Secure Relay Beamforming over Cognitive Radio Channels

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—In this paper, a cognitive relay channel is considered, and amplify-and-forward (AF) relay beamforming designs in the presence of an eavesdropper and a primary user are studied. Our objective is to optimize the performance of the cognitive relay beamforming system while limiting the interference in the direction of the primary receiver and keeping the transmitted signal secret from the eavesdropper. We show that under both total and individual power constraints, the problem becomes a quasiconvex optimization problem which can be solved by interior point methods. We also propose two sub-optimal null space beamforming schemes which are obtained in a more computationally efficient way.

Index Terms: Amplify-and-forward relaying, cognitive radio, physical-layer security, relay beamforming.

I. INTRODUCTION

The need for the efficient use of the scarce spectrum in wireless applications has led to significant interest in the analysis of cognitive radio systems. One possible scheme for the operation of the cognitive radio network is to allow the secondary users to transmit concurrently on the same frequency band with the primary users as long as the resulting interference power at the primary receivers is kept below the interference temperature limit [1]. Note that interference to the primary users is caused due to the broadcast nature of wireless transmissions, which allows the signals to be received by all users within the communication range. Note further that this broadcast nature also makes wireless communications vulnerable to eavesdropping. The problem of secure transmission in the presence of an eavesdropper was first studied from an information-theoretic perspective in [2] where Wyner considered a wiretap channel model. In [2], the secrecy capacity is defined as the maximum achievable rate from the transmitter to the legitimate receiver, which can be attained while keeping the eavesdropper completely ignorant of the transmitted messages. Later, Wyner’s result was extended to the Gaussian channel in [4]. Recently, motivated by the importance of security in wireless applications, information-theoretic security has been investigated in fading multi-antenna and multiuser channels. For instance, cooperative relaying under secrecy constraints was studied in [9]–[11].

In this paper, we investigate the collaborative relay beamforming under secrecy constraints in the cognitive radio network. We first characterize the secrecy rate of the amplify-and-forward (AF) cognitive relay channel. Then, we formulate the beamforming optimization as a quasiconvex optimization problem which can be solved through convex semidefinite programming (SDP). Furthermore, we propose two sub-optimal null space beamforming schemes to reduce the computational complexity.

II. CHANNEL MODEL

We consider a cognitive relay channel with a secondary user source $S$, a primary user $P$, a secondary user destination $D$, an eavesdropper $E$, and $M$ relays $\{R_m\}_{m=1}^M$, as depicted in Figure 1. We assume that there is no direct link between $S$ and $D$, $S$ and $P$, and $S$ and $E$. We also assume that relays work synchronously to perform beamforming by multiplying the signals to be transmitted with complex weights $\{w_m\}$. We denote the channel fading coefficient between $S$ and $R_m$ by $g_m \in \mathbb{C}$, the fading coefficient between $R_m$ and $D$ by $h_m \in \mathbb{C}$, $R_m$ and $P$ by $k_m \in \mathbb{C}$ and the fading coefficient between $R_m$ and $E$ by $z_m \in \mathbb{C}$. In this model, the source $S$ tries to transmit confidential messages to $D$ with the help of the relays on the same band as the primary user’s while keeping the interference on the primary user below some predefined interference temperature limit and keeping the eavesdropper $E$ ignorant of the information. It’s obvious that our channel is a two-hop relay network. In the first hop, the source $S$ transmits $x_s$ to relays with power $E||x_s||^2 = P_s$. The received signal at the $m^{th}$ relay $R_m$ is given by

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

(1)
where $\eta_m$ is the background noise that has a Gaussian distribution with zero mean and variance of $N_m$.

In the AF scenario, the received signal at $R_m$ is directly multiplied by $l_m w_m$ without decoding, and forwarded to $D$. The relay output can be written as:

$$x_{r,m} = w_m l_m (g_m x_s + \eta_m).$$  \hspace{1cm} (2)

The scaling factor,

$$l_m = \frac{1}{\sqrt{|g_m|^2 p + N_m}},$$  \hspace{1cm} (3)

is used to ensure $E[|x_{r,m}|^2] = |w_m|^2$. There are two kinds of power constraints for relays. First one is a total relay power constraint in the following form: $\|w\|^2 = w^\dagger w \leq P_T$ where $w = [w_1 \ldots w_M]^\dagger$ and $P_T$ is the maximum total power. $(\cdot)^\dagger$ and $(\cdot)^\dagger$ denote the transpose and conjugate transpose, respectively, of a matrix or vector. In a multiuser network such as the relay system we study in this paper, it is practically more relevant to consider individual power constraints as wireless nodes generally operate under such limitations. Motivated by this, we can impose $|w_m|^2 \leq p_m$ or equivalently $|w|^2 \leq \mathbf{p}$ where $|\cdot|^2$ denotes the element-wise norm-square operation and $\mathbf{p}$ is a column vector that contains the components $\{p_m\}$. $p_m$ is the maximum power for the $m^{th}$ relay node.

The received signals at the destination $D$ and eavesdropper $E$ are the superposition of the messages sent by the relays. These received signals are expressed, respectively, as

$$y_d = \sum_{m=1}^{M} h_m w_m l_m (g_m x_s + \eta_m) + n_0,$$  \hspace{1cm} (4)

$$y_e = \sum_{m=1}^{M} z_m w_m l_m (g_m x_s + \eta_m) + n_1,$$  \hspace{1cm} (5)

where $n_0$ and $n_1$ are the Gaussian background noise components with zero mean and variance $N_0$, at $D$ and $E$, respectively. It is easy to compute the received SNR at $D$ and $E$ as

$$\Gamma_d = \frac{|\sum_{m=1}^{M} h_m g_m l_m w_m|^2 P_s}{\sum_{m=1}^{M} |h_m|^2 |l_m|^2 |w_m|^2 N_m + N_0},$$  \hspace{1cm} (6)

$$\Gamma_e = \frac{|\sum_{m=1}^{M} z_m g_m l_m w_m|^2 P_s}{\sum_{m=1}^{M} |z_m|^2 |l_m|^2 |w_m|^2 N_m + N_0}.$$  \hspace{1cm} (7)

The secrecy rate is now given by

$$R_s = I(x_s; y_d) - I(x_s; y_e)$$  \hspace{1cm} (8)

$$= \log(1 + \Gamma_d) - \log(1 + \Gamma_e)$$  \hspace{1cm} (9)

$$= \log \left( \frac{\sum_{m=1}^{M} |h_m|^2 |l_m|^2 |w_m|^2 N_m + N_0}{\sum_{m=1}^{M} |h_m|^2 |l_m|^2 |w_m|^2 N_m + N_0} \times \frac{\sum_{m=1}^{M} |z_m|^2 |l_m|^2 |w_m|^2 N_m + N_0}{\sum_{m=1}^{M} |z_m|^2 |l_m|^2 |w_m|^2 N_m + N_0} \right)$$ \hspace{1cm} (10)

where $I(\cdot; \cdot)$ denotes the mutual information. The interference at the primary user is

$$\Lambda = \sum_{m=1}^{M} k_m g_m l_m w_m |w_m|^2 P_s + \sum_{m=1}^{M} |k_m|^2 |l_m|^2 |w_m|^2 N_m.$$  \hspace{1cm} (11)

In this paper, under the assumption that the relays have perfect channel side information (CSI), we address the joint optimization of $\{w_m\}$ and hence identify the optimum collaborative relay beamforming (CRB) direction that maximizes the secrecy rate in (10) while maintaining the interference on the primary user under a certain threshold, i.e., $\Lambda \leq \gamma$, where $\gamma$ is the interference temperature limit.

III. OPTIMAL BEAMFORMING

Let us define

$$\mathbf{h}_g = [h_1^* g_1^T l_1, \ldots, h_M^* g_M^T l_M]^T,$$  \hspace{1cm} (12)

$$\mathbf{h}_x = [z_1^* g_1^T l_1, \ldots, z_M^* g_M^T l_M]^T,$$  \hspace{1cm} (13)

$$\mathbf{h}_k = [k_1^* g_1^T l_1, \ldots, k_M^* g_M^T l_M]^T,$$  \hspace{1cm} (14)

$$\mathbf{D}_h = \text{Diag}(||h_1||^2 N_1, \ldots, ||h_M||^2 N_M),$$  \hspace{1cm} (15)

$$\mathbf{D}_z = \text{Diag}(||z_1||^2 N_1, \ldots, ||z_M||^2 N_M),$$  \hspace{1cm} (16)

$$\mathbf{D}_k = \text{Diag}(||k_1||^2 N_1, \ldots, ||k_M||^2 N_M),$$  \hspace{1cm} (17)

where superscript $^*$ denotes conjugate operation. Then, the received SNR at the destination and eavesdropper, and the interference on primary user can be written, respectively, as

$$\Gamma_d = \frac{P_s w^\dagger \mathbf{h}_g \mathbf{h}_g^\dagger w}{w^\dagger \mathbf{D}_h w + N_0},$$  \hspace{1cm} (18)

$$\Gamma_e = \frac{P_s w^\dagger \mathbf{h}_x \mathbf{h}_x^\dagger w}{w^\dagger \mathbf{D}_z w + N_0},$$  \hspace{1cm} (19)

$$\Lambda = P_s w^\dagger \mathbf{h}_k \mathbf{h}_k^\dagger w + w^\dagger \mathbf{D}_k w.$$  \hspace{1cm} (20)
in (10) as
\[
\frac{1 + \Gamma_d}{1 + \Gamma_c} = \frac{1 + \frac{P_c}{P_d}w_h^h h_e^h w}{w^H D_h w + N_0} = \frac{w^H D_h w + N_0}{w^H D_h w + N_0} \quad (21)
\]
\[
= \frac{N_0 + tr((D_h + P_s h_h h_g^H) w w^H)}{N_0 + tr((D_z + P_s h_h h_g^H) w w^H)} \times \frac{w^H D_z w + N_0}{w^H D_h w + N_0}.
\]
If we denote \( t_1 = \frac{N_0 + tr((D_h + P_s h_h h_g^H) w w^H)}{N_0 + tr((D_z + P_s h_h h_g^H) w w^H)} \),
\( t_2 = \frac{N_0 + tr((D_z w w^H))}{N_0 + tr((D_h w w^H))} \),
define \( X \triangleq w w^H \), and employ the semidefinite relaxation approach, we can express the beamforming optimization problem as
\[
\max_{X, t_1, t_2} \quad t_1 t_2
\]
\[
s.t \quad tr \left( X \left( D_h + P_s h_h h_g^H - t_1 \left( D_z + P_s h_h h_g^H \right) \right) \right) \geq N_0(t_1 - 1)
\]
\[
tr \left( X \left( D_z - t_2 D_h \right) \right) \geq N_0(t_2 - 1)
\]
\[
tr \left( X \left( D_k + P_s h_h h_g^H \right) \right) \leq \gamma
\]
and \( \text{diag}(X) \leq p \) \quad (and/or \( tr(X) \leq P_T \) \quad and \( X \succeq 0 \).
\]

The optimization problem here is similar to that in [1]. The only difference is that we have an additional constraint due to the interference limitation. Thus, we can use the same optimization framework. The optimal beamforming solution that maximizes the secrecy rate in the cognitive relay channel can be obtained by using semidefinite programming with a two-dimensional search for both total and individual power constraints. For simulation, one can use the well-developed interior point method based package SeDuMi [14], which produces a feasibility certificate if the problem is feasible, and its popular interface Yalmip [15]. It is important to note that we should have the optimal \( X \) to be of rank-one to determine the beamforming vector. While proving analytically the existence of a rank-one solution for the above optimization problem seems to be a difficult task [16], we would like to emphasize that the solutions are rank-one in our simulations. Thus, our numerical result are tight. Also, even in the case we encounter a solution with rank higher than one, the Gaussian randomization technique is practically proven to be effective in finding a feasible, rank-one approximate solution of the original problem. Details can be found in [8].

IV. SUB-OPTIMAL NULL SPACE BEAMFORMING

Obtaining the optimal solution requires significant computation. To simplify the analysis, we propose suboptimal null space beamforming techniques in this section.

A. Beamforming in the Null Space of Eavesdropper’s Channel (BNE)

We choose \( w \) to lie in the null space of \( h_z \). With this assumption, we eliminate \( E \)'s capability of eavesdropping on \( D \). Mathematically, this is equivalent to \( \sum_{m=1}^M g_m l_m w_m^2 = 0 \), which means \( w \) is in the null space of \( h_z \). We can write \( w = H_z^\perp v \), where \( H_z^\perp \) denotes the projection matrix onto the null space of \( h_z \). Specifically, the columns of \( H_z^\perp \) are orthonormal vectors which form the basis of the null space of \( h_z \). In our case, \( H_z^\perp \) is an \( M \times (M - 1) \) matrix. The total power constraint becomes \( w^H w = v^H H_z^\perp H_z^\perp v = v^H v \leq P_T \). The individual power constraint becomes \( |H_z^\perp v|^2 \leq p \).

Under the above null space beamforming assumption, \( \Gamma_c \) is zero. Hence, we only need to maximize \( \Gamma_d \) to get the highest achievable secrecy rate. \( \Gamma_d \) is now expressed as
\[
\Gamma_d = P_s v^H H_z^\perp h_h h_g^H H_z^\perp H_s^\perp v + v^H H_z^\perp D_h H_z^\perp v + N_0.
\]

The interference on the primary user can be written as
\[
\Lambda = P_s v^H H_z^\perp h_h h_g^H H_s^\perp v + v^H H_s^\perp D_k H_s^\perp v.
\]

Defining \( X \triangleq vv^H \), we can express the optimization problem as
\[
\max_{X,v} \quad t
\]
\[
s.t \quad tr \left( X \left( P_s H_z^\perp h_h h_g^H H_z^\perp - t H_z^\perp D_h H_z^\perp \right) \right) \geq N_0 t
\]
\[
tr \left( X \left( H_z^\perp D_k H_z^\perp + P_s H_z^\perp h_h h_g^H H_s^\perp \right) \right) \leq \gamma
\]
and \( \text{diag}(H_z^\perp X H_z^\perp) \leq p \) \quad (and/or \( tr(X) \leq P_T \) \quad and \( X \succeq 0 \).
\]

B. Beamforming in the Null Space of Eavesdropper’s and Primary User’s Channels (BNEP)

In this section, we choose \( w \) to lie in the null space of \( h_z \) and \( h_k \). Mathematically, this is equivalent to requiring \( \sum_{m=1}^M g_m l_m w_m^2 = 0 \), and \( \sum_{m=1}^M k_m g_m l_m w_m^2 = 0 \), and \( \sum_{m=1}^M k_m g_m l_m w_m^2 = 0 \). We can write \( w = H_z^\perp v \), where \( H_z^\perp \) denotes the projection matrix onto the null space of \( h_z \). Specifically, the columns of \( H_z^\perp \) are orthonormal vectors which form the basis of the null space. In our case, \( H_z^\perp \) is an \( M \times (M - 2) \) matrix. The total power constraint becomes \( w^H w = v^H H_z^\perp H_z^\perp v = v^H v \leq P_T \). The individual power constraint becomes \( |H_z^\perp v|^2 \leq p \).

With this beamforming strategy, we again have \( \Gamma_c = 0 \). Moreover, the interference on the primary user is now reduced to
\[
\Lambda = \sum_{m=1}^M k_m^2 g_m^2 l_m^2 |w_m|^2 N_m = v^H H_z^\perp D_k H_z^\perp v
\]

\[\text{(26)}\]
which is the sum of the forwarded additive noise components present at the relays. Now, the optimization problem becomes

$$\max_{X,t} \quad t$$

s.t. \( tr \left( X \left( P_s H^\perp_{x,k} h_g h_g^\dagger H^\perp_{x,k} - t H^\perp_{x,k} D_k H^\perp_{x,k} \right) \right) \geq N_0 t \)

$$tr \left( X \left( H^\perp_{x,k} D_k H^\perp_{x,k} \right) \right) \leq \gamma$$

and \( diag(H^\perp_{x,k} XH^\perp_{x,k}) \leq p, (and/or) \quad tr(X) \leq P_T \)

and \( X \succeq 0 \).

(27)

Again, this problem can be solved through semidefinite programming. With the following assumptions, we can also obtain a closed-form characterization of the beamforming structure. Since the interference experienced by the primary user consists of the forwarded noise components, we can assume that the interference constraint \( \Lambda \leq \gamma \) is inactive unless \( \gamma \) is very small. With this assumption, we can drop this constraint. If we further assume that the relays operate under the total power constraint expressed as \( v^\dagger v \leq P_T \), we can get the following closed-form solution:

$$\max_{v^\dagger v \leq P_T} \quad \Gamma_d$$

$$= \max_{v^\dagger v \leq P_T} P_r v^\dagger H^\perp_{x,k} h_g h_g^\dagger H^\perp_{x,k} v + N_0$$

$$= \max_{v^\dagger v \leq P_T} P_r v^\dagger H^\perp_{x,k} h_g h_g^\dagger H^\perp_{x,k} v + N_0$$

$$= P_r \lambda_{max} \left( H^\perp_{x,k} h_g h_g^\dagger H^\perp_{x,k} + \frac{N_0}{P_T} \mathbf{I} \right) v$$

where \( \lambda_{max}(A,B) \) is the largest generalized eigenvalue of the matrix pair \((A,B)\) \(^3\). Hence, the maximum secrecy rate is achieved by the beamforming vector \( v_{opt} = \zeta u \) where \( u \) is the eigenvector that corresponds to \( \lambda_{max} \left( H^\perp_{x,k} h_g h_g^\dagger H^\perp_{x,k} + \frac{N_0}{P_T} \mathbf{I} \right) \) and \( \zeta \) is chosen to ensure \( v_{opt}^\dagger v_{opt} = P_T \).

V. MULTIPLE PRIMARY USERS AND EAVESDROPPERS

The discussion in Section III can be easily extended to the case of more than one primary user in the network. Each primary user will introduce an interference constraint \( \Gamma_i \leq \gamma_i \) which can be straightforwardly included into (22). The beamforming optimization is still a semidefinite programming problem. On the other hand, the results in Section III cannot be easily extended to the multiple-eavesdropper scenario. In this case, the secrecy rate for AF relaying is \( R_s = I(x_s ; y_d) - \max_i I(x_s ; y_{e_i}) \), where the maximization is over the rates achieved over the links between the relays and different eavesdroppers. Hence, we have to consider the eavesdropper with the strongest channel. In this scenario, the objective function cannot be expressed in the form given in

\(^3\)For a Hermitian matrix \( A \in \mathbb{C}^{n \times n} \) and positive definite matrix \( B \in \mathbb{C}^{n \times n} \), \((\lambda, \psi)\) is referred to as a generalized eigenvalue – eigenvector pair of \((A,B)\) if \((\lambda, \psi)\) satisfy \( A \psi = \lambda B \psi \) \([13]\).

![Fig. 2. AF secrecy rate vs. \( P_T/P_s \). \( \sigma_g = 10, \sigma_h = 1, \sigma_k = 1, M = 10, \gamma = 0dB \).](image)

VI. NUMERICAL RESULTS AND DISCUSSION

We assume that \( \{ g_m \}, \{ h_m \}, \{ z_m \}, \{ k_m \} \) are complex, circularly symmetric Gaussian random variables with zero mean and variances \( \sigma_g^2, \sigma_h^2, \sigma_k^2 \) and \( \sigma^2 \) respectively. In this section, each figure is plotted for fixed realizations of the Gaussian channel coefficients. Hence, the secrecy rates in the plots are instantaneous secrecy rates.

In Fig. 2 we plot the optimal secrecy rates for the amplify-and-forward collaborative relay beamforming system under both individual and total power constraints. We also provide, for comparison, the secrecy rates attained by using the suboptimal beamforming schemes. The fixed parameters are \( \sigma_g = 10, \sigma_h = 1, \sigma_k = 1 \), \( \gamma = 0dB \), and \( M = 10 \). Since AF secrecy rates depend on both the source and relay powers, the rate curves are plotted as a function of \( P_T/P_s \). We assume that the relays have equal powers in the case in which individual power constraints are imposed, i.e., \( P_i = P_T/M \). It is immediately seen from the figure that the suboptimal null space beamforming achievable rates under both total and individual power constraints are very close to the corresponding optimal ones. Especially, they are nearly identical in the high SNR regime, which suggests that null space beamforming is optimal at high SNRs. Thus, null space beamforming schemes are good alternatives as they
rate achieved by beamforming in the null space of both the eavesdropper’s and primary user’s channels (BNEP) is almost insensitive to different interference temperature limits when \( \gamma \geq -4dB \) since it always forces the signal interference to be zero regardless of the value of \( \gamma \). It is further observed that beamforming in the null space of the eavesdropper’s channel (BNE) always achieves near optimal performance regardless the value of \( \gamma \) under both total and individual power constraints.

VII. CONCLUSION

In this paper, collaborative relay beamforming in cognitive radio networks is studied under secrecy constraints. Optimal beamforming designs that maximize secrecy rates are investigated under both total and individual relay power constraints. We have formulated the problem as a semidefinite programming problem and provided an optimization framework. In addition, we have proposed two sub-optimal null space beamforming schemes to simplify the computation. Finally, we have provided numerical results to illustrate the performances of different beamforming schemes.

REFERENCES

[1] S. Haykin “Cognitive radio: brain-empowered wireless communications,” IEEE J. Sel. Areas Commun, vol.23, no.2, pp.201-220, Feb 2005.
[2] A. Wyner “The wire-tap channel,” Bell. Syst Tech. J, vol.54, no.8, pp.1355-1387, Jan 1975.
[3] I. Csiszar and J. Körner “Broadcast channels with confidential messages,” IEEE Trans. Inform. Theory, vol.IT-24, no.3, pp.339-348, May 1978.
[4] 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.
[5] G. Zheng, K. Wong, A. Paulraj, and B. Ottersten, “Collaborative-relay beamforming with perfect CSI: Optimun and distributed implementation,” IEEE Signal Process Letters, vol. 16, no. 4, Apr. 2009.
[6] V. Nassab, S. Shahbazpanahi, A. Grami, and Z.-Q. Luo, “Distributed beamforming for relay networks based on second order statistics of the channel state information,” IEEE Trans on Signal Proc., Vol. 56, No 9, pp. 4306-4316, Sept. 2008.
[7] G. Zheng, K. K. Wong, A. Paulraj, and B. Ottersten, “Robust collaborative-relay beamforming,” IEEE Trans on Signal Proc., vol. 57, no. 8, Aug. 2009.
[8] Z-Q Luo , Wing-kin Ma , A-M-C. So ,Yinyu Ye , Shuzhong Zhang “Semidefinite relaxation of quadratic optimization problems” IEEE Signal Proc. Magn., vol. 27, no. 3, May 2010
[9] 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.
[10] J. Zhang and M. C. Gursoy, “Collaborative relay beamforming for secrecy,” Proc. of the IEEE International Conference on Communication (ICC), Cape Town, South Africa, May 2010.
[11] J. Zhang and M.C. Gursoy, “Relay beamforming strategies for physical-layer security,” Proc. of the 44th Annual Conference on Information Sciences and Systems, Princeton, March 2010.
[12] Y. Pei, Y-C. Liang, L. Zhang, K. C. Teh, and K. H. Li “Secure communication over MISO cognitive radio channel,” IEEE Trans. Wireless. Commun, vol.9, no.4, pp.1494-1502, April. 2010.
[13] G. Golub and C. F. Van Loan, Matrix Computations (3rd ed), Johns Hopkins University Press, 1996
[14] J. Sturm, “Using SeDuMi 1.02: A MATLAB toolbox for optimization over symmetric cones,” Opt. Methods and Software, vol. 11-12, pp. 625-653, 1999.
[15] J. Lofberg, “YALMIP: A MATLAB toolbox for modeling and optimization in MATLAB,” Proc. the CACSD Conf., Taipei, Taiwan, 2004.
[16] S. Boyd and L. Vandenberghe, Convex optimization. Cambridge, U.K.: Cambridge Univ. Press, 2004.