Cooperation Based on Decode-and-Forward Plus Cooperative Jamming for Wireless Physical Layer Security

Shuanglin HUANG [1], Jianjun TAN [1], Run JIANG [2]
[1]School of Information Engineering, Hubei University for Nationalities
EnShi City, China
[2]Center of Network Computing
Alket Co., Ltd., Dortmund 10981, Germany
huang-shuanglin@163.com

Journal of Digital Information Management

ABSTRACT: *We employed node cooperation in a cooperative wireless network to achieve physical layer-based security. The case of a source-destination pair that works with the assistance of multiple cooperating nodes in the presence of an eavesdropper was considered in this study to improve the performance of secure wireless communications. A novel cooperative scheme, called the decode-and-forward plus cooperative jamming (DFCJ), was proposed. In this scheme, relay nodes transmit a weighted version of the source signals plus a common weighted jamming signal to confound the eavesdropper. The novel system design was proposed to determine cooperative node weights and transmit power allocation. In DFCJ, a closed-form solution is obtained to minimize the total transmit power that is subjected to a secrecy rate constraint under complete nulling of jamming signals at the destination. The results of the numerical evaluation of the transmit power and the obtained secrecy rate show that the proposed scheme can significantly improve the performance of wireless physical layer security compared with the original decode-and-forward scheme.*

Categories and Subject Descriptors
C.2.1 [Computer Communication Networks]: Network Architecture and Design - Wireless communication

General Terms
Physical Layer Security, Cooperation

Keywords
Wireless Communciation, Physical Security, Wireless Network, Node Cooperation

Received: 16 November 2014, Revised 20 December 2014, Accepted 3 January 2015

1. Introduction

Information theoretic security in wireless networks has recently received considerable interest because of its capability to achieve perfect secrecy transmission without relying on traditional encryption mechanisms [1], [2]. In recent years, physical layer security issues have gained significant attention because of the broadcast nature of wireless channels. From an information theoretic perspective, the basic idea is to utilize the physical characteristics of a wireless channel, such that source messages can be transmitted securely. Wyner [3] introduced the wiretap channel, wherein a source could transmit confidential messages to a certain destination while keeping the messages hidden from a wiretapper. The maximum rate at which a source can transmit to its destination in the presence of an eavesdropper, called secrecy capacity, is $C_s = max\{0, C_d - C_e\}$, where C_d and C_e , which indicates the capacity of the link between the source and the destination as well as the capacity of the link between the source and the eavesdropper, respectively. In [4], the approach of Wyner was extended to the transmission of confidential messages over broadcast channels. However, secrecy capacity is affected by channel conditions between the source and the destination, as well as those between the source and the eavesdropper. Note that the achievable secrecy rate is typically zero [1], [2].

If the channel conditions between the legitimate transceiver and the destination are worse than those between the source and the eavesdropper, then using multiple antenna systems and node cooperation is preferable [5]–[8].

Some recent works that employ multiple antenna systems, such as multiple-input and multiple-output (MIMO) [5], single-input and multiple-output (SIMO) [6], and multiple-input and single-output (MISO) [7] systems, have proposed solutions to the aforementioned issue. However, multiple antennas may not be available in network nodes because of cost and size limitations. In such scenarios, node cooperation is an effective approach to experience the advantages attributed to multi-antenna systems even if single-antenna nodes are used. Node cooperation via relays is a low-cost approach that increases secrecy capacity by employing/mitigating channel effects. The application of cooperation nodes can be grouped into two categories. In the first category, relays or helpers transmit artificial noise to jam eavesdroppers; in the second category, relays or helpers support source–destination transmission. In [2], a four-node system model (i.e., source, destination, eavesdropper, and relay) was proposed. In this model, the relay transmits a noise signal that is independent of the source signals to confound eavesdroppers. Meanwhile, a basic approach to ensure confidentiality was proposed in [8]. The main idea of this approach was to schedule downlink base station transmissions simultaneously with concurrent uplink transmissions of interest to create intentional interference for possible eavesdroppers. In [9], a two-relay scheme to increase security against eavesdroppers was presented. The first relay used a decode-and-forward (DF) strategy to assist a source in delivering its data to its destination. The second relay was used to create intentional interference at eavesdropper nodes. However, only one cooperation node was considered for a secure link, although multiple relays or helpers could be used to experience the benefits of multiple-antenna systems. In [10]–[12], a scenario, in which a source communicates with a destination with the help of multiple relays in the presence of one or more eavesdroppers, was considered. An extended version of this scenario was recently proposed in [13]. Three cooperative schemes, DF [10], amplify-and-forward (AF) [11], and cooperative jamming (CJ) [12], have been studied to increase achievable secrecy rate or minimize the total transmit power. In Stage 1 of DF and AF, a source broadcasts the encoded signal to trusted relay nodes. In Stage 2 of DF, each relay decodes and re-encodes the message and then transmits a weighted version of the re-encoded signal. Meanwhile, each relay forwards a weighted version of the noisy signals from Stage 1 in Stage 2 of AF. In CJ, the source transmits the encoded signal and then relays the weighted jamming signal to confound eavesdroppers. DF and AF were also studied in [14] to obtain the optimal beamforming structure and maximize secrecy rates under both total and individual power constraints. In [15], friendly jammers charge sources with a certain price to interfere with unauthenticated malicious relays. In [16], the authors proposed two opportunistic secrecy transmission schemes: opportunistic CJ and relay chatting. In these two schemes, some of the relays and the destination are grouped together to transmit jamming signals and confuse eavesdroppers. Based on [13], the DF and CJ schemes were further discussed to improve the achievable secrecy rate or minimize the total transmit power in [17].

In previous works, however, relay nodes that transmit the message received from the source or the jamming signals with the aim of confounding eavesdroppers, were considered to establish a secure link from the source to the destination in a wireless network. That is, the advantages of DF, AF, and CJ are not simultaneously explored and utilized. In the present study, a novel cooperative scheme, called DFCJ, is proposed. This scheme focuses on cases with a single eavesdropper. Each relay is not only used to forward messages from the source but also to transmit jamming signals to confound an eavesdropper. Under special circumstances, some of the relays follow the proposed DFCJ strategy, whereas the others simply transmit jamming signals to confuse an eavesdropper. Therefore, more cooperation nodes are probably involved in the DFCJ scheme. In general, security performance is further improved in the proposed system by inviting more relays to cooperate.

In Stage 1, the source broadcasts the encoded signal to trusted relay nodes. In Stage 2, each relay node decodes the message, re-encodes it, and transmits a weighted version of the re-encoded signal. Meanwhile, relay nodes also transmit a weighted jamming signal to confound an eavesdropper and completely null out the total jamming signal during transmission to the destination.

We aim to design cooperative relay node weights and transmit power allocation to minimize the total cooperative power when subjected to a secrecy capacity constraint or maximize the achievable secrecy rate when subjected to a total transmit power constraint.

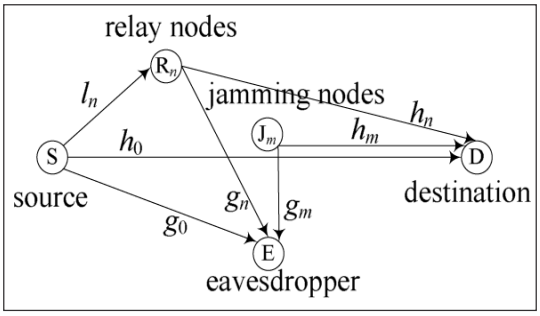

Figure 1. System model

2. System Model and Cooperative Scheme

We study a wireless network model that consists of one source node, *N* trusted relay nodes, one destination node, and one eavesdropper. As illustrated in Figure 1, the source (*S*) aims to transmit its data to the destination (*D*) in the presence of an eavesdropper (*E*). The N relays, i.e., R_1, …, R_N, simultaneously follow DF and CJ protocols. Each node has only one omni-directional antenna for both

transmission and reception, and operates at half-duplex mode. We assume that global channel state information (CSI) is available (a common assumption in physical layer security literature). Similar to a previous study [13], we assume that the encoding scheme at the source, the decoding methods at the destination and the eavesdropper, and the cooperative protocol are public information. Only the message from the source is confidential to the eavesdropper .

The following notations are adopted in the current study. Bold uppercase letters denote matrices, whereas bold lowercase letters denote column vectors. Conjugate, transpose, and conjugate transpose are represented by $(\ )^*$, $(\ )^T$ and $(\ )^\dagger$, respectively. All channels are assumed to undergo flat fading and are quasi-static. We denote P_S as the transmit power of the source, P_D as the transmit power of the re-encoded signal sent from relays to help source–destination transmission, and P_J as the transmit power of the jamming signal sent from relays to confound an eavesdropper. The relay message signal weight vector is defined as $\boldsymbol{w}_D(N\times 1)$, and the relay jamming signal weight vector as $\boldsymbol{w}_J\ (N\times 1)$. In addition, σ^2 denotes noise power, $\boldsymbol{h} = (N\times 1)$ represents the channel vector between *N* relays and the destination, and $\mathbf{g}\ (N\times 1)$ signifies the channel vector between *N* relays and an eavesdropper. Finally, matrices $\boldsymbol{R}_h = \mathbf{h}\mathbf{h}^\dagger$ and $\boldsymbol{R}_g = \mathbf{g}\mathbf{g}^\dagger$ are defined.

2.1 Direct Transmission (DT)

In DT, the source transmits its encoded symbols directly to the destination using all available transmit power within a transmission slot. When transmitting the symbol x in a time unit, the received signal at the destination is

$$y_d = \sqrt{P_s}\, h_0 x + n_d \qquad (1)$$

Meanwhile, the received signal at the eavesdropper is

$$y_e = \sqrt{P_s}\, g_0 x + n_e \qquad (2)$$

where n_d and n_d represent the complex Gaussian noise at the destination and at the eavesdropper, respectively (assumed to be white over time units).

2.2 DFCJ

DFCJ has two stages. In Stage 1, the source broadcasts *n* encoded symbols to trusted relay nodes using the first transmission slot.

When transmitting x, the received signals at N trusted relay nodes, which are stacked in vector, are as follows:

$$y_r = \sqrt{P_s}\,\eta x + n_r,\ r = 1, 2, ..., N \qquad (3)$$

where $\eta = (\eta_1, \eta_2, ... \eta_N)$ is the channel vector between the source and the *N* trusted relays, and n_r is the noise vector at the relay nodes. In Stage 1, the received signals at the i^{th} relay becomes

$$y_{ri} = \sqrt{P_s}\,\eta_i x + n_{ri} \qquad (4)$$

Hence, the worst secrecy rate between the source and the N relays is

$$R_r^{min} = \frac{1}{2} log\left(1 + \frac{P_s min\ \{|\eta_1|^2, |\eta_2|^2, ..., |\eta_N|^2}{\sigma^2}\right) \qquad (5)$$

and the achieved rate at the eavesdropper $R_e^{(1)}$ is

$$R_e^{(1)} = \frac{1}{2} log\left(1 + \frac{P_s |g_0|^2}{\sigma^2}\right) \qquad (6)$$

In this case, the worst secrecy rate between the source and the N relays is

$$R_s^{(1)} = max\ \{0, R_r^{min} - R_e^{(1)}\} \qquad (7)$$

In Stage 2, all the trusted relay nodes successfully decode the message, re-encode it, and cooperatively transmit the re-encoded symbols to the destination using the second transmission slot. For notational convenience, we assume that all the relay nodes that follow the DF protocol successfully decode the source message. In DFCJ, while N relay nodes are transmitting the re-encoded symbol, they are simultaneously transmitting weighted jamming signals that are independent of the source message to confound an eavesdropper.

Let the weights of all the relay nodes be stacked in vector, $\tilde{x}$ be the re-encoded symbol, and z be the jamming signal at the relay nodes. In Stage 2, the received signal at the destination is

$$y_d = \mathbf{h}^\dagger \boldsymbol{w}_D \tilde{x} + \mathbf{h}^\dagger \boldsymbol{w}_J\, z + n_d \qquad (8)$$

where as the received signal at an eavesdropper is

$$y_e = \mathbf{g}^\dagger \boldsymbol{w}_D \tilde{x} + \mathbf{g}^\dagger \boldsymbol{w}_J\, z + n_e \qquad (9)$$

where n_d and n_d are the noises at the destination and eavesdropper, respectively.

The rates at the destination $R_d^{(2)}$ and eavesdropper $R_e^{(2)}$ are respectively

$$R_d^{(2)} = \frac{1}{2} log\left(1 + \frac{P_s |h_0|^2}{\sigma^2} + \frac{w^\dagger_D R_h w_D}{\sigma^2 + w^\dagger_J R_h w_J}\right) \qquad (10)$$

and

$$R_e^{(2)} = \frac{1}{2} log\left(1 + \frac{P_s |g_0|^2}{\sigma^2} + \frac{w^\dagger_D R_g w_D}{\sigma^2 + w^\dagger_J R_g w_J}\right) \qquad (11)$$

The secrecy rate under the presence of one eavesdropper in Stage 2 is given by

$$R_S^{(2)} = max\ \{0, R_d^{(2)} - R_e^{(2)}\} \qquad (12)$$

Given that cooperative transmission is divided into two stages, the secrecy rate from the source to each relay in Stage 1 should not be less than that of the destination achieved in DFCJ. To guarantee the given rate $R_s^{(2)}$ in each link, $R_s^{(1)} \geq R_s^{(2)}$ must be achieved. In the end, the achieved secrecy rate can be expressed as follows:

$$R_s = max\ \{0, min\ \{R_s^{(2)} - R_s^{(2)}\}\} \quad (13)$$

We consider the practical case wherein the system can be designed to ensure that the secrecy rate is positive. In this case, the achieved secrecy rate can be rewritten as

$$R_s = min\ \{R_s^{(1)},\ R_s^{(2)}\} \quad (14)$$

3. Formulation for System Design Problems

Considering that global CSI is available, the achievable rate and the total transmit power of the cooperative scheme are determined as functions of relay weights $\boldsymbol{w}_D$ and $\boldsymbol{w}_J$ as well as the transmit power of source $\boldsymbol{P}_S$. Thus, our first design objective is to determine $\boldsymbol{w}_D$, $\boldsymbol{w}_J$, and $\boldsymbol{P}_S$ to minimize the total transmit power, which is subjected to an achievable secrecy rate constraint R_s^0, i.e.,

$$min\ P_0 = P_s + P_D + P_J,\ s.t. R_s \geq R_s^0 \quad (15)$$

To minimize the total transmit power, a high message signal power must be delivered to the destination, whereas a low message signal power must be sent to the eavesdropper. By contrast, a low jamming signal power must be delivered to the destination, whereas a high jamming signal power must be sent to the eavesdropper. This concept is fairly similar to the idea of transmit beamforming in array signal processing. In traditional transmit beamforming, the multi-antenna transmitter intends to maximize signal power in a desired direction and suppress or eliminate signals in undesired directions [18]. Therefore, our analysis is based on a signal processing framework [19].

First, we provide Lemmas 1 and 2, which will be the bases of the results.

Lemma 1: Let $w_J^{\dagger} g = \mu$ and $w_J^{\dagger} h = 0$. The solution [13] of problem

$$min\ w_J^{\dagger}\ w_J \quad (16)$$

is given by

$$w_J = \mu\,[g\ h] \begin{bmatrix} g^{\dagger} g & g^{\dagger} h \\ h^{\dagger} g & h^{\dagger} h \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (17)$$

Lemma 2: Let s and t be (known) linearly uncorrelated vectors. Matrix $ss^{\dagger} - tt^{\dagger}$ has only two nonzero eigenvalues, i.e., $\eta_1 > 0$ and $\eta_2 < 0$, which are given by [17]

$$\eta_1 = \|s\|^2 - c_1|s^{\dagger}t|,\ \eta_2 = \|s\|^2 - c_2|s^{\dagger}t| \quad (18)$$

The corresponding eigenvectors are

$$e_1 = c_3(s + c_1 te^{i(\pi-\theta)}),\ e_2 = c_4(s + c_2 te^{i(\pi-\theta)}) \quad (19)$$

where

$$c_3 = 1/\sqrt{\|s\|^2 + c_1\|t\|^2 - 2c_1|s^{\dagger}t|};\ c_4 = 1/\sqrt{\|s\|^2 + c_2\|t\|^2 - 2c_2|s^{\dagger}t|},$$

$$i = \sqrt{-1};\ 2c_1|s^{\dagger}t| = \|s\|^2 + \|t\|^2 - \sqrt{(\|s\|^2 + \|t\|^2 - 4|s^{\dagger}t|^2}};$$

4. Formulation for Transmit Power Minimization

In this section, the objective of designing the system for the DFCJ scheme is proposed to minimize the total transmit power subject to an achievable secrecy rate constraint R_s^0. First, source power P_S is fixed to obtain weight vectors w_D and w_J, minimize the total power of the relays, and then find the optimal value of P_S.

4.1 Relay Weight Optimization

First, we assume that $w_J^{\dagger} g = \mu$ and fix it to obtain weights w_D and w_J to minimize the transmit power of cooperative nodes. In the end, we find the optimal value of μ. Given that a high transmit power always yields a high achievable secrecy rate, equality and inequality secrecy rate constraints are equivalent. Thus, a design based on the equality rate constraint is proposed in this section.

Given the secrecy rate constraint $R_s = R_s^0$ and the source power P_S, the optimization problem of minimizing the transmit power in Stage 2 can be formulated as -

$$min\ P_0 = P_s + P_D + P_J,\ s.t.\ R_s^0 \quad (20)$$

Nulling signals at the undesired nodes is sometimes referred to as null-steering beamforming in array signal processing. By nulling jamming signals at the destination [13] [18], Equation (21) can be rewritten as

$$min\ P_0 = P_S + \|w_D\|^2 + \|w_J\|^2$$

$$s.t. \begin{cases} w_J^{\dagger} h = 0 \\ \dfrac{w_D^{\dagger} R_h w_D}{\sigma^2} - \dfrac{4^{R_s^0} w_D^{\dagger} R_g w_D}{\sigma^2 + w_J^{\dagger} R_g w_J} = \zeta \end{cases} \quad (21)$$

where

$$\zeta = \frac{P_S}{\sigma^2}\ 4^{R_s^0}|g_0|^2 - |h_0|^2 + 4^{R_s^0} - 1.$$

Without losing generality, we assume that μ is a positive real number $w_J^{\dagger} g = \mu$ and because the transmit power remains the same when the weight vector w_J is rotated at an arbitrary phase. Hence $w_J^{\dagger} R_g w_J = \mu^2$.

Then, Equation (21) can be further rewritten as

$$min\ P_0 = P_S + \|w_D\|^2 + \|w_J\|^2$$

$$s.t. \begin{cases} w_J^{\dagger} h = 0 \\ w_J^{\dagger} g = \mu \\ w_D^{\dagger} \tilde{R} w_D = \zeta \end{cases} \quad (22)$$

where $\tilde{R} = R_h / \sigma^2 - 4^{R_s^0} R_g / (\sigma^2 + \mu^2)$.

Theorem 1: For a given power source P_s, the optimal cooperative power consumption P_0 is a function of μ^2 and $P_0(\mu^2)$; it is also convex with respect to $\mu^2 (\mu^2 \geq 0)$. The optimum of μ^2 is existent and unique.

Proof: From Lemma 1, we initially know that $\|w_J\|^2$ can be represented as a function of μ^2, as follows:

$$\|w_J\|^2 = k\mu^2 \tag{23}$$

where $k > 0$ and

$$k = \left\| \begin{bmatrix} g^\dagger g & g^\dagger h \\ h^\dagger g & h^\dagger h \end{bmatrix}^{-1} (\|h\|^2 g - h^\dagger g h) \right\|^2 \tag{24}$$

The second objective is to determine the relationship between P_D and μ^2.

Without losing generality, we initially assume that $\zeta > 0$ and $\tilde{R}$ is positive definite. Let λ be one of the eigenvectors of matrix $\tilde{R}$. Hence, we have

$$\lambda w_D = \tilde{R} w_D \tag{25}$$

Multiplying both sides of Equation (12) with w_D / λ yields

$$w^\dagger_D w_D = w^\dagger_D \tilde{R} w_D / \lambda = \xi / \lambda \tag{26}$$

Minimizing $w^\dagger_D w_D$ is equivalent to maximizing λ; therefore, λ corresponds to the largest eigenvalue of $\tilde{R}$, and w_D should be the largest eigenvector of $\tilde{R}$.

By contrast, if $\zeta \leq 0$, then . $P_s \geq \dfrac{\sigma^2 (4^{R_s^0} - 1)}{|h_0| - 4^{R_s^0} |g_0|^2}$

However, if $P_s \geq \dfrac{\sigma^2 (4^{R_s^0} - 1)}{|h_0|^2 - 4^{R_s^0} |g_0|^2}$, then the destination can directly achieve secrecy rate R_s^0 in Stage 1. Node cooperation is not required in Stage 2, and thus, is meaningless for $\xi \leq 0$.

For simplicity, we define $p = \sigma^2 + \mu^2$, $v = 4^{R_s^0} \|g\|^2$, and $m = 4^{R_s^0} |gh|^2 / \sigma^2$. Evidently, $uv - m > 0$. Given that $R_h = hh^\dagger$ and $R_g = gg^\dagger$, $\tilde{R}$ can be expressed as

$$R = \frac{1}{\sigma^2} hh^\dagger - \frac{4^{R_s^0}}{p} gg^\dagger \tag{27}$$

According to Lemma 2, $\tilde{R}$ has only two non-zero eigenvalues. The positive eigenvalue is given by

$$\lambda = u/2 - v/2p + \frac{1}{2} \sqrt{(u + v/p)^2 - 4m/p} \tag{28}$$

Thus, P_D can be represented as a function of μ^2, as follows:

$$P_D(p) = \frac{2\zeta}{(u - v/p + \sqrt{u - v/p)^2 - 4m/p}} \tag{29}$$

According to Equations. (23) and (29), P_0 can be represented as a function of μ^2, as follows:

$$P_0 = \frac{2\zeta}{(u - v/p + \sqrt{u + v/p)^2 - 4m/p}} + P_s + k\mu^2 \tag{30}$$

Considering the second-order derivatives of $P_0(\mu^2)$with respect to μ^2, we can derive

$$\frac{\partial^2 P_0}{\partial (\mu^2)^2} = \frac{2\zeta m}{\left[\sqrt{(up - v)^2 + 4(uv - m)/p}\right]^3} \tag{31}$$

Verifying that $\frac{\partial^2 P_0}{\partial (\mu^2)^2} > 0$ is a straightforward process. is $P_0(\mu^2)$ convex with respect to μ^2. The constraint $\mu^2 \geq 0$ is obviously convex. Thus, the optimum of μ^2 is existent and unique. Theorem 1 is verified until this point.

First, if $\left.\frac{\partial P_0}{\partial (\mu^2)}\right|_{\mu^2 = 0} > 0$, then $\mu^2 = 0$, which corresponds to the case in the DF scheme.

Second, if , $\left.\frac{\partial P_0}{\partial (\mu^2)}\right|_{\mu^2 = 0} < 0$, then by considering the first-order derivative of $P_0(\mu^2)$ and setting it to zero, we can derive a quadratic equation of p.

$$Ap^2 + Bp + C = 0 \tag{32}$$

With $A = u^2 (u^2 - L^2)$, $B = 2uv - 4m) (u^2 - L^2)$, $C = (uv - 2m^2) - v^2 L^2$, and $L = u - 2k(uv - m) / \zeta$. Given that u^2 is a non-negative real number, $B^2 - 4Ac \geq 0$. Then, we have

$$64kmL^2 (uv - m)^2 [\zeta u - k(uv - m)] / \zeta \geq 0 \tag{33}$$

which must satisfy

$$\zeta u - k(uv - m) \geq 0 \tag{34}$$

After substituting Equation (24) into the preceding inequality equation and performing some manipulations, we can derive

$$4^{R_s^0} |g_0|^2 - |h_0|^2 \geq \sigma^2 / P_s \tag{35}$$

If the relation in Equation (35) is satisfied, then the proposed DFCJ scheme can work effectively to improve system performance. Given that $A > 0$, the roots of Equation (32) can be divided into three cases.

Case 1: $B > 0, C \geq 0$

A positive root does not exist.

Case 2: $B < 0, C \geq 0$

Two positive roots exist, i.e.,

$$p_1^* = \frac{\sqrt{B^2 - 4AC} - B}{2A} , p_2^* = \frac{-\sqrt{B^2 - 4Ac} - B}{2A} \tag{36}$$

Case 3: $C < 0$
The only positive root is given by

$$p^* = \frac{\sqrt{B^2 - 4AC} - B}{2A} \quad (37)$$

$p_2^* < \sigma^2$ is indicated in Equation (36). Hence, the optimal value of m^2 can be expressed as

$$\mu^2 = \frac{\sqrt{B^2 - 4AC} - B}{2A} - \sigma^2 \quad (38)$$

If the solution to Equation (38) is positive, then it must be the global optimum to Equation (22) because $P_0(\mu^2)$ is convex with respect to μ^2. Otherwise, $\mu^2 = 0$, which corresponds to the case of the DF scheme.

4.2 Selecting the Source Power

Theorem 2: Given the secrecy rate constraint , the total power consumption P_0 increases with P_s.

Proof: P_0 (P_s) can be expressed as

$$P_0 = \frac{2\zeta}{(u - v/p + \sqrt{u - v/p)^2 - 4m/p}} + P_s + k\mu^2 \quad (39)$$

Considering the first-order derivative of P_0 (P_s) with respect to P_s, we can derive

$$P'_0 = [\frac{\sqrt{m/k}}{2(uv - m)\sqrt{\zeta u - k(uv - m)}} + 1]\frac{\zeta'}{u} + 1 \quad (40)$$

where

$$P'_0 = \frac{\partial P_0}{\partial P_s} \text{ and } \zeta' = \frac{\partial \zeta}{\partial P_s} = 4^{R_s^0}|g_0|^2 - |h_0| / \sigma^2.$$

According to Equation (35), $4^{R_s^0}|g_0|^2 - |h_0|^2 \geq \sigma^2 / P_s$ hence, $\zeta \geq 1 / P_s$. Then, $P_0 \geq 1$. Thus, P'_0 increases with P_s. Theorem 2 has been proven until this point.

In Section 4.1, we assume that the source node transmits at a constant power. However, if the source node has a low transmission power, then the total transmit power P_s is also low. Hence, the minimal transmit power of the source should be at optimum value.

Considering that cooperative transmission is divided into two stages, the secrecy rate from the source to each relay in Stage 1 should not be less than that of the destination achieved in DFCJ. Therefore, to guarantee the given rate R_s^0 for each link $R_s^{(1)} \geq R_s^0$, must be satisfied. Hence, P_s must satisfy the relation

$$P_s \geq \frac{\sigma^2(4^{R_s^0} - 1)}{min\{|\eta_1|^2, |\eta_2|^2, \ldots, |\eta_N|^2\} - 4^{R_s^0}|g_0|^2} = P_s^{min} \quad (41)$$

Based on Equation (41), the relay with the worst channel toward the source imposes the transmit power level. According to Theorem 2, the minimal transmit power of the source is the optimal value of P_s.

First, based on Equation (41), the optimal value of P_s can be directly obtained. Then, the optimal value of μ^2 is computed using Equation (38). Based on the solution to the problem in Equation (22), the optimal weights w_D and w_J are achieved.

5. Numerical Results

In this section, several numerical simulations are presented to demonstrate the proposed scheme. The system configuration used in the present study is the same as those in some previous works, such as [13] and [17], in which the source, the destination, and the eavesdropper are placed along a line. To emphasize the effect of distances, the channel model between any two nodes is a line-of-sight channel model: $d^{-c/2}e^{i\theta}$, where d is the distance between any two nodes, $c = 3.5$ is the path loss exponent, and θ is the phase uniformly distributed within $[0, 2\pi]$. We assume that the distances between relay nodes are considerably smaller than the distances between relay nodes and the source/destination/ eavesdropper, such that path losses between different relay nodes and the source/destination can be regarded as approximately the same. The source, destination, and eavesdropper are located at fixed 2D coordinates (0, 0), (100, 0), and (60, 0), respectively (unit: meters). Noise power is $\sigma^2 = -90$ dBm. To obtain the average results, Monte Carlo experiments with 1000 independent trials are conducted.

The total transmit power is shown in Figure 2, where the secrecy rate constraint is fixed at $R_S^0 = 1$ bit/s/Hz. Some of the relays ($R_{1,2,\ldots,5}$) are fixed at $(5, 5)$, whereas the others ($R_{6,7,\ldots,10}$) are moved from point $(5, 5)$ to point $(95, 5)$ along a line. First, moving the position of relays $R_{6,7,\ldots,10}$ from (5, 5) to (39, 5), all relays implement the DFCJ and DF schemes in Stage 2, the two curves are labeled $R_{1,2,\ldots,10}$(DFCJ) and $R_{1,2,\ldots,10}$(DF), respectively. Then, the position of relays $R_{6,7,\ldots,10}$ is moved from (5, 5) to (95, 5). Two simulations for two cases are also conducted. In the first case, relays $R_{1,2,\ldots,5}$ perform the DFCJ scheme, whereas relays $R_{6,7,\ldots,10}$ implement Stage 2 of the CJ scheme. The curve is labeled $R_{1,2,\ldots,5}$(DFCJ), $R_{6,7,\ldots,10}$(CJ). In another case, relays $R_{1,2,\ldots,5}$ perform the DF scheme, whereas relays $R_{6,7,\ldots,10}$ are not involved in any cooperation. The curve is labeled $R_{1,2,\ldots,5}$(DF).

As shown in Figure 2, when $R_{6,7,\ldots,10}$ are at the left side of the double vertical line marked by arrow "A", optimal performance (i.e., the minimal total transmit power) can be achieved if all the relays perform the DF scheme because $R_{6,7,\ldots,10}$ are extremely close to the source and relatively far from the eavesdropper. Hence, the source uses minimal power to achieve the secrecy rate R_S^0 at $R_{6,7,\ldots,10}$ in Stage 1. Spending considerable power in transmitting the jamming signal in this situation is impractical. The power of the message signal

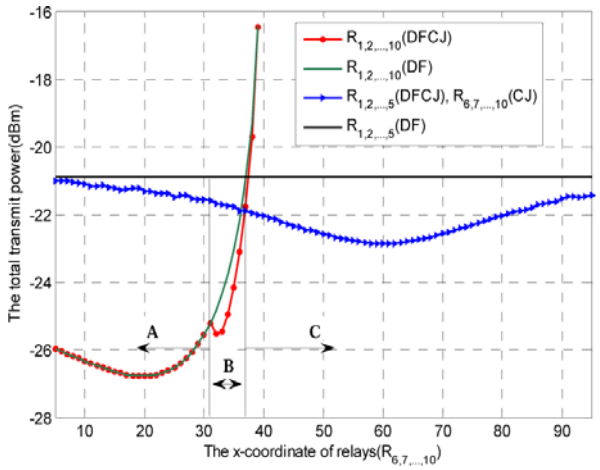

Figure 2. Total transmit power versus the *x* coordinate of $R_{6,7,\ldots,10}$. The position of $R_{6,7,\ldots,10}$ changes from (5, 5) to (95, 5)

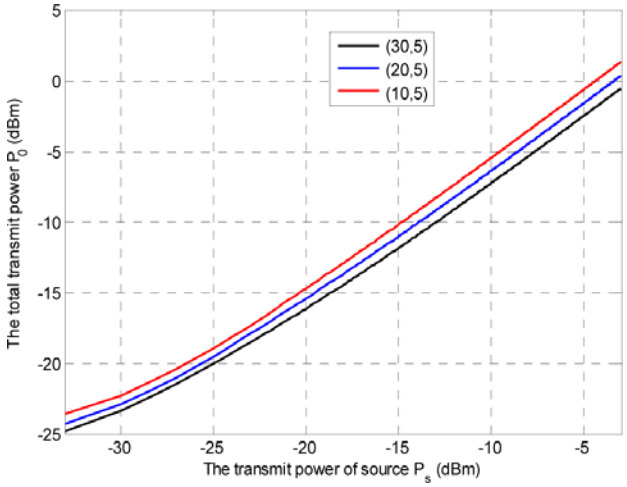

Figure 3. Total transmit power versus P_s. The value of P_s varies from 5×10^{-7}W to 5×10^{-4}W

received at the eavesdropper is always minimal (regardless of jamming) because of the large path loss in Stage 2. When $R_{6,7,\ldots,10}$ are in the middle of double vertical line marked by arrow "B", optimal performance can be achieved if all the relays implement the DFCJ scheme. In this situation, $R_{6,7,\ldots,10}$ are sufficiently close to the eavesdropper. Hence, spending power to transmit the jamming signal is practical, i.e., more power can be saved in transmitting the message signal. This finding explains the advantage of the DFCJ scheme over the DF scheme. Lastly, when $R_{6,7,\ldots,10}$ are located at the right side of the double vertical line marked by arrow "C", optimal performance can be achieved. If $R_{1,2,\ldots,5}$ perform the DFCJ scheme and $R_{6,7,\ldots,10}$ implement the CJ scheme, then spending a large amount of power to achieve the secrecy rate R_s^0 at $R_{6,7,\ldots,10}$ in Stage 1 is impractical. Given that $R_{6,7,\ldots,10}$ are far from the source but close to the eavesdropper, they should not perform the DF scheme and simply transmit the jamming signal in Stage 2 to confound the eavesdropper, and consequently, save more power. Thus, $R_{1,2,\ldots,5}$ and $R_{6,7,\ldots,10}$ are both involved in the proposed scheme.

As shown in Figure 3, simulations for $R_{6,7,\ldots,10}$ at (10, 5), (20, 5), and (30, 5) are conducted. As expected, the total transmit power increases with the source power.

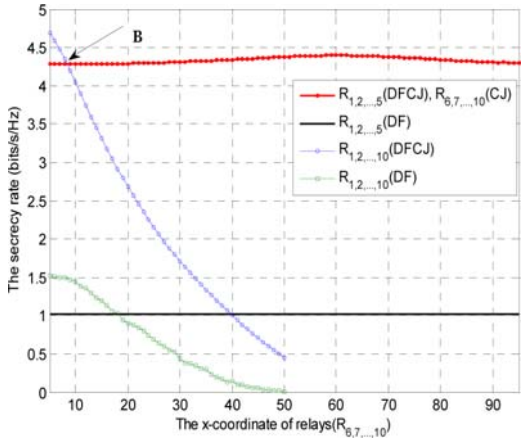

Figure 4. Secrecy rate versus the *x* coordinate of relays. The position of $R_{6,7,\ldots,10}$ varies from (5, 5) to (95, 5)

The secrecy rate is shown Figure 4, in which the total transmit power constraint is fixed at $P_0 = 10^{3}$ W. Some of the relays $R_{1,2,\ldots,5}$ are also fixed at (5, 5), whereas the rest $R_{6,7,\ldots,10}$ are moved from point (5, 5) to point (95, 5) along a line. First, after moving the position of $R_{6,7,\ldots,10}$ from (5, 5) to (50, 5), all the relays perform the DFCJ and DF schemes in Stage 2; the two curves are labeled $R_{1,2,\ldots,5}$(DFCJ) and $R_{1,2,\ldots,5}$(DF). Given that the position of relays $R_{6,7,\ldots,10}$ is moved from (5, 5) to (95, 5), two simulations are conducted for two cases. In the first case, $R_{1,2,\ldots,5}$ perform the DFCJ scheme, whereas $R_{6,7,\ldots,10}$ implement the CJ scheme in Stage 2. The curves are labeled $R_{1,2,\ldots,5}$(DFCJ) and $R_{6,7,\ldots,10}$(CJ). In the second case, $R_{1,2,\ldots,5}$ perform the DF scheme, whereas $R_{6,7,\ldots,10}$ are not involved in any cooperation. The curve is labeled $R_{1,2,\ldots,5}$(DF).

As shown in Figure 4, when $R_{6,7,\ldots,10}$ are located at the eft side of the point marked by arrow "B", optimal

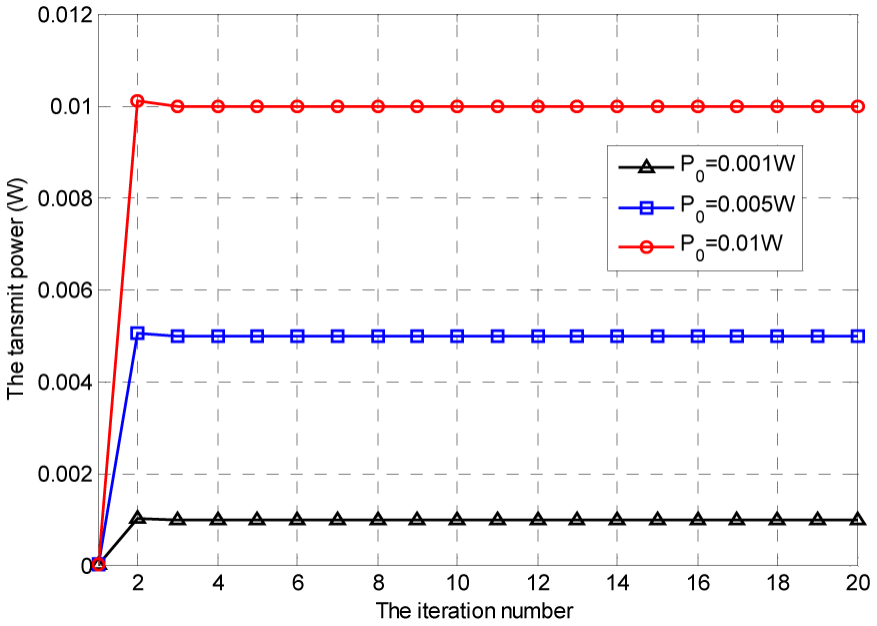

Figure 5. Convergence speed observation under different total transmit power constraints P_0

performance (i.e., maximal secrecy rate) can be achieved if all the relays perform the DFCJ scheme because $R_{6,7,\ldots,10}$ are extremely close to the source. The source can use minimal power to achieve the secrecy rate R_s at $R_{6,7,\ldots,10}$ in Stage 1. Furthermore, spending power to transmit jamming signals in Stage 2 is practical. The achieved secrecy rate will increase if minimal power is available for the relays to transmit jamming signals, even if the available power for relays to transmit message signals decreases. This finding explains the advantage of using the DFCJ scheme over the DF scheme. Meanwhile, when $R_{6,7,\ldots,10}$ are located at the right side of the point marked by arrow "B", optimal performance can be achieved. If $R_{1,2,\ldots,5}$ perform the DFCJ scheme, whereas $R_{6,7,\ldots,10}$ implement the CJ scheme, then spending a large amount of power to achieve the secrecy rate R_s at $R_{6,7,\ldots,10}$ in Stage 1 is impractical. Given that $R_{6,7,\ldots,10}$ are far from the source but close to the eavesdropper; these relays should not apply the DF scheme. Moreover, the same power can be used to achieve a high secrecy rate if $R_{6,7,\ldots,10}$ only transmit jamming signals to confound the eavesdropper in Stage 2. Thus, $R_{1,2,\ldots,5}$ and $R_{6,7,\ldots,10}$ are both cooperating in the proposed scheme.

As shown in Figure 5, simulations for the total transmit power constraints $P_0 = 0.001\ W$, $P_0 = 0.005\ W$, and $P_0 = 0.01\ W$ are conducted. The proposed iterative algorithm exhibits fast convergence toward the total transmit power, taking less than 10 iterations for P_s to converge to the optimum.

The results show that the DFCJ scheme can significantly improve system performance compared with the DF scheme presented in [13] and [17]. Given that DF is a special case of DFCJ for $P_J = 0$, the performance of DFCJ is not worse than that of DF. Furthermore, more cooperation nodes may be involved in the DFCJ scheme.

Conclusion

In this study, a novel system design has been proposed to allocate transmit power among the source and the relays, as well as to determine relay weights. These steps improve the performance of secure wireless communications in the presence of an eavesdropper. The proposed cooperative scheme, i.e., DFCJ, is designed to minimize the total transmit power subject to a secrecy rate constraint or maximize the achievable secrecy rate subject to a total transmit power constraint. Through analyses and numerical evaluations, we have demonstrated that the proposed DFCJ scheme can overcome the traditional limitations in channel conditions and significantly improve system performance compared with the DF scheme.

Future research includes a system design for cooperative schemes that uses partial CSI or channel statistics on eavesdropper channels. The effects of the ergodic secrecy rate and outage probability can also be explored. Further study is also required for the cases with more than one eavesdropper.

Acknowledgements

This work was supported by the National Science Foundation of China under Grant No. 61461018, the National Natural Science Foundation of China under Grant No. 61261016, and the Natural Science Foundation of Hubei Province under Grant No. 2014CFC1124.

References

[1] Bloch, M., Barros, J., Rodriques, M. R. D., McLaughlin, S. W. (2008). Wireless Information-theoretic Security. *IEEE Transactions on Information Theory*, 54 (1) 2515-2534.

[2] Lai, L., El Gamal, H. (2008). The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Transactions on Information Theory*, 54 (9) 4005-4019.

[3] Wyner, A. D. (1975). The wire-tap channel. *Bell Syst. Tech. J.*, 54 (8)1355-1387.

[4] Csiszár, I., Korner, J. (1978). Broadcast channels with confidential messages. *IEEE Transactions on InformationTheory*, 24 (1)339-348.

[5] Oggier, F., Hassibi, B. (2008). The secrecy capacity of the MIMO wiretap channel, *In: Proceedings of the 2008 IEEE International Smposium on Information theory*, p 524-528. Toronto, ON, July.

[6] Parada, P., Blahut, R. (2005). Secrecy capacity of SIMO and slow fading channels. *In: Proceedings of the IEEE International Smposium on Information Theory*, p 2152-2155. Adelaide, Australia, September.

[7] Shafiee, S., Ulukus, S. (2007). Achievable rates in Gaussian MISO channels with secrecy constraints. *In: Proceedings of the IEEE International Smposium on Information Theory*, p 112-119. Nice, France, June.

[8] Popovski Petar, Simeone Osvaldo. (2009). Wireless Secrecy in Cellular Systems With Infrastructure-Aided Cooperation. *IEEE Transaction on Information Forensics and Security*, 4 (2) 242-256.

[9] Krikidis, I., Thompson, J. S., McLaughlin, S. (2009). Relay selection for secure cooperative networks with jamming. *IEEE Transaction on Wireless Communications*, 51 (1) 5003-5011.

[10] Dong, L., Han, Z., Petropulu, A., Poor, H. V. (2008). Secure wireless communications via cooperation. *In:* Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing, p 1132-1138. UIUC, Illinois, USA, September.

[11] Dong, L., Han, Z., Petropulu, A., Poor, H. V. (2009). Amplify-and-forward based cooperation for secure wireless communications. *In: Proceedings of the IEEE Int. Conf. Acoust., Speech, Signal Process*, p 1-6. Taipei, Taiwan, Apr.

[12] Dong, L., Han, Z., Petropulu, A., Poor, H. V. (2009). Cooperative jamming for wireless physical layer security. *In:* Proceedings of the IEEE Statistical Signal Processing Workshop, p. 11-16. Cardiff, Wales, U.K., Aug-Sep.

[13] Dong, L., Han, Z., Petropulu, A., Poor, H. V.(2010). Improving wireless physical layer security via Cooperative relays. *IEEE Transaction on Signal Processing*, 58 (3) 1875-1888.

[14] Zhang, J., Gursoy, M. (2010). Collaborative relay beamforming for secrecy. *In:* Proceedings of the IEEE International Conference on Communications (ICC10), p 1-5. Cape Town, June. 2010.

[15] Zhang, R., Song, L., Han, Z., Jiao, B. (2010). Physical layer security for two way relay communications with friendly jammers. *In:* Proceedings of the IEEE Global Communications Conference, p 111-116. Miami, Florida, USA, Dec.

[16] Ding, ZG., Leung, KK., Goeckel, DL., Towsley, D (2011). Opportunistic Relaying for Secrecy Communications: Cooperative Jamming vs. Relay Chatting. *IEEE Transaction on Wireless Communications*, 10 (6) 1725-1729.

[17] Li, Jiangyuan., Petropulu, Athina P., Weber, Steven

(2011). On Cooperative Relaying Schemes for Wireless Physical Layer Security. *IEEE Transaction on Signal Processing*, 59 (10) 4985-4997.

[18] Godara, L. C. (1997). Application of antenna arrays to mobile communications, Part II: Beam-forming and direction-of-arrival considerations. *Proc. IEEE.* 85 (1) 1195-1245.

[19]Krzysztof, Stepien. (2014). Research on a surface texture analysis by dig ital signal processing methods. *Tehnicki Vjesnik*, 21 (3)485-493.