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 parallel relay channel in the presence of a passive eavesdropper. We consider a four-terminal relay-eavesdropper channel which consists of multiple 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 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. Furthermore, we study a special case in which the relay does not hear the source and show that under certain conditions the lower and upper bounds coincide. 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*—Eavesdropping, fading channels, parallel relay channels, secrecy, wire-tap channel.**

I. Introduction

In conventional point-to-point wired networks, security is facilitated by secret key sharing between relevant parties based on some common cryptographic algorithm. The premise is that only legitimate users have access to the encrypted messages and extraneous users (adversaries) are unable to access any useful information. The wireless channel is characterized by its inherit randomness and broadcast nature. Physical layer security exploits the basic attributes of the wireless channel for instance, difference of the fading gains between the legitimate channel (source to the legitimate receiver) and the channel to the adversary, to transmit information securely to the legitimate receiver. Thus, it eradicates the need of secret key sharing.

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 source 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]–[6], multiple access channels [7]–[9], fading channels [10], [11], etc. The idea of cooperation between users in context of security was introduced by [12]. The intuition 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. A special case in which there is a physically degraded relay-eavesdropper channel was studied in [13]. The case in which the relay does not acts as a trusted node is studied in [14] and [15].

In this paper, we study a parallel relay-eavesdropper channel. A parallel relay-eavesdropper channel is a generalization of the setup in [12], 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 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 [16], 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, e.g., the parallel wiretap channel studied in [17], 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 the parallel relay-eavesdropper channel. The inner bound is obtained through a coding scheme in which, for each subchannel, the relay operates either in decode-and-forward (DF) or in noise forwarding (NF) mode. We note that establishing our outer bound for DM case is not straightforward and it does not follow directly from the single-letter outer bound for the relay-eavesdropper channel developed in [12, Theorem 1]. Therefore

Manuscript received January 31, 2011; revised July 02, 2011 and October 20, 2011; accepted January 03, 2012. Date of publication January 23, 2012; date of current version March 08, 2012. This work was supported in part by the EU network of excellence NEWCOM++, and the Concerted Research Action, SCOOP. The result in this work was presented in part at the 48th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, September 2010. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Z. Jane Wang.

Z. H. Awan and L. Vandendorpe are with the ICTEAM Institute (École Polytechnique de Louvain), Université catholique de Louvain, Louvain-la-Neuve 1348, Belgium (e-mail: zohaib.awan@uclouvain.be; luc.vandendorpe@uclouvain.be).

A. Zaidi was with the ICTEAM Institute (École Polytechnique de Louvain), Université catholique de Louvain, Louvain-la-Neuve 1348, Belgium, and is now with the Université Paris-Est Marne-la-Vallée, 77454 Marne-la-Vallée Cedex 2, France (e-mail: abdellatif.zaidi@univ-mlv.fr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2012.2185493

a converse is needed. The converse includes a re-definition 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. However, 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 for the parallel Gaussian relay-eavesdropper channel. Our converse proof uses elements from converse techniques developed in [5] and [6] in context of multi-antenna wiretap channel; and in a sense, can be viewed as an extension of these results to the parallel relay-eavesdropper channel. This upper bound is especially useful when the multiple access part of the channel is the bottleneck. We show that, in contrast to upper bounding techniques for our model that can be obtained straightforwardly by applying recent results on multi-antenna wiretap channels [4]–[6], our upper bound shows some degree of *separability* for the different subchannels.

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 under some specific conditions noise-forwarding on all links achieves the secrecy capacity. The converse proof follows from 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 context of a class of classic relay-eavesdropper channel with orthogonal components [18]. These assumptions turn the parallel Gaussian relay-eavesdropper channel into a parallel Gaussian wiretap channel, the secrecy capacity of which is established in [3] and [17].

Furthermore, we study an application of the results established for the parallel Gaussian relay-eavesdropper channel to the fading relay-eavesdropper channel. We assume that perfect non-causal channel state information (CSI) is available at all nodes. 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 for the Gaussian model, and consider a special case in which under some specific conditions 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 $(X^n_1, X^n_2, \ldots, X^n_L)$ where for $l = 1, \ldots, L$, $X^n_l := (X_{l1}, X_{l2}, \ldots, X_{ln})$, the notation $X_{[1,L],i}$ is used as a shorthand for $(X_{1,i}, X_{2,i}, \ldots, X_{L,i})$, 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, $|\mathcal{X}|$ denotes the cardinality of set $\mathcal{X}$, L denotes the number of subchannels, 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 $\mathcal{C}(x) = (1/2) \cdot \log_2(1 + x)$ and $[x]^+ = \max\{0, x\}$. Throughout the paper the logarithm function is taken to the base 2.

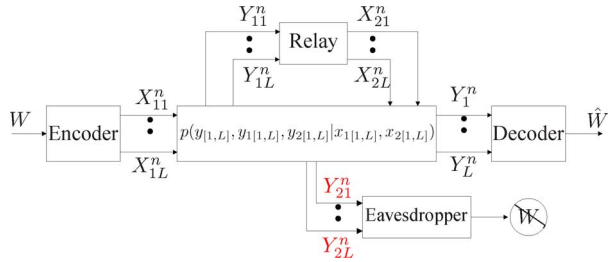


Fig. 1. Parallel relay-eavesdropper channel.

II. Discrete Memoryless Channel

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

A. Channel Model

Definition 1: The parallel relay-eavesdropper channel consists of four nodes, a source, a relay, a destination (legitimate receiver) and a passive eavesdropper. The communication takes place over L subchannels. Fig. 1 represents the studied model. The source wishes to send confidential messages to the destination, with the help of the relay to conceal them from passive eavesdropper. The source encodes the confidential message W to $(X^n_{11}, X^n_{12}, \ldots, X^n_{1L})$ codewords and broadcasts it over L subchannels to the relay and the destination. The relay helps to reduce the uncertainty about the confidential message at the destination by re-encoding whatever it has received from the source and transmits $(X^n_{21}, X^n_{22}, \ldots, X^n_{2L})$ codewords to the destination. The outputs at the relay and destination are given by $(Y^n_{11}, Y^n_{12}, \ldots, Y^n_{1L})$ and $(Y^n_1, Y^n_2, \ldots, Y^n_L)$, respectively. The passive eavesdropper overhears to the source and the relay transmission over the multiple-access link, which is denoted by $(Y^n_{21}, Y^n_{22}, \ldots, Y^n_{2L})$.

More precisely, the parallel relay-eavesdropper channel consists 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. Since the channel is memoryless, the transition probability distribution is given by

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

where $x_{1l,i} \in \mathcal{X}_{1l}, x_{2l,i} \in \mathcal{X}_{2l}, y_{l,i} \in \mathcal{Y}_l, y_{1l,i} \in \mathcal{Y}_{1l}$ and $y_{2l,i} \in \mathcal{Y}_{2l}$, for $l = 1, \ldots, L$ and $i = 1, \ldots, n$. The symbols x_{1l} and x_{2l} are the source and relay inputs on subchannel l, and y_{1l}, y_l, y_{2l} are the channel outputs at the relay, destination and eavesdropper for the lth subchannel, respectively.

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

- a stochastic encoder at the source that maps $W \to X^n_{1[1,L]}$;
- a relay encoder that maps $f_i(Y^{i-1}_{1[1,L]}) \to X_{2[1,L],i}$ for $1 \leq i \leq n$;
- a decoding function $g(\cdot)$, that maps the received codewords from the source and relay node to get an estimate of the confidential message, $g(Y^n_{[1,L]}) \to \hat{W}$.

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

$$P^n_e = \frac{1}{2^{nR}} \sum_{W \in \mathcal{W}} p\left\{ g\left(Y^n_{[1,L]}\right) \neq W | W \right\}. \tag{2}$$

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. The equivocation rate per channel use is defined as $R_e = H(W|Y^n_{2[1,L]})/n$. Perfect secrecy for the channel is obtained when the eavesdropper gets no information about the confidential message W from $Y^n_{2[1,L]}$. That is, the equivocation rate is equal to the unconditional source entropy.

Definition 4 [1]: A rate-equivocation pair (R, R_e) is achievable for the parallel relay-eavesdropper channel, if for any $\epsilon > 0$ there exists a sequence of codes $(2^{nR}, n)$ such that for any $n \geq n(\epsilon)$

$$\begin{aligned} \frac{H(W)}{n} &\geq R - \epsilon, \\ \frac{H\left(W \left| Y^n_{2[1,L]} \right.\right)}{n} &\geq R_e - \epsilon, \\ P^n_e &\leq \epsilon. \end{aligned} \tag{3}$$

B. Outer Bound

The following theorem provides an outer bound on the rate-equivocation region for the parallel relay-eavesdropper channel.

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

$$\begin{aligned} R &\leq \min\left\{ \sum_{l=1}^{L} I(V_{1l}, V_{2l}; Y_l), \sum_{l=1}^{L} I(V_{1l}; Y_l, Y_{1l} \mid V_{2l}) \right\} \\ R_e &\leq R \\ R_e &\leq \min\left\{ \sum_{l=1}^{L} I(V_{1l}, V_{2l}; Y_l \mid U_l) - I(V_{1l}, V_{2l}; Y_{2l} \mid U_l), \right. \\ &\qquad \left. \sum_{l=1}^{L} I(V_{1l}; Y_l, Y_{1l} \mid V_{2l}, U_l) - I(V_{1l}, V_{2l}; Y_{2l} \mid U_l) \right\}. \end{aligned} \tag{4}$$

Proof: The proof of Theorem 1 is given in Appendix A.□

Remark 1: The outer bound in Theorem 1 does not follow directly from the single-letter outer bound on the rate-equivocation region established for the relay-eavesdropper channel [12, Theorem 1]. Therefore a converse is required, in which we need to re-define the involved auxiliary random variables. The technique used to re-define the auxiliary random variables has some connection with the one used before in the context of secure transmission over broadcast channels [3].

Remark 2: The region (4) reduces to the rate-equivocation region developed for the relay-eavesdropper channel [12, Theorem 1] by setting $L := 1$ in (4).

Remark 3: The equivocation rate in Theorem 1 reduces to the secrecy capacity of the parallel wiretap channel established in [3, Corollary 1], by removing the relay, i.e., by setting $Y_{1l} = X_{2l} = V_{2l} = \phi$. The resulting term $\sum_{l=1}^{L} I(V_{1l}; Y_l \mid U_l) - I(V_{1l}; Y_{2l} \mid U_l)$ is maximized by $U_l := \text{constant}$, for $l = 1, \ldots, L$.

C. Achievable Rate-Equivocation Region

In this subsection we establish an achievable rate-equivocation region for the parallel relay-eavesdropper channel. The achievable region is established by the combination of two different coding schemes, namely decode-and-forward and noise forwarding. In DF scheme, for each message source associates a number of confusion codewords, the relay after receiving the source codewords, decodes it and re-transmits it towards the legitimate receiver and eavesdropper (see [12, Theorem 2] for details). In the NF scheme the relay does not decode the source codewords, but transmits confusion codewords independent from the source codewords, towards the legitimate receiver and the eavesdropper (see [12, Theorem 3] for details).

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

$$\begin{aligned} R &\leq \min\left\{ \sum_{l \in \mathcal{A}} I(V_{1l}, V_{2l}; Y_l | U_l), \quad \sum_{l \in \mathcal{A}} I(V_{1l}; Y_{1l} | V_{2l}, U_l) \right\} \\ &\quad + \sum_{l \in \mathcal{A}^c} I(V_{1l}; Y_l | V_{2l}) \\ R_e &\leq R \\ R_e &\leq \min\left\{ \sum_{l \in \mathcal{A}} I(V_{1l}, V_{2l}; Y_l | U_l) - I(V_{1l}, V_{2l}; Y_{2l} | U_l), \right. \\ &\qquad \left. \sum_{l \in \mathcal{A}} I(V_{1l}; Y_{1l} | V_{2l}, U_l) - I(V_{1l}, V_{2l}; Y_{2l} | U_l) \right\} \\ &\quad + \sum_{l \in \mathcal{A}^c} I(V_{1l}; Y_l | V_{2l}) + \min\left\{ \sum_{l \in \mathcal{A}^c} I(V_{2l}; Y_l), \right. \\ &\qquad \left. \sum_{l \in \mathcal{A}^c} I(V_{2l}; Y_{2l} | V_{1l}) \right\} - \min\left\{ \sum_{l \in \mathcal{A}^c} I(V_{2l}; Y_l), \right. \\ &\qquad \left. \sum_{l \in \mathcal{A}^c} I(V_{2l}; Y_{2l}) \right\} - \sum_{l \in \mathcal{A}^c} I(V_{1l}; Y_{2l} | V_{2l}) \end{aligned} \tag{5}$$

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.

Outline of Proof: The region in Theorem 2 is obtained through a coding scheme which combines appropriately DF and NF schemes. 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 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 [12, Theorem 2]. Similarly the rates for the 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 [12, Theorem 3]. □

Remark 4: For a parallel relay-eavesdropper channel in which all subchannels are degraded,[1] i.e.,

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

$l = 1, \ldots, L$, the perfect secrecy capacity is given by

$$C_s = \max \min \left\{ \sum_{l=1}^{L} [I(V_{1l}, V_{2l}; Y_l \mid U_l) - I(V_{1l}, V_{2l}; Y_{2l} \mid U_l)]^+, \sum_{l=1}^{L} [I(V_{1l}; Y_{1l} \mid V_{2l}, U_l) - I(V_{1l}, V_{2l}; Y_{2l} \mid U_l)]^+ \right\} \quad (6)$$

where the maximization is over $U_l \rightarrow (V_{1l}, V_{2l}) \rightarrow (X_{1l}, X_{2l}) \rightarrow (Y_l, Y_{1l}, Y_{2l})$, for $l = 1, \ldots, L$.

Proof: The achievability follows from Theorem 2 by setting $\mathcal{A}^c := \varnothing$. The converse follows along the lines of Theorem 1 and is omitted for brevity. □

III. Gaussian Channel

In this section we study a parallel Gaussian relay-eavesdropper channel. Fig. 2 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

$$\begin{aligned} Y_{1l,i} &= X_{1l,i} + Z_{1l,i} \\ Y_{l,i} &= X_{1l,i} + \sqrt{\rho_{1l}} X_{2l,i} + Z_{l,i} \\ Y_{2l,i} &= X_{1l,i} + \sqrt{\rho_{2l}} X_{2l,i} + Z_{2l,i} \end{aligned} \quad (7)$$

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 σ_{1l}^2, σ_l^2 and σ_{2l}^2, respectively, for $l = 1, \ldots, L$.

[1]In parallel relay-eavesdropper channel if all subchannels are degraded, the entire relay-eavesdropper channel may not necessarily be degraded.

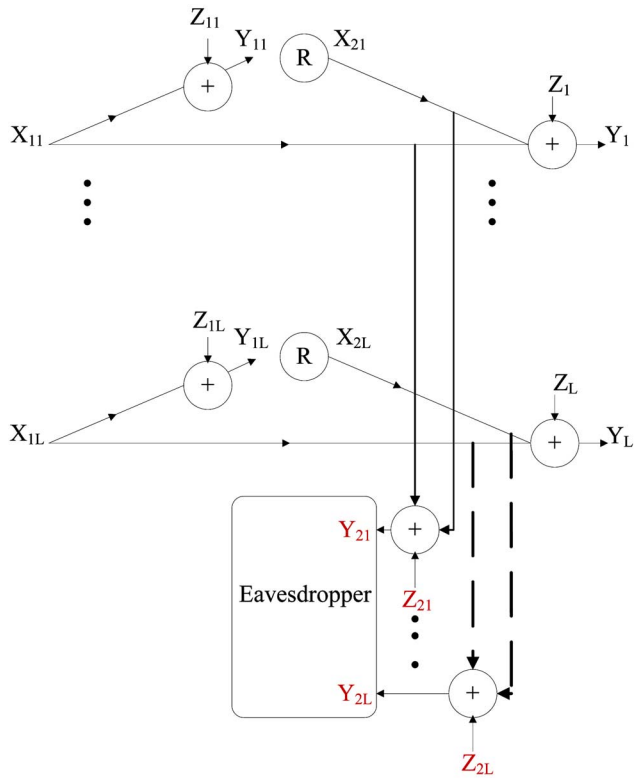


Fig. 2. Parallel Gaussian relay-eavesdropper channel.

We assume that the source and the relay know the noise variances present at the receivers. For the subchannel l, $X_{1l,i}$ and $X_{2l,i}$ are inputs from the source and relay nodes, respectively. The parameter ρ_{1l} indicates the ratio of the R-D link signal-to-noise ratio (SNR) to the S-D link SNR and ρ_{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.,

$$\frac{1}{n} \sum_{l=1}^{L} \sum_{i=1}^{n} \mathbb{E}\left[X_{1l,i}^2\right] \leq P_1 \quad (8)$$

$$\frac{1}{n} \sum_{l=1}^{L} \sum_{i=1}^{n} \mathbb{E}\left[X_{2l,i}^2\right] \leq P_2. \quad (9)$$

B. Lower Bound on the Perfect Secrecy Rate

For the parallel Gaussian relay-eavesdropper channel (7), we apply Theorem 2 to obtain a lower bound on the perfect secrecy rate.[2]

Corollary 1: For the parallel Gaussian relay-eavesdropper channel (7), a lower bound on the perfect secrecy rate is given by (10) at the bottom of the next page.

Proof: The achievability follows by applying Theorem 2 with the choice $U_l :=$ constant, $V_{1l} := X_{1l}, V_{2l} := X_{2l}, X_{1l} := \tilde{X}_{1l} + \sqrt{(\bar{\alpha}_l P_{1l}/P_{2l})} X_{2l}$, $\bar{\alpha}_l := 1 - \alpha_l$, $\tilde{X}_{1l} \sim \mathcal{N}(0, \alpha_l P_{1l})$ 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

[2]The results established for the DM case can be readily extended to memoryless channels with discrete time and continuous alphabets using standard techniques [19, Chap. 7].

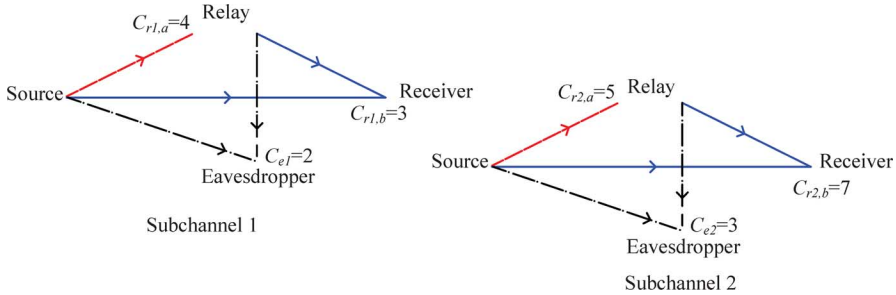


Fig. 3. Example of a deterministic parallel relay-eavesdropper channel with two subchannels.

$l \in \mathcal{A}^c$. Straightforward algebra which is omitted for brevity gives (10). □

The parameters P_{1l} and P_{2l} indicate the source and the relay power allocated for transmission over the lth subchannel. In (10), after some straightforward algebra, the contribution to the equivocation of information sent through NF (set $\mathcal{A}^c$ in Theorem 2) 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^{low} is given by (11) at the bottom of the page. In (11), for each subchannel $[\cdot]^+$ appears because achievable secrecy rate is always non-negative.

Remark 5: 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 Fig. 3. 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

$$\begin{aligned} R_e &= \min\left\{\sum_{i=1}^{2}(C_{ri,a}-C_{ei})^+, \sum_{i=1}^{2}(C_{ri,b}-C_{ei})^+\right\} \\ &= \min\{4,5\} = 4. \end{aligned} \tag{12}$$

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

$$\begin{aligned} R_e &= \sum_{i=1}^{2}\min\{(C_{ri,a}-C_{ei})^+, (C_{ri,b}-C_{ei})^+\} \\ &= \min\{2,1\} + \min\{2,4\} = 3 \end{aligned} \tag{13}$$

which is clearly smaller than (12). This shows the usefulness of coding across subchannels.

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

$$\begin{aligned} R_e^{\text{low}} = \max_{\substack{\sum_{l=1}^{L} P_{1l}\le P_1, \sum_{l=1}^{L} P_{2l}\le P_2, \\ 0\le\alpha_l\le 1, \text{ for } l=1,\ldots,|\mathcal{A}|}} & \min\left\{\sum_{l\in\mathcal{A}} \left[\mathcal{C}\left(\frac{P_{1l}+\rho_{1l}P_{2l}+2\sqrt{\bar{\alpha}_l\rho_{1l}P_{1l}P_{2l}}}{\sigma_l^2}\right) - \mathcal{C}\left(\frac{P_{1l}+\rho_{2l}P_{2l}+2\sqrt{\bar{\alpha}_l\rho_{2l}P_{1l}P_{2l}}}{\sigma_{2l}^2}\right)\right]^+,\right. \\ & \left.\sum_{l\in\mathcal{A}} \left[\mathcal{C}\left(\frac{\alpha_l P_{1l}}{\sigma_{1l}^2}\right) - \mathcal{C}\left(\frac{P_{1l}+\rho_{2l}P_{2l}+2\sqrt{\bar{\alpha}_l\rho_{2l}P_{1l}P_{2l}}}{\sigma_{2l}^2}\right)\right]^+\right\} \\ & + \min\left\{\sum_{l\in\mathcal{A}^c} \left[\mathcal{C}\left(\frac{P_{1l}+\rho_{1l}P_{2l}}{\sigma_l^2}\right) - \mathcal{C}\left(\frac{P_{1l}+\rho_{2l}P_{2l}}{\sigma_{2l}^2}\right)\right]^+, \sum_{l\in\mathcal{A}^c} \left[\mathcal{C}\left(\frac{P_{1l}}{\sigma_l^2}\right) + \mathcal{C}\left(\frac{\rho_{2l}P_{2l}}{\sigma_{2l}^2}\right) - \mathcal{C}\left(\frac{P_{1l}+\rho_{2l}P_{2l}}{\sigma_{2l}^2}\right)\right]^+\right\} \end{aligned} \tag{11}$$

C. Upper Bound on the Perfect Secrecy Rate

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

Theorem 3: For the parallel Gaussian relay-eavesdropper channel (7), an upper bound on the secrecy rate is given by

$$R_e^{\text{up}} = \max_{\{\mathbf{K}_{\mathbf{P}_l} \in \mathcal{K}_{P_l}\}_{l=1,\ldots,L}} \sum_{l=1}^{L} I(X_{1l}, X_{2l}; Y_l) - I(X_{1l}, X_{2l}; Y_{2l}) \quad (14)$$

where the maximization is over $[X_{1l}, X_{2l}] \sim \mathcal{N}(\mathbf{0}, \mathbf{K}_{\mathbf{P}_l})$ with $\mathcal{K}_{P_l} = \{\mathbf{K}_{\mathbf{P}_l} : \mathbf{K}_{\mathbf{P}_l} = \left[\begin{smallmatrix} P_{1l} & \psi_l\sqrt{P_{1l}P_{2l}} \\ \psi_l\sqrt{P_{1l}P_{2l}} & P_{2l} \end{smallmatrix}\right], -1 \leq \psi_l \leq 1\}, l = 1, \ldots, L$, 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 (8) and (9), 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

$$R_e \leq \max \sum_{l=1}^{L} I(V_{1l}, V_{2l}; Y_l \mid U_l) - I(V_{1l}, V_{2l}; Y_{2l} \mid U_l) \quad (15)$$

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 (15), we obtain

$$\begin{aligned}
R_e &\leq \sum_{l=1}^{L} I(V_{1l}, V_{2l}; Y_l \mid U_l) - I(V_{1l}, V_{2l}; Y_{2l} \mid U_l) \\
&\overset{(a)}{\leq} \sum_{l=1}^{L} I(V_{1l}, V_{2l}; Y_l) - I(V_{1l}, V_{2l}; Y_{2l}) \\
&\leq \sum_{l=1}^{L} I(V_{1l}, V_{2l}; Y_l, Y_{2l}) - I(V_{1l}, V_{2l}; Y_{2l}) \\
&\overset{(b)}{=} \sum_{l=1}^{L} [I(X_{1l}, X_{2l}; Y_l, Y_{2l}) - I(X_{1l}, X_{2l}; Y_l, Y_{2l} \mid V_{1l}, V_{2l})] \\
&\quad - [I(X_{1l}, X_{2l}; Y_{2l}) - I(X_{1l}, X_{2l}; Y_{2l} \mid V_{1l}, V_{2l})] \\
&= \sum_{l=1}^{L} [I(X_{1l}, X_{2l}; Y_l, Y_{2l}) - I(X_{1l}, X_{2l}; Y_{2l})] \\
&\quad - [I(X_{1l}, X_{2l}; Y_l, Y_{2l} \mid V_{1l}, V_{2l}) \\
&\quad - I(X_{1l}, X_{2l}; Y_{2l} \mid V_{1l}, V_{2l})] \\
&\leq \sum_{l=1}^{L} [I(X_{1l}, X_{2l}; Y_l, Y_{2l}) - I(X_{1l}, X_{2l}; Y_{2l})] \\
&= \sum_{l=1}^{L} I(X_{1l}, X_{2l}; Y_l \mid Y_{2l}) \qquad (16)
\end{aligned}$$

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 $U_l :=$ constant and (b) follows from the Markov chain condition $(V_{1l}, V_{2l}) \to (X_{1l}, X_{2l}) \to (Y_l, Y_{1l}, Y_{2l}), l = 1, \ldots, L$.

We now tighten the upper bound (16) by using an argument previously used in [5] and [6] in the context of multi-antenna wiretap channel. More specifically, observing that, the original bound (15) 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 (16) can be further tightened as

$$R_e \leq \min_{\{p(y_l', y_{2l}'|x_{1l}, x_{2l})\}} \max_{\{p(x_{1l}, x_{2l})\}} \sum_{l=1}^{L} I(X_{1l}, X_{2l}; Y_l' \mid Y_{2l}') \quad (17)$$

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 (17) 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 $\mathcal{K}_{P_l} = \{\mathbf{K}_{\mathbf{P}_l} : \mathbf{K}_{\mathbf{P}_l} = \left[\begin{smallmatrix} P_{1l} & \psi_l\sqrt{P_{1l}P_{2l}} \\ \psi_l\sqrt{P_{1l}P_{2l}} & P_{2l} \end{smallmatrix}\right], -1 \leq \psi_l \leq 1\}, l = 1, \ldots, L$ 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 (8) and (9), respectively [5], [6].

Next, using the specified Gaussian inputs, and proceeding as in [6] and [20], the evaluation of the upper bound (17) minimized over all possible correlations between Y_l', Y_{2l}', for $l = 1, \ldots, L$ yields

$$R_e \leq \max_{\{\mathbf{K}_{\mathbf{P}_l} \in \mathcal{K}_{P_l}\}_{l=1,\ldots,L}} \sum_{l=1}^{L} I(X_{1l}, X_{2l}; Y_l) - I(X_{1l}, X_{2l}; Y_{2l}). \quad (18)$$

This concludes the proof. □

The computation of the upper bound (14) is given in Appendix B.

Remark 6: Viewing our Gaussian model (7) as a specific MIMO relay-eavesdropper channel (i.e., one without interference), one can establish a genie-aided upper bound on the secrecy capacity of the model (7) by using recent results on MIMO wiretap channels [4]–[6], by upper bounding the secrecy rate that can be conveyed by the source and relay to the legitimate receiver on the multi-access part of the channel with that of an interference-free MIMO wiretap channel with $2L$-transmit antenna at the sender, L-receive antenna at the legitimate receiver and L-receive antenna at the eavesdropper. However, in contrast to (14), the upper bound obtained this way does not show any degree of separability. More specifically, using [4]–[6], one can argue that the following is an upper-bound on the secrecy capacity of the model (7):

$$R_e \leq I(X_{1[1,L]}, X_{2[1,L]}; Y_{[1,L]}) - I(X_{1[1,L]}, X_{2[1,L]}; Y_{2[1,L]}) \quad (19)$$

for some $[X_{1[1,L]}X_{2[1,L]}] \sim \mathcal{N}(\mathbf{0}, \mathbf{K}_{\mathbf{P}})$, and $\mathbf{K}_{\mathbf{P}} = \mathbb{E}[(X_{1[1,L]}X_{2[1,L]})(X_{1[1,L]}X_{2[1,L]})^T]$ has diagonal entries that satisfies (8) and (9), respectively.

Because the equivalent MIMO channel is interference-free, the upper bound (19) can be written equivalently as

$$R_e \leq \sum_{l=1}^{L} I(X_{1l}, X_{2l}; Y_l|Y^{l-1}) - I\left(X_{1l}, X_{2l}; Y_{2l}|Y_2^{l-1}\right). \quad (20)$$

Now, observe that (20) does not show any degree of separability as in (14), basically because of the additional conditioning on Y_2^{l-1}, for $l = 1, \ldots, L$.

Also, investigating our proof in the Gaussian case, one can see that the RHS of (15) and its proof are fundamental. As

mentioned in the proof, we could obtain the final form (18) essentially because the upper bound (15) that we established depends on the conditional joint distribution $p(y_l, y_{2l}|x_{1l}, x_{2l})$ only through its marginals.

Example Application: We consider a parallel relay channel with interference at the eavesdropper. The received signals at the relay, destination and eavesdropper are given by

$$\begin{aligned} Y_{1l,i} &= X_{1l,i} + Z_{1l,i} \\ Y_{l,i} &= X_{1l,i} + \sqrt{\rho_{1l}} X_{2l,i} + Z_{l,i} \\ Y_{2l,i} &= X_{1l,i} + \sqrt{\rho_{2l}} X_{2l,i} \\ &\quad + \underbrace{\sum_{k=1,k\neq l}^{L} X_{1k,i} + \sqrt{\rho_{2k}} X_{2k,i}}_{\text{interference}} + Z_{2l,i}. \end{aligned} \tag{21}$$

This model can represent the equivalent channel model of a MIMO relay-eavesdropper channel with the interference at the relay and legitimate receiver avoided through singular-value decomposition; as the source can always get some feedback from both the relay and legitimate receiver, and the relay from the legitimate receiver, which then transforms the MIMO transmission into one on parallel channels among the source, relay and legitimate receiver. The eavesdropper however does not feedback information on his channel, and so is subjected to cross-antenna interference. Constraining the eavesdropper to treat the cross-antenna interference as independent noise, one can obtain an upper bound on the secrecy capacity of the model with constrained eavesdropper by direct application of (14). Straightforward algebra gives (22) at the bottom of the page.

Then, it is clear that the upper bound (22) holds also for the model (21) with a non-constrained eavesdropper.

D. Secrecy Capacity in Some Special Cases

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 (7), if the relay does not hear the source:

1) An upper bound on the perfect secrecy rate is given by

$$R_e^{\text{up}} = \max \sum_{l=1}^{L} \mathcal{C}\left(\frac{P_{1l}}{\sigma_l^2}\right) - \mathcal{C}\left(\frac{P_{1l}}{\sigma_{2l}^2 + \rho_{2l} P_{2l}}\right) \tag{23}$$

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

2) A lower bound on the perfect secrecy rate is given by

$$R_e^{\text{low}} = \max \sum_{l=1}^{L} \mathcal{C}\left(\frac{P_{1l}}{\sigma_l^2}\right) - \mathcal{C}\left(\frac{P_{1l}}{\sigma_{2l}^2 + \rho_{2l} P_{2l}}\right) \tag{24}$$

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

$$\sum_{l=1}^{L} \mathcal{C}\left(\frac{\rho_{1l} P_{2l}}{P_{1l} + \sigma_l^2}\right) \geq \sum_{l=1}^{L} \mathcal{C}\left(\frac{\rho_{2l} P_{2l}}{\sigma_{2l}^2}\right). \tag{25}$$

Proof: Upper Bound. The bound in (23) is established as follows. Our approach borrows elements from an upper bounding technique that is used in [18], 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 [18], any upper bound for this model with full relay-destination cooperation and constrained eavesdropper also applies to the model of Theorem 4.

Now, for the model with full relay-destination cooperation and constrained eavesdropper, we develop an upper bound on the secrecy rate 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

$$Y'_{l,i} = X_{1l,i} + Z_{l,i}. \tag{26}$$

The eavesdropper is constrained in the sense that it is *restricted* not to decode the relay's signals. Mathematically, this can be stated as follows. Let Z'_{2l} be a random variable that has the same distribution as X_{2l} and $P_{Z'_{2l}}(z) = P_{X_{2l}}(z)$, and represents unknown noise at the eavesdropper. The channel output at the constrained eavesdropper is given by

$$Y'_{2l,i} = X_{1l,i} + \underbrace{\sqrt{\rho_{2l}} Z'_{2l,i}}_{\text{unknown noise}} + Z_{2l,i}. \tag{27}$$

For the constrained eavesdropper the relay's transmission acts as unknown noise, with the worst case obtained with Z'_{2l} being Gaussian, for $l = 1, \ldots, L$. 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

$$R_e \leq \max_{\substack{\sum_{l=1}^{L} P_{1l} \leq P_1, \\ \sum_{l=1}^{L} P_{2l} \leq P_2, \\ -1 \leq \psi_l \leq 1 \\ \text{for } l=1,\ldots,L}} \sum_{l=1}^{L} \mathcal{C}\left(\frac{P_{1l} + \rho_{1l} P_{2l} + 2\psi_l \sqrt{\rho_{1l} P_{1l} P_{2l}}}{\sigma_l^2}\right) - \mathcal{C}\left(\frac{P_{1l} + \rho_{2l} P_{2l} + 2\psi_l \sqrt{\rho_{2l} P_{1l} P_{2l}}}{\sum_{k=1,k\neq l}^{L} P_{1k} + \sqrt{\rho_{2k}} P_{2k} + 2\psi_k \sqrt{\rho_{2k} P_{1k} P_{2k}} + \sigma_{2l}^2}\right) \tag{22}$$

cooperation) is, in fact, a parallel Gaussian wiretap channel, the secrecy capacity of which is established in [3], i.e.,

$$C_s = \max \sum_{l=1}^{L} I(X_{1l}; Y_l') - I(X_{1l}; Y_{2l}') \tag{28}$$

where the maximization is over $X_{1l} \sim \mathcal{N}(0, P_{1l})$ and $X_{2l} \sim \mathcal{N}(0, P_{2l}), l = 1, \ldots, L$, 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 (28) gives (23).

Lower Bound: The proof of the lower bound follows by evaluating the equivocation in Theorem 2 with a specific choice of the variables. More specifically, evaluating (5) with the choice $|\mathcal{A}^c| := L$, $V_{1l} := X_{1l}$, $V_{2l} := X_{2l}$, with $X_{1l} \sim \mathcal{N}(0, P_{1l})$ independent of $X_{2l} \sim \mathcal{N}(0, P_{2l}), l = 1, \ldots, L$ and such that (25) is satisfied, we get the rate expression in the RHS of (24). The RHS of (24) then follows by maximization over all $\{P_{1l}, P_{2l}\}$, $l = 1, \ldots, L$, satisfying (25) and the total power constraints $\sum_{l=1}^{L} P_{1l} \leq P_1$ and $\sum_{l=1}^{L} P_{2l} \leq P_2$. □

Remark 7: The upper (23) and lower (24) bounds on the perfect secrecy rate of Theorem 4 have same expressions but are maximized over different input sets. These bounds coincide *only* when the inputs ($\{P_{1l}, P_{2l}\}$) that maximize the upper bound (23) also satisfy (25). For this specific case, perfect secrecy is established and is given by

$$C_s = \max \sum_{l=1}^{L} \mathcal{C}\left(\frac{P_{1l}}{\sigma_l^2}\right) - \mathcal{C}\left(\frac{P_{1l}}{\sigma_{2l}^2 + \rho_{2l} P_{2l}}\right) \tag{29}$$

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

$$\sum_{l=1}^{L} \mathcal{C}\left(\frac{\rho_{1l} P_{2l}}{P_{1l} + \sigma_l^2}\right) \geq \sum_{l=1}^{L} \mathcal{C}\left(\frac{\rho_{2l} P_{2l}}{\sigma_{2l}^2}\right). \tag{30}$$

IV. Example 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

$$\begin{aligned} Y_{1,i} &= h_{sr,i} X_{1,i} + Z_{1,i} \\ Y_i &= h_{sd,i} X_{1,i} + h_{rd,i} X_{2,i} + Z_i \\ Y_{2,i} &= h_{se,i} X_{1,i} + h_{re,i} X_{2,i} + Z_{2,i} \end{aligned} \tag{31}$$

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 σ_1^2, σ^2, and σ_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 non-causal CSI is available at all nodes. 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 (31), which follows from (11) is given by (32). The upper bound for the fading relay-eavesdropper channel (31) follows directly from the upper bound established for the parallel Gaussian relay-eavesdropper channel (14). Straightforward algebra which is omitted for brevity gives (33). See (32) and (33) at the bottom of the page.

$$\begin{aligned} R_e^{\text{low}} = \max_{\substack{\mathbb{E}[P_1(\bar{h})] \leq P_1, \\ \mathbb{E}[P_2(\bar{h})] \leq P_2, \\ 0 \leq \alpha(\bar{h}) \leq 1}} & \min \left\{ \mathbb{E}_{\bar{h} \in \mathcal{A}} \left[2\mathcal{C}\left(\frac{|h_{sd}|^2 P_1(\bar{h}) + |h_{rd}|^2 P_2(\bar{h}) + 2\sqrt{\bar{\alpha}(\bar{h}) |h_{sd}|^2 P_1(\bar{h}) |h_{rd}|^2 P_2(\bar{h})}}{\sigma^2} \right) \right. \right. \\ & \left. - 2\mathcal{C}\left(\frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h}) + 2\sqrt{\bar{\alpha}(\bar{h}) |h_{se}|^2 P_1(\bar{h}) |h_{re}|^2 P_2(\bar{h})}}{\sigma_2^2} \right) \right]^+, \quad \mathbb{E}_{\bar{h} \in \mathcal{A}} \left[2\mathcal{C}\left(\frac{\alpha(\bar{h}) |h_{sr}|^2 P_1(\bar{h})}{\sigma_1^2} \right) \right. \\ & \left. \left. - 2\mathcal{C}\left(\frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h}) + 2\sqrt{\bar{\alpha}(\bar{h}) |h_{se}|^2 P_1(\bar{h}) |h_{re}|^2 P_2(\bar{h})}}{\sigma_2^2} \right) \right]^+ \right\} + \min \left\{ \mathbb{E}_{\bar{h} \in \mathcal{A}^c} \left[2\mathcal{C}\left(\frac{|h_{sd}|^2 P_1(\bar{h}) + |h_{rd}|^2 P_2(\bar{h})}{\sigma^2} \right) \right. \right. \\ & \left. - 2\mathcal{C}\left(\frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h})}{\sigma_2^2} \right) \right]^+, \quad \mathbb{E}_{\bar{h} \in \mathcal{A}^c} \left[2\mathcal{C}\left(\frac{|h_{sd}|^2 P_1(\bar{h})}{\sigma^2} \right) + 2\mathcal{C}\left(\frac{|h_{re}|^2 P_2(\bar{h})}{\sigma_2^2} \right) \right. \quad \left. \left. - 2\mathcal{C}\left(\frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h})}{\sigma_2^2} \right) \right]^+ \right\}. \end{aligned} \tag{32}$$

$$\begin{aligned} R_e^{\text{up}} = \max_{\substack{\mathbb{E}[P_1(\bar{h})] \leq P_1, \\ \mathbb{E}[P_2(\bar{h})] \leq P_2, \\ -1 \leq \psi(\bar{h}) \leq 1}} & \mathbb{E}_{\bar{h}} \left\{ 2\mathcal{C}\left(\frac{|h_{sd}|^2 P_1(\bar{h}) + |h_{rd}|^2 P_2(\bar{h}) + 2\psi(\bar{h}) \sqrt{|h_{sd}|^2 P_1(\bar{h}) |h_{rd}|^2 P_2(\bar{h})}}{\sigma^2} \right) \right. \\ & \left. - 2\mathcal{C}\left(\frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h}) + 2\psi(\bar{h}) \sqrt{|h_{se}|^2 P_1(\bar{h}) |h_{re}|^2 P_2(\bar{h})}}{\sigma_2^2} \right) \right\} \end{aligned} \tag{33}$$

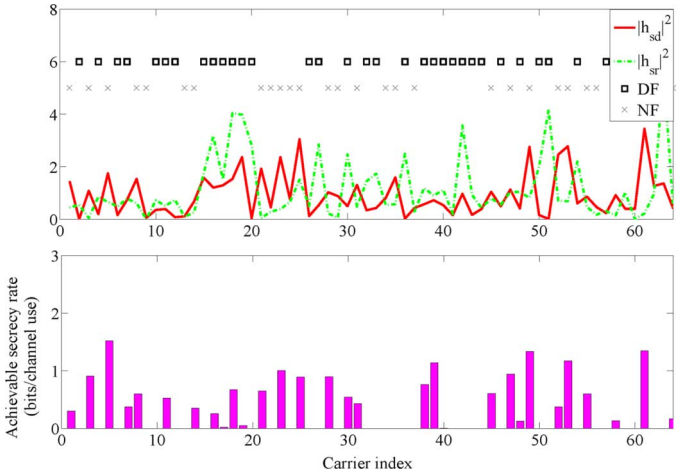


Fig. 4. Achievable perfect secrecy rate of a parallel relay-eavesdropper channel.

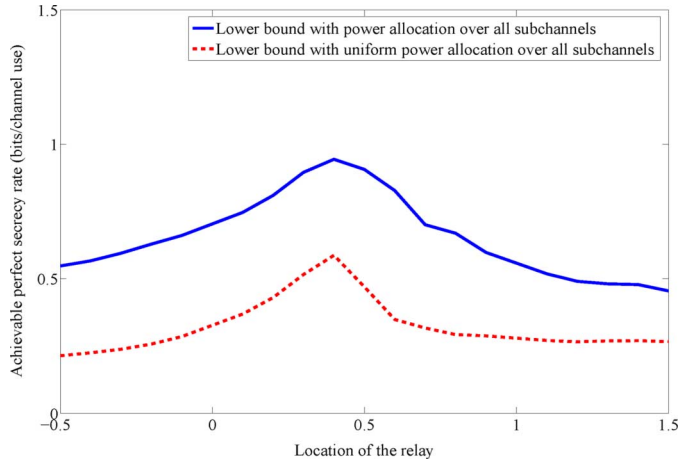


Fig. 5. Comparison of achievable perfect secrecy rate of the lower bound with optimized power allocation and with uniform power allocation over all subchannels.

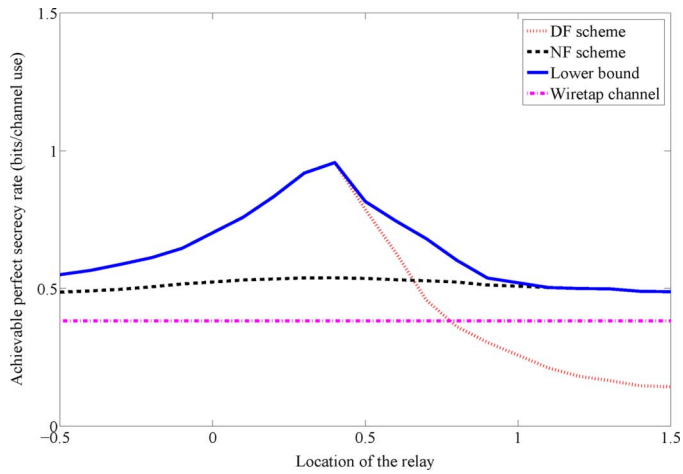


Fig. 6. Comparison of achievable perfect secrecy rate of some schemes with the lower bound.

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. Alternatively, this model can be seen as an OFDM system with L sub-carriers. 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 γ 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 all numerical examples, secrecy rate is given by bits per channel use. 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. 4 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. 4 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. 5 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 (32) 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. 6 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 $0.5 < d < 1.2$

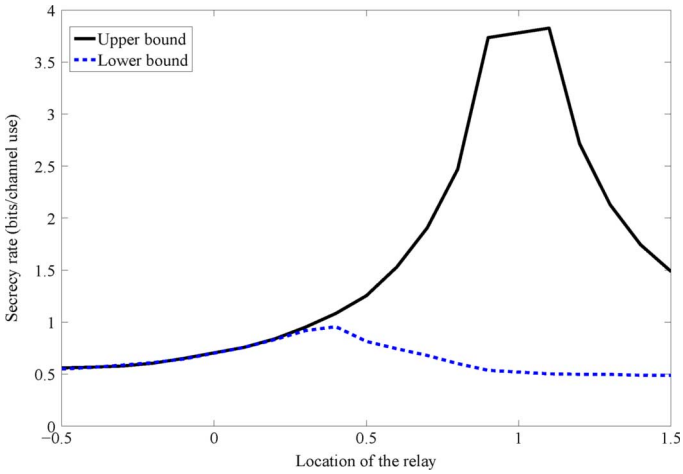


Fig. 7. Bounds on perfect secrecy rate.

is of particular interest. In this region the relay selects between DF scheme and NF scheme for each subchannel 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 codewords 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. 7 we compare the lower bound obtained in Fig. 6, 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 bounds coincide. This is achieved by using DF scheme on all subchannels.

VI. Conclusion

We studied the problem of secure communication over parallel relay channel. Outer and inner bounds on the rate-equivocation are established for the DM case. Developing an outer bound on the parallel relay-eavesdropper channel is non-trivial and it does not follow directly from the one established in [12]. For the Gaussian memoryless case, lower and upper bounds on the perfect secrecy rate are established. The computable upper bound for the Gaussian model shows some separability over subchannels. In the case in which the relay does not hear the source, under some specific conditions the lower and upper bounds 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 results in higher secrecy rate.

Appendix A
Proof of Theorem 1

The proof generalizes the results of [12, Theorem 1] and uses elements from a similar proof in the context of parallel BCC in [3].

1) We first bound the equivocation rate as follows:

$$
\begin{aligned}
nR_e &= H\left(W \mid Y^n_{2[1,L]}\right)\\
&= H(W) - I\left(W; Y^n_{2[1,L]}\right)\\
&= I\left(W; Y^n_{[1,L]}\right) - I\left(W; Y^n_{2[1,L]}\right) + H\left(W \,\middle|\, Y^n_{[1,L]}\right)\\
&\overset{(a)}{\leq} I\left(W; Y^n_{[1,L]}\right) - I\left(W; Y^n_{2[1,L]}\right) + n\epsilon_n\\
&= \sum_{l=1}^{L} I\left(W; Y_l^n \,\middle|\, Y^n_{[1,l-1]}\right) - I\left(W; Y^n_{2l} \,\middle|\, Y^n_{2[l+1,L]}\right) + n\epsilon_n\\
&= \sum_{l=1}^{L}\sum_{i=1}^{n} I\left(W; Y_{li} \,\middle|\, Y_l^{i-1}, Y^n_{[1,l-1]}\right)\\
&\quad - I\left(W; Y_{2li} \,\middle|\, Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}\right) + n\epsilon_n\\
&= \sum_{l=1}^{L}\sum_{i=1}^{n} I\left(W, Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}; Y_{li} \,\middle|\, Y_l^{i-1}, Y^n_{[1,l-1]}\right)\\
&\quad - I\left(Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}; Y_{li} \,\middle|\, W, Y_l^{i-1}, Y^n_{[1,l-1]}\right)\\
&\quad - I\left(W, Y_l^{i-1}, Y^n_{[1,l-1]}; Y_{2li} \,\middle|\, Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}\right)\\
&\quad + I\left(Y_l^{i-1}, Y^n_{[1,l-1]}; Y_{2li} \,\middle|\, W, Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}\right) + n\epsilon_n\\
&\overset{(b)}{=} \sum_{l=1}^{L}\sum_{i=1}^{n} I\left(W, Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}; Y_{li} \,\middle|\, Y_l^{i-1}, Y^n_{[1,l-1]}\right)\\
&\quad - I\left(W, Y_l^{i-1}, Y^n_{[1,l-1]}; Y_{2li} \,\middle|\, Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}\right) + n\epsilon_n\\
&= \sum_{l=1}^{L}\sum_{i=1}^{n} I\left(Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}; Y_{li} \,\middle|\, Y_l^{i-1}, Y^n_{[1,l-1]}\right)\\
&\quad + I\left(W; Y_{li} \,\middle|\, Y_l^{i-1}, Y^n_{[1,l-1]}, Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}\right)\\
&\quad - I\left(Y_l^{i-1}, Y^n_{[1,l-1]}; Y_{2li} \,\middle|\, Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}\right)\\
&\quad - I\left(W; Y_{2li} \,\middle|\, Y_l^{i-1}, Y^n_{[1,l-1]}, Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}\right) + n\epsilon_n\\
&\overset{(c)}{=} \sum_{l=1}^{L}\sum_{i=1}^{n} I\left(W; Y_{li} \,\middle|\, Y_l^{i-1}, Y^n_{[1,l-1]}, Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}\right)\\
&\quad - I\left(W; Y_{2li} \,\middle|\, Y_l^{i-1}, Y^n_{[1,l-1]}, Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}\right)\\
&\quad + n\epsilon_n \qquad (34)
\end{aligned}
$$

where $\epsilon_n \to 0$ as $n \to \infty$; (a) follows from Fano's inequality; and (b) and (c) follows from [2, Lemma 7].

We introduce a random variable T uniformly distributed over $\{1, 2, \ldots, n\}$ and set, $U_{li} := Y_l^{i-1}, Y^n_{[1,l-1]}, Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}$, $V_{1li} := W, Y^n_{2l[i+1]}, Y^n_{2[l+1,L]}$ and $V_{2li} := Y_l^{i-1}, Y^n_{[1,l-1]}$. We define $U_l = (T, U_{li}), V_{1l} = (T, V_{1li}), V_{2l} = (T, V_{2li}), X_{1l} = X_{1lT}, X_{2l} = X_{2lT}, Y_l = Y_{lT}, Y_{1l} = Y_{1lT}, Y_{2l} = Y_{2lT}$, for $l = 1, \ldots, L$. Note that $(U_l, V_{1l}, V_{2l}, X_{1l}, X_{2l}, Y_l, Y_{1l}, Y_{2l})$ satisfies the following Markov chain condition:

$$
\begin{aligned}
U_l \to (V_{1l}, V_{2l}) \to (X_{1l}, X_{2l})\\
\to (Y_l, Y_{1l}, Y_{2l}), \text{ for } l = 1, \ldots, L.
\end{aligned}
$$

Thus, we have

$$\begin{aligned}
R_e &\le \frac{1}{n}\sum_{l=1}^{L}\sum_{i=1}^{n} I\left(W;Y_{li}\left|Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n\right.\right)\\
&\quad - I\left(W;Y_{2li}\left|Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n\right.\right)+\epsilon_n\\
&= \frac{1}{n}\sum_{l=1}^{L}\sum_{i=1}^{n} I\Big(W,Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n;Y_{li}\Big|\\
&\quad Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n\Big)\\
&\quad - I\Big(W,Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n;Y_{2li}\Big|\\
&\quad Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n\Big)+\epsilon_n\\
&\overset{(d)}{=} \frac{1}{n}\sum_{l=1}^{L}\sum_{i=1}^{n} I(V_{1li},V_{2li};Y_{li}\,|\,U_{li})\\
&\quad - I(V_{1li},V_{2li};Y_{2li}\,|\,U_{li})+\epsilon_n \qquad (35)\\
&\overset{(e)}{=} \sum_{l=1}^{L} I(V_{1l},V_{2l};Y_l\,|\,U_l) - I(V_{1l},V_{2l};Y_{2l}\,|\,U_l)+\epsilon_n \qquad (36)
\end{aligned}$$

where (d) and (e) follow by using the above definition. We can also bound the equivocation rate as follows. We continue from (34) to get

$$\begin{aligned}
R_e &\le \frac{1}{n}\sum_{l=1}^{L}\sum_{i=1}^{n} I\left(W;Y_{li}\left|Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n\right.\right)\\
&\quad - I\left(W;Y_{2li}\left|Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n\right.\right)+\epsilon_n\\
&= \frac{1}{n}\sum_{l=1}^{L}\sum_{i=1}^{n} I\Big(W,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n;Y_{li}\Big|\\
&\quad Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n\Big)\\
&\quad - I\Big(W,Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n;Y_{2li}\Big|\\
&\quad Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n\Big)+\epsilon_n\\
&\le \frac{1}{n}\sum_{l=1}^{L}\sum_{i=1}^{n} I\Big(W,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n;Y_{li},Y_{1li}\Big|\\
&\quad Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n\Big)\\
&\quad - I\Big(W,Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n;Y_{2li}\Big|\\
&\quad Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n\Big)+\epsilon_n\\
&\overset{(f)}{=} \frac{1}{n}\sum_{l=1}^{L}\sum_{i=1}^{n} I\left(V_{1li};Y_{li},Y_{1li}\mid V_{2li},U_{li}\right)\\
&\quad - I\left(V_{1li},V_{2li};Y_{2li}\mid U_{li}\right)+\epsilon_n \qquad (37)\\
&\overset{(g)}{=} \sum_{l=1}^{L} I\left(V_{1l};Y_l,Y_{1l}\mid V_{2l},U_l\right) - I\left(V_{1l},V_{2l};Y_{2l}\mid U_l\right)+\epsilon_n \qquad (38)
\end{aligned}$$

where (f) and (g) follow from the above definition.

2) We now bound the rate R as follows:

$$\begin{aligned}
nR &= H(W)\\
&= I\left(W;Y_{[1,L]}^n\right)+H\left(W\left|Y_{[1,L]}^n\right.\right)\\
&\overset{(h)}{\le} I\left(W;Y_{[1,L]}^n\right)+n\epsilon_n\\
&= \sum_{l=1}^{L} I\left(W;Y_l^n\left|Y_{[1,l-1]}^n\right.\right)+n\epsilon_n\\
&= \sum_{l=1}^{L}\sum_{i=1}^{n} I\left(W;Y_{li}\left|Y_l^{i-1},Y_{[1,l-1]}^n\right.\right)+n\epsilon_n\\
&= \sum_{l=1}^{L}\sum_{i=1}^{n} H\left(Y_{li}\left|Y_l^{i-1},Y_{[1,l-1]}^n\right.\right)\\
&\quad - H\left(Y_{li}\left|W,Y_l^{i-1},Y_{[1,l-1]}^n\right.\right)+n\epsilon_n\\
&\overset{(i)}{\le} \sum_{l=1}^{L}\sum_{i=1}^{n} H(Y_{li}) - H\left(Y_{li}\left|W,Y_l^{i-1},Y_{[1,l-1]}^n\right.\right)+n\epsilon_n\\
&\overset{(j)}{\le} \sum_{l=1}^{L}\sum_{i=1}^{n} H(Y_{li})\\
&\quad - H\left(Y_{li}\left|W,Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n\right.\right)+n\epsilon_n\\
&= \sum_{l=1}^{L}\sum_{i=1}^{n} I\Big(W,Y_l^{i-1},Y_{[1,l-1]}^n,Y_{2l[i+1]}^n,Y_{2[l+1,L]}^n;Y_{li}\Big)+n\epsilon_n\\
&= \sum_{l=1}^{L}\sum_{i=1}^{n} I(V_{1li},V_{2li};Y_{li})+n\epsilon_n. \qquad (39)
\end{aligned}$$

Hence, we have

$$\begin{aligned}
R &\le \frac{1}{n}\sum_{l=1}^{L}\sum_{i=1}^{n} I(V_{1li},V_{2li};Y_{li})+\epsilon_n\\
&\le \sum_{l=1}^{L} I(V_{1l},V_{2l};Y_l)+\epsilon_n \qquad (40)
\end{aligned}$$

where (h) follows from Fano's inequality; (i) and (j) follows from the fact that conditioning reduces entropy.

We can also bound the rate R as follows:

$$\begin{aligned}
nR &= H(W)\\
&= I\left(W;Y_{[1,L]}^n\right)+H\left(W\left|Y_{[1,L]}^n\right.\right)\\
&\overset{(k)}{\le} I\left(W;Y_{[1,L]}^n\right)+n\epsilon_n\\
&= \sum_{l=1}^{L} I\left(W;Y_l^n\left|Y_{[1,l-1]}^n\right.\right)+n\epsilon_n\\
&= \sum_{l=1}^{L}\sum_{i=1}^{n} I\left(W;Y_{li}\left|Y_l^{i-1},Y_{[1,l-1]}^n\right.\right)+n\epsilon_n\\
&\le \sum_{l=1}^{L}\sum_{i=1}^{n} I\left(W;Y_{1li},Y_{li}\left|Y_l^{i-1},Y_{[1,l-1]}^n\right.\right)+n\epsilon_n
\end{aligned}$$

$$R_e^{\mathrm{up}} = \max_{\substack{\sum_{l=1}^{L} P_{1l} \le P_1,\\ \sum_{l=1}^{L} P_{2l} \le P_2,\\ -1 \le \psi_l \le 1\\ \text{for } l=1,\ldots,L}} \sum_{l=1}^{L} \frac{1}{2}\log\left(1+\frac{P_{1l}+\rho_{1l}P_{2l}+2\psi_l\sqrt{\rho_{1l}P_{1l}P_{2l}}}{\sigma_l^2}\right) - \frac{1}{2}\log\left(1+\frac{P_{1l}+\rho_{2l}P_{2l}+2\psi_l\sqrt{\rho_{2l}P_{1l}P_{2l}}}{\sigma_{2l}^2}\right) \quad (50)$$

$$\begin{aligned}
&= \sum_{l=1}^{L}\sum_{i=1}^{n} H\left(Y_{1li}, Y_{li}\left|Y_l^{i-1}, Y_{[1,l-1]}^n\right.\right)\\
&\quad - H\left(Y_{1li}, Y_{li}\left|W, Y_l^{i-1}, Y_{[1,l-1]}^n\right.\right) + n\epsilon_n\\
&\overset{(l)}{\le} \sum_{l=1}^{L}\sum_{i=1}^{n} H\left(Y_{1li}, Y_{li}\left|Y_l^{i-1}, Y_{[1,l-1]}^n\right.\right)\\
&\quad - H\left(Y_{1li}, Y_{li}\left|W, Y_l^{i-1}, Y_{[1,l-1]}^n, Y_{2l[i+1]}^n, Y_{2[l+1,L]}^n\right.\right) + n\epsilon_n\\
&= \sum_{l=1}^{L}\sum_{i=1}^{n} I\left(W, Y_{2l[i+1]}^n, Y_{2[l+1,L]}^n; Y_{1li}, Y_{li}\right|\\
&\quad \left. Y_l^{i-1}, Y_{[1,l-1]}^n\right) + n\epsilon_n\\
&= \sum_{l=1}^{L}\sum_{i=1}^{n} I(V_{1li}; Y_{1li}, Y_{li} \mid V_{2li}) + n\epsilon_n. \quad (41)
\end{aligned}$$

Hence, we have

$$\begin{aligned}
R &\le \frac{1}{n}\sum_{l=1}^{L}\sum_{i=1}^{n} I(V_{1li}; Y_{1li}, Y_{li} \mid V_{2li}) + \epsilon_n\\
&\le \sum_{l=1}^{L} I(V_{1l}; Y_l, Y_{1l} \mid V_{2l}) + \epsilon_n \quad (42)
\end{aligned}$$

where (k) follows from Fano's inequality; and (l) follows from the fact that conditioning reduces the entropy.

Therefore an outer bound on the achievable rate equivocation region is given by the following set:

$$\bigcup \{(R, R_e) \text{ that satisfy } (36), (38), (40), (42)\} \quad (43)$$

where the union is over all probability distributions $p(u_{[1,L]}, v_{1[1,L]}, v_{2[1,L]}, x_{1[1,L]}, x_{2[1,L]}, y_{[1,L]}, y_{1[1,L]}, y_{2[1,L]})$. Finally we note that the terms in (36), (38), (40), and (42) depend on the probability distribution $p(u_{[1,L]}, v_{1[1,L]}, v_{2[1,L]}, x_{1[1,L]}, x_{2[1,L]}, y_{[1,L]}, y_{1[1,L]}, y_{2[1,L]})$ only through $p(u_l, v_{1l}, v_{2l}, x_{1l}, x_{2l}, y_l, y_{1l}, y_{2l})$. Hence, there is no loss of optimality to consider only those distributions that have the form

$$\begin{aligned}
\prod_{l=1}^{L} &[p(u_l, v_{1l}, v_{2l}) p(x_{1l}, x_{2l} \mid u_l, v_{1l}, v_{2l})\\
&\cdot p(y_l, y_{1l}, y_{2l} \mid x_{1l}, x_{2l})]. \quad (44)
\end{aligned}$$

This completes the proof of Theorem 1.

Appendix B

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

$$\begin{aligned}
&\max_{\{\mathbf{K}_{\mathbf{P}_l} \in \mathcal{K}_{P_l}\}_{l=1,\ldots,L}} \sum_{l=1}^{L} I(X_{1l}, X_{2l}; Y_l) - I(X_{1l}, X_{2l}; Y_{2l})\\
&= \max_{\{\mathbf{K}_{\mathbf{P}_l} \in \mathcal{K}_{P_l}\}_{l=1,\ldots,L}} \sum_{l=1}^{L} [h(Y_l) - h(Y_l \mid X_{1l}, X_{2l}) - h(Y_{2l})\\
&\quad + h(Y_{2l} \mid X_{1l}, X_{2l})]\\
&= \max_{\{\mathbf{K}_{\mathbf{P}_l} \in \mathcal{K}_{P_l}\}_{l=1,\ldots,L}} \sum_{l=1}^{L} [h(Y_l) - h(Z_l) - h(Y_{2l}) + h(Z_{2l})]. \quad (45)
\end{aligned}$$

The first term in (45) is computed as follows:

$$\begin{aligned}
h(Y_l) &= h(X_{1l} + \sqrt{\rho_{1l}} X_{2l} + Z_l)\\
&= \frac{1}{2}\log(2\pi e)\left(P_{1l} + \rho_{1l}P_{2l} + 2\psi_l\sqrt{\rho_{1l}P_{1l}P_{2l}} + \sigma_l^2\right). \quad (46)
\end{aligned}$$

Similarly the second, third, and fourth term in (45) are computed as follows:

$$h(Z_l) = \frac{1}{2}\log 2\pi e\left(\sigma_l^2\right) \quad (47)$$

$$\begin{aligned}
h(Y_{2l}) = \frac{1}{2}\log(2\pi e)\big(&P_{1l} + \rho_{2l}P_{2l}\\
&+2\psi_l\sqrt{\rho_{2l}P_{1l}P_{2l}} + \sigma_{2l}^2\big) \quad (48)
\end{aligned}$$

$$h(Z_{2l}) = \frac{1}{2}\log 2\pi e\left(\sigma_{2l}^2\right). \quad (49)$$

Using (46)–(49) in (45) gives (50) at the top of the page.

References

[1] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. 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 Trans. Inf. 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 Trans. Inf. 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," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

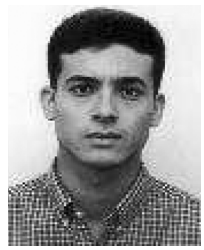
[6] F. Oggier and B. Hassibi, The Secrecy Capacity of the MIMO Wiretap Channel. [Online]. Available: http://arxiv.org/abs/0710.1920.

[7] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[8] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
[9] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.
[10] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006, pp. 356–360.
[11] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[12] L. Lai and H. E. Gamal, "The relay eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
[13] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in *Proc. 41st Annu. Conf. Information Sciences and Systems*, Baltimore, MD, Mar. 2007, pp. 13–18.
[14] M. Yuksel and E. Erkip, "Secure communication with a relay helping the wire-tapper," in *Proc. IEEE Information Theory Workshop*, Lake Tahoe, CA, Sep. 2007, pp. 595–600.
[15] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3801–3827, Aug. 2010.
[16] Y. Liang, V. V. Veeravalli, and H. V. Poor, "Resource allocation for wireless fading relay channels: Max-min solution," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3432–3453, Oct. 2007.
[17] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. 44th Annual Allerton Conf. Communication, Control and Computing*, Monticello, IL, Sep. 2006, pp. 841–848.
[18] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *EURASIP J. Wireless Commun. Netw., Special Issue on Wireless Physical Layer Security*, vol. 2009.
[19] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.
[20] A. A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

Zohaib Hassan Awan received the B.S. degree in electronics engineering from Ghulam Ishaq Khan Institute (GIKI), Topi, Pakistan, in 2005 and the M.S. degree in electrical engineering with majors in wireless systems from Royal Institute of Technology (KTH), Stockholm, Sweden, in 2008. Since January 2009, he has been working towards the Ph.D. degree with the ICTEAM Institute, Université Catholique de Louvain (UCL), Louvain-la-Neuve, Belgium.

His research interests include information-theoretic security, cooperative communications, and communication theory.



Abdellatif Zaidi received the B.S. degree in electrical engineering from École Nationale Supérieure de Techniques Avancés, ENSTA Paris Tech, Paris, France, in 2002 and the M.Sc. and Ph.D. degrees in electrical engineering from École Nationale Supérieure des Télécommunications, TELECOM ParisTech, Paris, France, in 2002 and 2005, respectively.

From December 2002 to December 2005, he was with the Communications and Electronics Department, TELECOM Paris Tech, and the Signals and Systems Laboratory, CNRS/Supélec, France, pursuing his Ph.D. degree. From May 2006 to September 2010, he was at École Polytechnique de Louvain, Université Catholique de Louvain, Louvain-la-Neuve, Belgium, working as a research assistant. He was "Research Visitor" at the University of Notre Dame, Notre Dame, IN, during fall 2007 and spring 2008. He is now an Assistant Professor at Université Paris-Est Marne-la-Vallée, France. His research interests cover a broad range of topics from signal processing for communication and multi-user information theory. Of particular interest are the problems of coding for side-informed channels, secure communication, coding and interference mitigation in multi-user channels, and relaying problems and cooperative communication with application to sensor networking and ad-hoc wireless networks.

Luc Vandendorpe (M'93–SM'99–F'06) was born in Mouscron, Belgium, in 1962. He received the Electrical Engineering degree (summa cum laude) and the Ph.D. degree from the Université Catholique de Louvain (UCL) Louvain-la-Neuve, Belgium, in 1985 and 1991, respectively.

Since 1985, he has been with the Communications and Remote Sensing Laboratory of UCL where he first worked in the field of bit rate reduction techniques for video coding. In 1992, he was a Visiting Scientist and Research Fellow at the Telecommunications and Traffic Control Systems Group of the Delft Technical University, Netherlands, where he worked on Spread Spectrum Techniques for Personal Communications Systems. From October 1992 to August 1997, he was a Senior Research Associate of the Belgian NSF at UCL. Presently, he is a Full Professor and Head of the Institute for Information and Communication Technologies, Electronics and Applied Mathematics of UCL. His current interest is in digital communication systems and more precisely resource allocation for OFDM(A) based multicell systems, MIMO and distributed MIMO, sensor networks, turbo-based communications systems, physical layer security, and UWB based positioning.

Dr. Vandendorpe was co-recipient of the Biennal Alcatel-Bell Award in 1990 from the Belgian NSF for a contribution in the field of image coding. In 2000, he was co-recipient (with J. Louveaux and F. Deryck) of the Biennal Siemens Award from the Belgian NSF for a contribution about filter bank based multicarrier transmission. In 2004, he was co-winner (with J. Czyz) of the Face Authentication Competition, FAC 2004. He is or has been TPC member for numerous IEEE conferences (VTC Fall, Globecom Communications Theory Symposium, SPAWC, ICC) and for the Turbo Symposium. He was co-technical chair (with P. Duhamel) for IEEE ICASSP 2006. He was an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS for Synchronization and Equalization between 2000 and 2002, an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS between 2003 and 2005, and an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING between 2004 and 2006. He was chair of the IEEE Benelux joint chapter on Communications and Vehicular Technology between 1999 and 2003. He was an elected member of the Signal Processing for Communications committee between 2000 and 2005, and between 2009 and 2011, and an elected member of the Sensor Array and Multichannel Signal Processing committee of the Signal Processing Society between 2006 and 2008. Currently, he is the Editor-in-Chief for the *EURASIP Journal on Wireless Communications and Networking*.