Deaf Cooperation for Secrecy in Multiple-Relay Networks

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

***Abstract*—In this paper, we investigate the roles of cooperative jamming (CJ) and noise forwarding (NF) in improving the achievable secrecy rates of a Gaussian wiretap channel (GWT). 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 study the conditions in which each mode of deaf cooperation improves over the secrecy capacity of the original wiretap channel. 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 with deaf cooperation using K relays. First, we give an optimal strategy for the case of $K = 1$, i.e., for the selection of a single deaf helper. We propose a suboptimal strategy for selection in the general case where $K > 1$. We discuss the complexity of each of the two strategies. Finally, we verify the performance of the proposed strategies through numerical examples.**

I. Introduction

The notion of introducing artificial noise in a GWT channel by a helpful interferer to confuse the eavesdropper and improve over the secrecy capacity of the original wiretap channel was introduced in [1], [2], [3], [4]. In [2], [3], [4], this notion was called *cooperative jamming* (CJ). The term refers to the cooperation strategy in which a helping interferer transmits white Gaussian noise when it can hurt the eavesdropper more than it can hurt the legitimate receiver and hence improve the achievable secrecy rate. In [5], the idea of helping interferer was applied to the GWT channel in a scheme tantamount to the CJ scheme of 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 fact the role of a helping node in improving secrecy can be better understood in the relay-eavesdropper channel in which 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 [7]. In particular, reference [7] 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. 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 study and 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 [8] 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 [9].

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. 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.

Another problem that was presented in the literature was the problem of relay selection under a secrecy constraint in cooperative networks with multiple relays. For example, reference [10] proposes a scheme that enables an opportunistic selection of two relays to increase security where one relay uses DF strategy while the other uses CJ strategy to introduce useful interference and thus help increase the achievable secrecy rate.

In this paper, we consider applying both CJ and NF strategies in multiple-relay networks to improve secrecy rates

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

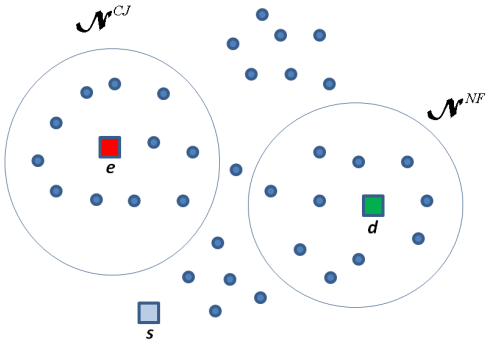

Fig. 1. A multiple-relay network.

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 propose an optimal Single Deaf Helper Selection (SDHS) strategy that identifies the optimal deaf helper node and its mode of cooperation (CJ or NF). Our strategy is simple and requires $O(N)$ computations. Second, we consider the general selection problem, i.e., the case where $K > 1$. Both the selection and the optimal power allocation problems are hard in this case. Therefore, we propose a suboptimal Multiple Deaf Helper Selection (MDHS) strategy that selects K (or less) relays over K (or less) selection stages in which the source and the relays negotiate to identify the deaf helpers to be selected one by one. We also show that the complexity of our strategy, compared to that of an optimal strategy, is reduced by an exponential factor for N large enough. 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), $\mathcal{N} = \{r_1, ..., r_N\}$, from which one is selected to help improve the achievable perfect secrecy through deaf cooperation, i.e., CJ or NF (see Figure 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

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

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

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

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

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

$$Y = X_s + X_r + N \quad (4)$$

$$Z = \sqrt{h_s}X_s + \sqrt{h_r}X_r + N' \quad (5)$$

with

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

where $X_k \triangleq \gamma_{k,d}\tilde{X}_k$ 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, R^{CJ} is given by

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

Whereas the secrecy rate achievable by the NF scheme [7], R^{NF}, is given by

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

On the other hand, when no helper node is involved, the secrecy capacity of the original GWT channel [11] for a given power value P_s is given by

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

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 $h_s < 1 \leq h_r,\ (h_s h_r - 1) + h_s(h_r - 1)P_s \geq h_r(1 - h_s)P_r$, or, $1 \leq h_s < h_r,\ P_r \geq \frac{h_s - 1}{h_r - h_s}$. On the other hand, $R^{NF}(P_s, P_r) \geq C^{GWT}(P_s)$ if and only if $h_r \leq h_s \leq 1$, or, $h_s < h_r \leq 1,\ P_s \leq \frac{1 - h_r}{h_r - h_s}$, or, $h_r < 1 \leq h_s,\ P_r \geq \max\left(\frac{h_s - 1}{h_r}, \frac{h_s - 1}{1 - h_r} P_s\right)$.

One important observation one can make in regard with Theorem 1 is that the CJ strategy cannot be beneficial, i.e., achieves 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 $h_r > 1$.

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 solution of the following optimization problems.

$$\max_{P_s, P_r} R^{CJ}(P_r, P_s) \quad \text{s.t.} \quad 0 \leq P_s \leq \bar{P}_s,\ 0 \leq P_r \leq \bar{P}_r \quad (10)$$

$$\max_{P_s, P_r} R^{NF}(P_r, P_s) \quad \text{s.t.} \quad 0 \leq P_s \leq \bar{P}_s,\ 0 \leq P_r \leq \bar{P}_r \quad (11)$$

Let $(\hat{P}_s^{CJ}, \hat{P}_r^{CJ})$ be the maximizer of (10) and $(\hat{P}_s^{NF}, \hat{P}_r^{NF})$ be the maximizer of (11). 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 (10) and (11) above is given in the following cases:

1) If $h_s < 1 \leq h_r$: $\hat{P}_s^{CJ} = \bar{P}_s$. $\hat{P}_r^{CJ} = \left(\min\left(\bar{P}_r, P_r^*\right)\right)^+$. $\hat{P}_s^{NF} = \bar{P}_s$. $\hat{P}_r^{NF} = 0$.
2) If $h_s < h_r < 1$: $\hat{P}_s^{CJ} = \bar{P}_s$. $\hat{P}_r^{CJ} = 0$. $\hat{P}_s^{NF} = \bar{P}_s$. $\hat{P}_r^{NF} = \bar{P}_r$ if $\bar{P}_s < \frac{1 - h_r}{h_r - h_s}$. $\hat{P}_r^{NF} = 0$ if $\bar{P}_s \geq \frac{1 - h_r}{h_r - h_s}$.
3) If $h_r \leq h_s < 1$: $\hat{P}_s^{CJ} = \bar{P}_s$. $\hat{P}_r^{CJ} = 0$. $\hat{P}_s^{NF} = \bar{P}_s$ if $\bar{P}_r < \frac{1 - h_s}{h_s - h_r}$. $\hat{P}_s^{NF} = \min\left(\bar{P}_s, \frac{1 - h_r}{h_r}\right)$ if $\bar{P}_r \geq \frac{1 - h_s}{h_s - h_r}$. $\hat{P}_r^{NF} = \bar{P}_r$.
4) If $1 \leq h_s < h_r$: $\hat{P}_s^{CJ} = 0$ and $\hat{P}_r^{CJ} = 0$ if $\bar{P}_r \leq \frac{h_s - 1}{h_r - h_s}$. $\hat{P}_s^{CJ} = \bar{P}_s$ and $\hat{P}_r^{CJ} = \min\left(\bar{P}_r, P_r^*\right)$ if $\bar{P}_r > \frac{h_s - 1}{h_r - h_s}$. $\hat{P}_s^{NF} = 0$. $\hat{P}_r^{NF} = 0$.
5) If $h_r < 1 \leq h_s$: $\hat{P}_s^{CJ} = 0$. $\hat{P}_r^{CJ} = 0$. $\hat{P}_s^{NF} = 0$ and $\hat{P}_r^{NF} = 0$ if $\bar{P}_r \leq \frac{h_s - 1}{h_r}$. $\hat{P}_s^{NF} = \min\left(\bar{P}_s, \frac{1 - h_r}{h_r}\right)$ and $\hat{P}_r^{NF} = \bar{P}_r$ if $\bar{P}_r > \frac{h_s - 1}{h_r}$.
6) If $1 \leq h_r \leq h_s$: $\hat{P}_s^{CJ} = 0$. $\hat{P}_r^{CJ} = 0$. $\hat{P}_s^{NF} = 0$. $\hat{P}_r^{NF} = 0$.

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

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

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

$$R^{CJ}(\rho_s, \rho_r) = \frac{1}{2} \log\left(\frac{(1 + \gamma_{s,d}\rho_s + \gamma_{r,d}\rho_r)(1 + \gamma_{r,e}\rho_r)}{(1 + \gamma_{s,e}\rho_s + \gamma_{r,e}\rho_r)(1 + \gamma_{r,d}\rho_r)}\right) \quad (12)$$

$$R^{NF}(\rho_s, \rho_r) = \min\left\{\frac{1}{2} \log\left(\frac{(1 + \gamma_{s,d}\rho_s)(1 + \gamma_{r,e}\rho_r)}{1 + \gamma_{s,e}\rho_s + \gamma_{r,e}\rho_r}\right), \frac{1}{2} \log\left(\frac{1 + \gamma_{s,d}\rho_s + \gamma_{r,d}\rho_r}{1 + \gamma_{s,e}\rho_s + \gamma_{r,e}\rho_r}\right)\right\} \quad (13)$$

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 (12) and (13), respectively. Hence, using Corollary 1, one can find two disjoint subsets of $\mathcal{N}$ which we denote by $\mathcal{N}^{CJ}$ and $\mathcal{N}^{NF}$, where

$$\mathcal{N}^{CJ} \triangleq \left\{r_j \in \mathcal{N} : \frac{\gamma_{r_j,e}}{\gamma_{r_j,d}} > \max\left(1, \frac{\gamma_{s,e}}{\gamma_{s,d}}\right)\right\} \quad (14)$$

is the set of potential cooperative jammers, and

$$\mathcal{N}^{NF} \triangleq \left\{r_j \in \mathcal{N} : \frac{\gamma_{r_j,e}}{\gamma_{r_j,d}} < \min\left(1, \frac{1 + \gamma_{s,e}\bar{\rho}_s}{1 + \gamma_{s,d}\bar{\rho}_s}\right)\right\} \quad (15)$$

is the set of potential noise forwarders. In other words, the set $\mathcal{N}^{CJ}$ is the set that contains every relay node that if acted as a cooperative jammer would, for appropriately allocated power, yield a secrecy rate that is greater than C^{GWT}. On the other hand, the set $\mathcal{N}^{NF}$ is the set that contains every relay node that if acted as a noise forwarder would, for appropriately allocated power, yield a secrecy rate that is greater or equal to C^{GWT}. 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.

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 (14)-(15), 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.

Assuming that evaluating any of the rate or power functions given above requires $O(1)$ computations since computation is done in a distributed fashion over N relays, it follows that the complexity of the above strategy in terms of the number of computations required during its execution is $O(N)$. This is due to the fact that finding the maximum of all the rates received by s from all $r \in \mathcal{N}$ requires $O(N)$ computations.

B. 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

$$R(\mathcal{K}^{CJ}, \mathcal{K}^{NF}) = \min_{\mathcal{M}\subseteq\mathcal{K}^{NF}} \left\{ \frac{1}{2}\log\left(\frac{1+\gamma_{s,d}\rho_s+\sum_{r\in\mathcal{M}}\gamma_{r,d}\rho_r}{1+\sum_{r\in\mathcal{K}^{CJ}}\gamma_{r,d}\rho_r}\right) - \frac{1}{2}\log\left(\frac{1+\gamma_{s,e}\rho_s+\sum_{r\in\mathcal{M}}\gamma_{r,e}\rho_r}{1+\sum_{r\in\mathcal{K}^{CJ}}\gamma_{r,e}\rho_r+\sum_{r\in\mathcal{K}^{NF}\setminus\mathcal{M}}\gamma_{r,e}\rho_r}\right)\right\} \tag{16}$$

In fact, the problem of finding the optimal set of deaf helpers whose size is at most K is hard for $K > 1$ in general. Not only the selection problem is hard in this case, but also even if we fix K deaf helpers, $K > 1$, then the problem of finding the optimal power allocations becomes analytically intractable in this case. Consequently, no closed-form solutions could be found and we are left with search algorithms whose running time could be unacceptably large and their convergence to the global optimum is not even guaranteed. Hence, we propose below a suboptimal strategy that builds upon the SDHS strategy presented earlier to select at most K out of the available N relays that would possibly operate in different modes of cooperation to achieve larger secrecy rate.

Multiple Deaf Helpers Selection (MDHS) strategy: The strategy is carried out over at most K stages to select at most K deaf helpers. 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. For $2 \leq i \leq K$, fix the transmission powers as $\rho_s = \bar{\rho}_s$ and $\rho_r = \bar{\rho}_r,\ r \in \mathcal{N}$. For each $r \in \mathcal{N}\setminus\{r_j^* : 1 \leq j \leq i-1\}$, r computes the secrecy rate $R(\mathcal{K}^{CJ}, \mathcal{K}^{NF})$ given by (16) where $\mathcal{K}^{CJ}$ and $\mathcal{K}^{NF}$ are given by

$$\mathcal{K}^{CJ} = \left(\{r\} \cap \mathcal{N}^{CJ}\right) \bigcup \{r_j^*,\ 1 \leq j \leq i-1 : r_j^* \in \mathcal{N}^{CJ}\} \tag{17}$$

$$\mathcal{K}^{NF} = \left(\{r\} \cap \mathcal{N}^{NF}\right) \bigcup \{r_j^*,\ 1 \leq j \leq i-1 : r_j^* \in \mathcal{N}^{NF}\} \tag{18}$$

Then r sends the rate it computed to s. Hence, 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 $i-1$. Otherwise, s identifies the relay r_i^* corresponding to the rate R_i^* and its mode of cooperation. Upon termination at stage t, $1 \leq t \leq K$, 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^*.

To derive the complexity of the MDHS strategy above, first, we note that in the ith selection stage in order to evaluate the rate in (16) where $\mathcal{K}^{CJ}$ and $\mathcal{K}^{NF}$ are given by (17) and (18), respectively, each relay $r \in \mathcal{N}$ has to find the minimum of 2^i terms. The evaluation of each of these terms is assumed to involve i computations. Thus, each relay $r \in \mathcal{N}$ performs $i2^i$ computations to evaluate the rate in (16). At the source s, finding the maximum rate R_i^* requires about N computations and comparing R_i^* with R_{i-1}^* requires a single computation. Thus, the ith stage of the MDHS strategy requires $N+i2^i+1$ computations. Note that each relay $r \in \mathcal{N}$ computes the rate in (16) on its own, i.e., the computation of all the rates is done in a distributed fashion over the N relays in every stage of the strategy. That is why the term $i2^i$ is not scaled by N. Since there are at most K selection stages in the MDHS strategy, in the worst case, the total number of computations required in the execution of the MDHS strategy is $K(2^{K+1}+N+1) - 2^{K+1} + 2$ which is indeed $O(K(2^K+N))$. On the other hand, an optimal strategy that computes the achievable secrecy rate using every possible set of relays $\mathcal{M} \subseteq \mathcal{N}$ with $|\mathcal{M}| \leq K$, then finding the maximum rate together with the optimal relay assignment would require $\sum_{i=1}^{K}\left(\binom{N}{i} i2^i + \binom{N}{i} + 1\right)$ computa-

tions. More loosely, the number of required computations is $O(2^{\alpha N} K 2^K)$ where $\alpha = H(\frac{K}{N})$, if $\frac{K}{N} < \frac{1}{2}$, and $\alpha = 1$, otherwise, where $H(.)$ is the binary entropy function. Clearly, the MDHS strategy requires much less computations. In particular, for N large enough, the reduction in complexity becomes exponential in N.

VI. Numerical Examples

We 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. We 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 $\bar{\rho}_r = 1 \ \forall r \in \mathcal{N}$. In Figure 2, we plot the achievable secrecy

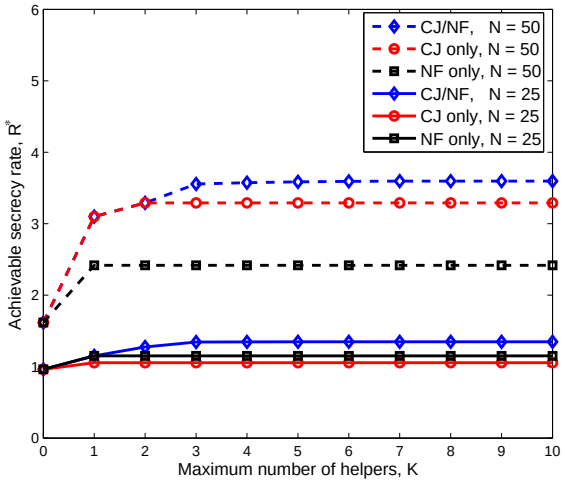

Fig. 2. The achievable secrecy rate, R^*, versus the maximum allowed number of deaf helpers, K, for three cases: CJ/NF, NF only, and CJ only. This is done for $N = 25$, and 50.

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 in $\mathcal{N}^{NF}$ and use the MDHS strategy for the nodes in $\mathcal{N}^{CJ}$ only. In the third case, we consider only NF as the only mode available of deaf cooperation. It is clear from Figure 2 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. In Figure 3 the achievable secrecy

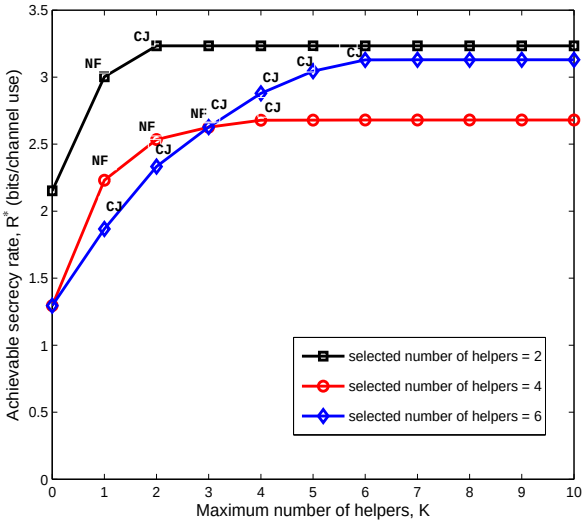

Fig. 3. The achievable secrecy rate versus the maximum allowed number of helpers, K, for three different realizations of relays locations, for $N = 50$.

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.

References

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

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

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

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

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

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

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

[8] A. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, Jan. 1975.

[9] E. Ekrem and S. Ulukus. Cooperative secrecy in wireless communications. *Securing Wireless Communications at the Physical Layer*. W. Trappe and R. Liu, Eds., Springer-Verlag, 2009.

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

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