Secrecy capacity of a class of orthogonal relay eavesdropper channels

Vaneet Aggarwal, Lalitha Sankar, A. Robert Calderbank, and H. Vincent Poor
Department of Electrical Engineering, Princeton University, Princeton, NJ 08544.

***Abstract*—The secrecy capacity is developed for a class of relay channels with orthogonal components and a passive eavesdropper node. The relay and destination receive signals from the source on two orthogonal channels such that the destination also receives transmissions from the relay on its channel. The eavesdropper can overhear either one or both of the orthogonal channels. Inner and outer bounds on the secrecy capacity are developed for both the discrete memoryless and the Gaussian channel models. For the discrete memoryless case, the secrecy capacity is shown to be achieved by a *partial decode-and-forward* (PDF) scheme when the eavesdropper can overhear only one of the two orthogonal channels. Two new outer bounds are presented for the Gaussian model using recent capacity results for a Gaussian multi-antenna channel with a multi-antenna eavesdropper. The outer bounds are shown to be tight for two sub-classes of channels. The first sub-class is one in which the source and relay are clustered and the eavesdropper overhears on only one of the two channels for which the PDF strategy is optimal. The second is a sub-class in which the source does not transmit to the relay for which a noise-forwarding strategy is optimal.**

I. Introduction

In wireless networks for which nodes can benefit from cooperation and packet-forwarding, there is also a need to preserve the confidentiality of transmitted information from untrusted nodes. Information privacy in wireless networks has traditionally been the domain of the higher layers of the protocol stack via the use of cryptographically secure schemes. In his seminal paper on the three-node wiretap channel, Wyner showed that perfect secrecy of transmitted data from the source node can be achieved when the physical channel to the eavesdropper is noisier than the channel to the intended destination, i.e., when the channel is a degraded broadcast channel [1]. This work was later extended by Csiszár and Körner to all broadcast channels with confidential messages, in which the source node sends common information to both the destination and the wiretapper and confidential information only to the destination [2].

Recently, the problem of secure communications has also been studied for a variety of multi-terminal networks; see for example, [3–10], and the references therein. In [11], the authors show that a relay node can facilitate the transmission of confidential messages from the source to the destination in the presence of a wiretapper, often referred to as an eavesdropper in the wireless setting. The authors develop the rate-equivocation region for this four node relay-eavesdropper channel and introduce a noise forwarding scheme in which the relay, even if it is unable to aid the source in its transmissions, transmits codewords independent of the source to confuse the eavesdropper. In contrast, the relay channel with confidential messages where the relay node acts as both a helper and eavesdropper is studied in [12]. Note that in both papers, the relay is assumed to be full-duplex, i.e., it can transmit and receive simultaneously over the entire bandwidth.

In this paper, we study the secrecy capacity of a relay channel with orthogonal components in the presence of a passive eavesdropper node. The orthogonality comes from the fact that the relay and destination receive signals from the source on orthogonal channels; furthermore, the destination also receives transmissions from the relay on its channel. The orthogonal model implicitly imposes a half-duplex transmission and reception constraint on the relay. For this channel, in the absence of an eavesdropper, El Gamal and Zahedi showed that a *partial decode-and-forward* (PDF) strategy in which the source transmits two messages on the two orthogonal channels and the relay decodes its received signal, achieves the capacity.

We study the secrecy capacity of this channel for both the discrete memoryless and Gaussian channel models. As a first step towards this, we develop a PDF strategy for the full-duplex relay eavesdropper channel and extend it to the orthogonal model. Further, since the eavesdropper can receive signals from either orthogonal channel or both, three cases arise in the development of the secrecy capacity. We specialize the outer bounds developed in [11] for the orthogonal case and show that for the discrete memoryless channel, PDF achieves the secrecy capacity for the two cases where the eavesdropper receives signals in only one of the two orthogonal channels.

For the Gaussian model, we develop two new outer bounds using recent results on the secrecy capacity of the Gaussian multiple-input multiple-output channels in the presence of a multi-antenna eavesdropper (MIMOME) in [4–6]. The first outer bound is a genie-aided bound that allows the source and relay to cooperate perfectly resulting in a Gaussian MIMOME channel for which jointly Gaussian inputs maximize the capacity. We show that these bounds are tight for a sub-class of channels in which the multiaccess channel from the source and relay to the destination is the bottleneck link. For a complementary sub-class of channels in which the source-relay link is unusable due to noise resulting in a *deaf* relay, we develop a genie-aided bound where the relay and destination act like a two-antenna receiver. We also show that noise forwarding achieves this bound for this sub-class of channels.

In [13], the authors study the secrecy rate of the channel

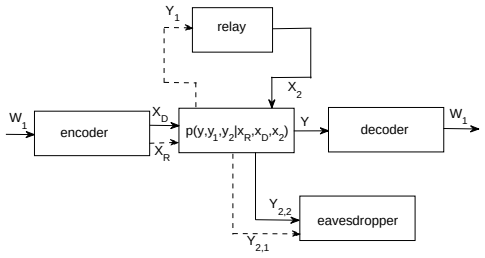


Fig. 1. The relay-eavesdropper channel with orthogonal components.

studied here under the assumption that the relay is co-located with the eavesdropper and the eavesdropper is completely cognizant of the transmit and receive signals at the relay. The authors found that using the relay does not increase the secrecy capacity and hence there is no security advantage to using the relay. In this paper, we consider the eavesdropper as a separate entity and show that using the relay increases the secrecy capacity in some cases. In the model of [13], the eavesdropper can only overhear on the channel to the relay while we consider three cases in which the eavesdropper can overhear on either or both the channels.

II. Channel Models and Preliminaries

A. Discrete Memoryless Model

A discrete-memoryless relay eavesdropper channel is denoted by $(\mathcal{X}_1 \times \mathcal{X}_2, p(y, y_1, y_2|x_1, x_2), \mathcal{Y} \times \mathcal{Y}_1 \times \mathcal{Y}_2)$ such that the inputs to the channel on a given channel use are $X_1 \in \mathcal{X}_1$ and $X_2 \in \mathcal{X}_2$ at the source and relay, respectively, the outputs of the channel are $Y_1 \in \mathcal{Y}_1$, $Y \in \mathcal{Y}$, and $Y_2 \in \mathcal{Y}_2$, at the relay, destination, and eavesdropper, respectively, and the channel transition probability is given by $p_{YY_1Y_2|XX_2}(y, y_1, y_2|x, x_2)$ [11]. The channel is assumed to be memoryless, i.e. the channel outputs at time i depend only on channel inputs at time i. The source transmits a message $W_1 \in \mathcal{W}_1 = \{1, 2, \cdots, M\}$ to the destination using the (M, n) code consisting of

1) a stochastic encoder f at the source such that $f : \mathcal{W}_1 \to X_1^n \in \mathcal{X}_1^n$,
2) a set of relay encoding functions $f_{r,i} : (Y_{1,1}, Y_{1,2}, \cdots, Y_{1,i-1}) \to x_{2,i}$ at every time instant i, and
3) a decoding function at the destination $\Phi : \mathcal{Y}^n \to \mathcal{W}_1$.

The average error probability of the code is defined as:

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

The equivocation rate at the eavesdropper is defined as $R_e = \frac{1}{n} H(W_1|Y_2^n)$. A perfect secrecy rate of R_1 is achieved if for any $\epsilon > 0$, there exists a sequence of codes (M, n) and an integer N such that for all $n \geq N$, we have

$$R_1 = \frac{1}{n} \log_2 M, \quad (2)$$

$$P_e^n \leq \epsilon \text{ and} \quad (3)$$

$$\frac{1}{n} H(W_1|Y_2) \geq R_1 - \epsilon. \quad (4)$$

The secrecy capacity is maximum such rate. The model described above considers a relay that transmits and receives simultaneously in the same orthogonal channel. Inner and outer bounds for this model are developed in [11, Theorem 1].

In this paper, we consider a relay eavesdropper channel with orthogonal components in which the relay receives and transmits in two orthogonal channels. The source transmits in both channels, one of which is received at the relay and the other at the destination. The relay transmits along with the source in the channel received at the destination. Thus, the source signal X_1 consists of two parts $X_R \in \mathcal{X}_R$ and $X_D \in \mathcal{X}_D$, transmitted to the relay and the destination, respectively, such that $\mathcal{X}_1 = \mathcal{X}_D \times \mathcal{X}_R$. The eavesdropper can receive transmissions in one or both orthogonal channels such that $Y_{2,i} \in \mathcal{Y}_{2,i}$ denotes the received signal at the eavesdropper in orthogonal channel i, $i = 1, 2$, and $\mathcal{Y}_2 = \mathcal{Y}_{2,1} \times \mathcal{Y}_{2,2}$. More formally, the relay eavesdropper channel with orthogonal components is defined as follows.

Definition 1: A discrete-memoryless relay eavesdropper channel is said to have orthogonal components if the sender alphabet $\mathcal{X}_1 = \mathcal{X}_D \times \mathcal{X}_R$ and the channel can be expressed as

$$p(y, y_1, y_2|x_1, x_2) = p(y_1, y_{2,1}|x_R, x_2) \cdot p(y, y_{2,2}|x_D, x_2). \quad (5)$$

Definition 1 assumes that the eavesdropper can receive signals in both channels. In general, the secrecy capacity bounds for this channel depend on the receiver capabilities of the eavesdropper. To this end, we explicitly include the following two definitions for the cases in which the eavesdropper can receive signals in only one of the channels.

Definition 2: The eavesdropper is limited to receiving signals on the channel from the source to the relay, if $y_{2,2} = 0$.

Definition 3: The eavesdropper is limited to receiving signals on the channel from the source and the relay to the destination, if $y_{2,1} = 0$.

Thus, depending on the receiver capabilities at the eavesdropper, there are three cases that arise in developing the secrecy capacity bounds. For brevity, we henceforth identify the three cases as cases 1, 2, and 3, where cases 1 and 2 correspond to Definitions 2 and 3, respectively, and case 3 is the general case where the eavesdropper receives signals from both the channels.

B. Gaussian Model

For a Gaussian relay eavesdropper channel with orthogonal components, the signals Y_1 and Y received at the relay and the destination respectively in each time symbol $i \in \{1, \cdots, n\}$, are

$$Y_1[i] = h_{s,r} X_R[i] + Z_1[i] \quad (6)$$

and

$$Y[i] = h_{s,d}X_D[i] + h_{r,d}X_2[i] + Z[i] \tag{7}$$

where $h_{k,m}$ is the channel gain from transmitter $k \in \{s, r\}$ to receiver $m \in \{r, d\}$, and where Z_1 and Z are zero mean unit variance Gaussian random variables. The transmitted signals X_R, X_D, and X_2 are subject to average power constraints given by

$$\begin{array}{l} \frac{1}{n}\sum_{i=1}^{n} x_R^2[i] \le P_R, \\ \frac{1}{n}\sum_{i=1}^{n} x_D^2[i] \le P_D \text{ and} \\ \frac{1}{n}\sum_{i=1}^{n} x_2^2[i] \le P_2. \end{array} \tag{8}$$

The signals at the eavesdropper are

$$Y_{2,1}[i] = h_{s,e,1}X_R[i]\mathbf{1}_{e,1} + Z_{2,1}[i] \tag{9}$$

$$Y_{2,2}[i] = h_{s,e,2}x_D[i]\mathbf{1}_{e,2} + h_{r,e}X_2[i]\mathbf{1}_{e,2} + Z_{2,2}[i] \tag{10}$$

where $h_{s,e,1}$ and $h_{s,e,2}$ are the channel gains from the source to the eavesdropper in the two orthogonal channels, $h_{r,e}$ is the channel gain from the relay to the eavesdropper, $Z_{2,1}$ and $Z_{2,2}$ are zero-mean unit variance Gaussian random variables assumed to be independent of the source and relay signals, and

$$\mathbf{1}_{e,j} = \begin{cases} 1 & \text{if the eavesdropper can eavesdrop} \\ & \text{in orthogonal channel } j = 1, 2 \\ 0 & 0 \text{ otherwise.} \end{cases}$$

Throughout the sequel, we assume that the channel gains are fixed and known at all nodes.

We use the standard notation for entropy and mutual information [14] and take all logarithms to the base 2 so that our rate units are bits. For ease of exposition, we write $C(x)$ to denote $\frac{1}{2}\log(1+x)$. We also write random variables with uppercase letters (e.g. W_k) and their realizations with the corresponding lowercase letters (e.g. w_k). We drop subscripts on probability distributions if the arguments are lowercase versions of the corresponding random variables. Finally, for brevity, we henceforth refer to the channel studied here as the orthogonal relay eavesdropper channel.

III. Discrete memoryless Channel: Outer and Inner Bounds

In this section, we give outer and inner bounds for the secrecy capacity of the discrete-memoryless orthogonal relay eavesdropper channel. The following theorems summarize the outer and inner bounds as well as the secrecy capacity results for the three cases in which the eavesdropper can receive in either one or both orthogonal channels. Detailed proofs and illustrations can be found in [15].

Theorem 1: An outer bound on the secrecy capacity of the relay eavesdropper channel with orthogonal components is given by

$$\begin{array}{lll} \underline{\text{Case 1}}: & C_s \le & \max[\min\{I(V_DV_R; YY_1|V_2U), \\ & & I(V_DV_2; Y|U)\} - I(V_R; Y_2|U)]^+ \\ \underline{\text{Case 2}}: & C_s \le & \max[\min\{I(V_DV_R; YY_1|V_2U), \\ & & I(V_DV_2; Y|U)\} - I(V_DV_2; Y_2|U)]^+ \\ \underline{\text{Case 3}}: & C_s \le & \max[\min\{I(V_DV_R; YY_1|V_2U), \\ & & I(V_DV_2; Y|U)\} - I(V_RV_DV_2; Y_2|U)]^+ \end{array}$$

where the maximum is over all joint distributions satisfying $U \to (V_R, V_D, V_2) \to (X_R, X_D, X_2) \to (Y, Y_1, Y_2)$.[1]

For a relay channel with orthogonal components, the authors of [16] show that a strategy where the source uses each channel to send an independent message and the relay decodes the message transmitted in its channel, achieves capacity. Due to the fact that the relay has partial access to the source transmissions, this strategy is sometimes also referred to as *partial decode and forward* [17]. The achievable scheme involves block Markov superposition encoding while the converse is developed using the max-flow, min-cut bounds. A natural question for the relay-eavesdropper channel with orthogonal components is whether the PDF strategy can achieve the secrecy capacity. To this end, we summarize the achievable PDF secrecy rates for the three cases.

Theorem 2: An inner bound on the secrecy capacity of the orthogonal relay eavesdropper channel, achieved using partial decode and forward over all input distributions of the form $p(x_R, x_D, x_2)$, is given by

$$\begin{array}{lll} \underline{\text{Case 1}}: & C_s \ge & \min\{I(X_DX_R; YY_1|X_2), I(X_DX_2; Y)\} \\ & & -I(X_R; Y_2) \qquad (11) \\ \underline{\text{Case 2}}: & C_s \ge & \min\{I(X_DX_R; YY_1|X_2), I(X_DX_2; Y)\} \\ & & -I(X_D, X_2; Y_2) \qquad (12) \\ \underline{\text{Case 3}}: & C_s \ge & \min\{I(X_DX_R; YY_1|X_2), I(X_DX_2; Y)\} \\ & & -I(X_R; Y_2|X_2) - I(X_D, X_2; Y_2) \qquad (13) \end{array}$$

The bounds in (13) can be generalized by randomizing the channel inputs. The following theorem summarizes our result that PDF with randomization achieves the secrecy capacity when the eavesdropper is limited to receiving signals on one of the two channels.

Theorem 3: The secrecy capacity of the relay channel with orthogonal complements is

$$\begin{array}{lll} \underline{\text{Case 1}}: & C_s = & \max[\min\{I(V_DV_R; YY_1|V_2U), \\ & & I(V_DV_2; Y|U)\} - I(V_R; Y_2|U)]^+ \\ \underline{\text{Case 2}}: & C_s = & \max[\min\{I(V_DV_R; YY_1|V_2U), \\ & & I(V_DV_2; Y|U)\} - I(V_DV_2; Y_2|U)]^+ \\ \underline{\text{Case 3}}: & C_s \le & \max[\min\{I(V_DV_R; YY_1|V_2U), \\ & & I(V_DV_2; Y|U)\} - I(V_RV_DV_2; Y_2|U)]^+ \end{array}$$

where the maximum is over all joint distributions satisfying $U \to (V_R, V_D, V_2) \to (X_R, X_D, X_2) \to (Y, Y_1, Y_2)$. Further-

[1]The notation $[x]^+$ denotes $\max(x, 0)$.

more, for Case 3,

$$C_s \geq \begin{array}{l}[\min\{I(V_DV_R;YY_1|V_2U), I(V_DV_2;Y|U)\} \\ -I(V_R;Y_2|V_2U) - I(V_D,V_2;Y_2|U)]^+\end{array}$$

for all joint distributions satisfying $U \rightarrow (V_R, V_D, V_2) \rightarrow (X_R, X_D, X_2) \rightarrow (Y, Y_1, Y_2)$.

Remark 1: In contrast to the non secrecy case, where the orthogonal channel model simplifies the cut-set bounds to match the inner PDF bounds, for the orthogonal relay-eavesdropper model in which the eavesdropper receives in both channels, i.e., when the orthogonal receiver restrictions at the relay and intended destination do not apply to the eavesdropper, in general, the outer bound can be strictly larger than the inner PDF bound.

We illustrate these results with an example in which we show that the secrecy capacity is achieved by the relay transmitting a part of the message as well as a random signal.

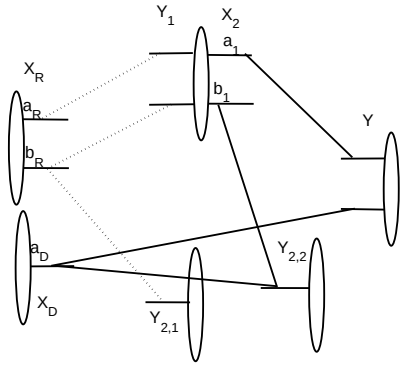


Fig. 2. Orthogonal relay eavesdropper channel model of Example 1.

Example 1: Consider an orthogonal relay eavesdropper channel where the input and output signals at the source, relay, and destination are binary two-tuples while $\mathcal{Y}_{2,1}$ and $\mathcal{Y}_{2,2}$ at the eavesdropper are binary alphabets. We write $X_R = (a_R, b_R)$, $X_D = a_D$ and $X_2 = (a_1, b_1)$ to denote the vector binary signals at the source and the relay. The outputs at the relay, destination and the eavesdropper are also vector binary signals given by

$$Y = (a_1, a_D), \qquad Y_1 = (a_R, b_R), \tag{14}$$

$$Y_{2,1} = (b_R) \text{ and } \qquad Y_{2,2} = (b_1 \oplus a_D), \tag{15}$$

as shown in Figure III. As in the previous example, the capacity of this channel is also at most 2 bits per channel use. We now show that a secrecy capacity of 2 bits per channel use can be achieved for this example channel. Consider the following coding scheme: in the i^{th} use of the channel, the source encodes 2 bits, denoted as $w_{1,i}$ and $w_{2,i}$ as

$$X_R = (w_{1,i}, 0), \quad X_D = (w_{2,i}).$$

The relay receives $w_{1,i-1}$ in the previous use of the channel. Furthermore, in each channel use, it also generates a uniformly random bit n_i, and transmits

$$X_2 = (w_{1,i-1}, n_i). \tag{16}$$

With these transmitted signals, the received signals at the receiver and the eavesdropper are

$$Y = (w_{1,i-1}, w_{2,i}), \quad Y_{2,1} = (0) \text{ and } \quad Y_{2,2} = (n_i \oplus w_{2,i}). \tag{17}$$

Thus, over $n+1$ uses of the channel the destination receives all n bits transmitted by the source. On the other hand, in every use of the channel, the eavesdropper cannot decode either source bit.

IV. Gaussian Model

A. Inner and Outer Bounds

Determining the optimal input distribution for all the auxiliary random variables in the outer bounds in Theorem 3 is not straightforward. To this end, we summarize new outer bounds using a recent result on the secrecy capacity of the class of Gaussian multiple input, multiple output, multi-antenna eavesdropper channels (see [4–6]).

Theorem 4: An outer bound on the secrecy capacity of the Gaussian orthogonal relay eavesdropper channel is given by

$$\begin{array}{ll}\underline{\text{Case 1}} & C_s \leq I(X_DX_2;Y) - I(X_R;Y_2) \\ \underline{\text{Case 2}} & C_s \leq I(X_DX_2;Y) - I(X_DX_2;Y_2) \\ \underline{\text{Case 3}} & C_s \leq I(X_DX_2;Y) - I(X_RX_DX_2;Y_2)\end{array} \tag{18}$$

for $[X_R\ X_D\ X_2]^T \sim \mathcal{N}(0, \mathbf{K_X})$ where $\mathbf{K_X} = E[\mathbf{X}\mathbf{X}^T]$ has diagonal entries that satisfy (8).

The PDF inner bounds developed in Section III for the discrete memoryless case can be applied to the Gaussian model with Gaussian inputs at the source and relay. In fact, for all three cases, the inner bounds require taking a minimum of two rates, one achieved jointly by the source and relay at the destination and the other achieved by the source at the relay and destination. Comparing the inner bounds in (13) with the outer bounds in (18), for those channels in which the source and relay are clustered close enough that the bottleneck link is the combined source-relay link to the destination and the eavesdropper overhears only one of the two channels, the secrecy capacity can be achieved. This is summarized in the following theorem.

Theorem 5: For a class of *clustered* orthogonal Gaussian relay channels with

$$I(X_DX_2;Y) < I(X_DX_R;YY_1|X_2) \tag{19}$$

where $\mathbf{X} = [X_R\ X_D\ X_2]^T \sim \mathcal{N}(0, \mathbf{K_X})$, the secrecy capacity for cases 1 and 2 is achieved by PDF and is given by

$$\begin{array}{ll}\underline{\text{Case 1}}: & C_s = I(X_DX_2;Y)\} - I(X_R;Y_2) \\ \underline{\text{Case 2}}: & C_s = I(X_DX_2;Y)\} - I(X_D,X_2;Y_2).\end{array}$$

Next theorem summarizes the capacity of a sub-class of Gaussian orthogonal relay eavesdropper channels for which $h_{s,r} = 0$, in which noise-forwarding is optimal.

Theorem 6: The secrecy capacity of a sub-class of Gaussian orthogonal relay eavesdropper channels with $h_{s,r} = 0$ in the cases 2 and 3 is given by

$$\begin{aligned} C_s \quad = \quad & \min \left\{ C\left(|h_{s,d}|^2 E[X_D^2] + |h_{r,d}|^2 E[X_2^2]\right) \right. \\ & -C\left(|h_{s,e,2}|^2 E[X_D^2] + |h_{r,e}|^2 E[X_2^2]\right), \\ & C(|h_{s,d}|^2 E[X_D^2]) \\ & \left. -C\left(|h_{s,e,1}|^2 E[X_D^2]/(1+|h_{r,e}|^2 E[X_2^2])\right) \right\} \quad (20) \end{aligned}$$

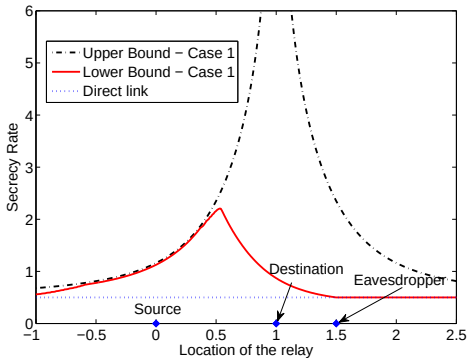
B. Illustration of Results

We illustrate our results for the Gaussian model for a class of linear networks in which the source is placed at the origin and the destination is unit distance from the source at $(1, 0)$. The eavesdropper is at $(1.5, 0)$. The channel gain $h_{m,k}$, between transmitter m and receiver k, for each m and k, is modeled as a distance dependent path-loss gain given by

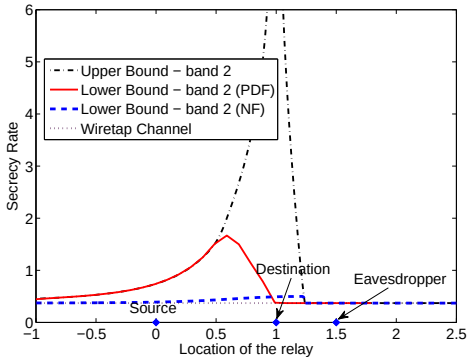
$$h_{m,k} = \frac{1}{d_{m,k}^{\alpha/2}} \quad \text{for all } m \in \{s, r\}, k \in \{r, d, e\} \qquad (21)$$

where α is the path-loss exponent. The maximum achievable PDF secrecy rate is plotted as a function of the relay position along the line connecting the source and the eavesdropper as shown in Figure IV-B. Furthermore, as a baseline assuming the relay does not transmit, i.e., $X_R = 0$, the secrecy capacity of the resulting direct link and the wire-tap channel for cases 2 and 3, respectively, are included in all three plots in Fig. IV-B. The rates are plotted in separate sub-figures for the three cases in which the eavesdropper receives signals in only one or both channels. In all cases, the path loss exponent α is set to 2 and the average power constraint on X_R, X_D, and X_2 is set to unity. In addition to PDF, the secrecy rate achieved by noise forwarding (NF) is also plotted.

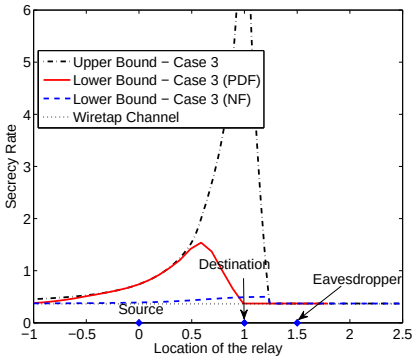
In Fig IV-B, for all three cases, the PDF secrecy rates are obtained by choosing the input signal $\mathbf{X} = [X_R \; X_D \; X_2]^T$ as Gaussian distributed and optimizing the rates over the covariance matrix $\mathbf{K_X} = E[\mathbf{X}\mathbf{X}^T]$. Thus, for all the cases, PDF is optimal when the relay is close to the source. On the other hand, when the relay is farther away than the eavesdropper and destination are from the source, there are no gains achieved by using the relay relative to the non-relay wiretap secrecy capacity. Finally, for cases 2 and 3, NF performs better than PDF when the relay is closer to the destination.



(a) Case 1.



(b) Case 2.



(c) Case 3.

Fig. 3. Source is at $(0, 0)$, destination at $(1, 0)$ and eavesdropper is at $(1.5, 0)$. Distance fading model with $\alpha = 2$ is taken and power constraints for X_R, X_D and X_2 are all unity.

V. Conclusions

We have developed bounds on the secrecy capacity of relay eavesdropper channels with orthogonal components in the presence of an additional passive eavesdropper for both the discrete memoryless and Gaussian channel models. Our results depend on the capability of the eavesdropper to overhear either or both of the two orthogonal channels that the source uses for its transmissions. For the discrete memoryless model, when the eavesdropper is restricted to receiving in only one of the two channels, we have shown that the secrecy capacity is achieved by a partial decode-and-forward strategy.

For the Gaussian model, we have developed a new outer bound using recent results on the secrecy capacity of Gaussian MIMOME channels. When the eavesdropper is restricted to overhearing only one of the two channels, our bound is tight for a sub-class of channels where the source and relay are clustered such that the combined link from the source and relay to the destination is the bottle-neck link. Furthermore, for a sub-class where the source-relay link is not used, we have developed a new MIMOME-based outer bound that matches the secrecy rate achieved by the noise forwarding strategy.

A natural extension to this model is to study the secrecy capacity of orthogonal relay channels with multiple relays

and multiple eavesdroppers. Also, the problem of developing an additional outer bound that considers a noiseless relay destination link remains open for the channel studied here.

REFERENCES

[1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *arXiv*, vol. abs/cs/0702112, 2007.

[4] A. Khisti and G. W. Wornell, "The MIMOME channel," in *Proc. 45th Annual Allerton Conf. Comm., Contr. and Computing*, Monticello, IL, Sep. 2007.

[5] T. Lie and S. Shamai, "A channel-enhancement approach to the secrecy capacity of the multi-antenna wiretap channel," 2007, preprint.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," 2007, preprint.

[7] M. Bloch and A. Thangaraj, "Confidential messages to a cooperative relay," May 2008, pp. 154–158.

[8] Y. Liang and H. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 976–1002, March 2008.

[9] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. THeory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[10] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," Submitted to IEEE Trans. Infor. Theory, Dec. 2007, preprint.

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

[12] Y. Oohama, "Relay channels with confidential messages," *arXiv*, vol. abs/cs/0611125, 2006.

[13] X. He and A. Yener, "On the equivocation region of relay channels with orthogonal components," in *Proc. 41st Annual Asilomar Conf. Signals, Systems, and Computers*, Pacific Grove, CA, Nov. 2007.

[14] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley and Sons, Inc., 1991.

[15] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *Submitted to Eurasip special issue on wireless physical layer security*, Dec. 2008.

[16] A. El Gamal and S. Zahedi, "Capacity of relay channels with orthogonal components," *IEEE Trans. Inform. Theory*, vol. 51, no. 5, pp. 1815–1817, May 2005.

[17] G. Kramer, "Models and theory for relay channels with receive constraints," in *Proc. 42nd Annual Allerton Conf. on Commun., Control, and Computing*, Monticello, IL, Sep. 2004.