Cooperative Decode-and-Forward Relaying for Secure Multicasting

Jong-Ho Lee, Illsoo Sohn, Sungju Song, and Yong-Hwa Kim

In this paper, secure multicasting with the help of cooperative decode-and-forward relays is considered for the case in which a source securely sends a common message to multiple destinations in the presence of a single eavesdropper. We show that the secrecy rate maximization problem in the secure multicasting scenario under an overall power constraint can be solved using semidefinite programing with semidefinite relaxation and a bisection technique. Further, a suboptimal approach using zero-forcing beamforming and linear programming based power allocation is also proposed. Numerical results illustrate the secrecy rates achieved by the proposed schemes under secure multicasting scenarios.

Keywords: Physical layer security, multicasting, node cooperation, semidefinite programming.

I. Introduction

To ensure secure communication in wireless networks, physical layer security schemes aim to maximize the amount of securely transmitted information to a legitimate receiver by exploiting the physical characteristics of wireless channels without a secrecy key [1]. An achievable secrecy rate is defined as the rate communicated between a source and its intended destination with eavesdroppers knowing no information regarding the messages. Because a positive secrecy rate may not generally be obtainable when the source-destination channel condition is worse than the source-eavesdropper channel condition, node cooperation has been widely studied to enhance the secrecy rate [2]–[6]. For node cooperation using relays, multiple relays located between a source and a destination are specifically designed to cooperatively perform one of three different operation modes: amplify-and-forward (AF), decode-and-forward (DF), or cooperative jamming. Whereas the above works consider a one-way relay network, the authors of [7] exploited a node cooperation approach to improve the secrecy sum rates in two-way AF relay networks.

It is noteworthy that the abovementioned works consider secure communication from a source to a single destination. In this work, let us consider secure broadcasting in [8], where two scenarios have been investigated: 1) there is a common message to be delivered to multiple destinations, and 2) there are individual messages to be delivered to each destination. We focus on the first scenario (secure multicasting), in which a source has a common message to be delivered securely to multiple destinations in the presence of a single eavesdropper. Further, we consider that the secure multicasting is assisted by multiple DF relays to receive the signal from the source and cooperatively forward the weighted versions of their

Manuscript received Dec. 1, 2015; revised Apr. 1, 2016; accepted May 16, 2016.

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2013R1A1A1A05004401 and NRF-2014R1A1A1A05005551) and in part by "Human Resources Program in Energy Technology" of the Korea Institute of Energy Technology Evaluation and Planning (KETEP), granted financial resource from the Ministry of Trade, Industry & Energy, Rep. of Korea. (No. 20134030200310).

Jong-Ho Lee (jongho.lee@gachon.ac.kr) and Illsoo Sohn (illsoo.sohn@gachon.ac.kr) are with the Department of Electronic Engineering, Gachon University, Seongnam, Rep. of Korea.

Sungju Song (chess12@naver.com) and Yong-Hwa Kim (corresponding author, yongkim@mju.ac.kr) are with the Department of Electronic Engineering, Myongji University, Yongin, Rep. of Korea.

re-encoded signal to multiple destinations. It is obvious that the conventional node cooperation schemes in [2] and [4] are tailored only for a single-destination case, which are unsuitable for secure multicasting. Recently, the authors of [9] considered a secure multicast transmission in which the destination nodes, which successfully decode the secure message from the source in the first phase, conduct the relaying operation in the second phase to forward their re-encoded signal to the other destination nodes, which fail to decode the message from the source, without considering the transmit power allocation or the cooperative relay beamformer optimization.

In this work, our objective is to maximize the achievable secrecy rate by jointly optimizing the power allocation and relay weights under an overall transmit power constraint in secure multicasting scenarios assisted by node cooperation using multiple DF relays. We show that our optimization problem can be formulated as a semidefinite programming (SDP) problem [10]. For computational efficiency, we also propose a suboptimal approach using the zero-forcing (ZF) beamforming associated with max-min fair beamforming [11] and a power allocation with linear programming (LP) [12]. Numerical results are presented to show the secrecy rates achieved by the proposed schemes under secure multicasting scenarios.

II. System Model

Let us consider a wireless relay network consisting of one source node S, N_{R}^{tot} trusted relays R, N_{D} destination nodes D, and one eavesdropper E. Each node is assumed to be equipped with a single antenna. Each relay uses DF mode to decode the signal from the source node and forward the re-encoded signal to the destination nodes. Here, the eavesdropper is assumed to overhear the source node and relays. All channels between nodes are assumed to undergo flat fading.

We assume that N_{R} relays among N_{R}^{tot} are selected for cooperative relaying with $2 \le N_{\mathrm{R}} \le N_{\mathrm{R}}^{tot}$ [13], and two time slots are used for DF relaying. In the first time slot, S sends its data symbol s with the unit power. The signals received at the relays, destination nodes, and eavesdropper can be given as

$$\begin{aligned} \mathbf{y}_{\mathrm{R}} &= \sqrt{P_{\mathrm{R}}}\mathbf{h}_{\mathrm{SR}}s + \mathbf{z}_{\mathrm{R}}, \\ \mathbf{y}_{\mathrm{D}} &= \sqrt{P_{\mathrm{S}}}\mathbf{h}_{\mathrm{SD}}s + \mathbf{z}_{\mathrm{D}}, \text{ and }, \\ y_{\mathrm{E}} &= \sqrt{P_{\mathrm{S}}}h_{\mathrm{SE}}s + z_{\mathrm{E}}, \end{aligned} \tag{1}$$

where P_{S} is the transmit power of S, $\mathbf{h}_{\mathrm{SR}}$ and $\mathbf{h}_{\mathrm{SD}}$ are $N_{\mathrm{R}} \times 1$ and $N_{\mathrm{D}} \times 1$ complex channel vectors including the complex channel gains from the source node to the trusted relays and from the source node to the destination nodes, respectively, and h_{SE} is a complex channel gain from the source node to the eavesdropper. Moreover, $\mathbf{z}_{\mathrm{R}}$, $\mathbf{z}_{\mathrm{D}}$, and z_{E} denote additive white Gaussian noise with zero mean and variance σ^2 at the trusted relays, destination nodes, and eavesdropper, respectively.

In the second time slot, each trusted relay decodes s successfully and transmits its weighted version of the re-encoded symbol. The received signals at the destination nodes and eavesdropper are expressed as

$$\begin{aligned} \mathbf{y}_{\mathrm{D}} &= \mathbf{H}_{\mathrm{RD}}\mathbf{w}s + \mathbf{z}_{\mathrm{D}}, \text{ and} \\ y_{\mathrm{E}} &= \mathbf{h}_{\mathrm{RE}}\mathbf{w}s + z_{\mathrm{E}}, \end{aligned} \tag{2}$$

where $\mathbf{H}_{\mathrm{RD}}$ is an $N_{\mathrm{D}} \times N_{\mathrm{R}}$ complex channel matrix from the trusted relays to the destination nodes, $\mathbf{h}_{\mathrm{RE}}$ is a $1 \times N_{\mathrm{R}}$ complex channel vector from the trusted relays to the eavesdropper, and $\mathbf{w}$ denotes an $N_{\mathrm{R}} \times 1$ beamforming weight vector containing the weights of N_{R} cooperative relays. Note that the trusted relays may use different codewords independent of the codewords of the source node, which can be randomly chosen from a secrecy codebook [14]. In this work, we assume that the source node and trusted relays use the same codewords as in [2] and [4] for analytical simplicity.

Based on (1) and (2), the rates at the ith destination node and eavesdropper, respectively, are

$$R_{\mathrm{D},i} = \frac{1}{2}\log_2\left(1 + P_{\mathrm{S}}\alpha_{\mathrm{SD},i} + \mathbf{w}^{\dagger}\mathbf{R}_{\mathrm{RD},i}\mathbf{w}\right) \text{ and} \tag{3}$$

$$R_{\mathrm{E}} = \frac{1}{2}\log_2\left(1 + P_{\mathrm{S}}\alpha_{\mathrm{SE}} + \mathbf{w}^{\dagger}\mathbf{R}_{\mathrm{RE}}\mathbf{w}\right), \tag{4}$$

where $\alpha_{\mathrm{SD},i} = \frac{|h_{\mathrm{SD},i}|^2}{\sigma^2}$, $\alpha_{\mathrm{SE}} = \frac{|h_{\mathrm{SE}}|^2}{\sigma^2}$, $\mathbf{R}_{\mathrm{RD},i} = \frac{\mathbf{h}_{\mathrm{RD},i}^{\dagger}\mathbf{h}_{\mathrm{RD},i}}{\sigma^2}$, $\mathbf{R}_{\mathrm{RE}} = \mathbf{h}_{\mathrm{RE}}^{\dagger}\mathbf{h}_{\mathrm{RE}}/\sigma^2$, and $(.)^{\dagger}$ denotes the conjugate transpose. Here, $h_{\mathrm{SD},i}$ is the ith entry of $\mathbf{h}_{\mathrm{SD}}$, and $\mathbf{h}_{\mathrm{RD},i}$ is the ith row of $\mathbf{H}_{\mathrm{RD}}$. The ith destination node and eavesdropper can perform the maximal ratio combining [2], [4] to achieve $R_{\mathrm{D},i}$ and R_{E}, respectively. Further, the rate at the jth trusted relay can be given as

$$R_{\mathrm{R},j} = \frac{1}{2}\log_2\left(1 + P_{\mathrm{S}}\alpha_{\mathrm{SR},j}\right), \tag{5}$$

where $\alpha_{\mathrm{SR},j} = |h_{\mathrm{SR},j}|^2/\sigma^2$, and $h_{\mathrm{SR},j}$ is the jth entry of $\mathbf{h}_{\mathrm{SR}}$. Note that the scaling factor of 1/2 is due to the fact that two time slots are required for the DF relaying.

III. Achievable Secrecy Rate Maximization

In the multicasting scenario, it is known that the weakest destination link determines the common information rate [11]. This implies that, because we have to guarantee that all the destinations correctly decode the common message, the common information rate should be $\min_i R_{\mathrm{D},i}$. Therefore, from (3) and (4), the achievable secrecy rate can be written as

$$R_s = [\min_i R_{\mathrm{D},i} - R_{\mathrm{E}}]^+, \tag{6}$$

where $[x]^+ = \max\{x, 0\}$.

It should also be guaranteed that each relay in DF mode correctly decodes the common message from the source node and forwards it to the destination nodes. This implies that the rates at the relays should be equal to or greater than the common information rate, which yields $R_{\mathrm{R},j} \geq \min_i R_{\mathrm{D},i}$ for all j. Further, let us consider the overall transmit power constraint P_0, in which the sum of the consumed powers during the two time slots (P_{S} for the first time slot, and $\mathbf{w}^\dagger\mathbf{w}$ for the second time slot) should be equal to or less than P_0. We expect that the proposed schemes described below can be extended to the case with an individual transmit power constraint, where each node has its own transmit power limit [15]. Considering the above constraints, we formulate the optimization problem to maximize the achievable secrecy rate shown:

$$\begin{aligned} &\max_{P_{\mathrm{S}},\mathbf{w}} \min_i R_{\mathrm{D},i} - R_{\mathrm{E}}, \\ &\text{s.t. } \min_j R_{\mathrm{R},j} \geq \min_i R_{\mathrm{D},i}, \\ &\quad \mathbf{w}^\dagger\mathbf{w} \leq P_0 - P_{\mathrm{S}}. \end{aligned} \tag{7}$$

Substituting (3) through (5) into (7), we have

$$\begin{aligned} &\max_{P_{\mathrm{S}},\mathbf{w}} \min_i \frac{1 + P_{\mathrm{S}}\alpha_{\mathrm{SD},i} + \mathbf{w}^\dagger\mathbf{R}_{\mathrm{RD},i}\mathbf{w}}{1 + P_{\mathrm{S}}\alpha_{\mathrm{SE}} + \mathbf{w}^\dagger\mathbf{R}_{\mathrm{RE}}\mathbf{w}}, \\ &\text{s.t. } P_{\mathrm{S}}\alpha_{\mathrm{SR}} \geq \min_i P_{\mathrm{S}}\alpha_{\mathrm{SD},i} + \mathbf{w}^\dagger\mathbf{R}_{\mathrm{RD},i}\mathbf{w}, \\ &\quad \mathbf{w}^\dagger\mathbf{w} \leq P_0 - P_{\mathrm{S}}, \end{aligned} \tag{8}$$

where $\alpha_{\mathrm{SR}} = \min_j \alpha_{\mathrm{SR},j}$.

In the following subsections, let us assume global channel state information, which is available when the eavesdropper is another legitimate user in the network whose transmission can be monitored [16]. In this scenario, we consider the eavesdropper to be a low-level user, and allow this user to access less information than the destination nodes.

1. ZF-Based Beamforming and LP-Based Power Allocation

First, we consider a suboptimal approach to solve (8). Let us design $\bar{\mathbf{w}}$ to null out the signal at the eavesdropper and maximize the minimum channel gain from the trusted relays to the destination nodes, which is given as

$$\bar{\mathbf{w}} = \underset{\tilde{\mathbf{w}}}{\operatorname{argmax}} \min_{i=1,\ldots,N_{\mathrm{D}}} \left|\mathbf{h}_{\mathrm{RD},i}\left(\mathbf{I}_{N_{\mathrm{R}}} - \mathbf{P}_{\mathrm{E}}\right)\tilde{\mathbf{w}}\right|^2, \tag{9}$$

where $\mathbf{I}_k$ is a $k \times k$ identity matrix and $\mathbf{P}_{\mathrm{E}}$ is the orthogonal projection matrix onto the subspace spanned by $\mathbf{h}_{\mathrm{RE}}$ given as $\mathbf{P}_{\mathrm{E}} = \mathbf{h}_{\mathrm{RE}}^\dagger\left(\mathbf{h}_{\mathrm{RE}}\mathbf{h}_{\mathrm{RE}}^\dagger\right)^{-1}\mathbf{h}_{\mathrm{RE}}$ [2]. Note that the optimization problem in (9) can be solved by following the max-min fair beamforming approach given in [11], which employs the SDP with randomization techniques. After obtaining $\bar{\mathbf{w}}$, we compute $\hat{\mathbf{w}}$ as

$$\hat{\mathbf{w}} = \frac{\left(\mathbf{I}_{N_{\mathrm{R}}} - \mathbf{P}_{\mathrm{E}}\right)\bar{\mathbf{w}}}{\left\|\left(\mathbf{I}_{N_{\mathrm{R}}} - \mathbf{P}_{\mathrm{E}}\right)\bar{\mathbf{w}}\right\|}, \tag{10}$$

with $\hat{\mathbf{w}}^\dagger\hat{\mathbf{w}} = 1$. Substituting $\mathbf{w} = \sqrt{P_{\mathrm{R}}}\hat{\mathbf{w}}$ into (8), we have the following power allocation problem:

$$\begin{aligned} &\max_{P_{\mathrm{S}},P_{\mathrm{R}}} \min_i \frac{1 + P_{\mathrm{S}}\alpha_{\mathrm{SD},i} + P_{\mathrm{R}}\alpha_{\mathrm{RD},i}}{1 + P_{\mathrm{S}}\alpha_{\mathrm{SE}}}, \\ &\text{s.t. } P_{\mathrm{S}}\alpha_{\mathrm{SR}} \geq \min_i P_{\mathrm{S}}\alpha_{\mathrm{SD},i} + P_{\mathrm{R}}\alpha_{\mathrm{RD},i}, \\ &\quad P_{\mathrm{S}} + P_{\mathrm{R}} \leq P_0,\ 0 \leq P_{\mathrm{S}} \leq P_0, 0 \leq P_{\mathrm{R}} \leq P_0, \end{aligned} \tag{11}$$

where P_{R} is the total transmit power consumed by the cooperative relays and $\alpha_{\mathrm{RD},i} = \hat{\mathbf{w}}^\dagger\mathbf{R}_{\mathrm{RD},i}\hat{\mathbf{w}}/\sigma^2$. Using the Charnes-Cooper transformation with $P_{\mathrm{S}} = \tilde{P}_{\mathrm{S}}/t$. and $P_{\mathrm{R}} = \tilde{P}_{\mathrm{R}}/t$ [17], we can rewrite (11) as an LP problem [12] shown as

$$\begin{aligned} &\max_{\tilde{P}_{\mathrm{S}},\tilde{P}_{\mathrm{R}},t,\tau} \tau, \\ &\text{s.t. } t + \tilde{P}_{\mathrm{S}}\alpha_{\mathrm{SD},i} + \tilde{P}_{\mathrm{R}}\alpha_{\mathrm{RD},i} \geq \tau, \quad \forall i, \\ &\quad t + \tilde{P}_{\mathrm{S}}\alpha_{\mathrm{SE}} = 1, \\ &\quad t + \tilde{P}_{\mathrm{S}}\alpha_{\mathrm{SR}} \geq \tau, \\ &\quad \tilde{P}_{\mathrm{S}} + \tilde{P}_{\mathrm{R}} \leq tP_0,\ t > 0, \\ &\quad 0 \leq \tilde{P}_{\mathrm{S}} \leq tP_0, 0 \leq \tilde{P}_{\mathrm{R}} \leq tP_0. \end{aligned} \tag{12}$$

In particular, let us define $\hat{\tau}$ as the maximum value of τ obtained by solving (12).

2. SDP-Based Optimization

Now, let us focus on the optimal solution of (8). The problem in (8) is equivalent to

$$\begin{aligned} &\max_{P_{\mathrm{S}},\mathbf{W}} \min_i \frac{1 + P_{\mathrm{S}}\alpha_{\mathrm{SD},i} + \mathrm{tr}(\mathbf{R}_{\mathrm{RD},i}\mathbf{W})}{1 + P_{\mathrm{S}}\alpha_{\mathrm{SE}} + \mathrm{tr}(\mathbf{R}_{\mathrm{RE}}\mathbf{W})} \\ &\text{s.t. } P_{\mathrm{S}}\alpha_{\mathrm{SR}} \geq \min_i P_{\mathrm{S}}\alpha_{\mathrm{SD},i} + \mathrm{tr}(\mathbf{R}_{\mathrm{RD},i}\mathbf{W}), \\ &\quad \mathrm{tr}(\mathbf{W}) \leq P_0 - P_{\mathrm{S}},\ \mathrm{rank}(\mathbf{W}) = 1,\ \ \mathbf{W} \succeq 0, \end{aligned} \tag{13}$$

where $\mathbf{W} = \mathbf{w}\mathbf{w}^\dagger$, tr(.) denotes trace operations, and $\mathbf{W} \succeq 0$ indicates that $\mathbf{W}$ must be a Hermitian positive semidefinite matrix. In (13), we use the Charnes-Cooper transformation with $P_{\mathrm{S}} = P/t$ and $\mathbf{W} = \mathbf{Z}/t$, and exploit a semidefinite relaxation to drop the rank constraint [18]. We then have

$$\begin{aligned} &\max_{P_{\mathrm{S}},\mathbf{W},t} \min_i \frac{t + P\alpha_{\mathrm{SD},i} + \mathrm{tr}(\mathbf{R}_{\mathrm{RD},i}\mathbf{Z})}{t + P\alpha_{\mathrm{SE}} + \mathrm{tr}(\mathbf{R}_{\mathrm{RE}}\mathbf{Z})}, \\ &\text{s.t. } \mathrm{P}\alpha_{\mathrm{SR}} \geq \min_i P\alpha_{\mathrm{SD},i} + \mathrm{tr}(\mathbf{R}_{\mathrm{RD},i}\mathbf{Z}), \\ &\quad \mathrm{tr}(\mathbf{Z}) \leq tP_0 - P,\ \ \mathbf{Z} \succeq 0,\ \ t > 0. \end{aligned} \tag{14}$$

Further, (14) can be reformulated as an SDP problem [8] shown as

$$\max_{P_S,\mathbf{W},t,\tau} \ \tau$$
$$\text{s.t.} \ \ t + P\alpha_{\text{SD},i} + \text{tr}(\mathbf{R}_{\text{RD},i}\mathbf{Z}) \geq \tau, \ \forall i,$$
$$t + P\alpha_{\text{SE}} + \text{tr}(\mathbf{R}_{\text{RE}}\mathbf{Z}) = 1, \qquad (15)$$
$$t + P\alpha_{\text{SR}} \geq \tau,$$
$$\text{tr}(\mathbf{Z}) \leq tP_0 - P, \ \mathbf{Z} \succeq 0, \ t > 0,$$

which can be solved using SeDuMi [19] and Yalmip [20]. Let P^*, Z^*, t^*, and τ^* be the solution to (15), where we obtain $P_S^* = P^*/t^*$ and $\mathbf{W}^* = \mathbf{Z}^*/t^*$.

Because semidefinite relaxation is used, $\mathbf{W}^*$ may have a rank higher than 1. When the solution is of rank 1, its principal eigenvector $\mathbf{w}^*$ can be used to obtain $\mathbf{w} = \sqrt{\lambda^*}\mathbf{w}^*$, where λ^* is the principal eigenvalue of $\mathbf{W}^*$. If the rank is higher than 1, we employ the penalty function method (PFM) in [21]. In this work, we set $\mathbf{Z}'^{(0)} = \mathbf{Z}^*$ and apply the initialization step of the PFM to obtain $\mathbf{Z}^{(0)}$ with $\text{rank}(\mathbf{Z}^{(0)}) \approx 1$. Using $\mathbf{Z}^{(0)}$ as a starting point, we apply the optimization step of the PFM. Both the initialization and optimization steps are an iterative process, where the following SDP problem is solved at the kth iteration:

$$\mathbf{Z}^{(k+1)} = \arg\min_{\tilde{\mathbf{Z}}} \text{tr}(\tilde{\mathbf{Z}}) - \lambda_{\max}(\mathbf{Z}^{(k)}) - \text{tr}\left(\mathbf{z}_{\max}^{(k)}(\mathbf{z}_{\max}^{(k)})^{\dagger}(\tilde{\mathbf{Z}} - \mathbf{Z}^{(k)})\right),$$
$$\text{s.t.} \ \ t^* + P^*\alpha_{\text{SD},i} + \text{tr}(\mathbf{R}_{\text{RD},i}\tilde{\mathbf{Z}}) \geq \tau^*, \ \forall i,$$
$$t^* + P^*\alpha_{\text{SE}} + \text{tr}(\mathbf{R}_{\text{RE}}\tilde{\mathbf{Z}}) = 1, \ \text{and} \qquad (16)$$
$$\text{tr}(\tilde{\mathbf{Z}}) \leq t^*P_0 - P^*, \ \tilde{\mathbf{Z}} \succeq 0,$$

where $\lambda_{\max}(\mathbf{Z}^{(k)})$ and $\mathbf{z}_{\max}^{(k)}$ are the maximal eigenvalue and the corresponding eigenvector of $\mathbf{Z}^{(k)}$, respectively. We use the principal eigenvalue and eigenvector of the converged solution of the PFM to obtain $\mathbf{W}$.

It is noteworthy that the converged solution of the PFM may still have a rank higher than 1 for a certain channel realization, which indicates that a rank-1 solution of (15) does not exist for the given τ^*. In this case, let $\tau_{\max}$ be the maximum value of τ under the rank-1 constraint. It is then reasonable to assume that $\hat{\tau} \leq \tau_{\max} < \tau^*$ because we proved that the feasible rank-1 solution exists for $\hat{\tau}$ when using the ZF-based beamforming and LP-based power allocation described in Section III. Based on this observation, we employ the concept of a bisection technique [12]. Let us start with an interval $[l, u]$. Note that $\hat{\tau}$ and τ^* are used for the initial interval. At the midpoint of the interval $\tau = (l+u)/2$, we first solve

$$\text{find} \ \ P, \mathbf{Z}, t,$$
$$\text{s.t.} \ \ t + P\alpha_{\text{SD},i} + \text{tr}\left(\mathbf{R}_{\text{RD},i}\mathbf{Z}\right) \geq \tau, \ \forall i,$$
$$t + P\alpha_{\text{SE}} + \text{tr}\left(\mathbf{R}_{\text{RE}}\mathbf{Z}\right) = 1, \qquad (17)$$
$$t + P\alpha_{\text{SR}} \geq \tau, \ \text{and}$$
$$\text{tr}(\mathbf{Z}) \leq tP_0 - P, \ \ \mathbf{Z} \succeq 0, \ \ t > 0,$$

using SeDuMi [19] and Yalmip [20]. Then, using $\bar{P}$, $\bar{\mathbf{Z}}$, and $\bar{t}$ obtained by solving (17), we apply the PFM described above to check whether a rank-1 solution is feasible for the given τ. If the converged solution of the PFM has a rank of 1, we update $l = \tau$. Otherwise, $u = \tau$ is chosen. For the updated interval, we perform this rank-1 feasibility check process again until the interval is sufficiently small.

3. Remarks

It is noteworthy that there is a trade off between the exploitation of spatial degrees of freedom and the computational efficiency. Whereas the SDP scheme in Section III is able to exploit the full spatial degrees of freedom for the relay beamformer design, the relay beamformer of the ZF-LP scheme in Section III was designed to null out the signal at an eavesdropper such that some loss of spatial degrees of freedom is inevitable. On the other hand, the ZF-LP scheme is more computationally efficient than the SDP scheme. Note that the ZF-LP scheme solves the SDP problem in (9) only once for a given channel realization, whereas the SDP scheme applies the PFM to solve the SDP problem in (16) during all iterations associated with the bisection technique solving (17).

IV. Numerical Results

In this section, numerical results are presented to show the secrecy rates achieved by the proposed schemes under secure multicasting scenarios. As shown in Fig. 1, we assume that the source node and eavesdropper are located along a line and that d_{SE} denotes the distance between them. Further, the trusted relays are assumed to be randomly located within a circle with a radius of d_{R}, whose center is on the line. The distance between the source node and the center is denoted as d_{SR}. Similarly, the destination nodes are randomly located within a circle with a radius of d_{D}, whose center is also on the line, and the distance between the source node and the center of the circle is d_{SD}. As in [2] and [4], channels between any two nodes are assumed to follow a line-of-sight channel model $d^{-c/2}e^{j\theta}$, where d is the distance between the nodes, θ denotes a random

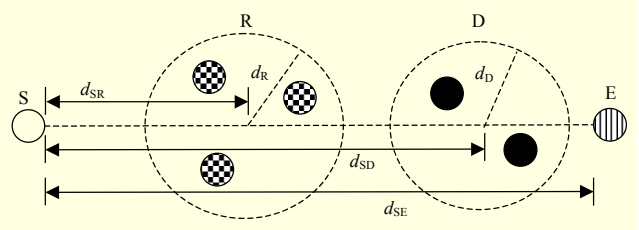

Fig. 1. Illustration of the simulation model.

phase distributed uniformly within $[0, 2\pi)$, and $c = 3.5$ is the path loss exponent. In the following results, the total transmit power is $P_0 = 30$ dBm, the noise power is $\sigma^2 = -30$ dBm, and $d_R = d_D = \gamma$ is assumed for simplicity. We conducted Monte Carlo simulations consisting of 5,000 independent channel realizations and random locations of the trusted relays and destination nodes. As mentioned above, we selected N_R relays among N_R^{tot} relays, and $\sum_{n=2}^{N_R^{tot}} \binom{N_R^{tot}}{n}$ relay selections are available. For each relay selection, we compute the secrecy rate and choose the relay selection that provides the best secrecy rate.

Figure 2 compares the secrecy rates as a function of d_{SD} when $d_{SR} = 20$ m, $d_{SE} = 50$ m, $N_R^{tot} = 3$, and $\gamma = 5$ m. For comparison, we also evaluated the secrecy rate for a single destination node ($N_D = 1$) using the result in [2]. It was observed that the secrecy rates decrease exponentially as the destination nodes move away from the source node. Comparing the secrecy rates for a single destination node and multicasting cases, we found that the decrease in secrecy rate with increasing d_{SD} becomes steeper as N_D increases. Further, the suboptimal ZF-LP scheme was shown to provide almost the same secrecy rates as the SDP scheme except for larger values of N_D and smaller values of d_{SD}. This implies that the loss of spatial degrees of freedom owing to the ZF beamforming becomes critical, as the destination nodes move closely to the trusted relays, and the number of destination nodes for multicasting increases.

In Fig. 3, we show how the secrecy rates vary with N_D for different values of γ when $d_{SR} = 20$ m, $d_{SD} = 50$ m, $d_{SE} = 50$ m, and $N_R^{tot} = 3$. It is noteworthy that the secrecy rates of the SDP and ZF-LP schemes decrease exponentially with an increasing N_D and that the performance gap between the SDP and ZF-LP schemes becomes more pronounced for larger values of N_D. For both the single destination node and multicasting cases, it was observed that smaller secrecy rates are achieved for larger values of γ. For the multicasting cases, the decrease in secrecy rates owing to an increase in γ is found to become severe. Particularly for $N_D = 5$, the SDP and ZF-LP schemes with $\gamma = 5$ m achieve 72.4% and 68.9% secrecy rates for a single destination node case, respectively. However, with $\gamma = 15$ m, 63.8% and 60.8% secrecy rates for a single destination node case are achieved by the SDP and ZF-LP schemes, respectively. It is also remarkable that the decrease in secrecy rates with an increasing N_D does not become steeper despite the increase in γ.

Figure 4 shows the secrecy rates as a function of N_R^{tot} for

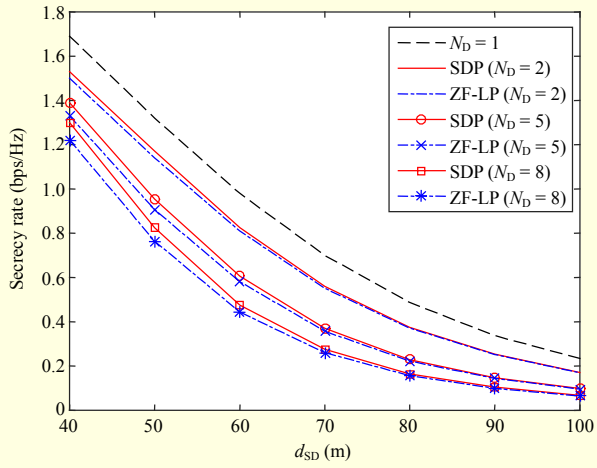

Fig. 2. Secrecy rate versus d_{SD} with different values of N_D when $d_{SR} = 20$ m, $d_{SE} = 50$ m, $N_R^{tot} = 3$, and $\gamma = 5$ m.

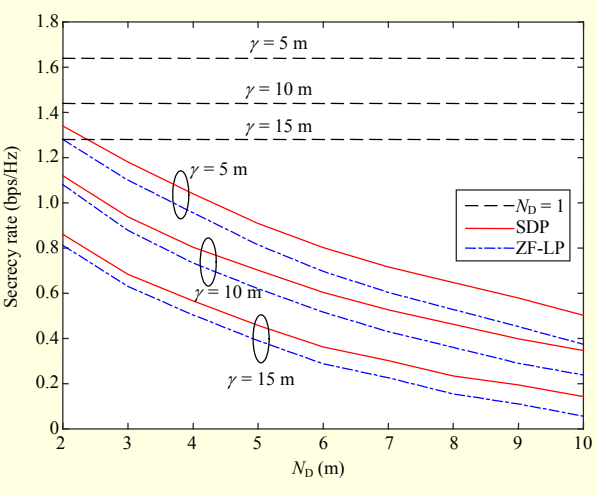

Fig. 3. Secrecy rate versus N_D with different values of γ when $d_{SR} = 20$ m, $d_{SD} = 50$ m, $d_{SE} = 50$ m, and $N_R^{tot} = 3$.

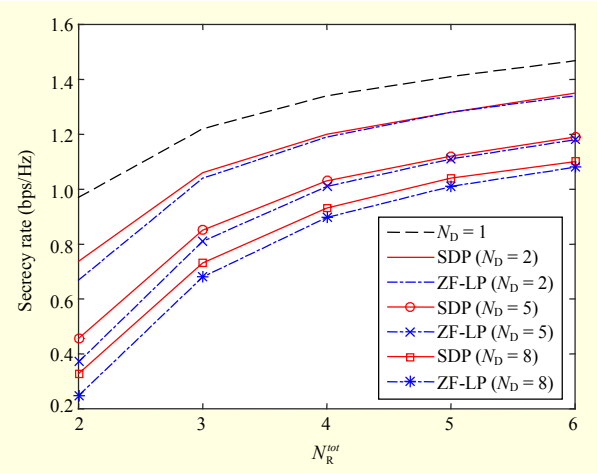

Fig. 4. Secrecy rate versus N_R^{tot} with different values of N_D when $d_{SR} = 20$ m, $d_{SD} = 50$ m, $d_{SE} = 50$ m, and $\gamma = 10$ m.

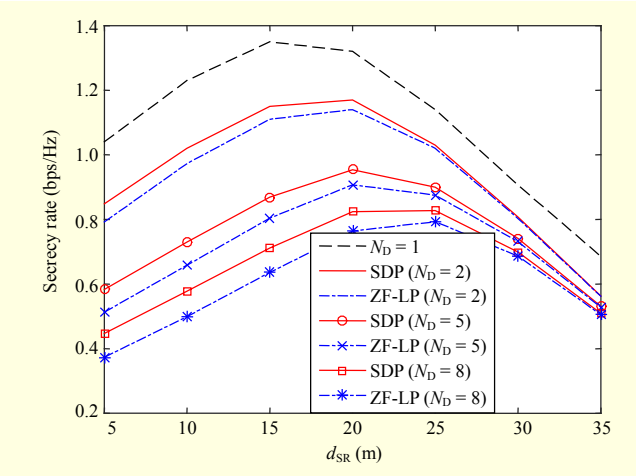

Fig. 5. Secrecy rate versus d_{SR} with different values of N_D when $d_{SD} = 50$ m, $d_{SE} = 50$ m, $N_R^{tot} = 3$, and $\gamma = 5$ m.

different values of N_D when $d_{SR} = 20$ m, $d_{SD} = 50$ m, $d_{SE} = 50$ m, and $\gamma = 10$ m. The secrecy rates increase with an increase in N_R^{tot}. Compared to the secrecy rate for a single destination node case, the secrecy rate degradation owing to multiple destination nodes is more remarkable for smaller values of N_R^{tot}. Further, the performance gap between the SDP and ZF-LP schemes was also found to be more pronounced for smaller values of N_R^{tot} and larger values of N_D. This implies that, when the number of trusted relays that are able to join the cooperative beamforming is small, whereas the number of destination nodes for multicasting is large, the loss of spatial degrees of freedom is found to be critical.

Let us now illustrate how the secrecy rates vary with d_{SR} when $d_{SD} = 50$ m, $d_{SE} = 50$ m, $N_R^{tot} = 3$, and $\gamma = 10$ m. In Fig. 5, it can be observed that the best location of trusted relays for a single destination node case is found to be $d_{SR} = 15$ m, whereas the best location for the SDP scheme with multiple destination nodes changes from 15 to 25, as N_D increases. Further, it can be seen that the performance gap between the SDP and ZF-LP schemes becomes significant for smaller values of d_{SR}.

V. Conclusion

In this paper, we investigated the secrecy rates under secure multicasting scenarios, where a source sends a common message securely to multiple destinations with the help of cooperative DF relays. Under an overall power constraint, we showed that the joint optimization problem for a relay beamformer design and the transmit power allocation to maximize the secrecy rate can be solved using the SDP with semidefinite relaxation and a bisection technique. Further, we also proposed a suboptimal approach using ZF-based beamforming and LP-based power allocation. Numerical results illustrate how the secrecy rates achieved by the proposed schemes vary in secure multicasting environments compared to the secrecy rate for a single-destination case. Further, the proposed suboptimal ZF-LP scheme was shown to provide a secrecy rate comparable to that of the SDP scheme.

References

[1] A. Mukherjee et al., "Principles of Physical Layer Security in Multiuser Wireless Networks: a Survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, 2014, pp. 1550–1573.

[2] L. Dong et al., "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, Mar. 2010, pp. 1875–1888.

[3] G. Zheng, L. Choo, and K. Wong, "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, 2011, pp. 1317–1322.

[4] J. Li, A.P. Petropulu, and S. Weber, "On Cooperative Relaying Schemes for Wireless Physical Layer Security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, Oct. 2011, pp. 4985–4997.

[5] H.-M. Wang, F. Liu, and M. Yang, "Joint Cooperative Beamforming, Jamming, and Power Allocation to Secure AF Relay Systems," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, Oct. 2015, pp. 4893–4898.

[6] H.-M. Wang and X.-G. Xia, "Enhancing Wireless Secrecy via Cooperation: Signal Design and Optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, Dec. 2015, pp. 47–53.

[7] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed Beamforming for Physical-Layer Security of Two-Way Relay Networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, July 2012, pp. 3532–3545.

[8] A. Khisti, A. Tchamkerten, and G.W. Wornell, "Secure Broadcasting over Fading Channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, June 2008, pp. 2453–2469.

[9] X. Wang, M. Tao, and Y. Xu, "Outage Analysis of Cooperative Secrecy Multicast Transmission," *IEEE Wireless Commun. Lett.*, vol. 3, no. 2, Apr. 2014, pp. 161–164.

[10] Q. Li and W.-K. Ma, "Optimal and Robust Transmit Designs for MISO Channel Secrecy by Semidefinite Programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, Aug. 2011, pp. 3799–3812.

[11] N.D. Sidiropoulos, T.N. Davidson, and Z. Lou, "Transmit Beamforming for Physical-Layer Multicasting," *IEEE Trans. Signal Process.*, vol. 54, no. 6, June 2006, pp. 2239–2251.

[12] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge, UK: Cambridge University Press, 2004.

[13] Y. Zou et al., "Relay-Selection Improves the Security-Reliability Trade-off in Cognitive Radio Systems," *IEEE Trans. Commun.*, vol. 63, no. 1, Jan. 2015, pp. 215–228.

[14] O.O. Koyluoglu, C.E. Koksal, and H.E. Gamal, "On Secrecy Capacity Scaling in Wireless Networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, May 2012, pp. 3000–3015.
[15] H.-M. Wang et al., "Joint Cooperative Beamforming and Jamming to Secure AF Relay Systems with Individual Power Constraint and No Eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 1, Jan. 2013, pp. 39–42.
[16] M. Bloch et al., "Wireless Information-Theoretic Security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, June 2008, pp. 2515–2534.
[17] A. Charnes and W.-W. Cooper, "Programming with Linear Fractional Functionals," *Naval Res. Logist.*, vol. 9, 1962, pp. 181–186.
[18] Z. Luo et al., "Semidefinite Relaxation of Quadratic Optimization Problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, May 2010, pp. 20–34.
[19] J.F. Sturm, "Using SeDuMi 1.02, a Matlab Toolbox for Optimization over Symmetric Cones," *Optimization Methods Softw.*, vol. 11, no. 1–4, 1999, pp. 625–653.
[20] J. Lofberg, "YALMIP: A Toolbox for Modeling and Optimization in MATLAB," *Int. Symp. Comput. Aided Contr. Syst. Design*, Taipei, Taiwan, Sept. 2–4, 2004, pp. 284–289.
[21] H. Wang et al., "Hybrid Cooperative Beamforming and Jamming for Physical-Layer Security of Two-Way Relay Networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, Dec. 2013, pp. 2007–2020.

Jong-Ho Lee received his BS degree in electrical engineering and his MS degree and PhD in electrical engineering and computer science from Seoul National University, Rep. of Korea in 1999, 2001, and 2006, respectively. From 2006 to 2008, he was a senior engineer with Samsung Electronics, Suwon, Rep. of Korea. From 2008 to 2009, he was a postdoctoral researcher with the Georgia Institute of Technology, Atlanta, USA. From 2009 to 2012, he was an assistant professor with the Division of Electrical, Electronic, and Control Engineering, Kongju National University, Cheonan, Rep. of Korea. Since 2012, he has been a faculty member in the Department of Electronic Engineering, Gachon University, Seongnam, Rep. of Korea. His research interests include wireless communication systems and signal processing for communication with a current emphasis on multiple-antenna techniques, multi-hop relay networks, physical layer security, and full-duplex wireless communications.

Illsoo Sohn received his BS and MS degrees and his PhD in 2003, 2005, and 2009, respectively, from Seoul National University, Rep. of Korea, all in the field of electrical engineering. From 2009 to 2010, he worked as a postdoctoral researcher at the Wireless Networking and Communication Group, University of Texas, Austin, USA. From 2010 to 2012, he worked as a senior research engineer at the Advanced Communication Technology Research Lab. of LG Electronics, Anyang, Rep. of Korea. From 2012 to 2013, he worked as a network design engineer in the Network Strategy Department of Korea Telecom, Daejeon, Rep. of Korea. Since 2013, he has been an assistant professor in the Department of Electronic Engineering in Gachon University. His current research interests include statistical inference, message-passing algorithms, multi-user MIMO, multi-cell MIMO, time-division duplexing, distributed antennas systems, and cross-layer optimization. Dr. Sohn is a recipient of the IEEE802.11ac Award for Significant Technical Contribution to the MAC (2014), LG Group R&D Award for core-technology development of next-generation WLAN (2012), Heinrich Hertz Award for Best Communications Letter (2011), Gold Prize in the 15th Samsung Humantech Paper Contest (2009), Silver Award in the IEEE International Student Paper Contest, Seoul Section (2008), and Best Poster Paper Award in the IEEE International Student Paper Contest, Seoul Section (2007). He received a Korea Government Fellowship during his PhD studies.

Sungju Song received his BS degree from the Department of Electronics Engineering, Myongji University, Yongin, Rep. of Korea in 2015. He is currently pursuing his MS degree at Myongji University. His current research interests include digital signal processing, motor drives and diagnosis, and partial discharge diagnosis.

Yong-Hwa Kim received his BS degree in electrical engineering and his PhD in electrical engineering and computer science from Seoul National University, in 2001, and 2007, respectively. From 2007 to 2011, he was a senior researcher with the Korea Electrotechnology Research Institute, Ansan, Rep. of Korea. From 2011 to 2013, he was an assistant professor with the Division of Maritime Electronic and Communication Engineering, Mokpo National Maritime University, Rep. of Korea. Since 2013, he has been a faculty member with the Department of Electronic Engineering, Myongji University, where he is now an associate professor. His research interests include communication systems, digital signal processing, motor drives and diagnosis, and machine learning for smart grids.