

Cooperative Secrecy: The Relay-Eavesdropper Channel

Lifeng Lai and Hesham El Gamal
Department of Electrical and Computer Engineering
Ohio State University
Columbus, OH 43202, USA
Email: {lail,helgamal}@ece.osu.edu

Abstract—“THIS PAPER IS ELIGIBLE FOR THE STUDENT PAPER AWARD”. This paper investigates the role of user cooperation in facilitating secure wireless communications. In particular, the four-terminal relay-eavesdropper channel is introduced and an outer-bound on the rate-equivocation region is derived. Several cooperation strategies are devised and the corresponding achievable rate-equivocation region are characterized. Of particular interest is the novel Noise-Forwarding (NF) strategy, where the relay node sends codewords independent of the source message to confuse the eavesdropper. This strategy is used to illustrate the deaf helper phenomenon, where the relay is able to facilitate secure communications while being totally ignorant of the transmitted messages. Furthermore, NF is shown to increase the perfect secrecy rate in the reversely degraded scenario, where the relay node fails to offer performance gains in the classical setting. The gain offered by the proposed cooperation strategies is then proved theoretically and validated numerically in the additive White Gaussian Noise (AWGN) channel.

I. INTRODUCTION

The notion of information theoretic secrecy was introduced by Shannon in [1], which assumed that the transmission is noiseless and used a key K to protect the confidential message W . Taking the transmission uncertainty into consideration, Wyner introduced the wiretap channel in [2]. In the three-terminal wiretap channel, a source wishes to transmit confidential messages to a destination while keeping the messages as secret as possible from a wiretapper. The wiretapper is assumed to have an unlimited computation ability and to know the coding/decoding scheme used in the main (source-destination) channel. Under the assumption that the source-wiretapper channel is a degraded version of the main channel, Wyner characterized the trade-off between the throughput of the main channel and the level of ignorance of the message at the wiretapper using the rate-equivocation region concept. If the equivocation rate at the wiretapper is arbitrarily close to the information rate, the transmission is called perfectly secure. Csiszár and Körner further extended the study to the broadcast channel with confidential messages [3].

Our work here is motivated by the fact that if the wiretapper channel is less noisy than the main channel, the perfect secrecy capacity of the channel is zero [3]. In this case, it is infeasible to establish a secure link under Wyner’s wiretap channel model. Our main idea is to exploit user cooperation in facilitating the transmission of confidential messages from the source to the destination. More specially, we consider a four-terminal relay-eavesdropper channel, where a source wishes to send messages to a destination while leveraging the help of a relay node to hide those messages from the eavesdropper.

The eavesdropper in our model can be viewed as the wireless counterpart of Wyner’s wiretapper.

The relay channel without security constraints was studied under various scenarios [4], [5]. In most of these works, cooperation strategies were constructed to increase the transmission rate and/or reliability function. In this paper, we identify a novel role of the relay node in establishing a secure link from the source to the destination. Towards this end, several cooperation strategies for the relay-eavesdropper channel are constructed and the corresponding achieved rate-equivocation regions are characterized. An outer-bound on the rate-equivocation region is also derived. The proposed schemes are shown to achieve a positive perfect secrecy rate in several scenarios where the secrecy capacity in the absence of the relay node is zero. Quite interestingly, we establish the deaf-helper phenomenon where the relay can help while being totally ignorant of the transmitted message from the source. Furthermore, we show that the relay node can aid in the transmission of confidential messages in some settings where classical cooperation fails to offer performance gains, e.g., the reversely degraded relay channel.

The relay channel with confidential messages was studied in [6], where the relay node acts both as an eavesdropper and a helper. In the model of [6], the source sends common messages to the destination using the help of the relay node, but also sends private messages to the destination while keeping them secret from the relay. In contrast with [6], the relay node in our work acts as a trusted “third-party” whose sole goal is to facilitate secure communications. The idea of using a “third-party” to facilitate secure communications also appeared in [7]. Contrary to our work on noisy channels, [7] focused on the generation of common random secret keys at two nodes under the assist of a third-party using a noiseless public discussion channel. The users then use the secret key to establish a secure link between the source-destination pair. Other recent works on secure communications investigated the multiple access channel (MAC) with confidential messages [8], [9], the multiple access channel with a degraded wiretapper [10], etc.

Due to the space limit, we omit the proof of the results here. Interested readers can refer to [11] for details.

II. THE RELAY-EAVESDROPPER CHANNEL

We consider a four-terminal discrete channel consisting of finite sets $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}, \mathcal{Y}_1, \mathcal{Y}_2$ and a transition probability distribution $p(y, y_1, y_2 | x_1, x_2)$, as shown in Figure 1. Here, $\mathcal{X}_1, \mathcal{X}_2$ are the channel inputs from the source and the relay

respectively, while $\mathcal{Y}, \mathcal{Y}_1, \mathcal{Y}_2$ are the channel outputs at the destination, relay and eavesdropper respectively. We consider the memoryless channel. The source wishes to send the message $W_1 \in \mathcal{W}_1 = \{1, \dots, M\}$ to the destination using the (M, n) code consisting: 1) a stochastic encoder f_n at the source that maps the message w_1 to a codeword $\mathbf{x}_1 \in \mathcal{X}_1^n$, 2) a relay encoder that maps the signals $(y_{1,1}, y_{1,2}, \dots, y_{1,i-1})$ received before time i to the channel input $x_{2,i}$, 3) a decoding function $\phi: \mathcal{Y}^n \rightarrow \mathcal{W}_1$. The average error probability of a (M, n) code is defined as

$$P_e^n = \sum_{w_1 \in \mathcal{W}_1} \frac{1}{M} \Pr\{\phi(\mathbf{y}) \neq w_1 | w_1 \text{ was sent}\}.$$

The equivocation rate at the eavesdropper is defined as $R_e = \frac{1}{n} H(W_1 | \mathbf{Y}_2)$.

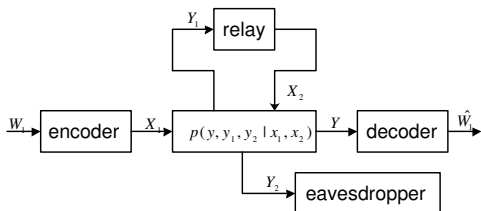


Fig. 1. The relay eavesdropper channel.

The rate-equivocation pair (R_1, R_e) is said to be achievable if for any $\epsilon > 0$, there exists a sequence of codes (M, n) such that for any $n \geq n(\epsilon)$, we have

$$R_1 = \frac{1}{n} \log_2 M, \quad P_e^n \leq \epsilon, \quad \frac{1}{n} H(W_1 | \mathbf{Y}_2) \geq R_e - \epsilon.$$

We further say that the perfect secrecy rate R_1 is achievable if the rate-equivocation pair (R_1, R_1) is achievable.

III. MAIN RESULTS

Our first result establishes an outer-bound on the optimal rate-equivocation region of the relay-eavesdropper channel.

Theorem 1: In the relay eavesdropper channel, for any rate-equivocation pair $\{R_1, R_e\}$ with $P_e^n \rightarrow 0$ and the equivocation rate at the eavesdropper larger than $R_e - \epsilon$, there exist some random variables $U \rightarrow (V_1, V_2) \rightarrow (X_1, X_2) \rightarrow (Y, Y_1, Y_2)$, such that (R_1, R_e) satisfies the following conditions

$$\begin{aligned} R_1 &\leq \min\{I(V_1, V_2; Y), I(V_1; Y, Y_1 | V_2)\}, \\ R_e &\leq R_1, \\ R_e &\leq [I(V_1, V_2; Y | U) - I(V_1, V_2; Y_2 | U)]^+. \end{aligned} \quad (1)$$

We now turn our attention to constructing cooperation strategies for the relay-eavesdropper channel. Our first step is to characterize the achievable rate-equivocation region of Cover-El Gamal Decode and Forward (DF) Strategy [4]. In DF cooperation strategy, the relay node will first decode codewords and then re-encode the message to cooperate with the source. Here, we use the regular coding and backward decoding scheme developed in the classical relay setting [5], [12], with the important difference that each message will be associated with many codewords in order to confuse the eavesdropper.

Theorem 2: The rate pairs in the closure of the convex hull of all (R_1, R_e) satisfying

$$\begin{aligned} R_1 &< \min\{I(V_1, V_2; Y), I(V_1; Y_1 | V_2)\}, \\ R_e &< R_1, \\ R_e &< [\min\{I(V_1, V_2; Y), I(V_1; Y_1 | V_2)\} - I(V_1, V_2; Y_2)]^+, \end{aligned} \quad (2)$$

for some distribution $p(v_1, v_2, x_1, x_2, y_1, y_2, y) = p(v_1, v_2)p(x_1, x_2 | v_1, v_2)p(y_1, y_2, y | x_1, x_2)$, are achievable using the DF strategy. Hence, for the DF scheme, the following perfect secrecy rate is achievable

$$R_s^{(DF)} = \sup_{p(v_1, v_2)} [\min\{I(V_1, V_2; Y), I(V_1; Y_1 | V_2)\} - I(V_1, V_2; Y_2)]^+.$$

The channel between the source and the relay becomes a bottleneck for the DF strategy when it is noisier than the source-destination channel. This motivates our Noise-Forwarding (NF) scheme, where the relay node does not attempt to decode the message but sends codewords that are independent of the source's message. The enabling observation behind this scheme is that, in the wiretap channel, in addition to its own information, the source should send extra codewords to confuse the wiretapper. In our setting, this task can be accomplished by the relay by allowing it to send independent codewords, which aid in confusing the eavesdropper.

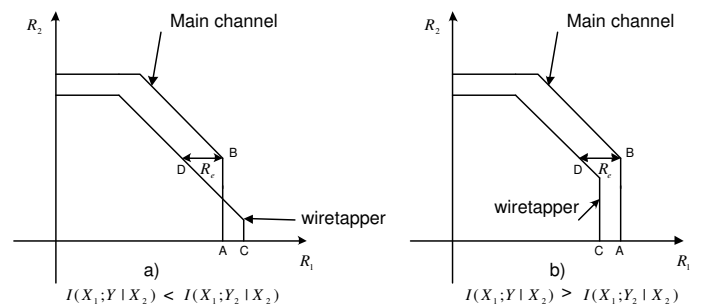


Fig. 2. The rate region of the compound MACs of the relay eavesdropper channel for a fixed input distribution $p(x_1)p(x_2)$.

Our NF scheme transforms the relay-eavesdropper channel into a compound multiple access channel (MAC), where the source/relay to the receiver is the first MAC and source/relay to the eavesdropper is the second one. Figure 2 shows the rate region of these two MACs for a fixed input distribution $p(x_1)p(x_2)$. In the figure, R_1 is the codeword rate of the source, and R_2 is the codeword rate of the relay. We can observe from Figure 2a) that if the relay node does not transmit, the perfect secrecy rate is zero for this input distribution since $R_1(A) < R_1(C)$. On the other hand, if the relay and the source coordinate their transmissions and operate at point B, we can achieve the equivocation rate R_e , which is strictly larger than zero. On the other hand, in Figure 2b), we can still get a positive perfect secrecy rate by operating at point A in the absence of the relay. But by moving the operating point to B, we can get a larger secrecy rate. This illustrates the main idea of our NF scheme.

Theorem 3: The rate pairs in the closure of the convex hull of all (R_1, R_e) satisfying

$$\begin{aligned} R_1 &< I(V_1; Y | V_2), \\ R_e &< R_1, \\ R_e &< [I(V_1; Y | V_2) + \min\{I(V_2; Y), I(V_2; Y_2 | V_1)\} \\ &\quad - \min\{I(V_2; Y), I(V_2; Y_2)\} - I(V_1; Y_2 | V_2)]^+, \end{aligned} \quad (3)$$

for some distribution $p(v_1, v_2, x_1, x_2, y_1, y_2, y) = p(v_1)p(v_2)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2, y|x_1, x_2)$, are achievable using the NF scheme. Hence, for the NF scheme, the achievable perfect secrecy rate is

$$R_s^{(NF)} = \sup_{p(v_1)p(v_2)} [I(V_1; Y|V_2) + \min\{I(V_2; Y), I(V_2; Y_2|V_1)\} - \min\{I(V_2; Y), I(V_2; Y_2)\} - I(V_1; Y_2|V_2)]^+.$$

In the NF scheme, the relay node does not need to listen to the source, and hence, this scheme is also suited for relay nodes limited by the half-duplex constraint [13], [14]. In NF cooperation, each user sends independent messages to the destination, which resembles the MAC. Hence, NF cooperation can be adapted to the multiple access eavesdropper channel where the multiple users in the MAC channel can help each other in communicating securely with the destination without listening to each other.

Now, we study another cooperation scheme that does not require decoding at the relay: Compress and Forward (CF). The CF cooperation strategy can be viewed as a generalization of NF where, in addition to the independent codewords, the relay also sends a quantized version of its noisy observations to the destination. This noisy version of the relay's observations helps the destination in decoding the source's message, while the independent codewords help in confusing the eavesdropper. The following result establishes the achievable rate-equivocation pair in the case when $I(X_1; \hat{Y}_1, Y|X_2) \leq I(X_1; \hat{Y}_1, Y_2|X_2)$, i.e., the source-eavesdropper channel is better than the source-receiver channel, a situation of particular interest to us.

Theorem 4: The rate pairs in the closure of the convex hull of all (R_1, R_e) satisfying

$$\begin{aligned} R_1 &< I(X_1; \hat{Y}_1, Y|X_2), \\ R_e &< R_1, \\ R_e &< \left[R_0 + I(X_1; \hat{Y}_1, Y|X_2) - I(X_1, X_2; Y_2) \right]^+, \end{aligned} \quad (4)$$

subject to $\min\{I(X_2; Y), I(X_2; Y_2|X_1)\} - R_0 \geq I(Y_1; \hat{Y}_1|X_2)$, for some distribution $p(x_1, x_2, y_1, y_2, y, \hat{y}_1) = p(x_1)p(x_2)p(y_1, y_2, y|x_1, x_2)p(\hat{y}_1|y_1, x_2)$ are achievable using CF strategy.

In Theorem 4, R_0 is the rate of pure noise generated by the relay to confuse the eavesdropper, while $\min\{I(X_2; Y), I(X_2; Y_2|X_1)\} - R_0$ is the part of the rate allocated to send the compressed signal \hat{Y}_1 to help the destination. If we set $R_0 = \min\{I(X_2; Y), I(X_2; Y_2|X_1)\}$, this scheme becomes the NF scheme. In order to enable analytical tractability, the coding/decoding scheme used in the proof is slightly different from that of [4]. In [4], the destination uses sliding-window decoding, while our proof uses backward decoding. Hence, the bound for R_e provided here is a lower-bound for the R_e achieved by the CF scheme. One may be able to achieve a larger R_e using exactly the CF scheme proposed in [4]. But, unfortunately, we are not yet able to bound R_e when sliding-window decoding is used. Compared with CF decoding, the proposed NF strategy enjoys the advantage of simplicity. Also, if one only focuses on the perfect secrecy rate, it is easy to see that these two schemes achieve identical performance. Again, this observation is limited to our lower bound on R_e in Theorem 4.

This section uses several examples to illustrate the unique features of the relay-eavesdropper channel. For simplicity, we only focus on the perfect secrecy rate of various schemes.

A. The Deaf Helper Phenomenon

The security constraints imposed on the network bring about a new phenomenon which we call the *deaf helper phenomenon*, where the relay node can still help even it is totally ignorant of the message transmitted from the source. In this setup, we impose an additional security constraint on the relay node, and say a rate R_s is achievable for a deaf helper if for any $\epsilon > 0$, there exists a sequence of codes (M, n) such that for any $n \geq n(\epsilon)$, we have

$$R_s = \frac{1}{n} \log_2 M, \quad P_e^n \leq \epsilon, \quad (5)$$

$$\frac{1}{n} H(W_1|Y_2) \geq R_s - \epsilon, \quad \frac{1}{n} H(W_1|Y_1, X_2) \geq R_s - \epsilon.$$

In this case, the signal received by the relay node does not leak any information about the transmitted message W_1 . This model describes a more conservative scenario where the source does not trust the relay but still wishes to exploit the benefit brought by cooperation. We assume that the relay node is not malicious and, hence, is willing to cooperate with the source. The following theorem characterizes the achievable perfect secrecy rate of the NF strategy in the deaf-helper setting.

Theorem 5: The perfect secrecy rate of the NF scheme with an additional security constraint on the relay node is $R_s = \max_{p(v_1)p(v_2)} \min\{R_{s1}, R_{s2}\}$, where

$$\begin{aligned} R_{s1} &= [I(V_1; Y|V_2) + \min\{I(V_2; Y), I(V_2; Y_2|V_1)\} \\ &\quad - \min\{I(V_2; Y), I(V_2; Y_2)\} - I(V_1; Y_2|V_2)]^+, \\ R_{s2} &= [I(V_1; Y|V_2) - I(V_1; Y_1|X_2)]^+. \end{aligned}$$

B. The Reversely Degraded Relay-Eavesdropper Channel

In the classical relay channel without security constraints, there exist some scenarios where the relay node does not provide any gain, for example, the reversely degraded relay channel shown in [4]. The relay channel is called reversely degraded, if $p(y, y_1|x_1, x_2) = p(y|x_1, x_2)p(y_1|y, x_2)$. Here, we focus on this scenario and show that the relay node can still offer a gain in the presence of the eavesdropper.

Theorem 2 of [4] shows that the capacity of the reversely degraded relay channel is $C_0 = \max_{x_2} \max_{p(x_1)} I(X_1; Y|x_2)$. This implies that the relay node should send a constant, and hence, does not contribute new information to the destination. In most channel models, the constant sent by the relay does not result in any capacity gain. The question now is whether the same conclusion holds in the presence of an eavesdropper. We first observe that the degradedness of the relay channel implies that DF and CF cooperation will not provide the destination with additional useful information. The relay node, however, can still send codewords independent of the received signal to confuse the eavesdropper, as proposed in the NF scheme. Since we do not require decoding at the relay node in NF, the degradedness imposed here does not affect the performance. Hence, we get the following achievable perfect secrecy rate for the reversely degraded relay-eavesdropper channel.

Corollary 1: The achievable perfect secrecy rate of the reversely degraded relay eavesdropper channel is

$$R_s = \max_{p(v_1)p(v_2)} [I(V_1; Y|V_2) + \min\{I(V_2; Y), I(V_2; Y_2|V_1)\} - \min\{I(V_2; Y), I(V_2; Y_2)\} - I(V_1; Y_2|V_2)]^+. \quad (6)$$

C. The AWGN Channel

Now we consider the Gaussian relay-eavesdropper channel, where the signal received at each node is $y_j[n] = \sum_{i \neq j} h_{ij}x_i[n] + z_j[n]$, here h_{ij} is the channel coefficient between node $i \in \{s, r\}$ and node $j \in \{r, w, d\}$, and z_j is the i.i.d Gaussian noise with unit variance at node j . The source and the relay have average power constraint P_1, P_2 respectively.

Applying the results of [9], [15], we know that the secrecy capacity of the Gaussian eavesdropper channel with the absence of the relay node is given by $\frac{1}{2} [\log_2(1 + |h_{sd}|^2 P_1) - \log_2(1 + |h_{sw}|^2 P_1)]^+$. Hence if $|h_{sw}|^2 \geq |h_{sd}|^2$ and the relay does not transmit, the secrecy capacity is zero, no matter how large P_1 is. On the other hand, as shown later, the relay can facilitate the source-destination pair to achieve a positive perfect secrecy rate under some conditions even when $|h_{sw}|^2 \geq |h_{sd}|^2$. In the following, we focus on such scenarios.

1) *DF and NF:* At this point, we do not know the optimal input distribution that maximizes $R_s^{(DF)}, R_s^{(NF)}$. Here, we let $V_1 = X_1, V_2 = X_2$ and use a Gaussian input distribution to obtain an achievable lower bound.

For DF cooperation scheme, we let $X_2 \sim \mathcal{N}(0, P_2), X_{10} \sim \mathcal{N}(0, P)$, where $\mathcal{N}(0, P)$ is the Gaussian distribution with zero mean and variance P . Also, we let $X_1 = c_1 X_2 + X_{10}$, where c_1 is a constant to be specified later. To satisfy the average power constraint at the source, we require $|c_1|^2 P_2 + P \leq P_1$.

Straightforward calculations show that

$$R_s^{(DF)} = \max_{c_1, P} \left[\min \left\{ \frac{1}{2} \log_2 \left(\frac{1 + |h_{sr}|^2 P}{1 + |h_{sw} c_1 + h_{rw}|^2 P_2 + |h_{sw}|^2 P} \right), \frac{1}{2} \log_2 \left(\frac{1 + |h_{sd} c_1 + h_{rd}|^2 P_2 + |h_{sd}|^2 P}{1 + |h_{sw} c_1 + h_{rw}|^2 P_2 + |h_{sw}|^2 P} \right) \right\} \right]^+. \quad (7)$$

For NF, we let $X_1 \sim \mathcal{N}(0, P_1), X_2 \sim \mathcal{N}(0, P_2)$. Here X_1, X_2 are independent, resulting in

$$R_s^{(NF)} = \left[\min \left\{ \frac{1}{2} \log_2 (1 + |h_{sd}|^2 P_1), \frac{1}{2} \log_2 \left(\frac{1 + |h_{sd}|^2 P_1 + |h_{rd}|^2 P_2}{1 + |h_{sw}|^2 P_1 + |h_{rw}|^2 P_2} \right), \frac{1}{2} \log_2 \left(\frac{(1 + |h_{rw}|^2 P_2)(1 + |h_{sd}|^2 P_1)}{1 + |h_{sw}|^2 P_1 + |h_{rw}|^2 P_2} \right) \right\} \right]^+.$$

2) *Amplify and Forward:* In this subsection, we quantify the achievable secrecy rate of Amplify and Forward (AF) cooperation. We did not consider this scheme in the discrete case since, in general, it does not lend itself to a single letter characterization. In AF, the source encodes its messages into codewords with length ML each, and divides each codeword into L sub-blocks each with M symbols, where L is chosen to be sufficiently large. At each sub-block, the relay sends a linear combination of the received noisy signal of this sub-block so far. For simplicity, we limit our discussion

to $M = 2$. In this case, the source sends $X_1(1)$ at the first symbol interval of each sub-block, the relay receives $Y_1(1) = h_{sr}X_1(1) + Z_1(1)$; At the second symbol interval, the source sends $\alpha X_1(1) + \beta X_1(2)$, while the relay sends $\gamma Y_1(1)$. Here α, β, γ are chosen to satisfy the average power constraints of the source and the relay. Thus, this scheme allows beam-forming between the source and relay without requiring the relay to fully decode. Writing the signal received at the destination and the eavesdropper in matrix form, we have $\mathbf{Y} = \mathbf{H}_1 \mathbf{X}_1 + \mathbf{Z}, \mathbf{Y}_2 = \mathbf{H}_2 \mathbf{X}_1 + \mathbf{Z}_2$, where

$$\mathbf{H}_1 = \begin{bmatrix} h_{sd} & 0 \\ \beta h_{sd} + \gamma h_{sr} h_{rd} & \alpha h_{sd} \end{bmatrix}, \mathbf{H}_2 = \begin{bmatrix} h_{sw} & 0 \\ \beta h_{sw} + \gamma h_{sr} h_{rw} & \alpha h_{sw} \end{bmatrix}, \\ \mathbf{X}_1 = [X_1(1), X_1(2)]^T, \mathbf{Z} = [Z(1), \gamma h_{rd} Z_1(1) + Z(2)]^T, \\ \mathbf{Z}_2 = [Z_2(1), \gamma h_{rw} Z_1(1) + Z_2(2)]^T, \\ \mathbf{Y} = [Y(1), Y(2)]^T, \mathbf{Y}_2 = [Y_2(1), Y_2(2)]^T.$$

The channel under consideration can be viewed as an equivalent standard memoryless eavesdropper channel with input \mathbf{X}_1 and outputs \mathbf{Y}, \mathbf{Y}_2 at the destination and the eavesdropper respectively. Then, based on the result of [3], an achievable perfect secrecy rate is $[I(\mathbf{X}_1; \mathbf{Y}) - I(\mathbf{X}_1; \mathbf{Y}_2)]^+$.

Choosing a Gaussian input with covariance matrix $\mathbb{E}\{\mathbf{X}\mathbf{X}^H\} = P\mathbf{I}$, where \mathbf{I} is the identity matrix, we get the following perfect secrecy rate

$$R_s^{(AF)} = \max_{\alpha, \beta, \gamma, P} \left[\frac{1}{4} \log_2 \frac{|\det\{P\mathbf{H}_1\mathbf{H}_1^H + \mathbf{A}\}\det\mathbf{B}|}{|\det\{P\mathbf{H}_2\mathbf{H}_2^H + \mathbf{B}\}\det\mathbf{A}|} \right]^+,$$

where

$$\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 + |\gamma h_{rd}|^2 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} 1 & 0 \\ 0 & 1 + |\gamma h_{rw}|^2 \end{bmatrix},$$

and the maximization is over the set of power constraints:

$$(1 + |\alpha|^2 + |\beta|^2)P \leq 2P_1, |\gamma|^2(|h_{sr}|^2 P + 1) \leq 2P_2.$$

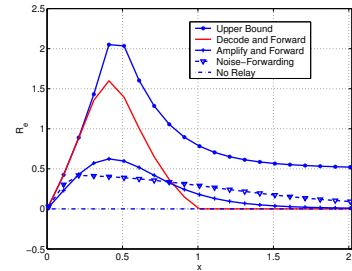


Fig. 3. The achievable perfect secrecy rate of the proposed schemes in the Gaussian relay eavesdropper channel.

3) *Numerical Results:* Here we give numerical results under two channel models. The first one is the real channel where $h_{ij} = d_{ij}^{-\gamma}$, with d_{ij} being the distance between node i and j and $\gamma > 1$ is the channel attenuation coefficient. In the second model, we assume that each channel experiences an independent phase fading, that is $h_{ij} = d_{ij}^{-\gamma} e^{j\theta_{ij}}$, where θ_{ij} is uniformly distributed over $[0, 2\pi)$.

Figure 3 shows the achievable perfect secrecy rate of the proposed schemes for the first channel model. In generating this figure, we use the network topology shown in Figure 4, where we put the source at $(0, 0)$, the destination at $(1, 0)$, the eavesdropper at $(0, 1)$, and the relay node at $(x, 0)$. We

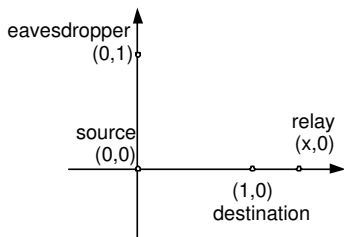


Fig. 4. The network topology.

let $P_1 = 1, P_2 = 8$. Since $d_{sd} = d_{sw}$, the perfect secrecy capacity of the eavesdropper channel without the relay node is zero. But, as shown in the figure, we can achieve a positive secrecy rate by introducing a relay node. In computing the upper-bound, we set $V_1 \sim \mathcal{N}(0, P_1), V_2 \sim \mathcal{N}(0, P_2)$ with a correlation coefficient ρ , and maximize over $\rho \in [-1, 1]$. Notice that the Gaussian input is not necessarily optimal for the upper-bound. We can see that, when the relay is near the source, the DF scheme touches the Gaussian upper-bound. Also, when $x > 1$, it is clear that DF cooperation does not offer any gain, while NF and AF still offer positive rates. Notice that when $x > 1$, both d_{sr}, d_{sd} are larger than d_{sw} . The interesting observation here is that though both the destination and relay are in disadvantage positions compared with the eavesdropper, they can cooperate with each other and gain some advantage over the eavesdropper. If the relay is at 0, our model is equivalent to the case where the source has two antennas. Notice that the upper-bound of the perfect secrecy capacity is zero under this scenario. Hence, increasing the number of transmitting antenna at the source does not increase the secrecy capacity under the real channel model. On the other hand, if there is a relay node at an appropriate position, we can exploit this relay node to establish a secure source-destination link.

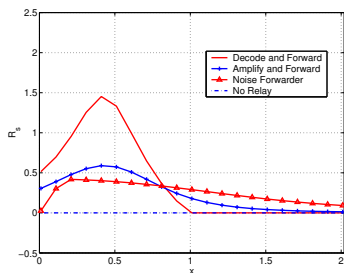


Fig. 5. The achievable perfect secrecy rate for various schemes in the Gaussian relay eavesdropper channel with phase fading.

In the second scenario, we assume that before transmission, the source knows the phases $\theta_{sr}, \theta_{sd}, \theta_{rd}$, but does not know θ_{sw}, θ_{rw} . The random phase will not affect the achievable perfect secrecy rate of NF since it does not depend on beamforming between the source and relay. But, the rates of DF and AF are different here. In both cases, the source can adjust its phase according to the knowledge of the phase information about $\theta_{sr}, \theta_{sd}, \theta_{rd}$. In this way, the signals of the source and the relay will add up coherently at the destination, but not at the eavesdropper since θ_{sw}, θ_{rw} are independent of $\theta_{sd}, \theta_{rd}, \theta_{sr}$. The secrecy rate of DF and AF could then be obtained by averaging (7), (8) over the random phases.

Figure 5 shows the achievable perfect secrecy rates of the proposed strategies for the same setup as the first scenario. Due to the random phases, the achievable perfect secrecy capacity when the relay is at the same position as the source is not zero anymore. In this case, it will be beneficial to have multiple transmitting antennas at the source. Similar to the first scenario, when $x > 1$, DF cooperation does not offer any benefit. But both NF and AF still enjoy non-zero perfect secrecy rates.

V. CONCLUSIONS

In this paper, the relay-eavesdropper channel was studied. In particular, several cooperation strategies were proposed and the corresponding achievable performance bounds were obtained. Furthermore, an outer-bound on the optimal rate-equivocation region for this channel was developed. Of particular interest is the proposed NF strategy which was used to illustrate the deaf-helper phenomenon, and to demonstrate the utility of the relay node in the reversely degraded relay-eavesdropper channel. Overall, our results establish the critical role of user cooperation in facilitating secure wireless communications. Among the many open problems posed by our work, how to close the gap between the achievable performance and the outer-bound is arguably the most important one. The investigation of the role of feedback in the relay-eavesdropper channel is another interesting problem. Finally, extending our work to a large scale network is of practical significance.

REFERENCES

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.
- [2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 24, pp. 339–348, May 1978.
- [4] T. Cover and A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Trans. on Information Theory*, vol. 25, pp. 572–584, Sep. 1979.
- [5] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," *IEEE Trans. on Information Theory*, vol. 51, pp. 3037–3063, Sep. 2005.
- [6] Y. Oohama, "Relay channels with confidential messages," *IEEE Trans. on Information Theory*, Nov. 2006. Submitted.
- [7] I. Csiszar and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. on Information Theory*, vol. 24, pp. 339–348, May 1978.
- [8] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Internat. Symposium on Information Theory*, (Seattle, WA), July 9-14, 2006.
- [9] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," *IEEE Trans. on Information Theory*, 2006. Submitted.
- [10] E. Tekin and A. Yener, "The gaussian multiple access wire-tap channel," *IEEE Trans. on Information Theory*, 2006. Submitted.
- [11] L. Lai and H. El-Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. on Information Theory*, Dec 2006. Submitted.
- [12] C.-M. Zing, F. Kuhlmann, and A. Buzo, "Achievability proof of some multiuser channel coding theorems using backward decoding," *IEEE Trans. on Information Theory*, vol. 35, no. 6, pp. 1160–1165, 1989.
- [13] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. on Information Theory*, vol. 50, pp. 3062–3080, Dec. 2004.
- [14] L. Lai, K. Liu, and H. El-Gamal, "The three node wireless network: Achievable rates and cooperation strategies," *IEEE Trans. on Information Theory*, vol. 52, pp. 805–828, Mar. 2006.
- [15] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel," *IEEE Trans. on Information Theory*, vol. 24, pp. 451–456, Jul. 1978.