Cooperative Beamformer Design for Improving Physical Layer Security in Multi-Hop Decode-and-Forward Relay Networks

Han-Byul Lee[1], Jong-Ho Lee[2] and Seong-Cheol Kim[1]
[1] School of Electrical Engineering and Computer Science, Seoul National University
Seoul 151-742, Korea
[e-mail: hblee,sckim@maxwell.snu.ac.kr]
[2] Department of Electronic Engineering, Gachon University
Seongnam, Gyeonggi 461-701, Korea
[e-mail: jongho.lee@gachon.ac.kr]
*Corresponding author: Jong-Ho Lee

Received September 4, 2015; revised October 27, 2015; accepted November 22, 2015; published January 31, 2016

Abstract

In this paper, we consider secure communications in multi-hop relaying systems, where multiple decode-and-forward (DF) relays are located at each individual hop and perform cooperative beamforming to improve physical layer security. In order to determine the cooperative relay beamformer at each hop, we propose an iterative beamformer update scheme using semidefinite relaxation and bisection techniques. Numerical results are presented to verify the secrecy rate performance of the proposed scheme.

Keywords: Physical layer security, relay networks, cooperative beamforming, secrecy rate

This research was supported in part by the Gachon University research fund of 2015 (GCU-2015-0084), and in part by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2013R1A1A1A05004401).

http://dx.doi.org/10.3837/tiis.2016.01.011 **ISSN : 1976-7277**

1. Introduction

Recently, physical layer security schemes have been widely studied to overcome the broadcast nature of wireless channels and enable secure communications by exploiting the physical characteristic of wireless channels itself without using upper-layer operations such as encryption techniques [1]. In an information theoretic point of view, the rate at which the source can send secure information to the intended destination without being eavesdropped by unintended receivers is defined as achievable secrecy rate. Further, the maximum achievable secrecy rate is referred to as secrecy capacity.

It is shown that positive secrecy rates can be achieved without using upper-layer operations as long as the source-eavesdropper channel is a degraded version of the source-destination channel [2]. Further, node cooperation approaches have been suggested to achieve positive secrecy rates even when the source-destination channel condition is worse than the source-eavesdropper channel condition. In [3]-[10], node cooperation approaches have been considered, where multiple relay nodes located between the source, destination, and eavesdroppers perform cooperative beamforming for improving secrecy rates, assuming that each node is equipped with a single antenna. In particular, [3] has suggested three different operation modes for cooperative relay nodes such as amplify-and-forward (AF), decode-and-forward (DF), and cooperative jamming (CJ). For AF and DF modes, the relay nodes receive the signal from the source in the first time slot. In the second time slot, the AF and DF relay nodes forward the weighted versions of its received signals and its re-encoded signals, respectively. On the other hand, the CJ relay nodes transmit the weighted jamming signals to interfere the eavesdroppers.

Since most of the previous works for node cooperation consider two-hop relaying systems, we investigate wireless multi-hop relaying systems, where more than two hops are required. Further, we consider that each node receives the signals only from the nodes located at the adjacent hop due to propagation losses. At each hop, multiple DF relays perform cooperative beamforming to forward information signals to the next nodes as well as minimize the leakage to the eavesdropper. One of the conventional relay beamformers in node cooperation approaches is a zero-forcing (ZF) beamformer to null out the signal at the eavesdropper. In [3] and [5], a generalized eigenvector problem for the relay beamformer design has been formulated and solved to improve the secrecy rate. However, this approach is tailored only for use in two-hop relaying systems. In multi-hop DF relaying systems, cooperative beamformer design at each hop should consider not only the rates at the destination and the eavesdropper to maximize the secrecy rate, but also the rates at the relays located at the next hops to satisfy the DF relaying constraints.

In this paper, we derive a relay beamformer design problem in a multi-hop DF relay network, which includes mode than two hops, and propose an iterative beamformer design scheme. In the proposed scheme, the relay beamformers are initialized by the conventional ZF and max-min fair (MMF) beamforming approaches [11]. Then, the relay beamformer at each hop is sequentially updated by using semidefinite relaxation and bisection techniques [12], [13]. Numerical results are presented to show that the proposed scheme significantly improves the secrecy rates compared to the conventional beamformers.

2. System Model

Let us consider a wireless (M+1)-hop DF relay network, which consists of one source node S, N_m DF relays at the R_m relay position with m = 1,2,…,M, one destination node D, and one eavesdropper E. It is assumed that R_m's and D receive the signal from only their adjacent nodes due to the propagation loss, whereas E overhears S as well as all the relays. All channels between the nodes undergo flat fading and the noise at each node is complex additive white Gaussian with zero-mean and variance σ^2.

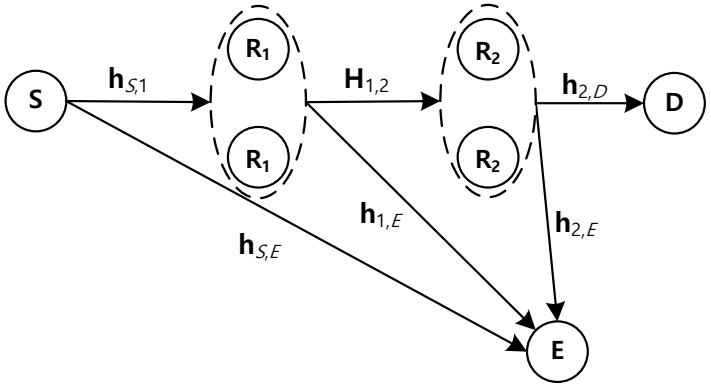


Fig. 1. Illustration of a multi-hop relay network for M=2 and N_1=N_2=2

In the 0th time slot, S sends a data symbol x with unit power and the received signals at R_1's and E can be expressed as

$$\begin{aligned} \mathbf{y}_1(0) &= \sqrt{P_S}\mathbf{h}_{S,1}x + \mathbf{z}_1(0), \\ y_E(0) &= \sqrt{P_S}h_{S,E}x + z_E(0), \end{aligned} \tag{1}$$

where $\mathbf{h}_{S,1}$ denote the complex N_1×1 channel vector between S and N_1 relays located at the R_1 relay position, the complex S-E channel gain is denoted as $h_{S,E}$, P_S is the transmit power of S, and $\mathrm{z}_n(0)$ and $z_E(0)$ denote additive white Gaussian noise at R_n's and E, respectively. Let all R_m's decode x successfully in the (m-1)th time slot. Then, the ith R_m transmits a weighted version of the re-encoded symbol, $w_{m,i}x$, to the next nodes in the mth time slot. Here, we define $w_{m,i}$ as the weight of the ith R_m with i=1, 2, …, N_m and let the weights of all R_m's be stacked in a $N_m \times 1$ vector $\mathbf{w}_m$ with $\mathbf{w}_m^{\dagger}\mathbf{w}_m = P_m$, where P_m is the total transmit power consumed by R_m's. This implies that multiple single-antenna relays located at the R_m relay position form a virtual antenna array and cooperatively perform transmit beamforming with the relay weight vector $\mathbf{w}_m$ [14]. In this viewpoint, we refer to $\mathbf{w}_m$ as a cooperative beamformer of R_m's [7], [8], [10]. The received signals in the mth time slot can be given as

$$\begin{aligned} \mathbf{y}_{m+1}(m) &= \mathbf{H}_{m,m+1}\mathbf{w}_m x + \mathbf{z}_{m+1}(m), \\ y_E(m) &= \mathbf{h}_{m,E}\mathbf{w}_m x + z_E(m), \end{aligned} \tag{2}$$

where the *i*th row of $\mathbf{H}_{m,m+1}$ is $\mathrm{h}_{m,m+1}^{(i)}$, which denotes the $1 \times N_m$ channel vector between N_m relays located at the R_m relay position and the *i*th R_{m+1}, $\mathbf{h}_{m,E}$ denotes the $1 \times N_m$ channel vector for R_m's-*E*, and $(.)^{\dagger}$ is the conjugated transpose. Finally, when all R_M's decode *x* successfully in the (*M*-1)th time slot and forward the re-encoded symbol in the *M*th time slot, we express the received signals at *D* and *E* in the *M*th time slot shown as

$$\begin{aligned} y_D(M) &= \mathbf{h}_{M,D}\mathbf{w}_M x + z_D(M), \\ y_E(M) &= \mathbf{h}_{M,E}\mathbf{w}_M x + z_E(M), \end{aligned} \tag{3}$$

where $\mathbf{h}_{M,D}$ and $\mathbf{h}_{M,E}$ denote the $1 \times N_M$ channel vectors for R_M's-*D* and R_M's-*E* channels, respectively, and $z_D(M)$ is additive white Gaussian noise at *D*. **Fig. 1** illustrates a multi-hop relay network model described above for $M = 2$ and $N_1 = N_2 = 2$.

Let us assume that *E* performs maximal ratio combining to decode *x* [3]. From (1)-(3), we obtain the rates at *D* and *E* shown as

$$\begin{aligned} \gamma_D &= \frac{1}{M+1}\log_2\left(1 + P_M \widehat{\mathbf{w}}_M^{\dagger}\mathbf{R}_{M,D}\widehat{\mathbf{w}}_M\right), \\ \gamma_E &= \frac{1}{M+1}\log_2\left(1 + \alpha_{S,E} + \sum_{m=1}^{M} P_m \widehat{\mathbf{w}}_m^{\dagger}\mathbf{R}_{m,E}\widehat{\mathbf{w}}_m\right), \end{aligned} \tag{4}$$

where $\widehat{\mathbf{w}}_m = \mathbf{w}_m/\sqrt{\mathrm{P}_m}$, $\alpha_{S,E} = P_S|h_{S,E}|^2/\sigma^2$, $\mathbf{R}_{M,D} = \mathbf{h}_{M,D}^{\dagger}\mathbf{h}_{M,D}/\sigma^2$, and $\mathbf{R}_{m,E} = \mathbf{h}_{m,E}^{\dagger}\mathbf{h}_{m,E}/\sigma^2$. The factor of $\frac{1}{M+1}$ is due to the fact that the information is transmitted over (*M*+1) time slots. The rate at the *i*th R_m is given as

$$\begin{aligned} \gamma_1^{(i)} &= \frac{1}{M+1}\log_2\left(1 + \alpha_{S,1}^{(i)}\right), \\ \gamma_m^{(i)} &= \frac{1}{M+1}\log_2\left(1 + P_{m-1}\widehat{\mathbf{w}}_{m-1}^{\dagger}\mathbf{R}_{m-1,m}^{(i)}\widehat{\mathbf{w}}_{m-1}\right), \end{aligned} \tag{5}$$

where $\alpha_{S,1}^{(i)} = P_S|h_{S,1}^{(i)}|^2/\sigma^2$, $\mathbf{R}_{m-1,m}^{(i)} = (\mathbf{h}_{m-1,m}^{(i)})^{\dagger}\mathbf{h}_{m-1,m}^{(i)}/\sigma^2$ with $i = 1,2,\ldots,N_m$, and $h_{S,1}^{(i)}$ denotes the *i*th entry of $\mathbf{h}_{S,1}$. Since the rates at the relays should be equal to or greater than the rate at *D* for the DF relaying [3], we can compute the achievable secrecy rate shown as

$$\gamma = \max\left\{\min\{\gamma_D, \gamma_1, \ldots, \gamma_M\} - \gamma_E, 0\right\}, \tag{6}$$

where $\gamma_m = \min_{i=1,\ldots,N_m} \gamma_m^{(i)}$.

3. Cooperative Beamformer Design

Let us assume global channel state information (CSI), which is available when the eavesdropper is another legitimate user in the network and its transmission can be monitored [15]. In this scenario, the eavesdropper is assumed to be a low-level user to access less information than the destination. In order to maximize the achievable secrecy rate, we have to solve the following optimization problem for the cooperative beamformer design:

$$\begin{aligned}\max_{\widehat{\mathbf{w}}_1,\widehat{\mathbf{w}}_2,\ldots,\widehat{\mathbf{w}}_M} \quad & \frac{1+P_M\widehat{\mathbf{w}}_M^{\dagger}\mathbf{R}_{M,D}\widehat{\mathbf{w}}_M}{1+\alpha_{S,E}+\sum_{m=1}^{M}P_m\widehat{\mathbf{w}}_m^{\dagger}\mathbf{R}_{m,E}\widehat{\mathbf{w}}_m}\\ \text{s.t.} \quad & \min_{i=1,\ldots,N_1}\alpha_{S,1}^{(i)} \geq P_M\widehat{\mathbf{w}}_M^{\dagger}\mathbf{R}_{M,D}\widehat{\mathbf{w}}_M\\ & \min_{i=1,\ldots,N_m}P_{m-1}\widehat{\mathbf{w}}_{m-1}^{\dagger}\mathbf{R}_{m-1,m}^{(i)}\widehat{\mathbf{w}}_{m-1} \geq P_M\widehat{\mathbf{w}}_M^{\dagger}\mathbf{R}_{M,D}\widehat{\mathbf{w}}_M, \quad m=2,3,\ldots,M\\ & \widehat{\mathbf{w}}_m^{\dagger}\widehat{\mathbf{w}}_m=1, \quad m=1,2,\ldots,M. \end{aligned} \tag{7}$$

The inequality constraints in (7) are the DF relaying constraints, which guarantee that all the relays correctly decode the information signal and forward it to the next nodes [3], [5]. Since it is hard to obtain the optimal solution of (7), we propose a suboptimal iterative approach as follows.

3.1 Initialization

In (2), it is observed that the beamformed signal of R_m's is destined for R_{m+1}'s. In order to initialize $\widehat{\mathbf{w}}_m$ with m = 1,2,…,M-1, we maximize the minimum channel gain of the next adjacent relays (i.e., $\widehat{\mathbf{w}}_m^{\dagger}\mathbf{R}_{m,m+1}^{(i)}\widehat{\mathbf{w}}_m$ in (7)) as well as null out the signal at E shown as

$$\breve{\mathbf{w}}_m = \text{argmax}_{\widetilde{\mathbf{w}}_m}\min_{i=1,\ldots,N_{m+1}}\left|\mathbf{h}_{m,m+1}^{(i)}\left(\mathbf{I}_{N_m}-\mathbf{P}_{m,E}\right)\widetilde{\mathbf{w}}_m\right|^2, \tag{8}$$

where $\mathbf{I}_k$ denotes a $k \times k$ identity matrix and $\mathbf{P}_{m,E}=\mathbf{h}_{m,E}^{\dagger}(\mathbf{h}_{m,E}\mathbf{h}_{m,E}^{\dagger})^{-1}\mathbf{h}_{m,E}$ [3]. The optimization problem in (8) can be considered as a MMF beamforming problem in a wireless broadcasting scenario, which can be solved by using the semidefinite relaxation and randomization technique as in [11]. Using $\breve{\mathbf{w}}_m$ in (8), we compute $\widehat{\mathbf{w}}_m$ shown as

$$\widehat{\mathbf{w}}_m = \frac{\left(\mathbf{I}_{N_m}-\mathbf{P}_{m,E}\right)\breve{\mathbf{w}}_m}{\left\|\left(\mathbf{I}_{N_m}-\mathbf{P}_{m,E}\right)\breve{\mathbf{w}}_m\right\|}. \tag{9}$$

We refer to (9) as a MMF-ZF beamformer. In order to initialize $\widehat{\mathbf{w}}_M$, we use the conventional ZF beamformer [3] shown as

$$\widehat{\mathbf{w}}_M = \frac{\left(\mathbf{I}_{N_M}-\mathbf{P}_{M,E}\right)\mathbf{h}_{M,D}^{\dagger}}{\left\|\left(\mathbf{I}_{N_M}-\mathbf{P}_{M,E}\right)\mathbf{h}_{M,D}^{\dagger}\right\|}, \tag{10}$$

Using the initial beamformers, we compute the initial secrecy rate as in (6).

3.2 Iterative Update

After initializing the beamformers, we propose to update $\widehat{\mathbf{w}}_m$ sequentially from m=M to 1 at each iteration using semidefinite relaxation and bisection techniques. The iteration continues until the secrecy rate cannot be enhanced.

Let us first update $\mathbf{w}_M=\sqrt{P_M}\widehat{\mathbf{w}}_M$ using given $\widehat{\mathbf{w}}_m$ with $m\neq M$ computed at the previous iteration. Then, we can set $\alpha_{m,E}=P_m\widehat{\mathbf{w}}_m^{\dagger}\mathbf{R}_{m,E}\widehat{\mathbf{w}}_m$ and $\alpha_{m,m+1}^{(i)}=P_m\widehat{\mathbf{w}}_m^{\dagger}\mathbf{R}_{m,m+1}^{(i)}\widehat{\mathbf{w}}_m$, and (7) can be rewritten as

$$\begin{aligned}\max_{\mathbf{w}_M} \quad & \frac{1+\mathbf{w}_M^{\dagger}\mathbf{R}_{M,D}\mathbf{w}_M}{\beta_E^{(M)}+\mathbf{w}_M^{\dagger}\mathbf{R}_{M,E}\mathbf{w}_M} \\ \text{s.t.} \quad & \min_{i=1,\ldots,N_1} \alpha_{S,1}^{(i)} \geq \mathbf{w}_M^{\dagger}\mathbf{R}_{M,D}\mathbf{w}_M \\ & \min_{i=1,\ldots,N_m} \alpha_{m,m+1}^{(i)} \geq \mathbf{w}_M^{\dagger}\mathbf{R}_{M,D}\mathbf{w}_M, \;\; m=1,2,\ldots,M-1 \\ & \mathbf{w}_M^{\dagger}\mathbf{w}_M = P_M, \end{aligned} \tag{11}$$

where $\beta_E^{(M)} = 1 + \alpha_{S,E} + \sum_{m=1}^{M-1} \alpha_{m,E}$. Note that (11) is equivalent to

$$\begin{aligned}\max_{\mathbf{W}_M,t} \quad & t, \\ \text{s.t.} \quad & \mathrm{tr}\left(\mathbf{W}_M\left(\mathbf{R}_{M,D}-t\mathbf{R}_{M,E}\right)\right) \geq t\beta_E^{(M)}-1, \\ & \mathrm{tr}\left(\mathbf{W}_M\mathbf{R}_{M,D}\right) \leq \min_{i=1,\ldots,N_1} \alpha_{S,1}^{(i)}, \\ & \mathrm{tr}\left(\mathbf{W}_M\mathbf{R}_{M,D}\right) \leq \min_{i=1,\ldots,N_{m+1}} \alpha_{m,m+1}^{(i)}, m=1,2,\ldots,M-1, \\ & \mathrm{tr}(\mathbf{W}_M)=P_M, \; \mathrm{rank}\,\mathbf{W}_M=1, \; \mathbf{W}_M \succcurlyeq 0, \end{aligned} \tag{12}$$

where $\mathbf{W}_M = \mathbf{w}_M\mathbf{w}_M^{\dagger}$, tr(.) denotes the trace operation, and $\mathbf{W}_M \succcurlyeq 0$ indicates that $\mathbf{W}_M$ is a Hermitian positive semidefinite matrix [16]. Here, we use semidefinite relaxation and bisection technique studied in [12] to solve (12).

In (12), we employ a semidefinite relaxation to ignore the rank constraint [12], [13]. Then, we have

$$\begin{aligned}\max_{\mathbf{W}_M,t} \quad & t, \\ \text{s.t.} \quad & \mathrm{tr}\left(\mathbf{W}_M\left(\mathbf{R}_{M,D}-t\mathbf{R}_{M,E}\right)\right) \geq t\beta_E^{(M)}-1, \\ & \mathrm{tr}\left(\mathbf{W}_M\mathbf{R}_{M,D}\right) \leq \min_{i=1,\ldots,N_1} \alpha_{S,1}^{(i)}, \\ & \mathrm{tr}\left(\mathbf{W}_M\mathbf{R}_{M,D}\right) \leq \min_{i=1,\ldots,N_{m+1}} \alpha_{m,m+1}^{(i)}, m=1,2,\ldots,M-1, \\ & \mathrm{tr}(\mathbf{W}_M)=P_M, \; \mathbf{W}_M \succcurlyeq 0, \end{aligned} \tag{13}$$

First, let us assume that t_{max} is the maximum value of t obtained by solving the optimization problem (13). For any given t, we aim to figure out whether we can obtain $\mathbf{W}_M$ which satisfies the constraints in (13) or not. This can be revealed by solving the following convex feasibility problem:

$$\begin{aligned}\text{find} \quad & \mathbf{W}_M, \\ \text{such that} \quad & \mathrm{tr}\left(\mathbf{W}_M\left(\mathbf{R}_{M,D}-t\mathbf{R}_{M,E}\right)\right) \geq t\beta_E^{(M)}-1, \\ & \mathrm{tr}\left(\mathbf{W}_M\mathbf{R}_{M,D}\right) \leq \min_{i=1,\ldots,N_1} \alpha_{S,1}^{(i)}, \\ & \mathrm{tr}\left(\mathbf{W}_M\mathbf{R}_{M,D}\right) \leq \min_{i=1,\ldots,N_{m+1}} \alpha_{m,m+1}^{(i)}, m=1,2,\ldots,M-1, \\ & \mathrm{tr}(\mathbf{W}_M)=P_M, \;\; \mathbf{W}_M \succcurlyeq 0. \end{aligned} \tag{14}$$

If the above problem is feasible for the given t, then we have $t_{max} \geq t$. Otherwise, it is obvious that $t_{max} < t$. Therefore, we can check whether the given value t is greater than or less than the optimal solution t_{max} by solving the convenx feasibility problem in (14) [12]. Based on this

observation, we employ a bisection technique [16] and start with an interval $[l, u]$, which is assumed to contain the optimal value $t_{\max}$. At the midpoint of the interval $t = (l+u)/2$, we solve the convex feasibility problem in (14). Then, we update the interval according to the feasibility of (14). If the problem is feasible, then we set $l = t$. Otherwise, $u = t$ is chosen. For the updated interval, we solve (14) again. The well-established interior-point-based package such as SeDuMi [17] and Yalmip [18] are used to solve the convex feasibility problem, which provides a feasibility certificate if the problem is feasible. We repeat the above process until the interval is small enough.

Note that the bisection technique requires the initial lower and upper values. In this work, we set the initial lower value as zero. For the initial upper value, it is reasonable to assume that the secrecy rate without the DF relaying constraints is larger than that with the DF relaying constraints. Therefore, we set the initial upper value as the maximal value of the objective function in (11) after ignoring the DF relaying constraints. Then, the problem in (11) becomes

$$\begin{aligned} &\max_{\widehat{\mathbf{w}}_M} \ \frac{\widehat{\mathbf{w}}_M^{\dagger}\bar{\mathbf{R}}_{M,D}\widehat{\mathbf{w}}_M}{\widehat{\mathbf{w}}_M^{\dagger}\bar{\mathbf{R}}_{M,E}\widehat{\mathbf{w}}_M}, \\ &s.t. \quad \widehat{\mathbf{w}}_M^{\dagger}\widehat{\mathbf{w}}_M = 1, \end{aligned} \tag{15}$$

where $\bar{\mathbf{R}}_{M,D} = \mathbf{I}_{N_M} + P_M\mathbf{R}_{M,D}$ and $\bar{\mathbf{R}}_{M,E} = \beta_E^{(M)}\mathbf{I}_{N_M} + P_M\mathbf{R}_{M,E}$. The problem in (15) is a generalized eigenvector problem and $\widehat{\mathbf{w}}_M$ can be determined as the eigenvector corresponding to the largest eigenvalue of the matrix $\bar{\mathbf{R}}_{M,E}^{-1}\bar{\mathbf{R}}_{M,D}$.

Furthermore, due to the semidefinite relaxation, the solution $\mathbf{W}_M^*$ may not be of rank one in general. When $\mathbf{W}_M^*$ is of rank one, its principal eigenvector is the solution of the original problem. For the case where $\mathbf{W}_M^*$ is of rank higher than one, we employ a randomization technique [11]. In this work, let us eigendecompose $\mathbf{W}_M^*$ as $\mathbf{W}_M^* = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^{\dagger}$ and generate K_{cand} candidate weight vectors by $\mathbf{w}_k = \mathbf{U}\mathbf{\Lambda}^{1/2}\mathbf{v}_k$, where each entry of $\mathbf{v}_k$ is $e^{j\theta}$ and θ is independently and uniformly distributed between 0 and 2π [11]. For each candidate weight vector, we check whether $\mathbf{w}_k$ satisfies the given constraints in (11) or not (i.e., $\min_{i=1,\ldots,N_1} \alpha_{S,1}^{(i)} \geq \mathbf{w}_k^{\dagger}\mathbf{R}_{M,D}\mathbf{w}_k$ and $\min_{i=1,\ldots,N_m} \alpha_{m,m+1}^{(i)} \geq \mathbf{w}_k^{\dagger}\mathbf{R}_{M,D}\mathbf{w}_k$ with $m = 1,2,\ldots,M-1$). If $\mathbf{w}_k$ satisfies the given constraints, we compute the corresponding secrecy rate using (6). Otherwise, we discard it. Among the candidate weight vectors satisfying the given constraints, we select $\acute{\mathbf{w}}_k$ to provide the highest secrecy rate. If $\acute{\mathbf{w}}_k$ provides higher secrecy rate than the cooperative beamformer determined at the previous iteration, we update $\mathbf{w}_M = \acute{\mathbf{w}}_k$.

Now, let us update $\widehat{\mathbf{w}}_m$. Note that $\widehat{\mathbf{w}}_n$ with $n > m$ is already updated at the current iteration, whereas $\widehat{\mathbf{w}}_n$ with $n < m$ is given at the previous iteration. Here, we can set $\alpha_{M,D} = P_M\widehat{\mathbf{w}}_M^{\dagger}\mathbf{R}_{M,D}\widehat{\mathbf{w}}_M$, and (7) can be simplified into

$$\begin{aligned} &\min_{\widehat{\mathbf{w}}_m} \quad \widehat{\mathbf{w}}_m^{\dagger}\mathbf{R}_{m,E}\widehat{\mathbf{w}}_m, \\ &s.t. \quad \min_{i=1,\ldots,N_{m+1}} P_m\widehat{\mathbf{w}}_m^{\dagger}\mathbf{R}_{m,m+1}^{(i)}\widehat{\mathbf{w}}_m \geq \alpha_{M,D}, \\ &\qquad \widehat{\mathbf{w}}_m^{\dagger}\widehat{\mathbf{w}}_m = 1. \end{aligned} \tag{16}$$

The problem in (16) is equivalent to

$$\min_{\widehat{\mathbf{w}}_m, t} \quad t,$$

$$\begin{aligned} \text{s.t.} \quad & \mathrm{tr}\left(\widehat{\mathbf{W}}_m \mathbf{R}_{m,E}\right) = t, \\ & \min_{i=1,\ldots,N_{m+1}} P_m \,\mathrm{tr}\left(\widehat{\mathbf{W}}_m \mathbf{R}_{m,m+1}^{(i)}\right) \geq \alpha_{M,D}, \\ & \mathrm{tr}\left(\widehat{\mathbf{W}}_m\right) = 1, \ \mathrm{rank}\,\widehat{\mathbf{W}}_m = 1, \ \widehat{\mathbf{W}}_m \succcurlyeq 0, \end{aligned} \tag{17}$$

where $\widehat{\mathbf{W}}_m = \widehat{\mathbf{w}}_m \widehat{\mathbf{w}}_m^{\dagger}$. Here, we employ a semidefinite relaxation to drop the rank constraint in (17). Then, this problem can be solved by SeDuMi [17] and Yalmip [18]. Further, if the solution is of rank one, we can use its principal eigenvector as $\widehat{\mathbf{w}}_m$. If the rank is higher than one, we employ the randomization technique described above.

4. Numerical Results

In this section, we present numerical results to investigate the secrecy rate performance of the proposed scheme. As shown in **Fig. 2**, we consider a (M+1)-hop relay network, where S, R_M's, and D are located in a line [3], [5], where the S-R_1, R_m-R_{m+1}, and R_M-D distances are defined as $d_{S,1}$, $d_{m,m+1}$, and $d_{M,D}$, respectively. Further, E is assumed to be located vertically away from the line. The S-E and R_m-E distances are computed as

$$\begin{aligned} d_{S,E} &= \sqrt{d_{Ex}^2 + d_E^2}, \\ d_{m,E} &= \sqrt{(d_{Ex} - d_{S,m})^2 + d_E^2}, \end{aligned} \tag{18}$$

respectively, where $d_{S,m} = d_{S,1} + \sum_{l=1}^{m-1} d_{l,l+1}$. As in [3] and [5], we assume a line-of-sight (LOS) channel model $d^{-\frac{c}{2}} e^{j\theta}$ for channels between any two nodes, where d is the distance between the nodes, θ denotes a random phase distributed uniformly within [0, 2π), and c = 3.5 is the path loss exponent. Moreover, the distances between relays are assumed to be much smaller than the distances between relays and source/destination/eavesdropper. Therefore, the path losses between different relays and the other node are assumed to be almost the same. For simplicity, we set K_{cand} = 10,000, $N_1 = N_2 = \ldots = N_M = N$, σ^2 = -30 dBm, and $P_S = P_1 = \ldots = P_M = P_T/(M+1)$ with P_T = 30 dBm, where P_T denotes the overall consumed power in multi-hop relay networks. As mentioned in Section 3.2, the proposed scheme performs the iterative beamformer update until the secrecy rates cannot be further enhanced. Note that, when the proposed scheme requires only one iteration, we cannot obtain the enhanced secrecy rate compared to the conventional scheme. From numerical results, we found that the proposed iteration always converges for all channel realizations.

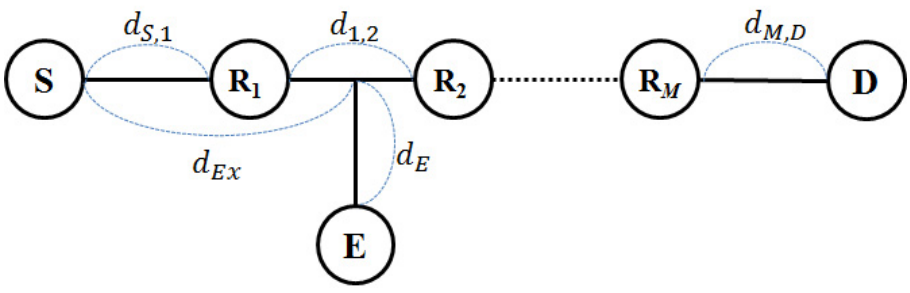


Fig. 2. Simulation Model

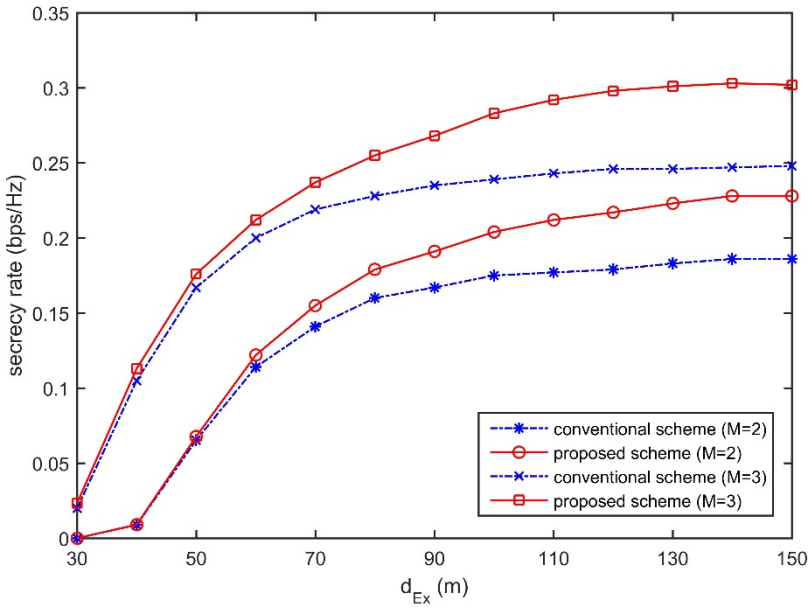
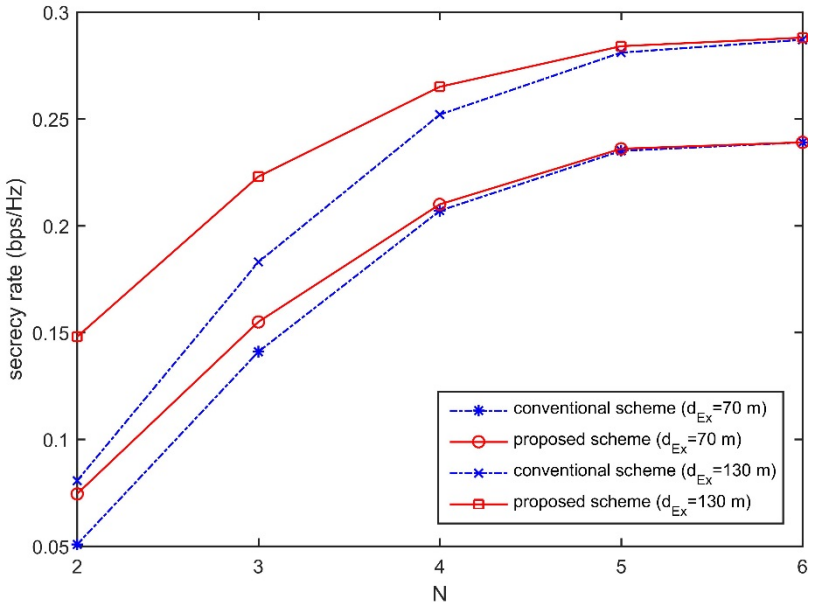
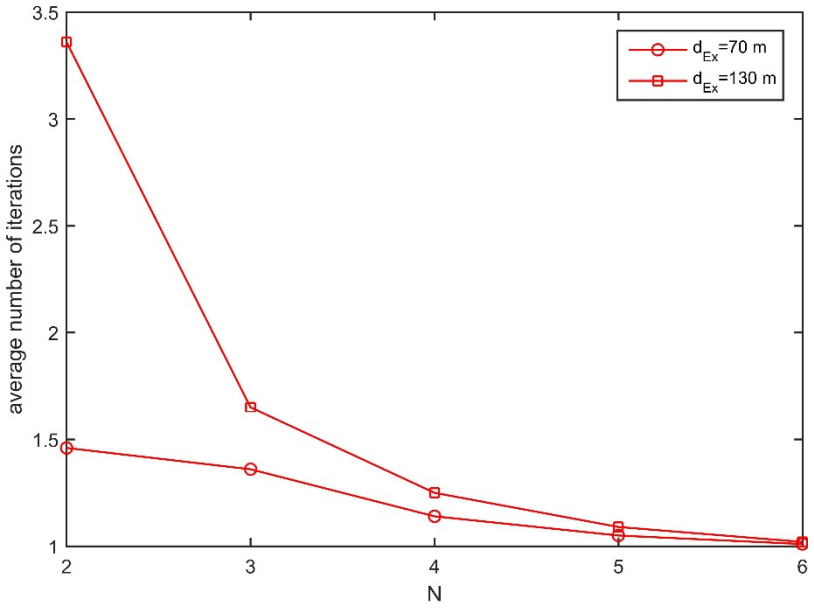


Fig. 3. Comparison of secrecy rates as a function of d_{Ex} for different values of M when $N = 3$ and $d_E = 5$ m.

Fig. 3 shows how the secrecy rate varies with d_{Ex} when $N = 3$ and $d_E = 5$ m. For $M = 2$, we set $d_{S,1} = 10$ m, $d_{1,2} = 45$ m, and $d_{2,D} = 45$ m, whereas $d_{S,1} = 10$ m, $d_{1,2} = 30$ m, $d_{2,3} = 30$ m, and $d_{3,D} = 30$ m are assumed for $M = 3$. In the above setting, the distance between S and D is given as $d_{S,D} = 100$ m for both three-hop ($M = 2$) and four-hop ($M = 3$) cases. As expected, the secrecy rate increases with the increase of d_{Ex}. For both $M = 2$ and 3, it is observed that the proposed beamformer design scheme provides better secrecy rates than the conventional MMF-ZF scheme in particular for larger values of d_{Ex}. Considering that the proposed scheme is initialized by the conventional MMF-ZF scheme, we confirm that the proposed iterative update using semidefinite relaxation and bisection techniques is quite effective to improve the secrecy rates in multi-hop DF relay networks. Further, it is also noteworthy that the secrecy rates can be enhanced by increasing M (i.e., the number of hops) in all ranges of d_{Ex}, even though P_T and $d_{S,D}$ are fixed.



(a)



(b)

Fig. 4. Performance comparison with varying N when $M = 2$, $d_{S,1} = 10$ m, $d_{1,2} = 45$ m, $d_{2,D} = 45$ m, and $d_E = 5$m. (a) Secrecy rate comparison, and (b) average number of iterations

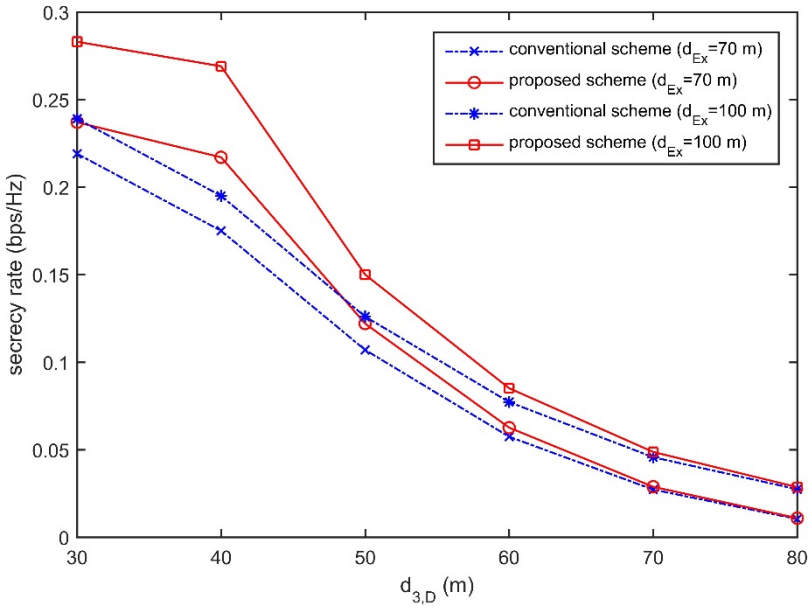


Fig. 5. Comparison of secrecy rates as a function of $d_{3,D}$ when $M = 3$, $N = 3$, $d_{S,1} = 10$ m, $d_{1,2} = 30$ m, $d_{2,3} = 30$ m, and $d_E = 5$ m

In **Fig. 4(a)**, we present the secrecy rates of the conventional MMF-ZF and proposed schemes as a function of N when $M = 2$, $d_{S,1} = 10$ m, $d_{1,2} = 45$ m, $d_{2,D} = 45$ m, and $d_E = 5$ m. The larger value of N indicates that more relays join the cooperative beamforming at each hop. It is observed that the increase of N yields the improvement of the secrecy rate for both schemes. Further, the proposed scheme is found to provide better secrecy rates than the conventional scheme in particular for smaller values of N. For the larger value of d_{Ex}, it is also found that the performance gain of the proposed scheme over the conventional scheme is more remarkable. In **Fig. 4(b)**, we show the average number of iterations, which are required for the proposed scheme to obtain the secrecy rates presented in **Fig. 4(a)**. For both $d_{Ex} = 70$ m and 130 m, the proposed scheme is found to require larger number of iterations for smaller values of N. Comparing the results in **Figs. 4(a)** and **(b)**, one can find that the performance gain of the proposed scheme becomes more remarkable as the required number of iterations increases.

Fig. 5 compares the secrecy rates of the conventional and proposed schemes as a function of $d_{3,D}$ when $M = 3$, $N = 3$, $d_{S,1} = 10$ m, $d_{1,2} = 30$ m, $d_{2,3} = 30$ m, and $d_E = 5$ m. As $d_{3,D}$ increases, the secrecy rates of both the conventional and proposed schemes decrease. It is observed that the performance gain of the proposed scheme over the conventional scheme becomes marginal as $d_{3,D}$ increases. However, in all ranges of $d_{3,D}$, it is also found that the proposed scheme outperforms the conventional scheme and the secrecy rate improvement achieved by the proposed scheme is more remarkable for larger values of d_{Ex}.

5. Conclusion

In this paper, we have investigated the secrecy rate in a multi-hop wireless DF relay network. The optimization problem for cooperative beamformer designs is derived to maximize the achievable secrecy rate. Since it is difficult to obtain the optimal solution in a close-form, we have proposed an iterative beamformer update scheme, where the cooperative beamformer at each hop is sequentially updated using semidefinite relaxation and bisection techniques.

Numerical results are presented to show that the proposed scheme provides enhanced secrecy rate compared to the conventional cooperative beamformers.

References

[1] A. Mukherjee, S. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550-1573, 2014. Article (CrossRef Link)

[2] A. D. Wyner, “The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975. Article (CrossRef Link)

[3] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875-1888, March 2010. Article (CrossRef Link)

[4] G. Zheng, L. Choo, and K. Wong, “Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317-1322, March 2011. Article (CrossRef Link)

[5] J. Li, A. P. Petropulu, and S. Weber, “On cooperative relaying schemes for wireless physical layer security," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985-4997, October 2011. Article (CrossRef Link)

[6] H. Wang, Q. Yin, and X. Xia, “Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Transactions on Signal Processing*, vol. 60, no. 7, pp. 3532-3545, July 2012. Article (CrossRef Link)

[7] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, “Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 2007-2020, December 2013. Article (CrossRef Link)

[8] M. Lin, J. Ge, Y. Yang, and Y. Ji, “Joint cooperative beamforming and artificial noise design for secrecy sum rate maximization in two-way AF relay networks," *IEEE Communications Letters*, vol. 18, no. 2, pp. 380-383, February 2014. Article (CrossRef Link)

[9] Y. Zou, X. Wang, W. Shen, and L. Hanzo, “Security versus reliability analysis of opportunistic relaying," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 6, pp. 2653-2661, July 2014. Article (CrossRef Link)

[10] H.-M. Wang, F. Liu, and M. Yang, “Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 10, pp. 4893-4898, October 2015. Article (CrossRef Link)

[11] N. D. Sidiropoulos, T. N. Davidson, and Z. Lou, “Transmit beamforming for physical-layer multicasting," *IEEE Transactions on Signal Processing*, vol. 54, no. 6, pp. 2239-2251, June 2006. Article (CrossRef Link)

[12] 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 Transactions on Signal Processing*, vol. 56, no. 9, pp. 4306-4316, September 2008. Article (CrossRef Link)

[13] Z. Luo, W. Ma, A. So, Y. Ye, and S. Zhang, “Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Processing Magazine*, vol. 27, no. 3, pp. 20-34, May 2010. Article (CrossRef Link)

[14] Y. Zou, J. Zhu, X. Wang, and V. C. M. Leung, “Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42-48, January-February 2015. Article (CrossRef Link)

[15] M. Bloch, J. O. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515-2534, June 2008. Article (CrossRef Link)

[16] S. Boyd and L. Vandenberghe, *Convex Optimization*, *Cambridge*, UK: Cambridge Univ. Press, 2004. Article (CrossRef Link)

[17] J. F. Sturm, "Using SeDuMi 1.02, a Matlab toolbox for optimization over symmetric cones," *Optimization Methods and Software*, vol. 11-12, pp. 625-653, 1999. Article (CrossRef Link)
[18] J. Lofberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in *Proc. of IEEE International Symposium on Computer Aided Control Systems Design*, pp.284-289, September 2004. Article (CrossRef Link)

Han-Byul Lee received the B.S. degree in electrical engineering from Kyongpook National University, Daegu, Korea, in 2007 and the M.S. degree in electrical engineering from Seoul National University, Seoul, Korea, in 2009, where he is currently pursuing the Ph.D. degree. His current research areas are performance analysis of wireless communications systems including orthogonal frequency-division multiplexing and multiple-input multiple-output systems.

Jong-Ho Lee received the B.S. degree in electrical engineering and the M.S. and Ph.D. degrees in electrical engineering and computer science from Seoul National University, Seoul, Korea, in 1999, 2001, and 2006, respectively. From 2006 to 2008, he was a Senior Engineer with Samsung Electronics, Suwon, Korea. From 2008 to 2009, he was a Postdoctoral Researcher with the Georgia Institute of Technology, Atlanta, GA, USA. From 2009 to 2012, he was an Assistant Professor with the Division of Electrical Electronic and Control Engineering, Kongju National University, Cheonan, Korea. Since 2012, he has been with the faculty of the Department of Electronic Engineering, Gachon University, Seongnam, Korea. His research interests are in the areas of wireless communication systems and signal processing for communication with current emphasis on multiple-antenna techniques, multi-hop relay networks, physical layer security, and full-duplex wireless communications.

Seong-Cheol Kim received the B.S. and M.S. degrees in electrical engineering from Seoul National University, Seoul, Korea, in 1984 and 1987, respectively, and the Ph.D. degree in electrical engineering from Polytechnic Institute of NYU, Brooklyn, NY, in 1995. From 1995 to 1999, he was with the Wireless Communications Systems Engineering Department, AT&T Bell Laboratories, Holmdel, NJ. Since 1999, he has been a Professor with the Department of Electrical Engineering and Computer Science, Seoul National University, Seoul, Korea. His research area covers systems engineering of wireless communication including propagation channel modeling, localization, and resource management. Currently, he is also interested in power-line communication and automotive radar system.