Deaf Cooperation for Secrecy with a Multi-Antenna Helper

Raef Bassily Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
bassily@umd.edu *ulukus@umd.edu*

Abstract—**In this paper, we investigate the roles of cooperative jamming (CJ) and noise forwarding (NF) in improving the achievable secrecy rates of a Gaussian wiretap channel (GWT) when the helper node is equipped with multiple antennas. We decompose the channel from the helper to the eavesdropper into two orthogonal components: one is aligned in the direction of the channel between the helper and the legitimate receiver (direct component) and the other is in the orthogonal direction to the channel between the helper and the legitimate receiver (orthogonal component). We then propose a strategy in which the helper uses the orthogonal component to transmit pure Gaussian noise as in the CJ strategy while he uses the direct component for either CJ or NF depending on the given channel conditions. We explicitly derive the optimal power control policy for this strategy and give the achievable secrecy rates when the direct component is used to perform CJ or NF. We hence derive the channel conditions where CJ is better than NF over the direct component and vice-versa.**

I. Introduction

The notion of introducing artificial noise in a GWT channel by a helpful interferer to confuse the eavesdropper and improve over the secrecy capacity of the original wiretap channel was introduced in [1], [2], [3], [4]. In [2], [3], [4], this notion was called *cooperative jamming* (CJ). The term refers to the cooperation strategy in which a helping interferer transmits white Gaussian noise when it can hurt the eavesdropper more than it can hurt the legitimate receiver and hence improve the achievable secrecy rate. In [5], the idea of helping interferer was applied to the GWT channel in a scheme tantamount to the CJ scheme for the two-user multiple access wiretap channel where one of the users performs cooperative jamming. In [6], the destination carried out jamming over the feedback channel to confuse the eavesdropper.

In the context of relay networks with secrecy constraints, the role of cooperative jamming when the relay node has a single antenna was further investigated in several works, e.g., [7], [8], [9], [10], and [11]. Cooperative jamming strategies in multiple antenna relay networks were investigated in [12], [13], and [14]. In [12], a cooperative jamming strategy is proposed when the relay is equipped with multiple antennas. Under the constraint that the jamming signals must lie in the subspace orthogonal to the channel vector between the relay and the destination, the antenna weights and transmit power of the source and the relay that maximize the achievable secrecy rate subject to a total transmit power constraint were derived in a closed form. In [13], cooperative jamming strategies were proposed for a half-duplex two-hop multiple antenna relay system where the eavesdropper's channel state information was unknown. In [14], a cooperative jamming strategy is proposed for two-hop relay networks where the eavesdropper can wiretap the transmission in both hops. In the model in [14], the source, the destination, and the eavesdropper have multiple antennas, whereas the relay has a single antenna. Under a similar constraint to the one in [12], closed-form solutions were derived for jamming beamformers that maximize the achievable secrecy rate, and the optimal power allocation was obtained using numerical methods.

In all the references above, the role of a helping node was restricted to cooperative jamming, decode-and-forward, and amplify-and-forward. However, a helping node can also play other roles to improve secrecy. In general, in the relay-eavesdropper channel, the relay, which is assumed to be a trusted entity, can help improve secrecy either by listening to the source or by acting as a deaf helper. The role of a relay node to provide and improve secrecy in a wiretap channel was first studied in [15]. In particular, reference [15] introduced another passive (deaf) mode of cooperation, called *noise forwarding* (NF), in which the relay node sends a dummy (context-free) codeword drawn at random from a codebook that is known to both the legitimate receiver and the eavesdropper to introduce helpful interference that would hurt the eavesdropper more than the legitimate receiver. This deaf cooperation strategy was applied without power control to the Gaussian single-relay single-eavesdropper channel in [16]. The idea of such strategy is to create a virtual multiple access wiretap channel where only one user (the source) is active, i.e., sending relevant information, while the other user (the relay) is acting as an interferer that sends a signal drawn from a given codebook. In this way, the destination can perform successive decoding and cancel out the relay signal and achieve higher secrecy rate for the intended message.

In [17], the roles of both CJ and NF strategies in single antenna relay networks was investigated. Reference [17] derives the conditions under which a deaf helper performing either CJ or NF strategy would give rise to a larger achievable secrecy rate than the secrecy capacity of the original GWT channel. In addition, the same reference gives the optimal power allocation

This work was supported by NSF Gants CCF 07-29127, CNS 09-64632, CCF 09-64645, CCF 10-18185 and CNS 11-47811.

policy for each of the two strategies under the assumption that the source, the deaf helper, the legitimate receiver, and the eavesdropper have perfect knowledge of all the relevant channel gains.

In this paper, we extend the model in [17] and consider the case where the deaf helper is equipped with multiple antennas. Interestingly, this extension leads to a new set of results that were not available in the single antenna case. In particular, we show that having multiple antennas allows us to decompose the relay-eavesdropper channel into two orthogonal components, one in the direction of the relay-destination channel (direct component) and the other in the orthogonal direction to the relay-destination channel (orthogonal component). Accordingly, we obtain the optimal deaf cooperation strategy (CJ or NF) along each channel component. It is intuitive that the orthogonal component should be used for cooperative jamming. However, it is not clear what strategy should be used along the direct component. It is not also clear how the relay should distribute its power on these two components.

In this paper, we fully answer these two questions. We give, in terms of the model fixed parameters, the necessary conditions for each of the CJ and the NF strategy to be useful when employed along the direct component, i.e., to improve over the optimal secrecy rate achievable when the transmission from the relay is constrained only to the orthogonal component. In particular, our results show that along the direct component of the channel either CJ is useful or NF is useful but not both. Moreover, there are some cases (which are described in this paper) in which neither CJ nor NF is useful along the direct component. We fully characterize in the closed-form the optimal power allocation policy at the source and the relay for each of the two strategies and hence show how the relay should optimally distribute its power on the two channel components.

Finally, we present numerical examples to illustrate the gains in the achievable secrecy rates by our CJ and NF strategies when the relay is equipped with multiple antennas. Our simulation results clearly show that the rate achievable by our strategies are, in general, significantly larger than those achieved when no splitting of power between CJ and NF is allowed.

II. System Model

We consider the following communication scenario. A single-antenna source, s, sends a confidential message to a single-antenna destination, d, over an AWGN channel in the presence of an informed eavesdropper, e, that also has a single antenna. The communication also occurs in the presence of a helper node, r, that is equipped with K antennas, $K \geq 1$. The helper node r is assumed to be a deaf relay, i.e., it can only help improve the secrecy capacity of the GWT by transmitting interfering signals that are independent of the source message. In literature, there are two proposed strategies for useful interference introduced by a helper node [2], [3], and [15]. In the first strategy, known as cooperative jamming, one allows r to help by transmitting pure Gaussian noise whereas in the second strategy, known as noise forwarding, r sends a dummy codeword from a codebook known to both the legitimate receiver and the eavesdropper. By proper scaling of the channel inputs and accordingly modifying the power constraints at the source and the helper nodes, without loss of generality, one can express the outputs of the GWT channel, with a multiple-antenna deaf helper, at the destination and the eavesdropper as

$$Y = X_s + \mathbf{h}_r^T \mathbf{X}_r + N \tag{1}$$

$$Z = \sqrt{g_s} X_s + \mathbf{g}_r^T \mathbf{X}_r + N' \tag{2}$$

where $\mathbf{h}_r \in \mathbb{R}^K$ is the vector of the channel coefficients between the helper r and the destination d, $g_s \in \mathbb{R}$, $\mathbf{g}_r \in \mathbb{R}^K$ are the channel coefficient scalar and the channel coefficient vector from the source s and the helper r to the eavesdropper, respectively, N and N' are standard Gaussian random variables that denote the noise at the destination and the eavesdropper, respectively, $X_s \in \mathbb{R}$, $\mathbf{X}_r \in \mathbb{R}^K$ are the channel input scalar and the channel input vector at the source s and the helper r, respectively. The channel inputs are subjected to the following average power constraints:

$$E[|X_s|^2] \leq \bar{P}_s, \qquad \text{and} \qquad E[\| \mathbf{X}_r \|^2] \quad \leq \bar{P}_r \tag{3}$$

By possibly writing $\mathbf{g}_r$ as the direct sum $\mathbf{g}_r = \sqrt{\alpha}\mathbf{h}_r + \mathbf{u}_r$ where $\mathbf{h}_r^T \mathbf{u}_r = 0$, one can write $\mathbf{X}_r$ in (1)-(2) as the sum of two orthogonal components. That is, $\mathbf{X}_r = \mathbf{X}_{r0} + \mathbf{X}_{r1}$ where

$$\mathbf{X}_{r0} = X_{r0}\mathbf{h}_r = \frac{\mathbf{h}_r^T \mathbf{X}_r^T}{\gamma_{r0}} \mathbf{h}_r \tag{4}$$

$$\mathbf{X}_{r1} = X_{r1}\mathbf{u}_r = \frac{\mathbf{u}_r^T \mathbf{X}_r}{\gamma_{r1}} \mathbf{u}_r \tag{5}$$

where $\gamma_{r0} = \| \mathbf{h}_r \|^2$ and $\gamma_{r1} = \| \mathbf{u}_r \|^2$. Thus, we can write (1)-(2) as

$$Y = X_s + \mathbf{h}_r^T \mathbf{X}_{r0} + N \tag{6}$$

$$Z = \sqrt{g_s} X_s + \sqrt{\alpha}\mathbf{h}_r^T \mathbf{X}_{r0} + \mathbf{u}_r^T \mathbf{X}_{r1} + N' \tag{7}$$

Note that X_{r0} and X_{r1} in (4) and (5), respectively, can be arbitrarily correlated. However, in order to obtain closed-form expressions for the power control policy of the strategies proposed below, we will take both X_{r0} and X_{r1} to be independent. We call $\mathbf{X}_{r0}$ the *direct* component of the helper's signal since it is in the same direction as the channel component $\mathbf{h}_r$ from the helper to the destination while we call $\mathbf{X}_{r1}$ the *orthogonal* component of the helper's signal since it is orthogonal to the channel component $\mathbf{h}_r$. We define $\mathbf{Q}_0 \triangleq E\left[\mathbf{X}_{r0}{\mathbf{X}_{r0}}^T\right]$ and $\mathbf{Q}_1 \triangleq E\left[\mathbf{X}_{r1}{\mathbf{X}_{r1}}^T\right]$. We also define $Q_{r0} \triangleq E\left[X_{r0}^2\right]$ and $Q_{r1} \triangleq E\left[X_{r1}^2\right]$. Hence, from (4)-(5), we have $\text{tr}(\mathbf{Q}_0) = \frac{Q_{r0}}{\gamma_{r0}}$ and $\text{tr}(\mathbf{Q}_1) = \frac{Q_{r1}}{\gamma_{r1}}$. Hence, it is easy to see that the second constraint in (3) is equivalent to

$$\frac{Q_{r0}}{\gamma_{r0}} + \frac{Q_{r1}}{\gamma_{r1}} \leq \bar{P}_r \tag{8}$$

Now, we consider the possible signalling $\mathbf{X}_{r0}$ and $\mathbf{X}_{r1}$ across the two orthogonal directions using either one of the two signalling strategies CJ or NF in every direction. Clearly, if the CJ strategy is used for $\mathbf{X}_{r1}$, the eavesdropper is the only one who is possibly harmed by the resulting noise, not the destination. Hence, we assume that the helper will use the orthogonal component $\mathbf{X}_{r1}$ for CJ, i.e., X_{r1} in (5) is a Gaussian random variable with zero mean and variance Q_{r1}. Hence, we distinguish between two possible strategies depending on whether the helper uses the direct component $\mathbf{X}_{r0}$ for CJ or NF. In both strategies, the channel input at the source X_s is a symbol of the codeword that represents the encoded confidential message. Such codeword is drawn from an i.i.d. Gaussian codebook, i.e., X_s is a Gaussian random variable with zero mean and variance P_s where $P_s \leq \bar{P}_s$. Also, in both strategies, the direct component of the channel input at the helper $\mathbf{X}_{r0}$ is given by (4) where X_{r0} is a Gaussian random variable with zero mean and variance Q_{r0}. The difference between the two strategies comes from the origin of X_{r0}. In the CJ strategy, X_{r0} is Gaussian random variable that plays the role of background noise at both the destination and the eavesdropper except for the fact that it is generated artificially. On the other hand, in the NF strategy, X_{r0} is a symbol of a dummy (context-free) codeword drawn from an i.i.d. Gaussian codebook that is assumed to be available at both the destination and the eavesdropper.

If $\mathbf{X}_{r0}$ is used for CJ, the achievable secrecy rate, denoted as R^{CJ}, is given by

$$R^{CJ} = \frac{1}{2}\log\left(\frac{(1+P_s+Q_{r0})\,(1+\alpha Q_{r0}+Q_{r1})}{(1+g_sP_s+\alpha Q_{r0}+Q_{r1})\,(1+Q_{r0})}\right) \quad (9)$$

On the other hand, if $\mathbf{X}_{r0}$ is used for NF, the achievable secrecy rate, denoted as R^{NF}, is given by

$$R^{NF} = \min\left\{\frac{1}{2}\log\left(\frac{(1+P_s)\,(1+\alpha Q_{r0}+Q_{r1})}{1+g_sP_s+\alpha Q_{r0}+Q_{r1}}\right),\right.$$
$$\left.\frac{1}{2}\log\left(\frac{(1+P_s+Q_{r0})\,(1+Q_{r1})}{1+g_sP_s+\alpha Q_{r0}+Q_{r1}}\right)\right\} \quad (10)$$

where, in (9)-(10), P_s, Q_{r0}, and Q_{r1} satisfy the first constraint in (3) and constraint (8). For the sake of comparison, when there is no relay involved, the secrecy capacity of the original GWT channel [18] is given by

$$C^{GWT} = \left(\frac{1}{2}\log\left(\frac{1+\bar{P}_s}{1+g_s\bar{P}_s}\right)\right)^{+} \quad (11)$$

where $(x)^{+} = \max(0, x)$.

III. Maximizing the Secrecy Rates Achievable by Deaf Cooperation

A. The CJ Strategy

We consider the following optimization problem:

$$\max_{P_s, Q_{r0}, Q_{r1}} R^{CJ}(P_s, Q_{r0}, Q_{r1}) \quad (12)$$

$$\text{s.t.} \quad 0 \leq P_s \leq \bar{P}_s, \quad \text{and} \quad 0 \leq \frac{Q_{r0}}{\gamma_{r0}} + \frac{Q_{r1}}{\gamma_{r1}} \leq \bar{P}_r \quad (13)$$

where $R^{CJ}(P_s, Q_{r0}, Q_{r1})$ is given by (9). Note that $\frac{\partial R^{CJ}(P_s,Q_{r0},Q_{r1})}{\partial Q_{r1}} > 0$. Thus, from the second constraint in (13), it is no loss of optimality to set $Q_{r1} = \gamma_{r1}\bar{P}_r - \frac{\gamma_{r1}}{\gamma_{r0}}Q_{r0}$ in (12). Hence, the optimization problem given by (12)-(13) reduces to

$$\max_{P_s, Q_{r0}} R^{CJ}(P_s, Q_{r0}) \triangleq \frac{1}{2}\log\left(\frac{(1+P_s+Q_{r0})(1+\tilde{\alpha}Q_{r0})}{(1+\tilde{g}_sP_s+\tilde{\alpha}Q_{r0})(1+Q_{r0})}\right) \quad (14)$$

$$\text{s.t.} \quad 0 \leq P_s \leq \bar{P}_s, \quad \text{and} \quad 0 \leq Q_{r0} \leq \gamma_{r0}\bar{P}_r \quad (15)$$

where

$$\tilde{\alpha} \triangleq \frac{\alpha - \frac{\gamma_{r1}}{\gamma_{r0}}}{1+\gamma_{r1}\bar{P}_r}, \quad \text{and} \quad \tilde{g}_s \triangleq \frac{g_s}{1+\gamma_{r1}\bar{P}_r} \quad (16)$$

Again, for the sake of comparison, let R_o denote the optimal secrecy rate achievable when no transmission is carried out along the direct component of the channel, i.e., when the transmission is constrained only to the orthogonal component of the channel. Hence, R_o is given by

$$R_o = \left(\frac{1}{2}\log\left(\frac{1+\bar{P}_s}{1+\tilde{g}_s\bar{P}_s}\right)\right)^{+} \quad (17)$$

We note that $\tilde{\alpha}$ could be positive or negative depending on the relative values of γ_{r0} and γ_{r1}. In particular, $\tilde{\alpha} \geq 0$ if and only if $\gamma_{r0} \geq \gamma_{r1}$, i.e., the magnitude of the direct component is greater than that of the orthogonal component.

Let $(\hat{P}_s^{CJ}, \hat{Q}_{r0}^{CJ})$ be the maximizer of (14) subject to (15). In the next theorem, we fully derive the optimal power control policy $(\hat{P}_s^{CJ}, \hat{Q}_{r0}^{CJ})$ for maximizing R^{CJ}.

Theorem 1: The optimal policy $(\hat{P}_s^{CJ}, \hat{Q}_{r0}^{CJ})$ is given as follows:

1) If $\tilde{\alpha} \leq 0$, then: $\hat{P}_s^{CJ} = \bar{P}_s$, if $\tilde{g}_s < 1$. $\hat{P}_s^{CJ} = 0$, if $\tilde{g}_s \geq 1$. $\hat{Q}_{r0}^{CJ} = 0$.
2) If $\tilde{\alpha} > 0$, then we have four possibilities depending on the relative values of $\tilde{\alpha}$ and $\tilde{g}_s$:
   a) If $\tilde{g}_s \geq \max(1, \tilde{\alpha})$, then $\hat{P}_s^{CJ} = 0$ and $\hat{Q}_{r0}^{CJ} = 0$.
   b) If $\tilde{g}_s < 1 \leq \tilde{\alpha}$, then $\hat{P}_s^{CJ} = \bar{P}_s$ and $\hat{Q}_{r0}^{CJ} = \left(\min\left(\bar{P}_r, Q_{r0}^{(1)}\right)\right)^{+}$.
   c) If $1 \leq \tilde{g}_s < \tilde{\alpha}$, then: $\hat{P}_s^{CJ} = 0$ and $\hat{Q}_{r0}^{CJ} = 0$, if $\bar{P}_r \leq \frac{\tilde{g}_s - 1}{\tilde{\alpha} - \tilde{g}_s}$. $\hat{P}_s^{CJ} = \bar{P}_s$ and $\hat{Q}_{r0}^{CJ} = \min\left(\bar{P}_r, Q_{r0}^{(1)}\right)$, if $\bar{P}_r > \frac{\tilde{g}_s - 1}{\tilde{\alpha} - \tilde{g}_s}$.
   d) If $\max(\tilde{g}_s, \tilde{\alpha}) < 1$, then $\hat{P}_s^{CJ} = \bar{P}_s$ and $\hat{Q}_{r0}^{CJ} = 0$.

where

$$Q_{r0}^{(1)} = \frac{\sqrt{\left(\tilde{g}_s\left(\tilde{\alpha} - \tilde{g}_s\right)\bar{P}_s + \tilde{g}_s\left(\tilde{\alpha} - 1\right)\right)\left(\tilde{\alpha} - 1\right)\tilde{\alpha}} - \tilde{\alpha}(1 - \tilde{g}_s)}{\tilde{\alpha}\left(\tilde{\alpha} - \tilde{g}_s\right)} \quad (18)$$

B. The NF Strategy

Here, we consider the following optimization problem

$$\max_{P_s, Q_{r0}, Q_{r1}} R^{NF}(P_s, Q_{r0}, Q_{r1}) \quad (19)$$

$$\text{s.t.} \quad 0 \leq P_s \leq \bar{P}_s, \quad \text{and} \quad 0 \leq \frac{Q_{r0}}{\gamma_{r0}} + \frac{Q_{r1}}{\gamma_{r1}} \leq \bar{P}_r \quad (20)$$

where $R^{NF}(P_s,Q_{r0},Q_{r1})$ is given by (10). For fixed power values P_s,Q_{r0},Q_{r1}, we define

$$R_1^{NF} = \frac{1}{2}\log\left(\frac{(1+P_s)(1+\alpha Q_{r0}+Q_{r1})}{1+g_sP_s+\alpha Q_{r0}+Q_{r1}}\right) \tag{21}$$

$$R_2^{NF} = \frac{1}{2}\log\left(\frac{(1+P_s+Q_{r0})(1+Q_{r1})}{1+g_sP_s+\alpha Q_{r0}+Q_{r1}}\right) \tag{22}$$

Hence,

$$R^{NF}(P_s,Q_{r0},Q_{r1}) = \min\left(R_1^{NF},R_2^{NF}\right) \tag{23}$$

It is easy to see that $\frac{\partial R_1^{NF}}{\partial Q_{r1}} > 0$ and $\frac{\partial R_2^{NF}}{\partial Q_{r1}} > 0$ and thus $\frac{\partial R^{NF}(P_s,Q_{r0},Q_{r1})}{\partial Q_{r1}} > 0$. Hence, from the second constraint in (20), it is no loss of optimality to set $Q_{r1} = \gamma_{r1}\bar{P}_r - \frac{\gamma_{r1}}{\gamma_{r0}}Q_{r0}$ in (19). Hence, the optimization problem given by (19)-(20) reduces to

$$\max_{P_s,Q_{r0}} R^{NF}(P_s,Q_{r0}) \triangleq \min\left(R_1^{NF}(P_s,Q_{r0}),R_2^{NF}(P_s,Q_{r0})\right) \tag{24}$$

$$\text{s.t.} \qquad 0 \le P_s \le \bar{P}_s, \quad \text{and} \quad 0 \le Q_{r0} \le \gamma_{r0}\bar{P}_r \tag{25}$$

where

$$R_1^{NF}(P_s,Q_{r0}) = \frac{1}{2}\log\left(\frac{(1+P_s)(1+\tilde{\alpha}Q_{r0})}{1+\tilde{g}_sP_s+\tilde{\alpha}Q_{r0}}\right) \tag{26}$$

$$R_2^{NF}(P_s,Q_{r0}) = \frac{1}{2}\log\left(\frac{(1+P_s+Q_{r0})(1-\beta Q_{r0})}{1+\tilde{g}_sP_s+\tilde{\alpha}Q_{r0}}\right) \tag{27}$$

where $\tilde{\alpha},\ \tilde{g}_s$ are as defined in (16) above, and

$$\beta \triangleq \frac{\gamma_{r1}}{\gamma_{r0}+\gamma_{r0}\gamma_{r1}\bar{P}_r} \tag{28}$$

As mentioned earlier, $\tilde{\alpha}$ can take a positive or negative value depending on the relative values of the magnitudes of the direct and orthogonal components of the helper-eavesdropper channel. Moreover, we note that the factor $(1-\beta Q_{r0})$ in R_2^{NF} given by (27) appears only when the helper has multiple antennas.

Let $(\hat{P}_s^{NF},\hat{Q}_{r0}^{NF})$ be the maximizer of (24) subject to (25). Before we give the optimal power control policy $(\hat{P}_s^{NF},\hat{Q}_{r0}^{NF})$, we first give the following useful lemmas.

Lemma 1: A necessary condition for the NF strategy to be useful along the direct component of the channel is to have $\tilde{\alpha} \ge 0$ and $\tilde{\alpha}+\beta < 1$.

Proof: First, to show that $\tilde{\alpha} \ge 0$ is necessary, suppose that $\tilde{\alpha} < 0$, one can easily verify that $\frac{\partial R_1^{NF}(P_s,Q_{r0})}{\partial Q_{r0}} \le 0$ for all $Q_{r0} \ge 0$ which implies that achievable rate is upper bounded by $\left(R_1^{NF}(\bar{P}_s,0)\right)^+ = R_o$ which is indeed the secrecy rate achievable when the transmission at the relay is constrained to the orthogonal component of the channel. On the other hand, suppose that $\tilde{\alpha}+\beta > 1$. Now, if $\tilde{g}_s < 1$, then we clearly have $R_2^{NF}(P_s,Q_{r0}) \le \frac{1}{2}\log\left(\frac{1+P_s}{1+\tilde{g}_sP_s}\right) \le \frac{1}{2}\log\left(\frac{1+\bar{P}_s}{1+\tilde{g}_s\bar{P}_s}\right)$ for all $P_s,\ Q_{r0} \ge 0$. If $\tilde{g}_s > 1$, then $R_2^{NF}(P_s,Q_{r0}) \le 0$ for all $P_s,\ Q_{r0} \ge 0$. Thus, we have $R^{NF}(P_s,Q_{r0}) \le R_o$ for all $P_s,\ Q_{r0} \ge 0$. ■

Lemma 2: Let $\phi \triangleq \tilde{g}_s\beta {P_s}^2 + (\tilde{\alpha}+\beta-\tilde{g}_s)P_s - (1-\tilde{\alpha}-\beta)$ and $\psi \triangleq (\tilde{\alpha}+\beta-\tilde{g}_s)^2 - 4\tilde{g}_s\beta\left(\tilde{\alpha}+\beta-1\right)$. If the conditions of Lemma 1 hold, i.e., if

$$\tilde{\alpha} \ge 0,\ \tilde{\alpha}+\beta < 1 \tag{29}$$

then, for any fixed P_s where

$$0 \le P_s \le P_s^* \triangleq \frac{\sqrt{\psi}-(\tilde{\alpha}+\beta-\tilde{g}_s)}{2\tilde{g}_s\beta}, \tag{30}$$

we have $\frac{\partial R_2^{NF}(P_s,Q_{r0})}{\partial Q_{r0}} \ge 0$ if and only if

$$0 \le Q_{r0} \le Q_{r0}^*(P_s) \triangleq \frac{\sqrt{\beta^2(1+\tilde{g}_sP_s)^2-\tilde{\alpha}\beta\phi}-\beta(1+\tilde{g}_sP_s)}{\tilde{\alpha}\beta} \tag{31}$$

Consequently, if conditions (29)-(30) hold, then

$$R_2^{NF}(P_s,Q_{r0}) \le R_2^{NF}\left(P_s,Q_{r0}^*(P_s)\right) \tag{32}$$

Proof: Define $f_2^{NF}(P_s,Q_{r0})$ as the numerator of $\frac{\partial R_2^{NF}(P_s,Q_{r0})}{\partial Q_{r0}}$. Note that the sign of $\frac{\partial R_2^{NF}(P_s,Q_{r0})}{\partial Q_{r0}}$ is the same as the sign of $f_2^{NF}(P_s,Q_{r0})$ for all $P_s,Q_{r0} \ge 0$. It is easy to verify that $f_2^{NF}(P_s,Q_{r0})$ is given by

$$f_2^{NF}(P_s,Q_{r0}) = -\tilde{\alpha}\beta {Q_{r0}}^2 - 2\beta(1+\tilde{g}_sP_s)Q_{r0} - \phi \tag{33}$$

Fix P_s and let $q_1(P_s),q_2(P_s)$ denote the two roots of $f_2^{NF}(P_s,Q_{r0})$. Since $\tilde{\alpha} \ge 0$, then $\frac{\partial R_2^{NF}(P_s,Q_{r0})}{\partial Q_{r0}} \ge 0$ if and only if $Q_{r0} \in [q_1(P_s),q_2(P_s)]$. However, it is not hard to see that $q_1(P_s) < 0$ for any $P_s > 0$. Thus, for any $P_s,Q_{r0} \ge 0$, we have $\frac{\partial R_2^{NF}(P_s,Q_{r0})}{\partial Q_{r0}} \ge 0$ if and only if $Q_{r0} \in [0,q_2(P_s)]$ where $q_2(P_s) = Q_{r0}^*(P_s)$ where Q_{r0}^* is given in (31). Thus, it remains to show that $Q_{r0}^*(P_s) \ge 0$ (and hence $[0,Q_{r0}^*(P_s)]$ is not empty) whenever $0 \le P_s \le P_s^*$ where P_s^* is given in (30). We note that $Q_{r0}^*(P_s) \ge 0$ if and only if $\phi \le 0$. Since ϕ is quadratic in P_s, it is not hard to see that $\phi \le 0$ whenever P_s lies between the two roots of ϕ. However, one of the roots is negative and the other is positive due to the fact that $\tilde{\alpha}+\beta < 1$. Indeed, the positive root is P_s^*. Hence, $\phi < 0$ and consequently $Q_{r0}^*(P_s) > 0$ whenever $0 \le P_s \le P_s^*$. ■

In the next theorem, we fully derive the optimal power policy $(\hat{P}_s^{NF},\hat{Q}_{r0}^{NF})$ for maximizing R^{NF}.

Theorem 2: Let $\tilde{Q}_{r0}$ be the value of Q_{r0} such that $R_1^{NF}(\bar{P}_s,Q_{r0}) = R_2^{NF}(\bar{P}_s,Q_{r0})$, i.e.,

$$\tilde{Q}_{r0} = \left(\frac{1-(\tilde{\alpha}+\beta)\left(1+\bar{P}_s\right)}{\beta}\right)^+ \tag{34}$$

Let Q_{r0}^* be as defined in (31). The optimal policy $(\hat{P}_s^{NF},\hat{Q}_{r0}^{NF})$ is given as follows:

1) If $\tilde{\alpha} \le 0$, then: $\hat{P}_s^{NF} = \bar{P}_s$, if $\tilde{g}_s < 1$. $\hat{P}_s^{NF} = 0$, if $\tilde{g}_s \ge 1$. $\hat{Q}_{r0}^{NF} = 0$.
2) If $\tilde{\alpha} > 0$: We have the following four possibilities depending on the values of $\tilde{\alpha},\tilde{g}_s$, and β:
   a) If $\tilde{\alpha}+\beta \ge 1$, then: $\hat{P}_s^{NF} = \bar{P}_s$, if $\tilde{g}_s < 1$. $\hat{P}_s^{NF} = 0$, if $\tilde{g}_s \ge 1$. $\hat{Q}_{r0}^{NF} = 0$.

b) If $\tilde{g}_s \leq \tilde{\alpha} < 1-\beta$, then: $\hat{P}_s^{NF} = \bar{P}_s$. $\hat{Q}_{r0}^{NF} = \min\left(\gamma_{r0}\bar{P}_r,\ \max\left(\tilde{Q}_{r0},\ Q_{r0}^{*}\left(\bar{P}_s\right)\right)\right)$, if $\bar{P}_s \leq P_s^{*}$. $\hat{Q}_{r0}^{NF} = 0$, if $\bar{P}_s > P_s^{*}$.

c) If $\tilde{\alpha} < \min\left(1-\beta,\ \tilde{g}_s\right) < 1$, then:

i) If $\gamma_{r0}\bar{P}_r \leq \frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}$, then: $\hat{P}_s^{NF} = \bar{P}_s$. $\hat{Q}_{r0}^{NF} = \min\left(\gamma_{r0}\bar{P}_r,\ \max\left(\tilde{Q}_{r0},\ Q_{r0}^{*}\left(\bar{P}_s\right)\right)\right)$, if $\bar{P}_s \leq P_s^{*}$. $\hat{Q}_{r0}^{NF} = 0$, if $\bar{P}_s > P_s^{*}$.

ii) If $\gamma_{r0}\bar{P}_r > \frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}$, $\left[\frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}, \gamma_{r0}\bar{P}_r\right] \cap \left[\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta}, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right] \neq \emptyset$, then: $(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF}) = ({P_s}^{(a)}, {Q_{r0}}^{(a)})$, if $R^{NF}\left({P_s}^{(a)}, {Q_{r0}}^{(a)}\right) \geq R^{NF}\left({P_s}^{(b)}, {Q_{r0}}^{(b)}\right)$. $(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF}) = ({P_s}^{(b)}, {Q_{r0}}^{(b)})$, if $R^{NF}\left({P_s}^{(a)}, {Q_{r0}}^{(a)}\right) < R^{NF}\left({P_s}^{(b)}, {Q_{r0}}^{(b)}\right)$, where ${P_s}^{(a)}, {Q_{r0}}^{(a)}$ are the optimal values $\hat{P}_s^{NF}$, $\hat{Q}_{r0}^{NF}$, respectively, of case 2(c-i) above, whereas ${P_s}^{(b)} = \frac{1-\beta {Q_{r0}}^{(b)}}{\tilde{\alpha}+\beta} - 1$. ${Q_{r0}}^{(b)} = \min\left(Q_{r0}^{(2)}, \gamma_{r0}\bar{P}_r, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right)$, where $Q_{r0}^{(2)} =$

$$\frac{\tilde{g}_s\left(1-(\tilde{\alpha}+\beta)+\sqrt{\tilde{\alpha}\beta}-\sqrt{(\tilde{\alpha}+\beta)\left((\tilde{\alpha}+\beta)-\tilde{g}_s\beta\right)\tilde{g}_s\left(1-\tilde{\alpha}\right)}\right)}{\sqrt{\tilde{\alpha}\beta}\left(\tilde{g}_s\beta-\tilde{\alpha}\left(\tilde{\alpha}+\beta\right)\right)} \tag{35}$$

iii) If $\gamma_{r0}\bar{P}_r > \frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}} > \frac{1-(\tilde{\alpha}+\beta)}{\beta}$, then: $\hat{P}_s^{NF} = \bar{P}_s$. $\hat{Q}_{r0}^{NF} = \min\left(\frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}},\ \max\left(\tilde{Q}_{r0},\ Q_{r0}^{*}\left(\bar{P}_s\right)\right)\right)$, if $\bar{P}_s \leq P_s^{*}$. $\hat{Q}_{r0}^{NF} = 0$, if $\bar{P}_s > P_s^{*}$.

iv) If $\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta} > \gamma_{r0}\bar{P}_r > \frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}$, then $\hat{P}_s^{NF} = \bar{P}_s$ and $\hat{Q}_{r0}^{NF} = \gamma_{r0}\bar{P}_r$.

d) If $\tilde{\alpha} < 1-\beta \leq 1 \leq \tilde{g}_s$, then:

i) If $\gamma_{r0}\bar{P}_r \leq \frac{\tilde{g}_s-1}{\tilde{\alpha}}$, then $\hat{P}_s^{NF} = \hat{Q}_{r0}^{NF} = 0$.

ii) If $\gamma_{r0}\bar{P}_r > \frac{\tilde{g}_s-1}{\tilde{\alpha}}$, $\left[\frac{\tilde{g}_s-1}{\tilde{\alpha}}, \gamma_{r0}\bar{P}_r\right] \cap \left[\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta}, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right] \neq \emptyset$, then $\hat{P}_s^{NF} = \frac{1-\beta\hat{Q}_{r0}^{NF}}{\tilde{\alpha}+\beta} - 1$ and $\hat{Q}_{r0}^{NF} = \min\left(Q_{r0}^{(2)}, \gamma_{r0}\bar{P}_r, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right)$, where $Q_{r0}^{(2)}$ is given by (35).

iii) If $\gamma_{r0}\bar{P}_r > \frac{\tilde{g}_s-1}{\tilde{\alpha}} > \frac{1-(\tilde{\alpha}+\beta)}{\beta}$, then $\hat{P}_s^{NF} = \hat{Q}_{r0}^{NF} = 0$.

iv) If $\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta} > \gamma_{r0}\bar{P}_r > \frac{\tilde{g}_s-1}{\tilde{\alpha}}$, then $\hat{P}_s^{NF} = \bar{P}_s$ and $\hat{Q}_{r0}^{NF} = \gamma_{r0}\bar{P}_r$.

C. CJ versus NF

In the next corollary, we use the results of the above two theorems to compare the two strategies. In particular, we show in terms of the parameters of the deaf cooperation model when it is better to use CJ than NF for transmission along the direct component $\mathbf{X}_{r0}$ and vice versa. We also give the conditions for which both CJ and NF along the direct component are useless.

Corollary 1: Let $\tilde{\alpha}$, $\tilde{g}_s$, and β be as defined in (16) and (28), respectively. For the CJ along the direct channel component to be useful, it is necessary to have $\tilde{\alpha} > \max(1, \tilde{g}_s)$. Whereas, for the NF along the direct channel component to be useful, it is necessary to have $0 < \tilde{\alpha} < 1-\beta$. In other words,

$$\text{If} \quad R^{CJ}\left(\hat{P}_s^{CJ}, \hat{Q}_{r0}^{CJ}\right) > R_o \quad \text{then} \quad \tilde{\alpha} > \max(1, \tilde{g}_s) \tag{36}$$

$$\text{If} \quad R^{NF}\left(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF}\right) > R_o \quad \text{then} \quad 0 < \tilde{\alpha} < 1-\beta \tag{37}$$

Hence, if

$$\tilde{\alpha} \in \left[1-\beta, \max(1, \tilde{g}_s)\right] \cup \left(-\infty, 0\right], \tag{38}$$

neither CJ nor NF along the direct component is useful, i.e., $\hat{Q}_{r0}^{CJ} = \hat{Q}_{r0}^{NF} = 0$. Moreover, if, in addition to (38), $\tilde{g}_s < 1$, then $\hat{P}_s^{CJ} = \hat{P}_s^{NF} = \bar{P}_s$ and $\hat{Q}_{r1} = \gamma_{r1}\bar{P}_r$, i.e., the optimal power strategy at the relay in this case is to jam with full power along the orthogonal component and transmit nothing along the direct component. Whereas, if, in addition to (38), $\tilde{g}_s \geq 1$, then $\hat{P}_s^{CJ} = \hat{P}_s^{NF} = \hat{Q}_{r1} = 0$, i.e., no transmission occurs at all and hence the achievable secrecy rate is zero in this case.

IV. Numerical Results

First, consider the system described in Section II. We compare the optimal secrecy rates R^{CJ} and R^{NF} achievable by our CJ and NF strategies proposed in Section III with the optimal secrecy rate R_o achievable by the strategy that uses only the orthogonal component of the channel for CJ. We also compare these rates to the secrecy capacity C^{GWT} of the original Gaussian wiretap channel with no relay. In Figure 1, we set $\bar{P}_s = 5$, $\bar{P}_r = 2$, $g_s = 0.85$, $\gamma_{r0} = 2$, and $\gamma_{r1} = 1$. We plot R^{CJ}, R^{NF}, R_o, and C^{GWT} versus $\sqrt{\alpha}$, $0 \leq \sqrt{\alpha} \leq 4$, where, as in Section II, $\sqrt{\alpha}$ is defined as $\frac{\mathbf{g}_r^T \mathbf{h}_r}{\gamma_{r0}}$. It is clear from Figure 1 that the necessary conditions given in Corollary 1 for $R^{CJ} > R_o$ and $R^{NF} > R_o$ are satisfied here. Note that the necessary condition in Corollary 1 for $R^{CJ} > R_o$ is equivalent to $\alpha > \frac{\gamma_{r1}}{\gamma_{r0}} + \max(g_s, 1+\gamma_{r1}\bar{P}_r)$, i.e., $\alpha > 3.5$ (or equivalently, $\alpha > 1.871$). Note also that the necessary condition in Corollary 1 for $R^{NF} > R_o$ is equivalent to $\frac{\gamma_{r1}}{\gamma_{r0}} < \alpha < 1 + \gamma_{r1}\bar{P}_r$, i.e., $0.5 < \alpha < 3$ (or equivalently, $0.707 < \alpha < 1.732$). It is clear that, in general, our CJ and NF strategy yield greater secrecy rates than R_o and C^{GWT}.

Next, we consider the case where the relay is constrained to using only one of the two modes (CJ or NF) over all the channel components, i.e., the relay cannot split its power between CJ and NF. We denote the optimal secrecy rate (with power control) achievable in this case by either R^{SM-CJ} or R^{SM-NF} depending on the single mode of deaf cooperation that the relay is using. It is clear that $R^{SM-CJ} = R^{CJ}$ where R^{CJ} is the optimal secrecy rate achieved by our CJ strategy since in this strategy the relay jams over the two orthogonal components of the channel and hence it is indeed a single-mode strategy. However, in our NF strategy the relay

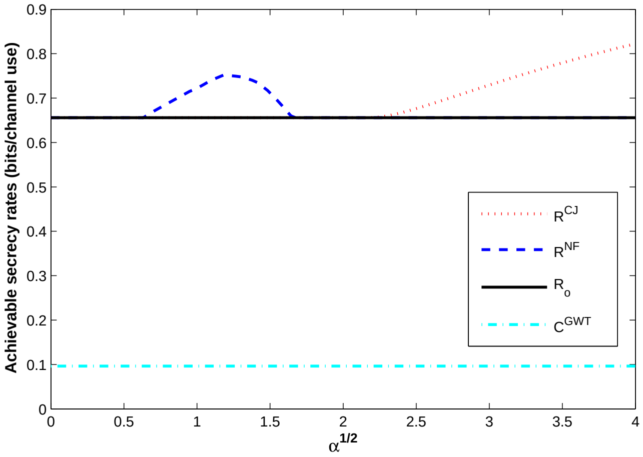

Fig. 1. The optimal achievable secrecy rates by the our CJ and NF strategies, R^{CJ} and R^{NF}, the optimal achievable secrecy rate with no transmission along the direct channel component, R_o, and the secrecy capacity of the original Gaussian wiretap channel, C^{GWT}, as functions of $\sqrt{\alpha}$ where, as in Section II, $\sqrt{\alpha}$ is defined as $\frac{\mathbf{g}_r^T \mathbf{h}_r}{\gamma_{r0}}$.

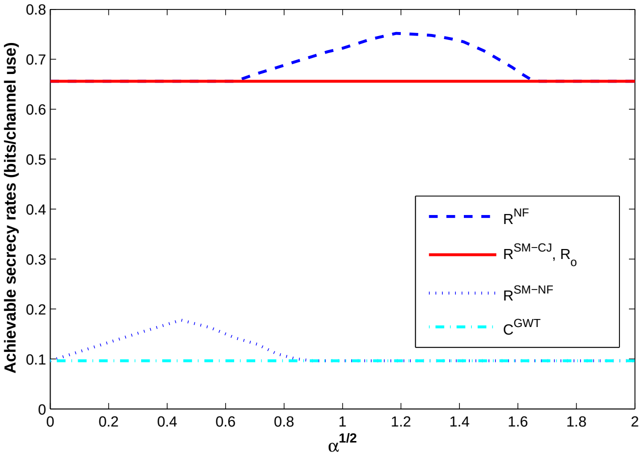

Fig. 2. The optimal achievable secrecy rate by our NF strategy, R^{NF}, the optimal achievable secrecy rate by the single-mode CJ strategy, R^{SM-CJ}, the optimal achievable secrecy rate by the single-mode NF strategy, R^{SM-NF}, and the secrecy capacity of the original Gaussian wiretap channel, C^{GWT}, as functions of $\sqrt{\alpha}$.

uses the orthogonal component for CJ whereas it uses the direct component for NF. Therefore, intuitively, we must have $R^{NF} > R^{SM-NF}$ in general. To illustrate this, in Figure 2, we plot R^{NF}, R^{SM-CJ}, R^{NF-SM}, and C^{GWT} versus $\sqrt{\alpha}$, $0 \leq \sqrt{\alpha} \leq 2$. The values of $\bar{P}_s$, $\bar{P}_r$, g_s, γ_{r0}, and γ_{r1} are fixed and chosen as in the previous example.

V. Conclusions

In this paper, we extended the idea of deaf cooperation to the multi-antenna deaf helper model. We showed that the multiple spatial dimensions available in this model can be exploited in the deaf cooperation paradigm by possibly decomposing the relay-eavesdropper channel into two components, a direct component in the direction of the relay-destination channel and an orthogonal component that is orthogonal to the relay-destination channel. We proposed two strategies for deaf cooperation in this model. In one strategy, the direct component is used by the relay to perform NF whereas in the other strategy, it is used for CJ. In both strategies, the orthogonal component is used for CJ. Under the assumption of independent signaling along each component, we derived the optimal power allocation for each strategy. We also found the necessary conditions for each strategy to be useful, i.e., to achieve secrecy rate higher than the secrecy capacity of the original Gaussian wiretap channel and showed that both strategies cannot be useful at the same time.

References

[1] R. Negi and S. Goel. Secret communication using artificial noise. In *IEEE Vehicular Technology Conference*, Sep. 2005.

[2] E. Tekin and A. Yener. Achievable rates for the general Gaussian multiple access wiretap channel with collective secrecy. In *44th Annual Allerton Conference on Communication, Control and Computing, Monticello, IL*, Sep. 2006.

[3] E. Tekin and A. Yener. The Gaussian multiple access wiretap channel. *IEEE Trans. on Inf. Theory*, 54(12):5747–5755, Dec. 2008.

[4] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. on Inf. Theory*, 54(6):2735–2751, Jun. 2008.

[5] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Interference-assisted secret communication. In *IEEE Information Theory Workshop*, May 2008.

[6] L. Lai, H. El Gamal, and H. V. Poor. The wiretap channel with feedback: Encryption over the channel. *IEEE Trans. on Inf. Theory*, 54(11):5059–5067, Nov. 2008.

[7] I. Krikidis, J. Thompson, and S. McLaughlin. Relay selection for secure cooperative networks with jamming. *IEEE Trans. on Wireless Comm.*, 8(10):5003–5011, Oct. 2009.

[8] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao. Joint relay and jammer selection for secure two-way relay networks. In *IEEE ICC 2011, Kyoto, Japan*, Jun. 2011.

[9] S. Vasudevan, S. Adams, D. Goeckel, Z. Ding, D. Towsley, and K. K. Leung. Secrecy in wireless relay channels through cooperative jamming. In *ACITA 2010*, Sep. 2010. Also available at: http://www.eecs.berkeley.edu/∼shadams/docs/SecrecyInWirelessRelayChannels.pdf.

[10] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin. Friendly jamming for wireless secrecy. In *IEEE ICC 2010, Capetown, South Africa*, May 2010.

[11] J. P. Vilela, P. C. Pinto, and J. Barros. Jammer selection policies for secure wireless networks. In *IEEE ICC 2011, Kyoto, Japan*, Jun. 2011.

[12] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor. Cooperative jamming for wireless physical layer security. In *15th IEEE Workshop on Statistical Signal Processing*, pages 417–420, Sep. 2009.

[13] J. Huang and A. L. Swindlehurst. Cooperation strategies for secrecy in mimo relay networks with unknown eavesdropper csi. In *ICASSP 2011, Prague, Czech Republic*, pages 3424–3427, May 2011.

[14] J. Huang and A. L. Swindlehurst. Secure communications via cooperative jamming in two-hop relay systems. In *IEEE GLOBECOM 2010, Miami, FL.*, Dec. 2010.

[15] L. Lai and H. El Gamal. Cooperation for secrecy: The relay-eavesdropper channel. *IEEE Trans. on Inf. Theory*, 54(9):4005–4019, Sep. 2008.

[16] L. Lai and H. El Gamal. Cooperation for secure communication: The relay wiretap channel. In *ICASSP 2007, Honolulu, HI*, pages III 149 – III 152, April 2007.

[17] R. Bassily and S. Ulukus. Deaf cooperation for secrecy in mutiple-relay networks. In *IEEE Globecom, Houston, TX*, Dec. 2011.

[18] S. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wire-tap channel. *IEEE Trans. on Inf. Theory*, 24(4):451–456, Jul. 1978.