

On Secure Transmission over Parallel Relay Eavesdropper Channel

Zohaib Hassan Awan, Abdellatif Zaidi and Luc Vandendorpe

ICTEAM institute, Université Catholique de Louvain, Louvain-la-Neuve 1348, Belgium.

E-mail: {zohaib.awan, abdellatif.zaidi, luc.vandendorpe}@uclouvain.be

Abstract—We study a four terminal parallel relay-eavesdropper channel which consists of multiple independent relay-eavesdropper channels as subchannels. For the discrete memoryless case, we establish inner and outer bounds on the rate-equivocation region. 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. The inner bound allows relay mode selection. For the Gaussian model we establish lower and upper bounds on the perfect secrecy rate. We show that the bounds meet in some special cases, including when the relay does not hear the source. We illustrate the analytical results through some numerical examples.

I. INTRODUCTION

The relay channel has been analyzed in [1], [2] (and references therein), but the focus was on how to increase achievable rate and reliability. The idea of cooperation between users in the context of security was introduced in [3] (and references therein). The premise is that when the main channel is more noisy than the channel to the eavesdropper, cooperation between users is utilized to obtain a positive secrecy capacity. Secrecy is achieved by using the relay as a trusted node which facilitates the information decoding at the destination while confusing the eavesdropper.

In this paper, we study a parallel relay-eavesdropper channel. A parallel relay-eavesdropper channel consists of a generalization of the setup in [3] to the case 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 model is depicted in Figure 1. For this model, we establish outer and inner bounds on the rate-equivocation region for the discrete memoryless case. The inner bound is obtained with a coding scheme in which, for each subchannel, the relay operates 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 [3, 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 [4]. We also show that the bounds on the equivocation rate coincide in the case in which all the subchannels are degraded, thus characterizing the secrecy capacity.

For the Gaussian model, we focus on the perfect secrecy case. We establish lower and upper bounds on the perfect

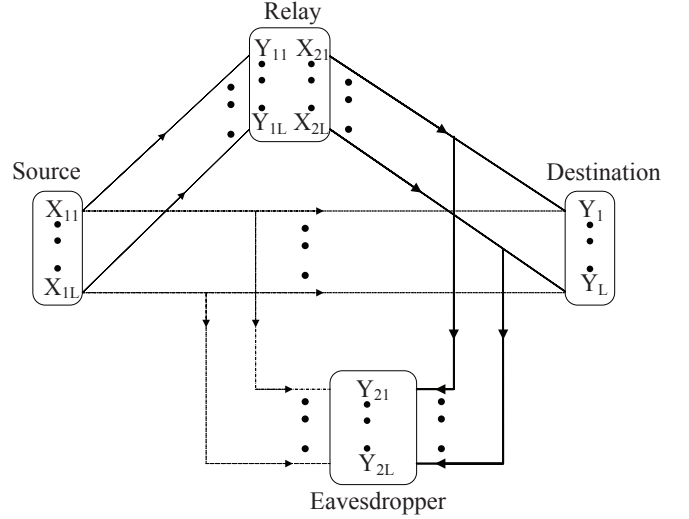


Fig. 1. Parallel relay-eavesdropper channel.

secrecy rate. We note that establishing a computable upper bounds on the secrecy rate for the Gaussian model is non-trivial. In part, this is because converse techniques that are obtained directly from the analysis in the discrete case involves auxiliary random variables, the optimal choice of which is difficult to obtain. 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], [6] in the 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 studied model. 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 Gaussian case in which the relay does not hear to 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 general Gaussian case, 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 in [7]. These assumptions turn the parallel Gaussian relay-eavesdropper channel into a parallel Gaussian wiretap channel, the secrecy capacity of which is established in [4].

Furthermore, we apply the results developed for the parallel Gaussian relay-eavesdropper channel to the fading relay-eavesdropper channel, which is a special case of parallel Gaussian relay-eavesdropper channel, with each fading state corresponding to one subchannel. We illustrate our results through some numerical examples.

In this paper, the notation $X_{[1,L]}$ is used as a shorthand for (X_1, X_2, \dots, X_L) , the notation $X_{[1,L]}^n$ is used as a shorthand for $(X_1^n, X_2^n, \dots, X_L^n)$ where for $l = 1, \dots, L$, $X_l^n := (X_{l1}, X_{l2}, \dots, X_{ln})$ and the notation $\mathcal{X}_{1[L]}$ is used as a shorthand for $\mathcal{X}_{11} \times \mathcal{X}_{12} \dots \times \mathcal{X}_{1L}$. We define the function $\mathcal{C}(x)$ as $\frac{1}{2} \log_2(1+x)$. Throughout the paper the logarithm function is taken to the base 2.

II. THE PARALLEL RELAY-EAVESDROPPER CHANNEL

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 $\mathcal{Y}_{1[1,L]}$, $\mathcal{Y}_{2[1,L]}$, $\mathcal{Y}_{3[1,L]}$ as finite output alphabets. The transition probability distribution is given by

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

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 $l = 1, \dots, L$. For the subchannel l , X_{1l} and X_{2l} are the inputs from the source and relay; and Y_{1l} , Y_{2l} , Y_l are the outputs at the relay, eavesdropper and destination, respectively. The source sends a message $W \in \mathcal{W} = \{1, \dots, 2^{nR}\}$ using a $(2^{nR}, n)$ code consisting of: 1) a stochastic encoder at the source that maps $W \rightarrow X_{1[1,L]}^n$, 2) a relay encoder that maps $f_i(Y_{1[1,L]}^{i-1}) \rightarrow X_{2[1,L],i}$ for $1 \leq i \leq n$, and 3) a decoding function $g(Y_{2[1,L]}^n) \rightarrow W$. The average error probability of a $(2^{nR}, n)$ code is defined as

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

The eavesdropper listens to what the source and relay transmit for free, due to the wireless nature of the medium. 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. 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 $n \geq n(\epsilon)$

$$\begin{aligned} \frac{H(W)}{n} &\geq R - \epsilon, \\ \frac{H(W | Y_{2[1,L]}^n)}{n} &\geq R_e - \epsilon, \\ P_e^n &\leq \epsilon. \end{aligned} \quad (3)$$

III. DISCRETE MEMORYLESS CHANNEL

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

A. Outer bound

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

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

Proof: The proof of Theorem 1 is given in Appendix I. \square

B. Achievable rate-equivocation region

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

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

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 [3, 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 [3, Theorem 3].

Remark 1: For a parallel relay-eavesdropper channel in which all subchannels are degraded¹, i.e.,

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

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

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

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

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

IV. GAUSSIAN CHANNEL

In this section we study a parallel Gaussian relay-eavesdropper channel. We focus on perfectly secure achievable rates, i.e., $(R, R_e) = (R, R)$. 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 ; $X_{1l,i}$ and $X_{2l,i}$ are the inputs from the source and relay nodes respectively. The parameter ρ_{1l} indicates the ratio of the R-D link signal-to-noise (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 the l^{th} subchannel. The source and relay input sequences are subject to the following average transmit power constraints

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

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

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

A. Lower bound on the perfect secrecy rate

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

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

Proof: The achievability follows by applying Theorem 2 with the choice $U_l = \text{constant}$, $V_{1l} = X_{1l}$, $V_{2l} = X_{2l}$, $X_{1l} = \tilde{X}_{1l} + \sqrt{\frac{\alpha_l P_{1l}}{P_{2l}}} X_{2l}$, $\tilde{\alpha}_l = 1 - \alpha_l$, $\tilde{X}_{1l} \sim \mathcal{N}(0, \alpha_l P_{1l})$ independent of $X_{2l} \sim \mathcal{N}(0, P_{2l})$ 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 (10). \square

The parameters P_{1l} and P_{2l} indicate the source and relay power allocated for transmission over the subchannel l . In (10), after some straightforward algebra, the contribution to the equivocation of information sent through NF (set \mathcal{A}^c) can be condensed by observing that we only need to consider $\min\{\sum_{l \in \mathcal{A}^c} I(X_{2l}, Y_{2l}), \sum_{l \in \mathcal{A}^c} I(X_{2l}, Y_l)\} = \sum_{l \in \mathcal{A}^c} I(X_{2l}, Y_{2l})$ in set \mathcal{A}^c , to get a higher secrecy rate. A simplified expression for R_e^{low} is given by (11).

B. 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 (7), an upper bound on the secrecy rate is given by

$$R_e^{\text{up}} \leq \max_{\{\mathbf{K}_{P_l} \in \mathcal{K}_{P_l}\}_{l=1, \dots, L}} \sum_{l=1}^L I(X_{1l}X_{2l}; Y_l) - I(X_{1l}X_{2l}; Y_{2l}) \quad (12)$$

where the maximization is over $[X_{1l}, X_{2l}] \sim \mathcal{N}(\mathbf{0}, \mathbf{K}_{P_l})$ with $\mathcal{K}_{P_l} = \left\{ \mathbf{K}_{P_l} : \mathbf{K}_{P_l} = \begin{bmatrix} P_{1l} & \psi_l \sqrt{P_{1l}P_{2l}} \\ \psi_l \sqrt{P_{1l}P_{2l}} & P_{2l} \end{bmatrix}, -1 \leq \psi_l \leq 1 \right\}$, for $l = 1, \dots, L$, 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 result in Theorem 1 established for the DM case can be extended to memoryless channels with discrete time and continuous alphabets using standard techniques [8, Chapter 7]. Taking the first term of the minimization in the bound on the equivocation rate, we get

$$R_e \leq \max \sum_{l=1}^L I(V_{1l}V_{2l}; Y_l \mid U_l) - I(V_{1l}V_{2l}; Y_{2l} \mid U_l) \quad (13)$$

where $U_l \rightarrow (V_{1l}, V_{2l}) \rightarrow (X_{1l}, X_{2l}) \rightarrow (Y_l, Y_{1l}, Y_{2l})$, for $l = 1, \dots, L$. The rest of the proof uses elements from related

works in [4] and [5]. Continuing from (13), we obtain

$$\begin{aligned}
R_e &\leq \sum_{l=1}^L I(V_{1l}V_{2l}; Y_l | U_l) - I(V_{1l}V_{2l}; Y_{2l} | U_l) \\
&\stackrel{(a)}{\leq} \sum_{l=1}^L I(V_{1l}V_{2l}; Y_l) - I(V_{1l}V_{2l}; Y_{2l}) \\
&\leq \sum_{l=1}^L I(V_{1l}V_{2l}; Y_l Y_{2l}) - I(V_{1l}V_{2l}; Y_{2l}) \\
&\stackrel{(b)}{=} \sum_{l=1}^L [I(X_{1l}X_{2l}; Y_l Y_{2l}) - I(X_{1l}X_{2l}; Y_l Y_{2l} | V_{1l}V_{2l})] \\
&\quad - [I(X_{1l}X_{2l}; Y_{2l}) - I(X_{1l}X_{2l}; Y_{2l} | V_{1l}V_{2l})] \\
&= \sum_{l=1}^L [I(X_{1l}X_{2l}; Y_l Y_{2l}) - I(X_{1l}X_{2l}; Y_{2l})] \\
&\quad - [I(X_{1l}X_{2l}; Y_l Y_{2l} | V_{1l}V_{2l}) - I(X_{1l}X_{2l}; Y_{2l} | V_{1l}V_{2l})] \\
&\leq \sum_{l=1}^L [I(X_{1l}X_{2l}; Y_l Y_{2l}) - I(X_{1l}X_{2l}; Y_{2l})] \\
&= \sum_{l=1}^L I(X_{1l}X_{2l}; Y_l | Y_{2l}), \tag{14}
\end{aligned}$$

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

We now tighten the upper bound (14) by using an argument previously used in [5], [6] in the context of multi-antennas wiretap channels. More specifically, observing that, the original bound (13) 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 (14) can be further tightened as

$$R_e \leq \max_{p(x_{1l}, x_{2l})} \sum_{l=1}^L \min_{p(y'_l, y'_{2l}|x_{1l}, x_{2l})} I(X_{1l}X_{2l}; Y'_l | Y'_{2l}) \tag{15}$$

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 (15) is maximized when the inputs are jointly Gaussian, i.e., $[X_{1l}, X_{2l}] \sim \mathcal{N}(\mathbf{0}, \mathbf{K}_{P_l})$, $\mathbf{K}_{P_l} \in \mathcal{K}_{P_l}$ with $\mathcal{K}_{P_l} = \left\{ \mathbf{K}_{P_l} : \right.$

$\mathbf{K}_{P_l} = \begin{bmatrix} P_{1l} & \psi_l \sqrt{P_{1l}P_{2l}} \\ \psi_l \sqrt{P_{1l}P_{2l}} & P_{2l} \end{bmatrix}, -1 \leq \psi_l \leq 1 \}$, for $l = 1, \dots, L$ 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, it can be shown that the evaluation of the upper bound (15) minimized over all possible correlations between Y'_l, Y'_{2l} , for $l = 1, \dots, L$ yields

$$R_e \leq \max_{\{\mathbf{K}_{P_l} \in \mathcal{K}_{P_l}\}_{l=1 \dots L}} \sum_{l=1}^L I(X_{1l}X_{2l}; Y_l) - I(X_{1l}X_{2l}; Y_{2l}). \tag{16}$$

This concludes the proof. \square

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

Theorem 4: For the model (7) in which the relay does not hear the source, the secrecy capacity is given by

$$\begin{aligned}
C_s &= \min \left\{ \max_{l=1}^L \mathcal{C}\left(\frac{P_{1l} + \rho_{1l}P_{2l}}{\sigma_l^2}\right) - \mathcal{C}\left(\frac{P_{1l} + \rho_{2l}P_{2l}}{\sigma_{2l}^2}\right), \right. \\
&\quad \left. \max_{l=1}^L \mathcal{C}\left(\frac{P_{1l}}{\sigma_l^2}\right) - \mathcal{C}\left(\frac{P_{1l}}{\sigma_{2l}^2 + \rho_{2l}P_{2l}}\right) \right\} \tag{17}
\end{aligned}$$

where the maximization is over $\{P_{1l}, P_{2l}\}$, for $l = 1 \dots L$, 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 (17) 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 (17) can be established as follows. Our approach borrows

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

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

elements from an upper bounding technique that is used in [7], and can be seen as an extension of it to the case of parallel relay-eavesdropper channels. Assume that all the 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 [7], any upper bound for this model with full relay-destination cooperation and constrained eavesdropper, also applies for 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

$$Y'_{l,i} = X_{1l,i} + Z_{l,i}. \quad (18)$$

For the constrained eavesdropper the relay's transmission acts as an interference, with the worst case obtained with Gaussian $X_{2[1,L]}$ [7]. The equivalent output at the eavesdropper in this case is given by

$$Y'_{2l,i} = X_{1l,i} + \sqrt{\rho_{2l}\mathbb{E}[X_{2l,i}^2]} + Z_{2l,i}. \quad (19)$$

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 [4],

$$C_s \leq \max \sum_{l=1}^L I(X_{1l}; Y'_l) - I(X_{1l}; Y'_{2l}) \quad (20)$$

where the maximization is over $X_{1l} \sim \mathcal{N}(0, P_{1l})$, $X_{2l} \sim \mathcal{N}(0, P_{2l})$ for $l = 1 \dots L$, 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 (20) gives the second term of the minimization in (17).

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

V. FADING RELAY-EAVESDROPPER CHANNEL

We consider a fading relay-eavesdropper channel that is corrupted by multiplicative fading gain processes in addition to additive white Gaussian noise (AWGN) processes. The received signals are given by

$$\begin{aligned} Y_{1,i} &= h_{sr,i} X_{1,i} + Z_{1,i} \\ Y_i &= h_{sd,i} X_{1,i} + h_{rd,i} X_{2,i} + Z_i \\ Y_{2,i} &= h_{se,i} X_{1,i} + h_{re,i} X_{2,i} + Z_{2,i} \end{aligned} \quad (21)$$

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., $\sum_{i=1}^n \mathbb{E}[|X_{1,i}|^2] \leq nP_1$, $\sum_{i=1}^n \mathbb{E}[|X_{2,i}|^2] \leq nP_2$. Let $\bar{h}_i := [h_{sd,i} \ h_{rd,i} \ h_{se,i} \ h_{re,i} \ h_{sr,i}]$ and we 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, 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 (21), which follows from (11) is given by (22). The upper bound for the fading relay-eavesdropper channel follows from (12) and is given by (23). In the achievable region we proposed a coding scheme which is a combination of DF and NF scheme. A pertinent question is how to decide which scheme to use on each subchannel? To accomplish this we define $\mathcal{A} := \{\bar{h} : |h_{sd}|^2 < |h_{sr}|^2\}$ contains all the fading state realizations in $\{\bar{h}\}$ where the S-R link is better than S-D link. The complement of set \mathcal{A} is $\mathcal{A}^c := \{\bar{h} : |h_{sd}|^2 \geq |h_{sr}|^2\}$.

VI. NUMERICAL RESULTS

We consider a fading relay-eavesdropper channel with L fading states. 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 γ is the path loss exponent and $h'_{i,j}$ is a complex Gaussian random variable with zero mean and variance one. Each subchannel is corrupted by AWGN with zero mean and variance one. The objective function for both lower and upper bounds are optimized numerically using AMPL with a commercially available solver, for instance SNOPT. Furthermore, for each symbol transmission same subchannel is used on S-R and R-D links to make the optimization tractable.

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 $\gamma := 2$. Fig. 2 shows the power allocation for a fading channel with 64 subchannels where the relay is located at (0.5,0), and marker 'x' denotes NF on a particular subchannel while marker '□' denotes DF on a particular subchannel. It can be seen from Fig. 2 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.

$$\begin{aligned}
R_e^{\text{low}} = & \max_{\substack{\mathbb{E}[P_1(\bar{h})] \leq P_1, \\ \mathbb{E}[P_2(\bar{h})] \leq P_2, \\ 0 \leq \alpha(\bar{h}) \leq 1}} \min \left\{ \mathbb{E}_{\bar{h} \in \mathcal{A}} \left[2\mathcal{C} \left(\frac{|h_{sd}|^2 P_1(\bar{h}) + |h_{rd}|^2 P_2(\bar{h}) + 2\sqrt{\alpha(\bar{h})|h_{sd}|^2 P_1(\bar{h})|h_{rd}|^2 P_2(\bar{h})}}{\sigma^2} \right) \right. \right. \\
& - 2\mathcal{C} \left(\frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h}) + 2\sqrt{\alpha(\bar{h})|h_{se}|^2 P_1(\bar{h})|h_{re}|^2 P_2(\bar{h})}}{\sigma_2^2} \right) \left. \right]^+, \mathbb{E}_{\bar{h} \in \mathcal{A}} \left[2\mathcal{C} \left(\frac{\alpha(\bar{h})|h_{sr}|^2 P_1(\bar{h})}{\sigma_1^2} \right) \right. \\
& - 2\mathcal{C} \left(\frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h}) + 2\sqrt{\alpha(\bar{h})|h_{se}|^2 P_1(\bar{h})|h_{re}|^2 P_2(\bar{h})}}{\sigma_2^2} \right) \left. \right]^+ \left. \right\} + \min \left\{ \mathbb{E}_{\bar{h} \in \mathcal{A}^c} \left[2\mathcal{C} \left(\frac{|h_{sd}|^2 P_1(\bar{h}) + |h_{rd}|^2 P_2(\bar{h})}{\sigma^2} \right) \right. \right. \\
& - 2\mathcal{C} \left(\frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h})}{\sigma_2^2} \right) \left. \right]^+, \mathbb{E}_{\bar{h} \in \mathcal{A}^c} \left[2\mathcal{C} \left(\frac{|h_{sd}|^2 P_1(\bar{h})}{\sigma^2} \right) + 2\mathcal{C} \left(\frac{|h_{re}|^2 P_2(\bar{h})}{\sigma_2^2} \right) - 2\mathcal{C} \left(\frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h})}{\sigma_2^2} \right) \right]^+ \left. \right\}. \tag{22}
\end{aligned}$$

$$\begin{aligned}
R_e^{\text{up}} \leq & \max_{\substack{\mathbb{E}[P_1(\bar{h})] \leq P_1, \\ \mathbb{E}[P_2(\bar{h})] \leq P_2, \\ -1 \leq \psi(\bar{h}) \leq 1}} \mathbb{E}_{\bar{h}} \left\{ 2\mathcal{C} \left(\frac{|h_{sd}|^2 P_1(\bar{h}) + |h_{rd}|^2 P_2(\bar{h}) + 2\psi(\bar{h})\sqrt{|h_{sd}|^2 P_1(\bar{h})|h_{rd}|^2 P_2(\bar{h})}}{\sigma^2} \right) \right. \\
& \left. - 2\mathcal{C} \left(\frac{|h_{se}|^2 P_1(\bar{h}) + |h_{re}|^2 P_2(\bar{h}) + 2\psi(\bar{h})\sqrt{|h_{se}|^2 P_1(\bar{h})|h_{re}|^2 P_2(\bar{h})}}{\sigma_2^2} \right) \right\}. \tag{23}
\end{aligned}$$

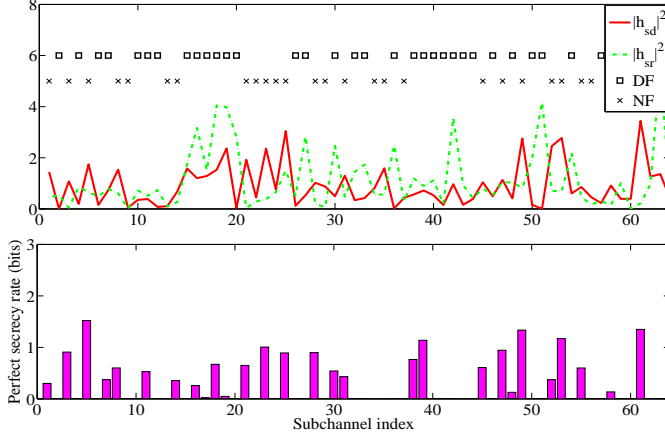


Fig. 2. Achievable perfect secrecy rate of a fading parallel relay-eavesdropper channel.

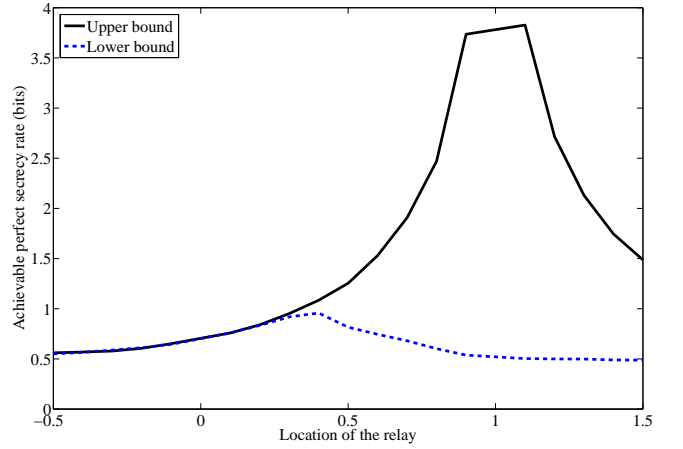


Fig. 3. Bounds on perfect secrecy rate.

Mode selection at the relay by only considering the relative strength of the S-D and the S-R link is suboptimal because the achievable secrecy rate (22) also depends on the other link gain. We now consider the case in which the relay independently selects the scheme which maximize the rate for each subchannel. When the relay is close to the source, it uses DF scheme on all subchannels. Similarly when the relay is close to the destination, use of NF scheme on all subchannels offers better rate. The region when the relay is between $0.5 < d < 1.2$, it selects between DF and NF scheme based on link gains of S-D, S-R link as mentioned above. In Fig. 3 we plot the optimized lower and upper bounds on the secrecy rate for 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.

APPENDIX I

The proof generalizes the results of Theorem 1 in [3] and uses elements from a similar proof in the context of parallel BCC in [4].

a) We first bound the equivocation rate as follows.

$$\begin{aligned}
nR_e &= H(W | Y_{2[1,L]}^n) \\
&= H(W) - I(W; Y_{2[1,L]}^n) \\
&= I(W; Y_{1[L]}^n) - I(W; Y_{2[1,L]}^n) + H(W | Y_{1[L]}^n) \\
&\stackrel{(a)}{\leq} I(W; Y_{1[L]}^n) - I(W; Y_{2[1,L]}^n) + n\epsilon_n \\
&= \sum_{l=1}^L I(W; Y_l^n | Y_{1[l-1]}^n) - I(W; Y_{2l}^n | Y_{2[l+1,L]}^n) + n\epsilon_n \\
&= \sum_{l=1}^L \sum_{i=1}^n I(W; Y_{li} | Y_l^{i-1} Y_{1[l-1]}^n) \\
&\quad - I(W; Y_{2li} | Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) + n\epsilon_n
\end{aligned}$$

$$\begin{aligned}
&= \sum_{l=1}^L \sum_{i=1}^n I(WY_{2l[i+1]}^n Y_{2[l+1,L]}^n; Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n) \\
&\quad - I(Y_{2l[i+1]}^n Y_{2[l+1,L]}^n; Y_{li} | WY_l^{i-1} Y_{[1,l-1]}^n) \\
&\quad - I(WY_l^{i-1} Y_{[1,l-1]}^n; Y_{2li} | Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) \\
&\quad + I(Y_l^{i-1} Y_{[1,l-1]}^n; Y_{2li} | WY_{2l[i+1]}^n Y_{2[l+1,L]}^n) + n\epsilon_n \\
&\stackrel{(b)}{\leq} \sum_{l=1}^L \sum_{i=1}^n I(WY_{2l[i+1]}^n Y_{2[l+1,L]}^n; Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n) \\
&\quad - I(WY_l^{i-1} Y_{[1,l-1]}^n; Y_{2li} | Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) + n\epsilon_n \\
&= \sum_{l=1}^L \sum_{i=1}^n I(Y_{2l[i+1]}^n Y_{2[l+1,L]}^n; Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n) \\
&\quad + I(W; Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) \\
&\quad - I(Y_l^{i-1} Y_{[1,l-1]}^n; Y_{2li} | Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) \\
&\quad - I(W; Y_{2li} | Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) + n\epsilon_n \\
&\stackrel{(c)}{=} \sum_{l=1}^L \sum_{i=1}^n I(W; Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) \\
&\quad - I(W; Y_{2li} | Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) + n\epsilon_n \quad (24)
\end{aligned}$$

where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$; (a) follows from Fano's inequality; and (b) and (c) follows from lemma 7 in [9].

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

$$U_l \rightarrow (V_{1l}, V_{2l}) \rightarrow (X_{1l}, X_{2l}) \rightarrow (Y_l, Y_{1l}, Y_{2l}), \text{ for } l = 1, \dots, L$$

Thus, we have

$$\begin{aligned}
R_e &\leq \frac{1}{n} \sum_{l=1}^L \sum_{i=1}^n I(W; Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) \\
&\quad - I(W; Y_{2li} | Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) + \epsilon_n \\
&= \frac{1}{n} \sum_{l=1}^L \sum_{i=1}^n I(WY_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n; Y_{li} | \\
&\quad Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) \\
&\quad - I(WY_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n; Y_{2li} | \\
&\quad Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) + \epsilon_n \\
&\stackrel{(d)}{=} \frac{1}{n} \sum_{l=1}^L \sum_{i=1}^n I(V_{1li} V_{2li}; Y_{li} | U_{li}) - I(V_{1li} V_{2li}; Y_{2li} | U_{li}) \\
&\quad + \epsilon_n \quad (25)
\end{aligned}$$

$$\stackrel{(e)}{\leq} \sum_{l=1}^L I(V_{1l} V_{2l}; Y_l | U_l) - I(V_{1l} V_{2l}; Y_{2l} | U_l) + \epsilon_n \quad (26)$$

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

continue from (24) to get

$$\begin{aligned}
R_e &\leq \frac{1}{n} \sum_{l=1}^L \sum_{i=1}^n I(W; Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) \\
&\quad - I(W; Y_{2li} | Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) + \epsilon_n \\
&= \frac{1}{n} \sum_{l=1}^L \sum_{i=1}^n I(WY_{2l[i+1]}^n Y_{2[l+1,L]}^n; Y_{li} | \\
&\quad Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) \\
&\quad - I(WY_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n; Y_{2li} | \\
&\quad Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) + \epsilon_n \\
&\leq \frac{1}{n} \sum_{l=1}^L \sum_{i=1}^n I(WY_{2l[i+1]}^n Y_{2[l+1,L]}^n; Y_{li} Y_{1li} | \\
&\quad Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) \\
&\quad - I(WY_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n; Y_{2li} | \\
&\quad Y_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) + \epsilon_n \\
&\stackrel{(f)}{=} \frac{1}{n} \sum_{l=1}^L \sum_{i=1}^n I(V_{1li}; Y_{li} Y_{1li} | U_{li} V_{2li}) \\
&\quad - I(V_{1li} V_{2li}; Y_{2li} | U_{li}) + \epsilon_n \quad (27)
\end{aligned}$$

$$\stackrel{(g)}{\leq} \sum_{l=1}^L I(V_{1l}; Y_l Y_{1l} | U_l V_{2l}) - I(V_{1l} V_{2l}; Y_{2l} | U_l) + \epsilon_n \quad (28)$$

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

b) We now bound the rate R as follows.

$$\begin{aligned}
R &= H(W) \\
&= I(W; Y_{[1,L]}^n) + H(W | Y_{[1,L]}^n) \\
&\stackrel{(h)}{\leq} I(W; Y_{[1,L]}^n) + n\epsilon_n \\
&= \sum_{l=1}^L I(W; Y_l^n | Y_{[1,l-1]}^n) + n\epsilon_n \\
&= \sum_{l=1}^L \sum_{i=1}^n I(W; Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n) + n\epsilon_n \\
&= \sum_{l=1}^L \sum_{i=1}^n H(Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n) \\
&\quad - H(Y_{li} | WY_l^{i-1} Y_{[1,l-1]}^n) + n\epsilon_n \\
&\stackrel{(i)}{\leq} \sum_{l=1}^L \sum_{i=1}^n H(Y_{li}) - H(Y_{li} | WY_l^{i-1} Y_{[1,l-1]}^n) + n\epsilon_n \\
&\stackrel{(j)}{\leq} \sum_{l=1}^L \sum_{i=1}^n H(Y_{li}) \\
&\quad - H(Y_{li} | WY_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n) + n\epsilon_n \\
&= \sum_{l=1}^L \sum_{i=1}^n I(WY_l^{i-1} Y_{[1,l-1]}^n Y_{2l[i+1]}^n Y_{2[l+1,L]}^n; Y_{li}) + n\epsilon_n
\end{aligned}$$

$$= \sum_{l=1}^L \sum_{i=1}^n I(V_{1li}, V_{2li}; Y_{li}) + n\epsilon_n. \quad (29)$$

Hence, we have

$$\begin{aligned} R &\leq \frac{1}{n} \sum_{l=1}^L \sum_{i=1}^n I(V_{1li}, V_{2li}; Y_{li}) + \epsilon_n \\ &\leq \sum_{l=1}^L I(V_{1l}, V_{2l}; Y_l) + \epsilon_n \end{aligned} \quad (30)$$

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

$$\begin{aligned} nR &= H(W) \\ &= I(W; Y_{[1,L]}^n) + H(W | Y_{[1,L]}^n) \\ &\stackrel{(k)}{\leq} I(W; Y_{[1,L]}^n) + n\epsilon_n \\ &= \sum_{l=1}^L I(W; Y_l^n | Y_{[1,L]}^n) + H(W | n\epsilon_n) \\ &= \sum_{l=1}^L \sum_{i=1}^n I(W; Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n) + n\epsilon_n \\ &\leq \sum_{l=1}^L \sum_{i=1}^n I(W; Y_{1li} Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n) + n\epsilon_n \\ &= \sum_{l=1}^L \sum_{i=1}^n H(Y_{1li} Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n) \\ &\quad - H(Y_{1li} Y_{li} | W Y_l^{i-1} Y_{[1,l-1]}^n) + n\epsilon_n \\ &\stackrel{(l)}{\leq} \sum_{l=1}^L \sum_{i=1}^n H(Y_{1li} Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n) \\ &\quad - H(Y_{1li} Y_{li} | W Y_l^{i-1} Y_{[1,l-1]}^n Y_{2[l+1]}^n Y_{2[l+1,L]}^n) \\ &\quad + n\epsilon_n \\ &= \sum_{l=1}^L \sum_{i=1}^n I(W Y_{2[l+1]}^n Y_{2[l+1,L]}^n; Y_{1li} Y_{li} | Y_l^{i-1} Y_{[1,l-1]}^n) \\ &\quad + n\epsilon_n \\ &= \sum_{l=1}^L \sum_{i=1}^n I(V_{1li}; Y_{1li} Y_{li} | V_{2li}) + n\epsilon_n. \end{aligned} \quad (31)$$

Hence, we have

$$\begin{aligned} R &\leq \frac{1}{n} \sum_{l=1}^L \sum_{i=1}^n I(V_{1li}; Y_{1li} Y_{li} | V_{2li}) + \epsilon_n \\ &\leq \sum_{l=1}^L I(V_{1l}; Y_l Y_{1l} | V_{2l}) + \epsilon_n \end{aligned} \quad (32)$$

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:

$$\bigcup \left\{ (R, R_e) \text{ that satisfy (26), (28), (30), (32)} \right\} \quad (33)$$

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 (26), (28), (30), and (32) 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

$$\prod_{l=1}^L \left[p(u_l, v_{1l}, v_{2l}) p(x_{1l}, x_{2l} | u_l, v_{1l}, v_{2l}) \cdot p(y_l, y_{1l}, y_{2l} | x_{1l}, x_{2l}) \right]. \quad (34)$$

This completes the proof of Theorem 1.

ACKNOWLEDGMENTS

This work is supported by the European Commission in the framework of the FP7 Network of Excellence in Wireless Communications. The authors would also like to thanks the concerted Action SCOOP for funding.

REFERENCES

- [1] T. Cover and A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Transactions on Information Theory*, vol. 25, no. 5, pp. 572–584, Sep. 1979.
- [2] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.
- [3] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
- [4] 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.
- [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] 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.
- [8] R. G. Gallager, *Information theory and reliable communication*. New York: Wiley, 1968.
- [9] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May. 1978.