and beamforming vector of relays was designed for the achievable secrecy rate maximization or transmit power minimization. However these works just took the circumstance with a total power constraint into account.

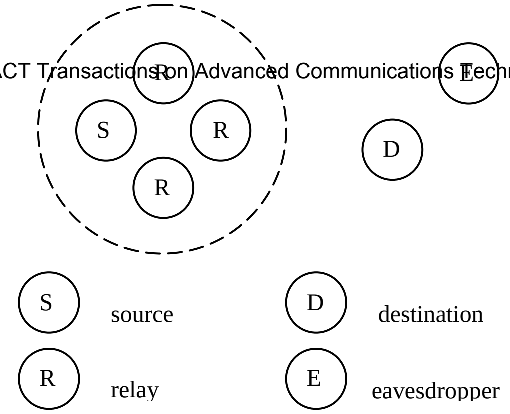
Because relays are distributed and independent in many applications, individual relay power constraints are more reasonable than the total power constraint in these case. As a complement, Junwei Zhang considered the maximization of the secrecy rate of DF model with individual relay power constraints through semidefinite programming (SDP) in [16]. But the optimal value we got through the SDP problem may not be the maximum secrecy rate of the system, because there is no proof that can show the existence of rank-one optimal solutions of the SDP problem in [16].

Figure 1. System model

In this paper, a more practical system model with different noise power at different nodes than that in [16] is studied.

Manuscript received May 15, 2012.

H. Ma and P.M. Ma are with the School of Information Science and Engineering, Shandong University, Jinan, China(corresponding author, P.M. Ma to provide phone:+86-531-88364613; fax:+86-531-88364613; e-mail: mapiming@ sdu.edu.cn).



Based on this model where each cooperating node is one antenna equipped, a new algorithm is proposed by combining the convex optimization and the one-dimensional search together to obtain the maximum achievable secrecy rate with sufficient proofs. Then a simplified problem with zero-forcing (ZF) constraint is discussed. Further more, in the end, the proposed algorithm is generalized to cope with the more complicate multi-antenna case.

This paper is organized as follows. In Section II, we will introduce the system model and the DF-based cooperative protocol. In Section III, we will propose and prove our algorithm for the maximum secrecy rate and the corresponding beamforming vector. Then we discuss the simplified problem in Section IV and the extension in Section V. Simulation results are presented in Section VI, and conclusions are given in Section VII.

II. System Model and Cooperative Protocol

In this paper, we first consider a scenario in which there is only one source node S, one eavesdropper node E, one destination node D and N relay nodes labelled as $\{R_0, \ldots\ldots, R_{N-1}\}$. As Figure 1 illustrates, the source and relays are in the same cluster, while the destination and eavesdropper are located far away from this cluster. Each network node is equipped with only an omni-directional antenna. All channels are flat fading, quasistatic and memoryless. The global CSI is available for system design. And thermal noise at all nodes is zero-mean white complex Gaussian. Besides, it is assumed that the number of relays is known before optimization.

The system works under a DF-based cooperative protocol. The protocol is divided into two stages and can be described as follows. In Stage I, the source transmits a message to other nodes within the cluster, and then the relays receive and decode it. When transmitting the symbol x_S, the received signal at the relay R_i can be expressed as

$$y_{R,i} = x_S l_i + n_{R,i} \tag{1}$$

where $l_i \in \mathbb{C}$ denotes the channel between R_i and S and $n_{R,i}$ is the noise at R_i with variance $\sigma_{R,i}^2$. As the distance between the source and the relays are not too long, the relays can decode the received signal properly. And the power of the signal broadcasted by the source would be small so that the faraway destination and eavesdropper can receive none of it.

In Stage II, relay nodes re-encode the decoded message and then cooperatively transmit weighted versions of the re-encoded symbols to the destination and the eavesdropper. When the re-encoded symbol $\tilde{x}_S$ is transmitted by relays, the signal y_D which is received at D equals

$$y_D = \sum_{i=0}^{N-1} w_i h_i \tilde{x}_S + n_D \tag{2}$$

where w_i $(i = 0, 1, \ldots\ldots N-1)$ means the beamforming factor at R_i, $h_i \in \mathbb{C}$ is the channel between R_i and D, and n_D is the noise at D with variance σ_D^2. Then the signal y_E which is the signal at E can be expressed as,

$$y_E = \sum_{i=0}^{N-1} w_i g_i \tilde{x}_S + n_E \tag{3}$$

where $g_i \in \mathbb{C}$ denotes the channel between R_i and E, and n_E is the noise at E with variance σ_E^2. Without the loss of generality, all the symbols in the re-encoded message are normalized, i.e. $E[|\tilde{x}_S|^2] = 1$ where $E[\cdot]$ denotes expectation.

Let's define $\mathbf{w} = [w_0, \ldots., w_{N-1}]^T$, $\mathbf{h} = [h_0, \ldots., h_{N-1}]^H$, $\mathbf{g} = [g_0, \ldots\ldots, g_{N-1}]^H$ and $R_{\mathbf{h}} = \mathbf{h}\mathbf{h}^H$, $R_{\mathbf{g}} = \mathbf{g}\mathbf{g}^H$ where superscripts $(\cdot)^T$ and $(\cdot)^H$ represent transpose and conjugate transpose respectively. Then the SNR at D and E can be expressed as $\Gamma_D = |\mathbf{h}^H\mathbf{w}|^2 / \sigma_D^2$ and $\Gamma_E = |\mathbf{g}^H\mathbf{w}|^2 / \sigma_E^2$ respectively. As discussed in [2], for a given $\mathbf{w}$ the secrecy capacity $C_S(\mathbf{w})$ is

$$\begin{aligned} C_S(\mathbf{w}) &= \max\{\frac{1}{2}\left(\log(1+\Gamma_D) - \log(1+\Gamma_E)\right), 0\} \\ &= \max\{\frac{1}{2}\log(\frac{1+\Gamma_D}{1+\Gamma_E}), 0\} \end{aligned} \tag{4}$$

III. Design for Achievable Secrecy Rate Maximization

Aiming at finding out the maximum achievable secrecy rate of this system which works under the protocol we described, it is obvious that we should try to maximize $C_S(\mathbf{w})$ via the design of the beamforming vector. Considering individual power constraints is more practical in the relay system, the problem what we are interested in is formulated as follows,

$$\begin{aligned} &\underset{\mathbf{w}}{\text{maximize}}: \quad C_S(\mathbf{w}) \\ &\text{subject to}: \quad |w_i|^2 \le p_i, \quad i = 0, \ldots, N-1 \end{aligned} \tag{5}$$

where p_i is the power constraint for R_i, $\forall i = 0, \ldots, N-1$.

Because of the property of function $\max\{\cdot, \ \}$ and $\log(\cdot)$, in order to solve (5), we could solve the following problem first,

$$\begin{aligned}&\underset{\mathbf{w}}{\text{maximize:}} \quad \frac{1+\dfrac{\mathbf{w}^H R_{\mathbf{h}}\mathbf{w}}{s_D^2}}{1+\dfrac{\mathbf{w}^H R_{\mathbf{g}}\mathbf{w}}{s_E^2}} \\ &\text{subject to:} \quad |w_i|^2 \leq p_i, \quad i = 0,\ldots,N-1\end{aligned} \tag{6}$$

which can be re-expressed as

$$\begin{aligned}&\underset{\mathbf{w}}{\text{maximize:}} \quad \frac{s_E^2(s_D^2+\mathbf{w}^H R_{\mathbf{h}}\mathbf{w})}{s_D^2(s_E^2+\mathbf{w}^H R_{\mathbf{g}}\mathbf{w})} \\ &\text{subject to:} \quad |w_i|^2 \leq p_i, \quad i = 0,\ldots,N-1\end{aligned} \tag{7}$$

Because s_E^2 / s_D^2 is a constant, (7) can be simplified into

$$\begin{aligned}&\underset{\mathbf{w}}{\text{maximize:}} \quad \frac{s_D^2+\mathbf{w}^H R_{\mathbf{h}}\mathbf{w}}{s_E^2+\mathbf{w}^H R_{\mathbf{g}}\mathbf{w}} \\ &\text{subject to:} \quad |w_i|^2 \leq p_i, \quad i = 0,\ldots,N-1\end{aligned} \tag{8}$$

However, solving (8) is challenging owing to its non-convex character. Motivated by [18] and [19], our method is to first study a subproblem with the denominator of (8)'s objective function fixed, and then use one dimension search to find the solution. Moreover, the strict proof of this method is presented.

A. Subproblem With Fixed $s_E^2+\mathbf{w}^H R_{\mathbf{g}}\mathbf{w}$

Fixing $s_E^2+\mathbf{w}^H R_{\mathbf{g}}\mathbf{w}$ in (8) to a scalar t, then our problem transforms into

$$\begin{aligned}&\underset{\mathbf{w}}{\text{maximize:}} \quad \mathbf{w}^H R_{\mathbf{h}}\mathbf{w} \\ &\text{subject to:} \quad s_E^2+\mathbf{w}^H R_{\mathbf{g}}\mathbf{w} = t \\ &\qquad\qquad\quad |w_i|^2 \leq p_i, \quad i = 0,\ldots,N-1\end{aligned} \tag{9}$$

It is shown that the optimal objective value and optimal solution of (9) are influenced by t, which are defined as $f(t)$ and $\mathbf{w}^*(t)$ respectively. To indicate the relationship between the optimal value of (8) and (9), we define a new function $R(t) = (f(t)+s_D^2)/t$. Definitely, if t^* maximizes $R(t)$, then $R(t^*)$ is the optimal value of (8) and $\mathbf{w}^*(t^*)$ is also the optimal point of it.

However, (9) is also difficult to tackle because of the existence of equality constraint. In order to overcome this, we changes (9) into the following optimization problem,

$$\begin{aligned}&\underset{\mathbf{w}}{\text{maximize:}} \quad \mathbf{w}^H R_{\mathbf{h}}\mathbf{w} \\ &\text{subject to:} \quad s_E^2+\mathbf{w}^H R_{\mathbf{g}}\mathbf{w} \leq t \\ &\qquad\qquad\quad |w_i|^2 \leq p_i, \quad i = 0,\ldots,N-1\end{aligned} \tag{10}$$

Let's define the optimal value of (10) as $f_1(t)$ and the corresponding optimal point as $w_1^*(t)$. Let $R_1(t) = j(t)/t$ where $j(t) = f_1(t)+s_D^2$ and denote $R_1(t)$'s maximum point as t_1. Then we will have the conclusion stated in theorem 1 as follows.

Theorem 1: $w_1^*(t_1)$ is the optimal point of (8), and $R_1(t_1)$ is its optimal value.

Proof:

When $t = t^*$, $\mathbf{w}^*(t^*)$ is the optimal point of (9) and also is the feasible point of (10). So $f_1(t^*) \geq f(t^*)$. Then we have the relation below,

$$\max_t R_1(t) = R_1(t_1) \geq R_1(t^*) \quad R(t^*) = \max_t R(t) \tag{11}$$

In addition, when $t = t_1$, assume that $\left(\mathbf{w}_1^*(t_1)\right)^H R_{\mathbf{g}}\mathbf{w}_1^*(t_1)$ $+s_E^2 = t_2 < t_1$. Then we have $f_1(t_1) = f_1(t_2)$. Because $t_2 < t_1$, $R_1(t_2) > R_1(t_1)$, which contradicts with the fact that t_1 is the maximum point of $R_1(t)$. So we have

$$\left(\mathbf{w}_1^*(t_1)\right)^H R_{\mathbf{g}}\mathbf{w}_1^*(t_1) + s_E^2 = t_1. \tag{12}$$

Then in order to obtain $f_1(t_1)$ and $\mathbf{w}_1^*(t_1)$ we could focus on the following problem,

$$\begin{aligned}&\underset{\mathbf{w}}{\text{maximize:}} \quad \mathbf{w}^H R_{\mathbf{h}}\mathbf{w} \\ &\text{subject to:} \quad s_E^2+\mathbf{w}^H R_{\mathbf{g}}\mathbf{w} = t_1 \\ &\qquad\qquad\quad |w_i|^2 \leq p_i, \quad i = 0,\ldots,N-1\end{aligned} \tag{13}$$

Comparing (13) with (9), it is obvious that $f_1(t_1) = f(t_1)$ so we can got

$$\max_t R_1(t) = R_1(t_1) = R(t_1) \leq \max_t R(t) \quad R(t^*) \tag{14}$$

Combine (11) and (14) together, we have

$$\max_t R_1(t) = \max_t R(t). \tag{15}$$

According to (13) and (15), t_1 is also $R(t)$'s maximum point, and $\mathbf{w}_1^*(t_1)$ is also (8)'s optimal point. ■

In the light of Theorem 1, we can find out the maximum point of $R_1(t)$ through solving (10) instead of trying to calculate the complicate problem (8) directly. However (10) is also non-convex. In order to solve (10), we define a convex optimization problem as follows

$$\begin{aligned}&\underset{\mathbf{w}}{\text{maximize:}} \quad \mathrm{Re}(\mathbf{w}^H\mathbf{h}) \\ &\text{subject to:} \quad s_E^2+\mathbf{w}^H R_{\mathbf{g}}\mathbf{w} \leq t \\ &\qquad\qquad\quad |w_i|^2 \leq p_i, \quad i = 0,\ldots,N-1\end{aligned} \tag{16}$$

where $\mathrm{Re}(\mathbf{w}^H\mathbf{h})$ is the real part of $\mathbf{w}^H\mathbf{h}$. Then we have the following theorem.

Theorem 2: The optimal solution of problem (16) is also the optimal solution of (10).

Proof:

Assuming that $\mathbf{w}_R^*(t)$ is an optimal solution of (16), then we have

$$\mathrm{Re}^2((\mathbf{w}_R^*(t))^H\mathbf{h}) = (\mathbf{w}_R^*(t))^H R_{\mathbf{h}}(\mathbf{w}_R^*(t)) \tag{17}$$

Supposing that the former equation is invalid, then we have

$(\mathbf{w}_R^*(t))^H R_{\mathbf{h}}(\mathbf{w}_R^*(t)) > \mathrm{Re}^2((\mathbf{w}_R^*(t))^H\mathbf{h})$? . So we can find out $\nu \in [0,2\pi)$ make $\mathrm{Re}^2((\mathbf{w}_R^*(t)e^{j\nu})^H\mathbf{h}) = (\mathbf{w}_R^*(t)e^{j\nu})^H R_{\mathbf{h}}(\mathbf{w}_R^*(t)e^{j\nu})$ and $\mathrm{Re}((\mathbf{w}_R^*(t)e^{j\nu})^H\mathbf{h}) > 0$. So $\mathrm{Re}((\mathbf{w}_R^*(t)e^{j\nu})^H\mathbf{h}) > \mathrm{Re}((\mathbf{w}_R^*(t))^H\mathbf{h})$ which contradicts that $\mathbf{w}_R^*(t)$ is an optimal solution of (16). Then we have (17).

Definitely $\mathbf{w}_R^*(t)$ is also a feasible point of (10) so

$$(\mathbf{w}_R^*(t))^H R_{\mathbf{h}}(\mathbf{w}_R^*(t)) \le f_1(t). \tag{18}$$

Now considering the fact that $\exists\theta \in [0,2\pi)$ which can make $\mathrm{Re}^2((\mathbf{w}_1^*(t)e^{j\theta})^H\mathbf{h}) = (\mathbf{w}_1^*(t)e^{j\theta})^H R_{\mathbf{h}}(\mathbf{w}_1^*(t)e^{j\theta})$ and $\mathrm{Re}((\mathbf{w}_1^*(t)e^{j\theta})^H\mathbf{h}) \ge 0$. Here we can find that $\mathbf{w}_1^*(t)e^{j\theta}$ is still the optimal point of (10) and the feasible point of (16). So

$$\begin{aligned}\mathrm{Re}^2((\mathbf{w}_R^*(t))^H\mathbf{h}) &\ge \mathrm{Re}^2((\mathbf{w}_1^*(t)e^{j\theta})^H\mathbf{h}) \\ &= (\mathbf{w}_1^*(t)e^{j\theta})^H R_{\mathbf{h}}(\mathbf{w}_1^*(t)e^{j\theta}) = f_1(t)\end{aligned} \tag{19}$$

(17), (18), (19) together lead $(\mathbf{w}_R^*(t))^H R_{\mathbf{h}}(\mathbf{w}_R^*(t)) = f_1(t)$ which means $\mathbf{w}_R^*(t)$ is an optimal point of (10). ■

B. Search for the Optimal Solution

In order to obtain $R_1(t)$'s maximum point through which we could find out $w_1^*(t_1)$, let's state some properties of $f_1(t)$ and $R_1(t)$.

Theorem 3: $\varphi(t)$ is a concave function of t.

Proof:

The proof is similar to the steps performed in [19, section IV], and therefore is sketched.

We convert (16) into an equivalent real case as shown below,

$$\begin{aligned}&\underset{\mathrm{W}}{\text{maximize:}} \quad \mathrm{W}^T\mathrm{H} \\ &\text{subject to:} \quad \sigma_E^2 + \mathrm{W}^T\mathrm{P}_{\mathbf{g}}\mathrm{W} \le t \\ &\qquad\qquad\quad \mathrm{W}_i^2 + \mathrm{W}_{i+N}^2 \le p_i, \quad i = 0,\dots,N-1\end{aligned} \tag{20}$$

where $\mathrm{W} = [\mathrm{Re}^T(\mathbf{w}), \mathrm{Im}^T(\mathbf{w})]^T$, $\mathrm{P}_{\mathbf{g}} = [\mathrm{Re}(R_g), -\mathrm{Im}(R_g); \mathrm{Im}(R_g), \mathrm{Re}(R_g)]$. And $\mathrm{Im}(R_g)$ is the imaginary part of matrix R_g, W_i is the ith element of vector W.

Then considering the following convex optimization problem,

$$\begin{aligned}&\underset{\mathrm{W}}{\text{minimize:}} \quad -\mathrm{W}^T\mathrm{H} \\ &\text{subject to:} \quad \sigma_E^2 + \mathrm{W}^T\mathrm{P}_{\mathbf{g}}\mathrm{W} \le t \\ &\qquad\qquad\quad \mathrm{W}_i^2 + \mathrm{W}_{i+N}^2 \le p_i, \quad i = 0,\dots,N-1\end{aligned} \tag{21}$$

it is obvious that (21)'s optimal value is the opposite to (20)'s and they have the same optimal solutions. The Lagrangian of (21) is

$$\begin{aligned}L(\mathrm{W},\mu,\lambda) &= -\mathrm{W}^T\mathrm{H} + \mu(\sigma_E^2 + \mathrm{W}^T\mathrm{P}_{\mathbf{g}}\mathrm{W} - t) \\ &\quad + \sum_{i=0}^{N-1}\lambda_i(W_i^2 + W_{i+N}^2 - p_i) \\ &= \mathrm{W}^T\left(-\frac{\mathrm{H}\mathrm{H}^T}{\mathrm{W}^T\mathrm{H}} + \mu\mathrm{P}_{\mathbf{g}} + \begin{bmatrix} diag(\lambda) & 0_{N\times N} \\ 0_{N\times N} & diag(\lambda)\end{bmatrix}\right)\mathrm{W} \\ &\quad + \mu\sigma_E^2 - \mu t - \sum_{i=0}^{N-1}\lambda_i p_i\end{aligned} \tag{22}$$

Then the dual objective function is $G(\mu,\lambda) = \underset{\mathrm{W}}{\text{minimize}}\, L(\mathrm{W},\mu,\lambda)$ which reaches the minimum at W^* which is an optimal solution of (21). So

$$\begin{aligned}&G(\mu,\lambda) = \\ &(\mathrm{W}^*)^T\left(-\frac{\mathrm{H}\mathrm{H}^T}{(\mathrm{W}^*)^T\mathrm{H}} + \mu\mathrm{P}_{\mathbf{g}} + \begin{bmatrix} diag(\lambda) & 0_{N\times N} \\ 0_{N\times N} & diag(\lambda)\end{bmatrix}\right)\mathrm{W}^* \\ &+ \mu\sigma_E^2 - \mu t - \sum_{i=0}^{N-1}\lambda_i p_i.\end{aligned} \tag{23}$$

Through a similar way in [19], (21)'s dual problem can be written as

$$\begin{aligned}&\underset{\mu\lambda}{\text{maximize}} \quad \mu\sigma_E^2 - \mu t - \sum_{i=0}^{N-1}\lambda_i p_i \\ &\text{subject to } \mu \ge 0 \\ &\qquad \lambda \ge 0 \\ &\qquad -\frac{\mathrm{H}\mathrm{H}^T}{(\mathrm{W}^*)^T\mathrm{H}} + \mu\mathrm{P}_{\mathbf{g}} + \begin{bmatrix} diag(\lambda) & 0_{N\times N} \\ 0_{N\times N} & diag(\lambda)\end{bmatrix} \ge 0\end{aligned} \tag{24}$$

Then (20)'s duality can be got through writing out the opposite of (24):

$$\begin{aligned}&\underset{\mu\lambda}{\text{minimize}} \quad \mu t + \sum_{i=0}^{N-1}\lambda_i p_i - \mu\sigma_E^2 \\ &\text{subject to } \mu \ge 0 \\ &\qquad \lambda \ge 0 \\ &\qquad -\frac{\mathrm{H}\mathrm{H}^T}{(\mathrm{W}^*)^T\mathrm{H}} + \mu\mathrm{P}_{\mathbf{g}} + \begin{bmatrix} diag(\lambda) & 0_{N\times N} \\ 0_{N\times N} & diag(\lambda)\end{bmatrix} \ge 0\end{aligned} \tag{25}$$

Due to the convexity of (20), strong duality holds and the optimal value of (25) is $(\mathrm{W}^*)^T\mathrm{H}$. Definitely multiplied by $(\mathrm{W}^*)^T\mathrm{H}$, the optimal value of (25) becomes $((\mathrm{W}^*)^T\mathrm{H})^2$. From Theorem 2 we know that the square of optimal value of (20) is equal to (10)'s optimal value. From all this, the optimal value of the following problem is exactly $f_1(t)$:

$$\begin{aligned}&\underset{\mu\lambda}{\text{minimize}} \quad (\mathrm{W}^*)^T\mathrm{H}\mu t + \sum_{i=0}^{N-1}(\mathrm{W}^*)^T\mathrm{H}\lambda_i p_i - (\mathrm{W}^*)^T\mathrm{H}\mu\sigma_E^2 \\ &\text{subject to } \mu \ge 0 \\ &\qquad \lambda \ge 0 \\ &\qquad -\frac{\mathrm{H}\mathrm{H}^T}{(\mathrm{W}^*)^T\mathrm{H}} + \mu\mathrm{P}_{\mathbf{g}} + \begin{bmatrix} diag(\lambda) & 0_{N\times N} \\ 0_{N\times N} & diag(\lambda)\end{bmatrix} \ge 0\end{aligned} \tag{26}$$

As there must be $(\mathrm{W}^*)^T\mathrm{H} \ge 0$, by defining $\mu' = (\mathrm{W}^*)^T\mathrm{H}\mu$, $\lambda_i' = (\mathrm{W}^*)^T\mathrm{H}\lambda_i$ and $\lambda' = (\lambda_0,\dots,\lambda_{N-1})^T$, (26) can be expressed as,

$$
\begin{aligned}
&\underset{\mu\lambda}{\text{minimize}} \ \mu t + \sum_{i=0}^{N-1} \lambda_i p_i - \mu\sigma_E^2 \\
&\text{subject to } \mu \geq 0 \\
&\qquad \lambda \succeq 0 \\
&\qquad -\mathrm{H}\mathrm{H}^T + \mu \mathrm{P}_{\mathbf{g}} + \begin{bmatrix} diag(\lambda) & 0_{N\times N} \\ 0_{N\times N} & diag(\lambda) \end{bmatrix} \succeq 0
\end{aligned} \tag{27}
$$

Then $\varphi(t)$ can be expressed as

$$
\begin{aligned}
&\underset{\mu\lambda}{\text{minimize}} \ \mu t + \sum_{i=0}^{N-1} \lambda_i p_i - \mu\sigma_E^2 + \sigma_D^2 \\
&\text{subject to } \mu \geq 0 \\
&\qquad \lambda \succeq 0 \\
&\qquad -\mathrm{H}\mathrm{H}^T + \mu \mathrm{P}_{\mathbf{g}} + \begin{bmatrix} diag(\lambda) & 0_{N\times N} \\ 0_{N\times N} & diag(\lambda) \end{bmatrix} \succeq 0
\end{aligned} \tag{28}
$$

(28) is a point-wise minimum of a family of affine functions, so $\varphi(t)$ is concave[20, p.80]. ■

Theorem 4: $R_1(t)$ is a quasiconcave function of t.

Proof:

Suppose $p(x)$ is a concave function and $q(x)$ is a convex function, with $p(x) > 0$ and $q(x) > 0$ on a convex set C. We can easily get $f(x) = p(x)/q(x)$ is quasiconcave on C according to the theorem in [20, p.103]. Then at the base of Theorem 3, it can be concluded that $R_1(t)$ is quasiconcave for $\varphi(t) > 0$ is concave, $t > 0$ is affine (so convex). ■

Theorem 5: There's at most a single interval in $Dom(R_1(t))$ where $R_1(t)$ is invariant and any t belongs to this interval will be the maximum point of $R_1(t)$. Here $Dom(R_1(t))$ represents the domain of $R_1(t)$.

Proof:

First, let's consider the fact that $R_1(t) = C$ in an interval if and only if $\varphi(t) = Ct$. Then we just need to prove that there's only a single interval in $Dom(R_1(t))$ where $\varphi(t)$ is proportional to t.

Part I:

Assume $\varphi(t) = Ct$ on two separate interval $[a,b]$ and $[c,d]$ where $a < b < c < d$. Then we can get $\varphi(t)$ is no bigger than Ct on $[b,c]$ from (28). As $\varphi(t)$ is concave, $\varphi(\theta b + (1-\theta)c) \geq \theta\varphi(b) + (1-\theta)\varphi(c)$, $\theta \in [0,1]$ [20, p. 67] which means $\varphi(t)$ is no smaller than Ct on $[b,c]$. Consequently, we have $\varphi(t) = Ct$ on $[b,c]$. Therefore, there is only a single interval where $\varphi(t) = Ct$.

Part II:

Assume $\varphi(t) = Ct$ on $[a,b]$ and $\varphi(t) = C_1 t$ on $[c,d]$ with $a < b < c < d$ and $C \neq C_1$. Because of (28) we have $\varphi(t) = Ct < C_1 t$ on $[a,b]$. As $t > 0$, $C < C_1$. Similarly, $\varphi(t) = C_1 t < Ct$ on $[c,d]$. As $t > 0$, $C > C_1$. Then contradiction appears. As a result, there is at most a single straight line through the original which partly overlaps with $\varphi(t)$.

Combining the two parts above, we could easily get that there's at most a single interval in $Dom(R_1(t))$ where $R_1(t)$ is constant.

Suppose $\varphi(t) = Ct$ if and only if $t \in [a,b], a \leq b$. Then from (28) we know $\varphi(t_2) < Ct_2$ for $t_2 > b$. So

$$R_1(t_2) = \frac{\varphi(t_2)}{t_2} < \frac{Ct_2}{t_2}. \tag{29}$$

Through the similar way, for $t_1 < a$, there is

$$R_1(t_1) < \frac{Ct_2}{t_2}. \tag{30}$$

Through (29) and (30), we can conclude $R_1(t)$ achieves its maximum for $\forall t \in [a,b]$ as $R_1(t) = C$ on $[a,b]$. ■

Considering Theorem 3-5, we will find that the optimal point and maximum value of $R_1(t)$ can be efficiently got using Golden Section method which is one of the classic one dimensional search algorithms. Before using this algorithm, we should find an interval including the optimal point of $R_1(t)$. Denote $[t_{\min}, t_{\max}]$ as this interval. Definitely, $t_{\min}$ would be σ_E^2, and $t_{\max}$ would be the optimal value of the following problem,

$$
\begin{aligned}
&\underset{\mathbf{w}}{\text{maximize:}} \ \sigma_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w} \\
&\text{subject to:} \ |w_i|^2 \leq p_i, \quad i = 0, \ldots, N-1
\end{aligned}. \tag{31}
$$

The complete algorithm is summarized as follows.

Proposed Algorithm

Input: $\sigma_D^2, \sigma_E^2, p_i, \mathbf{g}, \mathbf{h}$.
begin
  initialize $t_{\min}, t_{\max}, len = t_{\max} - t_{\min}$.
  while $len > \varepsilon$, where ε is the threshold.
    $t_{left} = t_{\max} - 0.618(t_{\max} - t_{\min})$.
    $t_{right} = t_{\min} + 0.618(t_{\max} - t_{\min})$.
    calculate $R_1(t_{left}), R_1(t_{right})$.
    if $R_1(t_{left}) < R_1(t_{right})$.
      $t_{\min} = t_{left}$.
    else if $R_1(t_{left}) > R_1(t_{right})$

$t_{\max} = t_{right}$
else
$t_{\min} = t_{left}$.
$t_{\max} = t_{right}$.
end
$len = t_{\max} - t_{\min}$
end
$t_1 = (t_{\max} + t_{\min})/2$
take $t = t_1$ into (16) to find out $\mathbf{w}^*$.
calculate $C_S(\mathbf{w}^*) = \max\{\log\left(\sigma_E^2 R_1(t_1)/\sigma_D^2\right)/2, 0\}$.
end.
output: $\mathbf{w}^*$, $C_S(\mathbf{w}^*)$.

IV. ZF CONSTRAINT BASED SIMPLIFICATION

As discussed above, maximizing $C_S(\mathbf{w})$ under individual power constraint is a complicate problem. In this section, we simplify the problem using a zero-forcing (ZF) constraint on the receiving signal at the eavesdropper, which is equivalent to asking $\mathbf{w}^H R_{\mathbf{g}} \mathbf{w} = 0$. It is clear from (5) that the optimal $\mathbf{w}$ under ZF constraint is given by

$$\begin{aligned} &\underset{\mathbf{w}}{\text{maximize}}: \mathbf{w}^H R_{\mathbf{h}} \mathbf{w} \\ &\text{subject to}: \mathbf{w}^H R_{\mathbf{g}} \mathbf{w} = 0 \\ &\qquad |w_i|^2 \le p_i, \quad i = 0, \dots, N-1 \end{aligned} \tag{32}$$

From the analysis similar to that in Theorem 2, we have (32)'s optimal solution can be got through solving the convex problem

$$\begin{aligned} &\underset{\mathbf{w}}{\text{maximize}}: \mathrm{Re}(\mathbf{w}^H \mathbf{h}) \\ &\text{subject to}: \mathbf{w}^H \mathbf{g} = 0 \\ &\qquad |w_i|^2 \le p_i, \quad i = 0, \dots, N-1 \end{aligned} \tag{33}$$

Then the maximum secrecy rate under ZF constraint can be written as

$$\max\{\frac{1}{2}\log(1 + \frac{(\mathbf{w}_z^*)^H R_{\mathbf{h}} (\mathbf{w}_z^*)}{\sigma_D^2}), 0\} \tag{34}$$

where $\mathbf{w}_z^*$ is an optimal solution of (33). Note that this value is just sub-optimal, because of the existence of the ZF constraint.

V. EXTENSION TO MULTI-ANTENNA CASE

In this section, we will study a more complex scenario as an extension. In this scenario, relay nodes are equipped with multiple omni-directional antennas and other conditions are still the same as those in the former scenario. So in stage I, when the symbol x_S is transmitted, the received signal $y_{R,i}$ at R_i is

$$y_{R,i} = \sum_{j=0}^{N_i - 1} x_S l_{i,j} + n_{R,i} \tag{35}$$

where $l_{i,j}$ means the channel between the source and R_i's jth antenna, N_i means the number of R_i's antenna, $n_{R,i}$ is the noise at R_i with variance $\sigma_{R,i}^2$.

In stage II, when symbol $\tilde{x}_S$ is transmitted, the received signal y_D at D equals

$$y_D = \sum_{i=0}^{N-1}\sum_{j=0}^{N_i - 1} w_{i,j} h_{i,j} \tilde{x}_S + n_D \tag{36}$$

where $w_{i,j}$ $(i = 0, 1, \dots, N-1; j = 0, 1, \dots, N_i - 1)$ means the beamforming factor at R_i's jth antenna, $h_{i,j} \in \mathbb{C}$ is the channel between R_i's jth antenna and D, and n_D is the noise at D with variance σ_D^2. The received signal y_E at E can be shown as,

$$y_E = \sum_{i=0}^{N-1}\sum_{j=0}^{N_i - 1} w_{i,j} g_{i,j} \tilde{x}_S + n_E \tag{37}$$

where $g_{i,j} \in \mathbb{C}$ is the channel between R_i's jth antenna and E. Define $\mathbf{w}_i = [w_{i,0}, \dots, w_{i,N_i-1}]^T$, $\mathbf{w} = [\mathbf{w}_0^T, \dots, \mathbf{w}_{N-1}^T]^T$, $\mathbf{h}_i = [h_{i,0}, \dots, h_{i,N_i-1}]^T$, $\mathbf{h} = [\mathbf{h}_0^T, \dots, \mathbf{h}_{N-1}^T]^H$, $\mathbf{g}_i = [g_{i,0}, \dots, g_{i,N_i-1}]^T$, $\mathbf{g} = [\mathbf{g}_0^T, \dots, \mathbf{g}_{N-1}^T]^H$ and $R_{\mathbf{h}} = \mathbf{h}\mathbf{h}^H$, $R_{\mathbf{g}} = \mathbf{g}\mathbf{g}^H$. Then we can still express the SNR at D and E as $\Gamma_D = |\mathbf{h}^H \mathbf{w}|^2 / \sigma_D^2$ and $\Gamma_E = |\mathbf{g}^H \mathbf{w}|^2 / \sigma_E^2$ respectively. So the secrecy capacity for a given $\mathbf{w}$ can still be shown as (4).

In order to get the maximum achievable secrecy rate, in this section, the core optimization problem becomes

$$\begin{aligned} &\underset{\mathbf{w}}{\text{maximize}}: \frac{\sigma_D^2 + \mathbf{w}^H R_{\mathbf{h}} \mathbf{w}}{\sigma_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w}} \\ &\text{subject to}: |\mathbf{w}_i|^2 \le p_i, \quad i = 0, \dots, N-1 \end{aligned} \tag{38}$$

Here we still obtain a subproblem by fixing the denominator of (38)'s objective function as t and change the equality constraint of it by substituting "$\le$" for "$=$" to get another optimization problem. And then, we still denote $f(t)$ and $f_1(t)$ as the optimal value of the two optimization problem above respectively and define $\mathbf{w}^*(t)$, $R(t)$, t^*, $w_1^*(t)$, $R_1(t)$, $\varphi(t)$, t_1 through the same way in section III. It can be seen that in this section we could have theorems similar with those stated in section III. For these theorems, what need to be noted is that (8), (10), (16) should be substituted by their counterpart, i.e. (38), (39), (40) respectively.

$$\begin{aligned} \underset{\mathbf{w}}{\text{maximize:}} \quad & \mathbf{w}^H R_{\mathbf{h}} \mathbf{w} \\ \text{subject to:} \quad & s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w} ? \ t \\ & |\mathbf{w}_i|^2 \ ? \ p_i, \quad i = 0, \ldots, N-1 \end{aligned} \tag{39}$$

$$\begin{aligned} \underset{\mathbf{w}}{\text{maximize:}} \quad & \mathrm{Re}(\mathbf{w}^H \mathbf{h}) \\ \text{subject to:} \quad & s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w} ? \ t \\ & |\mathbf{w}_i|^2 \ ? \ p_i, \quad i = 0, \ldots, N-1 \end{aligned} \tag{40}$$

So the proposed algorithm can be easily generalized to tackle the multi-antenna case.

VI. Simulation Result

In this section, simulations are carried out to investigate the performance of the proposed algorithm. For simplicity, we use a one-dimensional system model, as illustrated in Fig. 2, where the source, relays, destination and eavesdropper are along a horizontal line. What's more, because the source-relay distance and the distances between relays are very small compared to the source-destination distance and relay-destination distance, the source-destination distance and the distances between different relays and the destination can be considered as the same. So are the source-eavesdropper distance and the distances between the different relays and eavesdropper. To emphasize the effect of distance, a simple line-of-sight channel model which contains the pass loss and a random phase is used. Generally, we can express the channels as $h = d^{-c/2} e^{jq}$ where d is the distance, c is the path loss exponent chosen as 3.5 and random phase q is uniformly distributed over $[0, 2p)$. The number of relays is set to 6, i.e. $N = 6$ and the eavesdropper are fixed at 60 m. For individual power constraints, we assume each relay has the same power budget: $p_i = p_T / N$ where p_T represents the total power constraint of the DF based system. And the noise power $s_D^2 = -55\mathrm{dBm}$ and $s_E^2 = -65\mathrm{dBm}$.

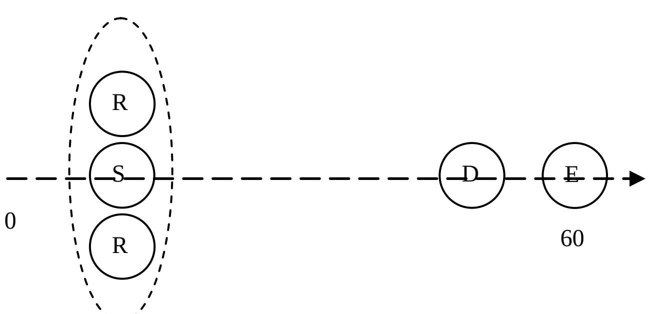


Figure 2. Model used for simulation

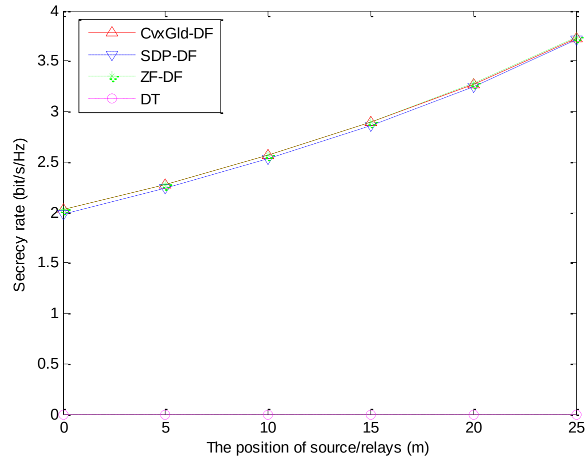


Figure 3. Secrecy rate versus the position of source/relays.

We will examine the maximum achievable secrecy rate of the DF based system calculated by the algorithm proposed in section III (labelled as CvxGld-DF) and the maximum secrecy rate under ZF constraint obtained by the simplified method discussed in section IV (labelled as ZF-DF). For comparison, we also examine the performance of direct transmission (DT) scheme and the SDP algorithm proposed in [16] (labelled as SDP-DF).

Firstly, we fix the position of destination at 50m and move the source/relays from 0 m to 25m. The transmit power is set as 10mdB for DT scheme. And for DF scheme p_T is also set as 10dBm. We can observe from Figure 3 that the maximum achievable secrecy rate always stays at 0 for DT. This is because the source-destination channel is always worse than the source-eavesdropper channel. And for all DF based algorithms, the curves coincided. Maximum secrecy rates got by three DF-based algorithms increase when relays move to the destination. This can be explained by the fact that even through the relay-destination channel and relay-eavesdropper channel both become better when the relays move from 0 to 25, the improving trend of the former is more remarkable.

Then we fix the source/relay location at 25m and move the destination from 40m to 100m with all other parameters unchanged. Figure 4 illustrate that there is a gap between the secrecy rate performances of the CvxGld-DF algorithm in this paper and the SDP-DF algorithm in [16] when the destination located at 90m and 100m. This means that we cannot get the

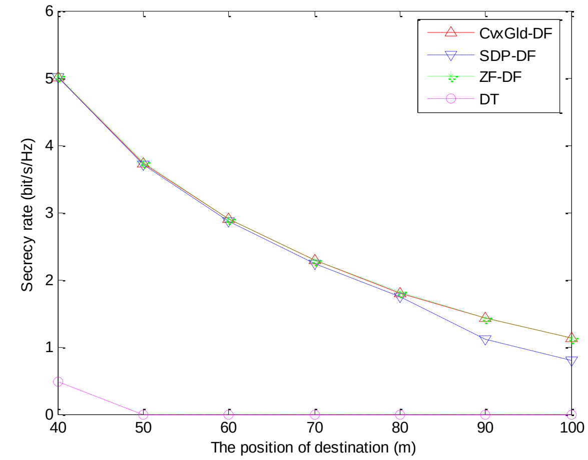


Figure 4. Secrecy rate versus the position of destiantion.

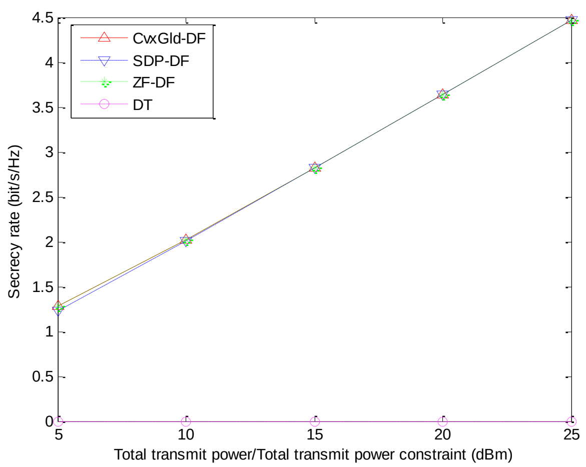


Figure 5. Secrecy rate versus total trasmit power/total transmit power constraint.

optimal beamforming vector through the SDP-DF algorithm in [16] sometimes. This problem comes from the reason that the rank of the optimal solution of the SDP optimization problem in [16] may be larger than one under some situation.

In Figure 5, we fix the destination and source/relays at 50m and 0m respectively and let p_T varies from 5dBm to 25dBm. Correspondingly, the transmit power of DT scheme also changes from 5dBm to 25dBm. Figure 5 shows that similar secrecy rate performances appear for all DF based algorithms with the increase of p_T. It is easy to understand that the secrecy rate performances become better when more power is allowed for transmitting. While for DT scheme, the maximum secrecy rate always stays at 0 even we use more power to transmit signals. This reveals that just enhancing transmit power is meaningless when Wyner's condition is not met for DT scheme.

In Figure 3, Figure 4 and Figure 5, there exists an interesting result that ZF-DF can always achieve nearly optimal performance. Thus we conjecture that, while we want to reach the maximum secrecy rate of an DF-based system under individual power constraint, the ZF constraint may be a good choice to simplify the optimization problem without leading much degradation. However, quantifying the impact of the ZF constraint remains an open problem.

VII. Conclusions

In this paper, we have considered a DF-based cooperative protocol to improve the physical layer security with one eavesdropper. Our attention is focused on the design of beamforming weight of each cooperating node which is one antenna equipped to find out the maximum secrecy rate. However our problem formulation is different from others because we assume a more practical scenario where the beamforming vector is subject to individual power constraints and noise power at different node is different. Under the assistance of perfect CSI, we have solved the optimal problem by combining convex optimization and one-dimensional search together and rigorous proof is presented for the correctness of our method. Further more, a simplified problem with zero-forcing (ZF) constraint and generalization to cope with the more complicate multi-antenna case are considered.

References

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

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, Jul. 1978.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels", *IEEE Trans. Inf. Theory*, vol. 54, no. 6, Jun. 2008.

[5] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, Oct. 2008.

[6] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[7] R. Negi and S. Goelm, "Secret communication using artificial noise," in *Proc. IEEE Vehicular Tech. Conf.*, Dallas, TX, Sep. 2005, vol. 3, pp. 1906–1910.

[8] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 2547–2553, Jun. 2009.

[9] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, Aug. 2007. [Online]. Available: http://arxiv.org/abs/0708.4219, submitted for publication.

[10] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, Oct. 2007 [Online]. Available: http://aps.arxiv.org/abs/0710.1920, submitted for publication.

[11] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155

[12] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Conf. Information Sciences Systems*, Baltimore, MD, Mar. 2007, pp. 905–910

[13] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 2466–2470

[14] J. Li, A. P. Petropulu, and S. Weber, "Optimal cooperative relaying schemes for improving wireless physical layer security," Jan. 2010 [Online]. Available: http://arxiv.org/abs/1001.1389, submitted for publication

[15] L. Dong, Z. Han, A. 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.

[16] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," Dec. 2009 [Online]. Available: http://arxiv.org/abs/0910.4132,submitted for publication

[17] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," Proc. *46th Annu. Allerton Conf. Commun., Control, Computing.*, Monticello, IL, Sep.-Oct. 2008.

[18] A.Wiesel, Y. C. Eldar, and A. Beck, "Maximum likelihood estimation in linear models with a Gaussian model matrix," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 292–295, May 2006.

[19] G. Zheng, L. Choo, and K. Wong, "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317—1322, Mar. 2011.

[20] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

Hui Ma received the B.S. degree in electrical engineering from Qufu Normal University, Rizhao, China, in 2010. Currently, he is working toward the M.S. degree in communication and information system in the School of Information Science and Engineering, Shandong University.

His research interests include physical layer security in multiple-input-multiple-output communication system and collaborative communication system.

Piming Ma received the B.S. degree in electrical engineering, the M.S. degree in signal processing and the Ph.D. degree in communications and information system from Shandong University, Jinan, China, in 1992, 1997 and 2005, respectively.

She is currently an Associate Professor in the School of Information Science and Engineering, Shandong University, Jinan, China. From 2008 to 2009, she was a Postdoctoral Fellow at the Ultra Wide Band Wireless Communications Research Center, Inha University, Nam-gu, Incheon, South Korea. She has published more than 20 technical (journal and conference) papers. Her search interests include LDPC codes, signal processing for wireless communications, software radio, physical layer security.