

Research Article

Secrecy Capacity of a Class of Orthogonal Relay Eavesdropper Channels

Vaneet Aggarwal, Lalitha Sankar, A. Robert Calderbank (EURASIP Member), and H. Vincent Poor

Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA

Correspondence should be addressed to Vaneet Aggarwal, vaggarwa@princeton.edu

Received 1 December 2008; Accepted 9 June 2009

Recommended by Shlomo Shamai (Shitz)

The secrecy capacity of relay channels with orthogonal components is studied in the presence of an additional 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 multiantenna point-to-point channel with a multiantenna eavesdropper. The outer bounds are shown to be tight for two subclasses of channels. The first subclass is one in which the source and relay are clustered, and the eavesdropper receives signals only on the channel from the source and the relay to the destination, for which the PDF strategy is optimal. The second is a subclass in which the source does not transmit to the relay, for which a noise-forwarding strategy is optimal.

Copyright © 2009 Vaneet Aggarwal et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. 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, that is, 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 multiterminal networks; see, for example, [3–10], and the references therein. In [11], Lai and El Gamal 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. Lai and El Gamal 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. A special case where the eavesdropper receives a degraded version of the destination's signal is studied in [12]. In contrast, the relay channel with confidential messages in which the relay node acts as both a helper and eavesdropper is studied in [13]. Note that in all the three papers, the relay is assumed to be full-duplex; that is, 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 (the destination's) 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 [14].

We study the secrecy capacity of this channel for both the discrete memoryless and Gaussian channel models. As a first step toward 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 subclass of channels in which the multiaccess channel from the source and relay to the destination is the bottleneck link, and the eavesdropper is limited to receiving signals on the channel from the source and the relay to the destination. For a complementary subclass 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 subclass of channels.

In [15], He and Yener study the secrecy rate of the channel studied here under the assumption that the relay is colocated 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 [15], the eavesdropper can overhear only on the channel to the relay, while we consider three cases in which the eavesdropper can overhear on either or both the channels.

The paper is organized as follows. In Section 2, we present the channel models. In Section 3, we develop the inner and outer bounds on the secrecy capacity of the discrete

memoryless model. We illustrate these results with examples in Section 4. In Section 5, we present inner and outer bounds for the Gaussian channel model and illustrate our results with examples. We conclude in Section 6.

2. Channel Models and Preliminaries

2.1. 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 in 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 $p_{Y Y_1 Y_2 | X X_2}(y, y_1, y_2 | x, x_2)$ [11]. The channel is assumed to be memoryless; that is, the channel outputs at time i depend only on channel inputs at time i . The source transmits a message $W_1 \in \mathcal{W}_1 = \{1, 2, \dots, M\}$ to the destination using the (M, n) code consisting of

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

The average error probability of the code is defined as

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

The equivocation rate at the eavesdropper is defined as $R_e = (1/n)H(W_1 | Y_2^n)$. 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

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

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

The secrecy capacity is the maximum rate satisfying (2). 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 on two orthogonal channels. The source transmits on both channels, one of which is received at the relay and the other at the destination. The relay transmits along with the source on 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

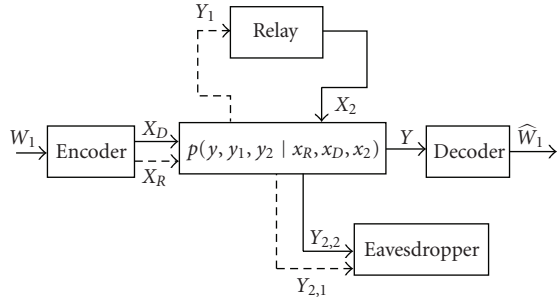


FIGURE 1: The relay-eavesdropper channel with orthogonal components.

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

$$p(y, y_1, y_2 | x_1, x_2) = p(y_1, y_{2,1} | x_R, x_2) \cdot p(y, y_{2,2} | x_D, x_2). \quad (3)$$

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

$$\begin{aligned} p(y, y_1, y_{2,1}, y_{2,2} | x_R, x_D, x_2) \\ = p(y_1, y_{2,1} | x_R, x_2) \cdot p(y | x_D, x_2) \cdot p(y_{2,2}). \end{aligned} \quad (4)$$

Definition 3. The eavesdropper is limited to receiving signals on the channel from the source and the relay to the destination, if

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

Remark 4. In the absence of an eavesdropper, that is, for $y_{2,1} = y_{2,2} = 0$, the channels in (3)–(5) simplify to that of a relay channel with orthogonal components.

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.

2.2. 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 $i \in \{1, \dots, n\}$, are

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

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

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

$$\begin{aligned} E[X_R^2] &\leq P_R, \\ E[X_D^2] &\leq P_D, \\ E[X_2^2] &\leq P_2, \end{aligned} \quad (8)$$

where $E[\cdot]$ denotes expectation of its argument. The signals at the eavesdropper are

$$\begin{aligned} Y_{2,1}[i] &= h_{s,e,1}X_R[i]\mathbf{1}_{e,1} + Z_{2,1}[i], \\ Y_{2,2}[i] &= h_{s,e,2}X_D[i]\mathbf{1}_{e,2} + h_{r,e}X_2[i]\mathbf{1}_{e,2} + Z_{2,2}[i], \end{aligned} \quad (9)$$

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

$$\mathbf{1}_{e,j} = \begin{cases} 1, & \text{if the eavesdropper can eavesdrop} \\ & \text{in orthogonal channel } j = 1, 2, \\ 0, & \text{otherwise.} \end{cases} \quad (10)$$

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

For a relay channel with orthogonal components, El Gamal and Zahedi of 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 [14]. 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* (see [16]). The achievable scheme involves block Markov superposition encoding while the converse is developed using the max-flow, min-cut bounds. The following proposition summarizes this result.

Proposition 5 ([14]). *The capacity of a relay channel with orthogonal component is given by*

$$\begin{aligned} C = \max \min \{ & I(X_R; Y_1 | X_2) + I(X_D; Y | X_2), \\ & I(X_R X_D X_2; Y) \}, \end{aligned} \quad (11)$$

where the maximum is over all input distributions of the form

$$p(x_2)p(x_R | x_2)p(x_D | x_2). \quad (12)$$

For the Gaussian model, the bounds in (11) are maximized by jointly Gaussian inputs transmitting at the maximum power and subject to (12).

Remark 6. While the converse allows for all possible joint distributions of X_R , X_D , and X_2 , from the form of the mutual information expressions in (11), it suffices to consider distributions only of the form given by (12).

We use the standard notation for entropy and mutual information [17] 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 $(1/2)\log(1+x)$ and write x^+ to denote $\max(x, 0)$. 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.

3. Discrete Memoryless Channel: Outer and Inner Bounds

In this section, we develop outer and inner bounds for the secrecy capacity of the discrete-memoryless orthogonal relay eavesdropper channel. The proof of the outer bounds follows along the same lines as that in [11, Theorem 1] for the full-duplex relay-eavesdropper channel and is specialized for the orthogonal model considered here. The following theorem summarizes the bounds for the three cases in which the eavesdropper can receive in either one or both orthogonal channels.

Theorem 7. *An outer bound on the secrecy capacity of the relay eavesdropper channel with orthogonal components is given by the following.*

Case 1.

$$C_s \leq \max\{\min\{I(V_D V_R; Y Y_1 | V_2 U), I(V_D V_2; Y | U)\} - I(V_R; Y_2 | U)\}^+.$$
 (13)

Case 2.

$$C_s \leq \max\{\min\{I(V_D V_R; Y Y_1 | V_2 U), I(V_D V_2; Y | U)\} - I(V_D V_2; Y_2 | U)\}^+.$$
 (14)

Case 3.

$$C_s \leq \max\{\min\{I(V_D V_R; Y Y_1 | V_2 U), I(V_D V_2; Y | U)\} - I(V_R V_D V_2; Y_2 | U)\}^+,$$
 (15)

where U , V_D , V_R , and V_2 are auxiliary random variables, and the maximum is over all joint distributions satisfying $U \rightarrow (V_R, V_D, V_2) \rightarrow (X_R, X_D, X_2) \rightarrow (Y, Y_1, Y_2)$.

Proof. The proof is extended from the outer bound in [11, Theorem 1] to include auxiliary random variables corresponding to each of the transmitted signals and is developed in Appendix A. \square

Following Proposition 5, 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 first develop the achievable PDF secrecy rates for the class of *full-duplex* relay-eavesdropper channels and then specialize the result for the orthogonal model. The following theorem summarizes the inner bounds on the secrecy capacity achieved by PDF for the full-duplex (nonorthogonal) relay-eavesdropper channels.

Theorem 8. *An inner bound on the secrecy capacity of a full-duplex relay eavesdropper channel, achieved using partial decode and forward, is given by*

$$C_s \geq \min\{I(X_1; Y | X_2, V) + I(V; Y_1 | X_2), I(X_1 X_2 V; Y)\} - I(X_1 X_2; Y_2)$$
 (16)

for all joint distributions of the form

$$p(v)p(x_1 | v)p(x_2 | v)p(y_1, y | x_1, x_2).$$
 (17)

Proof. The proof is developed in Appendix B and uses block Markov superposition encoding at the source such that, in each block, the relay decodes a part of the source message while the eavesdropper has access to both source messages. \square

The following theorem specializes Theorem 8 for the orthogonal relay-eavesdropper channel.

Theorem 9. *An inner bound on the secrecy capacity of the orthogonal relay eavesdropper channel, achieved using partial decode and forward over all joint distributions of the form $p(x_R, x_D, x_2)$, is given by the following.*

Case 1.

$$C_s \geq \min\{I(X_D X_R; Y Y_1 | X_2), I(X_D X_2; Y)\} - I(X_R; Y_2).$$
 (18)

Case 2.

$$C_s \geq \min\{I(X_D X_R; Y Y_1 | X_2), I(X_D X_2; Y)\} - I(X_D, X_2; Y_2).$$
 (19)

Case 3.

$$C_s \geq \min\{I(X_D X_R; Y Y_1 | X_2), I(X_D X_2; Y)\} - I(X_R; Y_2 | X_2) - I(X_D, X_2; Y_2).$$
 (20)

Proof. The proof is developed in Appendix C and involves specializing the bounds in Theorem 8 for the orthogonal model. It is further shown that the input distribution can be generalized to all joint probability distributions $p(x_R, x_D, x_2)$. \square

The bounds in (20) can be generalized by randomizing the channel inputs. We now prove that PDF with randomization achieves the secrecy capacity.

Theorem 10. *The secrecy capacity of the relay channel with orthogonal complements is the following.*

Case 1.

$$C_s = \max\{\min\{I(V_D V_R; Y Y_1 | V_2 U), I(V_D V_2; Y | U)\} - I(V_R; Y_2 | U)\}^+ \quad (21)$$

Case 2.

$$C_s = \max\{\min\{I(V_D V_R; Y Y_1 | V_2 U), I(V_D V_2; Y | U)\} - I(V_D V_2; Y_2 | U)\}^+ \quad (22)$$

Case 3.

$$C_s \leq \max\{\min\{I(V_D V_R; Y Y_1 | V_2 U), I(V_D V_2; Y | U)\} - I(V_R V_D V_2; Y_2 | U)\}^+ \quad (23)$$

where U , V_D , V_R , and V_2 are auxiliary random variables, and the maximum is over all joint distributions satisfying $U \rightarrow (V_R, V_D, V_2) \rightarrow (X_R, X_D, X_2) \rightarrow (Y, Y_1, Y_2)$. Furthermore, for Case 3,

$$C_s \geq [\min\{I(V_D V_R; Y Y_1 | V_2 U), I(V_D V_2; Y | U)\} - I(V_R; Y_2 | V_2 U) - I(V_D, V_2; Y_2 | U)]^+ \quad (24)$$

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

Proof. The upper bounds follow from Theorem 7. For the lower bound, we prefix a memoryless channel with inputs V_R, V_D , and V_2 and transition probability $p(x_R, x_D, x_2 | v_R, v_D, v_2)$ (this prefix can potentially increase the achievable secrecy rates as in [2, 11]). The time-sharing random variable U ensures that the set of achievable rates is convex. \square

Remark 11. In contrast to the nonsecrecy 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, that is, 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.

In the following section, we illustrate these results with three examples.

4. Examples

Example 12. Consider an orthogonal relay eavesdropper channel with $\mathcal{X}_R = \mathcal{X}_D = \mathcal{X}_2 = \{0, 1\}$. The outputs at the relay and destination are given by

$$Y_1 = X_R, \quad Y = X_D X_2, \quad (25)$$

while the output at the eavesdropper is

$$Y_{2,1} = X_R \quad (\text{channel 1}),$$

$$Y_{2,2} = \begin{cases} 1, & \text{if } X_D \leq X_2, \\ 0, & \text{otherwise,} \end{cases} \quad (\text{channel 2}). \quad (26)$$

Since the destination can receive at most 1 bit in every use of the channel, the secrecy capacity of this channel is at most 1 bit per channel use. We now show that this secrecy capacity can be achieved. In each channel use, let the source send bit $w \in \{0, 1\}$ such that $X_R = 0$, $X_D = w$, and $X_2 = 1$. Since $X_2 = 1$, the receiver obtains w while the eavesdropper receives $Y_{2,1} = 0$ and $Y_{2,2} = 1$ irrespective of the value of bit w . Hence, a perfect secrecy capacity of 1 can be achieved.

The code design in Example 12 did not require randomization. We now present an example where randomization is necessary.

Example 13. Consider an orthogonal relay eavesdropper channel where all the input and output alphabets are the same and given by $\{0, 1\}^2$. We write $X_R = (a_R, b_R)$, $X_D = (a_D, b_D)$, and $X_2 = (a_1, b_1)$ to denote the vector binary signals at the source and the relay. The outputs of this channel, shown in Figure 2(a), at the relay, destination, and the eavesdropper are given by

$$Y = (a_D, b_D \oplus a_1),$$

$$Y_1 = (a_R, b_R),$$

$$Y_{2,1} = (a_R, b_R),$$

$$Y_{2,2} = (a_1, b_1 \oplus a_D), \quad (27)$$

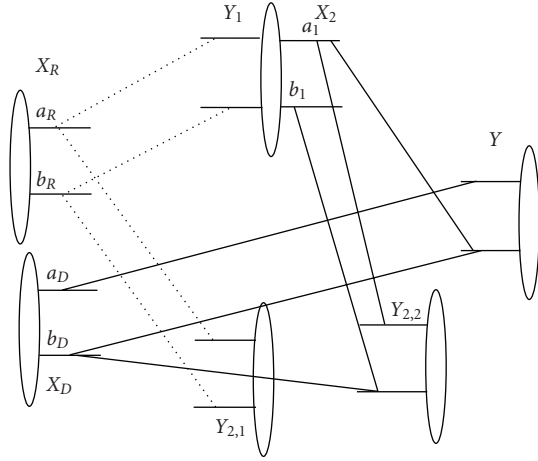
where \oplus denotes the binary XOR operation. The capacity of this channel is at most 2 bits per channel use as the destination, via Y , can receive at most 2 bits per channel use. We will now show that a secrecy capacity of 2 bits per channel use can be achieved. Consider the following coding scheme. In every channel use, the relay flips an unbiased coin to generate a bit $n \in \{0, 1\}$ such that its transmitted signal is

$$X_2 = (0, n). \quad (28)$$

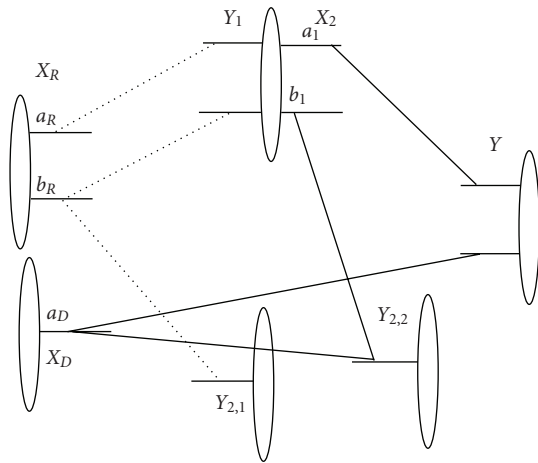
In every use of the channel, the source transmits 2 bits, denoted as w_1 and w_2 , using

$$X_R = (0, 0),$$

$$X_D = (w_1, w_2). \quad (29)$$



(a) Example 13



(b) Example 14

FIGURE 2: Orthogonal relay eavesdropper channel model of Examples 13 and 14.

For these transmitted signals, the receiver and eavesdropper receive

$$\begin{aligned} Y &= (w_1, w_2), \\ Y_{2,1} &= (0, 0), \\ Y_{2,2} &= (0, n \oplus w_1). \end{aligned} \quad (30)$$

Thus, the receiver receives both bits while the eavesdropper is unable to decode any information due to the randomness of n . This is an example where transmitting a random code from the relay is required to achieve the secrecy capacity.

In the above two examples, the source to relay link was completely available to the eavesdropper, and hence the relay could at best be just used to send random bits. In the next example, we show that the secrecy capacity is achieved by the relay transmitting a part of the message as well as a random signal.

Example 14. 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

$$\begin{aligned} Y &= (a_1, a_D), \\ Y_1 &= (a_R, b_R), \\ Y_{2,1} &= (b_R), \\ Y_{2,2} &= (b_1 \oplus a_D), \end{aligned} \quad (31)$$

as shown in Figure 2(b). 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

$$\begin{aligned} X_R &= (w_{1,i}, 0), \\ X_D &= (w_{2,i}). \end{aligned} \quad (32)$$

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

$$X_2 = (w_{1,i-1}, n_i). \quad (33)$$

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

$$\begin{aligned} Y &= (w_{1,i-1}, w_{2,i}), \\ Y_{2,1} &= (0), \\ Y_{2,2} &= (n_i \oplus w_{2,i}). \end{aligned} \quad (34)$$

Thus, over $n + 1$ uses of the channel the destination receives all $2n + 1$ bits transmitted by the source. On the other hand, in every use of the channel, the eavesdropper cannot decode either source bit.

5. Gaussian Model

5.1. Inner and Outer Bounds. We now develop inner and outer bounds for the Gaussian orthogonal relay eavesdropper channel. Determining the optimal input distribution for all the auxiliary random variables in the outer bounds in Theorem 10 is not straightforward. To this end, we develop new outer bounds using a recent result on the secrecy capacity of the class of Gaussian multiple input, multiple output, and multiantenna eavesdropper channels (see [4–6]). The class of MIMOME channels is characterized by a single source with an $m \times 1$ vector input \mathbf{X} and $k \times 1$ and

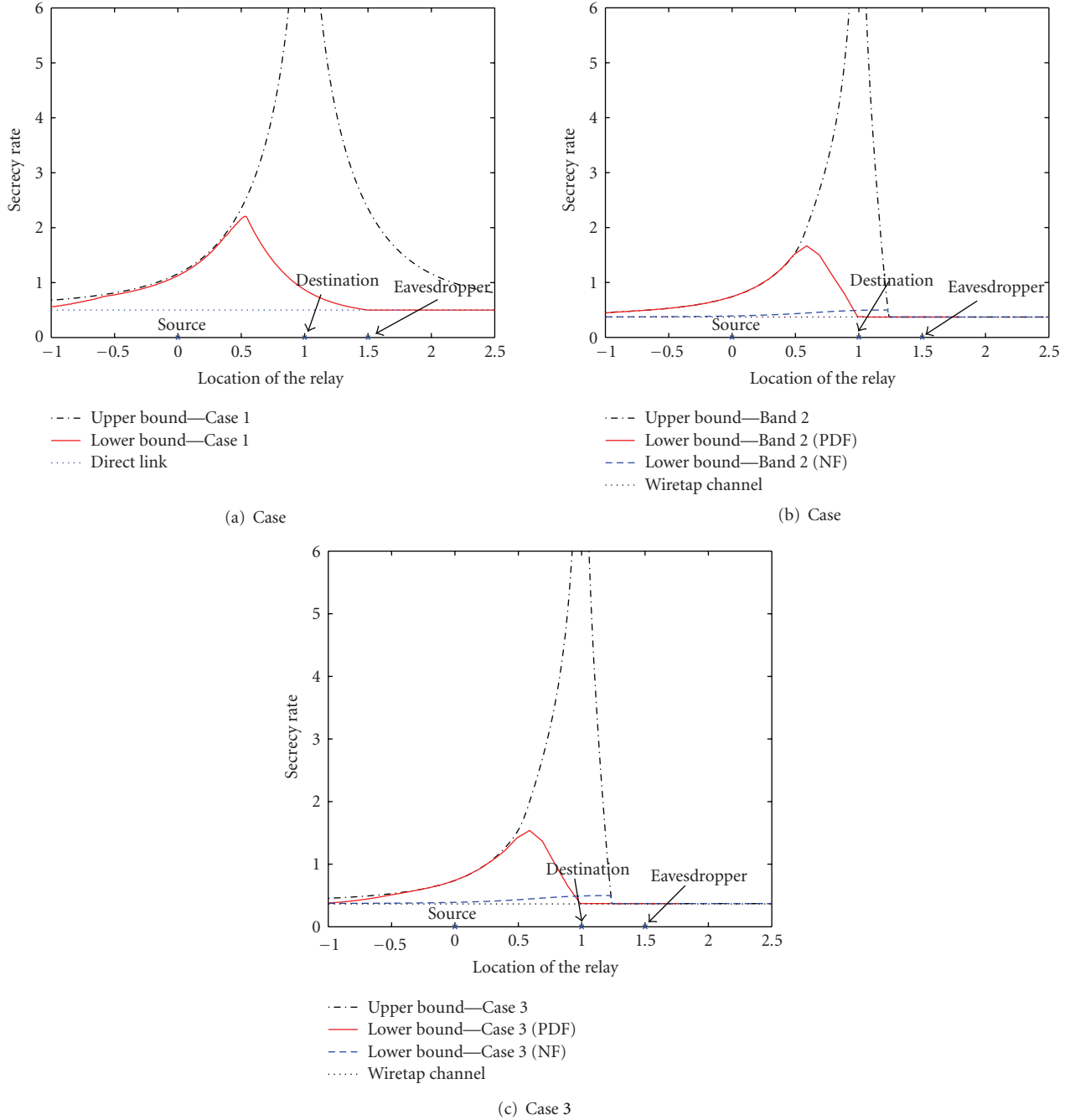


FIGURE 3: Source is at (0,0), destination is at (1,0), and eavesdropper is at (1.5,0). A distance fading model with $\alpha = 2$ is taken, and power constraints for X_R , X_D , and X_2 are all unity.

$t \times 1$ vector outputs \mathbf{Y} and \mathbf{Y}_e at the intended destination and eavesdropper, respectively, given by

$$\mathbf{Y}[i] = \mathbf{H}\mathbf{X}[i] + \mathbf{Z}[i], \quad (35)$$

$$\mathbf{Y}_e[i] = \mathbf{H}_e\mathbf{X}[i] + \mathbf{Z}_e[i], \quad (36)$$

where in every channel use i , $\mathbf{Z}[i]$ and $\mathbf{Z}_e[i]$ are zero-mean Gaussian vectors with identity covariance matrices that are

independent across time symbols. The channel input satisfies an average transmit power constraint:

$$\frac{1}{n} \sum_{i=1}^n \|\mathbf{x}\|^2 \leq P. \quad (37)$$

In applying the multiantenna secrecy capacity results, we develop an outer bound in which the source and relay are modeled jointly as a multiantenna transmitter. However, unlike the average power constraint for the MIMOME

channels in (37), our outer bound requires a per antenna power constraint. To this end, we apply the results developed in [5] in which a more general transmitter covariance constraint is considered such that

$$\frac{1}{n} \sum_{i=1}^n (\mathbf{x}[i] \mathbf{x}^T[i]) \preceq \mathbf{S}, \quad (38)$$

where \mathbf{S} is a positive semidefinite matrix, and $A \preceq B$ denotes that $B - A$ is a positive semidefinite matrix. The secrecy capacity of this channel is summarized in the following theorem.

Lemma 15 ([5]). *The secrecy capacity of the MIMOME channel of (36) subject to (38) is given by*

$$C_s = \max_{0 \preceq \mathbf{K}_X \preceq \mathbf{S}} \left(\frac{1}{2} \log \det(\mathbf{I} + \mathbf{H} \mathbf{K}_X \mathbf{H}^T) - \frac{1}{2} \log \det(\mathbf{I} + \mathbf{H}_e \mathbf{K}_X \mathbf{H}_e^T) \right). \quad (39)$$

Remark 16. The expression in (39) can also be written as

$$C_s = \max[I(\mathbf{X}^*; \mathbf{Y}) - I(\mathbf{X}^*; \mathbf{Y}_e)], \quad (40)$$

where the maximum is over all $\mathbf{X}^* \sim \mathcal{N}(0, \mathbf{K}_X)$.

We now present an outer bound on the Gaussian orthogonal relay eavesdropper channel using Lemma 15.

Theorem 17. *An outer bound on the secrecy capacity of the Gaussian orthogonal relay eavesdropper channel is given by the following.*

Case 1.

$$C_s \leq \max[I(X_D X_2; Y) - I(X_R; Y_2)]. \quad (41a)$$

Case 2.

$$C_s \leq \max[I(X_D X_2; Y) - I(X_D X_2; Y_2)]. \quad (41b)$$

Case 3.

$$C_s \leq \max[I(X_D X_2; Y) - I(X_R X_D X_2; Y_2)], \quad (41c)$$

where the maximum is over all $[X_R X_D X_2]^T \sim \mathcal{N}(0, \mathbf{K}_X)$ where $\mathbf{K}_X = E[\mathbf{X}\mathbf{X}^T]$ has diagonal entries that satisfy (8).

Remark 18. In (41a) and (41c), the X_R^* maximizing the outer bound on the secrecy capacity is $X_R^* = 0$. On the other hand, X_R^* can be chosen to be arbitrary for (41b).

Proof. An outer bound on the secrecy capacity of the relay eavesdropper channel results from assuming that the source and relay can cooperate over a noiseless link without causality constraints. Under this assumption, the problem reduces to that of a MIMOME channel. Thus, applying

Lemma 15 and using the form in (40), for $\mathbf{X} = [X_R X_D X_2]^T \sim \mathcal{N}(0, \mathbf{K}_X)$, the secrecy capacity can be upper bounded as

$$C_s \leq \max[I(X_R X_D X_2; Y) - I(X_R X_D X_2; Y_2)] \quad (42)$$

$$= \max[I(X_D X_2; Y) + I(X_R; Y | X_D X_2) - I(X_R X_D X_2; Y_2)] \quad (43)$$

$$= \max[I(X_D X_2; Y) - I(X_R X_D X_2; Y_2)], \quad (44)$$

where (44) follows from the orthogonal model in (3). Finally, applying the conditions on the eavesdropper receiver for the three cases simplifies the bounds in (44) to (41a), (41b), and (41c). \square

The PDF inner bounds developed in Section 3 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 (19) with the outer bounds in (41b), for those channels in which the source and relay are clustered close enough that the bottle-neck link is the combined source-relay link to the destination and the eavesdropper overhears only the channel from the source and the relay to the destination, the secrecy capacity can be achieved. This is summarized in the following theorem.

Theorem 19. *For a class of clustered orthogonal Gaussian relay channels with*

$$I(X_D X_2; Y) < \max_{p(x_R | x_D, x_2)} I(X_D X_R; Y Y_1 | X_2), \quad (45)$$

the secrecy capacity for Case 2 is achieved by PDF and is given by the following.

Case 2.

$$C_s = \max[I(X_D X_2; Y) - I(X_D, X_2; Y_2)], \quad (46)$$

where the maximum is over $\mathbf{X} = [X_R X_D X_2]^T \sim \mathcal{N}(0, \mathbf{K}_X)$.

For a relay channel without secrecy constraints, the cut-set outer bounds are equivalent to two multiple-input multiple-output (MIMO) bounds, one that results from assuming a noiseless source-relay link and the other that results from assuming a noiseless relay-destination link. Under a secrecy constraint, the outer bound in Theorem 17 is based on the assumption of a noiseless source-relay link. The corresponding bound with a noiseless relay-destination link remains unknown.

We now consider a subclass of Gaussian orthogonal relay eavesdropper channels for which $h_{s,r} = 0$. For this subclass, the source does not send any messages on channel 1, that is, $X_R = 0$. Such a subclass is a subset of a larger subclass of channels with very noisy unreliable links from the source to the relay. We present an upper bound on the secrecy

capacity for this subclass and show that the noise-forwarding strategy introduced in [11] achieves this outer bound. Central to our proof is an additional constraint introduced in developing the outer bounds on the eavesdropper that does not decode the relay transmissions. Clearly, limiting the eavesdropper capabilities can only improve the secrecy rates, and thus, an outer bound for this channel with a constrained eavesdropper is also an outer bound for the original channel (with $h_{s,r} = 0$ in both cases) with an unconstrained eavesdropper. We show that the outer bound for the constrained channel can be achieved by the strategy of noise-forwarding developed for the unconstrained channel.

Theorem 20. *The secrecy capacity of a subclass of Gaussian orthogonal relay eavesdropper channels with $h_{s,r} = 0$ for Cases 2 and 3 is given by*

$$C_s = \max_{E[X_D]^2 \leq P_D, E[X_2]^2 \leq P_2} \min \left\{ C(|h_{s,d}|^2 E[X_D^2] + |h_{r,d}|^2 E[X_2^2]) - C(|h_{s,e,2}|^2 E[X_D^2] + |h_{r,e}|^2 E[X_2^2]), \right. \\ \left. C(|h_{s,d}|^2 E[X_D^2]) - C\left(\frac{|h_{s,e,1}|^2 E[X_D^2]}{1 + |h_{r,e}|^2 E[X_2^2]}\right) \right\}. \quad (47)$$

Proof. Outer Bound. Since $h_{s,r} = 0$, it is sufficient to set $X_R = 0$. This follows from the fact that due to a lack of a communication link between the source and the relay, that is, $h_{s,r} = 0$, the relay is oblivious to the source transmissions. Since the relay and the source do not share common randomness, one can set $X_R = 0$. Finally, since X_2 depends on X_D only via X_R and $X_R = 0$, X_2 is independent of X_D .

We now provide two outer bounds for fixed $E[X_D^2]$ and $E[X_2^2]$. Thus, the minimum of the two is also an outer bound. Maximizing over $E[X_D^2]$ and $E[X_2^2]$ will then yield the outer bound as in the statement of Theorem 20.

An outer bound on the secrecy capacity is obtained by applying Theorem 17 for Cases 2 and 3 as

$$C_s \leq C(|h_{s,d}|^2 E[X_D^2] + |h_{r,d}|^2 E[X_2^2]) - C(|h_{s,e,2}|^2 E[X_D^2] + |h_{r,e}|^2 E[X_2^2]), \quad (48)$$

where (48) holds because X_D and X_2 are independent, and the Gaussian signaling is optimal, which follows from Theorem 17.

We develop a second outer bound under the assumption that the relay and the destination have a noiseless channel such that they act like a two-antenna receiver. One can alternately view this as an improved channel that results

from having a genie that shares perfectly the transmitted and received signals at the relay with the destination. Since X_2 is independent of X_D , the destination can perfectly cancel X_2 from its received signal, and thus, from (7), the effective received signal at the destination can be written as

$$Y' = h_{s,d}X_D + Z. \quad (49)$$

On the other hand for the constrained eavesdropper, since the relay's signal X_2 acts as interference and is independent of X_D , the information received at the eavesdropper is minimized when X_2 is the worst case noise, that is, when it is Gaussian distributed [18, Theorem II.1]. The equivalent signal received at the eavesdropper is then

$$Y'_{2,2} = h_{s,e,2}X_D + \sqrt{|h_{r,e}|^2 E[X_2^2] + 1}Z'_{2,2}, \quad (50)$$

where $Z'_{2,2}$ is Gaussian with zero mean and unit variance. Thus, the constrained eavesdropper channel simplifies to a MIMOME channel with a single-antenna source transmitting X_D and single-antenna receiver and eavesdropper receiving Y' and $Y'_{2,2}$, respectively. For this channel, from Lemma 15, the secrecy capacity of this constrained eavesdropper channel is upper bounded as

$$C_s \leq C(|h_{s,d}|^2 E[X_D^2]) - C\left(\frac{|h_{s,e,1}|^2 E[X_D^2]}{1 + |h_{r,e}|^2 E[X_2^2]}\right). \quad (51)$$

Finally, since (51) is an upper bound for the channel with an eavesdropper constrained to ignore X_2 , it is also an upper bound for the channel in which the eavesdropper is not constrained.

Inner Bound. The lower bound follows from the noise forwarding strategy introduced in [11, Theorem 3]. In this strategy, the relay sends codewords independent of the source message, which helps in confusing the eavesdropper. The noise forwarding strategy transforms the relay-eavesdropper channel into a compound multiple access channel, where the source/relay to the receiver is the first multiple access channel, and the source/relay to the eavesdropper is the second one. \square

5.2. 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

$$h_{m,k} = \frac{1}{d_{m,k}^{\alpha/2}} \quad \forall m \in \{s, r\}, k \in \{r, d, e\}, \quad (52)$$

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 3. Furthermore, as a baseline assuming that the relay does not transmit, that is, $X_R = 0$, 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 Figure 3. The rates are plotted in separate subfigures 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 Figure 3, for all three cases, the PDF secrecy rates are obtained by choosing the input signal $\mathbf{X} = [X_R \ X_D \ X_2]^T$ to be Gaussian distributed and numerically optimizing the rates over the covariance matrix $\mathbf{K}_X = E[\mathbf{X}\mathbf{X}^T]$ (more precisely the three variances of X_R, X_D, X_2 and the pairwise correlation among these three variables). We observe that the numerical results match the theoretical capacity result for Case 2 that PDF is optimal when the relay is close to the source. Further, the upper bounds for Cases 2 and 3 are the same as seen also in (41b)-(41c). 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 nonrelay wiretap secrecy capacity. Finally, for Cases 2 and 3, NF performs better than PDF when the relay is closer to the destination.

6. 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 on the channel from the source and the relay to the destination, our bound is tight for a subclass of channels where the source and the relay are clustered such that the combined link from the source and the relay to the destination is the bottleneck. Furthermore, for a subclass 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 (see, e.g., [19]). Also, the problem of developing an additional outer bound that considers a noiseless relay destination link remains open for the channel studied here.

Appendices

A. Proof of Theorem 7

In this section, we will prove the upper bounds on the secrecy capacity for all the three cases. Following a proof similar to that in [11, Theorem 1], we bound the equivocation as

$$nR_e \leq \sum_{i=1}^n \left[I(W_1; Y_i | Y^{i-1}, Y_{2,i+1}^n) - I(W_1; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + n\delta_n. \quad (\text{A.1})$$

Now, let J be a random variable uniformly distributed over $\{1, 2, \dots, n\}$ and set $U = JY^{i-1}Y_{2,i+1}^n$, $V_R = JY_{2,i+1}W_1$, $V_D = JY_{2,i+2}W_1$, $V_2 = JY^{i-1}$, $Y_1 = Y_{1,J}$, $Y_2 = Y_{2,J}$, and $Y = Y_J$. We specialize the bounds in (A.1) separately for each case.

Case 1. From (A.1), we have

$$\begin{aligned} R_e &\leq \frac{1}{n} \sum_{i=1}^n \left[I(W_1; Y_i | Y^{i-1}, Y_{2,i+1}^n) - I(W_1; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\ &= \frac{1}{n} \sum_{i=1}^n \left[I(W_1, Y_{2,i+2}, Y^{i-1}; Y_i | Y^{i-1}, Y_{2,i+1}^n) - I(W_1, Y_{2,i+1}; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\ &= I(V_D, V_2; Y | U) - I(V_R; Y_2 | U) + \delta_n. \end{aligned} \quad (\text{A.2})$$

Furthermore,

$$\begin{aligned} R_e &\leq \frac{1}{n} \sum_{i=1}^n \left[I(W_1; Y_i | Y^{i-1}, Y_{2,i+1}^n) - I(W_1; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\ &= \frac{1}{n} \sum_{i=1}^n \left[I(W_1, Y_{2,i+1}, Y^{i-1}; Y_i | Y^{i-1}, Y_{2,i+1}^n) - I(W_1, Y_{2,i+1}; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\ &\leq \frac{1}{n} \sum_{i=1}^n \left[I(W_1, Y_{2,i+1}, Y^{i-1}; Y_i, Y_{1,i} | Y^{i-1}, Y_{2,i+1}^n) - I(W_1, Y_{2,i+1}; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\ &= I(V_D, V_R, V_2; Y, Y_1 | V_2, U) - I(V_R; Y_2 | U) + \delta_n. \end{aligned} \quad (\text{A.3})$$

This proves the upper bound for Case 1.

Case 2. From (A.1), we have

$$\begin{aligned}
 R_e &\leq \frac{1}{n} \sum_{i=1}^n \left[I(W_1; Y_i | Y^{i-1}, Y_{2,i+1}^n) \right. \\
 &\quad \left. - I(W_1; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\
 &= \frac{1}{n} \sum_{i=1}^n \left[I(W_1, Y_{2,i+2}^n, Y^{i-1}; Y_i | Y^{i-1}, Y_{2,i+1}^n) \right. \\
 &\quad \left. - I(W_1, Y_{2,i+2}^n, Y^{i-1}; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\
 &= I(V_D, V_2; Y | U) - I(V_D, V_2; Y_2 | U) + \delta_n.
 \end{aligned} \tag{A.4}$$

Furthermore,

$$\begin{aligned}
 R_e &\leq \frac{1}{n} \sum_{i=1}^n \left[I(W_1; Y_i | Y^{i-1}, Y_{2,i+1}^n) \right. \\
 &\quad \left. - I(W_1; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\
 &= \frac{1}{n} \sum_{i=1}^n \left[I(W_1, Y_{2,i+1}^n, Y^{i-1}; Y_i | Y^{i-1}, Y_{2,i+1}^n) \right. \\
 &\quad \left. - I(W_1, Y_{2,i+2}^n, Y^{i-1}; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\
 &\leq \frac{1}{n} \sum_{i=1}^n \left[I(W_1, Y_{2,i+1}^n, Y^{i-1}; Y_i, Y_{1,i} | Y^{i-1}, Y_{2,i+1}^n) \right. \\
 &\quad \left. - I(W_1, Y_{2,i+2}^n, Y^{i-1}; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\
 &= I(V_D, V_R, V_2; Y, Y_1 | V_2, U) \\
 &\quad - I(V_D, V_2; Y_2 | U) + \delta_n.
 \end{aligned} \tag{A.5}$$

This proves the upper bound for Case 2.

Case 3. From (A.1), we have

$$\begin{aligned}
 R_e &\leq \frac{1}{n} \sum_{i=1}^n \left[I(W_1; Y_i | Y^{i-1}, Y_{2,i+1}^n) \right. \\
 &\quad \left. - I(W_1; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\
 &= \frac{1}{n} \sum_{i=1}^n \left[I(W_1, Y_{2,i+2}^n, Y^{i-1}; Y_i | Y^{i-1}, Y_{2,i+1}^n) \right. \\
 &\quad \left. - I(W_1, Y_{2,i+1}^n, Y^{i-1}; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\
 &= I(V_D, V_2; Y | U) - I(V_R, V_D, V_2; Y_2 | U) + \delta_n.
 \end{aligned} \tag{A.6}$$

Furthermore,

$$\begin{aligned}
 R_e &\leq \frac{1}{n} \sum_{i=1}^n \left[I(W_1; Y_i | Y^{i-1}, Y_{2,i+1}^n) \right. \\
 &\quad \left. - I(W_1; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\
 &= \frac{1}{n} \sum_{i=1}^n \left[I(W_1, Y_{2,i+1}^n, Y^{i-1}; Y_i | Y^{i-1}, Y_{2,i+1}^n) \right. \\
 &\quad \left. - I(W_1, Y_{2,i+1}^n, Y^{i-1}; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\
 &\leq \frac{1}{n} \sum_{i=1}^n \left[I(W_1, Y_{2,i+1}^n, Y^{i-1}; Y_i, Y_{1,i} | Y^{i-1}, Y_{2,i+1}^n) \right. \\
 &\quad \left. - I(W_1, Y_{2,i+1}^n, Y^{i-1}; Y_{2,i} | Y^{i-1}, Y_{2,i+1}^n) \right] + \delta_n \\
 &= I(V_D, V_R, V_2; Y, Y_1 | V_2, U) \\
 &\quad - I(V_D, V_2; Y_2 | U) + \delta_n.
 \end{aligned} \tag{A.7}$$

This proves the upper bound for Case 3. For perfect secrecy, setting $R_1 = R_e$ yields the upper bound on the secrecy capacity.

B. Proof of Theorem 8: PDF for Relay Eavesdropper Channel

Random Coding.

- (1) Generate $2^{n(I(X_2; Y) - \epsilon)}$ independent and identically distributed (i.i.d.) \mathbf{x}_2 's, each with probability $p(\mathbf{x}_2) = \prod_{i=1}^n p(x_{2,i})$. Label them $x_2(m)$, $m \in [1, 2^{n(I(X_2; Y) - \epsilon)}]$.
- (2) For each $x_2(m)$, generate 2^{nR_1} i.i.d. \mathbf{v} 's, each with probability $p(\mathbf{v} | x_2(m)) = \prod_{i=1}^n p(v_i | x_{2,i}(m))$. Label these $v(w' | m)$, $w \in [1, 2^{nR_1}]$.
- (3) For every $v(w' | m)$, generate 2^{nR_2} i.i.d. \mathbf{x}_1 's, each with probability $p(\mathbf{x}_1 | v(w' | m)) = \prod_{i=1}^n p(x_{1,i} | v_i(w' | m))$. Label these $x_1(w'' | m, w')$, $w'' \in [1, 2^{nR_2}]$.

Random Partition. Randomly partition the set $\{1, 2, \dots, 2^{nR_1}\}$ into $2^{n(I(X_2; Y) - \epsilon)}$ cells S_m .

Encoding. Let w_i be the message to be sent in block i where the total number of messages is $2^{n(R_1 + R_2 - I(X_1, X_2; Y_2))}$. Further, let $g_i = (w_i, l_i)$ where $l_i \in \{1, 2, \dots, 2^{nI(X_1, X_2; Y_2)}\}$. We can further partition g_i into two parts (w'_i, w''_i) of rates R_1 and R_2 , respectively. Assume that $(y_1(i-1), v(w'_{i-1} | m_{i-1}), x_2(m_{i-1}))$ are jointly ϵ -typical and $w'_{i-1} \in S_{m_i}$. Then the codeword $(x_1(w''_i | m_i, w'_i), x_2(m_i))$ will be transmitted in block i .

Decoding. At the end of block i , we have the following.

- (1) The receiver estimates m_i by looking at jointly ϵ -typical $x_2(m_i)$ with y_i . For sufficiently large n , this decoding step can be done with arbitrarily small probability of error. Let the estimate of m_i be \hat{m}_i .

- (2) The receiver calculates a set $L_1(y(i-1))$ of w' such that $w' \in L_1(y(i-1))$ if $(v(w' | m_{i-1}), y(i-1))$ are jointly ϵ -typical. The receiver then declares that w'_{i-1} was sent in block $i-1$ if $\hat{w}'_{i-1} \in S_{m_i} \cap L_1(y(i-1))$. The probability that $\hat{w}'_{i-1} = w'_{i-1}$ with arbitrarily high probability provided that n is sufficiently large and $R_1 < I(X_2; Y) + I(V; Y | X_2) - \epsilon$.
- (3) The receiver declares that w''_{i-1} was sent in block $i-1$ if $(x_1(\hat{w}''_{i-1} | \hat{m}_{i-1}, \hat{w}'_{i-1}), y(i-1))$ are jointly ϵ -typical. $\hat{w}''_{i-1} = w''_{i-1}$ with high probability if $R_2 = I(X_1; Y | X_2, V) - \epsilon$ and n is sufficiently large.
- (4) The relay upon receiving $y_1(i)$ declares that \hat{w}' was received if $(v(\hat{w}' | m_i), y_1(i), x_2(m_i))$ are jointly ϵ -typical. $w'_i = \hat{w}'$ with high probability if $R_1 < I(V; Y_1 | X_2)$ and n is sufficiently large. Thus, the relay knows that $w'_i \in S_{m_{i+1}}$.

Thus, we obtain

$$\begin{aligned} R_1 &< I(X_2; Y) + I(V; Y | X_2) - \epsilon, \\ R_1 &< I(V; Y_1 | X_2), \\ R_2 &= I(X_1; Y | X_2, V) - \epsilon. \end{aligned} \quad (\text{B.8})$$

Therefore, the rate of transmission from X_1 to Y is bounded by

$$\begin{aligned} R &= R_1 + R_2 - I(X_1 X_2; Y_2) \\ &= \min\{I(X_1; Y | X_2, V) + I(V; Y_1 | X_2), I(X_1 X_2 V; Y)\} \\ &\quad - I(X_1 X_2; Y_2). \end{aligned} \quad (\text{B.9})$$

Equivocation Computation. From [11, Theorem 2, equation (41)], we have

$$H(W_1 | Y_2) \geq H(X_1) - I(X_1, X_2; Y_2) - H(X_1, X_2 | W_1, Y_2). \quad (\text{B.10})$$

Consider $H(X_1, X_2 | W_1, Y_2)$. Since we know W_1 , the only uncertainty is the knowledge of l_i which can be decoded from Y_2 with arbitrarily small probability of error since $l_i \in \{1, \dots, 2^{nI(X_1 X_2; Y_2)}\}$. Hence,

$$H(W_1 | Y_2) \geq n(R_1 + R_2) - I(X_1, X_2; Y_2) = nR \quad (\text{B.11})$$

thus giving $R_e = R$, and hence we get perfect secrecy.

Thus, the secrecy rate is given by

$$\begin{aligned} R &= \min\{I(X_1; Y X_2, V) + I(V; Y_1 X_2), \\ &\quad I(X_1 X_2 V; Y)\} - I(X_1 X_2; Y_2). \end{aligned} \quad (\text{B.12})$$

C. Proof of Theorem 9: PDF for Relay Eavesdropper Channel with Orthogonal Components

From Theorem 8, a secrecy rate of

$$\begin{aligned} R &= \min\{I(X_1; Y | X_2, V) + I(V; Y_1 | X_2), \\ &\quad I(X_1 X_2 V; Y)\} - I(X_1 X_2; Y_2) \end{aligned} \quad (\text{C.13})$$

can be achieved by partial decode and forward. Let $X_1 = (X_R, X_D)$ and $V = X_R$ such that the input distribution is of the form $p(x_2)p(x_R | x_2)p(x_D | x_2)$. The achievable secrecy rate is then given by

$$\begin{aligned} R &= \min\{I(X_R X_D; Y | X_2, X_R) + I(X_R; Y_1 | X_2), \\ &\quad I(X_R X_D X_2; Y)\} - I(X_R X_D X_2; Y_2) \end{aligned} \quad (\text{C.14})$$

$$\begin{aligned} &= \min\{I(X_D; Y | X_2, X_R) + I(X_R; Y_1 | X_2), \\ &\quad I(X_D X_2; Y)\} - I(X_R X_D X_2; Y_2) \end{aligned} \quad (\text{C.15})$$

$$\begin{aligned} &= \min\{I(X_D; Y | X_2) + I(X_R; Y_1 | X_2), \\ &\quad I(X_D X_2; Y)\} - I(X_R X_D X_2; Y_2). \end{aligned} \quad (\text{C.16})$$

The equality in (C.16) follows from the fact that $X_D - X_2 - X_R$ is a Markov chain. We further specialize the bounds for the three cases based on the receiving capability of the eavesdropper.

Case 1.

$$\begin{aligned} R &= \min\{I(X_D; Y | X_2) + I(X_R; Y_1 | X_2), \\ &\quad I(X_D X_2; Y)\} - I(X_R; Y_2). \end{aligned} \quad (\text{C.17})$$

The maximization of the expression to the right of the equality in (C.17) over $p(x_D, x_R, x_2) = p(x_2)p(x_R | x_2)p(x_D | x_2)$ is equivalent to maximizing over the more general distribution $p(x_D, x_R, x_2)$, and henceforth, without loss of generality we consider the general probability distribution $p(x_D, x_R, x_2)$.

We now prove that $I(X_D; Y | X_2) + I(X_R; Y_1 | X_2) \geq I(X_D X_R; Y Y_1 | X_2)$ which completes the proof of this part of the theorem. We have

$$\begin{aligned} &I(X_D; Y | X_2) + I(X_R; Y_1 | X_2) \\ &= H(Y | X_2) - H(Y | X_2 X_D) + I(X_R; Y_1 | X_2) \\ &\geq H(Y | X_2 Y_1) - H(Y | X_2 X_D) + I(X_R; Y_1 | X_2) \\ &= H(Y | X_2 Y_1) - H(Y | X_2 X_D X_R Y_1) + I(X_R; Y_1 | X_2) \\ &= I(Y; X_D X_R | X_2 Y_1) + I(X_R; Y_1 | X_2) \\ &= I(Y; X_D X_R | X_2 Y_1) + I(X_D; Y_1 | X_2 X_R) \\ &\quad + I(X_R; Y_1 | X_2) \\ &= I(Y; X_D X_R | X_2 Y_1) + I(X_R X_D; Y_1 | X_2) \\ &= I(Y Y_1; X_D X_R | X_2). \end{aligned} \quad (\text{C.18})$$

Case 2.

$$\begin{aligned} R &= \min\{I(X_D; Y | X_2) + I(X_R; Y_1 | X_2), \\ &\quad I(X_D X_2; Y)\} - I(X_D X_2; Y_2). \end{aligned} \quad (\text{C.19})$$

Note that maximization of above term over $p(x_D, x_R, x_2) = p(x_2)p(x_R | x_2)p(x_D | x_2)$ is equivalent to

maximizing over general $p(x_D, x_R, x_2)$, and henceforth, without loss of generality we consider the general probability distribution $p(x_D, x_R, x_2)$.

We now prove that $I(X_D; Y | X_2) + I(X_R; Y_1 | X_2) \geq I(X_D X_R; Y Y_1 | X_2)$ which completes the proof of this part of the theorem. We have

$$\begin{aligned} & I(X_D; Y | X_2) + I(X_R; Y_1 | X_2) \\ &= H(Y | X_2) - H(Y | X_2 X_D) + I(X_R; Y_1 | X_2) \\ &\geq H(Y | X_2 Y_1) - H(Y | X_2 X_D) + I(X_R; Y_1 | X_2) \\ &= I(Y Y_1; X_D X_R | X_2), \end{aligned} \quad (\text{C.20})$$

where the last step follows as was shown earlier in (C.18).

Case 3.

$$\begin{aligned} R &= \min\{I(X_D; Y | X_2) + I(X_R; Y_1 | X_2), I(X_D X_2; Y)\} \\ &\quad - I(X_R; Y_2 | X_2 X_D) - I(X_D X_2; Y_2) \\ &= \min\{I(X_D; Y | X_2) + I(X_R; Y_1 | X_2), I(X_D X_2; Y)\} \\ &\quad - I(X_R; Y_2 | X_2) - I(X_D X_2; Y_2). \end{aligned} \quad (\text{C.21})$$

Note that maximization of above term over $p(x_D, x_R, x_2) = p(x_2)p(x_R | x_2)p(x_D | x_2)$ is equivalent to maximizing over general $p(x_D, x_R, x_2)$.

We now prove that $I(X_D; Y | X_2) + I(X_R; Y_1 | X_2) \geq I(X_D X_R; Y Y_1 | X_2)$ which completes the proof of this part of the theorem. We have

$$\begin{aligned} & I(X_D; Y | X_2) + I(X_R; Y_1 | X_2) \\ &= H(Y | X_2) - H(Y | X_2 X_D) + I(X_R; Y_1 | X_2) \\ &\geq H(Y | X_2 Y_1) - H(Y | X_2 X_D) + I(X_R; Y_1 | X_2) \\ &= I(Y Y_1; X_D X_R | X_2), \end{aligned} \quad (\text{C.22})$$

where the last step follows as was shown earlier in (C.18).

Acknowledgments

The authors wish to thank Elza Erkip of Polytechnic Institute of NYU and Lifeng Lai and Ruoheng Liu of Princeton University for useful discussions related to this paper. The work of V. Aggarwal and A. R. Calderbank was supported in part by NSF under Grant 0701226, by ONR under Grant N00173-06-1-G006, and by AFOSR under Grant FA9550-05-1-0443. The work of L. Sankar and H. V. Poor was supported in part by the National Science Foundation under Grant CNS-06-25637. The material in this paper was presented in part at the Information Theory and Applications Workshop, San Diego, CA, 2009 and at the IEEE International Symposium on Information Theory, Seoul, Korea, 2009.

References

- [1] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- [3] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.
- [4] A. Khisti and G. W. Wornell, "The MIMOME channel," in *Proceedings of the 45th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Ill, USA, September 2007.
- [5] T. Liu and S. Shamai, "A note on the secrecy capacity of the multi-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, 2009.
- [6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proceedings of the IEEE International Symposium on Information Theory*, pp. 524–528, Toronto, Canada, July 2008.
- [7] M. Bloch and A. Thangaraj, "Confidential messages to a cooperative relay," in *Proceedings of the IEEE Information Theory Workshop (ITW '08)*, pp. 154–158, Porto, Portugal, May 2008.
- [8] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 976–1002, 2008.
- [9] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.
- [10] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdú, "Capacity of cognitive interference channels with and without secrecy," *IEEE Transactions on Information Theory*, vol. 55, no. 2, pp. 604–619, 2009.
- [11] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.
- [12] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in *Proceedings of the 41st Annual Conference on Information Sciences and Systems (CISS '07)*, pp. 13–18, March 2007.
- [13] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proceedings of the IEEE International Symposium on Information Theory*, Nice, France, June 2007.
- [14] A. El Gamal and S. Zahedi, "Capacity of a class of relay channels with orthogonal components," *IEEE Transactions on Information Theory*, vol. 51, no. 5, pp. 1815–1817, 2005.
- [15] X. He and A. Yener, "On the equivocation region of relay channels with orthogonal components," in *Proceedings of the 41st Annual Asilomar Conference on Signals, Systems and Computers*, pp. 883–887, Pacific Grove, Calif, USA, November 2007.
- [16] G. Kramer, "Models and theory for relay channels with receive constraints," in *Proceedings of the 42nd Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Ill, USA, September 2004.
- [17] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley & Sons, New York, NY, USA, 1991.

- [18] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3072–3081, 2001.
- [19] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, "Information secrecy from multiple eavesdroppers in orthogonal relay channels," in *Proceedings of the IEEE International Symposium on Information Theory*, Seoul, Korea, June-July 2009.