A New Cooperative Transmission Strategy for Physical-Layer Security with Multiple Eavesdroppers

Chin-Liang Wang
Department of Electrical Engineering and
Institute of Communications Engineering
National Tsing Hua University
Hsinchu, Taiwan 30013, Republic of China
clwang@ee.nthu.edu.tw

Ting-Nan Cho† and Kai-Jie Yang‡
Institute of Communications Engineering
National Tsing Hua University
Hsinchu, Taiwan 30013, Republic of China
†s9964804@m99.nthu.edu.tw
‡d919608@oz.nthu.edu.tw

Abstract—**In this paper, we propose a two-phase cooperative transmission strategy using decode-and-forward (DF) relaying and cooperative null-steering beamforming (CN-SB) to overcome the multi-eavesdropper problem that reduces the secrecy capacity of wireless networks. First, two groups are built from all available relays—the jamming group and the cooperating group. Second, based on the proposed cooperative transmission strategy, we develop a new relay assignment and power allocation scheme to achieve a higher secrecy rate. Simulation results show that the secrecy rate of the proposed scheme linearly proportional to the signal-to-noise ratio (SNR), which is significantly larger than that of the scheme in which all relays perform CN-SB simultaneously in high SNR regions.**

Keywords—cooperating group; cooperative null-steering beamforming (CN-SB); decode-and-forward (DF) relaying; jamming group; multi-eavesdropper; power allocation; relay assignment

I. INTRODUCTION

Using wireless channel characteristics such as fading effects or noise to enhance network security has been established under the physical-layer in several decades. This was first proposed by Wyner [1], who investigated a wire-tap channel, and also verified that perfectly secure communications was attainable under a certain rate. Wyner's work was extended in [2], which considered an additive-white-Gaussian noise (AWGN) channel and provided secrecy capacity. Many researchers subsequently used the results of [1] and [2] to develop more powerful transmission strategies or coding techniques to improve the secrecy capacity of wireless networks.

To increase the secrecy capacity of wireless networks, multi-antenna systems are applied to overcome the broadcasting effect that results from one-isotropic-antenna systems. In [3], the authors assumed multiple antennas at the source to design a transmit beamforming strategy in which artificial noise is formed in the channel direction of the eavesdropper to confuse the eavesdropper. However, in the general case, all nodes with multiple antennas should be assumed; therefore, in [4], a more general multi-antenna system was discussed, and the authors also used the artificial noise produced by the source to interfere with the eavesdropper. Given the hardware cost limitation, it is sometimes assumed that all relays with multiple antennas are difficult to implement. In contrast, applying a virtual multiple antennas (i.e., multi-relay network) in physical-layer security has become more important. Consequently, in [5]–[7], a multi-relay network was used to address physical-layer security. In [5] and [6], the authors applied decode-and-forward (DF) relaying and amplify-and-forward (AF) relaying methods with a total power constraint and an individual power constraint to design the optimal beamforming vector based on maximizing the secrecy rate; however, in these works, the authors assumed no direct links existed between the source and the destination and between the source and the eavesdroppers, but this assumption is not true in some environments. Considering the more general multi-relay network presented by [7], the authors provided three cooperative transmission schemes: decode-and-forward (DF) relaying, AF relaying, and cooperative jamming (CJ). In [7], the authors take the direct source-destination link into account and considered the multi-eavesdropper problem. Nevertheless, in high SNR regions, the secrecy rate for these schemes will be bounded by the capacity of the source-eavesdropper links.

To solve the bounded secrecy rate problem in high SNR regions, our goal is to increase the capacity of the destination and diminish the capacity of each eavesdropper simultaneously. Therefore, we propose a two-phase cooperative transmission strategy by using DF relaying with two disjoint groups, which are collections of relays taken from all available relays; the first is the jamming group, which is intended to interfere with the eavesdroppers in Phase I, and the second is the cooperating group, which is intended to enhance the received SNR at the destination in Phase II. Based on the proposed cooperative transmission strategy, we present a new relay assignment and power allocation scheme to improve the secrecy rate of the source-destination link. Simulation results show that our proposed method has a higher secrecy rate than the scheme that assigns all relays performing CN-SB directly. In addition, the secrecy rate of our proposed method increases linearly proportional to the SNR. The remainder of this paper is organized as follows. Section II describes the system model and introduces the problem formulation. In Section III, we present a sub-optimal approach. Section IV shows the proposed relay assignment and power allocation. In Section V, we provide numerical results. Finally, we conclude with the main discussions in Section VI.

This work was supported by the National Science Council of the Republic of China under Grant NSC 100-2221-E-007-059-MY3.

978-1-4673-0990-5/12/$31.00 ©2012 IEEE

II. System Model and Problem Formulation

A. System Model

1) Notations

Suppose that a wireless network includes a source *S*, an intended destination *D*, a set of eavesdroppers ($E_i,\ i=1,\ .\ .\ .,Q$), and a set of *N* available relays ($R_i,\ i=1,\ .\ .\ .,N$). Fig. 1 shows the configuration of the system model. Two groups are constructed by all relays in the wireless network: the jamming group *J* and the cooperating group *G*. The number of relays is assumed to be *K* in *J*, i.e., $J=\{R_{J,i}\mid i=1,\ .\ .\ .,\ K\}$. On the other hand, *G* has *M* relays, where $G=\{R_{G,i}\mid i=1,\cdots,M\}$. Therefore, the total number of relays is *N=M+K*. Assume a two-phase cooperative transmission method; using DF relaying, Phase I is the broadcasting phase with the jamming phase, and Phase II is the cooperating phase, as illustrated in Fig. 2. We also assume that all channels are flat fading and quasi-static in a coherent time. $h_{S,D}$ and $\mathbf{h}_{S,E}$ are denoted as the baseband channel gains between the source and the destination and the source and the eavesdroppers, and $\mathbf{h}_{S,E}$ is a $Q\times 1$ vector. $\mathbf{h}_{J,D}$ and $\mathbf{H}_{J,E}$ are the $K\times 1$ channel vector and the $K\times Q$ channel matrix from *J* to the destination and the eavesdropper; $\mathbf{h}_{G,D}$ and $\mathbf{H}_{G,E}$ are the $M\times 1$ channel vector and the $M\times Q$ channel matrix between *G* to the destination and the eavesdroppers. $\mathbf{H}_{J,G}$ is the $K\times M$ channel matrix from *J* to *G*. $\mathbf{h}_{R,D}$ and $\mathbf{H}_{R,E}$ are the $N\times 1$ channel vector and $N\times Q$ channel matrix from all relays to the destination and to the eavesdroppers. $\mathbf{h}_{S,G}$ is the $M\times 1$ channel vector from the source to *G*. $\mathbf{h}_{J,D}$ and $\mathbf{h}_{G,D}$ are taken from $\mathbf{h}_{R,D}$, and $\mathbf{H}_{J,E}$ and $\mathbf{H}_{G,E}$ are drawn from $\mathbf{H}_{R,E}$.

2) Assumptions

To simplify the analysis, we make the following assumptions for the network:

i. The global channel-state-information (CSI) is available for all nodes (a basic assumption in physical-layer security).
ii. Each relay is equipped with a single ideal isotropic antenna, and operates in a half-duplex manner.

3) System analysis:

Consider a two-phase cooperative transmission applied in DF. In Phase I, the source transmits the signal and *J* forwards a weighted-sum version of the signal simultaneously. Therefore, the received signal at the destination and at the eavedroppers can be written as

$$y_{D,1}=\sqrt{P_S}h_{S,D}x+\sqrt{P_J}\mathbf{w}_J^H\mathbf{h}_{J,D}z+n_{D,1}, \tag{1}$$

$$\mathbf{y}_{E,1}=\sqrt{P_S}\mathbf{h}_{S,E}x+\sqrt{P_J}\mathbf{w}_J^H\mathbf{H}_{J,E}z+\mathbf{n}_{E,1}, \tag{2}$$

where x is a confidential symbol, z is the jamming symbol produced from each relay in *J*, and $E[\|x\|^2]=E[\|z\|^2]=1$. In addition, $n_{D,1}\sim CN(0,\ N_o)$ and $\mathbf{n}_{E,1}\sim CN(0,\ N_o\mathbf{I})$. The received signals of *G* can be represented as

$$\mathbf{y}_G=\sqrt{P_S}\mathbf{h}_{S,G}x+\sqrt{P_J}\mathbf{w}_J^H\mathbf{H}_{J,G}z+\mathbf{n}_G, \tag{3}$$

where $\mathbf{n}_G\sim CN(0,\ N_o\mathbf{I})$. On the other hand, in Phase II, *G* also forwards a weighted-sum version signal to the destination, but both the destination and the eavesdroppers receive the signals, which are expressed as

$$y_{D,2}=\sqrt{P_G}\mathbf{w}_G^H\mathbf{h}_{G,D}x+n_{D,2}, \tag{4}$$

$$\mathbf{y}_{E,2}=\sqrt{P_G}\mathbf{w}_G^H\mathbf{H}_{G,E}x+\mathbf{n}_{E,2} \tag{5}$$

where $n_{D,2}\sim CN(0,\ N_o)$ and $\mathbf{n}_{E,2}\sim CN(0,\ N_o\mathbf{I})$. P_T is the total transmission power, P_S is the source power, P_J is the power of *J*, and $P_G=P_T-P_S-P_J$ is viewed as the power of *G*. $\sqrt{P_J}\mathbf{w}_J^H\mathbf{H}_{J,C}z$ is interpreted as an inter-relay-interference (IRI) factor. To eliminate the IRI effect completely, we apply the CN-SB in *J* to null the signals from *J* to *G*, but the number of relays in *J* must be at least $M+Q+1$. Later, we combine the signals from Phase I and Phase II so that the received SNR, both at the destination and at the eavesdroppers, is calculated as

$$\mathrm{SNR}_D=\frac{P_S\left\|h_{S,D}\right\|^2}{N_o+P_J\mathbf{w}_J^H\mathbf{h}_{J,D}\mathbf{h}_{J,D}^H\mathbf{w}_J}+\frac{(P_o-P_S-P_J)\mathbf{w}_G^H\mathbf{h}_{G,D}\mathbf{h}_{G,D}^H\mathbf{w}_G}{N_0}, \tag{6}$$

$$\mathrm{SNR}_{E,i}=\frac{P_S\left\|h_{S,E,i}\right\|^2}{N_o+P_J\mathbf{w}_J^H\mathbf{h}_{J,E,i}\mathbf{h}_{J,E,i}^H\mathbf{w}_J}+\frac{(P_o-P_S-P_J)\mathbf{w}_G^H\mathbf{h}_{G,E,i}\mathbf{h}_{G,E,i}^H\mathbf{w}_G}{N_0},$$

for $i=1,\cdots,Q.$

(7)

In (6) and (7), we assume that $\mathbf{h}_{S,E}=[h_{S,E,1},\cdots,h_{S,E,Q}]^T$, $\mathbf{H}_{J,E}=[\mathbf{h}_{J,E,1},\cdots,\mathbf{h}_{J,E,Q}]$, and $\mathbf{H}_{G,E}=[\mathbf{h}_{G,E,1},\cdots,\mathbf{h}_{G,E,Q}]$.

B. Problem Formulation

Finding the secrecy capacity of a network and achieving it perfectly have become a main challenge in physical layer. Therefore, we propose a new cooperative transmission strategy by using two disjoint groups to achieve the secrecy capacity. By observing both (6) and (7), the capacity of the destination and of the eavesdroppers are given by $C_D=1/2\log(1+SNR_D)$ and $C_{E,i}=1/2\log(1+SNR_{E,i})$, respectively. Finally, the secrecy capacity of the multiple eavesdroppers can be formulated as

$$C_S=\min_{i\in\{1,\ 2,\ .\ .\ .,\ Q\}}\left\{\max_{P_S,\ P_J,\ P_G,\ \mathbf{w}_G,\mathbf{w}_J}\left\{C_D-C_{E,i}\right\}^+\right\}, \tag{8}$$

Because of the convexity of logarithm, the optimization of (8) is equivalent to

$$\min_{i\in\{1,2,\ldots,Q\}}\left\{\max_{\mathbf{w}_G,\,\mathbf{w}_J}\left\{\max_{P_S,\,P_J,\,P_G}\left\{(1+SNR_D)/(1+SNR_{E,i})\right\}\right\}\right\} \qquad (9)$$

In Phase I, J interferes with the eavesdroppers by using cooperative beamforming to increase the jamming power; however, at the same time, G also receives the jamming power, so we must make two constraints. The first constraint is to null the interference power from J to G (i.e., $\mathbf{w}_J^H\mathbf{H}_{J,G}=0$) to avoid the IRI effect completely. The second constraint is to zero the interference power from J to D (i.e., $\mathbf{w}_J^H\mathbf{h}_{J,D}=0$). In contrast, in Phase II, G is designed to increase the received SNR at D, with one constraint, which is to null the received power at E transmitted from G (i.e., $\mathbf{w}_G^H\mathbf{H}_{G,E}=0$). Therefore, (9) can be reformulated by

$$\begin{aligned}
&\arg\min_{i\in\{1,2,\ldots,Q\}}\left\{\max_{\mathbf{w}_G,\,\mathbf{w}_J}\left\{\max_{P_S,\,P_J,\,P_G}\left\{(1+SNR_D)/(1+SNR_{E,i})\right\}\right\}\right\}\\
&\text{subject to}\quad \mathbf{w}_J^H\mathbf{h}_{J,D}=0,\ \mathbf{w}_J^H\mathbf{H}_{J,G}=0,\\
&\qquad\qquad \mathbf{w}_J^H\mathbf{w}_J=P_J,\ \mathbf{w}_G^H\mathbf{H}_{G,E}=0,\ \mathbf{w}_G^H\mathbf{w}_G=P_G, \qquad (10)\\
&\qquad\qquad K\ge M+Q+1,\ P_o{=}P_S+P_G{+}P_J,\\
&\qquad\qquad P_S>0\ ,\ P_J>0\ ,\ \text{and}\ P_G>0.
\end{aligned}$$

This optimization problem considers the power allocation, the weighting vectors design ($\mathbf{w}_G$ and $\mathbf{w}_J$), and the group assignment jointly to maximize the secrecy rate for multiple eavesdroppers. It is observed that both the optimal $\mathbf{w}_G$ and $\mathbf{w}_J$ are dependent on the selection of G and J. As mentioned above, given the number of relays in G and the number of relays in J as M and $M+Q+1$, the number of combinations of G and J is at least $\binom{2M+Q+1}{M}$. From the above discussions, (10) is classified as an integer optimization problem. To evaluate it, we can use the optimal result and an integer programming method; however, the integer programming method has high computational complexity. To overcome the high computational complexity problem, in this work we provide a sub-optimal but effective approach to avoid the integer programming.

III. Weighting Vectors Optimization

Given a selection of G and J, the optimal $\mathbf{w}_G$ and the optimal $\mathbf{w}_J$ can be determined independently. First, to find the optimal $\mathbf{w}_J$, the optimization problem is to maximize the received power at all eavesdroppers, with three constraints. The first constraint is to zero the received power at D, the second constraint is to eliminate the IRI completely, and the third constraint is the power limitation, which is allocated to be unit power. Thus, the optimization problem for $\mathbf{w}_J$ is defined as

$$\begin{aligned}
&\mathbf{w}_J^*=\arg\max_{\mathbf{w}_J}\left\|\mathbf{w}_J^H\mathbf{H}_{J,E}\right\|^2 \qquad (11)\\
&\text{subject to}\ \mathbf{w}_J^H\mathbf{h}_{J,D}=0,\ \mathbf{w}_J^H\mathbf{H}_{J,G}=\mathbf{0},\ \text{and}\ \mathbf{w}_J^H\mathbf{w}_J=1.
\end{aligned}$$

Assume that $\mathbf{H}_J=\left[\mathbf{H}_{J,G}\ \mathbf{h}_{J,D}\right]$, and the two nulling constraints are simplified to one nulling constraint. Using Lagrange multiplier to solve (11), we obtain the solution given by

$$\begin{aligned}
&\mathbf{w}_J^*=\frac{1}{Q\left\|(\mathbf{I}_N-\mathbf{P}_{J,D})\frac{1}{Q}\mathbf{H}_{J,E}\mathbf{1}\right\|}(\mathbf{I}_N-\mathbf{P}_{J,D})\mathbf{H}_{J,E}\mathbf{1}, \qquad (12)\\
&\mathbf{P}_{J,D}=\mathbf{H}_J(\mathbf{H}_J^H\mathbf{H}_J)^{-1}\mathbf{H}_J^H,\ \text{and}\ \mathbf{1}_{Qx1}=[1,\cdots,1]^T.
\end{aligned}$$

The solution is the CN-SB with multiple beams, which maximizes the power of J in the eavesdroppers' directions and nulls the power of J to D and G. Because $(\mathbf{H}_J^H\mathbf{H}_J)^{-1}$ must be satisfied, the number of relays in J must be at least M+Q+1. Thus, the result also satisfies the constraints of (10). On the other hand, to achieve the optimal $\mathbf{w}_G$, its optimization problem is to maximize the received power at D with two constraints. The first constraint is to zero the received power at the eavesdroppers transmitted by G, and the second constraint is that the power must be 1; consequently, the optimization problem for $\mathbf{w}_G$ can be defined as

$$\begin{aligned}
&\mathbf{w}_G^*=\arg\max_{\mathbf{w}_G}\left\|\mathbf{w}_G^H\mathbf{h}_{G,D}\right\|^2 \qquad (13)\\
&\text{subject to}\ \mathbf{w}_G^H\mathbf{h}_{G,E}=0,\ \text{and}\ \mathbf{w}_G^H\mathbf{w}_G=1
\end{aligned}$$

Eq. (13) is also a CN-BF problem with one beam, so the solution is also obtained by using the Lagrange multiplier optimization technique directly, which can be denoted as

$$\mathbf{w}_G^*=\frac{(\mathbf{I}_N-\mathbf{P}_{G,E})\mathbf{h}_{G,D}}{\left\|(\mathbf{I}_N-\mathbf{P}_{G,E})\mathbf{h}_{G,D}\right\|},\ \text{and}\ \mathbf{P}_{G,E}=\mathbf{h}_{G,E}(\mathbf{h}_{G,E}^H\mathbf{h}_{G,E})^{-1}\mathbf{h}_{G,E}^H. \qquad (14)$$

The optimal result shows that the CN-SB maximizes the power of G in the D direction and nulls the power of G in the eavesdroppers' directions. We have gained $\mathbf{w}_G^*$ and $\mathbf{w}_J^*$ without considering the power allocation and relay assignment problems. In the next section, based on $\mathbf{w}_G^*$ and $\mathbf{w}_J^*$, we present a low-complexity relay assignment scheme and the corresponding power allocation method to attain a better secrecy rate.

IV. Relay Assignment and Power Allocation

A. Relay Assignment

As mentioned in Section II.B, the optimal relay assignment relies on an exhaustive search over all possible jamming/cooperating groups, the computational complexity increases rapidly as the number of relays increases. In this work, we propose a low-complexity relay assignment scheme which aims to maximize the received SNR at D in Phase II.

Assume that the channel power from all relays to D, $\mathbf{h}_{R,D}=[h_{R_1,D},\cdots,h_{R_N,D}]^T$, is sorted as $\|h_{R_{l_1},D}\|^2\ge\|h_{R_{l_2},D}\|^2\ge\cdots\ge\|h_{R_{l_N},D}\|^2$. To maximize the received SNR at D by applying M relays in G in Phase II, the relay assignment rule is represented as

$$G=\left\{R_{i_1},\cdots,R_{i_M}\right\}. \tag{15}$$

It is also noted that given the number of relays in G as M, the number of relays in J should be at least $M+Q+1$. Using the least required number of relays $N= 2M+Q+1$, the number of relays in G is decided by $M=(N-Q-1)/2$.

To ensure that the message from S is decodable at all the relays in G, a constraint should be claimed by

$$C_{SR_k}\geq C_S,\quad R_k\in G \tag{16}$$

The above inequality shows that the capacity of the source to the kth relay must be higher than the secrecy capacity. To use (16), we reformulate it to become

$$P_S^2\left[\frac{\left\|h_{S,R_k}\right\|^2}{N_o}\frac{\left\|h_{S,E}\right\|^2}{N_o+P_JA}\right]+P_S\left[\frac{\left\|h_{S,R_k}\right\|^2+B-\left\|h_{S,D}\right\|^2}{N_o}+\frac{\left\|h_{S,E}\right\|^2}{N_o+P_JA}\right]-\frac{P_o-P_J}{N_o}\geq 0, \tag{17}$$

where $A=(\mathbf{w}_J^*)^H\mathbf{H}_{J,E}\mathbf{H}_{J,E}^H\mathbf{w}_J^*$ and $B=(\mathbf{w}_G^*)^H\mathbf{h}_{G,D}\mathbf{h}_{G,D}^H\mathbf{w}_G^*$. This is a second-order equation to P_S, and the solution of P_S is given by (18). The result of (18) implies the minimum transmission power $P_{S,\min}^k$ for the source to let the kth relay decode the source's message successfully. Accordingly, we set $P_S=\max\{P_{S,\min}^{i_1},\ldots,P_{S,\min}^{i_2},P_{S,\min}^{i_M}\}$ to ensure the message from S to be decodable at all the relays in G. Based on the proposed relay assignment scheme and the corresponding source power P_S, a nearly optimal power allocation strategy is developed in the following.

B. Power Allocation

By observing (6)–(8), the secrecy capacity corresponding to the ith eavesdropper is denoted as $C_{S,i}=\max\limits_{P_S,P_J}(C_D-C_{E,i})^+$, which is a function of P_S and P_J for a given pair of groups $\{G, J\}$. According to (18), since P_S can be represented as a function of P_J, the secrecy capacity then becomes a single variable function of P_J. In addition, when $N>>1$, this implies that A and B are large enough to make $\left[\frac{\left\|h_{S,R_k}\right\|_{\min}^2+B-\left\|h_{S,D}\right\|^2}{N_o}+\frac{\left\|h_{S,E}\right\|^2}{N_o+P_JA}\right]^2>>4\left[\frac{\left\|h_{S,R_k}\right\|_{\min}^2}{N_o}\frac{\left\|h_{S,E}\right\|^2}{N_o+P_JA}\right]\frac{P_o-P_J}{N_o}$ in (18). Under this assumption, P_S can be simply approximated by

$$P_S\approx\frac{B(P_o-P_J)(N_o+AP_J)}{(N_o+AP_J)(B+\|h_{S,R_k}\|_{\min}^2-\|h_{S,D}\|^2)+N_o\|h_{S,E}\|^2} \tag{19}$$

Using the result of (19), we then find that $C_{S,i}$ is a concave function of P_J. After taking $\frac{dC_{S,i}}{dP_J}=0$, we can obtain the optimal $P_{J,i}$ and the corresponding $P_{S,i}$, denoted by $P_{J,i}^*$ and $P_{S,i}^*$, respectively. In addition, $P_{G,i}^*=P_o-P_{S,i}^*-P_{J,i}^*$. Define the ith eavesdropper-related optimal power allocation as

$$\Phi_i=\{P_{J,i}^*,\,P_{S,i}^*,\,P_{G,i}^*\},\qquad i=1,\cdots,Q \tag{20}$$

The secrecy capacity is expressed as

$$C_S=\min_{\Phi_i}(C_{S,i}(\Phi_i)). \tag{21}$$

By using the exhaustive search over $\{C_{S,i}\}_{i=1}^Q$, the secrecy capacity as well as the optimal power allocation Φ_{i^*} is obtained.

V. Simulation Results

In this section, computer simulation results are provided to verify the proposed theoretic analysis. In addition, [7] using DF relaying is compared with the proposed method. The greatest difference between our proposed scheme and the DF relaying in [7] is that all relays in [7] are operated only in Phase II by using CN-SB. We assume that $N=10$, $Q=3$ $M=(N-Q-1)/2=3$, and $K=M+Q+1=7$. The total transmission power is set to one (i.e., $P_T=1$). We assume that all channels are Rayleigh fading channels with unit channel power, and that all noises are independent complex Gaussian noises with zero mean and N_o variance.

Fig. 3 shows that the proposed cooperative transmission scheme has a larger secrecy capacity than [7] with DF relaying in high SNR regions. In low SNR regions, the eavesdroppers try to interpret the confidential message, which is not easy because of the low received SNR. Therefore, applying a J to interfere with the eavesdroppers may not be necessary. Because the received signal strength of eavesdroppers is low, the secrecy capacity will be dominated by the capacity of D. To maximize the secrecy rate in low SNR regions, all relays should be used in G. In other words, to maximize the secrecy rate in low SNR regions, it is more efficient to increase the capacity of D than it is to reduce the capacities of eavesdroppers. It is more difficult to provide a high secrecy capacity in high SNR regions than in low SNR regions because of the high received SNR at the eavesdroppers in Phase I; however, the proposed scheme uses the jamming group to reduce the received SNR at the eavesdroppers, which provides larger secrecy rates in high SNR regions than the methods in [7] with DF relaying or other existing schemes.

Fig. 4 shows that the secrecy capacity of [7] with DF relaying is bounded in high SNR regions because the received sig-

$$P_S^k\geq\frac{-\left[\frac{\left\|h_{S,R_k}\right\|^2+B-\left\|h_{S,D}\right\|^2}{N_o}+\frac{\left\|h_{S,E}\right\|^2}{N_o+P_JA}\right]+\sqrt{\left[\frac{\left\|h_{S,R_k}\right\|^2+B-\left\|h_{S,D}\right\|^2}{N_o}+\frac{\left\|h_{S,E}\right\|^2}{N_o+P_JA}\right]^2+4\left[\frac{\left\|h_{S,R_k}\right\|^2}{N_o}\frac{\left\|h_{S,E}\right\|^2}{N_o+P_JA}\right]\frac{P_o-P_J}{N_o}}}{2\left[\frac{\left\|h_{S,R_k}\right\|^2}{N_o}\frac{\left\|h_{S,E}\right\|^2}{N_o+P_JA}\right]}. \tag{18}$$

nal strength of the eavesdroppers is too large in Phase I to dominate the secrecy rate. In contrast, our proposed scheme applies a set J to reduce the capacities of eavesdroppers in Phase I and provides the cooperating group to increase the capacity at the destination; therefore, our proposed method has better performance than [7] with DF relaying in high SNR regions. In addition, our proposed scheme focuses on simultaneously maximizing the capacity at the destination and minimizing the capacities at the eavesdroppers in the two phases, so the secrecy rate will not be saturated in high SNR regions (i.e., the secrecy rate has no limit in high SNR regions) and the secrecy rate of proposed method increases linearly proportional to SNR. Obtaining this result is the primary contribution of this paper.

VI. Conclusions

We have proposed a two-phase cooperative transmission strategy using DF relaying and CN-SB techniques in multi-eavesdropper environments. We have also developed a practical relay assignment and power allocation scheme to improve the network secrecy rate. In high SNR regions, the secrecy rates of the existing methods are bounded due to the high received signal strength at the eavesdroppers without applying the jammers in Phase I; however, the simulation results show that the secrecy rate of our proposed method increases linearly proportional to the SNR.

References

[1] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[2] S. K. Leung-Yan-Cheong and Martin E. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Information Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[3] W.-C. Liao, T.-H. Chang, W.-K. Ma, C.-Y. Chi, “Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approch,” *IEEE Trans. Signal Processing*, vol. 59, no. 3, Mar. 2011

[4] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. Peter Hong, and C.-Y. Chi, “On the impact quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem,” *IEEE Trans. Wireless Communications*, vol. 10, no. 3, Mar. 2011.

[5] Junwei Zhang, and M. C. Gursoy, “Collaborative relay beamforming for secrecy,” In *Proceedings of the 2011 IEEE Internation Conference on Communications* (ICC 2010), 2010.

[6] Junwei Zhang, and M. C. Gursoy, “Relay beamforming strategies for physical-layer security,” In *Proceedings of IEEE Conference on Information Sciences and Systems* (CISS 2010), 2010.

[7] L. Dong, Z. H., A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Trans. Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

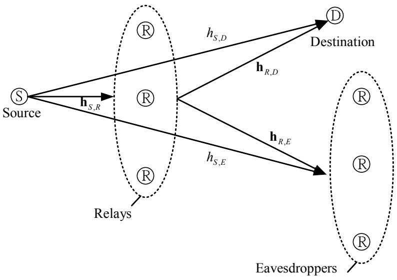

Figure 1. Illustration of system model.

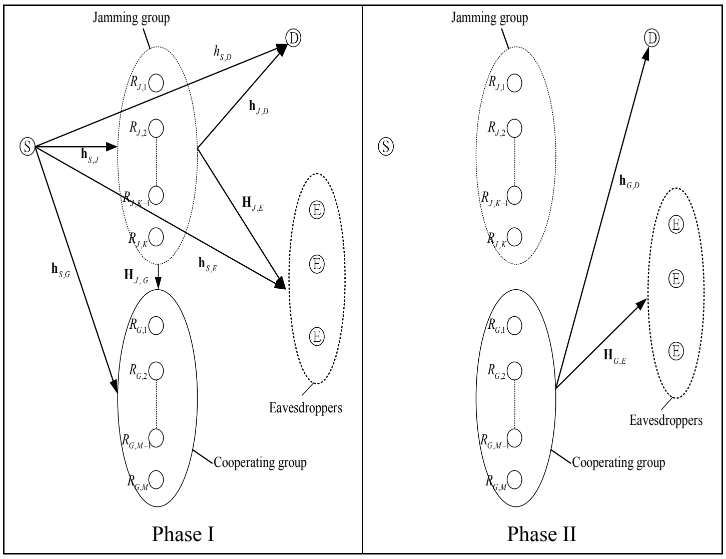

Figure 2. Illustration of the proposed cooperative transmission strategy.

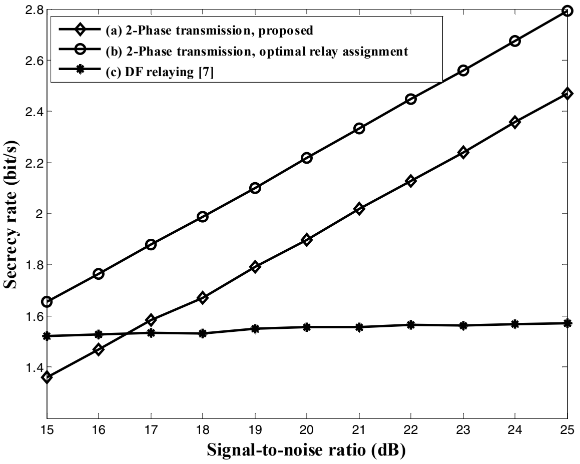

Figure 3. Secrecy rates of (a) two-phase transmission with the proposed power allocation and relay assignment scheme, (b) two-phase transmission with optimal relay assignment based on (19), and (c) DF relaying in [7].

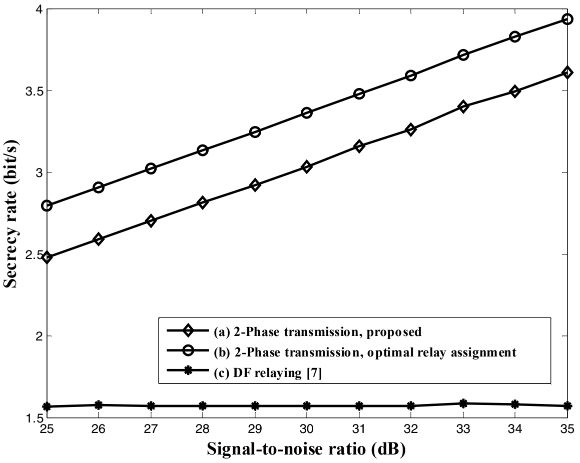

Figure 4. Secrecy rates of (a) two-phase transmission with the proposed power allocation and relay assignment scheme, (b) two-phase transmission with optimal relay assignment based on (19), and (c) DF relaying in [7] in high SNR regions.