Improving Wireless Physical Layer Security via Cooperating Relays

Lun Dong, *Member, IEEE*, Zhu Han, *Senior Member, IEEE*, Athina P. Petropulu, *Fellow, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—Physical (PHY) layer security approaches for wireless communications can prevent eavesdropping without upper layer data encryption. However, they are hampered by wireless channel conditions: absent feedback, they are typically feasible only when the source-destination channel is better than the source-eavesdropper channel. Node cooperation is a means to overcome this challenge and improve the performance of secure wireless communications. This paper addresses secure communications of one source-destination pair with the help of multiple cooperating relays in the presence of one or more eavesdroppers. Three cooperative schemes are considered: decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming (CJ). For these schemes, the relays transmit a weighted version of a reencoded noise-free message signal (for DF), a received noisy source signal (for AF), or a common jamming signal (for CJ). Novel system designs are proposed, consisting of the determination of relay weights and the allocation of transmit power, that maximize the achievable secrecy rate subject to a transmit power constraint, or, minimize the transmit power subject to a secrecy rate constraint. For DF in the presence of one eavesdropper, closed-form optimal solutions are derived for the relay weights. For other problems, since the optimal relay weights are difficult to obtain, several criteria are considered leading to suboptimal but simple solutions, i.e., the complete nulling of the message signals at all eavesdroppers (for DF and AF), or the complete nulling of jamming signal at the destination (for CJ). Based on the designed relay weights, for DF in the presence of multiple eavesdroppers, and for CJ in the presence of one eavesdropper, the optimal power allocation is obtained in closed-form; in all other cases the optimal power allocation is obtained via iterative algorithms. Numerical evaluation of the obtained secrecy rate and transmit power results show that the proposed design can significantly improve the performance of secure wireless communications.**

***Index Terms*—Cooperation, distributed wireless systems, physical layer security, relaying, secrecy rate.**

Manuscript received March 20, 2009; accepted November 17, 2009. First published December 11, 2009; current version published February 10, 2010. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Biao Chen. This research was supported in part by the National Science Foundation under Grants CNS-0905425, CNS-0831371, CNS-0905556 and CNS-0910461, and by the Office of Naval Research under Grant ONR-N-00014-09-1-0342.

L. Dong is with the Department of Electrical Engineering and Computer Science, University of California, Irvine, CA 92697 USA (e-mail: lund@uci.edu).

Z. Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA (e-mail: zhan2@mail.uh.edu).

A. P. Petropulu is with the Department of Electrical and Computer Engineering, Drexel University, Philadelphia, PA 19104 USA (e-mail: athina@coe.drexel.edu).

H. V. Poor is with the School of Engineering and Applied Science, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.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.2009.2038412

I. Introduction

DUE to the broadcast nature of wireless channels, the issues of privacy and security have taken on an increasingly important role in wireless networks, especially in military and homeland security applications. The purpose of secure communications is to enable the legitimate destination to successfully obtain source information, while the eavesdroppers (wire-tappers) are not able to interpret this information. Physical (PHY) layer security using an information-theoretic point of view has attracted considerable recent attention in this context. The basic idea of PHY layer security is to exploit the physical characteristics of the wireless channel in order to transmit messages securely. This line of work was pioneered by Wyner, who introduced the wire-tap channel and established the possibility of creating perfectly secure communication links without relying on private (secret) keys [1]. Wyner showed that when an eavesdropper's channel is a degraded version of the main source-destination channel, the source and destination can exchange perfectly secure messages at a non-zero rate, while the eavesdropper can learn almost nothing about the messages from its observations. A rate at which information can be transmitted secretly from the source to its intended destination is termed an achievable *secrecy rate*, and the maximal achievable secrecy rate is named the *secrecy capacity*. In [2], the secrecy capacity of the scalar Gaussian wire-tap channel was analyzed. In [3] Wyner's approach was generalized to the transmission of confidential messages over broadcast channels. For the basic wire-tap channel, suppose that the source input is X, and the channel outputs at the intended destination and eavesdropper are Y and Z, respectively. Then, the secrecy capacity is given by $\max[I(X;Y) - I(X;Z)]$, where the maximum is taken over possible input distributions, $I(X;Y)$ denotes the mutual information between X and Y, and $I(X;Z)$ is defined similarly. Recently, there have been considerable efforts devoted to generalizing this result to the wireless fading channel and to multi-user scenarios (see, e.g., in [4, ch. 6–8] for an overview).

The feasibility of traditional PHY layer security approaches based on single antenna systems is hampered by channel conditions: absent feedback, if the channel between source and destination is worse than the channel between source and eavesdropper, the secrecy rate is typically zero [1], [2]. Some recent work has been proposed to overcome this limitation by taking advantage of multiple antenna systems, e.g., multiple-input multiple-output (MIMO) [5]–[9], single-input multiple-output (SIMO) [10], and multiple-input single-output (MISO) [11], [12] systems. However, due to cost and size limitations,

multiple antennas may not be available at network nodes. Under such scenarios, node cooperation is an effective way to enable single-antenna nodes to enjoy the benefits of multiple-antenna systems.

In this paper, we consider a scenario in which a source communicates with a destination with the help of multiple relays in the presence of one or more eavesdroppers. We assume that each node carries a single omnidirectional antenna, and that global channel state information (CSI) is available. We study three cooperative schemes that improve the achievable secrecy rate, or the total transmit power (preliminary versions of this work have appeared in [13]–[16]). In particular, we consider decode-and-forward (DF), amplify-and-forward (AF) and cooperative jamming (CJ). For DF and AF, in Stage 1, a source broadcasts its encoded signal to trusted relay nodes. In Stage 2, in DF, each relay first decodes the message and then re-encodes it and transmits a weighted version of the re-encoded signal, while in AF, each relay forwards a weighted version of the noisy signal that it received in Stage 1. For CJ, while the source transmits the encoded signal, relays transmit a weighted jamming signal with the purpose of confounding the eavesdroppers.

In the context of the aforementioned schemes, we propose novel system designs, i.e., designs of relay weights and allocation of transmit power, that meet the following objectives: 1) maximize the achievable secrecy rate subject to a total transmit power constraint, or 2) minimize the total transmit power subject to a secrecy rate constraint. We should note that codeword design for meeting the achievable secrecy rates is not considered in this work. To facilitate the analysis, we first obtain the relay weights for a fixed source power, and then find the optimal value of the source power. For DF in the presence of one eavesdropper, we derive the closed-form optimal solutions for the relay weights. For other problems, optimal relay weights are difficult to obtain, so we consider several criteria for suboptimal weight design. More specifically, assuming that the number of relays is greater than the number of eavesdroppers, for DF and AF in the presence of multiple eavesdroppers, the total signal sent from relays is completely nulled out at the eavesdroppers; for CJ, the total jamming signal sent from relays is completely nulled out at the destination. The nulling constraint can be viewed as a null-steering beamformer in array signal processing. Based on the designed relay weights, for DF in the presence of multiple eavesdroppers, and for CJ in the presence of one eavesdropper, the optimal power allocation is obtained in closed-form. In all other cases the optimal power allocation is obtained via iterative "hill-climbing" and random search algorithms. Based on numerical evaluation of the obtained results, we investigate the effectiveness of the proposed cooperative schemes under various node locations, and show that cooperation can significantly improve system performance (i.e., secrecy rate or transmit power) as compared to direct transmission without cooperation.

This paper is organized as follows. In Section II, the system model and three cooperative schemes are described. In Section III, we analyze the achievable secrecy rate of the cooperative schemes and formulate the system design problems. In Section IV, single and multiple eavesdropper cases are investigated for the secrecy rate maximization problem. The transmit power minimization problem is studied in Section V. Numerical results are described in Section VI, and conclusions and topics of interest for future work are discussed in Section VII.

A. Related Work

DF and AF cooperative schemes for improving transmission rate in the absence of an eavesdropper were studied in [17]–[21]. Cooperative schemes for improving communications in the presence of an eavesdropper can be grouped into three categories. In the first category, a relay plays a dual role, i.e., it acts as both a helper and an eavesdropper [22], [23]; in the second one, a relay helps the eavesdropper [24], [25]; in the third one, a relay or a helper helps the source-destination transmission. Since our work falls under the third category, we next describe the corresponding literature in some more details.

In [26], the scenario where multiple users communicate with a common receiver (i.e., multiple access) in the presence of an eavesdropper is considered, and the optimal transmit power allocation policy is chosen to maximize the secrecy sum-rate. A user that is prevented from transmitting based on the obtained power allocation can help increase the secrecy rate for other users by transmitting artificial noise to the eavesdropper. In [27], a four-node system model is considered, (i.e., source, destination, eavesdropper and relay) in which the relay transmits a noise signal that is independent of the source signals in order to jam the eavesdropper. The rate-equivocation region is derived to show gains and applicable scenarios for cooperation (the equivocation denotes the uncertainty of the eavesdropper about the source message). A generalization of [26] and [27] is proposed in [28], in which the helper transmits signals from another source encoder (not necessarily Gaussian noise), and the helper's codewords do not have to be decoded by the receiver. In [29], inner and outer bounds on the rate-equivocation region are derived for the four-node model for both discrete memoryless and Gaussian channels. In [30], the secrecy rate of orthogonal relay eavesdropper channels is studied. In that scenario, relay and destination receive the source signals on two orthogonal channels, the destination also receives transmissions from the relay on its channel, and the eavesdropper overhears either one or both of the orthogonal channels.

Our work in this paper is different from the aforementioned works in the following aspects: i) The system models are different. Existing work has focused primarily on the case of one relay and one eavesdropper, while in this work the more general case of multiple relays and multiple eavesdroppers is considered and ii) The problems to be addressed are different. Existing work has focused primarily on the analysis of secrecy rate and the rate-achieving relaying strategy. In this paper, for each predefined cooperative scheme, we consider system design (relay weight design and power allocation) for secrecy rate maximization subject to a power constraint or power minimization subject to a secrecy rate constraint, and the obtained results are novel.

B. Notation

We adopt the following notation. Bold uppercase letters denote matrices and bold lowercase letters denote column vectors.

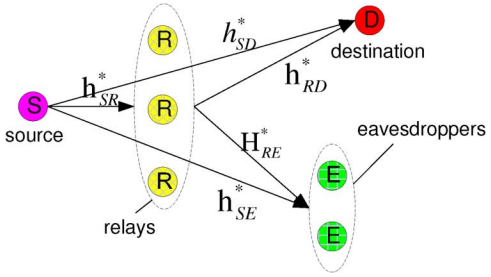


Fig. 1. Illustration of system model.

Conjugate, transpose, and conjugate transpose are represented by $(\cdot)^*$, $(\cdot)^T$ and $(\cdot)^\dagger$ respectively; $\mathbf{I}_M$ is the identity matrix of size $M \times M$; $\mathrm{diag}\{\mathbf{a}\}$ denotes a diagonal matrix with the elements of the vector $\mathbf{a}$ along its diagonal; $||\mathbf{a}||$ denotes the 2-norm of the vector $\mathbf{a}$; $\mathbf{0}_{M\times N}$ denotes an all-zero matrix of size $M\times N$; $\mathcal{CN}(\mu, \sigma^2)$ denotes the circularly symmetric, complex Gaussian distribution with mean μ and variance σ^2; $\mathbb{E}\{\cdot\}$ denotes expectation; $\log(\cdot)$ denotes the base-2 logarithm.

II. System Model and Cooperative Schemes

We consider a wireless network model consisting of one source node, N trusted relay nodes, one destination node, and J ($J \geq 1$) eavesdroppers (see Fig. 1). The eavesdroppers are passive and the goal is to interpret the source information without trying to modify it. The source message W is uniformly distributed over the message set $\mathcal{W} = \{1, 2, \ldots, 2^{nR}\}$, which is transmitted in n channel uses. Here, R denotes the source rate (unit: bits per channel use) and the message has entropy nR bits. A stochastic encoder at the source maps each message W to a codeword $x^n \in \mathcal{X}^n$, where $\mathcal{X}^n$ is an input alphabet of length-n. For the purpose of evaluating the achievable secrecy rate, we assume that the codewords used at the source are Gaussian inputs. We consider a time division multiple access system, in which there are n time units in each transmission slot. In a time unit, the average power of an encoded source symbol is normalized to unity. P is the total power budget for transmitting one source symbol. Thermal noise at any node is assumed to be zero-mean white complex Gaussian with variance σ^2, i.e., $\mathcal{CN}(0, \sigma^2)$. Each node is equipped with a single omni-directional antenna and operates in a half-duplex mode.

All channels are assumed to undergo flat fading and are quasi-static. We denote by h^*_{SD} the baseband complex channel gain between the source and the destination, by $\mathbf{h}^*_{SE}$ the channel vector $(J \times 1)$ between the source and the J eavesdroppers, by $\mathbf{h}^*_{SR}$ the channel vector $(N \times 1)$ between the source and the N relays, by $\mathbf{h}^*_{RD}$ the channel vector $(N\times 1)$ between the N relays and the destination, and by $\mathbf{H}^*_{RE}$ the channel matrix $(N \times J)$ between the N relays and the J eavesdroppers. For the case of one eavesdropper, the vector $\mathbf{h}^*_{SE}$ reduces to a scalar h^*_{SE} and the matrix $\mathbf{H}^*_{RE}$ reduces to a vector $\mathbf{h}^*_{RE}$.

We assume that global CSI is available (a common assumption in the PHY security literature), and even the eavesdroppers' channels are known. Information on the eavesdroppers' channels can be obtained in cases in which the eavesdroppers are active in the network and their transmissions can be monitored [31]. This is applicable particularly in networks combining multicast and unicast transmissions, in which terminals play dual roles as legitimate receivers for some signals and eavesdroppers for others. Note that there have been some recent works focusing on secrecy rates based on partial CSI or channel statistics (e.g., in [4, ch. 5] and [32]). System design of cooperative schemes that uses partial CSI or channel statistics will be considered in future work.

Similarly as in [24], we here assume that the source, destination and eavesdropper(s) know the existence of the relays who intend to help the destination, and also know which cooperative scheme will be used. In other words, encoding schemes at the source, the cooperative protocol, and decoding methods at the destination and at eavesdroppers are all public information; only the source message is confidential.

Next, we describe a benchmark scheme without cooperation (i.e., direct transmission) and three cooperative schemes (i.e., DF, AF and CJ). We should recall at this point that the ideas of DF and AF schemes were discussed in [17]–[19], and the idea of CJ can be found, e.g., in [7] and [26]–[28]. However, our system model and the problems to be addressed are different from those of existing works.

A. Direct Transmission (DT)

For DT, within a transmission slot, the source transmits its n encoded symbols directly to the destination using all the available transmit power. Without loss of generality, in the rest of the paper we focus on a specific symbol x occupying a specific time unit (out of n time units) within a transmission slot. The symbol x has unit power, i.e, $\mathbb{E}\{|x|^2\} = 1$. Also for notational convenience, the time index has been omitted.

When transmitting the symbol x in a time unit, the received signal at the destination is given by

$$y_d = \sqrt{P} h^*_{SD} x + n_d \tag{1}$$

where n_d represents complex Gaussian noise at the destination (which is assumed to be white over time units) and P is the total transmit power for transmitting one symbol.

The received signals at the J eavesdroppers, stacked in vector $\mathbf{y}_e(J \times 1)$, equal

$$\mathbf{y}_e = \sqrt{P} \mathbf{h}^*_{SE} x + \mathbf{n}_e \tag{2}$$

where $\mathbf{n}_e \sim \mathcal{CN}(0, \sigma^2 \mathbf{I}_J)$ is a complex Gaussian vector representing white noise at the J eavesdroppers.

B. Decode-and-Forward

There are two stages in DF. In Stage 1, the source broadcasts its n encoded symbols to its trusted relays using the first transmission slot. When transmitting the symbol x, the received signals at the N relays, stacked in vector $\mathbf{y}_r(N \times 1)$, equal

$$\mathbf{y}_r = \sqrt{P_s} \mathbf{h}^*_{SR} x + \mathbf{n}_r \tag{3}$$

where P_s is the transmit power of the source and $\mathbf{n}_r \sim \mathcal{CN}(0, \sigma^2 \mathbf{I}_N)$ is the noise vector at the relays. Recalling that P is the overall power for transmitting the symbol, it holds that $0 < P_s \leq P$.

In Stage 2, all the trusted relays that successfully decode the message, re-encode the message and cooperatively transmit the re-encoded symbols to the destination, using the second transmission slot. For notational convenience, we here assume that

all the N relays successfully decode the source message. The case in which not all the relays successfully decode the source message will be discussed in Section IV-A-2. Specifically, each relay transmits a weighted version of the re-encoded symbol. Let the weights of all relays be stacked in vector $\mathbf{w}(N \times 1)$ and let $\tilde{x}$ be the re-encoded symbol at relays. When transmitting the symbol $\tilde{x}$, the received signal at the destination is

$$y_d = \mathbf{h}_{RD}^{\dagger}\mathbf{w}\tilde{x} + n_d \tag{4}$$

while at the eavesdroppers, the vector containing the received signals is

$$\mathbf{y}_e = \mathbf{H}_{RE}^{\dagger}\mathbf{w}\tilde{x} + \mathbf{n}_e. \tag{5}$$

The transmit power budget for Stage 2 is $P - P_s$. The destination or eavesdroppers can exploit the received signals in both stages for interpreting the source information.

C. Amplify-and-Forward

Like DF, AF is also a two-stage scheme. Stage 1 is the same as in the DF scheme, except that the transmit power P_s can be different. In Stage 2, the N trusted relays forward to the destination the signals that they received during Stage 1, using the second transmission slot. More specifically, each relay transmits a weighted version of the noisy signal that they received during Stage 1. Let the transmitted signals of all relays be denoted by the product $\mathrm{diag}\{\mathbf{w}\}\mathbf{y}_r$, where $\mathbf{w}$ is the weight vector and $\mathbf{y}_r$ is given by (3). The transmit power budget for Stage 2 is $P - P_s$.

The received signal at the destination is

$$\begin{aligned} y_d &= \sqrt{P_s}\mathbf{h}_{RD}^{\dagger}\mathrm{diag}\{\mathbf{w}\}\mathbf{h}_{SR}^{*}x + \mathbf{h}_{RD}^{\dagger}\mathrm{diag}\{\mathbf{w}\}\mathbf{n}_r + n_d \\ &= \sqrt{P_s}\mathbf{h}_{RD}^{\dagger}\mathrm{diag}\left\{\mathbf{h}_{SR}^{*}\right\}\mathbf{w}x + \mathbf{n}_r^{T}\mathrm{diag}\{\mathbf{h}_{RD}^{*}\}\mathbf{w} + n_d \\ &= \mathbf{a}^{\dagger}\mathbf{w}x + \mathbf{n}_r^{T}\mathrm{diag}\{\mathbf{h}_{RD}^{*}\}\mathbf{w} + n_d \end{aligned} \tag{6}$$

where $\mathbf{a} \triangleq \sqrt{P_s}\mathrm{diag}\{\mathbf{h}_{SR}\}\mathbf{h}_{RD}$.

The received signals at the eavesdroppers, in a vector form, are

$$\begin{aligned} \mathbf{y}_e &= \sqrt{P_s}\mathbf{H}_{RE}^{\dagger}\mathrm{diag}\{\mathbf{w}\}\mathbf{h}_{SR}^{*}x + \mathbf{H}_{RE}^{\dagger}\mathrm{diag}\{\mathbf{w}\}\mathbf{n}_r + \mathbf{n}_e \\ &= \sqrt{P_s}\mathbf{H}_{RE}^{\dagger}\mathrm{diag}\left\{\mathbf{h}_{SR}^{*}\right\}\mathbf{w}x + \mathbf{H}_{RE}^{\dagger}\mathrm{diag}\{\mathbf{n}_r\}\mathbf{w} + \mathbf{n}_e \\ &= \mathbf{B}^{\dagger}\mathbf{w}x + \mathbf{H}_{RE}^{\dagger}\mathrm{diag}\{\mathbf{n}_r\}\mathbf{w} + \mathbf{n}_e \end{aligned} \tag{7}$$

where $\mathbf{B} \triangleq \sqrt{P_s}\mathrm{diag}\{\mathbf{h}_{SR}\}\mathbf{H}_{RE}$.

D. Cooperative Jamming

In CJ, while the source transmits, the relays transmit a weighted jamming signal that is independent of the source message, with the purpose of confounding the eavesdropper(s). In particular, while the source transmits the encoded signal $\sqrt{P_s}x$, the N relays transmit a weighted version of a common jamming signal z. The total transmit power budget for transmitting the jamming signal is thus $P - P_s$.

The received signal at the destination is

$$y_d = \sqrt{P_s}h_{SD}^{*}x + \mathbf{h}_{RD}^{\dagger}\mathbf{w}z + n_d, \tag{8}$$

and the received signals at the eavesdroppers equal

$$\mathbf{y}_e = \sqrt{P_s}\mathbf{h}_{SE}^{*}x + \mathbf{H}_{RE}^{\dagger}\mathbf{w}z + \mathbf{n}_e. \tag{9}$$

III. Achievable Secrecy Rates of the Cooperative Schemes

There have been several works that analyzed the MIMO wire-tap channels, in which source, destination and eavesdroppers are equipped with multiple antennas. Certainly, these results also cover the special case in which some or all nodes are equipped with one antenna only. In particular, for the case of one eavesdropper, an achievable secrecy rate is [6], [8], [9]

$$R_s = \max\{R_d - R_e\} \tag{10}$$

where the maximum is taken over possible input covariance matrices, R_d is the achievable rate of the source-destination link and R_e is the achievable rate of the source-eavesdropper link. The achievability of (10) was shown in [11] via the use of Gaussian inputs. In [6], [8], and [9], it was further shown that (10) is actually the secrecy capacity. For the case of multiple eavesdroppers, an achievable secrecy rate is given by [33]

$$R_s = \max \min_{j} \left\{R_d - R_e^{j}\right\} \tag{11}$$

in which the maximum is again taken over possible input covariance matrices, R_d is the achievable rate of the source-destination link and R_e^j is the achievable rate of the link between the source and the jth eavesdropper. The achievability of (11) was shown in [33] by the use of Gaussian inputs. The achievable secrecy rate in (11) can be interpreted as a worst-case result, i.e., the eavesdropper with the best channel dominates the secrecy rate. We should mention that the above works considered memoryless MIMO channels, i.e., channels in which the outputs at time i depend only on the inputs at time i. Also, for the aforementioned results there is no relay involved in transmissions, i.e., the source directly transmits messages to the destination.

Our proposed CJ scheme is a one-stage scheme, in which the source directly transmits messages to the destination and the relays transmit jamming signals at the same time. Thus, assuming that Gaussian codewords are used at the source input, the achievable secrecy rate of (10) and (11) can be directly applied to CJ. Also, our proposed two-stage AF scheme is mathematically equivalent to a 1×2 SIMO system (one-stage), so the achievable secrecy rates of (10) and (11) can be applied to AF as well. The feasibility of (10) on the AF scheme was also shown in [24].

For the DF scheme, after decoding the source information, the relays may re-encode the information by using a different codeword and forward this re-encoded message to the destination. We should note that the received signal at destination/eavesdropper at time i depends only on the relays' transmitted encoded signals at time i (though a relay's transmitted signal at time i depends on its received signal before time i). This is usually referred to as the "memoryless relay channel" in literature [27], [29]. For convenience, we focus on two specific cases for which the rates of source-destination and source-eavesdropper links admit simple closed-form expressions. In the first case, the relays still use the same codewords as the source, while in the second case, the relays use different codewords independent of source codewords. It was shown in [24] that the expression for the achievable secrecy rate of (10) is valid for the two cases of DF in the presence of one eavesdropper. Following the proof in [33] leading to (11), it can be further shown that the expression of (11) is also valid for the case of multiple eavesdroppers.

Since global CSI is available, the achievable rate and the total transmit power of the cooperative schemes are functions of the relay weights $\mathbf{w}$ and the source power P_s. Thus, our first design objective is to determine $\mathbf{w}$ and P_s in order to maximize the achievable secrecy rate, $R_s(\mathbf{w}, P_s)$, subject to a total transmit power constraint P_0, i.e.,

$$\begin{aligned} &\arg\max_{\mathbf{w},P_s} \quad R_s(\mathbf{w}, P_s) \\ &\text{s.t. } P(\mathbf{w}, P_s) \le P_0 \end{aligned} \tag{12}$$

where $P(\mathbf{w}, P_s)$ denotes the total transmit power.

The second design objective is to determine $\mathbf{w}$ and P_s to minimize the total transmit power subject to an achievable secrecy rate constraint R_s^0, i.e.,

$$\begin{aligned} &\arg\min_{\mathbf{w},P_s} \quad P(\mathbf{w}, P_s) \\ &\text{s.t. } R_s(\mathbf{w}, P_s) \ge R_s^0. \end{aligned} \tag{13}$$

Intuitively, to maximize the secrecy rate, we need to deliver high signal power to the destination, and low signal power to the eavesdroppers. This is somewhat similar to the idea of transmit beamforming in array signal processing: in traditional transmit beamforming, the multi-antenna transmitter intends to maximize the signal power on a desired direction and suppress/eliminate signals at undesired directions [34]. Therefore, our analysis is based on a signal processing framework.

IV. Design for Achievable Secrecy Rate Maximization

In this section, we provide a system design that maximizes the secrecy rate $R_s(\mathbf{w}, P_s)$ subject to a transmit power constraint P_0, for the case of one or multiple eavesdroppers. In particular, the design refers to relay weights and power allocation on source and relays. We first fix P_s to obtain the weights for secrecy rate maximization, and then find the optimal value of P_s. As we will show in Section IV-D, the inequality constraint ($\le P_0$) yields the same solutions as the equality power constraint ($= P_0$). Thus, for convenience, we next propose a design based on the equality power constraint ($= P_0$).

A. Decode-and-Forward

Recall that we here assume that all the N relays successfully decode the message signal, and the case in which not all the relay successfully decode the message signal will be discussed in Section IV-A-2.

For the first case considered in the DF scheme, the relays use the same codewords as the source, so the DF scheme is mathematically equivalent to a 1×2 SIMO system. Based on (3) and (4), the rate at the destination is

$$R_d^{(1)} = \frac{1}{2}\log\left(\alpha + \frac{\mathbf{w}^\dagger \mathbf{R}_{RD}\mathbf{w}}{\sigma^2}\right) \tag{14}$$

where $\mathbf{R}_{RD} = \mathbf{h}_{RD}\mathbf{h}_{RD}^\dagger$ and $\alpha = 1 + P_s|h_{SD}|^2/\sigma^2$. It is well-known that the strategy to achieve the capacity in (14) is maximal ratio combining (MRC) [35]. Note that $P_s|h_{SD}|^2/\sigma^2$ is the received signal-to-noise ratio (SNR) in Stage 1 at the destination, and the scalar factor 1/2 is due to the fact that two time units are required in two stages. The rate at the eavesdroppers is obtained in a similar way.

For the second case in DF, the relays use different codewords independent of the source codewords to transmit the same information. The rate at the destination is

$$R_d^{(2)} = \frac{1}{2}\log(\alpha) + \frac{1}{2}\log\left(1 + \frac{\mathbf{w}^\dagger \mathbf{R}_{RD}\mathbf{w}}{\sigma^2}\right). \tag{15}$$

It can be shown that the analyses for the above two cases are similar. Thus, in the rest of the paper, we focus on the analysis for the first case only. The analysis for the second case can be conducted in a similar fashion.

1) Relay Weight Optimization:

- **One eavesdropper**: We here discuss the simple scenario of one eavesdropper (for the case in which the relays use the same codewords as the source). From (3) and (5), the rate at the eavesdropper is

$$R_e = \frac{1}{2}\log\left(\beta + \frac{\mathbf{w}^\dagger \mathbf{R}_{RE}\mathbf{w}}{\sigma^2}\right) \tag{16}$$

where $\mathbf{R}_{RE} = \mathbf{h}_{RE}\mathbf{h}_{RE}^\dagger$ and $\beta = 1 + P_s|h_{SE}|^2/\sigma^2$. From (14) and (16), the achievable secrecy rate in (10) can be written as

$$R_s(\mathbf{w}, P_s) = \frac{1}{2}\log\left(\frac{\alpha\sigma^2 + \mathbf{w}^\dagger \mathbf{R}_{RD}\mathbf{w}}{\beta\sigma^2 + \mathbf{w}^\dagger \mathbf{R}_{RE}\mathbf{w}}\right) \tag{17}$$

where α and β are functions of P_s.

The problem of maximizing the achievable secrecy rate R_s for a fixed source power P_s can be formulated as

$$\begin{aligned} &\arg\max_{\mathbf{w}} \frac{\alpha\sigma^2 + \mathbf{w}^\dagger \mathbf{R}_{RD}\mathbf{w}}{\beta\sigma^2 + \mathbf{w}^\dagger \mathbf{R}_{RE}\mathbf{w}} \\ &\text{s.t.} \quad \mathbf{w}^\dagger\mathbf{w} = P_0 - P_s. \end{aligned} \tag{18}$$

Substituting the constraint into the objective function in (18), the optimization problem of (18) can be rewritten as

$$\arg\max_{\mathbf{w}} \frac{\mathbf{w}^\dagger \widetilde{\mathbf{R}}_{RD}\mathbf{w}}{\mathbf{w}^\dagger \widetilde{\mathbf{R}}_{RE}\mathbf{w}} \tag{19}$$

where

$$\widetilde{\mathbf{R}}_{RD} \triangleq \frac{\alpha\sigma^2}{P_0 - P_s}\mathbf{I}_N + \mathbf{R}_{RD} \tag{20}$$

and

$$\widetilde{\mathbf{R}}_{RE} \triangleq \frac{\beta\sigma^2}{P_0 - P_s}\mathbf{I}_N + \mathbf{R}_{RE}. \tag{21}$$

The problem in (19) is a generalized eigenvector problem. The maximal value of (18) corresponds to the maximal eigenvalue of the matrix $\widetilde{\mathbf{R}}_{RE}^{-1}\widetilde{\mathbf{R}}_{RD}$, and the corresponding eigenvector is the optimal weight vector [36]. Therefore, the optimal weight is $\sqrt{P_0 - P_s}\mathbf{q}_{\text{df}}$ where $\mathbf{q}_{\text{df}}$ is the unit-norm eigenvector of the matrix $\widetilde{\mathbf{R}}_{RE}^{-1}\widetilde{\mathbf{R}}_{RD}$ corresponding to its largest eigenvalue.

- **Multiple eavesdroppers**: From (11), the achievable secrecy rate in the presence of multiple eavesdroppers is related to the rates at all eavesdroppers $R_e^1, \ldots, R_e^J$. Deter-

mining the weights for the problem of secrecy rate maximization might be difficult. In the following, we consider a relatively easier problem, that maximizes a lower bound of the secrecy rate in (11) and leads to a simple closed-form solution.

Let us introduce an additional constraint to completely null out signals at all eavesdroppers in Stage 2, i.e., $\mathbf{H}_{RE}^{\dagger}\mathbf{w} = 0_{J\times 1}$. Note that the condition $N > J$ is needed here. In case of $N \leq J$, we cannot null out signals at all eavesdroppers; appropriate system design for the case of $N \leq J$ would be an interesting future research direction. For example, we may replace the nulling constraint with a constraint that the received power at eavesdroppers does not exceed a predefined threshold.

By nulling the signals at eavesdroppers, the Shannon capacity to the eavesdroppers in Stage 2 becomes zero, so the secrecy rate could be enhanced. Nulling signals at undesired nodes is sometimes referred to as null-steering beamforming in array signal processing [37], or zero-forcing in MIMO broadcast channels [38]. On the other hand, if the relays transmit signals without careful weight design, a positive secrecy rate may not be achieved when the relay-destination channels are worse than the relay-eavesdropper channels.

Under this nulling constraint the achievable secrecy rate to be maximized is

$$R_s(\mathbf{w}, P_s) = \frac{1}{2}\log\left(\alpha + \frac{\mathbf{w}^{\dagger}\mathbf{R}_{RD}\mathbf{w}}{\sigma^2}\right) - \log\left(\max_j(\beta_j)\right) \quad (22)$$

where $\beta_j = 1 + P_s|\mathbf{h}_{SE}(j)|^2/\sigma^2$ and $\mathbf{h}_{SE}(j)$ denotes the ith element of the vector $\mathbf{h}_{SE}$. It can be easily seen that the secrecy rate in (22) under both the power constraint and the additional constraint $\mathbf{H}_{RE}^{\dagger}\mathbf{w} = 0_{J\times 1}$ cannot be greater than the secrecy rate in (11) under the power constraint only.

The optimization problem of maximizing the achievable secrecy rate in (22) can be formulated as

$$\arg\max_{\mathbf{w}} |\mathbf{w}^{\dagger}\mathbf{h}_{RD}|^2 \quad \text{s.t.} \begin{cases} \mathbf{w}^{\dagger}\mathbf{H}_{RE} = \mathbf{0}_{1\times J} \\ \mathbf{w}^{\dagger}\mathbf{w} = P_0 - P_s. \end{cases} \quad (23)$$

As noted above, the problem in (23) is referred to as the null-steering beamformer in the array signal processing literature, and its optimal solution is given by [37]

$$\mathbf{w} = \frac{\sqrt{P_0 - P_s}}{\|(\mathbf{I}_N - \mathbf{P}_{RE})\mathbf{h}_{RD}\|}(\mathbf{I}_N - \mathbf{P}_{RE})\mathbf{h}_{RD} \quad (24)$$

where $\mathbf{P}_{RE} = \mathbf{H}_{RE}(\mathbf{H}_{RE}^{\dagger}\mathbf{H}_{RE})^{-1}\mathbf{H}_{RE}^{\dagger}$ is the orthogonal projection matrix onto the subspace spanned by the columns of $\mathbf{H}_{RE}$.

2) Selection of Source Power: A relay can correctly decode the source message if the rate at the relay (in Stage 1) is no less than the rate at the destination. Let us first consider the case of multiple eavesdroppers in which the weights are designed by (24). For the ith relay, it holds that

$$\frac{1}{2}\log\left(1 + \frac{P_s|\mathbf{h}_{SR}(i)|^2}{\sigma^2}\right) \geq \frac{1}{2}\log\left(1 + \frac{P_s|h_{SD}|^2}{\sigma^2} + \frac{(P_0 - P_s)|\tilde{\mathbf{w}}^{\dagger}\mathbf{h}_{RD}|^2}{\sigma^2}\right) \quad (25)$$

where $\tilde{\mathbf{w}} = (\mathbf{I}_N - \mathbf{P}_{RE})\mathbf{h}_{RD}/\|(\mathbf{I}_N - \mathbf{P}_{RE})\mathbf{h}_{RD}\|$ and $\mathbf{h}_{SR}(i)$ represents the ith element of the vector $\mathbf{h}_{SR}$. The above inequality further yields

$$P_s \geq \frac{P_0|\tilde{\mathbf{w}}^{\dagger}\mathbf{h}_{RD}|^2}{|\tilde{\mathbf{w}}^{\dagger}\mathbf{h}_{RD}|^2 + |\mathbf{h}_{SR}(i)|^2 - |h_{SD}|^2} \triangleq P_{\min}^{(i)}. \quad (26)$$

When the source-relay channel is better than the source-destination channel (i.e., $|\mathbf{h}_{SR}(i)| > |h_{SD}|$), the minimal source power required to enable successful decoding at the ith relay is $P_{\min}^{(i)}$.

We first determine the optimal number of relays. Without loss of generality, let us sort the relays such that $P_{\min}^{(1)} \leq P_{\min}^{(2)} \leq \ldots \leq P_{\min}^{(N)}$. Assuming that the first k $(0 \leq k \leq N)$ relays[1] are used, we compute the achievable secrecy rate based on the designed weights and the minimal power $P_{\min}^{(k)}$. Then, we can find the value of k that yields the maximal achievable secrecy rate, i.e., $\arg\max_k R_s(P_{\min}^{(k)})$. It can be shown that the sign of the derivative of $R_s(P_s)$ does not change with P_s. Considering that $R_s(P_{\min}^{(k)}) \geq R_s(P_{\min}^{(k+1)})$, the optimal value of P_s is thus $P_{\min}^{(k)}$.

For the case of one eavesdropper, the secrecy rate is not an elementary function of P_s since the largest eigenvalue of the matrix $\tilde{\mathbf{R}}_{RE}^{-1}\tilde{\mathbf{R}}_{RD}$ depends on P_s. It is in general difficult to obtain a closed-form solution for the optimal P_s. In the following we use a "hill-climbing" algorithm to iteratively reach the solution for P_s. ***Step 0***) Choose an initial value of P_s, e.g., the solution of P_s for the case of multiple eavesdroppers. Compute the corresponding unit-norm weight vector $\tilde{\mathbf{w}} = \mathbf{q}_{\mathrm{df}}$ based on the solution of the problem of (19). ***Step 1***) Fix $\tilde{\mathbf{w}}$, and compute the corresponding P_s and secrecy rate. It can be shown that an inequality similar to (26) needs to be satisfied, and a similar procedure leading to the solution for the case of multiple eavesdroppers can be used to compute P_s under a fixed $\tilde{\mathbf{w}}$. Update P_s if the computed P_s yields a higher secrecy rate. ***Step 2***) Fix P_s, and compute $\tilde{\mathbf{w}}$ by using the solution for the problem in (19). Update $\tilde{\mathbf{w}}$ if the computed $\tilde{\mathbf{w}}$ yields higher secrecy rate. ***Step 3***) Repeat steps 1)–2) until the secrecy rate cannot be improved further, or a predefined number of iterations has been reached.

In our numerical experiments, the iterative algorithm always converges to a globally optimal solution under the initial value suggested above. In theory, however, the iterative algorithm might lead to a local optimum. In that case, the random search algorithm that will be presented in Section IV-B-2 could be used to overcome this problem.

[1] $k = 0$ corresponds to the case of direct transmission and $P_{\min}^{(0)} = P_0$.

B. Amplify-and-Forward

The AF scheme is equivalent to a 1×2 SIMO system. Let us define the $N \times N$ matrices $\mathbf{R}_{\mathrm{a}} = \mathbf{a}\mathbf{a}^{\dagger}$ and $\mathbf{U} = \mathrm{diag}\{\mathbf{h}_{RD}^{*}\} \cdot \mathrm{diag}\{\mathbf{h}_{RD}\}$. From (3) and (6), the rate at the destination is

$$R_d = \frac{1}{2}\log\left(\alpha + \frac{\mathbf{w}^{\dagger}\mathbf{R}_{\mathrm{a}}\mathbf{w}}{(\mathbf{w}^{\dagger}\mathbf{U}\mathbf{w}+1)\sigma^2}\right). \tag{27}$$

1) Relay Weight Optimization:

- **One eavesdropper**: In case of one eavesdropper, the matrix $\mathbf{B}$ in (7) becomes a vector, which we denote by $\mathbf{b}$. Let us define the $N \times N$ matrices $\mathbf{R}_{\mathrm{b}} = \mathbf{b}\mathbf{b}^{\dagger}$ and $\mathbf{V} = \mathrm{diag}\{\mathbf{h}_{RE}^{*}\} \cdot \mathrm{diag}\{\mathbf{h}_{RE}\}$. The rate at the eavesdropper is

$$R_e = \frac{1}{2}\log\left(\beta + \frac{\mathbf{w}^{\dagger}\mathbf{R}_{\mathrm{b}}\mathbf{w}}{(\mathbf{w}^{\dagger}\mathbf{V}\mathbf{w}+1)\sigma^2}\right). \tag{28}$$

The secrecy rate is

$$R_s(\mathbf{w}, P_s) = \frac{1}{2}\log\left(\alpha + \frac{\mathbf{w}^{\dagger}\mathbf{R}_{\mathrm{a}}\mathbf{w}}{(\mathbf{w}^{\dagger}\mathbf{U}\mathbf{w}+1)\sigma^2}\right) - \frac{1}{2}\log\left(\beta + \frac{\mathbf{w}^{\dagger}\mathbf{R}_{\mathrm{b}}\mathbf{w}}{(\mathbf{w}^{\dagger}\mathbf{V}\mathbf{w}+1)\sigma^2}\right). \tag{29}$$

One can show that the transmit power of Stage 2 is $\mathbb{E}\{\|\mathrm{diag}\{\mathbf{y}_r\}\mathbf{w}\|^2\} = \mathbf{w}^{\dagger}\mathbf{T}\mathbf{w}$ where $\mathbf{T} \triangleq P_s \cdot \mathrm{diag}\{\mathbf{h}_{SR}^{*}\} \cdot \mathrm{diag}\{\mathbf{h}_{SR}\} + \sigma^2\mathbf{I}_N$. The optimization problem of the secrecy rate maximization can be readily formulated as

$$\begin{aligned} &\arg\max_{\mathbf{w}} \frac{\mathbf{w}^{\dagger}\widetilde{\mathbf{V}}\mathbf{w}}{\mathbf{w}^{\dagger}\widetilde{\mathbf{U}}\mathbf{w}} \cdot \frac{\mathbf{w}^{\dagger}\widetilde{\mathbf{R}}_{\mathrm{a}}\mathbf{w}}{\mathbf{w}^{\dagger}\widetilde{\mathbf{R}}_{\mathrm{b}}\mathbf{w}} \\ &\text{s.t.} \mathbf{w}^{\dagger}\mathbf{T}\mathbf{w} = P_0 - P_s \end{aligned} \tag{30}$$

where $\widetilde{\mathbf{U}} = \mathbf{U} + (P_0 - P_s)^{-1}\mathbf{T}$, $\widetilde{\mathbf{V}} = \mathbf{V} + (P_0 - P_s)^{-1}\mathbf{T}$, $\widetilde{\mathbf{R}}_{\mathrm{a}} = \mathbf{R}_{\mathrm{a}} + \alpha\sigma^2\widetilde{\mathbf{U}}$ and $\widetilde{\mathbf{R}}_{\mathrm{b}} = \mathbf{R}_{\mathrm{b}} + \beta\sigma^2\widetilde{\mathbf{V}}$. Note that $\widetilde{\mathbf{U}}$ and $\widetilde{\mathbf{V}}$ are diagonal. The objective function in (30) is a product of two correlated generalized eigenvector problems, and this problem is thus in general a difficult one. To simplify the analysis, in the following we derive the (suboptimal) weights that maximize the upper and lower bounds of the objective function in (30) instead.

Note that the maximum and minimum of $\mathbf{w}^{\dagger}\widetilde{\mathbf{V}}\mathbf{w}/\mathbf{w}^{\dagger}\widetilde{\mathbf{U}}\mathbf{w}$ correspond to the maximal eigenvalue $\lambda_{\max}$ and the minimal eigenvalue $\lambda_{\min}$ of the matrix $\widetilde{\mathbf{U}}^{-1}\widetilde{\mathbf{V}}$, respectively [36]. As the matrix $\widetilde{\mathbf{U}}^{-1}\widetilde{\mathbf{V}}$ is diagonal, we can readily show that

$$\lambda_{\max} = \max_i \left(\frac{P_s|\mathbf{h}_{SR}(i)|^2 + (P_0 - P_s)|\mathbf{h}_{RD}(i)|^2 + \sigma^2}{P_s|\mathbf{h}_{SR}(i)|^2 + (P_0 - P_s)|\mathbf{h}_{RE}(i)|^2 + \sigma^2}\right) \tag{31}$$

and

$$\lambda_{\min} = \min_i \left(\frac{P_s|\mathbf{h}_{SR}(i)|^2 + (P_0 - P_s)|\mathbf{h}_{RD}(i)|^2 + \sigma^2}{P_s|\mathbf{h}_{SR}(i)|^2 + (P_0 - P_s)|\mathbf{h}_{RE}(i)|^2 + \sigma^2}\right). \tag{32}$$

Then, the objective function in (30) is lower and upper bounded as

$$\lambda_{\min}\frac{\mathbf{w}^{\dagger}\widetilde{\mathbf{R}}_{\mathrm{a}}\mathbf{w}}{\mathbf{w}^{\dagger}\widetilde{\mathbf{R}}_{\mathrm{b}}\mathbf{w}} \le \frac{\mathbf{w}^{\dagger}\widetilde{\mathbf{V}}\mathbf{w}}{\mathbf{w}^{\dagger}\widetilde{\mathbf{U}}\mathbf{w}} \cdot \frac{\mathbf{w}^{\dagger}\widetilde{\mathbf{R}}_{\mathrm{a}}\mathbf{w}}{\mathbf{w}^{\dagger}\widetilde{\mathbf{R}}_{\mathrm{b}}\mathbf{w}} \le \lambda_{\max}\frac{\mathbf{w}^{\dagger}\widetilde{\mathbf{R}}_{\mathrm{a}}\mathbf{w}}{\mathbf{w}^{\dagger}\widetilde{\mathbf{R}}_{\mathrm{b}}\mathbf{w}}. \tag{33}$$

Finally, the weight vector that maximizes the lower or upper bound in (33) is $\mu\mathbf{q}_{\mathrm{af}}$ where $\mathbf{q}_{\mathrm{af}}$ is the unit-norm eigenvector of the matrix $\widetilde{\mathbf{R}}_{\mathrm{b}}^{-1}\widetilde{\mathbf{R}}_{\mathrm{a}}$ corresponding to its largest eigenvalue, and μ is a scalar chosen to satisfy the power constraint, and equals

$$\mu = \sqrt{\frac{P_0 - P_s}{(\mathbf{q}_{\mathrm{af}})^{\dagger}\mathbf{T}\mathbf{q}_{\mathrm{af}}}}. \tag{34}$$

Remark: The above suboptimal solution works well in the case of $\lambda_{\max} \approx \lambda_{\min}$. The possible scenarios include i) the channel amplitudes between the eavesdropper and relays are approximately the same as those between the destination and relays, i.e., $|\mathbf{h}_{RD}(i)| \approx |\mathbf{h}_{RE}(i)|$ for $i = 1, \ldots, N$; ii) the signal power at the relay is much greater than the signal power at the destination, i.e., $P_s|\mathbf{h}_{SR}(i)|^2 \gg (P_0 - P_s)|\mathbf{h}_{RD}(i)|^2$ and $P_s|\mathbf{h}_{SR}(i)|^2 \gg (P_0 - P_s)|\mathbf{h}_{RE}(i)|^2$ for $i = 1, \ldots, N$. In these cases, the bounds in (33) are tight and the above solution that maximizes the bounds of the secrecy rate is near-optimal. For other cases, the above suboptimal solution may not perform well and the solution proposed in the following could be used instead.

- **Multiple eavesdroppers**: For multiple eavesdroppers, we propose to completely null out signals at all eavesdroppers in Stage 2 (similarly as in the DF scheme). To null the signals at all eavesdroppers, we need $\mathbf{B}^{\dagger}\mathbf{w} = \mathbf{0}_{J\times 1}$ and also the condition $N > J$.

  The problem of secrecy rate maximization can then be formulated as

$$\begin{aligned} &\arg\max_{\mathbf{w}} \frac{\mathbf{w}^{\dagger}\mathbf{R}_{\mathrm{a}}\mathbf{w}}{\mathbf{w}^{\dagger}\mathbf{U}\mathbf{w}+1} \\ &\text{s.t.} \begin{cases} \mathbf{B}^{\dagger}\mathbf{w} = \mathbf{0}_{J\times 1} \\ \mathbf{w}^{\dagger}\mathbf{T}\mathbf{w} = P_0 - P_s. \end{cases} \end{aligned} \tag{35}$$

Let us define the matrix $\mathbf{F}$ to contain the orthogonal vectors that form the basis of the null space of $\mathbf{B}^{\dagger}$, i.e., the right singular vectors corresponding to zero singular values of $\mathbf{B}^{\dagger}$. To satisfy the first constraint in (35), $\mathbf{w}$ should be a linear combination of the basis of the null space of $\mathbf{B}^{\dagger}$, i.e., $\mathbf{w} = \mathbf{F}\mathbf{v}$, where $\mathbf{v}$ is a column vector. Then, the optimization problem in (35) is equivalent to

$$\begin{aligned} &\arg\max_{\mathbf{v}} \frac{\mathbf{v}^{\dagger}\mathbf{F}^{\dagger}\mathbf{R}_{\mathrm{a}}\mathbf{F}\mathbf{v}}{\mathbf{v}^{\dagger}\mathbf{F}^{\dagger}\mathbf{U}\mathbf{F}\mathbf{v}+1} \\ &\text{s.t. } \mathbf{v}^{\dagger}\mathbf{F}^{\dagger}\mathbf{T}\mathbf{F}\mathbf{v} = P_0 - P_s \end{aligned} \tag{36}$$

which is also a generalized eigenvector problem. The solution of (36) is then $\mathbf{v} \propto \mathbf{q}'_{\mathrm{af}}$ where $\mathbf{q}'_{\mathrm{af}}$ is the unit-norm eigenvector of the matrix $\mathbf{F}^{\dagger}[\mathbf{U} + (P_0 - P_s)^{-1}\mathbf{T}]^{-1}\mathbf{F}\mathbf{F}^{\dagger}\mathbf{R}_{\mathrm{a}}\mathbf{F}$ corresponding to its largest eigenvalue. Finally, the solution of (35) is $\mathbf{w} = \mu\mathbf{F}\mathbf{q}'_{\mathrm{af}}$ where

$$\mu = \sqrt{\frac{P_0 - P_s}{(\mathbf{q}'_{\mathrm{af}})^{\dagger}\mathbf{F}^{\dagger}\mathbf{T}\mathbf{F}\mathbf{q}'_{\mathrm{af}}}}. \tag{37}$$

2) Selection of Source Power: The secrecy rate based on the designed weights is in general not a simple function of P_s, and a closed-form expression for the optimal P_s is difficult to obtain.

For the case of multiple eavesdroppers, an iterative algorithm similar to that in Section IV-A-2 can be used to reach the solu-

tion. In the step of computing P_s under a fixed weight vector, the secrecy rate can be written as

$$R_s(P_s) = \log\left(\frac{e_0 + e_1 P_s + e_2 (P_s)^2}{f_0 + f_1 P_s + f_2 (P_s)^2}\right) \tag{38}$$

where e_i and f_i are coefficients independent of P_s. Taking the derivative of $2^{R_s(P_s)}$ and setting it to zero, the optimal value of P_s is the solution within $(0, P_0]$ of the quadratic equation

$$(e_1 f_2 - e_2 f_1)(P_s)^2 + (2e_0 f_2 - 2e_2 f_0) P_s + (e_0 f_1 - e_1 f_0) = 0. \tag{39}$$

In case no solution for (39) exists within $(0, P_0]$, $P_s = P_0$ which corresponds to the case of direct transmission.

For the case of one eavesdropper, we can use the solution for multiple eavesdroppers as the initial value and use a conventional local random search algorithm [39] to improve it. The procedure is summarized as follows. *Step 0*) Initialize the algorithm by setting an initial value of $P_s^{(0)}$, e.g., the solution for the case of multiple eavesdroppers. *Step 1*) In the ith iteration, generate a random perturbation δ_i (e.g., a zero-mean Gaussian random variable). Update the power $P_s^{(i)} = P_s^{(i-1)} + \delta_i$, if the secrecy rate under $P_s^{(i-1)} + \delta_i$ is greater than the secrecy rate under $P_s^{(i-1)}$. Otherwise, keep the same power, i.e., $P_s^{(i)} = P_s^{(i-1)}$. *Step 2*) Repeat Step 1) until a predefined number of iterations is reached or the secrecy rate cannot be improved further.

C. Cooperative Jamming

From (8), the rate at the destination is

$$R_d = \log\left(1 + \frac{P_s |h_{SD}|^2}{\mathbf{w}^\dagger \mathbf{R}_{RD} \mathbf{w} + \sigma^2}\right). \tag{40}$$

1) Relay Weight Optimization:

- **One eavesdropper**: From (9) the rate at the eavesdropper is

$$R_e = \log\left(1 + \frac{P_s |h_{SE}|^2}{\mathbf{w}^\dagger \mathbf{R}_{RE} \mathbf{w} + \sigma^2}\right). \tag{41}$$

From (40) and (41), the secrecy rate is

$$R_s(\mathbf{w}, P_s) = \log\left(1 + \frac{P_s |h_{SE}|^2}{\mathbf{w}^\dagger \mathbf{R}_{RD} \mathbf{w} + \sigma^2}\right) - \log\left(1 + \frac{P_s |h_{SE}|^2}{\mathbf{w}^\dagger \mathbf{R}_{RE} \mathbf{w} + \sigma^2}\right) \tag{42}$$

which is a product of two correlated generalized eigenvector problems and in general is quite difficult. To simplify the analysis, we will add one more constraint to completely null out the jamming signal at the destination, i.e., $\mathbf{h}_{RD}^\dagger \mathbf{w} = 0$.
Then, the problem of secrecy rate maximization can be formulated as

$$\arg\max_{\mathbf{w}} \left|\mathbf{w}^\dagger \mathbf{h}_{RE}\right|^2 \quad \text{s.t.} \begin{cases} \mathbf{w}^\dagger \mathbf{h}_{RD} = 0 \\ \mathbf{w}^\dagger \mathbf{w} = P_0 - P_s \end{cases} \tag{43}$$

which is of the same form as (23). Based on (24), it can be readily shown that the solution of (43) is given by

$$\mathbf{w} = \mu \|\mathbf{h}_{RD}\|^2 \mathbf{h}_{RE} - \mu \mathbf{h}_{RD}^\dagger \mathbf{h}_{RE} \mathbf{h}_{RD} \tag{44}$$

where the scalar μ is given by

$$\mu = \sqrt{\frac{P_0 - P_s}{\|\mathbf{h}_{RD}\|^4 \|\mathbf{h}_{RE}\|^2 - \|\mathbf{h}_{RD}\|^2 \left|\mathbf{h}_{RD}^\dagger \mathbf{h}_{RE}\right|^2}}. \tag{45}$$

Notice that a similar problem was discussed in [7], while a different scenario was considered in [7], i.e., the relay-eavesdropper channel is unavailable.

- **Multiple eavesdroppers**: We still propose to completely null the jamming signal at the destination, i.e., $\mathbf{h}_{RD}^\dagger \mathbf{w} = 0$. Then, the secrecy rate becomes

$$R_s = \log\left(1 + \frac{P_s |h_{SD}|^2}{\sigma^2}\right) - \max_j \left\{\log\left(1 + \frac{P_s \left|\mathbf{h}_{SE}(j)\right|^2}{\left|\mathbf{w}^\dagger \mathbf{H}_{RE}(:, j)\right|^2 + \sigma^2}\right)\right\} \tag{46}$$

where $\mathbf{H}_{RE}(:, j)$ denotes the jth column of the matrix $\mathbf{H}_{RE}$.
The problem of achievable secrecy rate maximization can be formulated as

$$\max_{\mathbf{w}} \min_j \frac{\left|\mathbf{w}^\dagger \mathbf{H}_{RE}(:, j)\right|^2 + \sigma^2}{\left|\mathbf{h}_{SE}(j)\right|^2} \quad \text{s.t.} \begin{cases} \mathbf{w}^\dagger \mathbf{h}_{RD} = 0 \\ \mathbf{w}^\dagger \mathbf{w} = P_0 - P_s. \end{cases} \tag{47}$$

A closed-form solution of the max-min problem in (47) is in general difficult to obtain. A suboptimal solution can be chosen as the one that yields the highest secrecy rate among the following J solutions: use (44) to find the J solutions in the presence of the jth eavesdropper only, for $j = 1, \ldots, J$, respectively (i.e., assume one single eavesdropper and ignore the other $J - 1$ eavesdroppers). The local random search algorithm (as mentioned in Section IV-B-2) could be used to further improve the corresponding weights.

2) Selection of Source Power: For the cases of one eavesdropper, it can be shown that the secrecy rate is of the following form:

$$R_s(P_s) = \log\left(\frac{e_0 + e_1 P_s + e_2 (P_s)^2}{f_0 + f_1 P_s}\right). \tag{48}$$

Thus, the optimal value of P_s is the solution within $(0, P_0]$ of the quadratic equation

$$e_2 f_1 (P_s)^2 + 2 e_2 f_0 P_s + (e_1 f_0 - e_0 f_1) = 0. \tag{49}$$

In case no solution exists within $(0, P_0]$, it holds that $P_s = P_0$.

For the case of multiple eavesdroppers, an iterative algorithm similar to that in Section IV-A-2 can be used to reach the solution. When computing P_s under a fixed unit-norm weight vector, the secrecy rate is of the same form as in (49).

D. Inequality Constraint

Thus far our focus is on optimization problems subject to equality constraints. In the following, we show that the inequality constraint, i.e., the total transmit power is no greater

than P_0, is actually equivalent to the equality constraint in term of the resulting solutions.

Let us first consider the DF scheme in which the relays use the same codewords as the source. We first consider the case of multiple eavesdroppers which is easier to deal with. From (24), it is easy to see that the secrecy rate is a monotonically increasing function of the transmit power P_0. Thus, the equality power constraint is equivalent to the inequality constraint.

For the case of one eavesdropper we discuss two cases and prove by contradiction that inequality and equality constraints are equivalent. Let us assume that $\hat{P}_s \leq P_0$ is the optimal power of the source in Stage 1, $\hat{P}_r < P_0 - \hat{P}_s$ is the optimal power of relays in Stage 2, and $\hat{\mathbf{w}}$ is the corresponding weight vector.

Case 1) $|h_{SD}| \leq |h_{SE}|$. Here, it holds that $\alpha \leq \beta$. Recalling that $\hat{P}_s + \hat{P}_r < P_0$, we can always find a scalar $\rho > 1$ such that the higher power in Stage 2, $\rho\hat{P}_r = P_0 - P_s$ (corresponding to the weight vector $\sqrt{\rho} \cdot \hat{\mathbf{w}}$), yields higher secrecy rate, because one can easily show that

$$\frac{dR_s(\rho)}{d\rho} \propto \beta\hat{\mathbf{w}}^\dagger \mathbf{R}_{RD}\hat{\mathbf{w}} - \alpha(\hat{\mathbf{w}})^\dagger \mathbf{R}_{RE}\hat{\mathbf{w}}^\dagger > 0 \quad (50)$$

where R_s is given by (17). This contradicts our assumption on the optimality of $\hat{P}_r$.

Case 2) $|h_{SD}| > |h_{SE}|$. Here, it holds that $\alpha > \beta$. We can always find a scalar $\rho > 1$ such that the higher transmit power in Stage 1, $\rho\hat{P}_s = P_0 - \hat{P}_r$, yields a higher secrecy rate. This contradicts our assumption on the optimality of $\hat{P}_s$.

Therefore, the equality and inequality constraints are equivalent for DF.

A similar procedure can be used to show that the inequality constraint is equivalent to the equality constraint in AF as well. We can also prove the same for CJ: if for CJ the equality and inequality constraints were not equivalent, the optimal weights could be scaled up to satisfy the constraint with equality, thereby increasing the secrecy rate and contradicting the optimality.

V. Design for Transmit Power Minimization

In this section, we consider the objective of designing the system for the cooperative schemes to minimize the total transmit power $P(\mathbf{w}, P_s)$ for an achievable secrecy rate constraint R_s^0. Again, we first fix the source power P_s, obtain the weight vector $\mathbf{w}$ to minimize the total power of relays, and then find the optimal value of P_s. As will be seen, a higher transmit power always yields a higher achievable secrecy rate, so the equality and inequality secrecy rate constraints are equivalent.

A. Decode-and-Forward

1) Relay Weight Optimization:

- **One eavesdropper**: For one eavesdropper, the optimization problem of minimizing the transmit power in Stage 2 can be formulated as

$$\begin{aligned} &\arg\min_{\mathbf{w}} \mathbf{w}^\dagger\mathbf{w} \\ &\text{s.t.} \frac{\alpha\sigma^2 + \mathbf{w}^\dagger\mathbf{R}_{RD}\mathbf{w}}{\beta\sigma^2 + \mathbf{w}^\dagger\mathbf{R}_{RE}\mathbf{w}} = 4^{R_s^0}. \end{aligned} \quad (51)$$

Then, (51) can be further rewritten as

$$\begin{aligned} &\arg\min_{\mathbf{w}} \mathbf{w}^\dagger\mathbf{w} \\ &\text{s.t. } \mathbf{w}^\dagger\widetilde{\mathbf{R}}\mathbf{w} = \zeta \end{aligned} \quad (52)$$

where

$$\widetilde{\mathbf{R}} = \mathbf{R}_{RD} - 4^{R_s^0}\mathbf{R}_{RE} \quad (53)$$

and

$$\zeta = \sigma^2\left(4^{R_s^0}\beta - \alpha\right). \quad (54)$$

Note that if R_s^0 is chosen such that $\zeta > 0 (< 0)$ but $\widetilde{\mathbf{R}}$ is negative (positive) definite, then the optimization problem in (52) will be infeasible, and the transmit power in Stage 2 is zero. A similar optimization problem was analyzed in [40]. Without loss of generality, let us first assume that $\zeta > 0$ and $\widetilde{\mathbf{R}}$ is positive definite. By using the method of Lagrange multipliers, we obtain

$$\widetilde{\mathbf{R}}\mathbf{w} = \frac{1}{\lambda}\mathbf{w} \quad (55)$$

where λ is the Lagrange multiplier. One can see that the optimal weights should be chosen as one of the eigenvectors of the matrix $\widetilde{\mathbf{R}}$ and $1/\lambda$ is the corresponding eigenvalue. Multiplying both sides of (55) with $\lambda\mathbf{w}^\dagger$ yields

$$\mathbf{w}^\dagger\mathbf{w} = \lambda\mathbf{w}^\dagger\widetilde{\mathbf{R}}\mathbf{w} = \lambda\zeta. \quad (56)$$

Then, minimizing $\mathbf{w}^\dagger\mathbf{w}$ is equivalent to minimizing λ, so $1/\lambda$ corresponds to the largest eigenvalue of $\widetilde{\mathbf{R}}$, and thus $\mathbf{w}$ should be the largest eigenvector of $\widetilde{\mathbf{R}}$. Finally, the solution of (51) is given by $\mu\mathbf{q}'_{\text{df}}$ where $\mathbf{q}'_{\text{df}}$ is the unit-norm eigenvector corresponding to the largest eigenvalue of $\widetilde{\mathbf{R}}$ and the scalar μ here is

$$\mu = \sqrt{\frac{\zeta}{(\mathbf{q}'_{\text{df}})^\dagger\widetilde{\mathbf{R}}\mathbf{q}'_{\text{df}}}}. \quad (57)$$

Similarly, if $\zeta < 0$ and $\widetilde{\mathbf{R}}$ is negative definite, the solution would correspond to the unit-norm eigenvector associated with the smallest eigenvalue of $\widetilde{\mathbf{R}}$.

- **Multiple eavesdroppers**: Recall that for multiple eavesdroppers we propose to completely null out signals at all eavesdroppers in Stage 2. The optimization problem of transmit power minimization can be formulated as

$$\begin{aligned} &\arg\min_{\mathbf{w}} \|\mathbf{w}\|^2 \\ &\text{s.t.} \begin{cases} \mathbf{w}^\dagger\mathbf{H}_{RE} = \mathbf{0}_{1\times J} \\ \mathbf{w}^\dagger\mathbf{h}_{RD} = \sqrt{\max_j \zeta_j} \end{cases} \end{aligned} \quad (58)$$

where $\zeta_j = \sigma^2(4^{R_s^0}\beta_j - \alpha)$.

In the above, without loss of generality we have assumed that $\mathbf{w}^\dagger\mathbf{h}_{RD}$ is a positive real number. This is because the transmit power remains the same when the weight vector $\mathbf{w}$

is rotated by an arbitrary phase. In case that $\max\{\zeta_j\} \leq 0$, the transmit power in Stage 2 is zero.

Defining the $(J+1)\times N$ matrix $\hat{\mathbf{H}} = [\mathbf{h}_{RD}, \mathbf{H}_{RE}]^\dagger$ and the $(J+1)\times 1$ vector $\mathbf{e} = [1, \mathbf{0}_{1\times J}]^T$, we can rewrite the constraints in (58) as $\tilde{\mathbf{H}}\mathbf{w} = \sqrt{\max \zeta_j}\cdot \mathbf{e}$. To guarantee a non-zero solution for $\mathbf{w}$, the condition $N > J$ is needed. The optimal solution that minimizes the transmit power corresponds to the least-squares solution produced by the pseudo-inverse of $\widetilde{\mathbf{H}}$ [41], i.e.,

$$\mathbf{w} = \sqrt{\max_j \zeta_j}\cdot \widetilde{\mathbf{H}}^\dagger (\widetilde{\mathbf{H}}\widetilde{\mathbf{H}}^\dagger)^{-1}\mathbf{e}. \tag{59}$$

2) Selection of Source Power: Recall that the ith relay can correctly decode the source message if the rate at the ith relay is no less than the rate at the destination. Let us first consider the case of multiple eavesdroppers in which the weights are designed by (59). For the ith relay, it holds that

$$\frac{1}{2}\log\left(1+\frac{P_s\left|\mathbf{h}_{SR}(i)\right|^2}{\sigma^2}\right) \geq R_s^0 + \frac{1}{2}\log\left(1+\frac{P_s\cdot\max_j\left\{\left|\mathbf{h}_{SE}(j)\right|^2\right\}}{\sigma^2}\right). \tag{60}$$

The above inequality further yields

$$P_s \geq \frac{\sigma^2\left(4^{R_s^0}-1\right)}{\left|\mathbf{h}_{SR}(i)\right|^2 - 4^{R_s^0}\max_j\left\{\left|\mathbf{h}_{SE}(j)\right|^2\right\}} \triangleq P_{\min}^{(i)}. \tag{61}$$

If $P_{\min}^{(i)} > 0$, the minimum source power to enable successful decoding at the ith relay is $P_{\min}^{(i)}$; otherwise, there does not exist a feasible solution to satisfy the secrecy rate requirement R_s^0.

Without loss of generality, let us sort the relays such that $P_{\min}^{(1)} \leq P_{\min}^{(2)} \leq \ldots \leq P_{\min}^{(N)}$. Assuming that the first k ($0 \leq k \leq N$) relays are used, we compute the total transmit power $P_{\min}^{(i)} + \mathbf{w}^\dagger\mathbf{w}$ based on the designed weights. Then, we can find the value of k that yields the minimal total transmit power, i.e., $\arg\min_k P(P_{\min}^{(k)})$. Also, it is easy to show that the total transmit power is a linear function of P_s, so the sign of the derivative of $P(P_s)$ does not change with P_s. Considering that $P(P_{\min}^{(k)}) \leq P(P_{\min}^{(k+1)})$, the optimal value of P_s is thus $P_{\min}^{(k)}$.

For the case of one eavesdropper, an iterative algorithm similar to that described in Section IV-A-2 can be used to reach the solution of P_s.

B. Amplify-and-Forward

- **One eavesdropper**: As discussed in Section IV-B-1, here we consider the case of $\lambda_{\max} \approx \lambda_{\min}$ which yields a tight upper/lower bound on the secrecy rate. The problem of minimizing the transmit power in Stage 2 can be formulated as

$$\arg\min_{\mathbf{w}} \mathbf{w}^\dagger\mathbf{T}\mathbf{w} \quad \text{s.t.}\ \frac{\mathbf{w}^\dagger(\mathbf{R}_{\mathrm{a}}+\alpha\sigma^2\mathbf{U})\mathbf{w}+\alpha\sigma^2}{\mathbf{w}^\dagger(\mathbf{R}_{\mathrm{b}}+\beta\sigma^2\mathbf{V})\mathbf{w}+\beta\sigma^2} = 4^{R_s^0}. \tag{62}$$

Defining $\mathbf{w} = \mathbf{T}^{-1/2}\tilde{\mathbf{w}}$, the optimization problem in (62) is equivalent to

$$\arg\min_{\tilde{\mathbf{w}}} \tilde{\mathbf{w}}^\dagger\tilde{\mathbf{w}} \quad \text{s.t.}\ \frac{\tilde{\mathbf{w}}^\dagger\mathbf{T}^{-1/2}(\mathbf{R}_{\mathrm{a}}+\alpha\sigma^2\mathbf{U})\mathbf{T}^{-1/2}\tilde{\mathbf{w}}+\alpha\sigma^2}{\tilde{\mathbf{w}}^\dagger\mathbf{T}^{-1/2}(\mathbf{R}_{\mathrm{b}}+\beta\sigma^2\mathbf{V})\mathbf{T}^{-1/2}\tilde{\mathbf{w}}+\beta\sigma^2} = 4^{R_s^0}. \tag{63}$$

- **Multiple eavesdroppers**: The problem of minimizing the transmit power in Stage 2 can be formulated as

$$\arg\min_{\mathbf{w}} \mathbf{w}^\dagger\mathbf{T}\mathbf{w} \quad \text{s.t.}\ \begin{cases}\mathbf{B}^\dagger\mathbf{w} = \mathbf{0}_{J\times 1}\\ \frac{\mathbf{w}^\dagger\mathbf{R}_{\mathrm{a}}\mathbf{w}}{\mathbf{w}^\dagger\mathbf{U}\mathbf{w}+1} = \left(\beta 4^{R_s^0}-\alpha\right)\sigma^2.\end{cases} \tag{64}$$

Recall that $\mathbf{F}$ denotes the matrix containing all of the right singular vectors corresponding to zero singular values of $\mathbf{B}^\dagger$, and $\mathbf{w}$ should be $\mathbf{w} = \mathbf{F}\mathbf{v}$, where $\mathbf{v}$ is a column vector. Defining $\tilde{\mathbf{v}} = (\mathbf{F}^\dagger\mathbf{T}\mathbf{F})^{1/2}\mathbf{v}$, it holds that $\mathbf{w} = \mathbf{F}(\mathbf{F}^\dagger\mathbf{T}\mathbf{F})^{-1/2}\tilde{\mathbf{v}}$, and the optimization problem in (64) is equivalent to

$$\arg\min_{\tilde{\mathbf{v}}} \tilde{\mathbf{v}}^\dagger\tilde{\mathbf{v}} \quad \text{s.t.}\ \frac{\tilde{\mathbf{v}}^\dagger(\mathbf{F}^\dagger\mathbf{T}\mathbf{F})^{-1/2}\mathbf{F}^\dagger\mathbf{R}_{\mathrm{a}}\mathbf{F}(\mathbf{F}^\dagger\mathbf{T}\mathbf{F})^{-1/2}\tilde{\mathbf{v}}}{\tilde{\mathbf{v}}^\dagger(\mathbf{F}^\dagger\mathbf{T}\mathbf{F})^{-1/2}\mathbf{F}^\dagger\mathbf{U}\mathbf{F}(\mathbf{F}^\dagger\mathbf{T}\mathbf{F})^{-1/2}\tilde{\mathbf{v}}+1} = \left(\beta 4^{R_s^0}-\alpha\right)\sigma^2. \tag{65}$$

Notice that (63) and (65) are of the same form as (52), so they can be solved based on the method presented in Section V-A-1. The total transmit power $P(P_s) = P_s + \mathbf{w}^\dagger\mathbf{T}\mathbf{w}$ depends on P_s, but is not an elementary function of P_s. A closed-form expression for optimal P_s is in general difficult to find, so this quantity could be determined by the local random search algorithm as in Section IV-B-2.

C. Cooperative Jamming

We first fix P_s, and find the weights that minimize transmit power of the jamming signal. Then, we find the value of P_s that minimizes the overall transmit power.

- **One eavesdropper**: The problem of minimizing the transmit power of the jamming signal can be formulated as

$$\arg\min_{\mathbf{w}} \|\mathbf{w}\|^2 \quad \text{s.t.}\ \begin{cases}\mathbf{w}^\dagger\mathbf{h}_{RD} = 0\\ \mathbf{w}^\dagger\mathbf{h}_{RE} = \sqrt{\frac{P_s|h_{SE}|^2}{2^{-R_s^0}(1+P_s|h_{SD}|^2/\sigma^2)-1}-\sigma^2}.\end{cases} \tag{66}$$

The problem in (66) is of the same form as (58). Based on (59), the solution of (66) is given by

$$\mathbf{w} = \mu[\mathbf{h}_{RE}\quad \mathbf{h}_{RD}]\begin{bmatrix}\mathbf{h}_{RE}^\dagger\mathbf{h}_{RE} & \mathbf{h}_{RE}^\dagger\mathbf{h}_{RD}\\ \mathbf{h}_{RD}^\dagger\mathbf{h}_{RE} & \mathbf{h}_{RD}^\dagger\mathbf{h}_{RD}\end{bmatrix}^{-1}\begin{bmatrix}1\\0\end{bmatrix} = \mu\|\mathbf{h}_{RD}\|^2\mathbf{h}_{RE} - \mu\mathbf{h}_{RD}^\dagger\mathbf{h}_{RE}\mathbf{h}_{RD} \tag{67}$$

where

$$\mu = \sqrt{\frac{P_s|h_{SE}|^2}{2^{-R_s^0}(1+P_s|h_{SD}|^2/\sigma^2)-1}-\sigma^2}. \tag{68}$$

- **Multiple eavesdroppers**: The problem of minimizing the transmit power of the jamming signal is

$$\min_{\mathbf{w}} ||\mathbf{w}||^2$$
$$\text{s.t.} \begin{cases} \frac{|\mathbf{w}^\dagger \mathbf{H}_{RE}(:,j)|^2+\sigma^2}{|h_{SE}|^2} \\ \quad \geq \frac{P_s}{2^{-R_s^0}(1+P_s|h_{SD}|^2/\sigma^2)-1}, \quad (j=1,\ldots,J) \\ \mathbf{w}^\dagger \mathbf{h}_{RD} = 0. \end{cases} \quad (69)$$

  Similarly as in Section IV-C-1, a suboptimal solution can be chosen as the one that yields the smallest power among the following J solutions: find the J solutions in the presence of the jth single eavesdropper only, for $j = 1, \ldots, J$, respectively. Then, the random search algorithm could be used to further improve this suboptimal solution.

Now we discuss the selection of source power P_s. Similarly as in Section IV-C-2, for the case of one eavesdropper, the total transmit power $P(P_s) = P_s + \mathbf{w}^\dagger \mathbf{w}$ can be represented as a function of P_s:

$$P(P_s) = \frac{e_0 + e_1 P_s + e_2 (P_s)^2}{f_0 + f_1 P_s}. \quad (70)$$

Then, the optimal value of P_s is obtained by solving a quadratic equation of the same form as (49). For the case of multiple eavesdroppers, an iterative algorithm similar to that in Section IV-A-2 can be used to reach the solution of P_s.

VI. Numerical Results

In this section, we investigate the performance of the proposed design algorithms numerically. For simplicity, we consider a simple one-dimensional system model, as illustrated in Fig. 2, in which the source, relays, destination and eavesdroppers are placed along a horizontal line. The source-relay distances are always smaller than the source-destination distance or the source-eavesdropper distance. To highlight the effects of distances, channels between any two nodes are modeled by a simple line-of-sight channel model including the path loss effect and a random phase. For example, $h_{SD} = d_{SD}^{-c/2} e^{j\theta}$ where d_{SD} is the distance between the source and the destination, $c = 3.5$ is the path loss exponent, θ is the random phase uniformly distributed within $[0, 2\pi)$. The distances between relays are assumed to be much smaller than the distances between relays and source/destination, so the path losses between different relays and source/destination are approximately the same. Similarly, the path losses between different eavesdroppers and source/destination/relay are approximately the same as well. The source and destination are located at fixed two-dimensional coordinates (0,0) and (50,0), respectively (unit: meters). The noise power is $\sigma^2 = -60$ dBm. We perform Monte Carlo experiments consisting of 1000 independent trials to obtain the average results.

We first fix the relay location at (25, 0) (i.e., the middle point of source and destination), and move the position of eavesdroppers from (30,0) to (90,0). The achievable secrecy rate is shown Fig. 3 in which the total transmit power constraint is fixed at $P_0 = 0$ dBm. The number of relays is $N = 5$ and the number of eavesdroppers is $J = 2$. As expected, the secrecy rate for DT becomes zero when the destination is at a farther position (to the source) than the eavesdroppers. As observed, when the eavesdroppers move away from the source, the secrecy rate increases

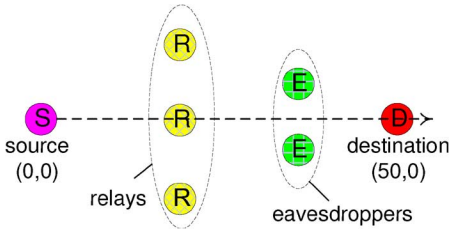


Fig. 2. Model used for numerical experiments.

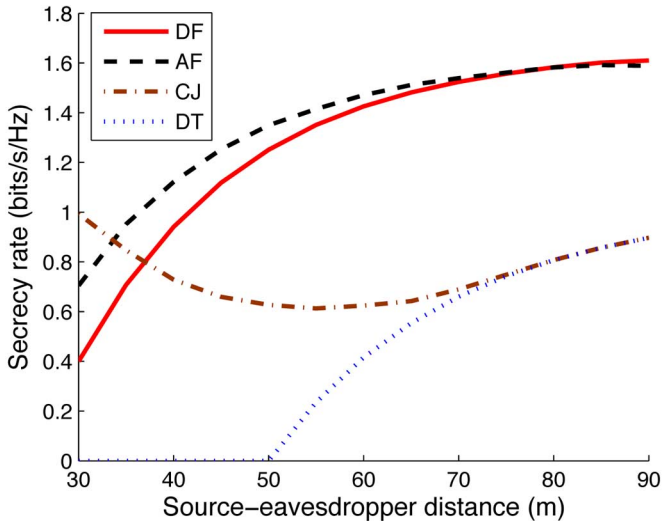


Fig. 3. Secrecy rate versus source-eavesdropper distance. The power constraint is $P_0 = 0$ dBm. The position of eavesdroppers varies from (30,0) to (90,0). The relay location is fixed at (25,0). The number of relays is $N = 5$. The number of eavesdroppers is $J = 2$.

for DF and AF, since the received signal power at the eavesdroppers decreases. Also, one can see that DF does not necessarily perform better than AF, since the optimal source power P_s could be different for DF and AF. For CJ, it is interesting to see that the secrecy rate at first decreases, then increases, and eventually becomes equal to the secrecy rate of DT. The decrease of secrecy rate is because more jamming power is needed for creating larger interference and less power is available for the source to transmit the message signal, when the eavesdroppers move away from the relays. However, when the eavesdroppers are very far from the relays and also the source, we should spend most of the power on transmitting the message signal. In this situation it is not worthy spending a large amount of power on transmitting the jamming signal, since the received power of the message signal at the eavesdropper is always small (regardless of jamming) due to the large path loss. This explains why the secrecy rate could increase. Since DT is a special case of CJ for $P_s = P_0$, the performance of CJ is no worse than that of DT.

In Fig. 4, we fix the eavesdropper location at (60, 0), and move the position of the relays from (5,0) to (45,0). All other parameters are the same as those used in Fig. 3. As expected, the secrecy rate of DT is independent of the relay location. When the relays move away from the source, the secrecy rate for DF or AF first increases and then decreases, and there is an optimal relay location somewhere between source and destination. When the relays are close to the source, DF performs better than AF; otherwise, AF performs better. The secrecy rate of CJ, on the other

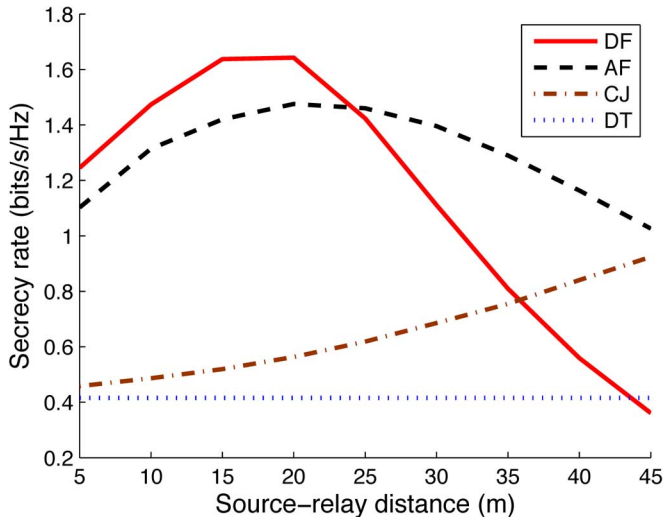


Fig. 4. Secrecy rate versus source-relay distance. The power constraint is $P_0 = 0$ dBm. The position of relays varies from (5,0) to (45,0). The eavesdropper location is fixed at (60,0). The number of relays is $N = 5$. The number of eavesdroppers is $J = 2$.

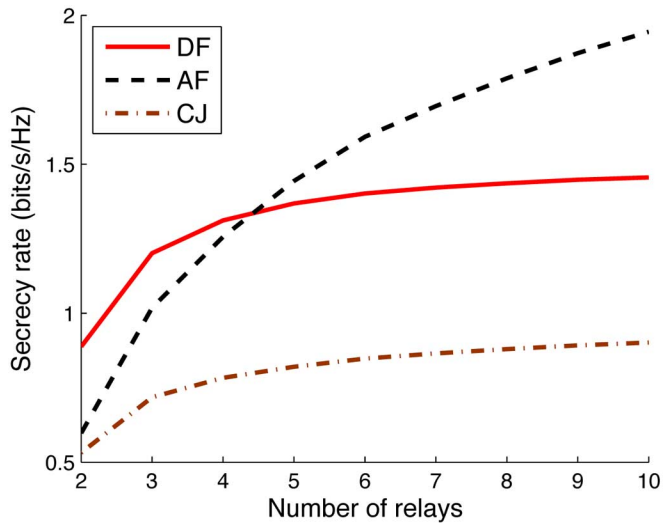


Fig. 5. Secrecy rate versus number of relays. The power constraint is $P_0 = 0$ dBm. The relay location is fixed at (25,0). The eavesdropper location is fixed at (40,0). The number of eavesdropper is $J = 1$.

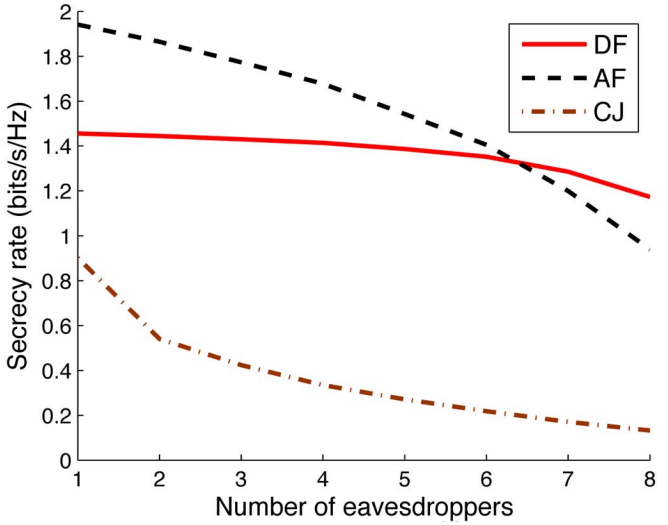


Fig. 6. Secrecy rate versus number of eavesdroppers. The power constraint is $P_0 = 0$ dBm. The relay location is fixed at (25,0). The eavesdropper location is fixed at (40,0). The number of relays is $N = 10$.

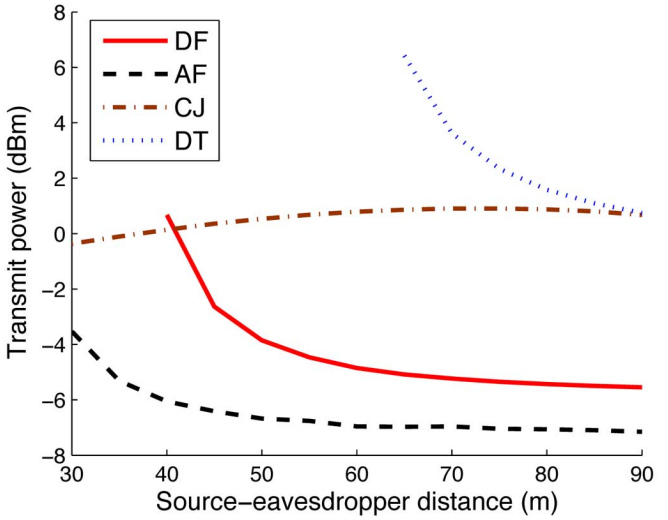


Fig. 7. Transmit power versus source-eavesdropper distance. The secrecy rate constraint is $R_s^0 = 1$ bits/s/Hz. The position of eavesdroppers varies from (30,0) to (90,0). The relay location is fixed at (25,0). The number of relays is $N = 10$. The number of eavesdroppers is $J = 3$.

hand, monotonically increases as the relays move close to the eavesdroppers, since the received jamming power at eavesdroppers is higher for a smaller relay-eavesdropper distance.

Figs. 5 shows the secrecy rate for different numbers of relays. The relay location is fixed at (25,0), the eavesdropper location is fixed at (40,0), and the number of eavesdroppers is $J = 1$. Increasing the number of relays improves the secrecy rate. The curve for DT is not shown, as the destination is at a farther position than the eavesdropper and the secrecy rate is always zero. Fig. 6 shows the secrecy rate performance for different numbers of eavesdroppers. As expected, the secrecy rate becomes smaller as the number of eavesdroppers increases.

Fig. 7 shows the performance of transmit power for different source-eavesdropper distances, in which the secrecy rate constraint is fixed at $R_s^0 = 1$ bits/s/Hz and the relay location is fixed at (25,0). The number of relays is $N = 10$. The number of eavesdroppers is $J = 3$. The curve for DT is shown only for the feasible ranges. For DF, when the source-eavesdropper distance is small, the condition in (61) may not be satisfied, so the curve is not drawn for such situations. Fig. 8 shows the transmit power versus source-relay distances, in which the eavesdropper location is fixed at (60,0). For DT in this configuration, the required secrecy rate cannot be achieved no matter how large the transmit power is, so the curve for DT is not drawn. The curves in Figs. 7 and 8 exhibit similar characteristics to Figs. 3 and 4, therefore detailed discussions are omitted.

VII. Conclusions and Future Work

In this paper, we have proposed to use cooperating relays to improve the performance of secure wireless communications

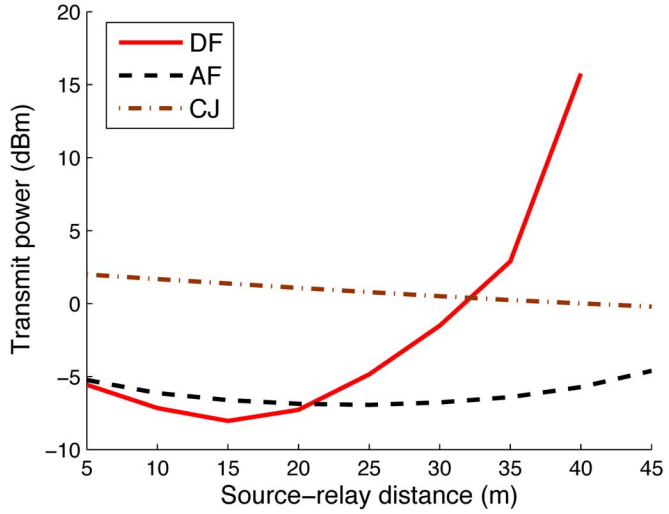


Fig. 8. Transmit power versus source-relay distance. The secrecy rate constraint is $R_s^0 = 1\,\mathrm{bits/s/Hz}$. The position of relays varies from (5,0) to (45,0). The eavesdropper location is fixed at (60,0). The number of relays is $N = 10$. The number of eavesdroppers is $J = 3$.

in the presence of one or more eavesdroppers. Three cooperative schemes have been considered: decode-and-forward, amplify-and-forward and cooperative jamming. We have considered two practical design problems, i.e., allocate transmit power at source and relays and determine the relay weights, to maximize the achievable secrecy rate subject to a transmit power constraint, or minimize the total transmit power subject to a secrecy rate constraint. We have proposed designs for one and more eavesdroppers. We have shown via analyses and numerical evaluations that cooperation can overcome the traditional limitation on channel conditions and significantly improve the system performance, as compared to direct transmission without cooperation.

Areas that warrant further research include performance degradation in the presence of imperfect channel estimates, and optimization based on partial channel knowledge only, e.g., only statistical information about the eavesdropper's channels is available, or each relay knows its own channel only. In those cases, other metrics such as ergodic secrecy rate, or outage probability could be employed. Also, design under alternative network scenarios would be of interest, such as scenarios where there is only one relay equipped with multiple antennas, or there is a single eavesdropper equipped with multiple antennas. These cases do not constitute a trivial extension of the work in this paper, as the optimization problems involved are significantly different. Moreover, recall that for the DF and AF schemes in the case of multiple eavesdroppers we have assumed that the number of relays is greater than the number of eavesdroppers, so that the relays' transmitted signals can be nulled at all eavesdroppers. Further study is needed for the case in which the number of relays is no greater than the number of eavesdroppers.

ACKNOWLEDGMENT

The authors are indebted to the associate editor and the anonymous reviewers for their insightful comments and suggestions. The paper was significantly strengthened because of their inputs.

REFERENCES

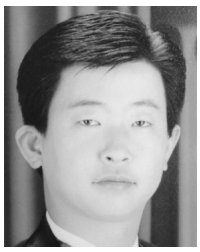
[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, Jul. 1978.
[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.
[4] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*. Delft, The Netherlands: Now Publishers, 2009.
[5] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.
[6] 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.
[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] 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.
[9] T. Liu and S. Shamai, "A note on the secrecy capacity of the multi-antenna wiretap channel," *IEEE Trans. Inf. Theory,* Nov. 2007 [Online]. Available: http://arxiv.org/abs/0710.4105, submitted for publication.
[10] 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.
[11] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Conf. Information Sciences Systems*, Baltimore, MD, Mar. 2007.
[12] 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.
[13] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Computing*, Monticello, IL, Sep.–Oct. 2008.
[14] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Taipei, Taiwan, Apr. 2009.
[15] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proc. IEEE Statistical Signal Processing Workshop*, Cardiff, Wales, U.K., Aug.–Sep. 2009.
[16] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: Interaction between source, eavesdropper and friendly jammer," *EURASIP J. Wireless Commun. Netw. (Special Issue on Wireless Physical Layer Security)*, vol. 2009, Jun. 2009.
[17] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3062–3080, Dec. 2004.
[18] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity—Part I: System description," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927–1938, Nov. 2003.
[19] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation in diversity—Part II: Implementation aspects and performance analysis," *IEEE Trans. Commun.*, vol. 51, pp. 1939–1948, Nov. 2003.
[20] Z. Han and H. V. Poor, "Lifetime improvement in wireless sensor networks via collaborative beamforming and cooperative transmission," *IET Proc. Microwaves, Antennas, Propagation (Special Issue on Antenna Systems and Propagation for Future Wireless Communications)*, vol. 1, no. 6, pp. 1103–1110, Dec. 2007.
[21] Z. Han and K. J. R. Liu, *Resource Allocation for Wireless Networks: Basics, Techniques, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2008.
[22] X. He and A. Yener, "On the equivocation region of relay channels with orthogonal components," in *Proc. 41st Asilomar Conf. Signals, Syst., Comput.*, Monterey, CA, Nov. 2007.
[23] Y. Oohama, "Relay channels with confidential messages," *IEEE Trans. Inf. Theory,* Mar. 2007 [Online]. Available: http://arxiv.org/abs/cs.IT/0611125, submitted for publication.
[24] M. Yuksel and E. Erkip, "Secure communication with a relay helping the wiretapper," in *Proc. 2007 IEEE Information Theory Workshop*, Lake Tahoe, CA, Sep. 2007.
[25] M. Yuksel and E. Erkip, "A secure communication game with a relay helping the eavesdropper," in *Proc. 2009 IEEE Inf. Theory Workshop*, Taormina, Italy, Oct. 2009.
[26] 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.

[27] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
[28] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian wiretap channel with a helping interferer," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008.
[29] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in *Proc. 41st Annu. Conf. Inf. Sci. Syst.*, Baltimore, MD, Mar. 2007.
[30] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, 2009, Article ID 494696, 14 pp.
[31] M. Bloch, J. O. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[32] P. K. 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.
[33] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wire-tap channels," in *Proc. 45th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, Sep. 2007.
[34] L. C. Godara, "Application of antenna arrays to mobile communications, Part II: Beam-forming and direction-of-arrival considerations," *Proc. IEEE*, vol. 85, pp. 1195–1245, Aug. 1997.
[35] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication, Cambridge*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[36] G. Golub and C. Van Loan, *Matrix Computations*, 3rd ed. Baltimore, MD: The Johns Hopkins Univ. Press, 1996.
[37] B. Friedlander and B. Porat, "Performance analysis of a null-steering algorithm based on direction of arrival estimation," *IEEE Trans. Signal Process.*, vol. 37, no. 4, pp. 461–466, Apr. 1989.
[38] Q. Spencer, A. Swindlehurst, and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 461–471, Feb. 2004.
[39] F. J. Solis and R. J.-B. Wets, "Minimization by random search techniques," *Math. Oper. Res.*, vol. 6, pp. 19–30, Feb. 1981.
[40] V. Havary-Nassab, S. Shahbazpanahi, A. Grami, and Z. Luo, "Distributed beamforming for relay networks based on second-order statistics of the channel state information," *IEEE Trans. Signal Process.*, vol. 56, no. 9, pp. 4306–4316, Sep. 2008.
[41] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

Lun Dong (S'06–M'09) received the B.S. and M.S. degrees from Tsinghua University, Beijing, China, in 2001 and 2004, respectively, and the Ph.D. degree from Drexel University, Philadelphia, PA, in 2008, all in electrical engineering.

He was a summer research intern at Mitsubishi Electric Research Laboratories, Cambridge, MA, in 2007. He was a summer research intern at NTT DOCOMO Communications Laboratories USA, Palo Alto, CA, in 2008. Currently, he is a Postdoctoral Scholar at the University of California, Irvine. His research interests are in the area of cooperative communications, cross-layer design and wireless security.

Dr. Dong is a recipient of the 2007 George Hill Jr. Endowed Fellowship of Drexel University.



Zhu Han (S'01–M'04–SM'09) received the B.S. degree in electronic engineering from Tsinghua University, Beijing, China, in 1997 and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland, College Park, in 1999 and 2003, respectively.

From 2000 to 2002, he was an R&D Engineer of JDSU, Germantown, MD. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an Assistant Professor in Boise State University, Boise, ID. Currently, he is an Assistant Professor in Electrical and Computer Engineering Department at the University of Houston, Houston, TX. From June to August 2006, he was a visiting scholar in Princeton University, Princeton, NJ. From May to August 2007, he was a Visiting Professor in Stanford University, Stanford, CA. From May to August 2008, he was a Visiting Professor in the University of Oslo, Norway, and Supelec, Paris, France. In July 2009, he was a Visiting Professor in the University of Illinois at Urbana-Champaign. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, wireless multimedia, and security.

Dr. Han was the MAC Symposium Vice-Chair of the IEEE Wireless Communications and Networking Conference 2008. He was the Guest Editor for a Special Issue on Fairness of Radio Resource Management Techniques in Wireless Networks in the *EURASIP Journal on Wireless Communications and Networking* and for a Special Issue on Game Theory in the *EURASIP Journal on Advances in Signal Processing*. He is the coauthor for papers that won the Best Paper Awards in the IEEE International Conference on Communications 2009 and the Seventh International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt09).

Athina P. Petropulu (S'87–M'87–SM'01–F'08) received the Diploma degree in electrical engineering from the National Technical University of Athens, Greece, in 1986 and the M.Sc. and Ph.D. degrees in electrical and computer engineering both from Northeastern University, Boston, MA, in 1988 and 1991, respectively.

Currently, she is a Professor at the Department of Electrical and Computer Engineering at Drexel University, Philadelphia, PA. She has held visiting appointments at SUPELEC in France and at Princeton University, Princeton, NJ. Her research interests span the area of statistical signal processing, wireless communications, signal processing in networking, and biomedical signal processing. She is the coauthor (with C. L. Nikias) of the textbook titled *Higher-Order Spectra Analysis: A Nonlinear Signal Processing Framework* (Englewood Cliffs, NJ: Prentice-Hall, 1993).

Dr. Petropulu is the recipient of the 1995 Presidential Faculty Fellow Award in Electrical Engineering given by the NSF and the White House. She is currently serving as Editor-in-Chief of the IEEE TRANSACTIONS ON SIGNAL PROCESSING (2009–2011). She was IEEE Signal Processing Society Vice-President—Conferences (2006–2008), and member-at-large of the IEEE Signal Processing Board of Governors. She has served as an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING and the IEEE SIGNAL PROCESSING LETTERS and was a member of the Editorial Board of the *IEEE Signal Processing Magazine* and the *EURASIP Journal on Wireless Communications and Networking*. She was the General Chair of the 2005 International Conference on Acoustics, Speech and Signal Processing (ICASSP), Philadelphia, PA. She is corecipient of the 2005 IEEE Signal Processing Magazine Best Paper Award.

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in EECS from Princeton University, Princeton, NJ, in 1977.

From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990, he has been on the faculty at Princeton, where he is the Michael Henry Strater University Professor of Electrical Engineering and Dean of the School of Engineering and Applied Science. His research interests are in the areas of stochastic analysis, statistical signal processing and their applications in wireless networks, and related fields. Among his publications in these areas are the recent books *MIMO Wireless Communications* (Cambridge Univ. Press, 2007) and *Quickest Detection* (Cambridge Univ. Press, 2009).

Dr. Poor is a member of the National Academy of Engineering, a Fellow of the American Academy of Arts and Sciences, and an International Fellow of the Royal Academy of Engineering (U.K.). He is also a Fellow of the Institute of Mathematical Statistics, the Optical Society of America, and other organizations. In 1990, he served as President of the IEEE Information Theory Society, and from 2004 to 2007, he served as the Editor-in-Chief of the IEEE TRANSACTIONS ON INFORMATION THEORY. He was the recipient of the 2005 IEEE Education Medal. Recent recognition of his work includes the 2007 Technical Achievement Award of the IEEE Signal Processing Society, the 2008 Aaron D. Wyner Award of the IEEE Information Theory Society, and the 2009 Edwin Howard Armstrong Award of the IEEE Communications Society.