Distributed Beamforming for Physical-Layer Security of Two-Way Relay Networks

Hui-Ming Wang, *Member, IEEE*, Qinye Yin, and Xiang-Gen Xia, *Fellow, IEEE*

***Abstract*—In this paper, we address the security of a two-way relay network in the presence of an eavesdropper, where each node is only equipped with single antenna. We propose two-phase *distributed analog network coding*, or *distributed beamforming* and power allocation to enhance the secrecy sum rate of the data exchange. In the first phase, the two terminals broadcast their information data simultaneously to all the relay nodes. In the second phase, three different security schemes are proposed: optimal beamforming, null-space beamforming, and artificial noise beamforming. In the first scheme, the objective is to achieve the maximum secrecy sum rate of the two terminals. Mathematically, the objective function is difficult to optimize. In the second scheme, we maximize the total information exchanged while we eliminate the information leakage completely, subject to the total transmission power constraint. We show that the problem has a unique and global optimum, which can be solved using bisection method. When the instantaneous channel state information of the eavesdropper is not available, we propose an artificial noise beamforming in the third scheme. We minimize the information transmission power so that the artificial noise power is maximized to eliminate information leakage, under the constraints of quality of service (QoS) required by terminals. It is a second-order convex cone programming (SOCP) problem, thus can be efficiently solved using interior point methods. Numerical results are provided and analyzed to show the properties and efficiency of the proposed designs.**

***Index Terms*—Analog network coding, distributed beamforming, physical layer security, second-order cone programming, secrecy rate, two-way relay networks.**

Manuscript received February 13, 2011; revised September 21, 2011 and February 14, 2012; accepted March 08, 2012. Date of publication March 20, 2012; date of current version June 12, 2012. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Josep Vidal. The work of H.-M. Wang and Q. Yin was supported in part by the National Natural Science Foundation of China under Grants 61102081 and 61071125, the Science Foundation for Innovation Research Group of China under Grant 60921003, the Specialized Research Fund for the Doctoral Program of Higher Education of China under Grant 20110201120013, and the Natural Science Fundamental Research Plan of Shaanxi Province under Grant 2011JQ8022. The work of X.-G. Xia was supported in part by the National Science Foundation (NSF) under Grant CCF-0964500, the Air Force Office of Scientific Research (AFOSR) under Grant FA9550-12-1-0055, and the World Class University (WCU) Program, National Research Foundation, South Korea.

H.-M. Wang and Q. Yin are with the School of Electronic and Information Engineering, Ministry of Education Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an 710049, P. R. China (e-mail: xjbswhm@gmail.com).

X.-G. Xia is with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA, and also with the Chonbuk National University, Jeonju, South Korea (e-mail: xxia@ee.udel.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSP.2012.2191543

I. Introduction

THE ISSUE of security is a fundamental problem in data communications. In wireless communications, the security issue becomes more challenging due to the fundamental characteristics of the *openness* of wireless medium. Any receiver located in the cover range of the transmitter can obtain the transmitted signal. In this context, physical layer security, or information-theoretic security, has attracted considerable attention recently [5]–[27], [33]–[41].

The information-theoretic security was first introduced by Shannon [1]. Wyner introduced the degraded wiretap channel model in [2] where a wire-tapper wants to access a degraded version of the intended receiver's signal, and defined the notion of *secrecy capacity* to measure the maximum transmission rate from source to the legitimate destination while making the amount of information leaked to the eavesdroppers negligible. The idea of [2] is generalized to nondegraded version of wiretap channel in [3] and Gaussian degraded wiretap channel in [4]. Physical layer security of fading channels is investigated very recently, in [5]–[7], for example.

Information-theoretic security of *multiple-antenna* systems has attracted a lot of attention recently [8]–[16]. Secure transmissions are investigated when the channel from source to the legitimate destination is single-input multiple-output (SIMO) channel [8], multiple-input single-output (MISO) channel [9]–[11], and multiple-input multiple-output (MIMO) channel [12]–[16]. It is worth mention that in [11], it is shown when the channel gains are fixed and known to all the transceivers, the optimal transmission scheme for Gaussian codebook that maximizes the secrecy rate of Gaussian MISO channels is *beamforming* along the direction of the generalized eigenvector corresponding to the maximum generalized eigenvalue of the matrix pencil of main channel and wiretap channel matrices. On the other hand, a lot of *multiuser* scenarios are considered for physical layer security transmission, such as broadcast channels [20]–[25], multiple access channels [26]–[28], cooperative relay channels [32]–[40], and two-way channels [27], [41], [42].

The secrecy capacities in the above works are almost all derived under the assumption that the eavesdropper's channel state information (CSI) is known at the transmitter. Clearly this assumption is sometimes impractical. In [17] and [18], a so-called *artificial noise* scheme is proposed, where interference signal is transmitted along with information signal to confuse the potential eavesdropper. This idea is generalized to MIMO case in [18] and [19]. The artificial noise signal is carefully designed such that the intended user will not be degraded. Interestingly, it is shown in [11] that the artificial noise scheme in MISO wiretap channel is asymptotically near-optimal in high SNR regime in

the sense that even without the eavesdropper's CSI, the achievable secrecy rate of this scheme only has a *fixed* loss compared to that of the case when eavesdropper's CSI is available.

In this paper, we investigate the physical layer security of bidirectional (two-way) information transmission of two terminals with the help of multiple relay nodes in the presence of an eavesdropper. We propose a two-phase complex-weighted and forward relay scheme. In the first phase, the two terminals broadcast their information data simultaneously to all the relay nodes. In the second phase, each relay node retransmits a complex-weighted version of the received signal in the first phase. Since each terminal knows the signal it transmitted in the first phase, it can subtract the backward self-interference and thus obtain the desired information data from the other terminal to complete one round of data exchange [29]–[31]. This can also be considered as an *analog network coding* scheme [29]–[31], or, a *distributed beamforming scheme based on amplify-and-forward protocol*. Note that information leakage to the potential eavesdropper happens in both of the two phases due to the openness of the wireless medium. We use the *secrecy sum rate* as the metric of security, which is the rate difference between the legitimate information exchange and the information leakage to the eavesdropper. Our goal is to design the weight coefficients and allocate proper transmit power to enhance the *security* of the data exchange. To do these, we consider three different approaches:

1) when all CSI is available, we aim to achieve the maximum achievable secrecy sum rate of the two terminals, subject to the total power constraint consumed by terminals and relay nodes;
2) with full eavesdropper's CSI, we aim to maximize the sum rate of the data exchange of the two terminals while prohibiting the information leakage to the eavesdropper in the second phase, subject to the total power constraint consumed by terminals and relay nodes;
3) with no eavesdropper's CSI, we adopt the artificial noise scheme to minimize the power allocated by information signal transmission at relays to achieve the required quality of service (QoS) at the two terminals, so that the power available for artificial noise can be as large as possible to confuse the potential eavesdropper, subject to the available power constraint of the relay nodes.

The first approach is the optimal one in the sense that the maximum achievable secrecy sum rate is achieved. However, it is shown that the optimization problem is mathematically difficult to solve. In the second approach, we have shown that although we can not get a closed-form solution, this problem has a unique optimal point, which can be obtained by some iterative algorithm such as Newton's method. The third approach can be mathematically transformed into a second-order convex cone programming (SOCP) problem [47], so that efficient interior point methods can be exploited to get the numerical global optimum.

A. Related Work

Exploiting relay nodes to improve physical layer security has been attracted increasing interest very lately, in both information-theoretic [33]–[36], and signal processing point of view [37]–[39]. Single relay cooperation schemes are proposed in [33]–[35]. When multiple distributed cooperative nodes are available to help the transmitter, relay beamforming designs[1] trying to maximize the achievable secrecy rate are studied under both decode-and-forward (DF) protocol [37], [39] and amplify-and-forward (AF) protocol [38], [39].

All the above mentioned literatures [33]–[39] considered *one-way* relay transmission. Our work in this paper investigates the physical layer security for two-way relay network in a signal processing point of view. When studying two-way transmission, it is a multiuser case and secrecy rate region should be considered. The optimization will be more difficult. The literature on security issue for two-way relay network is still sparse [27], [41], [42]. Our work is different from these works in the following aspects: 1) [27] investigates the problem in an information-theoretic point of view, and only one relay is used so that relay beamforming is not involved; 2) [41] considers the case when the relay acts as an eavesdropper while in our scheme the relay nodes are helpers; 3) [42] considers MIMO two-way secure transmission with relays equipped with colocated multiple antennas. Although the problem studied in [42] is more general than that we study in this paper, neither analytical result nor optimum solution is given there. In this paper, however, not only systematic distributed beamforming schemes are proposed, but also the solutions are shown to be unique and global optimum using convex optimization theory.

B. Organization and Notations

The organization of the paper is as follows. In Section II, we present the system model of the two-way wiretap channel with multiple relay nodes and one eavesdropper. From Section IIIto Section V, three different approaches mentioned above are investigated, respectively. In Section VI, simulations are taken to illustrate the performance of these scheme, and finally, Section VII concludes the paper.

We use upper- and lowercase bold-faced letters to denote matrices and column vectors, respectively. Superscripts $(\cdot)^*$, $(\cdot)^T$, $(\cdot)^H$, and $(\cdot)^{-1}$ represent conjugate, transpose, Hermitian, and inverse, respectively. $\boldsymbol{I}$ is the identity matrix. $\mathrm{diag}(\cdot)$ is diagonal matrix with main diagonal $(\cdot)$. $\det(\cdot)$ is the determinant of matrix $(\cdot)$. $|\cdot|$ and $\|\cdot\|$ are the absolute value of a complex scalar and Frobenius norm of a vector/matrix, respectively. $E(\cdot)$ is the mathematical expectation of a random variable. $\mathfrak{Re}(\cdot)$ is the real part of a complex.

II. System Model

We consider a wireless network in which two legitimate terminal nodes $\mathbb{T}_m$, $m = 1, 2$ wish to exchange information under the existence of an eavesdropper $\mathbb{E}$, with the help of N distributed relay nodes $\mathbb{R}_n$, $n = 1, 2, \cdots, N$, as depicted in Fig. 1. The eavesdropper is passive and the goal is to get the source information from terminal nodes $\mathbb{T}_1$ and $\mathbb{T}_2$. Each node in the whole network is only equipped with a single antenna. All the terminal and relay nodes are subject to the half-duplex constraint, i.e., they cannot transmit and receive simultaneously. Denote the quasi-stationary flat-fading channel between $\mathbb{T}_1$ and the nth relay $\mathbb{R}_n$ as $f_{R,n}$, and the channel between $\mathbb{R}_n$ and $\mathbb{T}_2$ as $g_{R,n}$, $n = 1, 2, \cdots, N$. Time-division duplex (TDD) mode is

[1]Distributed beamforming attracted much recent attention in relay networks, see [43]–[46], for example.

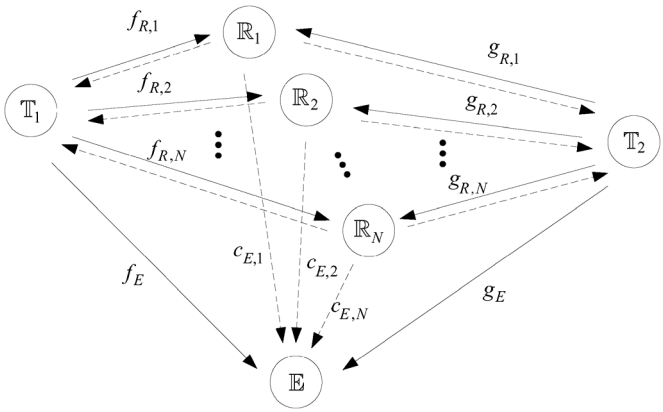


Fig. 1. System model of the security transmission in two-way relay network, where the solid lines are the transmission in the first phase and the dash lines are the transmission in the second phase.

adopted so that the channels are reciprocal, namely, the channel from the terminal nodes $\mathbb{T}_m$ to the relay node $\mathbb{R}_n$ is equal to that from $\mathbb{R}_n$ to $\mathbb{T}_m$. Further denote the channel between $\mathbb{T}_1$ and $\mathbb{E}$ as f_E, the channel between $\mathbb{T}_2$ and $\mathbb{E}$ as g_E, and the channel between relay nodes $\mathbb{R}_n$ and $\mathbb{E}$ as $c_{E,n}$, $n = 1, 2, \cdots, N$. We assume the channel coefficients $f_{R,n}, g_{R,n}, f_E, g_E, c_{E,n}$, $m = 1, 2$, $n = 1, 2, \cdots, N$ are all independent complex Gaussian random variables with zero-mean and unit-variance, and keep constant within the numbers of time slots considered.

Due to shadowing or too large distance, there is no direct connection between $\mathbb{T}_1$ and $\mathbb{T}_2$. Therefore, the relay nodes play two roles:

1) help to exchange information of two terminals $\mathbb{T}_1$ and $\mathbb{T}_2$ to guarantee reliable communications;
2) help to prevent the information leakage to the eavesdropper to enhance security.

To do these, we propose a two-phase complex-weighted-and-forward protocol for the bidirectional transmission. During the first phase, both terminals simultaneously transmit their data to the relays. The signals received at the relays can be represented, in vector form, as

$$\boldsymbol{y}_R = \sqrt{P_1}\boldsymbol{f}_R s_1 + \sqrt{P_2}\boldsymbol{g}_R s_2 + \boldsymbol{n}_R \tag{1}$$

where $\boldsymbol{y}_R$ is the $N \times 1$ received signal vector with the nth element $y_{R,n}$, $P_1(P_2)$ and $s_1(s_2)$ are the transmit power and information symbol of $\mathbb{T}_1(\mathbb{T}_2)$, respectively, $\boldsymbol{n}_R$ is the additive noise at the relay nodes, and

$$\boldsymbol{f}_R \triangleq [f_{R,1}, f_{R,2}, \cdots, f_{R,N}]^T,\ \boldsymbol{g}_R \triangleq [g_{R,1}, g_{R,2}, \cdots, g_{R,N}]^T \tag{2}$$

are the channel coefficients vectors between the relay nodes and the corresponding terminals.

Concurrently, the transmitted signals will also be received by the eavesdropper, if the eavesdropper lies in the cover range of both the terminals, which can be written as

$$y_E^{(1)} = \sqrt{P_1} f_E s_1 + \sqrt{P_2} g_E s_2 + n_E^{(1)} \tag{3}$$

where $n_E^{(1)}$ is the additive noise at the eavesdropper.

In the second phase, the nth relay multiplies its received signal by a complex weight ω_n^* and then retransmit the so-obtained signal $x_{R,n}$. Stack the transmitted signals into a column vector $\boldsymbol{x}_R$, which can be written as

$$\boldsymbol{x}_R = \boldsymbol{W}\boldsymbol{y}_R \tag{4}$$

where $\boldsymbol{W}$ is the weight matrix in the form of $\boldsymbol{W} = \mathrm{diag}([\omega_1^*, \omega_2^*, \cdots, \omega_N^*])$. Denote the received signal at $\mathbb{T}_1$ and $\mathbb{T}_2$ as y_{T_1}, y_{T_2}, which can be easily obtained as

$$\begin{aligned} y_{T_1} &= \boldsymbol{f}_R^T \boldsymbol{x}_R + n_{T_1} \\ &= \sqrt{P_1}\boldsymbol{f}_R^T \boldsymbol{W}\boldsymbol{f}_R s_1 + \sqrt{P_2}\boldsymbol{f}_R^T \boldsymbol{W}\boldsymbol{g}_R s_2 \\ &\quad + \boldsymbol{f}_R^T \boldsymbol{W}\boldsymbol{n}_R + n_{T_1}, \end{aligned} \tag{5}$$

$$\begin{aligned} y_{T_2} &= \boldsymbol{g}_R^T \boldsymbol{x}_R + n_{T_2} \\ &= \sqrt{P_1}\boldsymbol{g}_R^T \boldsymbol{W}\boldsymbol{f}_R s_1 + \sqrt{P_2}\boldsymbol{g}_R^T \boldsymbol{W}\boldsymbol{g}_R s_2 \\ &\quad + \boldsymbol{g}_R^T \boldsymbol{W}\boldsymbol{n}_R + n_{T_2} \end{aligned} \tag{6}$$

and similarly, the received signal at the eavesdropper during the second phase is

$$\begin{aligned} y_E^{(2)} &= \boldsymbol{c}_E^T \boldsymbol{x}_R + n_E^{(2)} \\ &= \sqrt{P_1}\boldsymbol{c}_E^T \boldsymbol{W}\boldsymbol{f}_R s_1 + \sqrt{P_2}\boldsymbol{c}_E^T \boldsymbol{W}\boldsymbol{g}_R s_2 \\ &\quad + \boldsymbol{c}_E^T \boldsymbol{W}\boldsymbol{n}_R + n_E^{(2)} \end{aligned} \tag{7}$$

where $\boldsymbol{c}_E \triangleq [c_{E,1}, c_{E,2}, \cdots, c_{E,N}]^T$ and $n_{T_1}, n_{T_2}, n_E^{(2)}$ are additive noise at $\mathbb{T}_1$, $\mathbb{T}_2$, and $\mathbb{E}$ during the second phase, respectively.

The two-phase information exchange can be considered as an *analog network coding* [29]–[31]. Note that the first term in (5) is the *backward self-interference* of s_1, and similar is the second term in (6). We assume that each terminal knows both the channels associated itself with the relay nodes and the weighted coefficients matrix $\boldsymbol{W}$, then similar to [29]–[31], it can subtract the backward self-interference from itself and only obtain the desired information from the other one. After this operation, (5) and (6) become

$$y_{T_1} = \sqrt{P_2}\boldsymbol{w}^H \boldsymbol{F}_R \boldsymbol{g}_R s_2 + \bar{n}_{T_1} = \sqrt{P_2}\boldsymbol{w}^H \boldsymbol{a}_{fg} s_2 + \bar{n}_{T_1} \tag{8}$$

$$y_{T_2} = \sqrt{P_1}\boldsymbol{w}^H \boldsymbol{G}_R \boldsymbol{f}_R s_1 + \bar{n}_{T_2} = \sqrt{P_1}\boldsymbol{w}^H \boldsymbol{a}_{fg} s_2 + \bar{n}_{T_2} \tag{9}$$

and (7) can be rewritten as

$$\begin{aligned} y_E^{(2)} &= \sqrt{P_1}\boldsymbol{w}^H \boldsymbol{C}_E \boldsymbol{f}_R s_1 + \sqrt{P_2}\boldsymbol{w}^H \boldsymbol{C}_E \boldsymbol{g}_R s_2 + \bar{n}_E^{(2)} \\ &= \sqrt{P_1}\boldsymbol{w}^H \boldsymbol{a}_{cf} s_1 + \sqrt{P_2}\boldsymbol{w}^H \boldsymbol{a}_{cg} s_2 + \bar{n}_E^{(2)} \end{aligned} \tag{10}$$

by using the equation $\boldsymbol{a}^H \mathrm{diag}(\boldsymbol{b}) = \boldsymbol{b}^H \mathrm{diag}(\boldsymbol{a})$, where $\boldsymbol{w} \triangleq [\omega_1, \omega_2, \cdots, \omega_N]^T$, $\boldsymbol{F}_R \triangleq \mathrm{diag}(\boldsymbol{f}_R)$, $\boldsymbol{G}_R \triangleq \mathrm{diag}(\boldsymbol{g}_R)$, $\boldsymbol{C}_E \triangleq \mathrm{diag}(\boldsymbol{c}_E)$, $\boldsymbol{a}_{fg} \triangleq \boldsymbol{F}_R \boldsymbol{g}_R = \boldsymbol{G}_R \boldsymbol{f}_R$, $\boldsymbol{a}_{cf} \triangleq \boldsymbol{C}_E \boldsymbol{f}_R$, $\boldsymbol{a}_{cg} \triangleq \boldsymbol{C}_E \boldsymbol{g}_R$, $\bar{n}_{T_1} \triangleq \boldsymbol{w}^H \boldsymbol{F}_R \boldsymbol{n}_R + n_{T_1}$, $\bar{n}_{T_2} \triangleq \boldsymbol{w}^H \boldsymbol{G}_R \boldsymbol{n}_R + n_{T_2}$, and $\bar{n}_E^{(2)} \triangleq \boldsymbol{w}^H \boldsymbol{C}_E \boldsymbol{n}_R + n_E^{(2)}$, respectively. Combining (3) and (10) yields the receive model of the eavesdropper in the whole procedure as

$$\boldsymbol{y}_E = \boldsymbol{H}_E \boldsymbol{s} + \boldsymbol{n}_E \tag{11}$$

where

$$\boldsymbol{y}_E = \begin{bmatrix} y_E^{(1)} \\ y_E^{(2)} \end{bmatrix}, \quad \boldsymbol{H}_E = \begin{bmatrix} \sqrt{P_1} f_E & \sqrt{P_2} g_E \\ \sqrt{P_1}\boldsymbol{w}^H \boldsymbol{a}_{cf} & \sqrt{P_2}\boldsymbol{w}^H \boldsymbol{a}_{cg} \end{bmatrix}$$
$$\boldsymbol{n}_E = \begin{bmatrix} n_E^{(1)} \\ \boldsymbol{w}^H \boldsymbol{C}_E \boldsymbol{n}_R + n_E^{(2)} \end{bmatrix} \tag{12}$$

and $\boldsymbol{s} = [s_1, s_2]^T$.

We assume that all the noise terms n_{T_1}, n_{T_2}, $n_E^{(1)}$, $n_E^{(2)}$, and $\boldsymbol{n}_R$ are zero-mean and time-spatially white independent complex Gaussian random variables with variance σ^2. Then $\bar{n}_{T_1}, \bar{n}_{T_2}$ are both zero-mean Gaussian variables with covariances $Q_{T_1} = \sigma^2(1+\boldsymbol{w}^H \boldsymbol{R}_{ff}\boldsymbol{w})$, and $Q_{T_2} = \sigma^2(1+\boldsymbol{w}^H \boldsymbol{R}_{gg}\boldsymbol{w})$, respectively, and $\boldsymbol{n}_E$ is zero-mean Gaussian vector with covariance matrix

$$\boldsymbol{Q}_E = \begin{bmatrix} \sigma^2 & 0 \\ 0 & \sigma^2(1+\boldsymbol{w}^H \boldsymbol{R}_{cc}\boldsymbol{w}) \end{bmatrix} \tag{13}$$

where $\boldsymbol{R}_{ff} \triangleq \boldsymbol{F}_R \boldsymbol{F}_R^H$, $\boldsymbol{R}_{gg} \triangleq \boldsymbol{G}_R \boldsymbol{G}_R^H$, and $\boldsymbol{R}_{cc} \triangleq \boldsymbol{C}_E \boldsymbol{C}_E^H$. We also have $E\{|s_m|^2\} = 1$ since we have already defined the transmitted power of $\mathbb{T}_m$ as P_m. We immediately have the following observations:

1) for the legitimate terminals $\mathbb{T}_1$ and $\mathbb{T}_2$, the equivalent models are two SISO systems as described in (8) and (9), respectively;
2) for the eavesdropper $\mathbb{E}$, each transmission phase grants it an opportunity to get the information. This implies the optimal strategy the eavesdropper should take is to combine the information received over the two phases to create an equivalent MIMO system, as described in (11).

III. Optimal Beamforming Scheme: Maximum Secrecy Sum Rate

To consider the security issue of the bidirectional transmission of two terminals, we should adopt the achievable secrecy rate region as the metric and assume all the channel matrices, including eavesdropper's CSI, are fixed and known to all the transceivers. In [26], the authors defined two secrecy constraints suitable for a *multiple user* system: One is *individual* and the other is *collective* secrecy constraints. The former one is utilized in a scenario when the multiple source terminals do not have to trust each other, while the latter applies when the source terminals trust each other. Obviously, as described in Section II, in the system under consideration we should adopt the notion of collective secrecy constraint. In [27], it was shown that using Gaussian inputs and stochastic encoders, the achievable *secrecy rate region* for the two-way wiretap channel is given by

$$\sum_{n\in\mathcal{S}} R_n^s \le \left[\sum_{n\in\mathcal{S}} I(y_n; s_n) - I(\boldsymbol{y}_E; \boldsymbol{s}_{\mathcal{S}})\right]^+, \quad \exists \mathcal{S} \subseteq \mathcal{N} \tag{14}$$

and the achievable *secrecy sum rate* is

$$R_{\text{sum}}^s \triangleq [I(y_{T_1}; s_2) + I(y_{T_2}; s_1) - I(\boldsymbol{y}_E; s_1, s_2)]^+ \tag{15}$$

where $\mathcal{N} = \{1, 2\}$, $[a]^+ = \max(0, a)$. In the first scheme, we hope to achieve the maximum secrecy sum rate, which is defined as $R_{max} \triangleq \max R_{\text{sum}}^s$.

The information rate achieved by each legitimate terminal over the two phases is, respectively,

$$R_{T_1} \triangleq I(y_{T_1}; s_2) = \frac{1}{2}\log\left(1 + \frac{P_2 \boldsymbol{w}^H \boldsymbol{R}_{fg} \boldsymbol{w}}{\sigma^2(1+\boldsymbol{w}^H \boldsymbol{R}_{ff}\boldsymbol{w})}\right) \tag{16}$$
$$R_{T_2} \triangleq I(y_{T_2}; s_1) = \frac{1}{2}\log\left(1 + \frac{P_1 \boldsymbol{w}^H \boldsymbol{R}_{fg} \boldsymbol{w}}{\sigma^2(1+\boldsymbol{w}^H \boldsymbol{R}_{gg}\boldsymbol{w})}\right) \tag{17}$$

where $\boldsymbol{R}_{fg} \triangleq \boldsymbol{a}_{fg}\boldsymbol{a}_{fg}^H$. On the other hand, the information rate leaked to the eavesdropper can be obtained from the sum rate of the MIMO system (11)

$$R_E \triangleq I(\boldsymbol{y}_E; \boldsymbol{s}) = \frac{1}{2}\log\det\left(\boldsymbol{I} + \boldsymbol{H}_E \boldsymbol{H}_E^H \boldsymbol{Q}_E^{-1}\right). \tag{18}$$

Substituting (16), (17), and (18) into (15) yields

$$\begin{aligned} R_{\text{sum}}^s &= [I(y_{T_1}; s_2) + I(y_{T_2}; s_1) - I(\boldsymbol{y}_E; \boldsymbol{s})]^+ \\ &= \frac{1}{2}\left[\log \frac{\left(1+\frac{P_2 \boldsymbol{w}^H \boldsymbol{R}_{fg}\boldsymbol{w}}{\sigma^2(1+\boldsymbol{w}^H \boldsymbol{R}_{ff}\boldsymbol{w})}\right)\left(1+\frac{P_1 \boldsymbol{w}^H \boldsymbol{R}_{fg}\boldsymbol{w}}{\sigma^2(1+\boldsymbol{w}^H \boldsymbol{R}_{gg}\boldsymbol{w})}\right)}{\det\left(\boldsymbol{I}+\boldsymbol{H}_E \boldsymbol{H}_E^H \boldsymbol{Q}_E^{-1}\right)}\right]^+. \end{aligned} \tag{19}$$

Noting that R_{sum}^s is a function of P_1, P_2, and $\boldsymbol{w}$, our goal is to maximize the achievable secrecy sum rate R_{sum}^s over P_1, P_2, and $\boldsymbol{w}$ to get the maximum secrecy sum rate R_{max}, subject to the total power constraint consumed by terminals and relay nodes, i.e.,

$$\begin{aligned} R_{\max} = \max_{P_1, P_2, \boldsymbol{w}} & R_{\text{sum}}^s, \\ s.t. \quad & P_S + P_R \le P_M \end{aligned} \tag{20}$$

where $P_S \triangleq P_1 + P_2$ and P_R are powers consumed by the source terminals and all relay nodes, respectively, and P_M is the total power constraint. From (4), we have

$$P_R = E\left\{\boldsymbol{x}_R^H \boldsymbol{x}_R\right\} = \boldsymbol{w}^H \boldsymbol{T} \boldsymbol{w} \tag{21}$$

where $\boldsymbol{T} \triangleq P_1 \boldsymbol{R}_{ff} + P_2 \boldsymbol{R}_{gg} + \sigma^2 \boldsymbol{I}$ using the conditions $E\{\boldsymbol{n}_R \boldsymbol{n}_R^H\} = \sigma^2 \boldsymbol{I}$ and $E\{|s_m|^2\} = 1$. We should observe that, at the optimum, the inequality constraint on $P_S + P_R$ in (20) will be active, i.e., $P_S + P_R = P_M$. Otherwise, we can increase P_1 or P_2 until the equality on the power constraint holds and R_{sum}^s can be increased further, which contradicts the optimality. Hence we have $\boldsymbol{w}^H \boldsymbol{T} \boldsymbol{w} = P_M - P_1 - P_2$ at the optimum.

Substituting (12) and (13) into (18) yields: (See the equation at the bottom of next the page) where $\boldsymbol{V}(P_1, P_2) \triangleq (P_1 P_2 |g_E|^2 + \sigma^2 P_1)\boldsymbol{R}_{cf} + (P_1 P_2 |f_E|^2 + \sigma^2 P_2)\boldsymbol{R}_{cg} + (P_1 \sigma^2 |f_E|^2 + P_2 \sigma^2 |g_E|^2 + \sigma^4)\boldsymbol{R}_{cc}$, $\boldsymbol{R}_{cf} \triangleq \boldsymbol{a}_{cf}\boldsymbol{a}_{cf}^H$, $\boldsymbol{R}_{cg} \triangleq \boldsymbol{a}_{cg}\boldsymbol{a}_{cg}^H$, and $\alpha \triangleq \sigma^2(P_1|f_E|^2 + P_2|g_E|^2) + \sigma^4$,

respectively. For convenience, let $\sigma^2 = 1$. Then the maximum secrecy sum rate (19) is now reformulated by

$$\begin{aligned}\max_{P_1,P_2,\boldsymbol{w}} \frac{1}{2}\Bigg[\log\Bigg(&\frac{\boldsymbol{w}^H(P_2\boldsymbol{R}_{fg}+\boldsymbol{R}_{ff})\boldsymbol{w}+1}{1+\boldsymbol{w}^H\boldsymbol{R}_{ff}\boldsymbol{w}}\\ &\cdot\frac{\boldsymbol{w}^H(P_1\boldsymbol{R}_{fg}+\boldsymbol{R}_{gg})\boldsymbol{w}+1}{1+\boldsymbol{w}^H\boldsymbol{R}_{gg}\boldsymbol{w}}\\ &\cdot\frac{1+\boldsymbol{w}^H\boldsymbol{R}_{cc}\boldsymbol{w}}{\boldsymbol{w}^H\boldsymbol{V}(P_1,P_2)\boldsymbol{w}+\alpha}\Bigg)\Bigg]^+\\ =\Bigg[\frac{1}{2}\log\Bigg(\max_{P_1,P_2,\boldsymbol{w}}&\frac{\boldsymbol{w}^H\boldsymbol{\Phi}(P_1,P_2)\boldsymbol{w}}{\boldsymbol{w}^H\bar{\boldsymbol{R}}_{ff}\boldsymbol{w}}\\ &\cdot\frac{\boldsymbol{w}^H\boldsymbol{\Psi}(P_1,P_2)\boldsymbol{w}}{\boldsymbol{w}^H\bar{\boldsymbol{R}}_{gg}\boldsymbol{w}}\\ &\cdot\frac{\boldsymbol{w}^H\bar{\boldsymbol{R}}_{cc}\boldsymbol{w}}{\boldsymbol{w}^H\bar{\boldsymbol{V}}(P_1,P_2)\boldsymbol{w}}\Bigg)\Bigg]^+\end{aligned}\tag{22}$$

where $\bar{\boldsymbol{R}}_{ff} \triangleq \beta\boldsymbol{T}+\boldsymbol{R}_{ff}$, $\beta \triangleq (P_M-P_1-P_2)^{-1}$, $\bar{\boldsymbol{R}}_{gg} \triangleq \beta\boldsymbol{T}+\boldsymbol{R}_{gg}$, $\bar{\boldsymbol{R}}_{cc} \triangleq \beta\boldsymbol{T}+\boldsymbol{R}_{cc}$, $\boldsymbol{\Phi}(P_1,P_2) \triangleq P_2\boldsymbol{R}_{fg}+\boldsymbol{R}_{ff}+\beta\boldsymbol{T}$, $\boldsymbol{\Psi}(P_1,P_2) \triangleq P_1\boldsymbol{R}_{fg}+\boldsymbol{R}_{gg}+\beta\boldsymbol{T}$, and $\bar{\boldsymbol{V}}(P_1,P_2) \triangleq \boldsymbol{V}(P_1,P_2)+\alpha\beta\boldsymbol{T}$, respectively. The second equality comes from the power constraint in (20) that $\beta\boldsymbol{w}^H\boldsymbol{T}\boldsymbol{w}=1$. In fact, we can normalized $\|\boldsymbol{w}\|^2=1$ due to the special structure of (22).

We can see the objective function (22) now is a product of three correlated generalized Rayleigh quotients problem, which is in general difficult to solve. Actually, from (19) we observe that the objective function is a difference between the sum of two concave functions and a third concave function, which therefore is neither convex nor concave. As a result, (20) is a constraint nonconvex optimization problem, for which a numerical solution method, such as gradient descent method or Newton's method, should be adopted to iteratively search for a local optimum. However, a global optimum cannot be guaranteed. In the simulation test, we give some examples using gradient descent method to get a local optimum.

IV. Suboptimal Security Scheme I: Null-space Beamforming With Full Eavesdropper's CSI

In the above derivations, it is shown that the maximum secrecy sum rate of the underlying system is difficult to obtain, i.e., the optimal security scheme is hard to be realized. In this section, we adopt a suboptimal criteria for the security issue. We still assume that eavesdropper's CSI is available.

From the system model, we can see that information leakage happens in both two phases. In the first phase, relay nodes can hardly do anything to help improving the security since they have to receive the signal. In the second phase, the relays actually do the distributed beamforming. If the relay nodes choose the beamforming vector lying in the null space of the eavesdropper's equivalent channel vectors, then the eavesdropper get nothing in the second phase. As such, the information leakage happens only in the first phase, which greatly improves the security of the information exchange. Mathematically, it implies from (7) that $\boldsymbol{w}^H\boldsymbol{a}_{cf}=0$, and $\boldsymbol{w}^H\boldsymbol{a}_{cg}=0$. Denote $\boldsymbol{H} \triangleq [\boldsymbol{a}_{cf},\boldsymbol{a}_{cg}]$, we then have:

$$\boldsymbol{w}^H\boldsymbol{H}=\boldsymbol{0} \Longrightarrow \boldsymbol{w}=\boldsymbol{H}_\perp\boldsymbol{v}\tag{23}$$

where $\boldsymbol{v}$ is any vector, and $\boldsymbol{H}_\perp$ is the projection matrix onto the null space of $\boldsymbol{H}$, the columns of which constitute an orthogonal basis for the null space of $\boldsymbol{H}$.

On the other hand, since the secrecy sum rate is the rate difference between the legitimate information exchange and the information leakage to the eavesdropper, we hope to design $\boldsymbol{w}$ to concurrently make the information exchange between legitimate terminals as much as possible. Using (16) and (17), the sum rate of $\mathbb{T}_1$ and $\mathbb{T}_2$ is

$$R_{\text{sum}}^T \triangleq R_{T_1}+R_{T_2}=\frac{1}{2}\log(1+\text{SNR}_1)(1+\text{SNR}_2)\tag{24}$$

where

$$\text{SNR}_1 \triangleq \frac{P_2}{\sigma^2}\frac{\boldsymbol{w}^H\boldsymbol{R}_{fg}\boldsymbol{w}}{1+\boldsymbol{w}^H\boldsymbol{R}_{ff}\boldsymbol{w}},\quad \text{SNR}_2 \triangleq \frac{P_1}{\sigma^2}\frac{\boldsymbol{w}^H\boldsymbol{R}_{fg}\boldsymbol{w}}{1+\boldsymbol{w}^H\boldsymbol{R}_{gg}\boldsymbol{w}}.\tag{25}$$

With these two considerations, our optimization criteria can be described as: to find the beamforming weight vector $\boldsymbol{w}$ and transmit powers P_1, P_2, such that 1) the information leaked to the eavesdropper is zero in the second phase; and 2) the information exchanged between legitimate terminals is as much as possible, subject to the total transmit power constraint consumed by both terminals and relays. Let $P_T \triangleq P_1+P_2+P_R$, using (23), (24), and the power constraint the same as (20), we can

---

$$\begin{aligned}&\det\left(\boldsymbol{I}+\boldsymbol{H}_E\boldsymbol{H}_E^H\boldsymbol{Q}_E^{-1}\right)\\ &=\det\left(\boldsymbol{I}+\begin{bmatrix}\frac{P_1|f_E|^2+P_2|g_E|^2}{\sigma^2} & \frac{\left(P_1f_E\boldsymbol{a}_{cf}^H+P_2g_E\boldsymbol{a}_{cg}^H\right)\boldsymbol{w}}{\sigma^2(1+\boldsymbol{w}^H\boldsymbol{R}_{cc}\boldsymbol{w})}\\ \frac{\boldsymbol{w}^H(P_1f_E^*\boldsymbol{a}_{cf}+P_2g_E^*\boldsymbol{a}_{cg})}{\sigma^2} & \frac{P_1\boldsymbol{w}^H\boldsymbol{R}_{cf}\boldsymbol{w}+P_2\boldsymbol{w}^H\boldsymbol{R}_{cg}\boldsymbol{w}}{\sigma^2(1+\boldsymbol{w}^H\boldsymbol{R}_{cc}\boldsymbol{w})}\end{bmatrix}\right)\\ &=\frac{1}{\sigma^4}\det\left(\begin{bmatrix}\left(P_1|f_E|^2+P_2|g_E|^2\right)+\sigma^2 & \frac{\left(P_1f_E\boldsymbol{a}_{cf}^H+P_2g_E\boldsymbol{a}_{cg}^H\right)\boldsymbol{w}}{(1+\boldsymbol{w}^H\boldsymbol{R}_{cc}\boldsymbol{w})}\\ \boldsymbol{w}^H\left(P_1f_E^*\boldsymbol{a}_{cf}+P_2g_E^*\boldsymbol{a}_{cg}\right) & \frac{\boldsymbol{w}^H(P_1\boldsymbol{R}_{cf}+P_2\boldsymbol{R}_{cg})\boldsymbol{w}}{(1+\boldsymbol{w}^H\boldsymbol{R}_{cc}\boldsymbol{w})}+\sigma^2\end{bmatrix}\right)\\ &=\frac{\boldsymbol{w}^H\boldsymbol{V}(P_1,P_2)\boldsymbol{w}+\alpha}{\sigma^4(1+\boldsymbol{w}^H\boldsymbol{R}_{cc}\boldsymbol{w})}\end{aligned}$$

readily formulate the security criteria as the following optimization problem:

$$\begin{aligned} \max_{P_1,P_2,\boldsymbol{w}} \quad & R_{\rm sum}^T, \\ s.t. \quad & \boldsymbol{w}=\boldsymbol{H}_\perp \boldsymbol{v}, \\ & P_1(1+\boldsymbol{w}^H\boldsymbol{R}_{ff}\boldsymbol{w})+P_2(1+\boldsymbol{w}^H\boldsymbol{R}_{gg}\boldsymbol{w}) \\ & +\sigma^2\boldsymbol{w}^H\boldsymbol{w}\le P_M, \end{aligned} \tag{26}$$

To solve (26), we firstly do the following simplifications:

1) since logarithm is an increasing function, the objective function can be equivalently changed into $\bar{R}_{\rm sum}^T \triangleq (1+{\rm SNR}_1)(1+{\rm SNR}_2)$, which will not impact the optimal P_1^o,P_2^o, and $\boldsymbol{w}^o$;
2) at the optimum, we will have $P_T=P_M$ due to the same reason as in the optimal beamforming scheme;
3) at the optimum, as proved in Appendix A, we will have ${\rm SNR}_1={\rm SNR}_2$. As a result, we have $P_1(1+\boldsymbol{w}^H\boldsymbol{R}_{ff}\boldsymbol{w})=P_2(1+\boldsymbol{w}^H\boldsymbol{R}_{gg}\boldsymbol{w})$, and $P_T=2P_1(1+\boldsymbol{w}^H\boldsymbol{R}_{ff}\boldsymbol{w})+\sigma^2\boldsymbol{w}^H\boldsymbol{w}$.

As such, (26) can be further reformulated to

$$\begin{aligned} \max_{P_1,\boldsymbol{w}} \quad & \left(\frac{P_1}{\sigma^2}\frac{\boldsymbol{w}^H\boldsymbol{R}_{fg}\boldsymbol{w}}{1+\boldsymbol{w}^H\boldsymbol{R}_{gg}\boldsymbol{w}}\right)^2 \\ s.t. \quad & 2P_1(1+\boldsymbol{w}^H\boldsymbol{R}_{ff}\boldsymbol{w})+\sigma^2\boldsymbol{w}^H\boldsymbol{w}=P_M \\ & \boldsymbol{w}=\boldsymbol{H}_\perp\boldsymbol{v}. \end{aligned} \tag{27}$$

or, equivalently

$$\begin{aligned} \max_{P_1,\boldsymbol{v}} \quad & \frac{P_1}{\sigma^2}\left(\frac{\boldsymbol{v}^H\boldsymbol{H}_\perp^H\boldsymbol{R}_{fg}\boldsymbol{H}_\perp\boldsymbol{v}}{1+\boldsymbol{v}^H\boldsymbol{H}_\perp^H\boldsymbol{R}_{gg}\boldsymbol{H}_\perp\boldsymbol{v}}\right) \\ s.t. \quad & \boldsymbol{v}^H\boldsymbol{A}(P_1)\boldsymbol{v}=K. \end{aligned} \tag{28}$$

by inserting $\boldsymbol{w}=\boldsymbol{H}_\perp\boldsymbol{v}$ into the objective function and the first constraint function, where $K\triangleq P_M-2P_1$, and $\boldsymbol{A}(P_1)\triangleq \boldsymbol{H}_\perp^H(2P_1\boldsymbol{R}_{ff}+\sigma^2\boldsymbol{I})\boldsymbol{H}_\perp$. $\boldsymbol{A}(P_1)$ is a positive definite matrix since $(2P_1\boldsymbol{R}_{ff}+\sigma^2\boldsymbol{I})$ is a positive definite diagonal matrix and $\boldsymbol{H}_\perp$ is column-orthogonal matrix. Define a new vector $\bar{\boldsymbol{v}}$ satisfying $\bar{\boldsymbol{v}}\triangleq\frac{1}{\sqrt{K}}\boldsymbol{A}^{\frac{1}{2}}(P_1)\boldsymbol{v}$. Substituting $\bar{\boldsymbol{v}}$ into (28) and noting that the term in brackets of (28) is only related to $\boldsymbol{v}$, we can rewrite (28) as

$$\begin{aligned} \max_{P_1\ge 0} \quad & \frac{P_1}{\sigma^2}\left(\max_{\bar{\boldsymbol{v}}}\frac{K\bar{\boldsymbol{v}}^H\boldsymbol{B}(P_1)\bar{\boldsymbol{v}}}{1+K\bar{\boldsymbol{v}}^H\boldsymbol{D}(P_1)\bar{\boldsymbol{v}}}\right) \\ s.t. \quad & \bar{\boldsymbol{v}}^H\bar{\boldsymbol{v}}=1, \end{aligned} \tag{29}$$

where $\boldsymbol{B}(P_1)\triangleq\boldsymbol{A}^{-\frac{1}{2}}(P_1)\boldsymbol{H}_\perp^H\boldsymbol{R}_{fg}\boldsymbol{H}_\perp\boldsymbol{A}^{-\frac{1}{2}}(P_1)$, $\boldsymbol{D}(P_1)\triangleq\boldsymbol{A}^{-\frac{1}{2}}(P_1)\boldsymbol{H}_\perp^H\boldsymbol{R}_{gg}\boldsymbol{H}_\perp\boldsymbol{A}^{-\frac{1}{2}}(P_1)$. It is readily to see the inner optimization of (29)

$$\max_{\bar{\boldsymbol{v}}}\frac{K\bar{\boldsymbol{v}}^H\boldsymbol{B}(P_1)\bar{\boldsymbol{v}}}{\bar{\boldsymbol{v}}^H\left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)\bar{\boldsymbol{v}}}, \qquad s.t. \qquad \bar{\boldsymbol{v}}^H\bar{\boldsymbol{v}}=1 \tag{30}$$

is a generalized Rayleigh quotient problem with unit-norm constraint. It is well known that the solution of (30) is the generalized eigenvector of matrix pair $(\boldsymbol{B}(P_1),\boldsymbol{I}+K\boldsymbol{D}(P_1))$ associated with the largest generalized eigenvalue, which is also the eigenvector of $(\boldsymbol{I}+K\boldsymbol{D}(P_1))^{-1}\boldsymbol{B}(P_1)$ associated with the largest eigenvalue. Mathematically, we have

$$\bar{\boldsymbol{v}}(P_1)=\alpha(P_1)\mathcal{E}\left[\left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)^{-1}\boldsymbol{B}(P_1)\right] \tag{31}$$

where $\alpha(P_1)$ is a scalar to normalize $\bar{\boldsymbol{v}}(P_1)$ to satisfy $\bar{\boldsymbol{v}}^H\bar{\boldsymbol{v}}=1$, and $\mathcal{E}[\mathbf{A}]$ is the eigenvector of matrix $\mathbf{A}$ associated with the largest eigenvalue. Note that $\boldsymbol{R}_{fg}=\boldsymbol{a}_{fg}\boldsymbol{a}_{fg}^H$, thus it is a rank-1 matrix and $\boldsymbol{B}(P_1)$ is also a rank-1 matrix. Therefore matrix $(\boldsymbol{I}+K\boldsymbol{D}(P_1))^{-1}\boldsymbol{B}(P_1)$ only has one nonzero eigenvalue, which is also the largest one. Denote $\bar{\boldsymbol{h}}\triangleq\boldsymbol{H}_\perp^H\boldsymbol{a}_{fg}$, since

$$\begin{aligned} & \left[\left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)^{-1}\boldsymbol{B}(P_1)\right]\left[\left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)^{-1}\boldsymbol{A}^{-1/2}(P_1)\bar{\boldsymbol{h}}\right] \\ &= \left[\left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)^{-1}\boldsymbol{A}^{-1/2}(P_1)\bar{\boldsymbol{h}}\bar{\boldsymbol{h}}^H\boldsymbol{A}^{-1/2}(P_1)\right] \\ &\quad\times\left[\left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)^{-1}\boldsymbol{A}^{-1/2}(P_1)\bar{\boldsymbol{h}}\right] \\ &= \left[\bar{\boldsymbol{h}}^H\boldsymbol{A}^{-1/2}(P_1)\left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)^{-1}\boldsymbol{A}^{-1/2}(P_1)\bar{\boldsymbol{h}}\right] \\ &\quad\times\left[\left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)^{-1}\boldsymbol{A}^{-1/2}(P_1)\bar{\boldsymbol{h}}\right] \\ &= \lambda(P_1)\left[\left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)^{-1}\boldsymbol{A}^{-1/2}(P_1)\bar{\boldsymbol{h}}\right] \end{aligned}$$

holds, where in the first equality we use $\boldsymbol{B}(P_1)=\boldsymbol{A}^{-\frac{1}{2}}(P_1)\bar{\boldsymbol{h}}\bar{\boldsymbol{h}}^H\boldsymbol{A}^{-\frac{1}{2}}(P_1)$, we thus find the nonzero eigenvalue and the corresponding eigenvector of $(\boldsymbol{I}+K\boldsymbol{D}(P_1))^{-1}\boldsymbol{B}(P_1)$ as, respectively

$$\begin{aligned} \lambda(P_1) &= \bar{\boldsymbol{h}}^H\boldsymbol{A}^{-1/2}(P_1)\left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)^{-1}\boldsymbol{A}^{-1/2}(P_1)\bar{\boldsymbol{h}}, \\ &= \bar{\boldsymbol{h}}^H\left(\boldsymbol{A}(P_1)+K\boldsymbol{H}_\perp^H\boldsymbol{R}_{gg}\boldsymbol{H}_\perp\right)^{-1}\bar{\boldsymbol{h}}, \end{aligned} \tag{32}$$

$$\begin{aligned} & \mathcal{E}\left[\left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)^{-1}\boldsymbol{B}(P_1)\right] \\ &= \left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)^{-1}\boldsymbol{A}^{-1/2}(P_1)\bar{\boldsymbol{h}}. \end{aligned} \tag{33}$$

and the normalizing scalar

$$\alpha(P_1)=\left(\bar{\boldsymbol{h}}^H\boldsymbol{A}^{-1/2}(P_1)\left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)^{-2}\boldsymbol{A}^{-1/2}(P_1)\bar{\boldsymbol{h}}\right)^{-1/2}.$$

Finally, substituting (32) and (33) into (31), we get the optimum beamforming weight vector as a function of P_1

$$\begin{aligned} \boldsymbol{v}(P_1) &= \sqrt{K}\boldsymbol{A}^{-1/2}(P_1)\bar{\boldsymbol{v}}(P_1) \\ &= \alpha(P_1)\sqrt{P_M-2P_1}\boldsymbol{A}^{-1/2}(P_1) \\ &\quad\times\left(\boldsymbol{I}+K\boldsymbol{D}(P_1)\right)^{-1}\boldsymbol{A}^{-1/2}(P_1)\bar{\boldsymbol{h}} \\ &= \alpha(P_1)\sqrt{P_M-2P_1} \\ &\quad\times\left(\boldsymbol{A}(P_1)+K\boldsymbol{H}_\perp^H\boldsymbol{R}_{gg}\boldsymbol{H}_\perp\right)^{-1}\bar{\boldsymbol{h}} \end{aligned} \tag{34}$$

and the maximum of (30) is $K\lambda(P_1)$. Using (32) and (29) becomes

$$\max_{P_1\ge 0}\quad\frac{P_1}{\sigma^2}(P_M-2P_1)\bar{\boldsymbol{h}}^H\left(\boldsymbol{A}(P_1)+K\boldsymbol{H}_\perp^H\boldsymbol{R}_{gg}\boldsymbol{H}_\perp\right)^{-1}\bar{\boldsymbol{h}}$$

which can be further reformulated by using $\boldsymbol{A}(P_1) = \boldsymbol{H}_\perp^H(2P_1\boldsymbol{R}_{ff}+\sigma^2\boldsymbol{I})\boldsymbol{H}_\perp$ as

$$\begin{aligned}\max_{P_1} \quad & \frac{P_1}{\sigma^2}(P_M-2P_1)\bar{\boldsymbol{h}}^H \\ & \times\left(2P_1\bar{\boldsymbol{R}}_{ff}+(P_M-2P_1)\bar{\boldsymbol{R}}_{gg}+\sigma^2\boldsymbol{I}\right)^{-1}\bar{\boldsymbol{h}} \\ s.t. \quad & 0\le P_1\le P_M/2.\end{aligned} \tag{35}$$

where $\bar{\boldsymbol{R}}_{ff}\triangleq\boldsymbol{H}_\perp^H\boldsymbol{R}_{ff}\boldsymbol{H}_\perp$, and $\bar{\boldsymbol{R}}_{gg}\triangleq\boldsymbol{H}_\perp^H\boldsymbol{R}_{gg}\boldsymbol{H}_\perp$.

Let $f(P_1)$ denote the objective function of (35), which is a polynomial function of P_1. In Appendix B, we have proved that $f(P_1)$ is a concave function of P_1 in $0\le P_1\le\frac{P_M}{2}$, thus the maximum is unique and globally optimal. As a result, the optimal power allocated to $\mathbb{T}_1$ is the solution of

$$\left.\frac{\partial f(P_1)}{\partial P_1}\right|_{P_1=P_1^o}=0. \tag{36}$$

Although generally there is no closed-form expression for P_1^o, we can obtain it using some iterative algorithms such as bisection method or Newton's method. Then, we get the optimal weight vector

$$\begin{aligned}\boldsymbol{w}^o=&\boldsymbol{H}_\perp\boldsymbol{v}(P_1^o)\\ =&\boldsymbol{H}_\perp\left(\alpha(P_1^o)\sqrt{P_M-2P_1^o}\left(\boldsymbol{A}(P_1^o)+K\bar{\boldsymbol{R}}_{gg}\right)^{-1}\bar{\boldsymbol{h}}\right)\end{aligned} \tag{37}$$

using (34), and the optimal power allocated to $\mathbb{T}_2$

$$P_2^o=P_1^o\frac{1+\boldsymbol{w}^{oH}\boldsymbol{R}_{ff}\boldsymbol{w}^o}{1+\boldsymbol{w}^{oH}\boldsymbol{R}_{gg}\boldsymbol{w}^o} \tag{38}$$

using $\mathrm{SNR}_1=\mathrm{SNR}_2$ at the optimum. Substituting P_1^o, P_2^o, and $\boldsymbol{w}^o$ into (19), we get the secrecy sum rate of this scheme as

$$\frac{1}{2}\left[\log\frac{\left(1+\frac{P_2^o\boldsymbol{w}^{oH}\boldsymbol{R}_{fg}\boldsymbol{w}^o}{\sigma^2(1+\boldsymbol{w}^{oH}\boldsymbol{R}_{ff}\boldsymbol{w}^o)}\right)\left(1+\frac{P_1^o\boldsymbol{w}^{oH}\boldsymbol{R}_{fg}\boldsymbol{w}^o}{\sigma^2(1+\boldsymbol{w}^{oH}\boldsymbol{R}_{gg}\boldsymbol{w}^o)}\right)}{1+\frac{1}{\sigma^2}\left(P_1^o|f_E|^2+P_2^o|g_E|^2\right)}\right]^+. \tag{39}$$

V. Suboptimal Security Scheme II: Artificial Noise Beamforming With No Eavesdropper's CSI

In the above two sections, we use the knowledge of the channel between relay nodes and the eavesdropper, i.e., $c_{E,n}$, $n=1,2,\cdots,N$, for selecting the beamforming coefficients and power allocation. However, in many applications, it may not be practical to know the eavesdropper's channel. In this section, we consider the scenario when the terminals and relay nodes are not aware there is an eavesdropper, i.e., without eavesdropper's CSI.

Since $\mathbb{T}_1$ and $\mathbb{T}_2$ do not know whether there is any eavesdropper, in the first phase, they transmit their information with the fixed available power P_m, $m=1,2$. In the second phase, we adopt the so-called *artificial noise* scheme proposed in [17], [18] for the relay nodes. In this scheme the relay nodes transmit artificial noise (interference) to mask the concurrent transmission of information bearing signal to the legitimate receivers. It is shown in [11] that this scheme is asymptotically near-optimal in high SNR regime in the sense that the achievable secrecy capacity loss compared to colocated MISO wiretap channel is a fixed constant. As such, the signal transmitted by the relay nodes in the second phase is

$$\boldsymbol{x}_R=\boldsymbol{W}\boldsymbol{y}_R+\boldsymbol{n}_a \tag{40}$$

where $\boldsymbol{n}_a$ is the artificial noise. After the backward self-interference cancelation, the obtained signal by $\mathbb{T}_1$, $\mathbb{T}_2$, and $\mathbb{E}$ are

$$\begin{aligned}y_{T_1}=&\boldsymbol{f}_R^T\boldsymbol{x}_R+n_{T_1}\\ =&\sqrt{P_2}\boldsymbol{f}_R^T\boldsymbol{W}\boldsymbol{g}_Rs_2+\boldsymbol{f}_R^T\boldsymbol{n}_a+\boldsymbol{f}_R^T\boldsymbol{W}\boldsymbol{n}_R+n_{T_1}\end{aligned} \tag{41}$$

$$\begin{aligned}y_{T_2}=&\boldsymbol{g}_R^T\boldsymbol{x}_R+n_{T_2}\\ =&\sqrt{P_1}\boldsymbol{g}_R^T\boldsymbol{W}\boldsymbol{f}_Rs_1+\boldsymbol{g}_R^T\boldsymbol{n}_a+\boldsymbol{g}_R^T\boldsymbol{W}\boldsymbol{n}_R+n_{T_2}\end{aligned} \tag{42}$$

$$\begin{aligned}y_E^{(2)}=&\boldsymbol{c}_E^T\boldsymbol{x}_R+n_E^{(2)}\\ =&\sqrt{P_1}\boldsymbol{c}_E^T\boldsymbol{W}\boldsymbol{f}_Rs_1+\sqrt{P_2}\boldsymbol{c}_E^T\boldsymbol{W}\boldsymbol{g}_Rs_2+n_E^{'(2)}.\end{aligned} \tag{43}$$

where $n_E^{'(2)}\triangleq\boldsymbol{c}_E^T\boldsymbol{n}_a+\boldsymbol{c}_E^T\boldsymbol{W}\boldsymbol{n}_R+n_E^{(2)}$. To avoid interfering the legitimate users, we should require $\boldsymbol{f}_R^T\boldsymbol{n}_a=\boldsymbol{g}_R^T\boldsymbol{n}_a=0$, i.e., the artificial noise should be broadcasted in the null space of the terminals's channels. On the other hand, due to the lack of eavesdropper's channel information, the relay nodes can only transmit artificial noise isotropically instead of concentrating the inference power in some direction. As a result, $\boldsymbol{n}_a$ is in the form of $\boldsymbol{n}_a=\boldsymbol{U}_\perp\boldsymbol{z}$ where $\boldsymbol{U}_\perp$ is the projection matrix onto the null space of $\boldsymbol{U}\triangleq[\boldsymbol{f},\boldsymbol{g}]$, and the component of $\boldsymbol{z}$ are i.i.d. Gaussian variables with zero mean and variance σ_z^2. Therefore, the power consumed by all the relays P_R can be written as $P_R=P_i+P_n$, where $P_i\triangleq\boldsymbol{w}^H(P_1\boldsymbol{R}_{ff}+P_2\boldsymbol{R}_{gg}+\sigma^2\boldsymbol{I})\boldsymbol{w}$ is allocated for information transmission and $P_n\triangleq E\{\boldsymbol{n}_a^H\boldsymbol{n}_a\}=\sigma_z^2(N-2)$ is allocated for artificial noise. As P_R is limited, we hope that under the constraint that the two terminals has the required quality of service (QoS), the power used for information transmission is minimized (decrease P_i) so that as much as power can be used to transmit artificial noise to confuse the potential eavesdropper (increase P_n) and improve security.

In summary, we adopt the following optimization criteria for the security issue: to find the beamforming weight vector $\boldsymbol{w}$, such that: 1) the two terminals has the required QoS, or, the received SNRs for the information bits are required to be above certain predefined thresholds; and 2) the power occupied to transmit desired information P_i is minimized so that the power available for transmitting artificial noise is maximized, under the constraint of total transmit power available by relays.

Based on (25) and (21), the optimization problem can be expressed as

$$\begin{aligned}\min_{\boldsymbol{w}} \quad & \boldsymbol{w}^H(P_1\boldsymbol{R}_{ff}+P_2\boldsymbol{R}_{gg}+\sigma^2\boldsymbol{I})\boldsymbol{w} \\ s.t. \quad & \frac{P_2}{\sigma^2}\frac{\boldsymbol{w}^H\boldsymbol{R}_{fg}\boldsymbol{w}}{1+\boldsymbol{w}^H\boldsymbol{R}_{ff}\boldsymbol{w}}\ge\gamma_1,\ \frac{P_1}{\sigma^2}\frac{\boldsymbol{w}^H\boldsymbol{R}_{fg}\boldsymbol{w}}{1+\boldsymbol{w}^H\boldsymbol{R}_{gg}\boldsymbol{w}}\ge\gamma_2\end{aligned} \tag{44}$$

where $\gamma_1 > 0$ and $\gamma_2 > 0$ are two required receive SNR thresholds. It can be further expressed as

$$\begin{aligned} \min_{\boldsymbol{w}} \quad & \boldsymbol{w}^H \boldsymbol{R} \boldsymbol{w} \\ s.t. \quad & \left|\boldsymbol{w}^H \boldsymbol{a}_{fg}\right|^2 \geq \bar{\gamma}_1 \left\| \begin{matrix} \sqrt{\boldsymbol{R}_{ff}}\boldsymbol{w} \\ 1 \end{matrix} \right\|^2 \\ & \left|\boldsymbol{w}^H \boldsymbol{a}_{fg}\right|^2 \geq \bar{\gamma}_2 \left\| \begin{matrix} \sqrt{\boldsymbol{R}_{gg}}\boldsymbol{w} \\ 1 \end{matrix} \right\|^2 \end{aligned} \tag{45}$$

where $\boldsymbol{R} \triangleq P_1 \boldsymbol{R}_{ff} + P_2 \boldsymbol{R}_{gg} + \sigma^2 \boldsymbol{I}$, $\bar{\gamma}_1 \triangleq \frac{\sigma^2 \gamma_1}{P_2}$ and $\bar{\gamma}_2 \triangleq \frac{\sigma^2 \gamma_2}{P_1}$, $\sqrt{\boldsymbol{R}_{ff}}$ means taking the element-wise square root of $\boldsymbol{R}_{ff}$. Note that in (45), $\boldsymbol{R}$ is a real diagonal matrix and constraint functions are based on Euclidean vector norm. Multiplying the optimal $\boldsymbol{w}^o$ by an arbitrary phase shift $e^{j\phi}$ will not affect the objective function or the constraints. Therefore, we can assume, without loss of generality, that $\boldsymbol{w}^H \boldsymbol{a}_{fg}$ is a real number. Consequently, (45) can be rewritten as

$$\begin{aligned} \min_{\boldsymbol{w}} \quad & t \\ s.t. \quad & \|\sqrt{\tilde{\boldsymbol{R}}}\tilde{\boldsymbol{w}}\| \leq t, \\ & \|\sqrt{\tilde{\boldsymbol{R}}_{ff}}\tilde{\boldsymbol{w}}\| \leq \frac{1}{\sqrt{\bar{\gamma}_1}}\tilde{\boldsymbol{a}}_{fg}^H \tilde{\boldsymbol{w}}, \quad \|\sqrt{\tilde{\boldsymbol{R}}_{gg}}\tilde{\boldsymbol{w}}\| \leq \frac{1}{\sqrt{\bar{\gamma}_2}}\tilde{\boldsymbol{a}}_{fg}^H \tilde{\boldsymbol{w}}, \\ & [\tilde{\boldsymbol{w}}]_{N+2} = 1 \end{aligned} \tag{46}$$

where $[\cdot]_{N+2}$ means the $(n+2)$th element of the vector, $\tilde{\boldsymbol{w}} \triangleq [\boldsymbol{w}^T, t, 1]^T$, $\tilde{\boldsymbol{a}}_{fg}^H \triangleq [\boldsymbol{a}_{fg}^H, 0, 0]$, and

$$\tilde{\boldsymbol{R}} \triangleq \begin{bmatrix} \boldsymbol{R} & & \\ & 0 & \\ & & 0 \end{bmatrix}, \ \tilde{\boldsymbol{R}}_{ff} \triangleq \begin{bmatrix} \boldsymbol{R}_{ff} & & \\ & 0 & \\ & & 1 \end{bmatrix}$$

$$\tilde{\boldsymbol{R}}_{gg} \triangleq \begin{bmatrix} \boldsymbol{R}_{gg} & & \\ & 0 & \\ & & 1 \end{bmatrix}.$$

(46) is a second-order convex cone programming (SOCP) problem with linear equation constraint [47]. Due to the convexity, the optimal $\boldsymbol{w}^o$ is unique and global, which can be efficiently solved using interior point methods. Using the so-obtained $\boldsymbol{w}^o$, the equivalent noise at the eavesdropper in the two phases becomes

$$\boldsymbol{n}_E = \begin{bmatrix} n_E^{(1)} \\ \boldsymbol{c}_E^T \boldsymbol{n}_a + \boldsymbol{w}^{oH} \boldsymbol{C}_E \boldsymbol{n}_R + n_E^{(2)} \end{bmatrix}$$

with covariance matrix

$$\boldsymbol{Q}_E = \begin{bmatrix} \sigma^2 & 0 \\ 0 & \sigma_z^2 \boldsymbol{c}_E^H \boldsymbol{U}_\perp \boldsymbol{U}_\perp^H \boldsymbol{c}_E + \sigma^2 \left(1 + \boldsymbol{w}^{oH} \boldsymbol{R}_{cc} \boldsymbol{w}^o\right) \end{bmatrix} \tag{47}$$

where $\sigma_z^2 = \frac{(P_R - \boldsymbol{w}^{oH} \boldsymbol{R} \boldsymbol{w}^o)}{(N-2)}$. Substituting (47) into (19) yields the secrecy sum rate of this scheme.

Without eavesdropper's CSI, the artificial noise should be transmitted isotropically. If most power of relay nodes is used to transmit artificial noise to eliminate the information leakage in the second phase, the scheme will be very power-low-efficient. Therefore, the choice of γ_1 and γ_2 will greatly impact the secrecy sum rate of this scheme. On one hand, larger γ_1 and γ_2 increase the information exchange rate between two terminals significantly and as a result enhance secrecy sum rate. On the other hand, for a fixed power P_R, too large γ_1 and γ_2 will make the SOCP problem unfeasible. In Section VI, simulation examples will show this point more clearly.

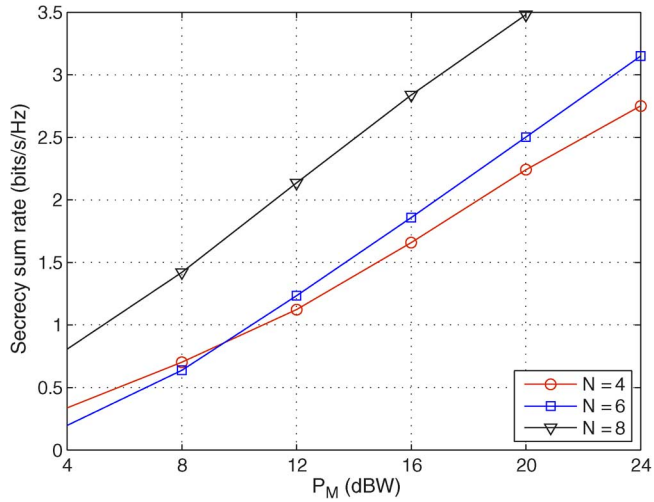


Fig. 2. Some examples of the secrecy sum rate of the optimal beamforming scheme versus the maximum available power, under different number of relay nodes.

VI. Simulation Results

In this section, computer simulation results are presented to evaluate the performances of the proposed security schemes. In all the simulation cases, all the channel coefficients $f_{R,n}, g_{R,n}, c_{E,n}, f_E, g_E$, $n = 1, 2, \cdots, N$, are randomly generated in each simulation run, as complex zero-mean Gaussian random vectors with unit covariance. The noise power σ^2 is normalized to be at 0 dBW. We use SeDuMi [48] toolbox to solve the SOCP problem. Secrecy sum rate is used as the metric of security, which is obtained by averaging 10 000 Monte Carlo simulations, unless otherwise stated.

A. Optimal Security Scheme

In Fig. 2, we give some examples of the secrecy sum rate of the optimal beamforming scheme versus the maximum available power. As analyzed in Section III, numerical iterative-searching method should be exploited to get a local optimum. Here, we use gradient descent method to find a local optimum of ω for each P_1 and P_2, and do exhausting searching for optimal P_1 and P_2 (two dimensions searching). In each searching, we randomly generate the initial $\boldsymbol{\omega}$. Even through, the calculation is still very complex. So here, we give three special cases for different channel realizations and numbers of relay nodes. The channel coefficients are realized randomly and listed in Table I (only one realization for each N but it is randomly generated). Note that since the problem is no convex, and the initial $\boldsymbol{\omega}$ is generated randomly, we can not guarantee that the global optimum is obtained.

B. Suboptimal Security Scheme I

In Fig. 3, we give some examples of secrecy rate region of null-space beamforming scheme with different number of relay nodes $N = 4, 6, 8$. The secrecy rate region is calculated by

$$\begin{aligned} R_1^s &\leq \left[I\left(y_{T_2}; s_1\right) - I(\boldsymbol{y}_E; s_1)\right]^+ \\ R_2^s &\leq \left[I\left(y_{T_1}; s_2\right) - I(\boldsymbol{y}_E; s_2)\right]^+ \\ R_1^s + R_2^s &\leq R_{\text{sum}}^s \end{aligned}$$

TABLE I
CHANNEL COEFFICIENTS IN FIG. 2

Number	Channel coefficients realizations (generated randomly)
$N=4$	$\boldsymbol{f}_R$=$\{-0.9713+0.2018j, 0.3587+0.1556j, -0.2622+0.6007j, -0.0495-0.4447j\}$, $\boldsymbol{g}_R$=$\{-0.5154-0.6750j, 0.9224-1.1338j, 0.2607-0.5625j, 0.1750-1.7148j\}$, $\boldsymbol{c}_E$=$\{0.0416-0.8452j, 0.8370-0.9942j, -0.3474-0.1654j, 0.3609-0.2038j\}$, f_e=$-0.0508+0.3523j$, g_e=$-1.0428-0.8649j$
$N=6$	$\boldsymbol{f}_R$=$\{-0.92-0.04j, 0.469-0.122j, 0.166-0.244j, -0.902+0.034j, 1.154-0.493j, -0.224+0.246i\}$, $\boldsymbol{g}_R$=$\{-0.73+0.478j, 0.746+0.424j, -0.291-0.562j, 0.622+0.414j, -0.759-0.012j, -0.053+0.318j\}$, $\boldsymbol{c}_E$=$\{-0.191+0.469j, 0.404+1.461j, -0.459-1.122j, 0.53+0.497j, 1.43-0.568j, -0.942+0.962j\}$ f_e=$0.486+0.051j$, g_e=$-0.004+1.234j$
$N=8$	$\boldsymbol{f}_R$=$\{0.423-0.341j, 0.736+0.925j, -0.322-0.292j, 0.074+0.768j, -0.107+0.199j, -1.226-0.635j, -0.285+0.808j, 0.846-0.504j\}$, $\boldsymbol{g}_R$=$\{-0.831+0.381j, 0.1-0.436j, 0.793-0.86j, 0.753-0.629j, 1.07-1.402j, 1.341+0.672j, 0.88+0.245j, 0.712-0.675j\}$, $\boldsymbol{c}_E$=$\{-0.537-1.175j, 0.226+0.37j, 0.425+0.015j, 0.71-0.0002j, -0.255-0.111i, -0.475+0.537j, -0.427-0.304j, -2.047-0.383j\}$, f_e=$-0.4056-0.3911j$, g_e=$-0.4079-0.4681j$

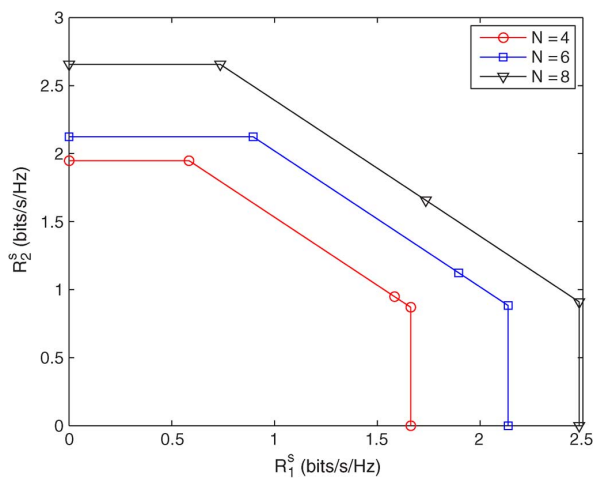


Fig. 3. Some examples of secrecy rate region of null-space beamforming scheme with different numbers of relay nodes.

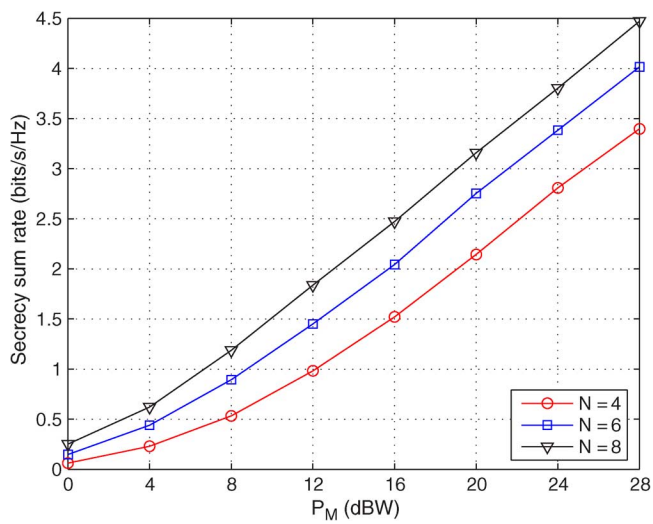


Fig. 4. Secrecy sum rate of null-space beamforming scheme versus the maximum available power of both the terminals and relay nodes, under different numbers of relay nodes.

where R_{sum}^s is in (15). They are all pentagons. In Fig. 4, we show the secrecy sum rate of null-space beamforming scheme versus the total power constraint P_M of all relay and terminals nodes. As the total available power P_M increases, the secrecy sum rate increase monotonically. Also, for a fixed P_M, increasing the number of relay nodes can enhance the security performance. This is because more relay nodes provide larger array gain to increase the average amount of information exchange in each round between legitimate terminals while the information leakage in the second phase is not increased, which is strictly zero duo to the null-space beamforming. To show the relationship between secrecy sum rate and the number of relay nodes N more clearly, in Fig. 5, we illustrate the secrecy sum rate versus N, under several total power constraint P_M. We can see the secrecy sum rate enhancement per relay nodes goes down as N goes up for any fixed P_M. This is due to the reason that the increase of array gain goes down as the number of antennas (relay nodes) increases.

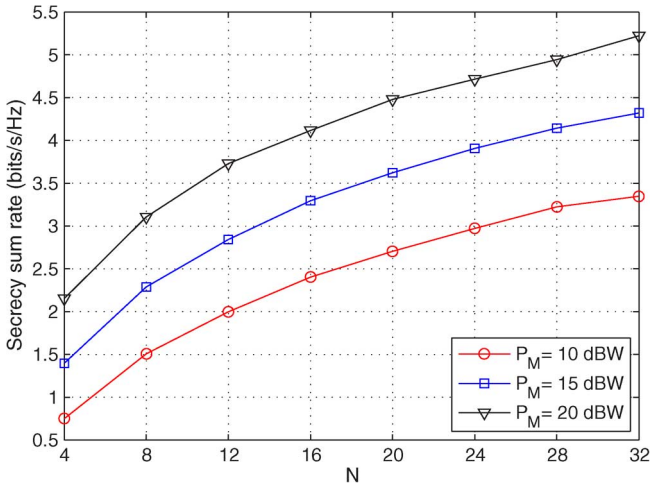


Fig. 5. Secrecy sum rate versus the number of relay nodes under different maximum power constraints.

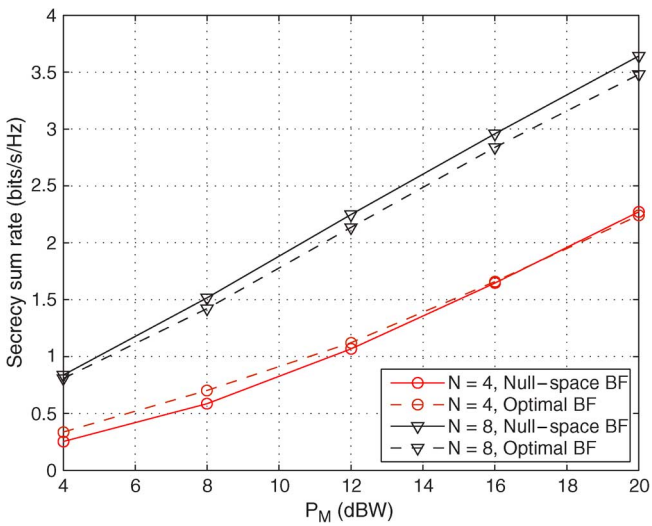


Fig. 6. Comparison of the optimal beamforming scheme and the null-space beamforming scheme under two channel random realization examples when $N = 4$ and 8. The channel coefficients are adopted from Table I.

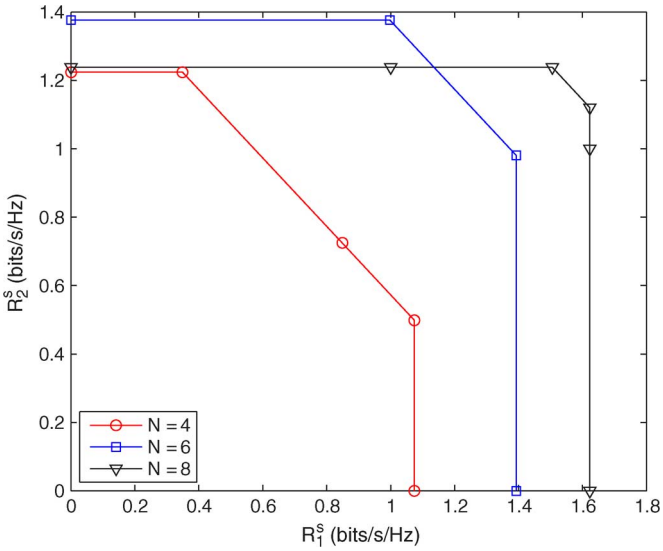


Fig. 7. Some examples of secrecy rate region of artificial noise beamforming scheme with different numbers of relay nodes.

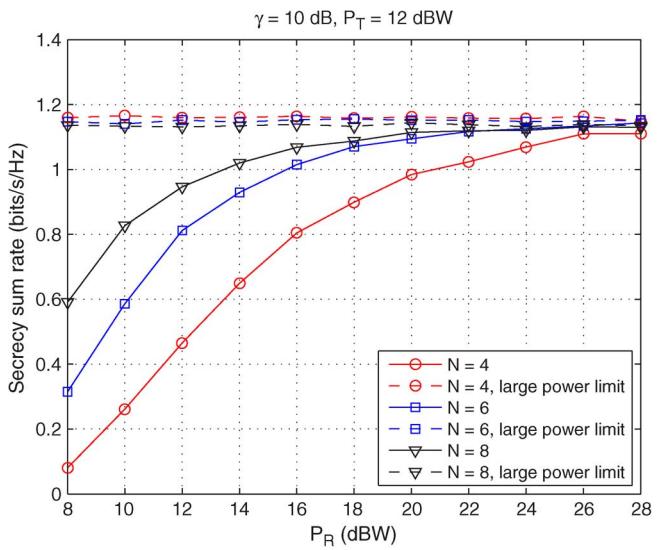


Fig. 8. Secrecy sum rate of artificial noise beamforming scheme versus the maximum available power of relay nodes under different numbers of relay nodes, where $\gamma_1 = \gamma_2 = \gamma = 10$ dB and $P_{T_1} = P_{T_2} = P_T = 12$ dBW. The dash lines are the asymptotic limits with sufficient large power of artificial noise.

For comparison, in Fig. 6, we show the secrecy sum rates of the optimal beamforming and the null-space beamforming under two channel random realizations when $N = 4$, and 8, where the channel coefficients are adopted from Table I. We can see that when $N = 4$, optimal beamforming scheme is better while null-space beamforming is better when $N = 8$. We have to emphasis here again that this is because the optimization problem of optimal beamforming is no convex, we can not guarantee that the iterative algorithm can find the global optimum. In this case, we cannot guarantee the optimal beamforming is always better than the null-space beamforming. Therefore, considering the heavy computational burden of the optimal beamforming scheme, the null-space beamforming scheme achieves a better performance-complexity tradeoff.

C. Suboptimal Security Scheme II

Fig. 7 illustrates some examples of secrecy rate region of artificial noise beamforming scheme with different number of relay nodes $N = 4$, 6, 8, which are all pentagons. In Fig. 8, we show the secrecy sum rate of artificial noise beamforming scheme versus the maximum available power P_R of relay nodes under different number of relay nodes. We set the required receive SNRs as $\gamma_1 = \gamma_2 = \gamma = 10$ dB, and the transmit power of terminals are fixed to $P_{T_1} = P_{T_2} = P_T = 12$ dBW. For any P_R, if it can not support the required QoS $\gamma = 10$ dB, i.e., the required power exceed P_R, we say the information exchange fails and set the secrecy rate to zero. It can be observed from Fig. 8 that although increasing the relay power P_R will enhance secrecy rate, there is a limit of maximum achievable secrecy sum rate even we have unlimited P_R. The dash lines demonstrate the corresponding cases when the relay nodes have sufficient power such that the power of artificial noise $P_n = P_R - P_i$ goes to infinite and the information leakage during the second phase goes to zero. The limit exists because even with enough relay power, the

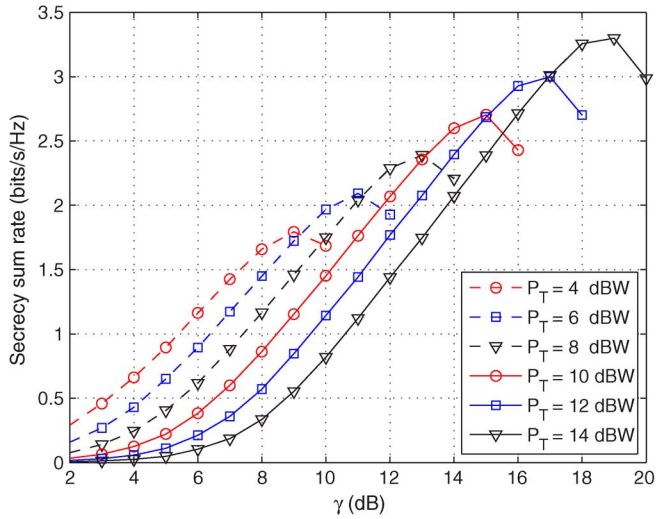


Fig. 9. Secrecy sum rate versus the required SNR $\gamma = \gamma_1 = \gamma_2$ with different transmit powers $P_{T_1} = P_{T_2} = P_T$ of terminals. We set $N = 8$ and assume P_R is infinite.

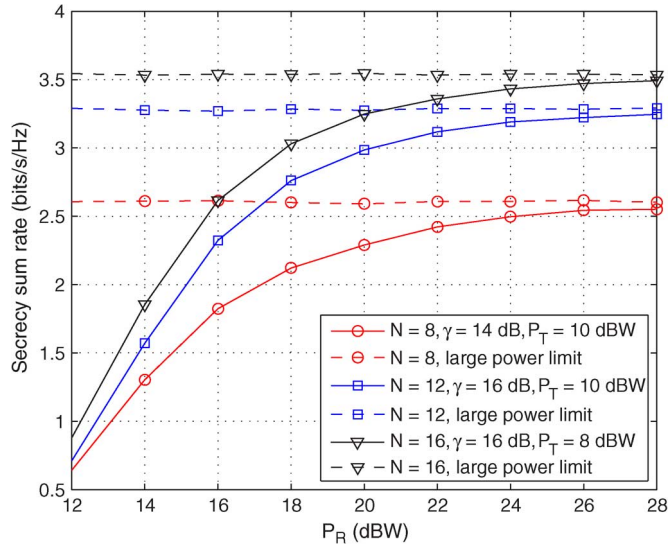


Fig. 10. Secrecy sum rate versus the maximum available power of relay nodes, under different numbers of relay nodes, required SNRs $\gamma = \gamma_1 = \gamma_2$, and transmit powers $P_{T_1} = P_{T_2} = P_T$ of terminals.

required receive SNRs γ are fixed so the information exchange between legitimate terminals do not increase much, while most relay power is used to jam the potential eavesdropper. For any fixed P_R, more relay nodes also increase the secrecy sum rate since more relay nodes provide larger array gain thus decrease the power P_i consumed by information exchange to fulfill the receive SNR requirement, and consequently increase the artificial noise power to jam the eavesdropper.

In Fig. 9, we demonstrate the secrecy sum rate versus the required SNRs $\gamma = \gamma_1 = \gamma_2$ under different transmit powers $P_{T_1} = P_{T_2} = P_T$ of terminals. The number of relay nodes is fixed to 8, and we assume P_R is infinite such that the relay nodes power is not a bottleneck to show the relationship between γ and secrecy sum rate more clearly. As we can see, for any fixed P_T, increasing SNR requirements can increase secrecy sum rate greatly compared with the Fig. 8 cases, due to the great information exchange increase. However, as γ increases, the curves go down, even with unlimited power of relay nodes. This is due to the reason that the transmit power P_T is fixed, it can not support too high γ. In this case, the SOCP problem becomes infeasible. For example, for $P_T = 6$ dB, the largest γ equals 10 dB (At $\gamma = 11$ dB, there are already many infeasible cases), and for $P_T = 12$ dBW, $\gamma = 16$ dB. Similar phenomenon can also be observed in AF protocol based one-way or two-way relay networks. Because the AF transmission in the second phase also amplifies noise at the relay nodes, if the receive SNRs at the relay nodes are not good, the receive SNR at the destination can not be arbitrary high even the relay nodes have sufficient retransmit power.

From both Fig. 8 and Fig. 9, we can see that all the number of relay nodes N, the transmit power of terminals P_T, the transmit power of relay nodes P_R, and the required SNR threshold γ are related to the secrecy sum rate of the artificial noise beamforming scheme. In Fig. 10, we give some comparisons to show the relationship more clearly. We still set $\gamma = \gamma_1 = \gamma_2$, and $P_{T_1} = P_{T_2} = P_T$.

Let us first compare the circle-curve ($N = 8$, $\gamma = 14$ dB, $P_T = 10$ dBW), and square-curve ($N = 12$, $\gamma = 16$ dB, $P_T = 10$ dBW). The circle-curve shows that when $N = 8$, $\gamma = 14$ dB, and $P_T = 10$ dBW, the secrecy sum rate is about 2.6 bits/s/Hz when $P_R > 28$ dB. In fact, recalling Fig. 9, it can already be observed that for $N = 8$, if the terminal transmit power is $P_T = 10$ dB, the largest supported receive SNR at the destination is $\gamma = 14$ dB and the secrecy sum rate is about 2.6 bits/s/Hz, even with sufficient relay power. From the square-curve of Fig. 10, we can see if we increase the number of relay nodes from $N = 8$ to $N = 12$, then $\gamma = 16$ dB is available, while the transmit power of terminals remain $P_T = 10$ dBW. For any fixed power of relay nodes P_R, the secrecy sum rate is enhanced compared to the $N = 8$, $\gamma = 14$ dB case. This is due to the reason that increasing γ results in more information exchange between legitimate terminals. The maximum secrecy sum rate can be increased to about 3.3 bits/s/Hz when $P_R > 28$ dB. This comparison means that for fixed terminal power P_T, we should *simultaneously* increase N and γ to improve the maximum secrecy sum rate, while Fig. 8 and Fig. 9 shows that neither increasing N nor increasing γ, separately, can increase the maximum secrecy sum rate.

Next let us compare the square-curve and the triangle-curve ($N = 16, \gamma = 16$ dB, $P_T = 8$ dBW). By increasing the number of relay nodes to 16, the achievable γ can be kept unchanged while the transmit power of terminals P_T can be reduced from 10 dBW to 8 dBW, which further enhances the secrecy sum rate. This is because reducing P_T will reduce the information leakage during the first phase. The maximum secrecy sum rate now becomes about 3.5 bits/s/Hz. Note from Fig. 9 that if $P_T = 8$ dBW, the largest receive SNR requirement is $\gamma = 12$ dB with 8 relay nodes, we can see that we should *simultaneously* increase N and decrease P_T to increase secrecy sum rate. It also implies that if the powers of terminals are limited, we can use more relay nodes to support sufficient large γ to improve the security performance.

VII. Conclusions

In this paper, we addressed the physical-layer security issue of bidirectional transmissions with the help of multiple relay nodes in the presence of an eavesdropper, using the metric of secrecy sum rate. We proposed three different security schemes using two-phase analog network coding and power control to enhance the security of the data exchange. In the first scheme of optimal beamforming, we hope to maximize the secrecy sum rate. However, it has been shown that the problem is a product of three correlated generalized Rayleigh quotients, which is in general difficult to solve. In the second scheme, we designed null-space beamforming and power allocation to eliminate the information leakage to the eavesdropper in the second phase and maximized the sum rate of the two terminals. We showed the optimum is unique and global using the convexity, which can be solved using some simple iterative algorithm such as bisection or Newton's method. When the instantaneous CSI of the eavesdropper is not available, we proposed a third artificial noise beamforming scheme, where artificial noise is sent at the relay nodes to mask the information signal and confuse the eavesdropper. We minimized the power allocated for transmitting desired information so that the power available for transmitting artificial noise is maximized to reduce the information leakage while guarantee the terminals to have the required QoS, under the constraint of total transmit power available by relays. We showed that this problem is an SOCP problem, thus the optimum is unique and global as well, which can be efficiently solved using interior point methods. Numerical evaluation results of the obtained secrecy rate and transmit power were provided and analyzed to show that properties and efficiency of the proposed designs.

Appendix

In this appendix, we prove that at the optimum of (26), we will have $\mathrm{SNR}_1 = \mathrm{SNR}_2$. Assume we have solved (26) and the optimal points are P_1^o, P_2^o, and $\boldsymbol{w}^o$. Then we will have $P_1^o(1+\boldsymbol{w}^{oH}\boldsymbol{R}_{ff}\boldsymbol{w}^o)+P_2^o(1+\boldsymbol{w}^{oH}\boldsymbol{R}_{gg}\boldsymbol{w}^o)+\sigma^2\boldsymbol{w}^{oH}\boldsymbol{w}^o = P_M$. Define $a(\boldsymbol{w}^o) \triangleq \boldsymbol{w}^{oH}\boldsymbol{R}_{fg}\boldsymbol{w}^o$, $b(\boldsymbol{w}^o) \triangleq \sigma^2(1+\boldsymbol{w}^{oH}\boldsymbol{R}_{ff}\boldsymbol{w}^o)$, $c(\boldsymbol{w}^o) \triangleq \sigma^2(1+\boldsymbol{w}^{oH}\boldsymbol{R}_{gg}\boldsymbol{w}^o)$, $d(\boldsymbol{w}^o) \triangleq \sigma^2 P_M - \sigma^4\boldsymbol{w}^{oH}\boldsymbol{w}^o$ and let us consider the following optimization problem

$$\begin{aligned} \max_{P_1,P_2} \quad & \left(1+P_2\frac{a(\boldsymbol{w}^o)}{b(\boldsymbol{w}^o)}\right)\left(1+P_1\frac{a(\boldsymbol{w}^o)}{c(\boldsymbol{w}^o)}\right) \\ s.t. \quad & P_1 b(\boldsymbol{w}^o)+P_2 c(\boldsymbol{w}^o) = d(\boldsymbol{w}^o). \end{aligned}$$

Obviously, this problem is equivalent to (26) after $\boldsymbol{w}^o$ is obtained. Substitute the equality constraint into the objective function, which yields an unconstraint 2nd-order polynomial objective function with the closed-form optimal point

$$P_1^o = \frac{d(\boldsymbol{w}^o)}{2b(\boldsymbol{w}^o)}, \quad \text{and} \quad P_2^o = \frac{d(\boldsymbol{w}^o)}{2c(\boldsymbol{w}^o)}.$$

As a result, we have $P_2^o\frac{a(\boldsymbol{w}^o)}{b(\boldsymbol{w}^o)} = P_1^o\frac{a(\boldsymbol{w}^o)}{c(\boldsymbol{w}^o)}$, which is $\mathrm{SNR}_1 = \mathrm{SNR}_2$.

Appendix

In this appendix, we will prove that $f(P_1)$

$$\frac{P_1}{\sigma^2}(P_M-2P_1)\bar{\boldsymbol{h}}^H\left(2P_1\bar{\boldsymbol{R}}_{ff}+(P_M-2P_1)\bar{\boldsymbol{R}}_{gg}+\sigma^2\boldsymbol{I}\right)^{-1}\bar{\boldsymbol{h}}$$

is a concave function of P_1, and thus the maximum is unique and globally optimal. To show this, we will prove the second derivative of $f(P_1)$ is negative when $0 \le P_1 \le \frac{P}{2}$.

Towards this, we first prove the following fact: For any two positive definite matrices $\boldsymbol{M}$ and $\boldsymbol{N}$ with the same dimension, we have the production $\boldsymbol{MN}$ is a positive definite matrix as well.

Proof: Since both $\boldsymbol{M}$ and $\boldsymbol{N}$ are positive definite, we have $\boldsymbol{w}^H\boldsymbol{M}^{-1}\boldsymbol{w} > 0$, $\boldsymbol{w}^H\boldsymbol{N}\boldsymbol{w} > 0$. The generalized Rayleigh quotient of matrix pencil $\boldsymbol{P} = (\boldsymbol{N}, \boldsymbol{M}^{-1})$ is

$$\min_{\boldsymbol{w}} \frac{\boldsymbol{w}^H\boldsymbol{N}\boldsymbol{w}}{\boldsymbol{w}^H\boldsymbol{M}^{-1}\boldsymbol{w}} = \lambda_{\min}^g(\boldsymbol{P}) = \lambda_{\min}(\boldsymbol{MN}) > 0$$

where $\lambda_{\min}^g(\boldsymbol{P})$ is the minimum generalized eigenvalue of matrix pencil $\boldsymbol{P}$, which is equal to the minimum eigenvalue of $\boldsymbol{MN}$. Thus all the eigenvalues of $\boldsymbol{MN}$ are positive values and $\boldsymbol{MN}$ is a positive definite matrix. ■

Denote $\varphi(P_1) \triangleq P_1(P_M-2P_1)$, and $\boldsymbol{J}(P_1) \triangleq (2P_1\bar{\boldsymbol{R}}_{ff}+(P_M-2P_1)\bar{\boldsymbol{R}}_{gg}+\sigma^2\boldsymbol{I})^{-1}$, it is not hard to obtain the first and second derivatives of $f(P_1)$ as

$$\begin{aligned} \frac{\partial f(P_1)}{\partial P_1} &= (P_M-4P_1)\bar{\boldsymbol{h}}^H\boldsymbol{J}(P_1)\bar{\boldsymbol{h}} \\ &\quad - 2P_1(P_M-2P_1)\bar{\boldsymbol{h}}^H\boldsymbol{J}^2(P_1)(\bar{\boldsymbol{R}}_{ff}-\bar{\boldsymbol{R}}_{gg})\bar{\boldsymbol{h}}, \\ \frac{\partial^2 f(P_1)}{\partial P_1^2} &= -4\bar{\boldsymbol{h}}^H\boldsymbol{Z}(P_1)\bar{\boldsymbol{h}} \end{aligned}$$

where

$$\begin{aligned} \boldsymbol{Z}(P_1) &\triangleq \boldsymbol{J}(P_1)+(P_M-4P_1)\boldsymbol{J}^2(P_1)(\bar{\boldsymbol{R}}_{ff}-\bar{\boldsymbol{R}}_{gg}) \\ &\quad - 2P_1(P_M-2P_1)\boldsymbol{J}^3(P_1)(\bar{\boldsymbol{R}}_{ff}-\bar{\boldsymbol{R}}_{gg})^2 \\ &= \boldsymbol{J}^3(P_1)\Big(\boldsymbol{J}^{-2}(P_1)+(P_M-4P_1)\boldsymbol{J}^{-1}(P_1)(\bar{\boldsymbol{R}}_{ff}-\bar{\boldsymbol{R}}_{gg}) \\ &\quad - 2P_1(P_M-2P_1)(\bar{\boldsymbol{R}}_{ff}-\bar{\boldsymbol{R}}_{gg})^2\Big). \end{aligned}$$

Inserting $\boldsymbol{J}(P_1)$ and after some simplifications, we finally obtain

$$\boldsymbol{Z}(P_1) = \boldsymbol{J}^3(P_1)\left(\sigma^2\boldsymbol{I}+P\bar{\boldsymbol{R}}_{ff}\right)\left(\sigma^2\boldsymbol{I}+P\bar{\boldsymbol{R}}_{gg}\right).$$

Note that $\boldsymbol{J}(P_1)$, $\sigma^2\boldsymbol{I}+\bar{\boldsymbol{R}}_{ff}$, and $\sigma^2\boldsymbol{I}+\bar{\boldsymbol{R}}_{gg}$ are all positive definite matrices, thus the product of them is positive definite as well, which implies

$$\frac{\partial^2 f(P_1)}{\partial P_1^2} = -4\bar{\boldsymbol{h}}^H\boldsymbol{Z}(P_1)\bar{\boldsymbol{h}} < 0$$

and this completes the proof that $f(P_1)$ is a concave function of P_1 when $0 \le P_1 \le \frac{P}{2}$. As a result, the maximum is unique and is also globally optimal.

References

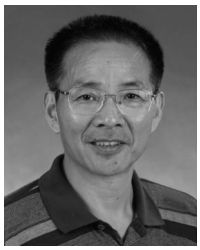
[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[4] S. L. Y. Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.
[5] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inform. Theory*, Seattle, WA, Jul. 2006.
[6] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE Int. Symp. Inform. Theory*, Nice, France, Jul. 2007.
[7] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[8] 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.
[9] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Conf. Inform. Sci. Syst.*, Baltimore, MD, Mar. 2007.
[10] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inform. Theory*, Nice, France, Jun. 2007.
[11] A. Khisti and G. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[12] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.
[13] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int Symp. Inform. Theory*, Nice, France, Jun. 2007, pp. 2471–2475.
[14] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inform. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 524–528.
[15] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, 2010, to be published.
[16] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 5, pp. 2547–2553, Jun. 2009.
[17] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Tech. Conf.*, Dallas, TX, Sep. 2005, vol. 3, pp. 1906–1910.
[18] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[19] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoustic, Speech Signal Process. (ICASSP)*, Taipei, Taiwan, Apr. 2009, pp. 2437–2440.
[20] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.
[21] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235–1249, Mar. 2009.
[22] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP J. Wireless Commun. Netw., Special Isssue on Wireless Physical Layer Security*, vol. 2009, 2009, Article ID 824235, 29 pages.
[23] E. Ekrem and S. Ulukus, "The secrecy capacity region of the gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.
[24] E. Ekrem and S. Ulukus, "Secure broadcasting using multiple antennas," *J. Commun. Netw.*, vol. 12, no. 5, pp. 411–432, Oct. 2010.
[25] S. Al-Sayed and A. Sezgin, "Secrecy in gaussian MIMO bidirectional broadcast wiretap channels: Transmit strategies," in *Proc. Asilomar SSC*, Pacific Grove, CA, Nov. 2010, pp. 285–289.
[26] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.
[27] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
[28] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *Proc. 46th Annu. Allerton Conf. Commun., Contr., Comput.*, Monticello, IL, Sep. 2008, pp. 1014–1021.
[29] B. Rankov and A. Wittneben, "Spectral efficient protocols for half-duplex fading relay channels," *IEEE J. Sel. Areas Commun.*, vol. 25, pp. 379–389, Feb. 2007.
[30] P. Popovski and H. Yomo, "Wireless network coding by amplify-and-forward for bi-directional traffic flows," *IEEE Commun. Lett.*, vol. 11, no. 1, pp. 16–18, Jan. 2007.
[31] R. Zhang, Y.-C. Liang, C. C. Chai, and S. Cui, "Optimal beamforming for two-way multi-antenna relay channel with analogue network coding," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 5, pp. 699–712, Jun. 2009.
[32] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 926–930.
[33] O. Simeone and P. Popovski, "Secure communications via cooperating base stations," *IEEE Commun. Lett.*, vol. 12, no. 3, pp. 188–190, Mar. 2008.
[34] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secrect communication," in *Proc. IEEE Inform. Theory Workshop (ITW)*, Porto, Portugal, May 2008, pp. 164–168.
[35] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
[36] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.
[37] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secure broadcasting," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Princeton, NJ, Apr. 2010, pp. 1–6.
[38] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical-layer security," in *Proc. 44th Annu. Conf. Inform. Sci. Syst. (CISS)*, Syndeney, Australia, Mar. 2010, pp. 1–6.
[39] 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.
[40] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137–155, Jan. 2011.
[41] R. Zhang, L. Song, Z. Han, B. Jiaa, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Proc. IEEE GLOBECOM*, Miami, FL, 2010.
[42] A. Mukherjee and A. L. Swindlehurst, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in *Proc. 11th IEEE SPAWC*, Jun. 2010.
[43] Y. Jing and H. Jafarkhani, "Network beamforming using relays with perfect channel information," *IEEE Trans. Inf. Theory*, vol. 55, pp. 2499–2517, Jun. 2009.
[44] V. Havary-Nassab, S. Shahbazpanahi, A. Grami, and Z.-Q. Luo, "Distributed beamforming for relay networks based on second-order statistics of the channel state information," *IEEE Trans. Signal Process.*, vol. 56, pp. 4306–4316, Sep. 2008.
[45] V. Havary-Nassab, S. Shahbazpanahi, and A. Grami, "Optimal distributed beamforming for two-way relay network," *IEEE Trans. Signal Process.*, vol. 58, pp. 1238–1250, Mar. 2010.
[46] M. Zeng, R. Zhang, and S. Cui, "On design of collaborative beamforming for two-way relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 5, pp. 2284–2295, May 2011.
[47] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[48] J. F. Sturm, "Using SeDuMi 1.02, a Matlab toolbox for optimization over symmetric cones," *Optimiz. Methods Softw.*, vol. 11–12, pp. 625–653, 1999.

Hui-Ming Wang (S'07–M'10) received the B.Sc. and Ph.D. degrees in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 2004 and 2010, respectively.

He is currently an Associate Professor at the Department of Information and Communications Engineering, Xi'an Jiaotong University, and also with the Ministry of Education Key Lab for Intelligent Networks and Network Security, China. From 2007 to 2008, and from January to June 2010, he was a Visiting Scholar at the Department of Electrical and Computer Engineering, University of Delaware, Newark. His research interests include cooperative communication systems, physical-layer security of wireless communications system, space-timing coding, and signal processing for broadband wireless communications,



Qinye Yin received the B.Sc., M.Sc., and Ph.D. degrees in communication and electronic systems from Xi'an Jiaotong University, Xi'an, China, in 1982, 1985, and 1989, respectively.

Since 1989, he has been a Professor within the Information and Communications Engineering Department, Xi'an Jiaotong University, Xi'an, China, where he is also Chair of the Academy Committee of School of Electronic and Information Engineering. From 1987 to 1989, he was a Visiting Scholar at the University of Maryland, College Park. From June to December 1996, he was a Visiting Scholar at the University of Taxes, Austin. His research interests include the joint time-frequency analysis and synthesis, the theory and applications of wireless sensor networks, multiple antenna MIMO broadband communication systems (including smart antenna systems), parameter estimation, and array signal processing.

Xiang-Gen Xia (M'97–S'00–F'09) received the B.Sc. degree in mathematics from Nanjing Normal University, Nanjing, China, and the M.Sc. degree in mathematics from Nankai University, Tianjin, China, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1983, 1986, and 1992, respectively.

He was a Senior Research Staff Member at Hughes Research Laboratories, Malibu, CA, during 1995–1996. In September 1996, he joined the Department of Electrical and Computer Engineering, University of Delaware, Newark, where he is the Charles Black Evans Professor. His current research interests include space-time coding, MIMO and OFDM systems, digital signal processing, and SAR and ISAR imaging. He has over 230 refereed journal articles published and accepted, and seven U.S. patents awarded. He is the author of the book *Modulated Coding for Intersymbol Interference Channels* (New York, Marcel Dekker, 2000).

Dr. Xia received the National Science Foundation (NSF) Faculty Early Career Development (CAREER) Program Award in 1997, the Office of Naval Research (ONR) Young Investigator Award in 1998, and the Outstanding Overseas Young Investigator Award from the National Nature Science Foundation of China in 2001. He also received the Outstanding Junior Faculty Award of the Engineering School of the University of Delaware in 2001. He is currently an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON SIGNAL PROCESSING, Signal Processing (China), and the *Journal of Communications and Networks (JCN)*. He was a Guest Editor of Space-Time Coding and Its Applications in the *EURASIP Journal of Applied Signal Processing* in 2002. He served as an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING from 1996 to 2003, the IEEE TRANSACTIONS ON MOBILE COMPUTING from 2001 to 2004, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY from 2005 to 2008, the IEEE SIGNAL PROCESSING LETTERS from 2003 to 2007, *Signal Processing (EURASIP)* from 2008 to 2011, and the *EURASIP Journal of Applied Signal Processing* from 2001 to 2004. He served as a Member of the Signal Processing for Communications Committee from 2000 to 2005 and a Member of the Sensor Array and Multichannel (SAM) Technical Committee from 2004 to 2009 in the IEEE Signal Processing Society. He serves as IEEE Sensors Council Representative of IEEE Signal Processing Society (from 2002). He also served as the Representative of IEEE Signal Processing Society to the Steering Committee for IEEE TRANSACTIONS ON MOBILE COMPUTING from 2005 to 2006. He is Technical Program Chair of the Signal Processing Symp., Globecom 2007 in Washington D.C. and the General CoChair of ICASSP 2005 in Philadelphia.