Secure Relay Beamforming over Cognitive Radio Channels

Junwei Zhang  
*University of Nebraska - Lincoln, junwei.zhang@huskers.unl.edu*

Mustafa Cenk Gursoy  
*University of Nebraska - Lincoln, gursoy@engr.unl.edu*

Follow this and additional works at: [http://digitalcommons.unl.edu/electricalengineeringfacpub](http://digitalcommons.unl.edu/electricalengineeringfacpub)

Part of the [Electrical and Computer Engineering Commons](http://digitalcommons.unl.edu/electricalengineeringfacpub)


[http://digitalcommons.unl.edu/electricalengineeringfacpub/219](http://digitalcommons.unl.edu/electricalengineeringfacpub/219)
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 [11], for amplify and forward relaying scheme, not having analytical solutions for the optimal beamforming design under both total and individual power constraints, an iterative algorithm is proposed to numerically obtain the optimal beamforming structure and maximize the secrecy rates.

Although cognitive radio networks are also susceptible to eavesdropping, the combination of cognitive radio channels and information-theoretic security has received little attention. Very recently, Pei et al. in [12] studied secure communication over multiple input, single output (MISO) cognitive radio channels. In this work, finding the secrecy-capacity-achieving transmit covariance matrix under joint transmit and interference power constraints is formulated as a quasiconvex optimization problem.

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 $h_m \in \mathbb{C}$, 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

\[ y_{r,m} = g_m x_s + \eta_m \]
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 \( \ell_m \) without decoding, and forwarded to \( D \). The relay output can be written as

\[
x_{r,m} = \ell_m x_m + \eta_m.
\]

The scaling factor,

\[
\ell_m = \frac{1}{\sqrt{|\gamma_m|^2 P_s + N_m}},
\]

is used to ensure \( E[|x_{r,m}|^2] = |\ell_m|^2 \). 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 \( w = [w_1, ... w_M]^T \) and \( P_T \) is the maximum total power. \((\cdot)^\dagger \) and \((\cdot)^T \) 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 \(|w|^2 \leq p_m \) where \(|\cdot|^2\) denotes the element-wise norm-square operation and \( p \) 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

\[
y_d = \sum_{m=1}^{M} h_m \ell_m (g_m x_s + \eta_m) + n_0, \quad \text{and} \quad \gamma_d = \frac{\sum_{m=1}^{M} |h_m|^2 |\ell_m|^2 |w_m|^2 P_s}{\sum_{m=1}^{M} |h_m|^2 |w_m|^2 N_m + N_0}, \quad \Gamma_d = \frac{\Gamma_d}{\gamma_d} \label{eq:gamma_d}
\]

\[
y_e = \sum_{m=1}^{M} z_m \ell_m (g_m x_s + \eta_m) + n_1, \quad \text{and} \quad \gamma_e = \frac{\sum_{m=1}^{M} |z_m|^2 |\ell_m|^2 |w_m|^2 P_s}{\sum_{m=1}^{M} |z_m|^2 |w_m|^2 N_m + N_0}, \quad \Gamma_e = \frac{\Gamma_e}{\gamma_e} \label{eq:gamma_e}
\]

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

\[
\Gamma_d = \frac{\sum_{m=1}^{M} |h_m|^2 |\ell_m|^2 |w_m|^2 P_s}{\sum_{m=1}^{M} |h_m|^2 |w_m|^2 N_m + N_0}
\]

\[
\Gamma_e = \frac{\sum_{m=1}^{M} |z_m|^2 |\ell_m|^2 |w_m|^2 P_s}{\sum_{m=1}^{M} |z_m|^2 |w_m|^2 N_m + N_0}.
\]

The secrecy rate is now given by

\[
\Rs = I(x_s;y_d) - I(x_s;y_e) = \log(1 + \Gamma_d) - \log(1 + \Gamma_e)
\]

\[
= \log \left( \frac{\sum_{m=1}^{M} |z_m|^2 |\ell_m|^2 |w_m|^2 N_m + N_0}{\sum_{m=1}^{M} |h_m|^2 |\ell_m|^2 |w_m|^2 N_m + N_0} \right)
\]

\[
= \log \left( \frac{\sum_{m=1}^{M} |h_m|^2 |\ell_m|^2 |w_m|^2 P_s}{\sum_{m=1}^{M} |z_m|^2 |\ell_m|^2 |w_m|^2 N_m + N_0} \right)
\]

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

\[
\Lambda = \sum_{m=1}^{M} |k_m|^2 |\ell_m|^2 |w_m|^2 N_m.
\]

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

\[
h_g = [h_1^*, g_1^*, ..., h_M^*, g_M^*]^T,
\]

\[
h_z = [z_1^*, g_1^*, ..., z_M^*, g_M^*]^T,
\]

\[
h_k = [k_1^*, g_1^*, ..., k_M^*, g_M^*]^T,
\]

\[
D_h = \text{Diag}(|h_1|^2 N_1, ..., |h_M|^2 N_M),
\]

\[
D_z = \text{Diag}(|z_1|^2 N_1, ..., |z_M|^2 N_M),
\]

\[
D_k = \text{Diag}(|k_1|^2 N_1, ..., |k_M|^2 N_M)
\]

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

\[
\Gamma_d = \frac{P_s w^\dagger h_g h_g^\dagger w}{w^\dagger D_h w + N_0},
\]

\[
\Gamma_e = \frac{P_s w^\dagger h_z h_z^\dagger w}{w^\dagger D_z w + N_0},
\]

\[
\Lambda = P_s w^\dagger h_k h_k^\dagger w + w^\dagger D_k w.
\]

With these notations, we can write the objective function of the optimization problem (i.e., the term inside the logarithm...
in (10)) as

\[ 1 + \Gamma_d = \frac{1}{1 + \Gamma} = \frac{1}{1 + \frac{P_d \epsilon h_g h_g^\dagger w}{w' D_w + N_0}}. \]

The optimization problem here is similar to that in [11]. 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 2, we would like to emphasize that the solutions are rank-one in our simulations.

\[ \max_{X,t_1,t_2} \quad t_1 t_2 \\
\text{s.t} \quad tr \left( X \left( D_h + P_h h_g h_g^\dagger \right) \right) \geq N_0 (t_1 - 1), \\
tr \left( X \left( D_h - t_2 D_h \right) \right) \geq N_0 (t_2 - 1), \\
tr \left( X \left( D_k + P_h h_k h_k^\dagger \right) \right) \leq \gamma, \\
\text{and} \quad \text{diag}(X) \leq \rho, \quad (\text{and/or} \quad tr(X) \leq \rho_T) \quad \text{and} \quad X \succeq 0. \]

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

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

Under the above null space beamforming assumption, \( \Gamma_e \) is zero. Hence, we only need to maximize \( \Gamma_d \) to get the highest achievable secrecy rate. \( \Gamma_d \) is now expressed as

\[ \Gamma_d = \frac{P_d v^h H_x^\perp h_g h_g^\dagger H_x^\perp v + v^h D_h H_x^\perp v + N_0}{v^h H_x^\perp D_h H_x^\perp v}. \]

The interference on the primary user can be written as

\[ \Lambda = P_d v^h H_x^\perp h_k h_k^\dagger H_x^\perp v + v^h D_h H_x^\perp v. \]

Defining \( X \triangleq vv \), we can express the optimization problem as

\[ \max_{X,v,t} \quad t \\
\text{s.t} \quad tr \left( X \left( D_h + P_h h_g h_g^\dagger - tD_h \right) \right) \geq N_0 t \\
tr \left( X \left( D_h - t D_h \right) \right) \geq N_0 (t_2 - 1), \\
tr \left( X \left( D_k + P_h h_k h_k^\dagger \right) \right) \leq \gamma, \\
\text{and} \quad \text{diag}(H_x^\perp X H_x^\perp) \leq \rho, \quad (\text{and/or} \quad tr(X) \leq \rho_T) \quad \text{and} \quad X \succeq 0. \]

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

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

With this beamforming strategy, we again have \( \Gamma_e = 0 \). Moreover, the interference on the primary user is now reduced to

\[ \Lambda = \sum_{m=1}^{M} |k_m|^2 |l_m|^2 |w_m|^2 N_m = v^h H_{z,k}^\perp D_k H_{z,k}^\perp v. \]
which is the sum of the forward additive noise components present at the relays. Now, the optimization problem becomes

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

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

$$\text{tr} \left( X \left( H_{x,k}^\dagger D_k H_{x,k}^\dagger \right) \right) \leq \gamma$$

and \( \text{diag}(H_{x,k}^\dagger X H_{x,k}^\dagger) \leq \rho \), (and/or \( \text{tr}(X) \leq P_T \)) and \( X \succeq 0 \).

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 \( \mathbf{v}^\dagger \mathbf{v} \leq P_T \), we can get the following closed-form solution:

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

$$= \max_{\mathbf{v}^\dagger \mathbf{v} \leq P_T} \frac{P_s \mathbf{v}^\dagger H_{x,k}^\dagger h_g ^\dagger h_g H_{x,k}^\dagger \mathbf{v}}{\mathbf{v}^\dagger H_{x,k}^\dagger D_k H_{x,k}^\dagger \mathbf{v} + N_0}$$

$$= \max_{\mathbf{v}^\dagger \mathbf{v} \leq P_T} \frac{P_s \mathbf{v}^\dagger H_{x,k}^\dagger h_g ^\dagger h_g H_{x,k}^\dagger \mathbf{v}}{\mathbf{v}^\dagger H_{x,k}^\dagger D_k H_{x,k}^\dagger \mathbf{v} + N_0}$$

$$= P_s \lambda_{max} \left( H_{x,k}^\dagger h_g ^\dagger h_g H_{x,k}^\dagger + N_0 \frac{1}{P_T} I \right)$$

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 \( \mathbf{v}_{opt} = \zeta \mathbf{u} \) where \( \mathbf{u} \) is the eigenvector that corresponds to \( \lambda_{max} \left( H_{x,k}^\dagger h_g ^\dagger h_g H_{x,k}^\dagger + N_0 \frac{1}{P_T} I \right) \) and \( \zeta \) is chosen to ensure \( \mathbf{v}_{opt}^\dagger \mathbf{v}_{opt} = P_T \).

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 \( \Gamma_i \leq \gamma \) 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 (10) and the optimization framework provided in Section III does not directly apply to the multi-eavesdropper model.

However, the null space beamforming schemes discussed in Section IV can be extended to the case of multiple primary users and eavesdroppers under the condition that the number of relay nodes is greater than the number of eavesdroppers or the total number of eavesdroppers and primary users depending on which null space beamforming is used. The reason for this condition is to make sure the projection matrix \( H^\perp \) exists. Note that the null space of \( i \) channels in general has the dimension \( M \times (M - i) \) where \( M \) is the number of relays.

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 \( \sigma_g^2, \sigma_b^2, \sigma_z^2 \) and \( \sigma_k^2 \) 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 \( \sigma_g = 10, \sigma_b = 1, \sigma_z = 1, \sigma_k = 1, M = 10, \gamma = 0dB \). 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

\(^3\)For a Hermitian matrix \( A \in \mathbb{C}^{m \times n} \) 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].
are obtained with much less computational burden. Moreover, we interestingly observe that imposing individual relay power constraints leads to small losses in the secrecy rates.

In Fig. 3, we change the parameters to $\sigma_g = 10, \sigma_h = 1, \sigma_x = 2, \sigma_k = 4, M = 10, \gamma = 10 dB$. In this case, channels between the relays and the eavesdropper and between the relays and the primary-user are on average stronger than the channels between the relays and the destination. We note that beamforming schemes can still attain good performance and we observe similar trends as before.

In Fig. 4, we plot the optimal secrecy rate and the secrecy rates of the two suboptimal null space beamforming schemes (under both total and individual power constraints) as a function of the interference temperature limit $\gamma$. We assume that $P_T = P_s = 0 dB$. It is observed that the secrecy 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 $\gamma \geq -4 dB$ 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