# Secure Communication over Parallel Relay Channel

Zohaib Hassan Awan, Abdellatif Zaidi, and Luc Vandendorpe, *Fellow, IEEE* .

## Abstract

We investigate the problem of secure communication over the parallel relay channel in the presence of a passive eavesdropper. We consider a four terminal relay-eavesdropper channel which consists of multiple independent relay-eavesdropper channels as subchannels. For the discrete memoryless model, we establish outer and inner bounds on the rate-equivocation region. The inner bound allows mode selection at the relay. For each subchannel, secure transmission is obtained through one of the two coding schemes at the relay: decoding-and-forwarding the source message or confusing the eavesdropper through noise injection. For the Gaussian memoryless channel, we establish lower and upper bounds on the perfect secrecy rate. We show that lower and upper bound coincide in some special cases, including when the relay does not hear the source. The results established for the parallel Gaussian relay-eavesdropper channel are then applied to study the fading relay-eavesdropper channel. Analytical results are illustrated through some numerical examples.

## Index Terms

Parallel relay channels, fading channels, security, power allocation.

arXiv:1011.2115v1 [cs.IT] 9 Nov 2010

## I. INTRODUCTION

The wiretap channel introduced by Wyner is a basic information theoretic model which incorporates physical layer attributes of the channel to transmit information securely [1]. Wyner's basic model consists of a source, a legitimate receiver and an eavesdropper (wiretapper) under noisy channel conditions. Secrecy capacity is established when the eavesdropper channel (the channel from the transmitter to the eavesdropper) is a degraded version of the main channel (the channel from the source to the legitimate receiver). The discrete memoryless (DM) channel studied by Wyner is further extended to study some other channels for which secrecy capacity is established, i.e, broadcast channels (BC) [2], [3], multi-antenna channels [4], [5], [6], etc. The idea of cooperation between users in context of security was introduced in [7]. The premise is that when the main channel is more noisy than the channel to the eavesdropper, cooperation between users is utilized to achieve positive secrecy capacity. Secrecy is achieved by using the relay as a trusted node that facilitates the information decoding at the destination while concealing the information from the eavesdropper.

In this paper, we study a parallel relay-eavesdropper channel. A parallel relay-eavesdropper channel is a generalization of the setup in [7], in which each of the source-to-relay (S-R), source-to-destination (S-D), source-to-eavesdropper (S-E), relay-to-destination (R-D) and relay-to-eavesdropper (R-E) link is composed of several independent parallel channels as subchannels. The eavesdropper is passive in the sense that it just listens to the transmitted information without modifying it. We only focus on the *perfect secrecy rate*, i.e., the maximum achievable rate at which information is reliably sent to the legitimate receiver and the eavesdropper is unable to decode it.

The parallel relay-eavesdropper channel considered in this paper relates to some of the channels studied previously. Compared to the parallel relay channel studied in [8], the parallel relay-eavesdropper channel requires an additional secrecy constraint. The parallel relay-eavesdropper channel without relay simplifies to a number of channels discussed previously. For example, the independent parallel wiretap channel studied in [9], the parallel broadcast channel with confidential messages (BCC) and no common message studied in [3].

*Contributions.* The main contributions of this paper are summarized as follows. For the discrete memoryless case, we establish inner and outer bounds on the rate-equivocation region for a

parallel relay-eavesdropper channel. The inner bound is obtained with a coding scheme in which, for each subchannel, the relay operates either in decode-and-forward (DF) or noise forwarding (NF) mode. The outer bound does not follow directly from the single-letter outer bound for the relay-eavesdropper channel developed in [7, Theorem 1] and so, a converse is needed. This converse includes a redefinition of the involved auxiliary random variables, a technique much similar to the one used before in the context of secure transmission over broadcast channels [3]. For the Gaussian memoryless model, we establish lower and upper bounds on the perfect secrecy rate. The lower bound established for the Gaussian model follows directly from the DM case. We note that establishing a computable upper bound on the secrecy rate for the Gaussian model is non-trivial, and it does not follow directly from the DM case. In part, this is because the upper bound established for the DM case involves auxiliary random variables, the optimal choice of which is difficult to obtain. In this work, we develop a new upper bound on the secrecy rate of the parallel Gaussian relay-eavesdropper channel. Our converse proof uses elements from converse techniques developed in [5], [6] in context of multi-antennas wiretap channel; and in a sense, can be viewed as a partial extension of these results to the case of the parallel relay-eavesdropper channel. The established upper bound on the secrecy rate shows some degree of separability for different parallel subchannels. It is especially useful when the multiple access part of the channel is the bottleneck.

We also study a special case in which the relay does not hear the source, for example due to very noisy source-to-relay links. In this case we show that noise-forwarding on all links achieves the secrecy capacity. The converse proof follows from the general converse established for the parallel Gaussian relay-eavesdropper channel and a new genie-aided upper bound that assumes full cooperation between the relay and the destination and a constrained eavesdropper. The eavesdropper is constrained in the sense that it has to treat the relay's transmission as unknown noise for all subchannels, an idea used previously in the context of a class of classic relay-eavesdropper channel with orthogonal components [10]. These assumptions turn the parallel Gaussian relay-eavesdropper channel into a parallel Gaussian wiretap channel, the secrecy capacity of which is established in [3], [9].

Furthermore, we apply the results established for the parallel Gaussian relay-eavesdropper channel to the fading relay-eavesdropper channel. The fading relay-eavesdropper channel is a special case of the parallel Gaussian relay-eavesdropper channel in which each realization of a

fading state corresponds to one subchannel. We illustrate our results through some numerical examples.

The rest of the paper is organized as follows. In Section II, we establish outer and inner bounds on the rate equivocation region for the DM channel. In section III, we establish lower and upper bounds on the perfect secrecy rate and consider a special case in which secrecy capacity is achieved. In Section IV, we present an application of the results established in section III to the fading model. We illustrate these results with some numerical examples in section V. Section VI concludes the paper by summarizing its contribution.

***Notations.*** In this paper, the notation $X_{[1,L]}$ is used as a shorthand for $(X_1, X_2, \ldots, X_L)$, the notation $X^n_{[1,L]}$ is used as a shorthand for $(X^n_1, X^n_2, \cdots, X^n_L)$ where for $l = 1, \ldots, L$, $X^n_l :=$ $(X_{l1}, X_{l2}, \cdots, X_{ln})$, the notation $\mathcal{X}_{1[1,L]}$ is used as a shorthand for $\mathcal{X}_{11} \times \mathcal{X}_{12} \ldots \times \mathcal{X}_{1L}$, $\mathbb{E}\{.\}$ denotes the expectation operator, the boldface letter $\mathbf{X}$ denotes the covariance matrix. We denote the entropy of a discrete and continuous random variable $X$ by $H(X)$ and $h(X)$ respectively. We define the functions $\mathcal{C}(x) = \frac{1}{2}\log_2(1 + x)$ and $[x]^+ = \max\{0, x\}$. Throughout the paper the logarithm function is taken to the base 2.

## II. DISCRETE MEMORYLESS CHANNEL

In this section, we establish outer and inner bounds on the rate-equivocation region for a parallel relay-eavesdropper channel.

### A. Channel Model

*Definition 1:* A parallel relay-eavesdropper channel is a four terminal network consisting of $\mathcal{X}_{1[1,L]}, \mathcal{X}_{2[1,L]}$ as finite input alphabets and $\mathcal{Y}_{[1,L]}, \mathcal{Y}_{1[1,L]}, \mathcal{Y}_{2[1,L]}$ as finite output alphabets. The transition probability distribution is given by

$$\prod_{l=1}^{L} p(y_l, y_{1l}, y_{2l} \mid x_{1l}, x_{2l}) \tag{1}$$

where $x_{1l} \in \mathcal{X}_{1l}, x_{2l} \in \mathcal{X}_{2l}, y_{1l} \in \mathcal{Y}_{1l}, y_l \in \mathcal{Y}_l$ and $y_{2l} \in \mathcal{Y}_{2l}$, for $l = 1, \cdots, L$.

*Definition 2:* The source sends a message $W \in \mathcal{W} = \{1, \cdots, 2^{nR}\}$ using a $(2^{nR}, n)$ code consisting of

- a stochastic encoder at the source that maps $W \rightarrow X^n_{1[1,L]}$,

- a relay encoder that maps $f_i(Y_{1[1,L]}^{i-1}) \to X_{2[1,L],i}$ for $1 \le i \le n$,
- a decoding function $g(Y_{[1,L]}^n) \to W$.

*Definition 3:* The average error probability of a $(2^{nR}, n)$ code is defined as

$$P_e^n = \frac{1}{2^{nR}} \sum_{W \in \mathcal{W}} p\{g(Y_{[1,L]}^n) \ne W|W\}. \tag{2}$$

Due to the openness of the wireless medium, the eavesdropper listens for free to what the source and relay transmit. It then tries to guess the information being transmitted. Denoting $Y_{2[1,L]}^n$ the output at the eavesdropper, the equivocation rate per channel use is defined as $R_e = H(W|Y_{2[1,L]}^n)/n$. Perfect secrecy for the channel is obtained when the eavesdropper gets no information about $W$ from $Y_{2[1,L]}^n$. That is, the equivocation rate is equal to the unconditional source entropy.

*Definition 4:* A rate equivocation pair $(R, R_e)$ is achievable, if for any $\epsilon > 0$ there exists a sequence of codes $(2^{nR}, n)$ such that for any $n \ge n(\epsilon)$

$$\frac{H(W)}{n} \ge R - \epsilon,$$
$$\frac{H(W|Y_{2[1,L]}^n)}{n} \ge R_e - \epsilon,$$
$$P_e^n \le \epsilon. \tag{3}$$

### B. Outer bound

*Theorem 1:* For a parallel relay-eavesdropper channel with $L$ subchannels, and for any achievable rate-equivocation pair $(R, R_e)$, there exists a set of random variables $U_l \to (V_{1l}, V_{2l}) \to (X_{1l}, X_{2l}) \to (Y_l, Y_{1l}, Y_{2l})$, $l = 1, \ldots, L$, such that $(R, R_e)$ satisfies

$$R \le \min \left\{ \sum_{l=1}^{L} I(V_{1l}V_{2l}; Y_l), \sum_{l=1}^{L} I(V_{1l}; Y_l Y_{1l} \mid V_{2l}) \right\}$$

$$R_e \le R$$

$$R_e \le \min \left\{ \sum_{l=1}^{L} I(V_{1l}V_{2l}; Y_l \mid U_l) - I(V_{1l}V_{2l}; Y_{2l} \mid U_l), \sum_{l=1}^{L} I(V_{1l}; Y_l Y_{1l} \mid V_{2l}U_l) - I(V_{1l}V_{2l}; Y_{2l} \mid U_l) \right\}. \tag{4}$$

*Proof:* See [11] for details of the proof. □

*Remark 1:* The bound in Theorem 1 does not follow directly from the single letter outer bound on the rate-equivocation region of relay-eavesdropper channel given in [7]. A converse proof is needed because we need to redefine the auxiliary random variables.

### C. Achievable rate-equivocation region

*Theorem 2:* For a parallel relay-eavesdropper channel with $L$ subchannels, the rate pairs in the closure of the convex hull of all $(R, R_e)$ satisfying

$$R \leq \min \left\{ \sum_{l \in \mathcal{A}} I(V_{1l} V_{2l}; Y_l | U_l), \sum_{l \in \mathcal{A}} I(V_{1l}; Y_{1l} | V_{2l} U_l) \right\} + \sum_{l \in \mathcal{A}^c} I(V_{1l}; Y_l | V_{2l})$$

$$R_e \leq R$$

$$R_e \leq \min \left\{ \sum_{l \in \mathcal{A}} I(V_{1l} V_{2l}; Y_l | U_l) - I(V_{1l} V_{2l}; Y_{2l} | U_l), \sum_{l \in \mathcal{A}} I(V_{1l}; Y_{1l} | V_{2l} U_l) - I(V_{1l} V_{2l}; Y_{2l} | U_l) \right\}$$

$$+ \sum_{l \in \mathcal{A}^c} I(V_{1l}; Y_l | V_{2l}) + \min \left\{ \sum_{l \in \mathcal{A}^c} I(V_{2l}; Y_l), \sum_{l \in \mathcal{A}^c} I(V_{2l}; Y_{2l} | V_{1l}) \right\} - \min \left\{ \sum_{l \in \mathcal{A}^c} I(V_{2l}; Y_l), \right.$$

$$\left. \sum_{l \in \mathcal{A}^c} I(V_{2l}; Y_{2l}) \right\} - \sum_{l \in \mathcal{A}^c} I(V_{1l}; Y_{2l} | V_{2l}), \tag{5}$$

for some distribution $p(u_l, v_{1l}, v_{2l}, x_{1l}, x_{2l}, y_l, y_{1l}, y_{2l}) = p(u_l)p(v_{1l}, v_{2l} | u_l)p(x_{1l}, x_{2l} | v_{1l}, v_{2l})p(y_l, y_{1l}, y_{2l} | x_{1l}, x_{2l})$ for $l \in \mathcal{A}$ and $p(v_{1l}, v_{2l}, x_{1l}, x_{2l}, y_l, y_{1l}, y_{2l}) = p(v_{1l})p(v_{2l})p(x_{1l} | v_{1l})p(x_{2l} | v_{2l})p(y_l, y_{1l}, y_{2l} | x_{1l}, x_{2l})$ for $l \in \mathcal{A}^c$, are achievable.

In the statement of Theorem 2, sets $\mathcal{A}$ and $\mathcal{A}^c$ represent the subchannels for which relay operates in DF and NF mode, respectively. The region in Theorem 2 is obtained through a coding scheme which combines appropriately DF and NF schemes. The rates for the DF scheme can be obtained readily by setting $U := U_{[1,|\mathcal{A}|]}, V_1 := V_{1[1,|\mathcal{A}|]}, V_2 := V_{2[1,|\mathcal{A}|]}, Y := Y_{[1,|\mathcal{A}|]}$, $Y_1 := Y_{1[1,|\mathcal{A}|]}$ and $Y_2 := Y_{2[1,|\mathcal{A}|]}$, for $l \in \mathcal{A}$ in [7, Theorem 2]. Similarly the rates for NF scheme can be readily obtained by setting $V_1 := V_{1[1,|\mathcal{A}^c|]}, V_2 := V_{2[1,|\mathcal{A}^c|]}, Y := Y_{[1,|\mathcal{A}^c|]}, Y_1 := Y_{1[1,|\mathcal{A}^c|]}$ and $Y_2 := Y_{2[1,|\mathcal{A}^c|]}$, for $l \in \mathcal{A}^c$ in [7, Theorem 3].

## III. GAUSSIAN MODEL

In this section we study a parallel Gaussian relay-eavesdropper channel. Figure 1 depicts the studied model. We only focus on the perfectly secure achievable rates, i.e., $(R, R_e) = (R, R)$.

## A. Channel Model

For a parallel Gaussian relay-eavesdropper channel, the received signals at the relay, destination and eavesdropper are given by

$$Y_{1l,i} = X_{1l,i} + Z_{1l,i}$$

$$Y_{l,i} = X_{1l,i} + \sqrt{\rho_{1l}} X_{2l,i} + Z_{l,i}$$

$$Y_{2l,i} = X_{1l,i} + \sqrt{\rho_{2l}} X_{2l,i} + Z_{2l,i} \tag{6}$$

where $i$ is the time index, $\{Z_{1l,i}\}, \{Z_{l,i}\}$ and $\{Z_{2l,i}\}$ are noise processes, independent and identically distributed (i.i.d) with the components being zero mean Gaussian random variables with variances $\sigma_{1l}^2$, $\sigma_l^2$ and $\sigma_{2l}^2$ respectively, for $l = 1, \ldots, L$. For the subchannel $l$, $X_{1l,i}$ and $X_{2l,i}$ are the inputs from the source and relay nodes respectively. The parameter $\rho_{1l}$ indicates the ratio of the R-D link signal-to-noise (SNR) to the S-D link SNR and $\rho_{2l}$ indicates the ratio of the R-E link SNR to the S-E link SNR for subchannel $l$ respectively. The source and relay input sequences are subject to separate power constraints $P_1$ and $P_2$, i.e,

$$\frac{1}{n} \sum_{l=1}^{L} \sum_{i=1}^{n} \mathbb{E}[X_{1l,i}^2] \leq P_1, \tag{7}$$

$$\frac{1}{n} \sum_{l=1}^{L} \sum_{i=1}^{n} \mathbb{E}[X_{2l,i}^2] \leq P_2. \tag{8}$$

## B. Lower Bound on the Perfect Secrecy Rate

For the parallel Gaussian relay-eavesdropper channel (6), we apply Theorem 2 to obtain a lower bound on the perfect secrecy rate.[1]

*Corollary 1:* For the parallel Gaussian relay-eavesdropper channel (6), a lower bound on the

---

[1]The results established for the DM case can be readily extended to memoryless channels with discrete time and continuous alphabets using standard techniques [12, Chapter 7].

perfect secrecy rate is given by

$$
\begin{aligned}
R_e^{\text{low}} = \max_{\substack{\sum_{l=1}^{L} P_{1l} \leq P_1, \sum_{l=1}^{L} P_{2l} \leq P_2, \\ 0 \leq \alpha_l \leq 1, \text{ for } l = 1, \ldots, |\mathcal{A}|}} \min \Bigg\{ &\sum_{l \in \mathcal{A}} \mathcal{C}\left(\frac{P_{1l} + \rho_{1l} P_{2l} + 2\sqrt{\bar{\alpha}_l \rho_{1l} P_{1l} P_{2l}}}{\sigma_l^2}\right) \\
&- \mathcal{C}\left(\frac{P_{1l} + \rho_{2l} P_{2l} + 2\sqrt{\bar{\alpha}_l \rho_{2l} P_{1l} P_{2l}}}{\sigma_{2l}^2}\right), \sum_{l \in \mathcal{A}} \mathcal{C}\left(\frac{\alpha_l P_{1l}}{\sigma_{1l}^2}\right) - \mathcal{C}\left(\frac{P_{1l} + \rho_{2l} P_{2l} + 2\sqrt{\bar{\alpha}_l \rho_{2l} P_{1l} P_{2l}}}{\sigma_{2l}^2}\right) \Bigg\} \\
&+ \sum_{l \in \mathcal{A}^c} \mathcal{C}\left(\frac{P_{1l}}{\sigma_l^2}\right) + \min\Bigg\{\sum_{l \in \mathcal{A}^c} \mathcal{C}\left(\frac{\rho_{1l} P_{2l}}{P_{1l} + \sigma_l^2}\right), \sum_{l \in \mathcal{A}^c} \mathcal{C}\left(\frac{\rho_{2l} P_{2l}}{\sigma_{2l}^2}\right)\Bigg\} \\
&- \min\Bigg\{\sum_{l \in \mathcal{A}^c} \mathcal{C}\left(\frac{\rho_{1l} P_{2l}}{P_{1l} + \sigma_l^2}\right), \sum_{l \in \mathcal{A}^c} \mathcal{C}\left(\frac{\rho_{2l} P_{2l}}{P_{1l} + \sigma_{2l}^2}\right)\Bigg\} - \sum_{l \in \mathcal{A}^c} \mathcal{C}\left(\frac{P_{1l}}{\sigma_{2l}^2}\right).
\end{aligned} \tag{9}
$$

*Proof:* The achievability follows by applying Theorem 2 with the choice $U_l =$ constant, $V_{1l} = X_{1l}$, $V_{2l} = X_{2l}$, $X_{1l} = \tilde{X}_{1l} + \sqrt{\frac{\bar{\alpha}_l P_{1l}}{P_{2l}}} X_{2l}$, $\bar{\alpha}_l = 1 - \alpha_l$, $\tilde{X}_{1l} \sim \mathcal{N}(0, \alpha_l P_{1l})$ independent of $X_{2l} \sim \mathcal{N}(0, P_{2l})$, where $\alpha_l \in [0,1]$ for $l \in \mathcal{A}$; and $X_{1l} \sim \mathcal{N}(0, P_{1l})$ independent of $X_{2l} \sim \mathcal{N}(0, P_{2l})$ for $l \in \mathcal{A}^c$. Straightforward algebra which is omitted for brevity gives (9). $\qquad\square$

The parameters $P_{1l}$ and $P_{2l}$ indicate the source and relay power allocated for transmission over the subchannel $l$. In (9), after some straightforward algebra, the contribution to the equivocation of information sent through NF (in set $\mathcal{A}^c$) can be condensed by observing that we only need to consider $\min\{\sum_{l \in \mathcal{A}^c} I(X_{2l}, Y_{2l}), \sum_{l \in \mathcal{A}^c} I(X_{2l}, Y_l)\} = \sum_{l \in \mathcal{A}^c} I(X_{2l}, Y_{2l})$, to get higher secrecy rate. A simplified expression for $R_e^{\text{low}}$ is given by

$$
\begin{aligned}
R_e^{\text{low}} = \max_{\substack{\sum_{l=1}^{L} P_{1l} \leq P_1, \sum_{l=1}^{L} P_{2l} \leq P_2, \\ 0 \leq \alpha_l \leq 1, \text{ for } l = 1, \ldots, |\mathcal{A}|}} \min \Bigg\{ &\sum_{l \in \mathcal{A}} \Bigg[ \mathcal{C}\left(\frac{P_{1l} + \rho_{1l} P_{2l} + 2\sqrt{\bar{\alpha}_l \rho_{1l} P_{1l} P_{2l}}}{\sigma_l^2}\right) \\
&- \mathcal{C}\left(\frac{P_{1l} + \rho_{2l} P_{2l} + 2\sqrt{\bar{\alpha}_l \rho_{2l} P_{1l} P_{2l}}}{\sigma_{2l}^2}\right) \Bigg]^+, \sum_{l \in \mathcal{A}} \Bigg[ \mathcal{C}\left(\frac{\alpha_l P_{1l}}{\sigma_{1l}^2}\right) - \mathcal{C}\left(\frac{P_{1l} + \rho_{2l} P_{2l} + 2\sqrt{\bar{\alpha}_l \rho_{2l} P_{1l} P_{2l}}}{\sigma_{2l}^2}\right) \Bigg]^+ \Bigg\} \\
&+ \min\Bigg\{\sum_{l \in \mathcal{A}^c}\Bigg[ \mathcal{C}\left(\frac{P_{1l} + \rho_{1l} P_{2l}}{\sigma_l^2}\right) - \mathcal{C}\left(\frac{P_{1l} + \rho_{2l} P_{2l}}{\sigma_{2l}^2}\right)\Bigg]^+, \sum_{l \in \mathcal{A}^c}\Bigg[ \mathcal{C}\left(\frac{P_{1l}}{\sigma_l^2}\right) + \mathcal{C}\left(\frac{\rho_{2l} P_{2l}}{\sigma_{2l}^2}\right) \\
&- \mathcal{C}\left(\frac{P_{1l} + \rho_{2l} P_{2l}}{\sigma_{2l}^2}\right)\Bigg]^+ \Bigg\}.
\end{aligned} \tag{10}
$$

*Remark 2:* The achievable perfect secrecy rate established in Corollary 1 can be larger than the one obtained by coding separately over different parallel subchannels.

This remark is elucidated by the following example.

*Example:* We consider a deterministic parallel relay-eavesdropper channel with two subchannels, i.e, $L = 2$, as shown in figure 2. For simplicity, we assume that the relay uses the same scheme on all subchannels (either DF or NF). For subchannel 1, the link capacities to the relay, legitimate receiver and eavesdropper are given by $C_{r1,a} = 4, C_{r1,b} = 3$ and $C_{e1} = 2$ respectively. For subchannel 2, the link capacities to the relay, legitimate receiver and eavesdropper are given by $C_{r2,a} = 5, C_{r2,b} = 7$ and $C_{e2} = 3$ respectively. For this channel, achievable rate obtained by coding across subchannels is given by

$$R_e = \min \left\{ \sum_{i=1}^{2} (C_{ri,a} - C_{ei})^+, \sum_{i=1}^{2} (C_{ri,b} - C_{ei})^+ \right\}$$

$$= \min\{4, 5\} = 4. \tag{11}$$

Similarly achievable rate obtained by coding independently over each subchannel is given by

$$R_e = \sum_{i=1}^{2} \min\{(C_{ri,a} - C_{ei})^+, (C_{ri,b} - C_{ei})^+\}$$

$$= \min\{2, 1\} + \min\{2, 4\} = 3 \tag{12}$$

which is clearly smaller than (11). This shows the usefulness of coding across subchannels.

## C. Upper Bound on the Perfect Secrecy Rate

The following theorem provides an upper bound on the secrecy rate of the parallel Gaussian relay-eavesdropper channel.

*Theorem 3:* For the parallel Gaussian relay-eavesdropper channel (6), an upper bound on the secrecy rate is given by

$$R_e^{\text{up}} \leq \max_{\{\mathbf{K}_{\mathbf{P}_l} \in \mathcal{K}_{P_l}\}_{l=1...L}} \sum_{l=1}^{L} I(X_{1l} X_{2l}; Y_l) - I(X_{1l} X_{2l}; Y_{2l}) \tag{13}$$

where the maximization is over $[X_{1l}, X_{2l}] \sim \mathcal{N}(\mathbf{0}, \mathbf{K_{P}}_l)$ with $\mathcal{K}_{P_l} = \left\{ \mathbf{K_{P}}_l : \mathbf{K_{P}}_l = \begin{bmatrix} P_{1l} & \psi_l \sqrt{P_{1l}P_{2l}} \\ \psi_l \sqrt{P_{1l}P_{2l}} & P_{2l} \end{bmatrix}, \right.$

$\left. -1 \leq \psi_l \leq 1 \right\}$, for $l = 1, \ldots, L$, with the covariance matrices $\mathbb{E}[X_{1[1,L]} X_{1[1,L]}^T]$, $\mathbb{E}[X_{2[1,L]} X_{2[1,L]}^T]$

satisfying (7) and (8) respectively.

*Proof:* The proof follows from the rate-equivocation region established for the DM case in Theorem 1. Taking the first term of minimization in the bound on the equivocation rate in Theorem 1, we get

$$R_e^{\text{up}} \leq \max \sum_{l=1}^{L} I(V_{1l}V_{2l}; Y_l \mid U_l) - I(V_{1l}V_{2l}; Y_{2l} \mid U_l) \tag{14}$$

where $U_l \to (V_{1l}, V_{2l}) \to (X_{1l}, X_{2l}) \to (Y_l, Y_{1l}, Y_{2l})$, for $l = 1, \ldots, L$. The rest of the proof uses elements from related works in [3] and [5]. Continuing from (14), we obtain

$$R_e^{\text{up}} \leq \sum_{l=1}^{L} I(V_{1l}V_{2l}; Y_l \mid U_l) - I(V_{1l}V_{2l}; Y_{2l} \mid U_l)$$

$$\overset{(a)}{\leq} \sum_{l=1}^{L} I(V_{1l}V_{2l}; Y_l) - I(V_{1l}V_{2l}; Y_{2l})$$

$$\leq \sum_{l=1}^{L} I(V_{1l}V_{2l}; Y_l Y_{2l}) - I(V_{1l}V_{2l}; Y_{2l})$$

$$\overset{(b)}{=} \sum_{l=1}^{L} [I(X_{1l}X_{2l}; Y_l Y_{2l}) - I(X_{1l}X_{2l}; Y_l Y_{2l} \mid V_{1l}V_{2l})]$$

$$\quad - [I(X_{1l}X_{2l}; Y_{2l}) - I(X_{1l}X_{2l}; Y_{2l} \mid V_{1l}V_{2l})]$$

$$= \sum_{l=1}^{L} [I(X_{1l}X_{2l}; Y_l Y_{2l}) - I(X_{1l}X_{2l}; Y_{2l})]$$

$$\quad - [I(X_{1l}X_{2l}; Y_l Y_{2l} \mid V_{1l}V_{2l}) - I(X_{1l}X_{2l}; Y_{2l} \mid V_{1l}V_{2l})]$$

$$\leq \sum_{l=1}^{L} [I(X_{1l}X_{2l}; Y_l Y_{2l}) - I(X_{1l}X_{2l}; Y_{2l})]$$

$$= \sum_{l=1}^{L} I(X_{1l}X_{2l}; Y_l \mid Y_{2l}) \tag{15}$$

where (a) follows by noticing that $I(V_{1l}V_{2l}; Y_l \mid U_l) - I(V_{1l}V_{2l}; Y_{2l} \mid U_l)$ is maximized by setting $U_l = $ constant and (b) follows from the Markov chain condition $(V_{1l}, V_{2l}) \to (X_{1l}, X_{2l}) \to (Y_l, Y_{1l}, Y_{2l})$, for $l = 1, \ldots, L$.

We now tighten the upper bound (15) by using an argument previously used in [5], [6] in the context of multi-antennas wiretap channel. More specifically, observing that, the original bound (14) depends on $p(y_l, y_{2l}|x_{1l}, x_{2l})$ only through its marginals $p(y_l|x_{1l}, x_{2l})$ and $p(y_{2l}|x_{1l}, x_{2l})$, the upper bound (15) can be further tightened as

$$R_e^{\text{up}} \leq \max_{p(x_{1l}, x_{2l})} \sum_{l=1}^{L} \min_{p(y_l', y_{2l}'|x_{1l}, x_{2l})} I(X_{1l}X_{2l}; Y_l' \mid Y_{2l}') \qquad (16)$$

where the joint conditional $p(y_l', y_{2l}'|x_{1l}, x_{2l})$ has the same marginals as $p(y_l, y_{2l}|x_{1l}, x_{2l})$, i.e., $p(y_l'|x_{1l}, x_{2l}) = p(y_l|x_{1l}, x_{2l})$ and $p(y_{2l}'|x_{1l}, x_{2l}) = p(y_{2l}|x_{1l}, x_{2l})$.

It can be easily shown that the bound in (16) is maximized when the inputs are jointly Gaussian, i.e., $[X_{1l}, X_{2l}] \sim \mathcal{N}(\mathbf{0}, \mathbf{K}_{\mathbf{P}_l})$, $\mathbf{K}_{\mathbf{P}_l} \in \mathcal{K}_{P_l}$ with $\mathcal{K}_{P_l} = \left\{ \mathbf{K}_{\mathbf{P}_l} : \mathbf{K}_{\mathbf{P}_l} = \begin{bmatrix} P_{1l} & \psi_l \sqrt{P_{1l}P_{2l}} \\ \psi_l \sqrt{P_{1l}P_{2l}} & P_{2l} \end{bmatrix}, -1 \leq \psi_l \leq 1 \right\}$, for $l = 1, \ldots, L$ with the covariance matrices $\mathbb{E}[X_{1[1,L]}X_{1[1,L]}^T]$ and $\mathbb{E}[X_{2[1,L]}X_{2[1,L]}^T]$ satisfying (7) and (8) respectively [5], [6].

Next, using the specified Gaussian inputs, it can be shown that the evaluation of the upper bound (16) minimized over all possible correlations between $Y_l', Y_{2l}'$, for $l = 1, \ldots, L$ yields

$$R_e^{\text{up}} \leq \max_{\{\mathbf{K}_{\mathbf{P}_l} \in \mathcal{K}_{P_l}\}_{l=1\ldots L}} \sum_{l=1}^{L} I(X_{1l}X_{2l}; Y_l) - I(X_{1l}X_{2l}; Y_{2l}). \qquad (17)$$

This concludes the proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

The computation of the upper bound is given in Appendix I

### D. Special Case

We now study the case in which the S-R links are very noisy, i.e., the relay does not hear the source.

**Theorem 4:** For the model (6) in which the relay does not hear the source, the secrecy capacity is given by

$$C_s = \min \left\{ \max \sum_{l=1}^{L} \mathcal{C}\left(\frac{P_{1l} + \rho_{1l}P_{2l}}{\sigma_l^2}\right) - \mathcal{C}\left(\frac{P_{1l} + \rho_{2l}P_{2l}}{\sigma_{2l}^2}\right), \max \sum_{l=1}^{L} \mathcal{C}\left(\frac{P_{1l}}{\sigma_l^2}\right) - \mathcal{C}\left(\frac{P_{1l}}{\sigma_{2l}^2 + \rho_{2l}P_{2l}}\right) \right\}$$

$$\qquad\qquad (18)$$

where the maximization is over $\{P_{1l}, P_{2l}\}$, for $l = 1 \ldots L$, such that $\sum_{l=1}^{L} P_{1l} \leq P_1$ and $\sum_{l=1}^{L} P_{2l} \leq P_2$.

   *Proof:*

**Upper Bound**: The bound given by the first term of the minimization in (18) follows from a straightforward application of the result in Theorem 3 — taking independent source and relay inputs since the relay does not hear the source transmission in this case.

   The bound given by the second term of the minimization in (18) can be established as follows. Our approach borrows elements from an upper bounding technique that is used in [10], and can be seen as an extension of it to the case of parallel relay-eavesdropper channels. Assume that all links between the relay and the destination are noiseless, and the eavesdropper is constrained to treat the relay's signal as unknown noise. As mentioned in [10], any upper bound for this model with full relay-destination cooperation and constrained eavesdropper, also applies to the general model.

   Now, for the model with full relay-destination cooperation and constrained eavesdropper, we develop an upper bound on the secrecy capacity as follows. In this case, the destination can remove the effect of the relay transmission (which is independent from the source transmission as the relay does not hear the source), and the equivalent channel to the destination can be written as

$$Y'_{l,i} = X_{1l,i} + Z_{l,i}. \tag{19}$$

For the constrained eavesdropper the relay's transmission acts as an interference, with the worst case obtained with the Gaussian $X_{2l}$, for $l = 1 \ldots, L$ [10]. The equivalent output at the eavesdropper in this case is given by

$$Y'_{2l,i} = X_{1l,i} + \sqrt{\rho_{2l}\mathbb{E}[X_{2l,i}^2]} + Z_{2l,i}. \tag{20}$$

The rest of the proof follows by simply observing that the resulting model (with the worst case relay transmission to the eavesdropper and full relay-destination cooperation) is, in fact, a parallel Gaussian wiretap channel, the secrecy capacity of which is established in [3], i.e,

$$C_s \leq \max \sum_{l=1}^{L} I(X_{1l}; Y'_l) - I(X_{1l}; Y'_{2l}) \tag{21}$$

where the maximization is over $X_{1l} \sim \mathcal{N}(0, P_{1l})$, $X_{2l} \sim \mathcal{N}(0, P_{2l})$ for $l = 1 \ldots L$, with $\sum_{l=1}^{L} P_{1l} \leq P_1$ and $\sum_{l=1}^{L} P_{2l} \leq P_2$.

Finally straightforward algebra which is omitted for brevity shows that the computation of (21) gives the second term of the minimization in (18).

**Lower Bound**: The achievability follows by computing the lower bound in Theorem 2 with the choices $|\mathcal{A}^c| := L$, $V_{1l} := X_{1l}$, $V_{2l} := X_{2l}$, and $X_{1l} \sim \mathcal{N}(0, P_{1l})$ independent of $X_{2l} \sim \mathcal{N}(0, P_{2l})$.

$\square$

## IV. APPLICATION

In this section we apply the results which we established for the Gaussian memoryless model in section III to study a fading relay-eavesdropper channel.

For a fading relay-eavesdropper channel, the received signals at the relay, legitimate receiver and eavesdropper are given by

$$Y_{1,i} = h_{sr,i} X_{1,i} + Z_{1,i}$$

$$Y_i = h_{sd,i} X_{1,i} + h_{rd,i} X_{2,i} + Z_i$$

$$Y_{2,i} = h_{se,i} X_{1,i} + h_{re,i} X_{2,i} + Z_{2,i} \tag{22}$$

where $i$ is the time index, $h_{sd,i}$, $h_{rd,i}$, $h_{se,i}$, $h_{re,i}$ and $h_{sr,i}$ are the fading gain coefficients associated with S-D, R-D, S-E, R-E and S-R links, given by complex Gaussian random variables with zero mean and unit variance respectively. The noise processes $\{Z_{1,i}\}, \{Z_i\}, \{Z_{2,i}\}$ are zero mean i.i.d complex Gaussian random variables with variances $\sigma_1^2$, $\sigma^2$ and $\sigma_2^2$ respectively. The source and relay input sequences are subject to an average power constraint, i.e, $\sum_{i=1}^{n} \mathbb{E}[|X_{1,i}|^2] \leq nP_1$, $\sum_{i=1}^{n} \mathbb{E}[|X_{2,i}|^2] \leq nP_2$. We define $\bar{h}_i := [h_{sd,i} \ h_{rd,i} \ h_{se,i} \ h_{re,i} \ h_{sr,i}]$ and assume that perfect channel state information (CSI) is available at all nodes, i.e, each node has access to the instantaneous CSI and its statistics. For a given fading state realization $\bar{h}_i$, the fading relay-eavesdropper channel is a Gaussian relay-eavesdropper channel. Therefore, for a given channel state with $L$ fading state realizations, i.e, $\bar{h} = \{\bar{h}_i\}_{i=1}^{L}$, the fading relay-eavesdropper channel can be seen as a parallel Gaussian relay-eavesdropper channel with $L$ subchannels. The power allocation vectors at the source and relay are denoted by $P_1(\bar{h})$ and $P_2(\bar{h})$ respectively. The ergodic achievable secrecy rate of the fading relay-eavesdropper channel (22), which follows

from (10) is given by

$$
\begin{aligned}
R_e^{\text{low}} = \max_{\substack{\mathbb{E}[P_1(\bar{h})] \leq P_1, \\ \mathbb{E}[P_2(\bar{h})] \leq P_2, \\ 0 \leq \alpha(\bar{h}) \leq 1}} \min \Bigg\{ & \mathbb{E}_{\bar{h} \in \mathcal{A}} \Bigg[ 2\mathcal{C} \left( \frac{|h_{sd}|^2 P_1(\bar{h}) + |h_{rd}|^2 P_2(\bar{h}) + 2\sqrt{\alpha(\bar{h})} |h_{sd}|^2 P_1(\bar{h}) |h_{rd}|^2 P_2(\bar{h})}{\sigma^2} \right) \\
& - 2\mathcal{C} \left( \frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h}) + 2\sqrt{\alpha(\bar{h})} |h_{se}|^2 P_1(\bar{h}) |h_{re}|^2 P_2(\bar{h})}{\sigma_2^2} \right) \Bigg]^+, \mathbb{E}_{\bar{h} \in \mathcal{A}} \Bigg[ 2\mathcal{C} \left( \frac{\alpha(\bar{h}) |h_{sr}|^2 P_1(\bar{h})}{\sigma_1^2} \right) \\
& - 2\mathcal{C} \left( \frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h}) + 2\sqrt{\alpha(\bar{h})} |h_{se}|^2 P_1(\bar{h}) |h_{re}|^2 P_2(\bar{h})}{\sigma_2^2} \right) \Bigg]^+ \Bigg\} \\
& + \min \Bigg\{ \mathbb{E}_{\bar{h} \in \mathcal{A}^c} \Bigg[ 2\mathcal{C} \left( \frac{|h_{sd}|^2 P_1(\bar{h}) + |h_{rd}|^2 P_2(\bar{h})}{\sigma^2} \right) - 2\mathcal{C} \left( \frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h})}{\sigma_2^2} \right) \Bigg]^+, \\
& \mathbb{E}_{\bar{h} \in \mathcal{A}^c} \Bigg[ 2\mathcal{C} \left( \frac{|h_{sd}|^2 P_1(\bar{h})}{\sigma^2} \right) + 2\mathcal{C} \left( \frac{|h_{re}|^2 P_2(\bar{h})}{\sigma_2^2} \right) - 2\mathcal{C} \left( \frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h})}{\sigma_2^2} \right) \Bigg]^+ \Bigg\}. \quad (23)
\end{aligned}
$$

The upper bound for the fading relay-eavesdropper channel (22) follows directly from the upper bound established for the parallel Gaussian relay-eavesdropper channel (30). Straightforward algebra which is omitted here for brevity gives

$$
\begin{aligned}
R_e^{\text{up}} \leq \max_{\substack{\mathbb{E}[P_1(\bar{h})] \leq P_1, \\ \mathbb{E}[P_2(\bar{h})] \leq P_2, \\ -1 \leq \psi(\bar{h}) \leq 1}} \mathbb{E}_{\bar{h}} \Bigg\{ & 2\mathcal{C} \left( \frac{|h_{sd}|^2 P_1(\bar{h}) + |h_{rd}|^2 P_2(\bar{h}) + 2\psi(\bar{h}) \sqrt{|h_{sd}|^2 P_1(\bar{h}) |h_{rd}|^2 P_2(\bar{h})}}{\sigma^2} \right) \\
& - 2\mathcal{C} \left( \frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h}) + 2\psi(\bar{h}) \sqrt{|h_{se}|^2 P_1(\bar{h}) |h_{re}|^2 P_2(\bar{h})}}{\sigma_2^2} \right) \Bigg\}. \quad (24)
\end{aligned}
$$

## V. NUMERICAL RESULTS

In this section we provide numerical examples to illustrate the performance of fading relay-eavesdropper channel. We consider a fading relay-eavesdropper channel with $L$ realizations of fading state. It is assumed that perfect channel state information is available at all nodes. We can consider this channel as a Gaussian relay-eavesdropper channel with $L$ subchannels. We model channel gain between node $i \in \{s, r\}$ and $j \in \{r, d, e\}$ as distance dependent Rayleigh fading, that is, $h_{i,j} = h'_{i,j} d_{i,j}^{-\gamma/2}$, where $\gamma$ is the path loss exponent, $d_{i,j}$ is the distance between the node

$i$ and $j$, and $h'_{i,j}$ is a complex Gaussian random variable with zero mean and variance one. Each subchannel is corrupted by additive white Gaussian noise with zero mean and variance one. Furthermore, for each symbol transmission same subchannel is used on S-R and R-D links to make the optimization tractable. The objective function for both lower and upper bounds are optimized numerically using AMPL with a commercially available solver, for instance SNOPT.

To illustrate the system performance, we set the source and relay power to 64 Watt each. We consider a network geometry in which the source is located at the point (0,0), the relay is located at the point ($d$,0), the destination is located at the point (1,0) and the eavesdropper is located at the point (0,1), where $d$ is the distance between the source and the relay. In all numerical results we set path loss exponent $\gamma:=2$ and $L:=64$. For each subchannel the selection of the coding scheme at the relay is based on the relative strength of the S-D link w.r.t the S-R link, i.e, we use NF scheme (set $\mathcal{A}^c$) when $|h_{sd}|^2 \geq |h_{sr}|^2$ and DF scheme (set $\mathcal{A}$) when $|h_{sd}|^2 < |h_{sr}|^2$. Fig. 3 shows the power allocation for a fading channel with 64 subchannels where the relay is located at (0.5,0), and marker '$\times$' denotes NF on a particular subchannel while marker '$\square$' denotes DF on a particular subchannel. It can be seen from Fig. 3 that, achievable perfect secrecy rate is zero for some subchannels. Roughly speaking, this happens when the condition $|h_{rd}|^2 > |h_{re}|^2$ is violated.

Fig. 4 compares the average perfect secrecy rate of the lower bound, with optimized power allocation and with uniform power allocation, i.e., allocating same power at the source and relay for all subchannels in $\bar{h} \in \mathcal{A}$ and in $\bar{h} \in \mathcal{A}^c$. It can be seen that for separate source and relay powers, optimized power allocation scheme outperforms uniform power allocation scheme. This fact follows because optimized power allocation scheme maximizes the achievable perfect secrecy rate and hence enhances the system performance.

Mode selection at the relay by only considering the relative strength of the S-D and the S-R link in the lower bound is suboptimal because the achievable secrecy rate (23) also depends on the gain of other link. We now consider the case in which the relay selects the scheme which maximizes the rate for each subchannel. We plot the lower bound with this criteria and compare it with the case in which same scheme is used on all subchannels. As a reference we consider the case in which there is no relay i.e. a parallel wiretap channel. Fig. 5 shows the achievable average perfect secrecy rate of different schemes. It can be seen that when the relay is close to the source, DF scheme on all subchannels gives higher secrecy rate. Similarly when the relay is

close to the destination, NF scheme on all subchannels offers better rate. The region when the relay is between $0.5 < d < 1.2$ is of particular interest. In this region the relay selects between DF scheme and NF scheme for each subchannel based on the relative strength of the S-D link w.r.t the S-R link as mentioned above, and utilizes the gain from both schemes. It is interesting to note that when the relay is close to the destination, use of DF scheme on all subchannels does not offer any gain because in this case the relay is unable to decode the source information and hence the average secrecy rate decreases. The lower bound always perform better than the wiretap channel which shows the usefulness of the relay.

In Fig. 6 we compare the lower bound obtained in Fig. 5, with the upper bound on the secrecy capacity for the fading relay-eavesdropper channel. It can be seen that when the relay is close to the source, the lower and upper bound matches. This follows because of using DF scheme on all subchannels.

## VI. CONCLUSIONS

We studied the problem of secure communication over the parallel relay channel. Outer and inner bounds on the rate-equivocation are established for the DM case. We established lower and upper bound on the perfect secrecy rate for the Gaussian memoryless case. For the Gaussian model, the case in which the relay does not hear the source, the lower and upper bound coincide and secrecy capacity is established. We apply the results established for the Gaussian memoryless model to a more practical fading relay-eavesdropper channel. Numerical examples showed that power adjustment among parallel channels result in higher secrecy rate.

## APPENDIX I

We compute the upper bound on secrecy rate for the parallel Gaussian relay-eavesdropper channel as follows.

$$\max_{\{\mathbf{K}_{\mathbf{P}_l} \in \mathcal{K}_{P_l}\}_{l=1\ldots L}} \sum_{l=1}^{L} I(X_{1l}X_{2l}; Y_l) - I(X_{1l}X_{2l}; Y_{2l})$$

$$= \max_{\{\mathbf{K}_{\mathbf{P}_l} \in \mathcal{K}_{P_l}\}_{l=1\ldots L}} \sum_{l=1}^{L} [h(Y_l) - h(Y_l \mid X_{1l}X_{2l}) - h(Y_{2l}) + h(Y_{2l} \mid X_{1l}X_{2l})]$$

$$= \max_{\{\mathbf{K}_{\mathbf{P}_l} \in \mathcal{K}_{P_l}\}_{l=1\ldots L}} \sum_{l=1}^{L} [h(Y_l) - h(Z_l) - h(Y_{2l}) + h(Z_{2l})]. \tag{25}$$

The first term in (25) is computed as follows.

$$
\begin{aligned}
h(Y_l) &= h(X_{1l} + \sqrt{\rho_{1l}}X_{2l} + Z_l) \\
&= \frac{1}{2}\log(2\pi e)(P_{1l} + \rho_{1l}P_{2l} + 2\psi_l\sqrt{\rho_{1l}P_{1l}P_{2l}} + \sigma_l^2).
\end{aligned}
\tag{26}
$$

Similarly the second, third and fourth term in (25) are computed as follows.

$$
h(Z_l) = \frac{1}{2}\log 2\pi e(\sigma_l^2)
\tag{27}
$$

$$
h(Y_{2l}) = \frac{1}{2}\log(2\pi e)(P_{1l} + \rho_{2l}P_{2l} + 2\psi_l\sqrt{\rho_{2l}P_{1l}P_{2l}} + \sigma_{2l}^2)
\tag{28}
$$

$$
h(Z_{2l}) = \frac{1}{2}\log 2\pi e(\sigma_{2l}^2).
\tag{29}
$$

Using (26)-(29) in (25) gives

$$
R_e^{\mathrm{up}} \leq \max_{\substack{\sum_{l=1}^L P_{1l} \leq P_1, \\ \sum_{l=1}^L P_{2l} \leq P_2, \\ -1 \leq \psi_l \leq 1 \\ \text{for } l = 1 \ldots, L}} \sum_{l=1}^L \frac{1}{2}\log\left(1 + \frac{P_{1l} + \rho_{1l}P_{2l} + 2\psi_l\sqrt{\rho_{1l}P_{1l}P_{2l}}}{\sigma_l^2}\right) - \frac{1}{2}\log\left(1 + \frac{P_{1l} + \rho_{2l}P_{2l} + 2\psi_l\sqrt{\rho_{2l}P_{1l}P_{2l}}}{\sigma_{2l}^2}\right).
\tag{30}
$$

## REFERENCES

[1] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

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

[3] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[4] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *to appear, IEEE Transactions on Information Theory*.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *Available: http://arxiv.org/abs/0710.1920*.

[7] L. Lai and H. E. Gamal, "The relayeavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[8] Y. Liang, V. V. Veeravalli, and H. V. Poor, "Resource allocation for wireless fading relay channels: max-min solution," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3432–3453, Oct. 2007.

[9] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *44th Annual Allerton Conference Communication, Control and Computing*, Monticello, IL, USA, Sept. 2006, pp. 841–848.

[10] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, vol. 2009.

[11] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "on secure transmission over parallel relay eavesdropper channel," in *48th Annual Allerton Conference Communication, Control and Computing*, Monticello, IL, USA, Sept. 2010.

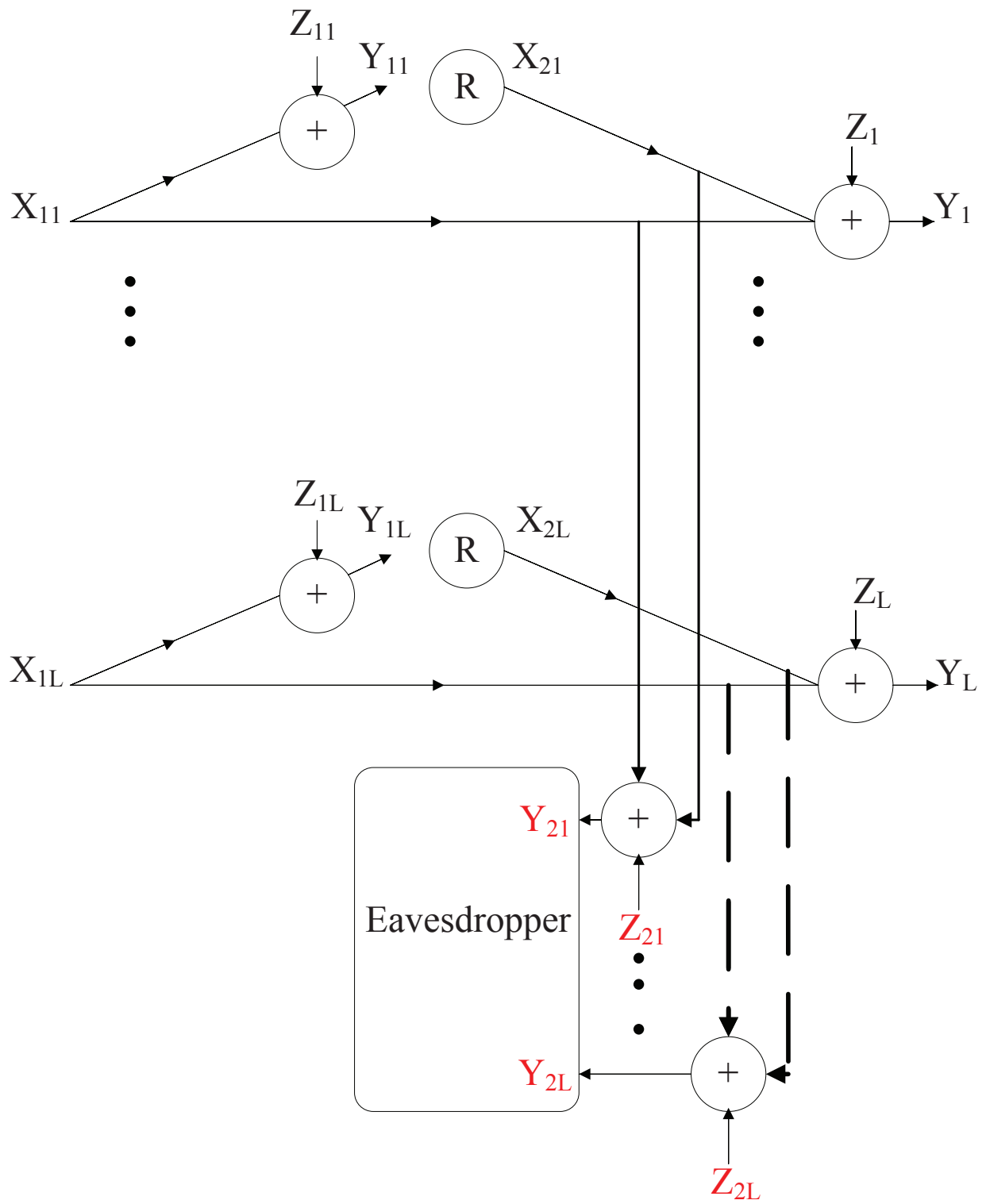[12] R. G. Gallager, *Information theory and reliable communication*. New York:Wiley, 1968.

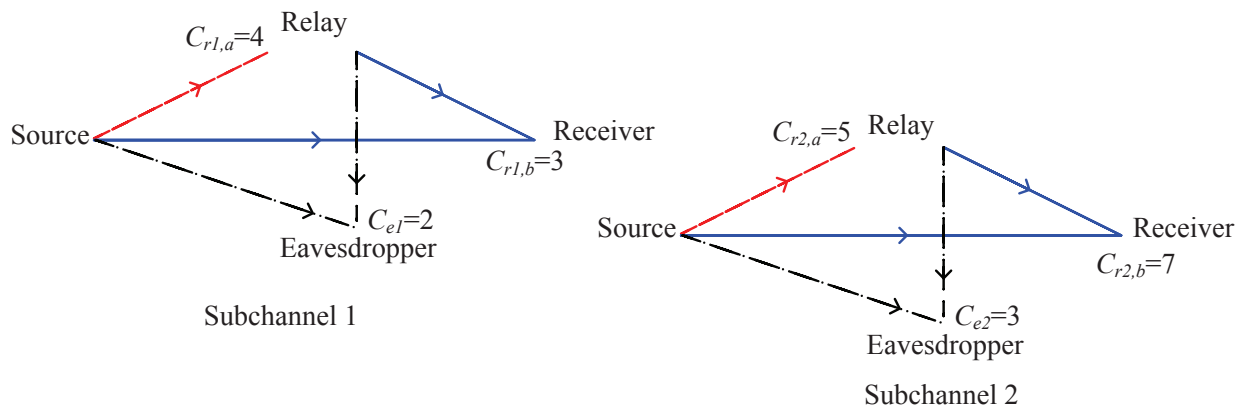Fig. 1.   The parallel Gaussian relay-eavesdropper channel.

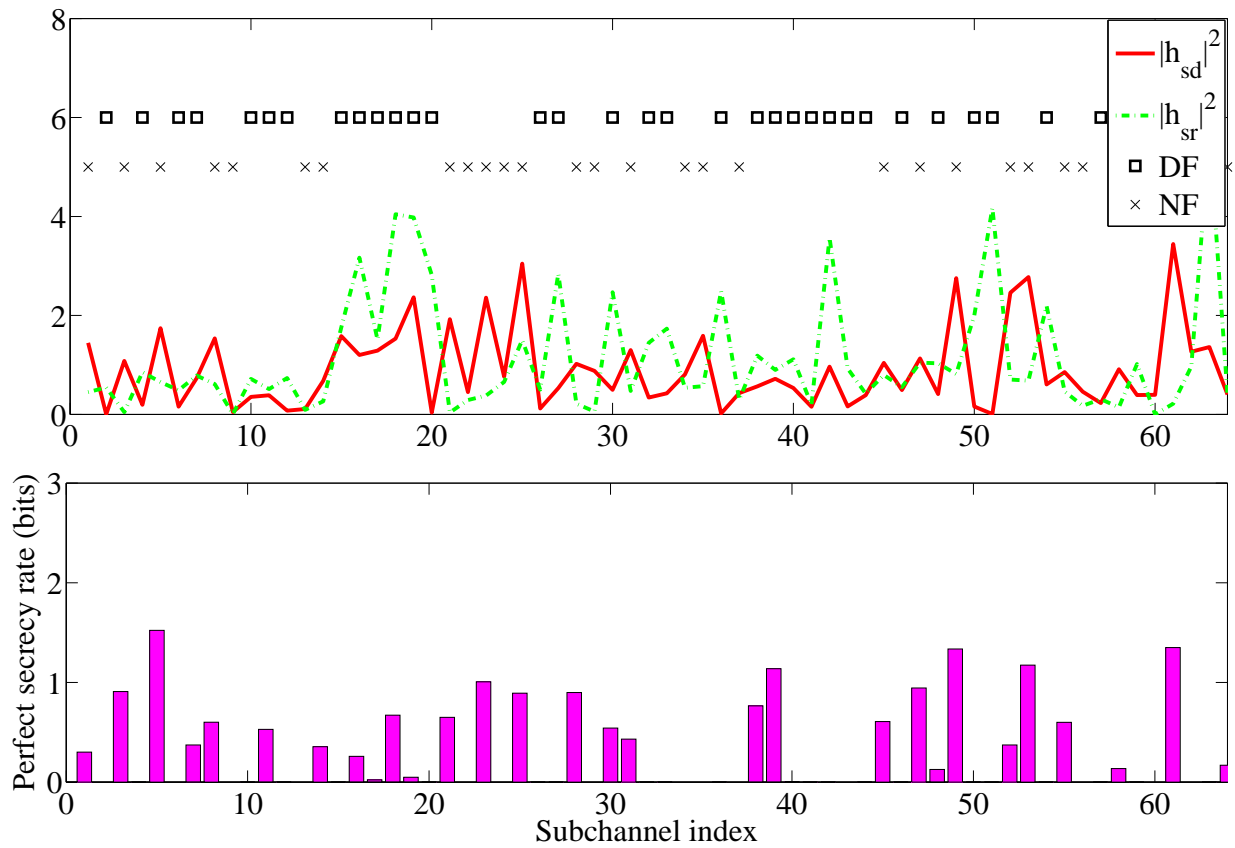Fig. 2.    An example of a deterministic parallel relay-eavesdropper channel with two subchannels.



Fig. 3.    Achievable perfect secrecy rate of a parallel relay-eavesdropper channel.
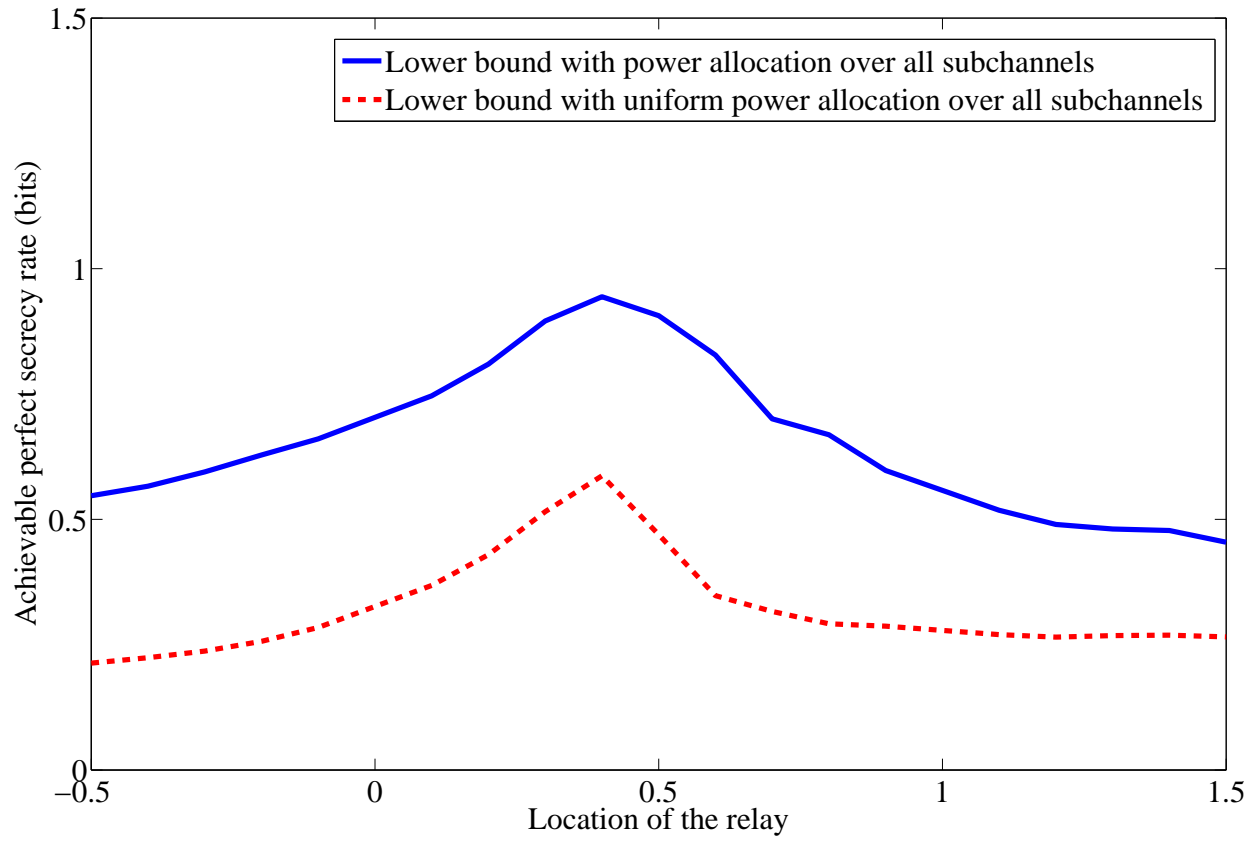
Fig. 4. Comparison of achievable perfect secrecy rate of the lower bound with optimized power allocation and with uniform power allocation over all subchannels.
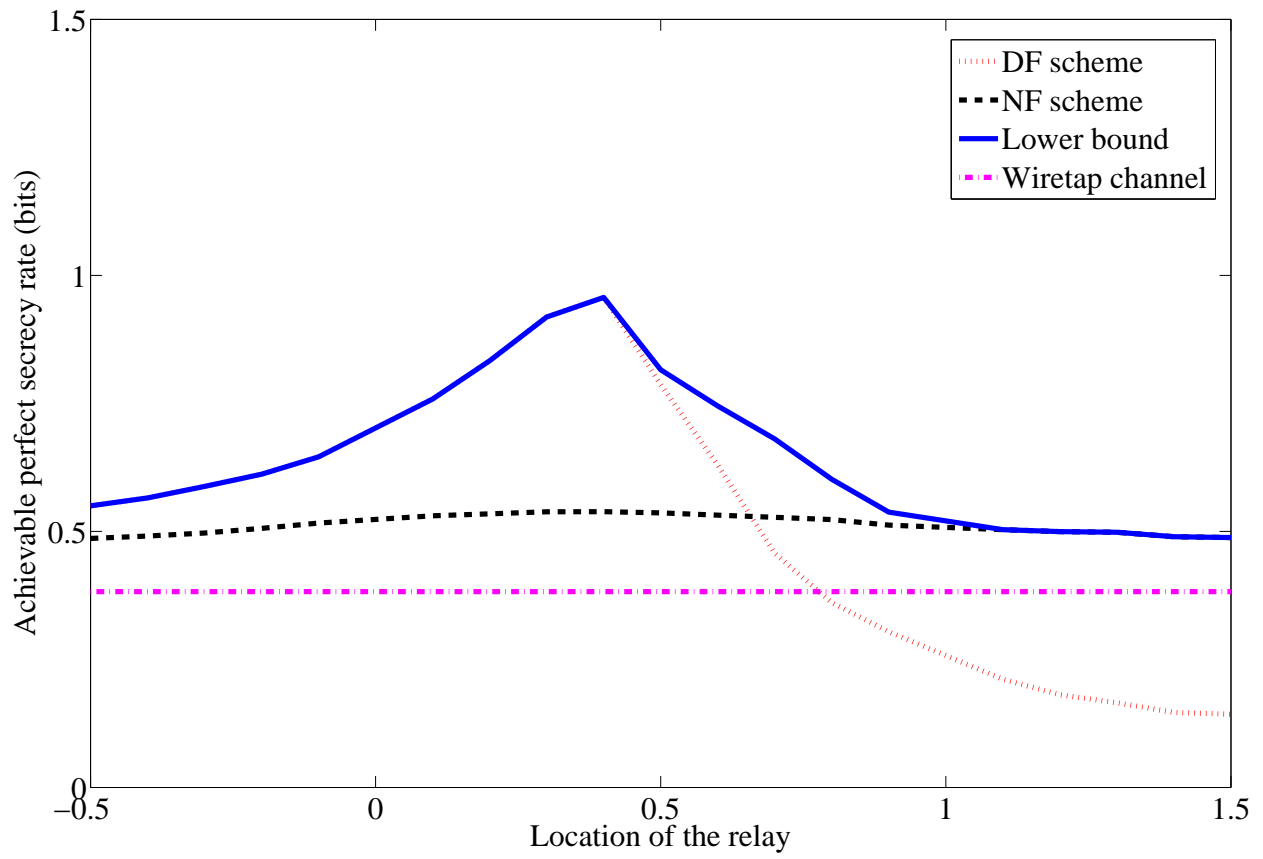
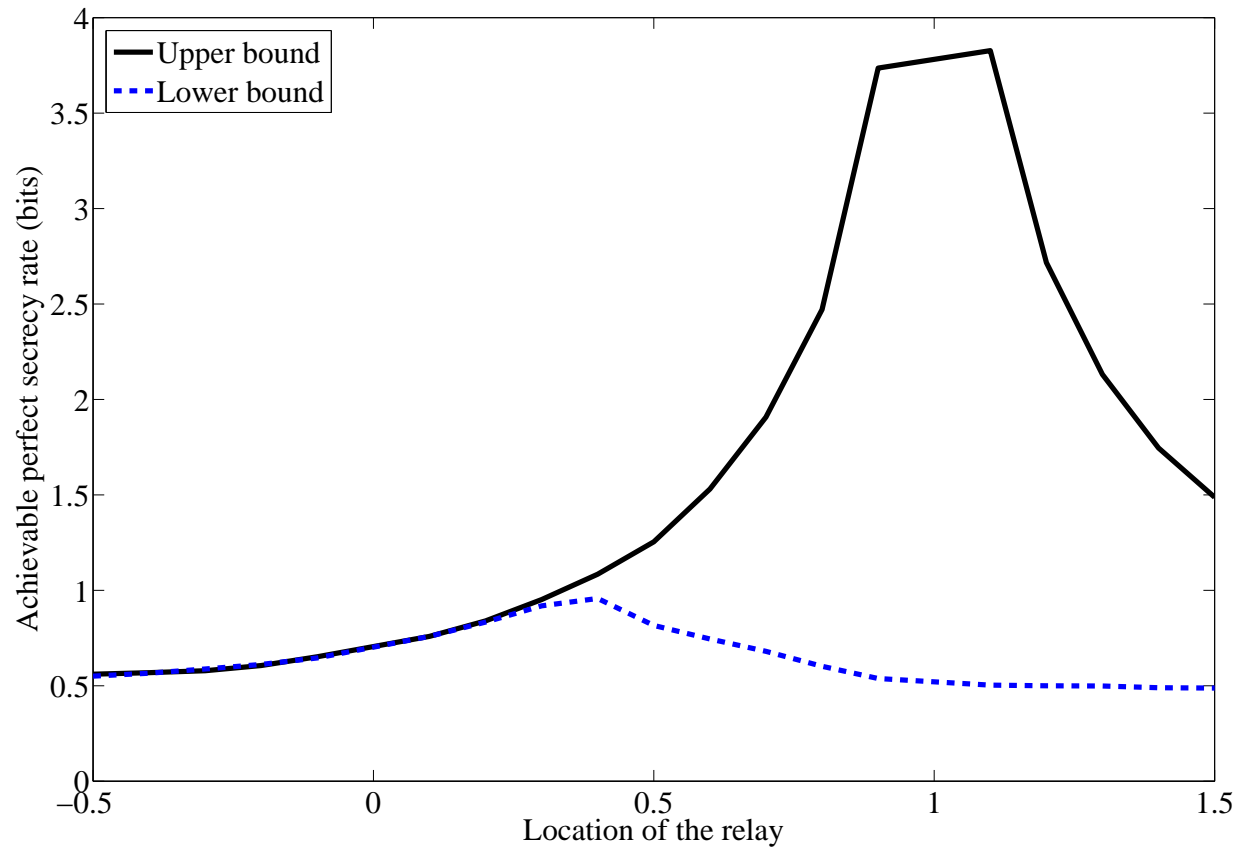Fig. 5.  Comparison of achievable perfect secrecy rate of some schemes with the lower bound.

Fig. 6.   Bounds on perfect secrecy rate.