Collaborative Relay Beamforming for Secure Broadcasting

Junwei Zhang and Mustafa Cenk Gursoy
Department of Electrical Engineering
University of Nebraska-Lincoln, Lincoln, NE 68588
Email: junwei.zhang@huskers.unl.edu, gursoy@engr.unl.edu

***Abstract*—[1] In this paper, collaborative use of relays to form a beamforming system with the aid of perfect channel state information (CSI) and to provide communication in physical-layer security between a transmitter and two receivers is investigated. In particular, we describe decode-and-forward based null space beamforming schemes and optimize the relay weights jointly to obtain the largest secrecy rate region. Furthermore, the optimality of the proposed schemes is investigated by comparing them with the outer bound secrecy rate region.**

I. INTRODUCTION

The open nature of wireless communications allows for the signals to be received by all users within the communication range. Thus, secure transmission of confidential messages is a critical issue in wireless communications. This problem was first studied in [1] where Wyner identified the rate-equivocation region and established the secrecy capacity of the discrete memoryless wiretap channel in which eavesdropper's channel is a degraded version of the main channel. Later, Wyner's result was extended to the Gaussian channel in [3] and recently to fading channels in [4]. In addition to the single antenna case, secure transmission in multi-antenna models is addressed in [5] – [6]. For multi-user channels, Liu *et al.* [7] presented inner and outer bounds on secrecy capacity regions for broadcast and interference channels. The secrecy capacity of multi-antenna broadcasting channel is obtained in [8]. Moreover, it's well known that that users can cooperate to form a distributed multi-antenna system by relaying. Cooperative relaying with secrecy constraints was recently discussed in [10]–[11] .

In this paper, we study the relay-aided secure broadcasting scenario. We assume that the source has two independent messages, each of which is intended for one of the receivers but needs to be kept asymptotically perfectly secret from the other. This is achieved via relay node cooperation in decode and forward fashion to produce virtual beam points to two receivers. The problem is formulated as a problem of designing the relay node weights in order to maximize the secrecy rate for both receivers for a fixed total relay power. We assume that the global channel state information (CSI) is available for weight design. Due to the difficulty of the general optimization problem, we propose null space beamforming transmission schemes and compare their performance with the outer bound secrecy rate region.

[1]This work was supported by the National Science Foundation under Grant CCF – 0546384 (CAREER).

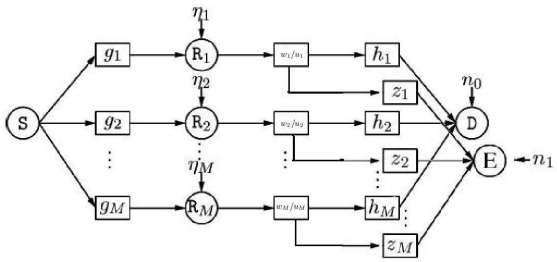

Fig. 1. Channel Model1

II. CHANNEL

We consider a communication channel with a source S, two destination nodes D and E, and M relays $\{R_m\}_{m=1}^{M}$ as depicted in Figure 1. We assume that there is no direct link between S and D, and S and E. We also assume that relays work synchronously and multiply the signals to be transmitted by complex weights to produce virtual beam points to D and E. We denote the channel fading coefficient between S and R_m as $g_m \in \mathbb{C}$, the channel fading coefficient between R_m and D as $h_m \in \mathbb{C}$, and the channel coefficient between R_m and E as $z_m \in \mathbb{C}$. In this model, the source S tries to transmit confidential messages to D and E with the help of the relays . It is obvious that our channel is a two hop relay network. In the first hop, the source S transmits x_s which contains the confidential messages intended for both D and E to the relays with power $E[|x_s|^2] = P_s$. The received signal at relay R_m is given by

$$y_{r,m} = g_m x_s + \eta_m \tag{1}$$

where η_m is the background noise that has a Gaussian distribution with zero mean and a variance of N_m.

In the first hop, the secrecy rates for destination D and E

lie in the following triangle region.

$$R_d \geq 0 \text{ and } R_e \geq 0 \tag{2}$$

$$R_d + R_e \leq \min_{m=1,\ldots,M} \log\left(1 + \frac{|g_m|^2 P_s}{N_m}\right) \tag{3}$$

where R_d and R_e denote the secrecy rates for destination D and E, respectively.

III. Relay Beamforming

We consider the scenario in which relays are much more closer to the source than the destinations, and hence, the first-hop rate does not become a bottleneck of the whole system. Due to this assumption, we in the following focus on characterizing the secrecy rate region of the second-hop. We consider the decode-and-forward relaying protocol in which each relay R_m first decodes the message x_s,and subsequently scales the decoded messages to obtain $x_r = w_m x_d + u_m x_e$, where w_m and u_m are the weight values. x_d and x_e are independent, zero-mean, unit-variance Gaussian signals which include the confidential messages to D and E, respectively. Under these assumptions, the output power of relay R_m is

$$E[|x_r|^2] = E[|w_m x_d + u_m x_e|^2] = |w_m|^2 + |u_m|^2 \tag{4}$$

The received signals at the destination nodes D and E are the superpositions of the signals transmitted from the relays. These signals can be expressed, respectively, as

$$\begin{aligned} y_d &= \sum_{m=1}^{M} h_m w_m x_d + \sum_{m=1}^{M} h_m u_m x_e + n_0 \\ &= \mathbf{h}^\dagger \mathbf{w} x_d + \mathbf{h}^\dagger \mathbf{u} x_e + n_0 \end{aligned} \tag{5}$$

$$\begin{aligned} y_e &= \sum_{m=1}^{M} z_m w_m x_d + \sum_{m=1}^{M} z_m u_m x_e + n_1 \\ &= \mathbf{z}^\dagger \mathbf{w} x_d + \mathbf{z}^\dagger \mathbf{u} x_e + n_1 \end{aligned} \tag{6}$$

where n_0 and n_1 are the Gaussian background noise components at D and E, respectively, with zero mean and variance N_0. Additionally, we have above defined $\mathbf{h} = [h_1^*, \ldots h_M^*]^T, \mathbf{z} = [z_1^*, \ldots z_M^*]^T$, $\mathbf{w} = [w_1, \ldots w_M]^T$, and $\mathbf{u} = [u_1, \ldots u_M]^T$. In these notations, while superscript $*$ denotes the conjugate operation, $(\cdot)^T$ and $(\cdot)^\dagger$ denote the transpose and conjugate transpose , respectively, of a matrix or vector. From the transmitting and receiving relationship in (5) and (6), we can see that the channel we consider can be treated as an interference channel with secrecy constraints studied in [7]. The achievable secrecy rate region is shown to be

$$\begin{aligned} 0 \leq R_d \leq & \log\left(1 + \frac{|\sum_{m=1}^{M} h_m w_m|^2}{N_0 + |\sum_{m=1}^{M} h_m u_m|^2}\right) \\ & - \log\left(1 + \frac{|\sum_{m=1}^{M} z_m w_m|^2}{N_0}\right) \end{aligned} \tag{7}$$

$$\begin{aligned} 0 \leq R_e \leq & \log\left(1 + \frac{|\sum_{m=1}^{M} z_m u_m|^2}{N_0 + |\sum_{m=1}^{M} z_m w_m|^2}\right) \\ & - \log\left(1 + \frac{|\sum_{m=1}^{M} h_m u_m|^2}{N_0}\right). \end{aligned} \tag{8}$$

In this paper, we address the joint optimization $\{w_m\}$ and $\{u_m\}$ with the aid of perfect CSI, and hence identify the optimal collaborative relay beamforming (CRB) direction that maximizes the secrecy rate region given by (7) and (8). Since the optimization problem above is in general intractable, we investigate suboptimal schemes.

A. Single Null Space Beamforming

In this scheme, we choose one user's (e.g., E) beamforming vector (e.g., $\mathbf{u}$) to lie in the null space of the other user's channel. With this assumption, we eliminate the user E's interference on D and hence D's capability of eavesdropping on E. Mathematically, this is equivalent to $|\sum_{m=1}^{M} h_m u_m|^2 = \mathbf{h}^\dagger \mathbf{u} = 0$, which means $\mathbf{u}$ is in the null space of $\mathbf{h}^\dagger$.

We further assume α fraction of total relay transmitting power P_r is used for sending confidential message to D. Under these assumptions, we can solve the optimization problem in (7). The maximum R_d can be computed as

$$\begin{aligned} & R_{d,m}(\mathbf{h}, \mathbf{z}, P_r, \alpha) \\ &= \max_{\mathbf{w}^\dagger \mathbf{w} \leq \alpha P_r} \log \frac{N_0 + |\sum_{m=1}^{M} h_m w_m|^2}{N_0 + |\sum_{m=1}^{M} z_m w_m|^2} \qquad (9) \\ &= \log \max_{\mathbf{w}^\dagger \mathbf{w} \leq \alpha P_R} \frac{N_0 + |\sum_{m=1}^{M} h_m w_m|^2}{N_0 + |\sum_{m=1}^{M} z_m w_m|^2} \qquad (10) \\ &= \log \max \frac{\mathbf{w}^\dagger (\frac{N_0}{\alpha P_r} \mathbf{I} + \mathbf{h}\mathbf{h}^\dagger) \mathbf{w}}{\mathbf{w}^\dagger (\frac{N_0}{\alpha P_r} \mathbf{I} + \mathbf{z}\mathbf{z}^\dagger) \mathbf{w}} \qquad (11) \\ &= \log \max \frac{\mathbf{w}^\dagger (N_0 \mathbf{I} + \alpha P_r \mathbf{h}\mathbf{h}^\dagger) \mathbf{w}}{\mathbf{w}^\dagger (N_0 \mathbf{I} + \alpha P_r \mathbf{z}\mathbf{z}^\dagger) \mathbf{w}} \qquad (12) \\ &= \log \lambda_{max}(N_0 \mathbf{I} + \alpha P_r \mathbf{h}\mathbf{h}^\dagger, N_0 \mathbf{I} + \alpha P_r \mathbf{z}\mathbf{z}^\dagger) \qquad (13) \end{aligned}$$

Here, we use the fact that (12) is the Rayleigh quotient problem, and its maximum value is as given in (13) where $\lambda_{max}(\mathbf{A}, \mathbf{B})$ is the largest generalized eigenvalue of the matrix pair $(\mathbf{A}, \mathbf{B})$. Note that we will also use $\lambda_{max}(\cdot)$ to denote largest eigenvalue of the matrix in later discussion. The optimum beamforming weights $\mathbf{w}$ is

$$\mathbf{w}_{opt} = \varsigma \psi_w \tag{14}$$

where ψ_w is the eigenvector that corresponds to $\lambda_{max}(N_0 \mathbf{I} + \alpha P_r \mathbf{h}\mathbf{h}^\dagger, N_0 \mathbf{I} + \alpha P_r \mathbf{z}\mathbf{z}^\dagger)$ and ς is chosen to ensure $\mathbf{w}_{opt}^\dagger \mathbf{w}_{opt} = \alpha P_r$.

Now we turn our attention to the maximization of R_e when $\mathbf{w} = \mathbf{w}_{opt}$. Note that $N_0 + |\sum_{m=1}^{M} z_m w_m|^2$ is a constant denoted by N_t, Due to the null space constraint, we can write $\mathbf{u} = \mathbf{H}_h^\perp \mathbf{v}$, where $\mathbf{H}_h^\perp$ denotes the projection matrix onto the null space of $\mathbf{h}^\dagger$. Specifically, the columns of $\mathbf{H}_h^\perp$ are orthonormal vectors which form the basis of the null space of $\mathbf{h}^\dagger$. In our case, $\mathbf{H}_h^\perp$ is an $M \times (M-1)$ matrix. The power constraint $\mathbf{u}^\dagger \mathbf{u} = \mathbf{v}^\dagger \mathbf{H}_h^{\perp\dagger} \mathbf{H}_h^\perp \mathbf{v} = \mathbf{v}^\dagger \mathbf{v} \leq (1-\alpha) P_r$.

The maximum R_e under this condition can be computed as

$$
\begin{aligned}
&R_{e,m}(\mathbf{h},\mathbf{z},P_r,\alpha)\\
&=\max_{\mathbf{u}^\dagger\mathbf{u}\le(1-\alpha)P_r}\log\left(1+\frac{|\sum_{m=1}^{M}z_m u_m|^2}{N_t}\right) &(15)\\
&=\log\left(1+\frac{\max_{\mathbf{u}^\dagger\mathbf{u}\le(1-\alpha)P_r}(\mathbf{u}^\dagger\mathbf{z}\mathbf{z}^\dagger\mathbf{u})}{N_t}\right) &(16)\\
&=\log\left(1+\frac{\max_{\mathbf{v}^\dagger\mathbf{v}\le(1-\alpha)P_r}(\mathbf{v}^\dagger{\mathbf{H}_h^\perp}^\dagger\mathbf{z}\mathbf{z}^\dagger\mathbf{H}_h^\perp\mathbf{v})}{N_t}\right) &(17)\\
&=\log\left(1+\frac{(1-\alpha)P_r\lambda_{max}({\mathbf{H}_h^\perp}^\dagger\mathbf{z}\mathbf{z}^\dagger\mathbf{H}_h^\perp)}{N_t}\right) &(18)\\
&=\log\left(1+\frac{(1-\alpha)P_r\mathbf{z}^\dagger\mathbf{H}_h^\perp{\mathbf{H}_h^\perp}^\dagger\mathbf{z}}{N_t}\right) &(19)
\end{aligned}
$$

The optimum beamforming vector $\mathbf{u}$ is

$$\mathbf{u}_{opt}=\mathbf{H}_h^\perp\mathbf{v}=\varsigma_1\mathbf{H}_h^\perp{\mathbf{H}_h^\perp}^\dagger\mathbf{z} \tag{20}$$

where ς_1 is a constant introduced to satisfy the power constraint. Hence, secrecy rate region $\mathbb{R}_{s,b}$ achieved with this strategy is

$$
\begin{aligned}
0\le R_d&\le R_{d,m}(\mathbf{h},\mathbf{z},P_r,\alpha)\\
0\le R_e&\le R_{e,m}(\mathbf{h},\mathbf{z},P_r,\alpha)
\end{aligned} \tag{21}
$$

Note that we can switch the role of D and E, and choose $\mathbf{w}$ to be in the null space of $\mathbf{z}^\dagger$. In general, the union of region described in (21) and its switched counterpart is the secrecy rate region of single null space beamforming strategy.

B. Double Null Space Beamforming

In this scheme, we simultaneously choose the beamforming vectors for D and E to lie in the null space of each other's channel vector. That is $|\sum_{m=1}^{M}h_m u_m|^2=\mathbf{h}^\dagger\mathbf{u}=0$, and $|\sum_{m=1}^{M}z_m w_m|^2=\mathbf{z}^\dagger\mathbf{w}=0$. In this case, the channel reduces to two parallel channels. Since interference is completely eliminated, the secrecy constraint is automatically satisfied. Coding for secrecy is not needed at the relays. The channel input-output relations are

$$y_d=\mathbf{h}^\dagger\mathbf{w}x_d+n_0 \tag{22}$$
$$y_e=\mathbf{z}^\dagger\mathbf{u}x_e+n_1 \tag{23}$$

Now, we only need to solve the following problems:

$$\max_{\mathbf{w}^\dagger\mathbf{w}\le\alpha P_r}\log\left(1+\frac{|\sum_{m=1}^{M}h_m w_m|^2}{N_0}\right)\qquad s.t\ \ \mathbf{z}^\dagger\mathbf{w}=0 \tag{24}$$

$$\max_{\mathbf{u}^\dagger\mathbf{u}\le(1-\alpha)P_r}\log\left(1+\frac{|\sum_{m=1}^{M}z_m u_m|^2}{N_0}\right)\qquad s.t\ \ \mathbf{h}^\dagger\mathbf{u}=0. \tag{25}$$

Similarly as in Section III-A, we can easily find the secrecy rate region $\mathbb{R}_{d,b}$ for double null space beamforming as

$$0\le R_d\le\log\left(1+\frac{\alpha P_r\mathbf{h}^\dagger\mathbf{H}_z^\perp{\mathbf{H}_z^\perp}^\dagger\mathbf{h}}{N_0}\right) \tag{26}$$

$$0\le R_e\le\log\left(1+\frac{(1-\alpha)P_r\mathbf{z}^\dagger\mathbf{H}_h^\perp{\mathbf{H}_h^\perp}^\dagger\mathbf{z}}{N_0}\right) \tag{27}$$

where $\mathbf{H}_z^\perp$ denote the projection matrix onto the null space of $\mathbf{z}^\dagger$ and is defined similarly as $\mathbf{H}_h^\perp$.

C. TDMA

For comparison, we consider in the second-hop that the relay only transmits secret information to one user at a time and treat the other user as the eavesdropper. We assume that relay uses α fraction of time to transmit x_d where $(1-\alpha)$ fraction of the time is used to transmit x_e. The channel now is the standard gaussian wiretap channel instead of an interference channel. It can be easily shown that the rate region $\mathbb{R}_{tdma}$ is

$$0\le R_d\le\alpha\log\lambda_{max}(N_0\mathbf{I}+P_r\mathbf{h}\mathbf{h}^\dagger,N_0\mathbf{I}+P_r\mathbf{z}\mathbf{z}^\dagger) \tag{28}$$
$$0\le R_e\le(1-\alpha)\log\lambda_{max}(N_0\mathbf{I}+P_r\mathbf{z}\mathbf{z}^\dagger,N_0\mathbf{I}+P_r\mathbf{h}\mathbf{h}^\dagger) \tag{29}$$

IV. Optimality

In this section, we investigate the optimality of our proposed null space beamforming techniques. Although the optimal values of $\mathbf{w}$ and $\mathbf{u}$ that maximize the rate region (7) and (8) is unknown, we can easily see that the following rate region is an outer bound region of our original achievable secrecy rate region.

$$0\le R_d\le\log\left(1+\frac{|\sum_{m=1}^{M}h_m w_m|^2}{N_0}\right) &(30)$$
$$-\log\left(1+\frac{|\sum_{m=1}^{M}z_m w_m|^2}{N_0}\right) &(31)$$
$$0\le R_e\le\log\left(1+\frac{|\sum_{m=1}^{M}z_m u_m|^2}{N_0}\right) &(32)$$
$$-\log\left(1+\frac{|\sum_{m=1}^{M}h_m u_m|^2}{N_0}\right). &(33)$$

Again, this rate region should be maximized with all possible $\mathbf{w}$ and $\mathbf{u}$ satisfying $||\mathbf{w}||^2+||\mathbf{u}||^2\le P_r$. From the above expressions, we can see that this outer bound can be interpreted as two simultaneously transmitting wire-tap channels. Fortunately, the optimization problem in this case can be solved analytically. With the same assumptions as before that $||\mathbf{w}||^2=\alpha P_r$, $||\mathbf{u}||^2=(1-\alpha)P_r$, we can easily show that the outer bound secrecy rate region $\mathbb{R}_{outer}$ of our collaborative relay beamforming system is

$$0\le R_d\le\log\lambda_{max}(N_0\mathbf{I}+\alpha P_r\mathbf{h}\mathbf{h}^\dagger,N_0\mathbf{I}+\alpha P_r\mathbf{z}\mathbf{z}^\dagger) \tag{34}$$
$$0\le R_e\le\log\lambda_{max}(N_0\mathbf{I}+(1-\alpha)P_r\mathbf{z}\mathbf{z}^\dagger,N_0\mathbf{I}+(1-\alpha)P_r\mathbf{h}\mathbf{h}^\dagger) \tag{35}$$

The expression for R_d and R_e here coincide with the secrecy capacity of Gaussian MISO wiretap channel [5] [6] with transmit power levels αP and $(1-\alpha)P$.

A. Optimality in the High-SNR Regime

In this section, we show that the outer bound region $\mathbb{R}_{outer}$ converges to the proposed null space beamforming regions at high SNR. For the single null space beamforming scheme, the maximum R_d in (13) has the same express as in (34), and thus it is automatically optimal. R_e in single null space beamforming has basically the same expression as that of R_e in double null space beamforming with N_0 replaced by N_t. This difference is negligible as P goes infinity. Hence, we focus on double null space beamforming and show that in the high-SNR regime, the $\mathbb{R}_{outer}$ coincide with the double null space region described by (26) and (27). In the following analysis, for simplicity and without loss of generality, we assume $N_0 = 1$. From the Corollary 4 in Chapter 4 of [6], we can see that

$$\lim_{P_r\to\infty} \frac{1}{P_r}\lambda_{max}(\mathbf{I}+P_r\mathbf{h}\mathbf{h}^\dagger, \mathbf{I}+P_r\mathbf{z}\mathbf{z}^\dagger) = \max_{\tilde{\psi}} |\mathbf{h}^\dagger\tilde{\psi}|^2 \quad (36)$$

where $\tilde{\psi}$ is a unit vector on the null space of $\mathbf{z}^\dagger$. Similarly, we can define $\tilde{\psi}_1$ as a unit vector on the null space of $\mathbf{h}^\dagger$. Combining this result with (34) and (35), we can express the region $\mathbb{R}_{outer}$ at high SNRs as

$$0 \le R_d \le \log(\alpha P_r) + \log(\max_{\tilde{\psi}} |\mathbf{h}^\dagger\tilde{\psi}|^2) + o(1) \quad (37)$$

$$0 \le R_e \le \log((1-\alpha)P_r) + \log(\max_{\tilde{\psi}_1} |\mathbf{z}^\dagger\tilde{\psi}_1|^2) + o(1) \quad (38)$$

where $o(1) \to 0$ as $P_r \to \infty$. On the other hand, double null space beamforming region satisfies

$$0 \le R_d \le \max_{\mathbf{w}^\dagger\mathbf{w}\le\alpha P_r} \log\left(1+|\sum_{m=1}^{M} h_m w_m|^2\right) \quad (39)$$

$$= \log(\alpha P_r) + \log(\max_{\tilde{\psi}} |\mathbf{h}^\dagger\tilde{\psi}|^2) + o(1) \quad (40)$$

$$0 \le R_e \le \max_{\mathbf{u}^\dagger\mathbf{u}\le(1-\alpha)P_r} \log\left(1+|\sum_{m=1}^{M} z_m u_m|^2\right) \quad (41)$$

$$= \log((1-\alpha)P_r) + \log(\max_{\tilde{\psi}_1} |\mathbf{z}^\dagger\tilde{\psi}_1|^2) + o(1). \quad (42)$$

Above, (40) follows from the observation that

$$\lim_{P_r\to\infty} \log\left(1+|\sum_{m=1}^{M} h_m w_m|^2\right) - \log(\alpha P_r) \quad (43)$$

$$= \lim_{P_r\to\infty} \log\left(\frac{1}{\alpha P_r} + \left|\sum_{m=1}^{M} h_m \frac{w_m}{\sqrt{\alpha P_r}}\right|^2\right) \quad (44)$$

$$= \log|\mathbf{h}^\dagger\tilde{\psi}|^2 \quad (45)$$

where $\tilde{\psi}$ is a unit vector and is in the null space of $\mathbf{z}^\dagger$ because $\mathbf{w}$ is in the null space of $\mathbf{z}^\dagger$. (42) follows similarly. Thus, the outer bound secrecy rate region converges to the double null space beamforming region in the high-SNR regime, showing that the null space beamforming strategies are optimal in this regime.

B. Optimality of TDMA in the Low-SNR Regime

In this section, we consider the limit $P_r \to 0$. In the following steps, the order notation $o(P_r)$ means that $o(P_r)/P_r \to 0$ as $P_r \to 0$.

$$\lambda_{max}(\mathbf{I}+P_r\mathbf{h}\mathbf{h}^\dagger, \mathbf{I}+P_r\mathbf{z}\mathbf{z}^\dagger) \quad (46)$$

$$= \lambda_{max}\left((\mathbf{I}+P_r\mathbf{z}\mathbf{z}^\dagger)^{-1}(\mathbf{I}+P_r\mathbf{h}\mathbf{h}^\dagger)\right) \quad (47)$$

$$= \lambda_{max}\left((\mathbf{I}-P_r\mathbf{z}\mathbf{z}^\dagger+o(P_r))(\mathbf{I}+P_r\mathbf{h}\mathbf{h}^\dagger)\right) \quad (48)$$

$$= \lambda_{max}\left((\mathbf{I}-P_r\mathbf{z}^\dagger\mathbf{z})(\mathbf{I}+P_r\mathbf{h}\mathbf{h}^\dagger)\right) + o(P_r) \quad (49)$$

$$= \lambda_{max}\left(\mathbf{I}+P_r(\mathbf{h}\mathbf{h}^\dagger-\mathbf{z}\mathbf{z}^\dagger)\right) + o(P_r) \quad (50)$$

$$= 1 + P_r\lambda_{max}(\mathbf{h}\mathbf{h}^\dagger-\mathbf{z}\mathbf{z}^\dagger) + o(P_r) \quad (51)$$

Combining this low-SNR approximation with (34) and (35), we can see that the $\mathbb{R}_{outer}$ at low SNRs is

$$0 \le R_d \le \log\lambda_{max}(\mathbf{I}+\alpha P_r\mathbf{h}\mathbf{h}^\dagger, \mathbf{I}+\alpha P_r\mathbf{z}\mathbf{z}^\dagger)$$
$$= \alpha P_r\lambda_{max}(\mathbf{h}\mathbf{h}^\dagger-\mathbf{z}\mathbf{z}^\dagger) + o(P_r) \quad (52)$$

$$0 \le R_e \le \log\lambda_{max}(\mathbf{I}+(1-\alpha)P_r\mathbf{z}\mathbf{z}^\dagger, \mathbf{I}+(1-\alpha P_r)\mathbf{h}\mathbf{h}^\dagger)$$
$$= (1-\alpha)P_r\lambda_{max}(\mathbf{z}\mathbf{z}^\dagger-\mathbf{h}\mathbf{h}^\dagger) + o(P_r) \quad (53)$$

Note that (52) and (53) are also the low-SNR approximations for the TDMA approach. Thus, the TDMA scheme can achieve the optimal rate region in the low-SNR regime. For the completeness, we give the lower SNR approximations for single and double null space beamforming as well. For single null space beamforming scheme, the low-SNR approximation of (21) is

$$0 \le R_d \le \alpha P_r\lambda_{max}(\mathbf{h}\mathbf{h}^\dagger-\mathbf{z}\mathbf{z}^\dagger) + o(P_r) \quad (54)$$

$$0 \le R_e \le (1-\alpha)P_r/N_t\mathbf{z}^\dagger\mathbf{H}_z^\perp{\mathbf{H}_z^\perp}^\dagger\mathbf{z} + o(P_r) \quad (55)$$

while for the double null space beamforming scheme, low-SNR approximations of (26) and (27) are

$$0 \le R_d \le \alpha P_r\mathbf{h}^\dagger\mathbf{H}_z^\perp{\mathbf{H}_z^\perp}^\dagger\mathbf{h} + o(P_r) \quad (56)$$

$$0 \le R_e \le (1-\alpha)P_r\mathbf{z}^\dagger\mathbf{H}_h^\perp{\mathbf{H}_h^\perp}^\dagger\mathbf{z} + o(P_r) \quad (57)$$

C. Optimality when the Number of Relays is Large

It is easy to show that

$$\lambda_{max}(\mathbf{I}+\alpha P_r\mathbf{h}\mathbf{h}^\dagger, \mathbf{I}+\alpha P_r\mathbf{z}\mathbf{z}^\dagger) \le \lambda_{max}(\mathbf{I}+\alpha P_r\mathbf{h}\mathbf{h}^\dagger)$$
$$= 1+\alpha P_r\mathbf{h}^\dagger\mathbf{h} \quad (58)$$

Now, consider the function

$$1+\alpha P_r\mathbf{h}^\dagger\mathbf{H}_z^\perp{\mathbf{H}_z^\perp}^\dagger\mathbf{h} \quad (59)$$

which is inside the $\log$ function in the double null space beamforming R_d boundary rate (26). In our numerical results, we observe that when M is large and $\mathbf{h}$ and $\mathbf{z}$ are Gaussian distributed (Rayleigh fading environment), (58) and (59) converge to the same value. Similar results are also noted when R_e in (27) is considered. These numerical observations indicate the optimality of null space beamforming strategies in the regime in which the number of relays, M, is large.

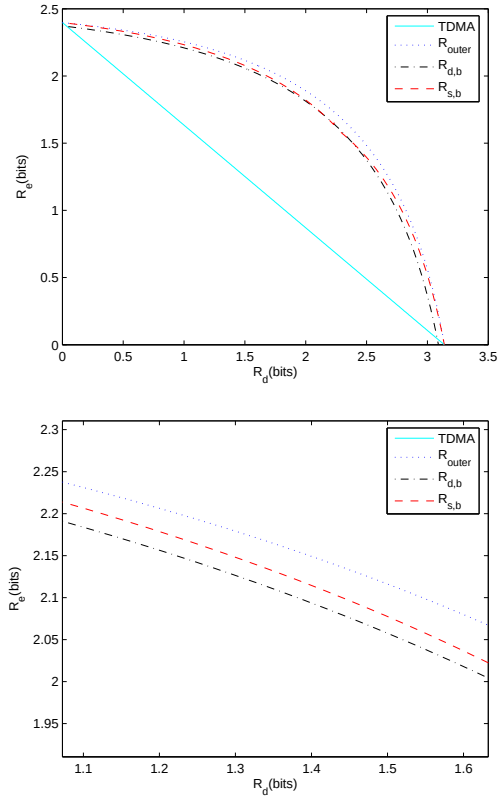

Fig. 2. Second-hop secrecy rate region $\sigma_h = 2, \sigma_z = 2, P_r = 1, M = 5$. Lower figure provides a zoomed version.

V. SIMULATION RESULTS

In our simulations, we assume $N_m = N_0 = 1$, and $\{g_m\}$, $\{h_m\}, \{z_m\}$ are complex, circularly symmetric Gaussian random variables with zero mean and variances σ_g^2, σ_h^2, and σ_z^2 respectively.

In Figures 2 and 3, we plot the second-hop secrecy rate region of different schemes in which we see $\mathbb{R}_{outer} \supset \mathbb{R}_{s,b} \supset \mathbb{R}_{d,b} \supset \mathbb{R}_{tdma}$. We notice that our proposed suboptimal beamforming region is very close to outer bound secrecy region $\mathbb{R}_{outer}$. Furthermore, the larger the M, the smaller the rate gap between $\mathbb{R}_{outer}$ and our proposed null space beamforming schemes. Also, we note that increasing the number of relays,M, enlargens the rate region. Moreover, we can see that $M = 15$ is sufficient for the null space beamforming schemes to coincide with the $\mathbb{R}_{outer}$.

Next, we examine the null space beamforming's optimality in the high-SNR regime in Fig. 4. In this simulation, we can see that when the relay power is large enough, $\mathbb{R}_{outer}$ coincides with the regions of our proposed null space beamforming schemes as expected even M is very small. Finally, in Fig. 5 where relay power small, we observe that $\mathbb{R}_{outer}$ coincides with the rate region of the TDMA transmission scheme. Also, we note that the double null space beamforming has better performance than single null space beamforming at some operation points. This is mainly because N_t is no longer negligible at very low SNR values.

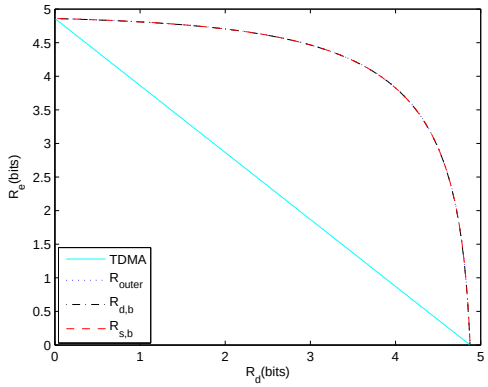

Fig. 3. Second-hop secrecy rate region $\sigma_h = 2, \sigma_z = 2, P_r = 1, M = 15$

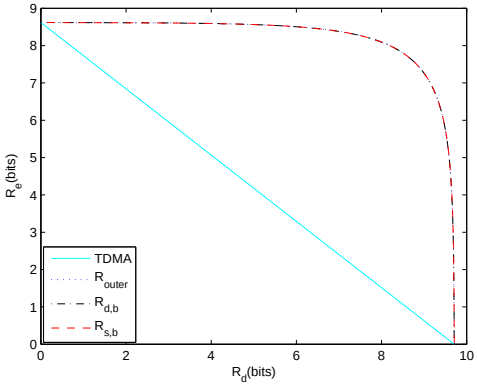

Fig. 4. Second hop secrecy rate region $\sigma_h = 2, \sigma_z = 2, P_r = 100, M = 3$

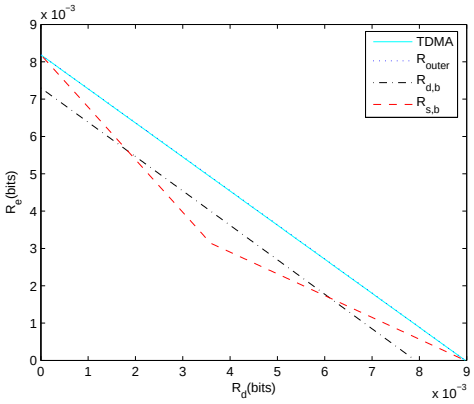

Fig. 5. Second hop secrecy rate region $\sigma_h = 2, \sigma_z = 2, P_r = 0.001, M = 10$

VI. Conclusion

In this paper, we have considered a DF-based collaborative relay beamforming protocol to achieve secure broadcasting to two users. As the general optimization of relay weights is a difficult task, we have proposed single and double null space beamforming schemes. We have compared the rate regions of these two schemes and the TDMA scheme with the outer bound secrecy rate region of the original the relay beamforming system. We have analytically shown that null space beamforming schemes are optimal in the high-SNR regime, and TDMA scheme is optimal in the low-SNR regime. In our numerical results, we have seen that our proposed null space beamforming schemes perform in general very close to outer bound secrecy rate region. We have numerically shown that when the number of relays is large, the null space beamforming schemes are optimal.

References

[1] A. Wyner "The wire-tap channel," *Bell. Syst Tech. J*, vol.54, no.8, pp.1355-1387, Jan 1975.

[2] I. Csiszar and J. Korner "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol.IT-24, no.3, pp.339-348, May 1978.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol.IT-24, no.4, pp.451-456, July 1978.

[4] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels" *IEEE Trans. Inform. Theory*, vol.54, no.10, pp.4687-4698, Oct 2008

[5] S. Shafiee and S. Ulukus "Achievable rates in Gaussian MISO channels with secrecy constraint," *IEEE Intl Symp. on Inform. Theory*, Nice, France, June 2007.

[6] A. Khisti, " Algorithms and Architectures for Multiuser, Multiterminal, and Multilayer Information-Theoretic Security " Doctoral Thesis, MIT 2008.

[7] R. Liu, I. Maric, P. Spasojevic and R. D. Yates, "Discrete Memoryless Interference and Broadcast Channels with Confidential Messages: Secrecy Capacity Regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493-2507, Jun. 2008.

[8] R. Liu and H. V. Poor, "Secrecy Capacity Region of a Multi-Antenna Gaussian Broadcast Channel with Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235-1249, Mar. 2009.

[9] G. Zheng, K. Wong, A. Paulraj, and B. Ottersten, "Collaborative-Relay Beamforming With Perfect CSI: Optimum and Distributed Implementation," *IEEE Signal Process Letters*, vol. 16, no. 4, April 2009

[10] L. Dong, Z. Han, A. Petropulu and H. V. Poor, "Secure wireless communications via cooperation," *Proc. 46th Annual Allerton Conf. Commun., Control, and Computing*, Monticello, IL, Sept. 2008.

[11] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," *Proc. IEEE Intl Conf. Acoust. Speech Signal Proc.*, Taipei, Taiwan, Apr. 2009.