Deaf Cooperation and Relay Selection Strategies for Secure Communication in Multiple Relay Networks

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). In particular, we study the role of a deaf helper in confusing the eavesdropper in a GWT channel by either transmitting white Gaussian noise (cooperative jamming) or by transmitting a dummy codeword of no context yet drawn from a codebook known to both the destination and the eavesdropper (noise forwarding). We first derive the conditions under which each mode of deaf cooperation improves over the secrecy capacity of the original wiretap channel and show that a helping node can be either a useful cooperative jammer or a useful noise forwarder but not both at the same time. Secondly, we derive the optimal power allocation for both the source and the helping node to be used in each of the two modes of deaf helping. Thirdly, we consider the deaf helper selection problem where there are N relays present in the system and it is required to select the best K deaf helpers, $K \geq 1$, that yield the maximum possible achievable secrecy rate. For the case of $K = 1$, we give the optimal selection strategy with optimal power allocation. The computational complexity of the optimal selection strategy when $K > 1$ is relatively large, especially for large values of K and N. Thus, we propose a suboptimal strategy for the selection problem when $K > 1$. We derive the complexity of the proposed selection strategies and show that, for $K > 1$, our suboptimal strategy, which works in a greedy fashion, enjoys a significantly less computational complexity than the optimal strategy. Nevertheless, as demonstrated by numerical examples, our suboptimal strategy gives rise to reasonable performance gains in terms of the achievable secrecy rate with respect to the case of $K = 1$.**

***Index Terms*—Complexity, cooperative jamming, deaf cooperation, information theoretic secrecy, noise forwarding, relay networks, secrecy rates, selection strategies.**

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 was further investigated in several works. For example, the discrete memoryless relay network was investigated in [7] where achievable secrecy rates were developed when relays help increase secrecy rate by inserting noise into the network. On the other hand, the relay selection problem in the secrecy context was investigated, e.g., in [8] and [9]. In particular, [8] proposed a scheme that enables an opportunistic selection of two relays to increase security where one relay uses the decode-and-forward (DF) strategy while the other uses the CJ strategy to introduce useful interference and thus help increase the achievable secrecy rate. In [9], one relay node is selected to assist two source nodes to exchange messages with each other using the amplify-and-forward (AF) strategy while one or two additional relay nodes are selected to transmit jamming signals to confuse the eavesdropper. The role of cooperative jamming in the presence of multiple eavesdroppers was studied in [10] where noise generators (cooperative jammers) were employed in a multiple-relay multiple-eavesdropper network to improve security. The impact of cooperative jamming on the secrecy outage probability of a slow fading wiretap channel was studied in [11] where related security metrics, namely, jamming coverage and jamming efficiency, were introduced and different jamming strategies were proposed depending on the various levels of available channel state information. In a stochastic network model, it was shown in [12] that packet collisions caused by jamming nodes can be used to increase the level of secrecy. Cooperative jamming strategies in multiple antenna relays networks were investigated in [13], [14], and [15].

Power allocation for the the source and relay nodes in cooperative jamming relay networks was studied, e.g., in [16], [13], and [15]. In [16], the communication between the source and destination occurs in two hops. Both the source and the relay are allowed to split their available power into a useful information part and a jamming part. Reference [16] solves for the power allocation under the assumption that both the relay and

Manuscript received February 04, 2012; revised May 19, 2012, August 28, 2012, and October 10, 2012; accepted October 23, 2012. Date of publication December 19, 2012; date of current version February 26, 2013. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Walaa Hamouda. This work was supported by the NSF by Gants CCF 07-29127, CNS 09-64632, CCF 09-64645, CCF 10-18185, and CNS 11-47811.

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 (e-mail: bassily@psu.edu).

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/TSP.2012.2235433

the destination have the knowledge of the jamming signals. In [13], 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 [15], 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 [15], the source, the destination, and the eavesdropper have multiple antennas, whereas the relay has a single antenna. Under similar constraint to the one in [13], namely, that the jamming signals lie in the subspace orthogonal to the channels to the legitimate nodes, 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 [17]. In particular, [17] 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 [18]. 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.

At this point, it is useful to compare the two aforementioned alternatives of deaf cooperation for secrecy introduced in the literature. Generally speaking, it is not useful to perform CJ when the helper is closer to the destination than to the eavesdropper, on the other hand, one can still introduce helpful interference in this case by transmitting a dummy codeword from a codebook that is known to the destination and the eavesdropper. The transmission of dummy codewords refers to Wyner's idea of stochastic encoding for secrecy [19] where multiple codewords are associated with a single message. Since the cost of these dummy codewords is a decrease in the transmitter's rate, if the helper takes the responsibility of sending these dummy codewords, then the secrecy rate of the transmitter may improve [20].

In this paper, we investigate in detail 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, we give the necessary and sufficient conditions, in terms of power values and relative channel gains, for each of the two strategies to yield higher secrecy rate than the secrecy capacity of the original GWT channel. We also obtain, in terms of the channel gains solely, the necessary conditions for each of the CJ and the NF strategies to yield a secrecy rate higher than the secrecy capacity of the GWT channel. In particular, we reach the following useful conclusion. 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, or it may not be useful at all as a deaf helper. Moreover, we derive the optimal power allocation policy for each of the two strategies where we assume that the source, the deaf helper, the legitimate receiver, and the eavesdropper have perfect knowledge of all the relevant channel gains.

On the other hand, we consider applying both CJ and NF strategies in multiple relay networks to improve secrecy rates achievable when only CJ strategy is used. In particular, we consider a multiple relay network of N relays in addition to a source, a legitimate receiver, and an eavesdropper. The objective is to select a set of $K, K \leq N$, relays that act as the best deaf helpers, i.e., that maximize the secrecy rate achievable by deaf cooperation using K relays. We first consider the special case of $K = 1$. We give the optimal Single Deaf Helper Selection (SDHS) strategy that identifies the optimal deaf helper node and its mode of cooperation (CJ or NF). The optimal strategy in this case is obvious and clearly requires $O(N)$ computations. However, our strategy enjoys the extra advantage of using the optimal power allocation at both the source and the selected relay without any additional cost in complexity that could be incurred by using a numerical algorithm to find the optimal power allocations. This is due to the fact that we have a closed-form for the optimal power allocation policy in this case and hence we avoid using numerical algorithms to find the optimal power allocations.

Next, we consider the general selection problem, i.e., the case where $K > 1$. Deriving a closed-form for the optimal power allocations becomes intractable in this case. To avoid using numerical methods that generally do not guarantee convergence to the global optimum and that are usually computationally expensive, we use a constant power allocation at each node. Having fixed the power allocation policy in this case, we note that the computational complexity of the optimal selection strategy is still relatively large, especially for large values of K and N. Thus, we propose a suboptimal Multiple Deaf Helper Selection (MDHS) strategy that selects at most K relays over at most K selection stages in which the source and the relays negotiate to identify the deaf helpers to be selected one by one in a greedy fashion.

In terms of the computational complexity of the multiple deaf helper selection strategies, we distinguish between two cases. In the first case, K is a fixed constant that does not depend on N, whereas, in the second case, K is some fixed fraction of N, i.e., $\frac{K}{N} = \alpha$ for some rational $\alpha \in (0, 1]$. In the first case, we show that our MDHS strategy requires $O(N)$ computations while the optimal strategy requires $\Omega(N^K)$ computations. Hence, our strategy leads to a reduction of $O(N^{K-1})$ in

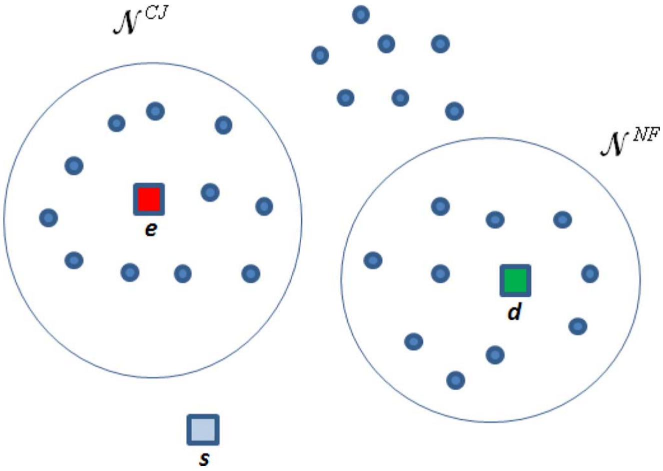

Fig. 1. A multiple relay network.

complexity with respect to the optimal strategy. In the second case, we show that the reduction in complexity by using our MDHS strategy as compared to using the optimal strategy is $O(\frac{2^{\alpha N \log(\frac{3}{2\alpha})}}{N})$, i.e., using our strategy leads to an exponential reduction in complexity with respect to the optimal strategy.

Finally, we give some numerical examples to compare our strategies, in terms of the achievable secrecy rate, with those based on only one mode of deaf cooperation. We also quantify through some numerical examples the improvement in the achievable secrecy rate when the MDHS strategy is used instead of the SDHS strategy.

II. System Model

We consider the following communication scenario. A source, s, sends a confidential message to a destination, d, over an AWGN channel in the presence of an informed eavesdropper, e. The communication occurs in the presence of a set of N nodes (relays), $\mathcal{N} = \{r_1, \ldots, r_N\}$, from which one is selected to help improve the achievable perfect secrecy through deaf cooperation, i.e., CJ or NF (see Fig. 1). Assuming that the relay node $r \in \mathcal{N}$ is selected to be the deaf helper, the outputs of the GWT channel, with the deaf helper r, at the destination and the eavesdropper are given by

$$Y = \sqrt{\gamma_{s,d}}\tilde{X}_s + \sqrt{\gamma_{r,d}}\tilde{X}_r + N \tag{1}$$

$$Z = \sqrt{\gamma_{s,e}}\tilde{X}_s + \sqrt{\gamma_{r,e}}\tilde{X}_r + N' \tag{2}$$

where $\gamma_{k,l}$, $k \in \{s,r\}$, $l \in \{d,e\}$, is the channel gain between nodes k and l, $\tilde{X}_k$, $k \in \{s,r\}$ is the channel input at node k, and N, N' are real-valued zero mean, unit variance AWGN at the destination and the eavesdropper, respectively. The channel inputs satisfy the following average power constraints

$$E[\tilde{X}_k^2] \leq \bar{\rho}_k, \quad k \in \{s,r\} \tag{3}$$

It is assumed that all channel gains in (1)–(2) are known to s, d, r, and e. For a fixed deaf helper node, r, the above system given by (1)–(2) and power constraints (3) is equivalent to

$$Y = X_s + X_r + N \tag{4}$$

$$Z = \sqrt{h_s}X_s + \sqrt{h_r}X_r + N' \tag{5}$$

with

$$E\left[X_k^2\right] \leq \bar{P}_k \triangleq \bar{\rho}_k\gamma_{k,d}, \quad k \in \{s,r\} \tag{6}$$

where $X_k \triangleq \sqrt{\gamma_{k,d}}\tilde{X}_k$ and $h_k \triangleq \frac{\gamma_{k,e}}{\gamma_{k,d}}$, $k \in \{s,r\}$.

III. Improving Secrecy Through Deaf Cooperation

In this section, we consider the CJ and the NF schemes. In both schemes, the channel input at the source X_s in (4)–(5) 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 Gaussian random variable with zero mean and variance P_s where $P_s \leq \bar{P}_s$. Also, in both schemes, the channel input at the deaf helper X_r in (4)–(5) is also Gaussian with zero mean and variance P_r where $P_r \leq \bar{P}_r$. However, the difference between the two schemes comes from the origin of X_r. In the CJ scheme, X_r is white Gaussian noise that plays the same role as the background noise at the destination and the eavesdropper except for the fact that it is generated artificially. On the other hand, in the NF scheme, X_r is a symbol of a dummy (context-free) codeword drawn from a Gaussian codebook that is assumed to be available at both the destination and the eavesdropper. Accordingly, for given power values P_s and P_r, the secrecy rate achievable by the CJ scheme [4], R^{CJ} is given by

$$R^{CJ}(P_s,P_r) = \frac{1}{2}\log\left(\frac{(1+P_s+P_r)(1+h_rP_r)}{(1+h_sP_s+h_rP_r)(1+P_r)}\right) \tag{7}$$

Whereas the secrecy rate achievable by the NF scheme [17], R^{NF}, is given by

$$R^{NF}(P_s,P_r) = \min\left\{\frac{1}{2}\log\left(\frac{(1+P_s)(1+h_rP_r)}{1+h_sP_s+h_rP_r}\right), \frac{1}{2}\log\left(\frac{1+P_s+P_r}{1+h_sP_s+h_rP_r}\right)\right\} \tag{8}$$

On the other hand, when no helper node is involved, the secrecy capacity of the original GWT channel [21] for a given power value P_s is given by

$$C^{GWT}(P_s) = \left(\frac{1}{2}\log\left(\frac{1+P_s}{1+h_sP_s}\right)\right)^+ \tag{9}$$

where $(x)^+ = \max(0,x)$. In the following theorem, we give the necessary and sufficient conditions for $R^{CJ}(P_s,P_r) \geq C^{GWT}(P_s)$ and $R^{NF}(P_s,P_r) \geq C^{GWT}(P_s)$.

Theorem 1: $R^{CJ}(P_s,P_r) \geq C^{GWT}(P_s)$ if and only if one of conditions (10) or (11) below is satisfied:

$$h_s < 1 \leq h_r \text{ and } (h_sh_r - 1) + h_s(h_r-1)P_s \geq h_r(1-h_s)P_r \tag{10}$$

$$1 \leq h_s < h_r \text{ and } P_r \geq \frac{h_s - 1}{h_r - h_s} \tag{11}$$

On the other hand, $R^{NF}(P_s, P_r) \geq C^{GWT}(P_s)$ if and only if one of conditions (12), (13), or (14) below is satisfied:

$$h_r \leq h_s \leq 1 \tag{12}$$

$$h_s < h_r \leq 1 \quad \text{and} \quad P_s \leq \frac{1-h_r}{h_r - h_s} \tag{13}$$

$$h_r < 1 \leq h_s \quad \text{and} \quad P_r \geq \max\left(\frac{h_s-1}{h_r}, \frac{h_s-1}{1-h_r}P_s\right) \tag{14}$$

A proof of Theorem 1 is given in Appendix A.

One important observation one can make in regard with Theorem 1 is that the CJ strategy cannot be beneficial, i.e., it cannot achieve higher secrecy rate than the secrecy capacity of the original GWT channel, if the value of the relative channel gain between the relay node and the eavesdropper h_r is less than 1 or less than the value of the relative channel gain between the source and the eavesdropper h_s. On the other hand, the NF strategy is not useful, if $h_r > 1$. This observation is stated formally in the following corollary.

Corollary 1: $h_r \geq \max(h_s, 1)$ is a necessary condition for the CJ scheme to achieve higher secrecy rate than the secrecy capacity of the original GWT channel. On the other hand, $h_r \leq 1$ is a necessary condition for the NF scheme to achieve higher secrecy rate than the secrecy capacity of the original GWT channel.

IV. Maximizing the Secrecy Rates Achievable by the CJ and NF Schemes

For fixed relative channel gains h_s and h_r, we obtain the solutions of the following optimization problems.

$$\max_{P_s, P_r} R^{CJ}(P_r, P_s) \quad \text{s.t.} \quad 0 \leq P_s \leq \bar{P}_s, 0 \leq P_r \leq \bar{P}_r \tag{15}$$

$$\max_{P_s, P_r} R^{NF}(P_r, P_s) \quad \text{s.t.} \quad 0 \leq P_s \leq \bar{P}_s, 0 \leq P_r \leq \bar{P}_r \tag{16}$$

Let $(\hat{P}_s^{CJ}, \hat{P}_r^{CJ})$ be the maximizer of (15) and $(\hat{P}_s^{NF}, \hat{P}_r^{NF})$ be the maximizer of (16). We define $\bar{R}^{CJ} \triangleq R^{CJ}(\hat{P}_s^{CJ}, \hat{P}_r^{CJ})$ and $\bar{R}^{NF} \triangleq R^{NF}(\hat{P}_s^{NF}, \hat{P}_r^{NF})$.

Theorem 2: The solution of (15) and (16) above is given in the following cases:

1) $h_s < 1$: In this case, we have the following three possibilities depending on the value of h_r:

a) If $h_s < 1 \leq h_r$, then

$$\hat{P}_s^{CJ} = \bar{P}_s, \hat{P}_r^{CJ} = \left(\min\left(\bar{P}_r, P_r^*\right)\right)^+ \tag{17}$$

$$\hat{P}_s^{NF} = \bar{P}_s, \hat{P}_r^{NF} = 0 \tag{18}$$

b) If $h_s < h_r < 1$, then

$$\hat{P}_s^{CJ} = \bar{P}_s, \hat{P}_r^{CJ} = 0 \tag{19}$$

$$\hat{P}_s^{NF} = \bar{P}_s \tag{20}$$

$$\hat{P}_r^{NF} = \bar{P}_r, \text{ if } \bar{P}_s < \frac{1-h_r}{h_r - h_s} \tag{21}$$

$$\hat{P}_r^{NF} = 0, \text{ if } \bar{P}_s \geq \frac{1-h_r}{h_r - h_s} \tag{22}$$

c) If $h_r \leq h_s < 1$, then

$$\hat{P}_s^{CJ} = \bar{P}_s, \hat{P}_r^{CJ} = 0 \tag{23}$$

$$\hat{P}_s^{NF} = \bar{P}_s, \text{ if } \bar{P}_r < \frac{1-h_s}{h_s - h_r} \tag{24}$$

$$\hat{P}_s^{NF} = \min\left(\bar{P}_s, \frac{1-h_r}{h_r}\right), \text{ if } \bar{P}_r \geq \frac{1-h_s}{h_s - h_r} \tag{25}$$

$$\hat{P}_r^{NF} = \bar{P}_r \tag{26}$$

2) $h_s \geq 1$: In this case, we have the following three possibilities depending on the value of h_r:

a) If $1 \leq h_s < h_r$, then

$$\hat{P}_s^{CJ} = 0, \hat{P}_r^{CJ} = 0, \text{ if } \bar{P}_r \leq \frac{h_s - 1}{h_r - h_s} \tag{27}$$

$$\hat{P}_s^{CJ} = \bar{P}_s \text{ and}$$

$$\hat{P}_r^{CJ} = \min(\bar{P}_r, P_r^*), \text{ if } \bar{P}_r > \frac{h_s - 1}{h_r - h_s} \tag{28}$$

$$\hat{P}_s^{NF} = 0, \hat{P}_r^{NF} = 0 \tag{29}$$

b) If $h_r < 1 \leq h_s$, then

$$\hat{P}_s^{CJ} = 0, \hat{P}_r^{CJ} = 0 \tag{30}$$

$$\hat{P}_s^{NF} = 0, \hat{P}_r^{NF} = 0, \text{ if } \bar{P}_r \leq \frac{h_s - 1}{h_r} \tag{31}$$

$$\hat{P}_s^{NF} = \min\left(\bar{P}_s, \frac{1-h_r}{h_r}\right) \text{ and}$$

$$\hat{P}_r^{NF} = \bar{P}_r, \text{ if } \bar{P}_r > \frac{h_s - 1}{h_r} \tag{32}$$

c) If $1 \leq h_r \leq h_s$, then

$$\hat{P}_s^{CJ} = 0, \hat{P}_r^{CJ} = 0 \tag{33}$$

$$\hat{P}_s^{NF} = 0, \hat{P}_r^{NF} = 0 \tag{34}$$

where

$$P_r^* = \frac{\sqrt{(h_s(h_r - h_s)\bar{P}_s + h_s(h_r - 1))(h_r - 1)h_r} - h_r(1 - h_s)}{h_r(h_r - h_s)} \tag{35}$$

A proof of Theorem 2 is given in Appendix B.

As a consequence of Theorem 2, one can identify, in terms of the relative channel gains solely, the minimal set of necessary conditions for each of $\bar{R}^{CJ} > C^{GWT}$ and $\bar{R}^{NF} > C^{GWT}$ to hold. These conditions are stated formally in the following corollary.

Corollary 2: If $\bar{R}^{CJ} > C^{GWT}$, then $h_r > \max(1, h_s)$. On the other hand, if $\bar{R}^{NF} > C^{GWT}$ then $h_r < \min(1, \frac{1+h_s\bar{P}_s}{1+\bar{P}_s})$.

V. Deaf Helper Selection Problem

A. Single Deaf Helper Selection

In this section, we are interested in selecting one relay from the set $\mathcal{N}$ of N relays that would act as the best deaf helper that maximizes the achievable secrecy rate which could be either $\bar{R}^{CJ}$ if the best deaf helper is a cooperative jammer or $\bar{R}^{NF}$ if the best deaf helper is a noise forwarder. Here, we assume that the original power constraints at the relays $\bar{\rho}_r, r \in \mathcal{N}$ given by (3) are equal. That is $\bar{\rho}_r = \bar{\rho} \forall r \in \mathcal{N}$. Consequently, the scaled power constraints at the relays $\bar{P}_r, r \in \mathcal{N}$, given by (6), have different values depending on the values of the corresponding channel gains $\gamma_{r,d}, r \in \mathcal{N}$. Thus, in order to clarify the presentation in this section, we choose to consider the original system given by (1)–(2) together with the original power constraints (3). Let ρ_s and ρ_r denote the variance of $\tilde{X}_s$ and $\tilde{X}_r, r \in \mathcal{N}$, respectively, where $\rho_s \leq \bar{\rho}_s$ and $\rho_r \leq \bar{\rho}_r, r \in \mathcal{N}$.

The secrecy rates R^{CJ} and R^{NF} in (7) and (8), respectively, can be written as functions of ρ_s and ρ_r as follows

$$R^{CJ}(\rho_s, \rho_r) = \frac{1}{2} \log \left(\frac{(1 + \gamma_{s,d}\rho_s + \gamma_{r,d}\rho_r)(1 + \gamma_{r,e}\rho_r)}{(1 + \gamma_{s,e}\rho_s + \gamma_{r,e}\rho_r)(1 + \gamma_{r,d}\rho_r)} \right) \tag{36}$$

$$\begin{aligned} R^{NF}(\rho_s, \rho_r) = \min \Bigg\{ &\frac{1}{2} \log \left(\frac{(1 + \gamma_{s,d}\rho_s)(1 + \gamma_{r,e}\rho_r)}{1 + \gamma_{s,e}\rho_s + \gamma_{r,e}\rho_r} \right), \\ &\frac{1}{2} \log \left(\frac{1 + \gamma_{s,d}\rho_s + \gamma_{r,d}\rho_r}{1 + \gamma_{s,e}\rho_s + \gamma_{r,e}\rho_r} \right) \Bigg\} \end{aligned} \tag{37}$$

We note that all the results of Theorems 1 and 2 as well as Corollary 1 are valid here by replacing h_k with $\frac{\gamma_{k,e}}{\gamma_{k,d}}$, h_k with $\frac{\gamma_{k,e}}{\gamma_{k,d}}$, P_k with $\gamma_{k,d}\rho_k$, $\bar{P}_k$ with $\gamma_{k,d}\bar{\rho}_k$, $\hat{P}_k^{CJ}$ and $\hat{P}_k^{NF}$ with $\gamma_{k,d}\hat{\rho}_k^{CJ}$ and $\gamma_{k,d}\hat{\rho}_k^{NF}$, respectively, for $k \in \{s, r\}$ and $r \in \mathcal{N}$ where $(\hat{\rho}_s^{CJ}, \hat{\rho}_r^{CJ})$ and $(\hat{\rho}_s^{NF}, \hat{\rho}_r^{NF})$ are the optimal power control policies that maximize (36) and (37), respectively. Hence, using Corollary 2, one can find two disjoint subsets of $\mathcal{N}$ which we denote by $\mathcal{N}^{CJ}$ and $\mathcal{N}^{NF}$, where

$$\mathcal{N}^{CJ} \triangleq \left\{ r_j \in \mathcal{N} : \frac{\gamma_{r_j,e}}{\gamma_{r_j,d}} > \max\left(1, \frac{\gamma_{s,e}}{\gamma_{s,d}}\right) \right\} \tag{38}$$

is the set of potential cooperative jammers, and

$$\mathcal{N}^{NF} \triangleq \left\{ r_j \in \mathcal{N} : \frac{\gamma_{r_j,e}}{\gamma_{r_j,d}} < \min\left(1, \frac{1 + \gamma_{s,e}\bar{\rho}_s}{1 + \gamma_{s,d}\bar{\rho}_s}\right) \right\} \tag{39}$$

is the set of potential noise forwarders. In other words, the set $\mathcal{N}^{CJ}$ is the set that contains every relay node whose relative channel gain satisfies the condition in Corollary 2 necessary for the CJ scheme to achieve a secrecy rate larger than C^{GWT}. On the other hand, the set $\mathcal{N}^{NF}$ is the set that contains every relay node whose relative channel gain satisfies the condition in Corollary 2 necessary for the NF scheme to achieve a secrecy rate larger than C^{GWT}. Since these two subsets are disjoint, it follows that a node in $\mathcal{N}$ cannot be a useful cooperative jammer and a useful noise forwarder at the same time. It is also noteworthy that there might be some other nodes in $\mathcal{N}$ that do not fall in any of the two subsets $\mathcal{N}^{CJ}$ and $\mathcal{N}^{NF}$.

One can always regard the optimal power allocation policies $(\hat{\rho}_s^{CJ}, \hat{\rho}_r^{CJ})$ and $(\hat{\rho}_s^{NF}, \hat{\rho}_r^{NF})$ as functions of the channel gains $(\gamma_{r,d}, \gamma_{r,e})$ where $r \in \mathcal{N}^{CJ}$ and $r \in \mathcal{N}^{NF}$, respectively. Hence, the optimal rates $\bar{R}^{CJ}$ and $\bar{R}^{NF}$ can be also regarded as functions of $(\gamma_{r,d}, \gamma_{r,e})$. Below, we describe a strategy for selecting the optimal relay node $r^* \in \mathcal{N}$ that maximizes the deaf cooperation secrecy rate.

B. Single Deaf Helper Selection (SDHS) Strategy

For each $r \in \mathcal{N}$, using its knowledge of its own channel gains and using the conditions in (38)–(39), r identifies which mode of cooperation (CJ or NF) it should target. Accordingly, r computes one of the two rates $\bar{R}^{CJ}(\gamma_{r,d}, \gamma_{r,e})$ and $\bar{R}^{NF}(\gamma_{r,d}, \gamma_{r,e})$ depending on the target mode of cooperation. We note that the rate is computed using the values of the optimal power allocations that are given by Theorem 2. Then r sends this information to s. Upon receiving such information from all $r \in \mathcal{N}$, s identifies the relay r^* with the maximum rate R^* and knows its mode of cooperation. Consequently, s notifies r^* that it has been selected as the optimal deaf helper which in turn notifies d of the former's selection. It is assumed that this information is also intercepted by e. By executing the SDHS strategy described above, the optimal relay r^* that achieves $\max_{r \in \mathcal{N}} \max\{\bar{R}^{CJ}(\gamma_{r,d}, \gamma_{r,e}), \bar{R}^{NF}(\gamma_{r,d}, \gamma_{r,e})\}$ is identified together with its mode of deaf cooperation.

C. Multiple Deaf Helpers Selection

The system permits us to involve at most K relays, $1 \leq K \leq N$, in deaf cooperation. Each relay can be either a cooperative jammer or a noise forwarder. Let $\mathcal{K}^{CJ} \subseteq \mathcal{N}^{CJ}$ denote the set of the selected cooperative jammers and $\mathcal{K}^{NF} \subseteq \mathcal{N}^{NF}$ denote the set of the selected noise forwarders where $|\mathcal{K}^{CJ} \bigcup \mathcal{K}^{NF}| \leq K$. The achievable secrecy rate in this case for fixed power values $\rho_s, \rho_r, r \in \mathcal{K}^{CJ} \bigcup \mathcal{K}^{NF}$, is given as a function of $(\mathcal{K}^{CJ}, \mathcal{K}^{NF})$ by

$$\begin{aligned} &R(\mathcal{K}^{CJ}, \mathcal{K}^{NF}) \\ &= \min_{\mathcal{M} \subseteq \mathcal{K}^{NF}} \Bigg\{ \frac{1}{2} \log \left(\frac{1 + \gamma_{s,d}\rho_s + \sum_{r \in \mathcal{M}} \gamma_{r,d}\rho_r}{1 + \sum_{r \in \mathcal{K}^{CJ}} \gamma_{r,d}\rho_r} \right) \\ &\quad - \frac{1}{2} \log \left(\frac{1 + \gamma_{s,e}\rho_s + \sum_{r \in \mathcal{M}} \gamma_{r,e}\rho_r}{1 + \sum_{r \in \mathcal{K}^{CJ}} \gamma_{r,e}\rho_r + \sum_{r \in \mathcal{K}^{NF} \setminus \mathcal{M}} \gamma_{r,e}\rho_r} \right) \Bigg\} \end{aligned} \tag{40}$$

The expression above is a generalization of (7) and (8) when there are more than one deaf helper in the system. To see this, recall that the set $\mathcal{K}^{NF}$ of noise forwarders together with the source s create a multiple access wiretap channel to the destination d and the eavesdropper e where the received noise level at d and e is modified by the sum of the respective jamming powers (scaled by the respective channel gains) of the cooperative jammers in $\mathcal{K}^{CJ}$. The achievable deaf cooperation rate $R(\mathcal{K}^{CJ}, \mathcal{K}^{NF})$ is simply the maximum individual rate of s in the achievable secrecy rate region of this multiple access wiretap channel [4]. Hence, the rate $R(\mathcal{K}^{CJ}, \mathcal{K}^{NF})$ results from the intersection of all the rate constraints that involve node s in the achievable secrecy rate region of this multiple access wiretap channel.

In fact, when there are more than one deaf helper, the problem of finding an optimal power control policy for (40) becomes analytically intractable and no closed-form solution could be found. One could possibly resort in this case to numerical algorithms. However, numerical algorithms usually have large running time and their convergence to the global optimum is not guaranteed. Hence, using one such algorithm inside a selection strategy will slow it down and substantially increase the total number of computations carried out through the selection strategy. Thus, in the context of the selection problem, using numerical methods for finding the optimal power allocations is not an efficient option. Therefore, when the number of deaf helpers to be selected is greater than 1, we will use a fixed power allocation policy. That is, when $K > 1$, we set $\rho_s = \bar{\rho}_s$ and $\rho_r = \bar{\rho}_r, r \in \mathcal{N}$.

Having fixed the power allocation policy, we turn our attention to the selection problem. In fact, the problem of finding a subset of at most K deaf helpers that maximizes the secrecy rate out of N available relays is a combinatorial optimization problem that can be reduced to the following integer program. Suppose that each relay is associated with a variable that can be assigned one of three labels: CJ, NF, or IDLE, depending on whether the relay is a cooperative jammer, noise forwarder, or idle (i.e., non-transmitting). Note that for each set of assignments that assigns labels to the N variables, one can compute the rate (40) in polynomial time. In the integer program, it is required to find the set of label assignments to the N variables that maximizes (40). Clearly, the integer program described above can be reduced to our multiple relay selection problem in polynomial time. That is, if we are given the sets $\mathcal{K}^{CJ}$ and $\mathcal{K}^{NF}$ that maximizes (40), then we can obviously obtain the optimal set of label assignments for the above integer program in polynomial time (more specifically, linear time). This implies that our multiple relay selection problem is at least as hard as the above integer programming problem which is generally known to be NP-hard. Hence, we assume that the optimal selection strategy, that chooses the best K deaf helpers out of the N available relays, would, in general, have to evaluate the achievable rate using every possible disjoint pair of subsets $\mathcal{K}^{CJ}, \mathcal{K}^{NF} \subseteq \mathcal{N}$ such that $|\mathcal{K}^{CJ} \bigcup \mathcal{K}^{NF}| \leq K$. As it will be discussed in Section V.E below, the computational complexity of this strategy is significantly high especially for large values of N and K. Thus, we propose below a suboptimal strategy that builds upon the SDHS strategy presented earlier in a greedy fashion for the multiple deaf helper selection problem. Later, in Section V.E, we show that our suboptimal strategy leads to a substantial reduction in computational complexity with respect to the optimal selection strategy.

D. Multiple Deaf Helpers Selection (MDHS) Strategy

The strategy is carried out over at most K stages to select at most K deaf helpers. As mentioned above, we set the transmission power at the source and the relay nodes as $\rho_s = \bar{\rho}_s$ and $\rho_r = \bar{\rho}_r, r \in \mathcal{N}$. We define $\mathcal{K}_i^{CJ}$ and $\mathcal{K}_i^{NF}$ as the set of selected cooperative jammers and noise forwarders by the end of stage i, respectively. Before the first selection stage, we have $\mathcal{K}_0^{CJ} = \mathcal{K}_0^{NF} = \emptyset$. In the first stage, we run the SDHS strategy to obtain the best deaf helper $r_1^* \in \mathcal{N}$, identify its mode of cooperation (CJ or NF), and compute the corresponding achievable secrecy rate R_1^*. These are all made known to s. Moreover, the identity of r_1^* and its cooperation mode are known to d, e, and the rest of the relays by the end of the first stage. Accordingly, we either have $\mathcal{K}_1^{CJ} = \{r_1^*\}$ and $\mathcal{K}_1^{NF} = \emptyset$ or vice versa depending on the identified mode of cooperation of r_1^*. For $2 \leq i \leq K$, we do the following: For each $r \in \mathcal{N} \setminus \{r_j^* : 1 \leq j \leq i-1\}$, r computes two secrecy rates, namely, $R(\mathcal{K}_{i-1}^{CJ} \cup \{r\}, \mathcal{K}_{i-1}^{NF})$ and $R(\mathcal{K}_{i-1}^{CJ}, \mathcal{K}_{i-1}^{NF} \cup \{r\})$ using (40), i.e., the secrecy rates when r plays the role of a cooperative jammer and when it plays the role of a noise forwarder. Hence, r finds the maximum of the two rates and its corresponding mode of cooperation. Then r sends this rate to s. Consequently, s finds the maximum R_i^* of all the rates it receives from all the relays involved in stage i. If $R_i^* \leq R_{i-1}^*$, then the strategy is terminated and the last selection stage would be $i-1$. Note that this means that the strategy may terminate with less than K selected helpers. Otherwise, s identifies the relay r_i^* corresponding to the rate R_i^* and its mode of cooperation. Upon termination at stage t where $1 \leq t \leq K$, the set of the selected deaf helpers $\{r_i^* : 1 \leq i \leq t\}$ and their modes of cooperation are eventually known to s, d, and e and the achievable secrecy rate in this case is R_t^*. We summarize the steps of the MDHS strategy above in the following. First fix the power allocation policy as $\rho_s = \bar{\rho}_s$ and $\rho_r = \bar{\rho}_r, r \in \mathcal{N}$, then do the following:

1) Find the best deaf helper, its mode of cooperation, and the corresponding achievable rate as in the SDHS strategy.
2) While the number of selected deaf helpers is less than K, do the following:
   a) every *unselected* node in the set available relays $\mathcal{N}$, computes the achievable secrecy rate twice: once when it adds itself to the set of already selected cooperative jammers, and another time when it adds itself to the set of already selected noise forwarders. This is done using formula (40). Then, it finds the maximum of the two rates, identifies the corresponding mode of deaf cooperation that it should take (whether it is CJ or NF), and sends the resulting rate and the mode of cooperation to the source.
   b) The source finds the maximum of all the values it receives from all the relays involved in the step 2-a. This is the value of the achievable rate of the current selection stage. The source also identifies the corresponding relay whose rate is the maximum among all the rates it received in step 2-a and identifies its mode of cooperation (CJ or NF). Then, the source compares the current rate value with the rate value obtained in the previous selection stage.
      i) If the rate obtained in the previous selection stage is greater than or equal to the current rate value: stop and output the selected helpers (the set of the selected cooperative jammers and the set of the selected noise forwarders) up to the previous selection stage, and the achievable rate obtained in the previous selection stage as the resulting achievable rate. Note that if the strategy is terminated at this step, then the number of the selected deaf helpers could be less than K.
      ii) Otherwise, the source updates the value of the achievable rate with the current value it obtained in step 2-b, adds the corresponding relay either to the set of the selected cooperative jammers or the set of the selected noise forwarders depending on its mode of deaf cooperation identified in step 2-b above.

E. Complexity Analysis

We measure the complexity of a selection strategy by the total number of computations carried out during the execution of the strategy. In regard to the SDHS strategy, it is obvious that the strategy involves $O(N)$ computations since evaluating the rates (together with the power functions) given in (36) and (37) at all the nodes $r \in \mathcal{N}$ requires $O(N)$ computations ($O(1)$ computations per relay) and finding the maximum of all the rate values received by s from all $r \in \mathcal{N}$ also requires $O(N)$ computations. It is indeed intuitive that, given some fixed power allocation policy, the complexity of the optimal single deaf helper selection strategy is no more than $O(N)$, however, what we have here is stronger since we ensure that the source and the selected helper will use the optimal power allocation without any additional cost in complexity that could be incurred, for example, by using a numerical algorithm to compute the optimal power values. Clearly, by Theorem 2 where we have derived the optimal power allocation policy for the single helper problem in closed-form, there is no additional cost in complexity.

Now, we turn our attention to the multiple deaf helper selection problem. Let $\mathcal{K}^{CJ}, \mathcal{K}^{NF} \subseteq \mathcal{N}$ be disjoint sets of cooperative jammers and noise forwarders, respectively. Let $i = |\mathcal{K}^{CJ} \bigcup \mathcal{K}^{NF}|$ and $j = |\mathcal{K}^{NF}|$. Consider the expression in (40) for the achievable rate $R(\mathcal{K}^{CJ}, \mathcal{K}^{NF})$. It is clear that the number of all subsets $\mathcal{M} \subseteq \mathcal{K}^{NF}$ is 2^j. Hence, the minimization in (40) is taken over 2^j values. On the other hand, for each $\mathcal{M} \subseteq \mathcal{K}^{NF}$, the evaluation of the expression inside the $\min$ in (40) requires $O(i)$ computations since there are i terms involved in the computation of this expression. For simplicity, we will assume that the number of computations is i rather than $O(i)$ since this will not affect the overall complexity order. Finding the minimum of 2^j values requires $O(2^j)$ computations (again, for simplicity, we will assume that this requires 2^j computations). Thus, the evaluation of $R(\mathcal{K}^{CJ}, \mathcal{K}^{NF})$ requires a total of $2^j(i+1)$ computations.

As shown earlier in Section V.C, our multiple relay selection problem is at least as hard as an integer programming problem which is generally known to be NP-hard. Hence, it is reasonable to assume that the optimal strategy would require computing the rates achieved by all the possible pairs of disjoint subsets $\mathcal{K}^{CJ}, \mathcal{K}^{NF} \subseteq \mathcal{N}$ where $|\mathcal{K}^{CJ} \bigcup \mathcal{K}^{NF}| \leq K$. On the other hand, our MDHS strategy avoids computing the achievable rates for all such pairs due to its greedy nature. In the next theorem, we quantify the complexity of both strategies, i.e., the optimal strategy and our MDHS strategy, and show the substantial reduction in complexity that is achieved by using our MDHS strategy compared to the optimal strategy. The next theorem distinguishes between two cases in the complexity analysis of the strategies. In the first case, K is a fixed constant that is not allowed to grow with N. Whereas, in the second case, K is a fixed fraction of N, i.e., $\frac{K}{N} = \alpha$ for some rational $\alpha \in (0, 1]$.

Theorem 3: Let $\mathcal{C}_o(N)$ be the complexity of the optimal strategy that selects $K > 1$ deaf helpers out of N available relay nodes as described above. We assume that the optimal strategy requires computing the rates achieved by all the possible pairs of disjoint subsets $\mathcal{K}^{CJ}, \mathcal{K}^{NF} \subseteq \mathcal{N}$ where $|\mathcal{K}^{CJ} \bigcup \mathcal{K}^{NF}| \leq K$. Let $\mathcal{C}_{\mathrm{MDHS}}(N)$ be the complexity of the MDHS strategy of Section V.D. Define the complexity reduction ratio as $\Gamma(N) \triangleq \frac{\mathcal{C}_o(N)}{\mathcal{C}_{MDHS}(N)}$. For any $K, N, 1 < K \leq N$, we have

$$\mathcal{C}_o(N) = \sum_{i=1}^{K} \binom{N}{i} (i+1)3^i \tag{41}$$

$$\mathcal{C}_{\mathrm{MDHS}}(N) \leq \sum_{i=1}^{K} (N-i+1)(1+2^{i+1}(i+1)) \tag{42}$$

If $K > 1$ is a fixed constant (i.e., it does not depend on N), then

$$\mathcal{C}_o(N) \text{ is } \Omega(N^K) \quad \text{and} \quad \mathcal{C}_{\mathrm{MDHS}} \text{ is } O(N) \tag{43}$$

$$\text{Hence,} \quad \Gamma(N) \text{ is } O(N^{K-1}) \tag{44}$$

On the other hand, if K is a fixed fraction of N, i.e., $\frac{K}{N} = \alpha$ for some rational $\alpha \in (0, 1]$, then

$$\mathcal{C}_o(N) \text{ is } \Omega(N 2^{\alpha N \log\left(\frac{3}{\alpha}\right)}) \quad \text{and} \quad \mathcal{C}_{\mathrm{MDHS}} \text{ is } O(N^2 2^{\alpha N}) \tag{45}$$

$$\text{Hence,} \quad \Gamma(N) \text{ is } O\left(\frac{2^{\alpha N \log\left(\frac{3}{2\alpha}\right)}}{N}\right) \tag{46}$$

Proof: First, consider the complexity of the optimal selection strategy $\mathcal{C}_o(N)$. The number of subsets $\mathcal{K}^{CJ}, \mathcal{K}^{NF}$ with $|\mathcal{K}^{CJ} \bigcup \mathcal{K}^{NF}| = i$ and $\mathcal{K}^{NF} = j$, for some $1 \leq i \leq K, 0 \leq j \leq i$, is $\binom{N}{i}\binom{i}{j}$. For each such pair of subsets, the evaluation of $R(\mathcal{K}^{CJ}, \mathcal{K}^{NF})$ requires $2^j(i+1)$ computations as discussed above. Thus, $\mathcal{C}_o(N)$ is given by $\mathcal{C}_o = \sum_{i=1}^{K} \sum_{j=0}^{i} \binom{N}{i}\binom{i}{j} 2^j (i+1)$ which reduces to (41). Next, consider the complexity of the MDHS strategy $\mathcal{C}_{\mathrm{MDHS}}$. Let $\mathcal{K}_i^{CJ}, \mathcal{K}_i^{NF}$ be the sets of cooperative jammers and noise forwarders selected by the end of the ith selection stage, $1 \leq i \leq t$ where $t \leq K$ is the termination stage. Note that the number of computations required to evaluate $R(\mathcal{K}_i^{CJ}, \mathcal{K}_i^{NF})$ is upper bounded by $2^i(i+1)$. Note also that the worst case for $\mathcal{C}_{\mathrm{MDHS}}$ is when $t = K$. The previous two facts will be used to obtain an upper bound on $\mathcal{C}_{\mathrm{MDHS}}$. Now, observe that at the ith selection stage of this strategy, each relay r of the $N-i+1$ remaining relays, that are not selected up till stage $i-1$, computes $R(\mathcal{K}_i^{CJ}, \mathcal{K}_i^{NF})$ twice. One time for the choice $\mathcal{K}_i^{CJ} = \mathcal{K}_{i-1}^{CJ} \bigcup \{r\}, \mathcal{K}_i^{NF} = \mathcal{K}_{i-1}^{NF}$, and another time for the choice $\mathcal{K}_i^{CJ} = \mathcal{K}_{i-1}^{CJ}, \mathcal{K}_i^{NF} = \mathcal{K}_{i-1}^{NF} \bigcup \{r\}$. Hence, the total number of computations executed by all such relays is upper bounded by $(N-i+1)2^{i+1}(i+1)$. The total number of computations carried out by the source to find the maximum of the rate values it receives from the $N-i+1$ relays is $N-i+1$. Therefore, the complexity of the MDHS strategy is upper bounded as in (42).

Now, suppose that $K > 1$ is a fixed constant. Thus, it is clear from (41) and (42) that $\mathcal{C}_o(N)$ is $\Omega(\binom{N}{K}) = \Omega(N^K)$ whereas $\mathcal{C}_{\mathrm{MDHS}}(N)$ is $O(N)$. Hence, (44) follows immediately. Next, suppose that $K = \alpha N$. Then, $\mathcal{C}_o(N)$ is lower bounded as $\mathcal{C}_o(N) = \sum_{i=1}^{\alpha N} \binom{N}{i}(i+1)3^i \geq \sum_{i=1}^{\alpha N} (\frac{3N}{i})^i (i+1) \geq \alpha N (\frac{3}{\alpha})^{\alpha N} = \alpha N 2^{\alpha N \log(\frac{3}{\alpha})}$ where the first inequality above follows from the fact that $\binom{N}{i} \geq (\frac{N}{i})^i, 1 \leq i \leq N$. On the other hand, from (42), it is easy to see that $\mathcal{C}_{\mathrm{MDHS}}(N)$ is $O(KN2^K)$ which, in this case, is $O(N^2 2^{\alpha N})$. This proves (45). It is easy to see that (46) follows immediately. ■

Indeed Theorem 3 quantifies the order of reduction in complexity obtained when our MDHS strategy is used compared to the case when the optimal selection strategy is used under the reasonable assumption that the optimal strategy has to compute the rates achieved by all the possible pairs of disjoint subsets of relays. Theorem 3 shows that the complexity reduction is of polynomial order, namely, $O(N^{K-1})$ when K is a fixed constant, and the reduction is of exponential order, namely, $O(\frac{2^{\alpha N \log(\frac{3}{2\alpha})}}{N})$ when $K = \alpha N$ for some rational $\alpha \in (0, 1]$. In fact, this implies that our MDHS strategy actually gives a substantial reduction in complexity and thus it operates significantly faster than the optimal strategy. For example, if $N = 50$ and $K = 25$, then using (41) and (42) above, one can compute a lower bound on the actual reduction ratio Γ (i.e., the worst case reduction ratio) which is approximately 2^{55} in this case. That is, our MDHS strategy runs approximately 2^{55} faster than the optimal strategy when $N = 50$ and $K = 25$. Consider another example where $N = 15$ and $K = 5$. In this case, the worst case reduction ratio is approximately 665, i.e., our MDHS strategy runs approximately 665 faster than the optimal strategy. One can notice that the reduction ratio has decreased substantially for smaller values of N and K, however, it is still large enough to make the MDHS strategy significantly faster than the optimal strategy.

VI. Numerical Examples

First, we consider the single deaf helper case. We compare the two modes of deaf cooperation and verify the conditions of Corollary 2 by plotting the optimal secrecy rate achievable by each of CJ and NF modes against the relative channel gain between the deaf helper and the eavesdropper, h_r.

In Fig. 2, we set the scaled power constraints of the source and the deaf helper defined in (6) as $\bar{P}_s = \bar{P}_r = 5$. We consider two cases. In the first case, we choose $h_s < 1$, namely, we set $h_s = 0.75$. In the second case, we choose $h_s > 1$, namely, $h_s = 1.25$. For each case, we plot $\bar{R}^{CJ}$ and $\bar{R}^{NF}$ versus the relative channel gain h_r. We observe that $\bar{R}^{CJ} = C^{GWT}$ when $h_r \leq \max(1, h_s)$ and $\bar{R}^{CJ} > C^{GWT}$ otherwise. One can also see that $\lim_{h_r \to \infty} \bar{R}^{CJ}(h_r) = C^G$ where C^G is the capacity of the Gaussian channel between the source and the destination when no secrecy constraint is imposed, i.e., when the eavesdropper is not present. On the other hand, we observe that $\bar{R}^{NF} = C^{GWT}$ when $h_r \geq \min(1, \frac{1+h_s\bar{P}_s}{1+\bar{P}_s})$ whereas $\bar{R}^{NF} > C^{GWT}$ otherwise.

Next, we consider the multiple deaf helper case. Consider a disk of radius 1 km where the source is located at the center, both the destination and the eavesdropper are located at some fixed points on the circumference. Consider N relays whose locations are chosen randomly and uniformly in this disk. Each channel gain is generated according to the formula: $\gamma = \frac{SV}{d^\alpha}$ where γ is the channel gain, S is a lognormal random variable to account for shadowing, and V is a Rayleigh random variable for fading, d is the distance, and α is the path loss. We assume that the underlying Gaussian random variables from which S and V are generated are independent, zero mean, and unit variance Gaussian random variables. We also take $\alpha = 3$. We set $\bar{\rho}_s = 10$ and $\bar{\rho}_r = 1 \forall r \in \mathcal{N}$.

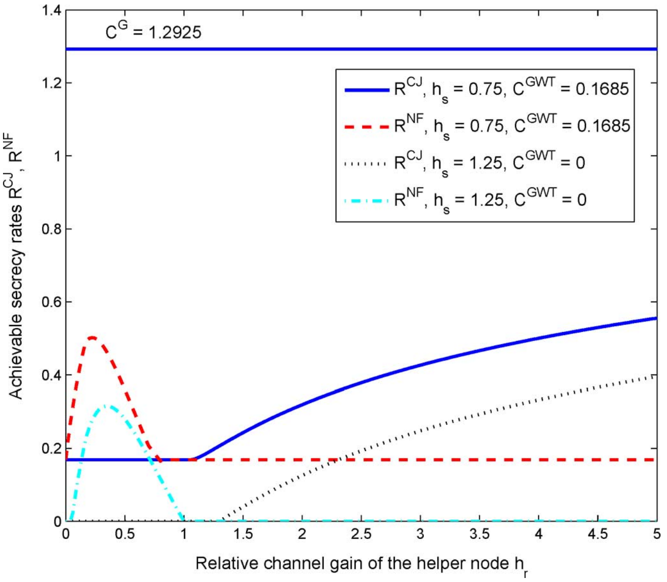

Fig. 2. The optimal achievable rates by the two modes of deaf cooperation, $\bar{R}^{CJ}$ and $\bar{R}^{NF}$ as functions of the relative channel gain from the deaf helper to the eavesdropper h_r, plotted for two cases of the relative channel gain from the source to the eavesdropper h_s.

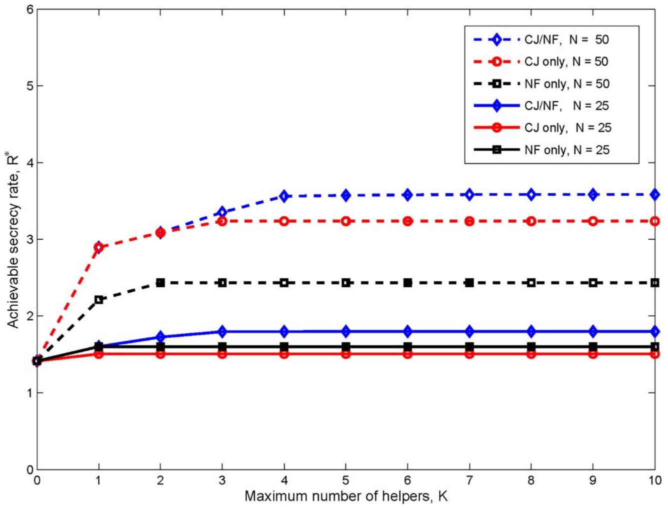

Fig. 3. The achievable secrecy rate, R^*, versus the maximum allowed number of deaf helpers, K, for three cases: CJ/NF, NF only, and CJ only. This is done for $N = 25$, and 50.

In Fig. 3, we plot the achievable secrecy rate against the maximum allowed number of helpers, K, for $N = 25$ and 50, in three different cases. In the first case, the secrecy rate is obtained using the MDHS strategy described in the previous section. In the second case, we only consider CJ as the only deaf cooperation mode, i.e., ignore all the relays that could be useful noise forwarders and use the MDHS strategy only for useful cooperative jammers. In the third case, we consider only NF as the only mode available for deaf cooperation. It is clear from Fig. 3 that making use of the two modes (CJ/NF) together in the system could significantly increase the achievable secrecy rates. Also, we notice that one could benefit from considering a larger set of relays, i.e., larger N, as this may lead to a better selected set of helpers.

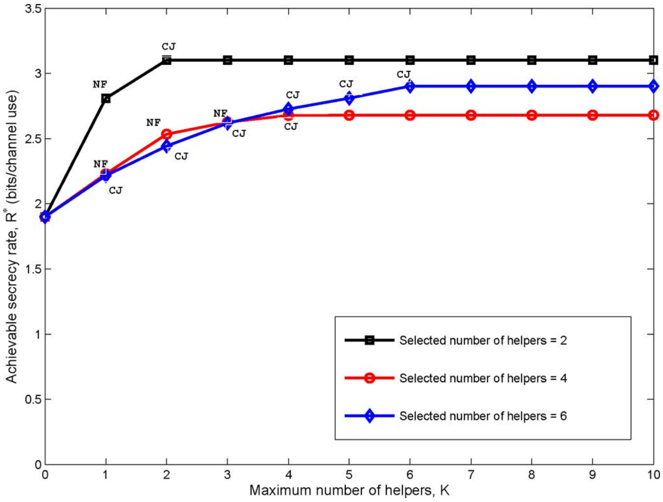

Fig. 4. The achievable secrecy rate versus the maximum allowed number of helpers, K, for three different realizations of relays locations, for $N = 50$.

In Fig. 4 the achievable secrecy rate, R^*, is plotted against the maximum allowed number of helpers, K, for three different realizations of the relays where $N = 50$. It can be seen that the selected helpers could be cooperative jammers (CJ) or noise forwarders (NF), or both, and that one can improve the achievable rate by selecting more than one helper. One can also see that the number of selected helpers could be less than K. Specifically, for the realizations considered here, the numbers of selected helpers are 2, 4, and 6.

VII. Conclusion

In this paper, we considered two modes of deaf cooperation for secrecy, CJ and NF. We gave the necessary and sufficient conditions for each of the two modes to yield higher secrecy rates than the secrecy capacity of the original GWT channel. We also showed that a node cannot be both useful jammer and noise forwarder at the same time. Moreover, we derived the optimal power control policy that maximizes the secrecy rate achieved by each of the two modes. For the deaf helper selection problem, we proposed an optimal strategy to select a single deaf helper that maximizes the secrecy rate achievable by deaf cooperation with a single helper. We also proposed a suboptimal strategy for the selection of multiple deaf helpers to increase the achievable secrecy rates. We discussed the complexity of the two proposed strategies. Finally, we gave numerical examples to verify our results.

Appendix
Proof of Theorem 1

First, we show that $R^{CJ}(P_s,P_r) \geq C^{GWT}(P_s)$ if and only if (10) or (11) holds. It is easy to see that if any of (10) and (11) holds, then $R^{CJ}(P_s,P_r) \geq C^{GWT}(P_s)$. Now, suppose that $R^{CJ}(P_s,P_r) \geq C^{GWT}(P_s)$, then from (7) and (9), we have $R^{CJ}(P_s,P_r) \geq \frac{1}{2}\log(\frac{1+P_s}{1+h_sP_s})$ and $R^{CJ}(P_s,P_r) \geq 0$ which imply

$$(h_sh_r - 1) + h_s(h_r - 1)P_s \geq h_r(1 - h_s)P_r \qquad (47)$$

$$h_s - 1 \leq (h_r - h_s)P_r \qquad (48)$$

Condition (48) implies $h_s \leq \max(1, h_r)$. On the other hand, we cannot have $\max(h_r, h_s) < 1$ since this contradicts (47). By considering the remaining possibilities, we either have

$$1 \leq h_s < h_r \qquad (49)$$

which directly implies (47), or we have

$$h_s < 1 \leq h_r \qquad (50)$$

which directly implies (48). Thus, if $R^{CJ}(P_s,P_r) \geq C^{GWT}(P_s)$, then we either have (47) and (50) satisfied together which is indeed condition (10), or we have (48) and (49) satisfied together which is condition (11).

Now, we prove the second part of Theorem 1. Again, it is easy to verify that if any of conditions (12)–(14) holds, then $R^{NF}(P_s,P_r) \geq C^{GWT}(P_s)$. Now, suppose that $R^{NF}(P_s,P_r) \geq C^{GWT}(P_s)$, then from (8) and (9), we have $R^{NF}(P_s,P_r) \geq \frac{1}{2}\log(\frac{1+P_s}{1+h_sP_s})$ and $R^{NF}(P_s,P_r) \geq 0$ which imply

$$(h_r - h_s)P_s \leq (1 - h_r) \qquad (51)$$

$$h_rP_r \geq h_s - 1 \qquad (52)$$

$$(1 - h_r)P_r \geq (h_s - 1)P_s \qquad (53)$$

Condition (53) implies that $\min(h_s, h_r) \leq 1$. On the other hand, we cannot have $h_s \leq 1 < h_r$ since this contradicts (51). Now, we consider the three remaining possible cases of relative channel gains. We either have

$$h_r \leq h_s \leq 1 \qquad (54)$$

which directly implies all the conditions (51)–(53) above, or we have

$$h_s < h_r \leq 1 \qquad (55)$$

which directly implies both conditions (52) and (53), or we have

$$h_r < 1 \leq h_s \qquad (56)$$

which directly implies condition (51). Thus, if $R^{NF}(P_s,P_r) \geq C^{GWT}(P_s)$, we either have condition (54) satisfied which is indeed condition (12), or we have conditions (51) and (55) both satisfied which is the same as (13), or we have conditions (52),(53), and (56) satisfied together which is the same as (14).

Appendix
Proof of Theorem 2

We define $f^{CJ}(P_s,P_r) \triangleq \frac{(1+P_s+P_r)(1+h_rP_r)}{(1+h_sP_s+h_rP_r)(1+P_r)}$, $f_1^{NF}(P_s,P_r) \triangleq \frac{(1+P_s)(1+h_rP_r)}{(1+h_sP_s+h_rP_r)}$, and $f_2^{NF}(P_s,P_r) \triangleq \frac{(1+P_s+P_r)}{(1+h_sP_s+h_rP_r)}$. Hence, $R^{CJ}(P_s,P_r) = \frac{1}{2}\log(f^{CJ}(P_s,P_r))$, and $R^{NF}(P_s,P_r) = \min(\frac{1}{2}\log(f_1^{NF}(P_s,P_r)), \frac{1}{2}\log(f_2^{NF}(P_s,P_r)))$. We first consider the case where $h_r \geq 1$. Following Corollary 1, the NF strategy is not useful in this case, hence, in this case if $h_s < 1$ then $\hat{P}_s^{NF} = \bar{P}_s, \hat{P}_r^{NF} = 0$, otherwise $\hat{P}_s^{NF} = \bar{P}_s, \hat{P}_r^{NF} = 0$. This proves (18) and (29). On the other hand, if $1 \leq h_r \leq h_s$, then again following Corollary 1, both strategies are useless and we have $\hat{P}_s^{CJ} = \hat{P}_r^{CJ} = 0$ and $\hat{P}_s^{NF} = \hat{P}_r^{NF} = 0$.

This proves (33)–(34). The remaining possible cases where $h_r \geq 1$ are $h_s < 1 \leq h_r$ and $1 \leq h_s < h_r$, i.e., cases 1-(a) and 2-(a) in Theorem 2. Suppose that $h_s < 1 \leq h_r$. The derivatives $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_s}$ and $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_r}$ are given by $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_s} = \frac{(1-h_s+(h_r-h_s)P_r)(1+h_rP_r)}{(1+P_r)(1+h_sP_s+h_rP_r)^2}$ and $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_r} = \frac{(h_r(h_s-h_r)P_r^2+2h_r(h_s-1)P_r)P_s}{(1+P_r)^2(1+h_sP_s+h_rP_r)^2} + \frac{(h_s(h_r(1+P_s)-P_s)-1)P_s}{(1+P_r)^2(1+h_sP_s+h_rP_r)^2}$. We note that $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_s} > 0, \forall P_s, P_r$. Moreover, $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_r}$ has two zeros, one of them is at $P_r = P_r^*$ where P_r^* is given by (35) which turns out to be the unconstrained global maximum of $f^{CJ}(\bar{P}_s, P_r)$. Thus, the optimal power values $\hat{P}_s^{CJ}$ and $\hat{P}_r^{CJ}$ are given by (17). Suppose now that $1 \leq h_s < h_r$. If $\bar{P}_r \leq \frac{h_s-1}{h_r-h_s}$, then from condition (11) in Theorem 1, we must have $\hat{P}_s^{CJ} = \hat{P}_r^{CJ} = 0$ since $h_s \geq 1$. Otherwise, suppose that $\bar{P}_r > \frac{h_s-1}{h_r-h_s}$. First, note that for all P_s, $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_s} > 0$ if $P_r > \frac{h_s-1}{h_r-h_s}$. On the other hand, $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_r}$ has two zeros, one of them is the unconstrained global maximizer of $f^{CJ}(P_s, P_r)$ with respect to P_r for any given P_s. Moreover, for all P_s, this unconstrained global maximizer is greater than $\frac{h_s-1}{h_r-h_s}$. Noting that the value of such unconstrained global maximizer at $P_s = \bar{P}_s$ is P_r^*, we conclude that $\hat{P}_r^{CJ} = \min(\bar{P}_r, P_r^*)$ and $\hat{P}_s^{CJ} = \bar{P}_s$ which proves (28).

Next, we consider then case where $h_r < 1$. By Corollary 1, the CJ strategy is not useful in this case, hence, in this case if $h_s < 1$ then $\hat{P}_s^{CJ} = \bar{P}_s, \hat{P}_r^{CJ} = 0$, otherwise, $\hat{P}_s^{CJ} = \hat{P}_r^{CJ} = 0$. This proves (19), (23), and (30). The remaining possible cases where $h_r < 1$ are $h_s < h_r < 1$, $h_r \leq h_s < 1$, and $h_r < 1 \leq h_s$, i.e., cases 1-(b), 1-(c), and 2-(b) in Theorem 2. First, one can easily verify that

$$f_1^{NF}(P_s, P_r) \leq f_2^{NF}(P_s, P_r) \\ \text{if and only if } P_s \leq \tfrac{1-h_r}{h_r} \quad (57)$$

We also have $\frac{\partial f_1^{NF}(P_s,P_r)}{\partial P_s} = \frac{(1-h_s+h_rP_r)}{(1+h_sP_s+h_rP_r)^2}$, $\frac{\partial f_1^{NF}(P_s,P_r)}{\partial P_r} = \frac{(h_sh_rP_s(1+P_s))}{(1+h_sP_s+h_rP_r)^2}$, $\frac{\partial f_2^{NF}(P_s,P_r)}{\partial P_s} = \frac{(1-h_s+(h_r-h_s)P_r)}{(1+h_sP_s+h_rP_r)^2}$, and $\frac{\partial f_2^{NF}(P_s,P_r)}{\partial P_r} = \frac{(1-h_r+(h_s-h_r)P_s)}{(1+h_sP_s+h_rP_r)^2}$. Now, suppose first that $h_s < h_r < 1$. We note that $\frac{\partial f_1^{NF}(P_s,P_r)}{\partial P_s}$ and $\frac{\partial f_2^{NF}(P_s,P_r)}{\partial P_s}$ are positive for all P_s, P_r. Hence, we must have $\hat{P}_s^{NF} = \bar{P}_s$. On the other hand, $\frac{\partial f_1^{NF}(P_s,P_r)}{\partial P_r} > 0$ is positive for all P_s, P_r while $\frac{\partial f_2^{NF}(P_s,P_r)}{\partial P_r} > 0$ if and only if $\bar{P}_s < \frac{1-h_r}{h_r-h_s}$. Hence, if $\bar{P}_s < \frac{1-h_r}{h_r-h_s}$, then $\hat{P}_r^{NF} = \bar{P}_r$. If $\bar{P}_s \geq \frac{1-h_r}{h_r-h_s}$, then from (57), (8), and by noting that $\frac{1-h_r}{h_r} > \frac{1-h_r}{h_s-h_r}$, we must have $\hat{P}_r^{NF} = 0$. This proves (20)–(22). Suppose now that $h_r \leq h_s < 1$. In this case, $\frac{\partial f_1^{NF}(P_s,P_r)}{\partial P_r}$ and $\frac{\partial f_2^{NF}(P_s,P_r)}{\partial P_r}$ are positive for all P_s, P_r. Thus, both $f_1^{NF}(P_s, P_r)$ and $f_2^{NF}(P_s, P_r)$ are increasing in P_r for any given value of P_s, hence their minimum is also increasing in P_r. Thus, $\hat{P}_r^{NF} = \bar{P}_r$ which proves (26). Now, if $\bar{P}_r < \frac{1-h_s}{h_s-h_r}$, then $\frac{\partial f_1^{NF}(P_s,P_r)}{\partial P_s}$ and $\frac{\partial f_2^{NF}(P_s,P_r)}{\partial P_s}$ are both positive. Hence, $\hat{P}_s^{NF} = \bar{P}_s$ which proves (24). If $\bar{P}_r \geq \frac{1-h_s}{h_s-h_r}$, then one can verify that $f_1^{NF}(P_s, \bar{P}_r)$ is increasing in P_s while $f_2^{NF}(P_s, P_r)$ is decreasing in P_s. Thus, the unconstrained global maximizer of their minimum is the point where they are equal, i.e., $P_s = \frac{1-h_r}{h_r}$. Hence, $\hat{P}_s^{NF} = \min(\bar{P}_s, \frac{1-h_r}{h_r})$ which proves (25). Finally, suppose that $h_r < 1 \leq h_s$. If $\bar{P}_r \leq \frac{h_s-1}{h_r}$, then from condition (14) in Theorem 1, we must have $\hat{P}_s^{NF} = \hat{P}_r^{NF} = 0$ since $h_s \geq 1$, which proves (31). If $\bar{P}_r > \frac{h_s-1}{h_r}$, then again in this case $\frac{\partial f_1^{NF}(P_s,P_r)}{\partial P_r}$ and $\frac{\partial f_2^{NF}(P_s,P_r)}{\partial P_r}$ are positive for all P_s and P_r. Thus, arguing as above, we conclude that $\hat{P}_r^{NF} = \bar{P}_r$. On the other hand, $\frac{\partial f_1^{NF}(P_s,\bar{P}_r)}{\partial P_s} > 0$ while $\frac{\partial f_2^{NF}(P_s,\bar{P}_r)}{\partial P_s} < 0$. Thus, again by arguing as above, we must have $\hat{P}_s^{NF} = \min(\bar{P}_s, \frac{1-h_r}{h_r})$ which proves (32).

References

[1] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Technol. 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. Commun., Contr., Comput.*, Monticello, IL, Sep. 2006.

[3] E. Tekin and A. Yener, "The Gaussian multiple access wiretap channel," *IEEE Trans. Inf. Theory*, vol. 54, 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, pp. 2735–2751, Jun. 2008.

[5] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secret communication," in *Proc. IEEE Inf. 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, pp. 5059–5067, Nov. 2008.

[7] E. Perron, S. Diggavi, and E. Telatar, "On cooperative secrecy for discrete memoryless relay networks," in *Proc. IEEE ISIT 2010*, Austin, TX, Jun. 2010, pp. 2573–2577.

[8] I. Krikidis, J. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, pp. 5003–5011, Oct. 2009.

[9] 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.

[10] 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

[11] 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.

[12] 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.

[13] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proc. 15th IEEE Workshop on Statist. Signal Process.*, Sep. 2009, pp. 417–420.

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

[15] 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.

[16] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani, "Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper," in *Proc. IEEE ICC 2011*, Kyoto, Japan, Jun. 2011.

[17] L. Lai and H. E. Gamal, "Cooperation for secrecy: The relay-eavesdropper channel," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4005–4019, Sep. 2008.

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

[19] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Jan. 1975.

[20] E. Ekrem and S. Ulukus, "Cooperative secrecy in wireless communications," in *Securing Wireless Communications at the Physical Layer*, W. Trappe and R. Liu, Eds. New York, NY, USA: Springer-Verlag, 2009.

[21] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, Jul. 1978.

Raef Bassily (S'11–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 (UMD) at College Park in 2011.

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

Sennur Ulukus (S'90–M'98) received the B.S. and M.S. degrees in electrical and electronics engineering from Bilkent University, and the Ph.D. degree in electrical and computer engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, New Brunswick, NJ.

She is a Professor of Electrical and Computer Engineering at the University of Maryland (UMD) 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 with AT&T Labs-Research. 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 2007–2010, for the IEEE TRANSACTIONS ON COMMUNICATIONS between 2003–2007, as a Guest Editor for the *Journal of Communications and Networks* for the 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 Co-Chair 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, 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.