Deaf Cooperation for Secrecy With Multiple Antennas at the Helper

Raef Bassily, *Member, IEEE*, and Sennur Ulukus, *Member, IEEE*

***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. Finally, we consider the reversely degraded multiple antenna relay-eavesdropper channel. We show that a simple strategy in which the relay jams with full power along the orthogonal component and transmits nothing in the direct component achieves a secrecy rate that approaches the secrecy capacity of this channel as the relay's average power goes to infinity. Moreover, we show that this result holds almost surely even if the relay-eavesdropper's channel state information is unavailable.**

***Index Terms*—Channel decomposition, cooperative jamming, information theoretic secrecy, multiple antennas, noise forwarding, relay-eavesdropper channel, reversely degraded channel, secrecy rates.**

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]–[4]. In [2]–[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]–[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 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, [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].

Manuscript received March 03, 2012; revised July 25, 2012; accepted August 13, 2012. Date of publication August 27, 2012; date of current version November 15, 2012. This work was supported by the NSF under Gant CCF 07-29127, Gant CNS 09-64632, Gant CCF 09-64645, Gant CCF 10-18185, and Gant CNS 11-47811. This paper was presented in part at the Conference on Information Sciences and Systems (CISS), Princeton, NJ, March 2012. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Wade Trappe.

R. Bassily was with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA. He is now with the Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA 16802 USA.

S. Ulukus is with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: ulukus@umd.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2012.2215325

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 were 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 particular, it was shown in [17], that depending on the relative location of a helping node with respect to the destination and the eavesdropper, a helping node may either be a useful jammer or a useful noise forwarder but not both at the same time. In addition, the same reference gives the optimal power allocation 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.

Next, we turn our attention to a certain class of the multiple antenna relay-eavesdropper channels, namely, the reversely degraded channel. We show that the strategy in which the relay jams with full power along the orthogonal component of the channel and transmits nothing in the direct component is optimal when the relay's average power goes to infinity. In fact, we even prove a stronger result. The secrecy rate achieved by this strategy approaches the capacity of the reversely degraded multiple antenna relay channel as the relay's average power increases, and hence this strategy achieves the optimal secure degrees of freedom (DoF) of the reversely degraded multiple antenna relay-eavesdropper channel. Interestingly, this strategy is clearly suboptimal in general for a bounded relay's power. Moreover, we show that this result is valid with probability 1 even when the relay-eavesdropper's channel state information is unavailable.

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 improving the secrecy capacity of the GWT by transmitting interfering signals that are independent of the source message. 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 output symbols Y and Z of the GWT channel, with a multiantenna deaf helper, at the destination and the eavesdropper, respectively, 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:

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

We may write $\mathbf{g}_r$ as the direct sum $\mathbf{g}_r = \sqrt{\alpha}\mathbf{h}_r + \mathbf{u}_r$ where $\mathbf{h}_r^T \mathbf{u}_r = 0$, i.e., we decompose $\mathbf{g}_r$ into two orthogonal components: $\sqrt{\alpha}\mathbf{h}_r$ (in the direction of the legitimate channel $\mathbf{h}_r$) and $\mathbf{u}_r$ (orthogonal to $\mathbf{h}_r$). Hence, one can write $\mathbf{X}_r$ in (1)–(2) as the sum of two orthogonal components: $\mathbf{X}_{r0}$ (in the direction of $\mathbf{h}_r$) and $\mathbf{X}_{r1}$ (in the direction of $\mathbf{u}_r$). That is, $\mathbf{X}_r = \mathbf{X}_{r0} + \mathbf{X}_{r1}$ where

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

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

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

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

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

Clearly, X_{r0} and X_{r1}, in (4) and (5), are the scaled projections of $\mathbf{X}_r$ in the direction of $\mathbf{h}_r$ and $\mathbf{u}_r$, respectively. Note that X_{r0} and X_{r1} 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 $\mathrm{tr}(\mathbf{Q}_0) = \frac{Q_{r0}}{\gamma_{r0}}$ and $\mathrm{tr}(\mathbf{Q}_1) = \frac{Q_{r1}}{\gamma_{r1}}$. 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 [4], [5], denoted as R^{CJ}, is given by

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

On the other hand, if $\mathbf{X}_{r0}$ is used for NF, the achievable secrecy rate [15], denoted as R^{NF}, is given by

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

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

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

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

III. Maximizing the Secrecy Rates Achievable by Deaf Cooperation

A. The CJ Strategy

We consider the following optimization problem:

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

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

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

$$Q_{r1} = \gamma_{r1}\bar{P}_r - \frac{\gamma_{r1}}{\gamma_{r0}}Q_{r0} \tag{14}$$

in (12). Hence, the optimization problem given by (12)–(13) reduces to

$$\max_{P_s, Q_{r0}} \quad R^{CJ}(P_s, Q_{r0}) \triangleq \frac{1}{2}\log\left(\frac{(1+P_s+Q_{r0})(1+\tilde{\alpha}Q_{r0})}{(1+\tilde{g}_sP_s+\tilde{\alpha}Q_{r0})(1+Q_{r0})}\right) \tag{15}$$

$$\text{s.t.} \quad 0 \leq P_s \leq \bar{P}_s, \quad \text{and} \quad 0 \leq Q_{r0} \leq \gamma_{r0}\bar{P}_r \tag{16}$$

where

$$\tilde{\alpha} \triangleq \frac{\alpha - \frac{\gamma_{r1}}{\gamma_{r0}}}{1+\gamma_{r1}\bar{P}_r}, \quad \text{and} \quad \tilde{g}_s \triangleq \frac{g_s}{1+\gamma_{r1}\bar{P}_r}. \tag{17}$$

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

$$R_o = \left(\frac{1}{2}\log\left(\frac{1+\bar{P}_s}{1+\tilde{g}_s\bar{P}_s}\right)\right)^+. \tag{18}$$

Note that the optimization problem (15)–(16) may look similar to the one considered in [17] for the single-antenna case. However, a notable difference is 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 (15) subject to (16). Note that, once $\hat{Q}_{r0}^{CJ}$ is derived, the optimal value of Q_{r1}, denoted as $\hat{Q}_{r1}^{CJ}$, can be easily found from (14) where Q_{r0} is set to $\hat{Q}_{r0}^{CJ}$. The optimal covariance matrices $\hat{\mathbf{Q}}_{r0}^{CJ}$ and $\hat{\mathbf{Q}}_{r1}^{CJ}$ are given by $\hat{Q}_{r0}^{CJ} \frac{\mathbf{h}_r \mathbf{h}_r^T}{{\gamma_{r0}}^2}$ and $\hat{Q}_{r1}^{CJ} \frac{\mathbf{u}_r \mathbf{u}_r^T}{{\gamma_{r1}}^2}$. 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

$$Q_{r0}^{(1)} = \frac{\sqrt{\left(\tilde{g}_s\left(\tilde{\alpha} - \tilde{g}_s\right)\bar{P}_s + \tilde{g}_s\left(\tilde{\alpha} - 1\right)\right)\left(\tilde{\alpha} - 1\right)\tilde{\alpha}} - \tilde{\alpha}(1 - \tilde{g}_s)}{\tilde{\alpha}\left(\tilde{\alpha} - \tilde{g}_s\right)}. \tag{19}$$

Proof: First, observe that $\frac{\partial R^{CJ}(P_s, Q_{r0})}{\partial Q_{r0}}$ is given by

$$\frac{\partial R^{CJ}(P_s, Q_{r0})}{\partial Q_{r0}} = \frac{\tilde{\alpha}(\tilde{g}_s - \tilde{\alpha}){Q_{r0}}^2 + 2Q_{r0}(\tilde{g}_s - 1)\tilde{\alpha} + \tilde{g}_s(\tilde{\alpha} - 1)P_s + \tilde{g}_s\tilde{\alpha} - 1}{(1 + Q_{r0})(1 + \tilde{g}_s P_s + \tilde{\alpha} Q_{r0})(1 + P_s + Q_{r0})(1 + \tilde{\alpha} Q_{r0})} P_s. \tag{20}$$

It is easy to see that if $\tilde{\alpha} \leq 0$, then $\frac{\partial R^{CJ}(P_s, Q_{r0})}{\partial Q_{r0}} < 0 \; \forall P_s, Q_{r0}$. Hence, $\hat{Q}_{r0}^{CJ} = 0$ and case 1 follows. On the other hand, case 2 of this theorem is exactly the same as the case of single antenna relay given by Theorem 2 in [17]. ∎

Theorem 1 tells us that CJ along the direct component can be useful only when the magnitude of the direct component of $\mathbf{g}_r$ is larger than that of the orthogonal component, i.e., when $\tilde{\alpha} > 0$. Otherwise, the optimal power allocation strategy at the multiple antenna deaf helper would be to jam only along the orthogonal component and transmit nothing along the direct component.

B. The NF Strategy

Here, we consider the following optimization problem

$$\max_{P_s, Q_{r0}, Q_{r1}} \quad R^{NF}(P_s, Q_{r0}, Q_{r1}) \tag{21}$$

$$\text{s.t.} \quad 0 \leq P_s \leq \bar{P}_s, \quad \text{and} \quad 0 \leq \frac{Q_{r0}}{\gamma_{r0}} + \frac{Q_{r1}}{\gamma_{r1}} \leq \bar{P}_r \tag{22}$$

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

$$R_1^{NF} = \frac{1}{2}\log\left(\frac{(1 + P_s)(1 + \alpha Q_{r0} + Q_{r1})}{1 + g_s P_s + \alpha Q_{r0} + Q_{r1}}\right) \tag{23}$$

$$R_2^{NF} = \frac{1}{2}\log\left(\frac{(1 + P_s + Q_{r0})(1 + Q_{r1})}{1 + g_s P_s + \alpha Q_{r0} + Q_{r1}}\right). \tag{24}$$

Hence,

$$R^{NF}(P_s, Q_{r0}, Q_{r1}) = \min\left(R_1^{NF}, R_2^{NF}\right). \tag{25}$$

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 (22), it is no loss of optimality to set $Q_{r1} = \gamma_{r1}\bar{P}_r - \frac{\gamma_{r1}}{\gamma_{r0}} Q_{r0}$ in (21). Hence, the optimization problem given by (21)–(22) reduces to

$$\max_{P_s, Q_{r0}} \quad R^{NF}(P_s, Q_{r0}) \triangleq \min\left(R_1^{NF}(P_s, Q_{r0}), R_2^{NF}(P_s, Q_{r0})\right) \tag{26}$$

$$\text{s.t.} \quad 0 \leq P_s \leq \bar{P}_s, \quad \text{and} \quad 0 \leq Q_{r0} \leq \gamma_{r0}\bar{P}_r \tag{27}$$

where

$$R_1^{NF}(P_s, Q_{r0}) = \frac{1}{2}\log\left(\frac{(1 + P_s)(1 + \tilde{\alpha} Q_{r0})}{1 + \tilde{g}_s P_s + \tilde{\alpha} Q_{r0}}\right) \tag{28}$$

$$R_2^{NF}(P_s, Q_{r0}) = \frac{1}{2}\log\left(\frac{(1 + P_s + Q_{r0})(1 - \beta Q_{r0})}{1 + \tilde{g}_s P_s + \tilde{\alpha} Q_{r0}}\right) \tag{29}$$

where $\tilde{\alpha}$, $\tilde{g}_s$ are as defined in (17) above, and

$$\beta \triangleq \frac{\gamma_{r1}}{\gamma_{r0} + \gamma_{r0}\gamma_{r1}\bar{P}_r}. \tag{30}$$

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 (29) appears only when the helper has multiple antennas.

Let $(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF})$ be the maximizer of (26) subject to (27). As discussed above, once $\hat{Q}_{r0}^{NF}$ is derived, the optimal value of Q_{r1}, denoted as $\hat{Q}_{r1}^{NF}$, can be easily found from (14) where Q_{r0} is set to $\hat{Q}_{r0}^{NF}$. The optimal covariance matrices $\hat{\mathbf{Q}}_{r0}^{NF}$ and $\hat{\mathbf{Q}}_{r1}^{NF}$ are given by $\hat{Q}_{r0}^{NF} \frac{\mathbf{h}_r \mathbf{h}_r^T}{{\gamma_{r0}}^2}$ and $\hat{Q}_{r1}^{NF} \frac{\mathbf{u}_r \mathbf{u}_r^T}{{\gamma_{r1}}^2}$, respectively. 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 $\tilde{\alpha} \geq 0$ and $\tilde{\alpha} + \beta < 1$.

Proof: First, to show that $\tilde{\alpha} \geq 0$ is necessary, suppose that $\tilde{\alpha} < 0$, one can easily verify that $\frac{\partial R_1^{NF}(P_s, Q_{r0})}{\partial Q_{r0}} \leq 0$ for all $Q_{r0} \geq 0$ 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 $R_2^{NF}(P_s,Q_{r0}) \leq \frac{1}{2}\log\left(\frac{1+P_s}{1+\tilde{g}_sP_s}\right) \leq \frac{1}{2}\log\left(\frac{1+\bar{P}_s}{1+\tilde{g}_s\bar{P}_s}\right)$ for all $P_s,\ Q_{r0}\geq 0$. If $\tilde{g}_s>1$, then $R_2^{NF}(P_s,Q_{r0})\leq 0$ for all $P_s,\ Q_{r0}\geq 0$. Thus, we have $R^{NF}(P_s,Q_{r0})\leq R_o$ for all $P_s,\ Q_{r0}\geq 0$. ∎

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

$$\tilde{\alpha}\geq 0,\ \tilde{\alpha}+\beta<1 \tag{31}$$

then, for any fixed P_s where

$$0\leq P_s\leq P_s^* \triangleq \frac{\sqrt{\psi}-(\tilde{\alpha}+\beta-\tilde{g}_s)}{2\tilde{g}_s\beta}, \tag{32}$$

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

$$\begin{aligned}0\leq Q_{r0}&\leq Q_{r0}^*(P_s)\\ &\triangleq \frac{\sqrt{\beta^2(1+\tilde{g}_sP_s)^2-\tilde{\alpha}\beta\phi}-\beta(1+\tilde{g}_sP_s)}{\tilde{\alpha}\beta}.\end{aligned} \tag{33}$$

Consequently, if conditions (31)–(32) hold, then

$$R_2^{NF}(P_s,Q_{r0})\leq R_2^{NF}\left(P_s,Q_{r0}^*(P_s)\right). \tag{34}$$

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 $P_s,Q_{r0}\geq 0$. It is easy to verify that $f_2^{NF}(P_s,Q_{r0})$ is given by

$$f_2^{NF}(P_s,Q_{r0})=-\tilde{\alpha}\beta {Q_{r0}}^2-2\beta(1+\tilde{g}_sP_s)Q_{r0}-\phi. \tag{35}$$

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 $\tilde{\alpha}\geq 0$, then $\frac{\partial R_2^{NF}(P_s,Q_{r0})}{\partial Q_{r0}}\geq 0$ 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 $P_s,Q_{r0}\geq 0$, we have $\frac{\partial R_2^{NF}(P_s,Q_{r0})}{\partial Q_{r0}}\geq 0$ 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 (33). Thus, it remains to show that $Q_{r0}^*(P_s)\geq 0$ (and hence $[0,Q_{r0}^*(P_s)]$ is not empty) whenever $0\leq P_s\leq P_s^*$ where P_s^* is given in (32). We note that $Q_{r0}^*(P_s)\geq 0$ if and only if $\phi\leq 0$. Since ϕ is quadratic in P_s, it is not hard to see that $\phi\leq 0$ 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 $0\leq P_s\leq P_s^*$. ∎

In the next theorem, we fully derive the optimal power policy $(\hat{P}_s^{NF},\hat{Q}_{r0}^{NF})$ for maximizing R^{NF}. A proof of this theorem is given in Appendix A.

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.,

$$\tilde{Q}_{r0}=\left(\frac{1-(\tilde{\alpha}+\beta)\left(1+\bar{P}_s\right)}{\beta}\right)^+. \tag{36}$$

Let Q_{r0}^* be as defined in (33). The optimal policy $(\hat{P}_s^{NF},\hat{Q}_{r0}^{NF})$ is given as follows:

1) If $\tilde{\alpha}\leq 0$, then: $\hat{P}_s^{NF}=\bar{P}_s$, if $\tilde{g}_s<1$. $\hat{P}_s^{NF}=0$, if $\tilde{g}_s\geq 1$. $\hat{Q}_{r0}^{NF}=0$.
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 $\tilde{\alpha}+\beta\geq 1$, then: $\hat{P}_s^{NF}=\bar{P}_s$, if $\tilde{g}_s<1$. $\hat{P}_s^{NF}=0$, if $\tilde{g}_s\geq 1$. $\hat{Q}_{r0}^{NF}=0$.
   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 $Q_{r0}^{(2)}=$

$$\frac{\tilde{g}_s\left(1-(\tilde{\alpha}+\beta)+\sqrt{\tilde{\alpha}\beta}-\sqrt{(\tilde{\alpha}+\beta)((\tilde{\alpha}+\beta)-\tilde{g}_s\beta)\tilde{g}_s(1-\tilde{\alpha})}\right)}{\sqrt{\tilde{\alpha}\beta}(\tilde{g}_s\beta-\tilde{\alpha}(\tilde{\alpha}+\beta))} \tag{37}$$

      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 (37).
      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 (17) and (30), 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,

$$\text{If} \quad R^{CJ}\left(\hat{P}_s^{CJ}, \hat{Q}_{r0}^{CJ}\right) > R_o \quad \text{then} \quad \tilde{\alpha} > \max(1, \tilde{g}_s) \tag{38}$$

$$\text{If} \quad R^{NF}\left(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF}\right) > R_o \quad \text{then} \quad 0 < \tilde{\alpha} < 1 - \beta. \tag{39}$$

Hence, if

$$\tilde{\alpha} \in [1 - \beta, \max(1, \tilde{g}_s)] \cup (-\infty, 0], \tag{40}$$

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 (40), $\tilde{g}_s < 1$, 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 (40), $\tilde{g}_s \geq 1$, 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. Reversely Degraded Relay-Eavesdropper Channel With a Multiantenna Relay

In this section, we consider a similar model to the one described in Section II except for two differences. First, we assume that the relay receives a vector $\mathbf{Y}_r$ which is a noisy version of the source transmission and hence the relay can use this observation in one way or another to help increase the achievable secrecy rate. Second, we assume that, given the relay's channel input $\mathbf{X}_r$, the relay's observation is a degraded version of the destination's observation. In particular, we consider the system where the destination's and the eavesdropper's observations are given by (6) and (7), respectively. The relay's observation, $\mathbf{Y}_r \in \mathbb{R}^K$, is given by

$$\mathbf{Y}_r = \boldsymbol{\eta} Y + \boldsymbol{\Theta}\mathbf{X}_r + \mathbf{N}_r \tag{41}$$

where $\boldsymbol{\eta} \in \mathbb{R}^K$ is the vector of equivalent channel coefficients from the destination's observation Y to the relay's observation $\mathbf{Y}_r$, $\boldsymbol{\Theta} \in \mathbb{R}^{K\times K}$ is the matrix of channel coefficients from the relay's input $\mathbf{X}_r$ to the relay's output $\mathbf{Y}_r$, and $\mathbf{N}_r \in \mathbb{R}^K$ is AWGN vector of zero mean and identity covariance matrix and is independent of $(X_s,\ \mathbf{X}_r,\ N,\ N')$. Accordingly, we have the following Markov chain $X_s \rightarrow (Y, \mathbf{X}_r) \rightarrow \mathbf{Y}_r$. We further assume that in (7) $\mathbf{u}_r \neq \mathbf{0}$, i.e., given the source's input X_s, neither the destination's observation Y nor the eavesdropper's observation Z is a degraded version of one another.

In the following theorem, we show that for the channel described in this section, using only the CJ strategy over the orthogonal component $\mathbf{X}_{r1}$ (no signaling over the direct component $\mathbf{X}_{r0}$) yields a secrecy rate that approaches the secrecy capacity of this channel as $\bar{P}_r \rightarrow \infty$. In other words, we show that for high SNR over the relay-destination and the relay-eavesdropper channel, the secrecy rate achieved by CJ over the orthogonal component of the relay-eavesdropper channel (and no signaling over the direct component) approaches the secrecy capacity of the channel described above, and as a consequence, this strategy achieves the optimal secure DoF of such channel.

Theorem 3: Let $C_s(\bar{P}_r)$ be the secrecy capacity of the reversely degraded relay-eavesdropper channel given by (6), (7), and (41) for a given value of the relay's average power constraint $\bar{P}_r$. Suppose that $\mathbf{u}_r \neq \mathbf{0}$. Let $R_o(\bar{P}_r)$ be R_o of (18) written as a function of $\bar{P}_r$, i.e., $R_o(\bar{P}_r)$ denote the secrecy rate achievable by using the total source's power $\bar{P}_s$ for information transmission and using the total relay's power $\bar{P}_r$ for CJ along the orthogonal component of the relay-eavesdropper channel (i.e., setting $P_s = \bar{P}_s$, $Q_{r1} = \gamma_{r1}\bar{P}_r$ and $Q_{r0} = 0$ in any one of the two strategies described in Section III). Then, for every $\varepsilon > 0$, there is a sufficiently large value $\bar{P}_r$ such that

$$R_o(\bar{P}_r) > C_s(\bar{P}_r) - \varepsilon. \tag{42}$$

In particular,

$$\lim_{\bar{P}_r \rightarrow \infty} R_o(\bar{P}_r) = C^G \tag{43}$$

where $C^G = \frac{1}{2}\log\left(1 + \bar{P}_s\right)$ is the capacity of the Gaussian channel between the source and the destination when there is no eavesdropper in the system.

In Theorem 3, one should note that C^G is indeed an upper bound on the secrecy capacity of the reversely degraded relay-eavesdropper channel. This is due to the fact that the relay in this case cannot increase the reliable information rate from the source to the destination and hence the capacity of the relay channel with no secrecy constraints is indeed C^G. Therefore, C^G is an upper bound on the secrecy capacity of the reversely degraded relay-eavesdropper channel. It is easy to see that

$$R_o(\bar{P}_r) = \frac{1}{2}\log\left(1 + \bar{P}_s\right) - \frac{1}{2}\log\left(\frac{1 + \gamma_{r1}\bar{P}_r + g_s\bar{P}_s}{1 + \gamma_{r1}\bar{P}_r}\right). \tag{44}$$

Hence, (43) follows. This indeed proves (42).

We can even make a stronger statement than the one Theorem 3. In fact, if the relay-eavesdropper channel $\mathbf{g}_r$ is unknown at all the nodes (except possibly the eavesdropper itself), we let the relay choose at random a signaling direction for jamming in the subspace orthogonal to $\mathbf{h}_r$, i.e., chooses a unit vector $\mathbf{s}_r \in \mathbb{R}^K$ at random and chooses the covariance matrix $\mathbf{Q}$ of $\mathbf{X}_r$ as $\mathbf{s}_r\mathbf{s}_r^T\bar{P}_r$. In this case, conditioned on some choice of $\mathbf{s}_r$, the achievable secrecy rate by this strategy, as a function in $\bar{P}_r$, is given by

$$R_o(\bar{P}_r) = \frac{1}{2}\log\left(1 + \bar{P}_s\right) - \frac{1}{2}\log\left(\frac{1 + \mathbf{g}_r^T\mathbf{s}_r\bar{P}_r + g_s\bar{P}_s}{1 + \mathbf{g}_r^T\mathbf{s}_r\bar{P}_r}\right). \tag{45}$$

It is clear that $\mathbf{g}_r^T\mathbf{s}_r \neq 0$ with probability 1. Hence, $R_o(\bar{P}_r) \rightarrow C^G$ almost surely as $\bar{P}_r \rightarrow \infty$. Thus, even if the relay-eavesdropper's channel $\mathbf{g}_r$ is unknown, the result of

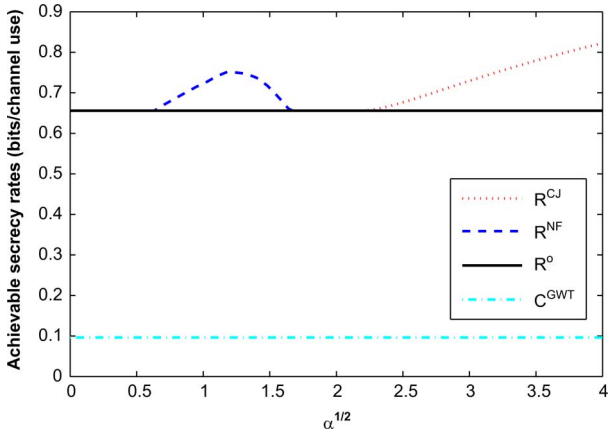

Fig. 1. Optimal achievable secrecy rates by our CJ and NF strategies, R^{CJ} and R^{NF}, the optimal achievable secrecy rate with no transmission along the direct channel component, R_o, and the secrecy capacity of the original Gaussian wiretap channel, C^{GWT}, as functions $\sqrt{\alpha}$ where, as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

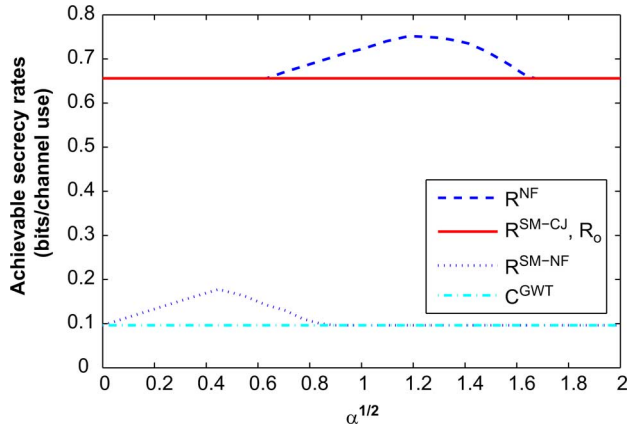

Fig. 2. Optimal achievable secrecy rate by our NF strategy, R^{NF}, the optimal achievable secrecy rate by the single-mode CJ strategy, R^{SM-CJ}, the optimal achievable secrecy rate by the single-mode NF strategy, R^{SM-NF}, and the secrecy capacity of the original Gaussian wiretap channel, C^{GWT},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

Theorem 3 would still hold with probability 1. This stronger result is stated formally in the following theorem.

Theorem 4: If the relay-eavesdropper's channel information $\mathbf{g}_r$ is unavailable (except possibly at the eavesdropper), then using a simple randomized version of the relay's strategy given in Theorem 3, the achievable secrecy rate $R_o(\bar{P}_r)$ converges to C^G as $\bar{P}_r \to \infty$ with probability 1 where C^G is the capacity of the Gaussian channel between the source and the destination when there is no eavesdropper in the system. Hence, with probability 1, $R_o(\bar{P}_r)$ approaches the secrecy capacity of the reversely degraded relay-eavesdropper channel with multiple antennas at the relay as the total average relay's power $\bar{P}_r$ becomes sufficiently large.

V. 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 Fig. 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 $\sqrt{\alpha}$, $0 \le \sqrt{\alpha} \le 4$, where, as in Section II, $\sqrt{\alpha}$ is defined as $\frac{\mathbf{g}_r^T \mathbf{h}_r}{\gamma_{r0}}$. It is clear from Fig. 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, $\sqrt{\alpha} > 1.871$). 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, $0.707 < \sqrt{\alpha} < 1.732$). It is clear that, in general, our CJ and NF strategy yields 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 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 Fig. 2, we plot R^{NF}, R^{SM-CJ}, R^{NF-SM}, and C^{GWT} versus $\sqrt{\alpha}$, $0 \le \sqrt{\alpha} \le 2$. 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.

Finally, we consider a reversely degraded relay-eavesdropper channel with multiple antennas at the relay as the one described in Section IV. In Fig. 3, we illustrate the result of Theorem 3. We fix $\bar{P}_s = 5, \gamma_{r1} = 1$. We plot the achievable secrecy rate R_o of Theorem 3 as a function of $\bar{P}_r$ for three different values of the channel gain g_s, namely, $g_s = 0.25$, 0.75, and 1.5. In this example, the capacity of the Gaussian channel between the source and the destination without secrecy constraints is $C^G = \frac{1}{2}\log(1 + \bar{P}_s) = 1.292$ bits/channel use. It is clear from Fig. 3 that $R_o(\bar{P}_r)$ converges to C^G as $\bar{P}_r$ increases and the rate of convergence increases as g_s decreases.

VI. Conclusions

In this paper, we extended the idea of deaf cooperation to the multiantenna 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

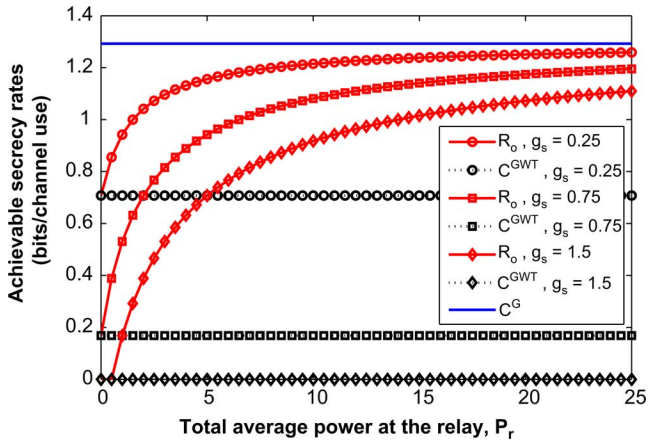

Fig. 3. Achievable secrecy rate of Theorem 3 as a function of $\bar{P}_r$, $R_o(\bar{P}_r)$, the capacity of the Gaussian channel between the source and the destination without secrecy constraints, C^G, and the secrecy capacity of the original Gaussian wiretap channel, C^{GWT}.

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. Finally, we considered the reversely degraded relay channel and showed that by using a simple CJ strategy, we can approach the secrecy capacity of this reversely degraded channel as we increase the relay's power.

Appendix
Proof of Theorem 2

For cases 1 and 2(a), the proof of these cases follows easily from Lemma 1. Before we prove the rest of the cases, one can easily see that the conditions below hold for the rest of the cases, i.e., whenever $\tilde{\alpha} > 0$ and $\tilde{\alpha} + \beta < 1$.

$$\forall\, P_s \geq 0, \quad \frac{\partial R_1^{NF}(P_s, Q_{r0})}{\partial P_s} \geq 0 \quad \text{if and only if} \quad Q_{r0} \geq \frac{\tilde{g}_s - 1}{\tilde{\alpha}} \tag{46}$$

$$\forall\, P_s \geq 0, \quad \frac{\partial R_1^{NF}(P_s, Q_{r0})}{\partial Q_{r0}} \geq 0 \quad \forall\, Q_{r0} \geq 0 \tag{47}$$

$$\text{If } \tilde{g}_s < \tilde{\alpha}, \text{ then } \quad \forall\, P_s \geq 0, \quad \frac{\partial R_2^{NF}(P_s, Q_{r0})}{\partial P_s} \geq 0 \quad \text{if and only if} \quad Q_{r0} \geq \frac{\tilde{g}_s - 1}{\tilde{\alpha} - \tilde{g}_s} \tag{48}$$

$$\text{If } \tilde{g}_s > \tilde{\alpha}, \text{ then } \quad \forall\, P_s \geq 0, \quad \frac{\partial R_2^{NF}(P_s, Q_{r0})}{\partial P_s} \geq 0 \quad \text{if and only if} \quad Q_{r0} \leq \frac{1 - \tilde{g}_s}{\tilde{g}_s - \tilde{\alpha}} \tag{49}$$

$$\text{If } \tilde{g}_s = \tilde{\alpha}, \text{ then } \quad \forall\, P_s, Q_{r0} \geq 0, \quad \frac{\partial R_2^{NF}(P_s, Q_{r0})}{\partial P_s} \geq 0. \tag{50}$$

Also, from Lemma 1, we have

$$\forall\, P_s \in [0, P_s^*], \quad \frac{\partial R_2^{NF}(P_s, Q_{r0})}{\partial Q_{r0}} \geq 0 \quad \text{if and only if} \quad Q_{r0} \in [0, Q_{r0}^*(P_s)]. \tag{51}$$

Now, we consider case 2(b). From (46) and (48), both R_1^{NF} and R_2^{NF} are increasing in P_s. Hence, $\hat{P}_s^{NF} = \bar{P}_s$. We have one of the following two cases depending on whether $\bar{P}_s \leq P_s^*$. First, if $\bar{P}_s \leq P_s^*$, then it follows from (51) that, $R_2^{NF}(\bar{P}_s, Q_{r0})$, as a function of Q_{r0}, attains its unconstrained maximum at $Q_{r0} = Q_{r0}^*(\bar{P}_s)$. On the other hand, from (46), $R_1^{NF}(\bar{P}_s, Q_{r0})$, as a function of Q_{r0}, is increasing in Q_{r0} for all $Q_{r0} \geq 0$ and hence the curves of $R_1^{NF}(\bar{P}_s, Q_{r0})$ and $R_2^{NF}(\bar{P}_s, Q_{r0})$ may intersect at some positive Q_{r0} (note that they already intersect at $Q_{r0} = 0$). It is easy to see that such point is indeed $\tilde{Q}_{r0}$ given by (36). Note also that $R^{NF}(\bar{P}_s, Q_{r0}) = R_1^{NF}(\bar{P}_s, Q_{r0})$ whenever $Q_{r0} \leq \tilde{Q}_{r0}$, i.e., $R_1^{NF}(\bar{P}_s, Q_{r0}) \leq R_2^{NF}(\bar{P}_s, Q_{r0})$ whenever $Q_{r0} \leq \tilde{Q}_{r0}$. Hence, the unconstrained maximizer of $R^{NF}(\bar{P}_s, Q_{r0})$ as a function of Q_{r0} is $\max\left(Q_{r0}^*(\bar{P}_s), \tilde{Q}_{r0}\right)$. Since both $R_1^{NF}(\bar{P}_s, Q_{r0})$ and $R_2^{NF}(\bar{P}_s, Q_{r0})$ are increasing in Q_{r0} for all $0 \leq Q_{r0} \leq \max\left(Q_{r0}^*(\bar{P}_s), \tilde{Q}_{r0}\right)$, it follows that the constrained maximizer $\hat{Q}_{r0}^{NF}$ is given by $\min\left(\gamma_{r0}\bar{P}_r, \max\left(Q_{r0}^*(\bar{P}_s), \tilde{Q}_{r0}\right)\right)$. If $\bar{P}_s > P_s^*$, then from (51), $R_2^{NF}(\bar{P}_s, Q_{r0})$ (and consequently $R^{NF}(\bar{P}_s, Q_{r0})$) is upper bounded by $R_2^{NF}(\bar{P}_s, 0) = R_o$ which is the optimal secrecy rate achieved when there is no transmission along the direct channel component. Hence, $\hat{Q}_{r0}^{NF} = 0$.

Next, we consider case 2(c). From (46), $R_1^{NF}(P_s, Q_{r0})$ is increasing in P_s for all $P_s, Q_{r0} \geq 0$. In case 2(c-i), from (49), $R_2^{NF}(P_s, Q_{r0})$ is also increasing in P_s for all $P_s \geq 0$ and for all $0 \leq Q_{r0} \leq \gamma_{r0}\bar{P}_r$. Hence, in this case $\hat{P}_s^{NF} = \bar{P}_s$. The rest of case 2(c-i) follows using the same argument of case 2(b).

We analyze the rest of the subcases of (c) as follows. Since in these subcases $\gamma_{r0}\bar{P}_r > \frac{1-\tilde{g}_s}{\tilde{g}_s - \tilde{\alpha}}$, we solve the optimization problem in two steps. First, we find the local maximizer $({P_s}^{(a)}, {Q_{r0}}^{(a)})$ of $R^{NF}(P_s, Q_{r0})$ for $0 \leq P_s \leq \bar{P}_s$, $0 \leq Q_{r0} \leq \frac{1-\tilde{g}_s}{\tilde{g}_s - \tilde{\alpha}}$. Then, we find the local maximizer $({P_s}^{(b)}, {Q_{r0}}^{(b)})$ of $R^{NF}(P_s, Q_{r0})$ for $0 \leq P_s \bar{P}_s$, $\frac{1-\tilde{g}_s}{\tilde{g}_s - \tilde{\alpha}} \leq Q_{r0} \leq \gamma_{r0}\bar{P}_r$. Finally, we set $(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF}) = ({P_s}^{(a)}, {Q_{r0}}^{(a)})$ if $R^{NF}({P_s}^{(a)}, {Q_{r0}}^{(a)}) \geq R^{NF}({P_s}^{(b)}, {Q_{r0}}^{(b)})$ and set $(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF}) = ({P_s}^{(b)}, {Q_{r0}}^{(b)})$ otherwise.

Clearly, $({P_s}^{(a)}, {Q_{r0}}^{(a)})$ can be easily obtained in the same way the maximizer in case 2(c-i) was obtained. In particular, ${P_s}^{(a)} = \bar{P}_s$ and ${Q_{r0}}^{(a)} = \min\left(\frac{1-\tilde{g}_s}{\tilde{g}_s - \tilde{\alpha}}, \max\left(Q_{r0}^*(\bar{P}_s), \tilde{Q}_{r0}\right)\right)$ if $\bar{P}_s \leq P_s^*$ whereas ${Q_{r0}}^{(a)} = 0$ if $\bar{P}_s > P_s^*$. We consider now the case where

$$\frac{1 - \tilde{g}_s}{\tilde{g}_s - \tilde{\alpha}} \leq Q_{r0} \leq \gamma_{r0}\bar{P}_r. \tag{52}$$

From (46) and (49), it follows that, for all Q_{r0} satisfying (52), $R_1^{NF}(P_s, Q_{r0})$ is increasing in P_s whereas $R_2^{NF}(P_s, Q_{r0})$ is decreasing in P_s. Let $\tilde{P}_s(Q_{r0})$ be the value of P_s such that

$R_1^{NF}(P_s, Q_{r0}) = R_2^{NF}(P_s, Q_{r0})$. It is easy to see that $\tilde{P}_s(Q_{r0})$ is given by

$$\tilde{P}_s(Q_{r0}) = \frac{1-\beta Q_{r0}}{\tilde{\alpha}+\beta} - 1. \tag{53}$$

It follows from (53) that in order to have $R_1^{NF}(P_s, Q_{r0}) = R_2^{NF}(P_s, Q_{r0})$ for some $P_s \in [0, \bar{P}_s]$, we must have

$$\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta} \leq Q_{r0} \leq \frac{1-(\tilde{\alpha}+\beta)}{\beta}. \tag{54}$$

Now, consider the maximizer of

$$R^{NF}(\tilde{P}_s(Q_{r0}), Q_{r0}) = \frac{1}{2}\log\left(\frac{(1+\tilde{\alpha}Q_{r0})(1-\beta Q_{r0})}{(\tilde{\alpha}+\beta)(1+\tilde{\alpha}Q_{r0}) + \tilde{g}_s\left(1-(\tilde{\alpha}+\beta)-\beta Q_{r0}\right)}\right) \tag{55}$$

subject to conditions (52) and (54), i.e., subject to

$$\begin{aligned} Q_{r0} &\in \left[\frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}, \gamma_{r0}\bar{P}_r\right] \\ &\quad \cap \left[\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta}, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right] \\ &= \Big[\max\left(\frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}, \frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta}\right), \\ &\qquad \min\left(\gamma_{r0}\bar{P}_r, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right)\Big]. \end{aligned} \tag{56}$$

It is not hard to check that $R^{NF}(\tilde{P}_s(Q_{r0}), Q_{r0})$ has one unconstrained maximum at $Q_{r0} = Q_{r0}^{(2)}$ where $Q_{r0}^{(2)}$ is given by (37). Hence, if the interval in (56) is not empty, then the constrained maximizer of (55) subject to (56) is given by $\min\left(Q_{r0}^{(2)}, \gamma_{r0}\bar{P}_r, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right)$. Hence, ${Q_{r0}}^{(b)} = \min\left(Q_{r0}^{(2)}, \gamma_{r0}\bar{P}_r, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right)$. Consequently, from (53), ${P_s}^{(b)} = \tilde{P}_s({Q_{r0}}^{(b)}) = \frac{1-\beta {Q_{r0}}^{(b)}}{\tilde{\alpha}+\beta} - 1$.

If the interval in (56) is empty, then we have either one of two cases. That is $\frac{1-(\tilde{\alpha}+\beta)}{\beta} < \frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}$ or $\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta} > \gamma_{r0}\bar{P}_r$. First, if $\frac{1-(\tilde{\alpha}+\beta)}{\beta} < \frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}$, then $R_2^{NF}(P_s, Q_{r0}) \leq 0$ for all $P_s \geq 0$ and all $Q_{r0} \in \left[\frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}, \gamma_{r0}\bar{P}_r\right]$. Hence, the choice of $({P_s}^{(b)}, {Q_{r0}}^{(b)})$ is irrelevant in this case and the maximizer of R^{NF} is given by $({P_s}^{a}, {Q_{r0}}^{a})$. Second, if $\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta} > \gamma_{r0}\bar{P}_r$, then $R_1^{NF}(P_s, Q_{r0}) < R_2^{NF}(P_s, Q_{r0})$ for all $P_s \in [0, \bar{P}_s]$ and all $Q_{r0} \in \left[0, \gamma_{r0}\bar{P}_r\right]$. Hence, $R^{NF}(P_s, Q_{r0}) = R_1^{NF}(P_s, Q_{r0})$ for all $P_s \in [0, \bar{P}_s]$ and all $Q_{r0} \in \left[0, \gamma_{r0}\bar{P}_r\right]$. Thus, it follows from (46) and (47) that the maximizer of R^{NF} is given by $(\bar{P}_s, \gamma_{r0}\bar{P}_r)$.

Finally, we consider case 2(d). To prove the statement in case 2(d-i), we note that

$$\forall\, P_s \geq 0, \quad \text{if} \quad R_1^{NF}(P_s, Q_{r0}) > 0 \quad \text{then} \quad Q_{r0} > \frac{\tilde{g}_s - 1}{\tilde{\alpha}}. \tag{57}$$

Hence, if $\gamma_{r0}\bar{P}_r \leq \frac{\tilde{g}_s-1}{\tilde{\alpha}}$, then we necessarily have $R^{NF}(P_s, Q_{r0}) = 0$ for all $P_s \geq 0$ and all $0 \leq Q_{r0} \leq \gamma_{r0}\bar{P}_r$. Thus, in this case, $\hat{P}_s^{NF} = \hat{Q}_{r0}^{NF} = 0$. For the rest of the subcases of 2(d), the proof follows the same steps of the proof of cases 2(c-ii), 2(c-iii), and 2(c-iv) above.

REFERENCES

[1] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Vehicular Technology Conf.*, Sep. 2005.

[2] E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wiretap channel with collective secrecy," in *Proc. 44th Ann. Allerton Conf. Communication, Control and Computing*, Monticello, IL, Sep. 2006.

[3] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 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. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

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

[6] L. Lai, H. E. Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5059–5067, Nov. 2008.

[7] I. Krikidis, J. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 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 *Proc. 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 *Proc. ACITA 2010*, Sep. 2010 [Online]. Available: 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 *Proc. 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 *Proc. 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 *Proc. 15th IEEE Workshop on Statistical Signal Processing*, Sep. 2009, pp. 417–420.

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

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

[15] L. Lai and H. E. Gamal, "Cooperation for secrecy: The relay-eavesdropper channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[16] L. Lai and H. E. Gamal, "Cooperation for secure communication: The relay wiretap channel," in *Proc. ICASSP 2007*, Honolulu, HI, Apr. 2007, pp. III 149–III 152.

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

[18] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 7, pp. 451–456, Jul. 1978.

Raef Bassily (M'12) received the B.S. degree in electrical and computer engineering and the M.S. degree in engineering mathematics from Cairo University, Giza, Egypt, in 2003 and 2006, respectively. He received the Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park, in 2011.

He was a research associate in the Department of Computer Science at the University of Maryland, College Park, from January to August 2012. Since August 2012, he has been a research associate in the Department of Computer Science and Engineering at the Pennsylvania State University. His research interests include information theory, wireless communications, cryptography, network security, statistical data privacy, and machine learning.

Sennur Ulukus (S'90–M'98) is a Professor of Electrical and Computer Engineering at the University of Maryland at College Park, where she also holds a joint appointment with the Institute for Systems Research (ISR). Prior to joining UMD, she was a Senior Technical Staff Member at AT&T Labs-Research. She received the Ph.D. degree in electrical and computer engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, and the B.S. and M.S. degrees in electrical and electronics engineering from Bilkent University. Her research interests are in wireless communication theory and networking, network information theory for wireless communications, signal processing for wireless communications, physical-layer information-theoretic security for wireless networks, and energy-harvesting wireless communications.

Dr. Ulukus received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, the 2005 NSF CAREER Award, and the 2010–2011 ISR Outstanding Systems Engineering Faculty Award. She served as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY between 2007 and 2010, as an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS between 2003 and 2007, as a Guest Editor for the *Journal of Communications and Networks, Special Issue on Energy Harvesting in Wireless Networks*, as a Guest Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY, SPECIAL ISSUE ON INTERFERENCE NETWORKS, and as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, SPECIAL ISSUE ON MULTIUSER DETECTION FOR ADVANCED COMMUNICATION SYSTEMS AND NETWORKS. She served as the TPC cochair of the Communication Theory Symposium at the 2007 IEEE Global Telecommunications Conference, the Medium Access Control (MAC) Track at the 2008 IEEE Wireless Communications and Networking Conference, the Wireless Communications Symposium at the 2010 IEEE International Conference on Communications, the 2011 Communication Theory Workshop, the Physical-Layer Security Workshop at the 2011 IEEE International Conference on Communications, and the Physical-Layer Security Workshop at the 2011 IEEE Global Telecommunications Conference. She was the Secretary of the IEEE Communication Theory Technical Committee (CTTC) in 2007–2009.