Ergodic Secrecy Capacity Region of the Fading Broadcast Channel

Ersen Ekrem Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
ersen@umd.edu *ulukus@umd.edu*

Abstract— **We consider the fading broadcast channel from a secrecy point of view. In this channel, each user views the other user as an eavesdropper, and wants to keep its information as secret from the other user as possible. First, we consider a more general channel model which consists of L independent sub-channels, where in each sub-channel, one of the users' channel is less noisy with respect to the other user. Since the user which has the less noisy observation can be different in each sub-channel, the overall channel is not less noisy for any one of the users. We establish the secrecy capacity region of this channel for the case where the transmitter sends a common message to both users and an individual confidential message to each user. This channel model encompasses the sub-class of channels, where in each sub-channel, one of the users' observation is degraded with respect to the other user. The parallel Gaussian broadcast channel belongs to this sub-class. In the Gaussian case, we identify the optimum input distribution, which is Gaussian, and the optimum power allocation corresponding to each point on the boundary of the secrecy capacity region. Finally, noting that the fading Gaussian broadcast channel is equivalent to a parallel Gaussian broadcast channel from an ergodic capacity perspective, we explicitly evaluate the ergodic secrecy capacity region of the fading broadcast channel.**

I. Introduction

The field of information theoretic secrecy was initiated by the pioneering works of Wyner [1] and Csiszar and Korner [2] on the wiretap channel. In a wiretap channel, the transmitter wants to have confidential communication with the receiver, in the presence of a passive eavesdropper, by hiding its message as much as possible from the eavesdropper. Recently, multiuser versions of the secrecy problem have been studied for various multiuser channel models [3]–[7]. The main motivation for the multiuser extension of the wiretap channel comes from wireless communication network applications, where the inherent openness of the wireless medium allows all users in the system to over-hear all ongoing communications, raising the issue of confidentiality and multiuser secrecy. However, in order to model the multiuser wireless channel more appropriately, the other most important aspect of wireless medium needs to be considered, which is fading. Fading refers to the random, time-varying fluctuations in the channel gains.

Fading channels have been considered from a secrecy point of view in [8]–[14]. The fading wiretap channel is studied in [8]–[10] for the case where the channel state information (CSI) of both the legitimate receiver and the eavesdropper are available at all terminals, and the ergodic secrecy capacity is derived for this case. The ergodic secrecy capacity gives the amount of confidential information that the transmitter can send to the receiver, when the receiver can afford arbitrarily long delays, hence can average its secrecy rate over all channel realizations. The case where the transmitter has the CSI of only the legitimate receiver (but not the eavesdropper) is studied in [10]–[12] from the ergodic secrecy perspective. In [10], a slow-fading channel is considered and the ergodic secrecy capacity is found. The fast-fading case is investigated in [11], [12], where achievable rates are given.

Another information theoretic measure for fading channels is the outage capacity, i.e., delay-limited capacity, which refers to the the amount of information that can be transmitted within a certain time, i.e., when the receiver is delay-intolerant [15]. The concept of outage capacity is used in the context of fading wiretap channels in [9], [13], [14], where the outage probability is derived. The outage probability can be interpreted as the fraction of time that the legitimate receiver cannot get a pre-specified target secrecy rate.

In this work, we consider the *simultaneous* confidentiality of the messages of a two-user fading broadcast channel (BC). In this channel model, each receiver views the other one as an eavesdropper and wants to keep its information as confidential as possible. Hence, our work can be considered as a generalization of [8]–[10] where only one of the receivers requires confidential communication, while the other one is a pure eavesdropper, to a symmetric setting where both receivers want to have confidential communication with the receiver. Similar to [8], [9], we assume that the fading coefficients are ergodic and stationary over time, and are known to all parties (the transmitter and both receivers) perfectly and instantaneously. Generally speaking, the assumption of the availability of the eavesdropper's CSI at the transmitter may be viewed as unrealistic [8], [9], especially given the malicious and passive nature of the eavesdropper. However, in our model, where both users are active participants of the network, and both wish to receive confidential messages from the transmitter, the availability of their CSI at the transmitter (which, in turn, can broadcast this information back to the receivers, allowing all receivers to know the CSIs also) is more realistic.

This work was supported by NSF Grants CCF 04-47613, CCF 05-14846, CNS 07-16311 and CCF 07-29127.

We first consider the class of discrete two-user BCs with L sub-channels, where in each sub-channel, one of the users' observation is less noisy with respect to the other user. However, since the user which has the less noisy observation can be different in each sub-channel, the overall channel is not less noisy for any one of the users. We obtain the secrecy capacity region of this channel for the case where the transmitter sends a common message to both users and an individual confidential message to each user. Since degradedness implies less noisiness [2], this model encompasses the sub-class of channels, where in each sub-channel, one of the users' observation is degraded with respect to the other user. Similar to the less noisy case, since the user which has the degraded observation can be different in each sub-channel, the overall channel is not degraded for any one of the users. The parallel Gaussian BC, where each sub-channel is a Gaussian BC, belongs to this sub-class. Using the secrecy capacity region we found for the discrete case, we explicitly evaluate the secrecy capacity region of the parallel Gaussian BC by finding the optimal input distribution and the optimal power allocation that achieves each point on the boundary of the secrecy capacity region. This result is instrumental in finding the secrecy capacity region of the fading BC.

We then focus on the ergodic secrecy capacity region of the fading BC, where we assume that there are no delay constraints, in that, each receiver can wait arbitrarily long to decode its message; this allows the transmitted codeword to experience all possible channel realizations, and consequently, the achievable rate becomes an average of the rates achievable at all channel states. Since for a given realization of the channel gain coefficients, the fading channel is a Gaussian BC, the overall channel can be viewed as a parallel Gaussian BC where each sub-channel corresponds to a particular realization of the channel gains. Thus, the secrecy capacity we find for the parallel Gaussian BC applies to the fading BC, letting us establish the ergodic secrecy capacity region of the fading BC explicitly. We finally present some numerical results which demonstrate that fading enables both users to have positive secrecy rates which is impossible for scalar non-fading Gaussian BC.

After the inclusion of this paper into the conference program, we encountered a related work in [16]. Although the main emphasis of [16] is to analyze the secrecy and stability jointly, it obtains the secrecy capacity region of the fading BC as a side result; see Theorem 1 of [16]. The proof in [16] is quite different than ours in the sense that, our proof is obtained by using the single-letter capacity region of a generic channel model, whereas [16] uses a Sato-type outer bound for the converse, while its achievability follows from [1], [2]. Besides these differences in the proof techniques, we also provide the secrecy capacity region of a more general channel model, which may be useful in the analysis of the secrecy of the BC with memory, and the multiple-input multiple-output (MIMO) BC [17].

II. Parallel Less Noisy Broadcast Channels with Confidential Messages

We consider the class of two-user parallel BCs with L sub-channels, where in each sub-channel, one user's channel is less noisy with respect to the other user. However, the overall channel is not less noisy for any one of the users, as discussed earlier. The transmitter sends an individual confidential message to each user that needs to be kept hidden from the other user, in addition to a common message that needs to be delivered to both users.

This channel consists of one input alphabet $x = (x_1,\ldots,x_L) \in \mathcal{X} = \mathcal{X}_1 \times \ldots \times \mathcal{X}_L$ and two output alphabets $y_j = (y_{j1},\ldots,y_{jL}) \in \mathcal{Y}_j = \mathcal{Y}_{j1} \times \ldots \times \mathcal{Y}_{jL}, j = 1,2,$ where $x_\ell, \ell = 1,\ldots,L,$ is the input to the ℓth sub-channel and $y_{j\ell}, j = 1,2, \ell \in \{1,\ldots,L\}$, is the output of the jth user's ℓth sub-channel. The channel transition probability is given by

$$p(y_{11}^n, y_{21}^n, \ldots, y_{1L}^n, y_{2L}^n | x_1^n, \ldots, x_L^n) = \prod_{\ell=1}^{L}\prod_{i=1}^{n} p(y_{1\ell,i}, y_{2\ell,i}|x_{\ell,i}) \qquad (1)$$

which implies that the sub-channels are all independent and each sub-channel is memoryless. Furthermore, in each sub-channel, one user's channel is less noisy with respect to the other user, i.e., for any random variable U satisfying the Markov chain $U \rightarrow X_\ell \rightarrow (Y_{1\ell}, Y_{2\ell})$, we have [2]

$$I(U;Y_{1\ell}) > I(U;Y_{2\ell}), \quad \ell \in \mathcal{S}_1 \qquad (2)$$

$$I(U;Y_{2\ell}) > I(U;Y_{1\ell}), \quad \ell \in \mathcal{S}_2 \qquad (3)$$

where $\mathcal{S}_j$, $j = 1,2$, is the set of the sub-channel indices in which user j's channel is less noisy. We remark that as long as $\mathcal{S}_j \neq \{1,\ldots,L\}$, $j = 1,2$, the overall channel is not less noisy for any one of the users.

An $(n, 2^{nR_0}, 2^{nR_1}, 2^{nR_2})$ code for this channel consists of three message sets $\mathcal{W}_0 = \{1,\ldots,2^{nR_0}\}$, $\mathcal{W}_j = \{1,\ldots,2^{nR_j}\}, j = 1,2,$ one encoder $f : \mathcal{W}_0 \times \mathcal{W}_1 \times \mathcal{W}_2 \rightarrow \mathcal{X}_1^n \times \ldots \times \mathcal{X}_L^n$ and two decoders, one at each receiver, $g_j : \mathcal{Y}_{j1}^n \times \ldots \mathcal{Y}_{jL}^n \rightarrow \mathcal{W}_0 \times \mathcal{W}_j, j = 1,2$. The probability of error for the jth user is defined as $P_{e,j}^n = \Pr\left[(\hat{W}_0, \hat{W}_j) \neq (W_0, W_j)\right], j = 1,2,$ where $(\hat{W}_0, \hat{W}_j)$ is the output of the jth user's decoder. The secrecy of the code is measured through equivocation rates which are $\frac{1}{n}H(W_1|Y_2^n), \frac{1}{n}H(W_2|Y_1^n)$.

A rate tuple (R_0, R_1, R_2) is said to be achievable if there exist codes such that $\lim_{n\rightarrow\infty} P_{e,j}^n = 0, j = 1,2,$ and

$$\lim_{n\rightarrow\infty} \frac{1}{n}H(W_1|Y_2^n) \geq R_1, \quad \lim_{n\rightarrow\infty} \frac{1}{n}H(W_2|Y_1^n) \geq R_2 \qquad (4)$$

Thus, our focus will be on the perfect secrecy rates.

The secrecy capacity region of this channel is given by the following theorem.

Theorem 1: The secrecy capacity region of the parallel less noisy BC is given by the union of the rate tuples (R_0, R_1, R_2)

satisfying

$$R_0 \leq \min \left[\sum_{\ell=1}^{L} I(U_\ell; Y_{1\ell}), \sum_{\ell=1}^{L} I(U_\ell; Y_{2\ell}) \right] \tag{5}$$

$$R_1 \leq \sum_{\ell \in \mathcal{S}_1} \left[I(X_\ell; Y_{1\ell}|U_\ell) - I(X_\ell; Y_{2\ell}|U_\ell) \right] \tag{6}$$

$$R_2 \leq \sum_{\ell \in \mathcal{S}_2} \left[I(X_\ell; Y_{2\ell}|U_\ell) - I(X_\ell; Y_{1\ell}|U_\ell) \right] \tag{7}$$

where the union is over all distributions of the form $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$.

The proof of this theorem and the proofs of all other forthcoming results are omitted here due to space limitations.

Remark 1: The capacity achieving scheme uses all of the sub-channels to transmit the common message on which, of course, no secrecy constraint is imposed. The confidential messages of user j are sent over the sub-channels where user j has a less noisy observation with respect to the other user, i.e., over sub-channels in $\mathcal{S}_j$.

Remark 2: The region given in Theorem 1 remains unchanged if we let arbitrary correlation among $\{u_\ell, x_\ell\}_{\ell=1}^{L}$ because all of the expressions in Theorem 1 depend on one of the distributions $\{p(u_\ell, x_\ell, y_{1\ell}, y_{2\ell})\}_{\ell=1}^{L}$, but not on any joint distributions across sub-channels. Thus, the use of independent inputs for each sub-channel is capacity achieving.

We now consider a special instance of this channel, where in each sub-channel, one of the users' channel is degraded with respect to the other user. For this so-called parallel degraded BC, we have,

$$X_\ell \rightarrow Y_{1\ell} \rightarrow Y_{2\ell}, \quad \ell \in \mathcal{S}_1 \tag{8}$$

$$X_\ell \rightarrow Y_{2\ell} \rightarrow Y_{1\ell}, \quad \ell \in \mathcal{S}_2 \tag{9}$$

We note that the channels satisfying (8)-(9) satisfy (2)-(3). We also note that since the user which has degraded channel can be different in each sub-channel, the overall channel is not degraded for any one of the users. In other words, as long as $\mathcal{S}_j \neq \{1, \ldots, L\}, j = 1, 2$, the overall channel is not degraded. The secrecy capacity region of the parallel degraded BC is given as follows.

Corollary 1: The secrecy capacity region of the parallel degraded BC is given by the union of the rate tuples (R_0, R_1, R_2) satisfying

$$R_0 \leq \min \left[\sum_{\ell=1}^{L} I(U_\ell; Y_{1\ell}), \sum_{\ell=1}^{L} I(U_\ell; Y_{2\ell}) \right] \tag{10}$$

$$R_1 \leq \sum_{\ell \in \mathcal{S}_1} I(X_\ell; Y_{1\ell}|U_\ell, Y_{2\ell}) \tag{11}$$

$$R_2 \leq \sum_{\ell \in \mathcal{S}_2} I(X_\ell; Y_{2\ell}|U_\ell, Y_{1\ell}) \tag{12}$$

where the union is over all distributions of the form $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$.

We now specialize the result in Corollary 1 to the case where there is no common message to be transmitted.

Corollary 2: The secrecy capacity region of the parallel degraded BC without a common message is given by the union of the rate pairs (R_1, R_2) satisfying

$$R_1 \leq \sum_{\ell \in \mathcal{S}_1} I(X_\ell; Y_{1\ell}|Y_{2\ell}) \tag{13}$$

$$R_2 \leq \sum_{\ell \in \mathcal{S}_2} I(X_\ell; Y_{2\ell}|Y_{1\ell}) \tag{14}$$

where the union is over all distributions of the form $\prod_{\ell=1}^{L} p(x_\ell)$.

III. Parallel Gaussian Broadcast Channels

We now consider the two-user parallel Gaussian BC with L independent sub-channels. The ℓth, $\ell \in \{1, \ldots, L\}$, sub-channel is described by

$$Y_{1\ell,i} = h_{1\ell} X_{\ell,i} + N_{1\ell,i} \tag{15}$$

$$Y_{2\ell,i} = h_{2\ell} X_{\ell,i} + N_{2\ell,i} \tag{16}$$

where for any given $\ell \in \{1, \ldots, L\}$ and $j = 1, 2$, the noise process $\{N_{j\ell,i}\}_{i=1}^{n}$ has components which are i.i.d. Gaussian with zero-mean and unit-variance. Moreover, the noise processes of different sub-channels are independent implying the independence of the sub-channels. We have an average power constraint on the input signal as

$$\frac{1}{n} \sum_{i=1}^{n} \sum_{\ell=1}^{L} x_{\ell,i}^2 \leq P \tag{17}$$

We want to obtain the secrecy capacity region of this channel. To this end, we first show that the parallel Gaussian BC is an instance of the parallel degraded BC described in the previous section in Corollaries 1 and 2. To see this point, we argue that the secrecy capacity region of the parallel Gaussian BC is invariant with respect to the correlation between $N_{1\ell,i}$ and $N_{2\ell,i}$. Since each user decodes its own message and gets information about the other user's message only through its own observation, the only probability distribution that matters is the marginal distribution of the channel, i.e., $p(y_{1\ell,i}|x_{\ell,i})$ and $p(y_{2\ell,i}|x_{\ell,i})$, but not the joint distribution $p(y_{1\ell,i}, y_{2\ell,i}|x_{\ell,i})$. Hence, the correlation between $N_{1\ell,i}$ and $N_{2\ell,i}$ for any given ℓ has no effect on the secrecy capacity region of the parallel Gaussian BC [9]. Therefore, we can introduce an equivalent Gaussian channel which is defined for $\ell \in \mathcal{S}_1$ by

$$Y_{1\ell,i} = h_{1\ell} X_{\ell,i} + N_{1\ell,i}, \quad \tilde{Y}_{2\ell,i} = \frac{h_{2\ell}}{h_{1\ell}} Y_{1\ell,i} + \tilde{N}_{2\ell,i} \tag{18}$$

and for $\ell \in \mathcal{S}_2$ by

$$Y_{2\ell,i} = h_{2\ell} X_{\ell,i} + N_{2\ell,i} \quad \tilde{Y}_{1\ell,i} = \frac{h_{1\ell}}{h_{2\ell}} Y_{2\ell,i} + \tilde{N}_{1\ell,i} \tag{19}$$

where the sets $\mathcal{S}_1$ and $\mathcal{S}_2$ are given by

$$\mathcal{S}_1 = \{\ell : h_{1\ell} > h_{2\ell}\}, \quad \mathcal{S}_2 = \{\ell : h_{2\ell} > h_{1\ell}\} \tag{20}$$

and $\tilde{N}_{1\ell,i}$, $\tilde{N}_{2\ell,i}$ are Gaussian with zero-mean and variances $1 - (h_{1\ell}/h_{2\ell})^2$, $1 - (h_{2\ell}/h_{1\ell})^2$, respectively, and they are independent of each other and the rest of the random variables.

Since the channel described by (18)-(19) satisfies the degradedness conditions in (8)-(9), it is a parallel degraded BC. Thus, the secrecy capacity region of the parallel Gaussian BC is given by Corollaries 1 and 2. Moreover, since the channels described by (15)-(16) and (18)-(19) have the same marginal distributions, they have the same secrecy capacity region.

Theorem 2: The secrecy capacity region of the parallel Gaussian BC is given by the union of the rate pairs (R_1, R_2) satisfying

$$R_1 \leq \frac{1}{2} \sum_{\ell \in \mathcal{S}_1} \left[\log(1+\alpha_{1\ell} h_{1\ell}^2) - \log(1+\alpha_{1\ell} h_{2\ell}^2) \right] \tag{21}$$

$$R_2 \leq \frac{1}{2} \sum_{\ell \in \mathcal{S}_2} \left[\log(1+\alpha_{2\ell} h_{2\ell}^2) - \log(1+\alpha_{2\ell} h_{1\ell}^2) \right] \tag{22}$$

where the union is over all $\beta \in [0,1]$, and $\{\alpha_{j\ell}\}_{\ell \in \mathcal{S}_j}, j = 1,2$, are defined by

$$\alpha_{1\ell} = \left[-\frac{1}{2}\left(\frac{1}{h_{1\ell}^2} + \frac{1}{h_{2\ell}^2}\right) + \frac{1}{2}\sqrt{\left(\frac{1}{h_{1\ell}^2} - \frac{1}{h_{2\ell}^2}\right)^2 + \frac{2P}{\lambda_1}\left(\frac{1}{h_{2\ell}^2} - \frac{1}{h_{1\ell}^2}\right)} \right]^+ \tag{23}$$

$$\alpha_{2\ell} = \left[-\frac{1}{2}\left(\frac{1}{h_{1\ell}^2} + \frac{1}{h_{2\ell}^2}\right) + \frac{1}{2}\sqrt{\left(\frac{1}{h_{1\ell}^2} - \frac{1}{h_{2\ell}^2}\right)^2 + \frac{2P}{\lambda_2}\left(\frac{1}{h_{1\ell}^2} - \frac{1}{h_{2\ell}^2}\right)} \right]^+ \tag{24}$$

where $(x)^+ = \max(0,x)$, and λ_1, λ_2 are selected to satisfy

$$\sum_{\ell \in \mathcal{S}_1} \alpha_{1\ell} = \beta P, \qquad \sum_{\ell \in \mathcal{S}_2} \alpha_{2\ell} = (1-\beta)P \tag{25}$$

Remark 3: If we set one of the users' secrecy rate to zero, we can recover the secrecy capacity of the parallel Gaussian wiretap channel found in [8], [9].

The proof of this theorem consists of two steps. In the first step, we identify the input distribution maximizing the terms in Corollary 2, which is Gaussian [18]. Secondly, we compute the optimal power allocation to obtain the boundary of the capacity region. The resulting optimal power allocation scheme is reminiscent of the water-filling solution, however, here we use the difference of the noise levels in each subchannel, as the "base of the tank" on which we water-fill. More precisely, the water-filling solution here considers the difference

$$\left| \frac{1}{h_{1\ell}^2} - \frac{1}{h_{2\ell}^2} \right| \tag{26}$$

which can be viewed as the difference between the effective noise levels of the two users in sub-channel ℓ, because $h_{j\ell}^2$ is the signal-to-noise ratio of the jth user in the ℓth sub-channel. Consequently, if this difference is sufficiently large, then the corresponding sub-channel is used, otherwise it is not used.

IV. Ergodic Secrecy Capacity Region of the Fading Broadcast Channel

We now consider the fading BC which is given by

$$Y_{1,i} = h_{1,i} X_i + N_{1,i} \tag{27}$$

$$Y_{2,i} = h_{2,i} X_i + N_{2,i} \tag{28}$$

where $\{N_{j,i}\}_{i=1}^n,\ j = 1,2$, is an i.i.d. Gaussian random sequence with zero-mean and unit-variance. We assume that the fading processes $\{h_{j,i}\}_{i=1}^n,\ j = 1,2$, are ergodic and stationary. We have the power constraint on the channel input as $(1/n)\sum_{i=1}^n x_i^2 \leq P$. The joint cumulative probability distribution of $(h_{1,i}, h_{2,i})$ is denoted by $F(\mathbf{h})$.

We want to obtain the secrecy capacity region of this fading BC. We assume that CSI of both users $\mathbf{h}_i = (h_{1,i}, h_{2,i})$ is instantaneously known by all parties. We further assume that none of the users has a delay constraint on the transmission, thus the notion of ergodic capacity can be used. To find the corresponding secrecy capacity region, we invoke the equivalence of the fading BC channel with the parallel Gaussian BC which was studied in Section III. Thus, we use the secrecy capacity region of the parallel Gaussian BC given in Theorem 2 to obtain the ergodic secrecy capacity of the fading BC.

Corollary 3: The ergodic secrecy capacity region of the fading BC is given by the union of the rate pairs (R_1, R_2) satisfying

$$R_1 \leq \frac{1}{2}\int_{\mathcal{H}_1} \left[\log\left(1+\alpha_1(\mathbf{h})h_1^2\right) - \log\left(1+\alpha_1(\mathbf{h})h_2^2\right) \right] dF(\mathbf{h}) \tag{29}$$

$$R_2 \leq \frac{1}{2}\int_{\mathcal{H}_2} \left[\log\left(1+\alpha_2(\mathbf{h})h_2^2\right) - \log\left(1+\alpha_2(\mathbf{h})h_1^2\right) \right] dF(\mathbf{h}) \tag{30}$$

where the union is over all $\beta \in [0,1]$, and the regions $\mathcal{H}_1, \mathcal{H}_2$ are defined by

$$\mathcal{H}_1 = \{\mathbf{h} : h_1 > h_2\}, \quad \mathcal{H}_2 = \{\mathbf{h} : h_2 > h_1\} \tag{31}$$

Here, $\{\alpha_j(\mathbf{h})\}_{j=1}^2$ are also given by (23)-(24) and λ_1, λ_2 are selected to satisfy

$$\int_{\mathcal{H}_1} \alpha_1(\mathbf{h}) dF(\mathbf{h}) = \beta P, \quad \int_{\mathcal{H}_2} \alpha_2(\mathbf{h}) dF(\mathbf{h}) = (1-\beta)P \tag{32}$$

Remark 4: If we set one of the users' secrecy rate to zero, we can recover the ergodic secrecy capacity of the fading wiretap channel found in [8], [9].

Remark 5: We only assumed that the fading processes $\{h_{j,i}\}_{i=1}^n,\ j = 1,2$, are ergodic and stationary, and did not impose any restrictions on the correlation structure. Consequently, Corollary 3 gives the secrecy capacity region for any ergodic and stationary fading process.

This corollary is a direct consequence of Theorem 2. To adopt the corresponding result, we need to identify the channel states which are equivalent to the sub-channels of a parallel Gaussian BC. Thus, we define the sets $\mathcal{H}_j, j = 1,2$, which are similar to $\mathcal{S}_j, j = 1,2$. Consequently, when the first (resp. second) user has a stronger channel in the sense that $h_1 > h_2$ (resp. $h_2 > h_1$), first (resp. second) user's confidential message is transmitted. Moreover, using Theorem 2, we also obtain the optimal power allocations $\alpha_1(\mathbf{h})$ and $\alpha_2(\mathbf{h})$ that give the boundary of the secrecy capacity region.

V. Numerical Results

We now present some numerical illustrations for the ergodic secrecy capacity region. We select h_1, h_2 to be independent Rayleigh random variables. Consequently, the powers of the channel gains, i.e., h_1^2 and h_2^2, are exponential random variables with mean values σ_1 and σ_2, respectively. The difference between these mean values can be viewed as a measure of the relative strengths of the users' channels on average. Thus, we expect that the user that has a larger mean value would have larger secrecy rates. In Figure 1, ergodic secrecy capacity region is given for two different sets of $\{\sigma_1, \sigma_2\}$. For the first set, we have $\sigma_1 = \sigma_2 = 1$ which results in a symmetric ergodic secrecy capacity region. For the second set, we select $\sigma_1 = 1, \sigma_2 = 0.5$. Since user 2's average signal-to-noise ratio is lower in this case, the maximum secrecy rate of user 1 is larger while the maximum secrecy rate of user 2 is lower.

To observe the effect of optimal power allocation, we compute the achievable secrecy region obtained by using a uniform power allocation, i.e., $\alpha_1(\mathbf{h})$ (resp. $\alpha_2(\mathbf{h})$) is selected to be constant over $\mathcal{H}_1$ (resp. $\mathcal{H}_2$). The corresponding plot is given in Figure 2. We note that the optimal power allocation offers a significant advantage over the suboptimal uniform power allocation. This also implies that the availability of the CSI at the transmitter results in a noticeable secrecy rate gain.

VI. Conclusions

We considered the two-user fading BC from a secrecy point of view. We first obtained the secrecy capacity region of a general parallel channel, where in each one of the L sub-channels, one of the users is less noisy with respect to the other user. This model subsumes the sub-class of parallel BCs, where in each sub-channel, one of the users has a degraded channel with respect to the other user. The parallel Gaussian BC belongs to this sub-class. For the parallel Gaussian BC, we evaluated the secrecy capacity region. Finally, using the similarity between the parallel Gaussian BC and the fading BC, we established the ergodic secrecy capacity region of the fading BC.

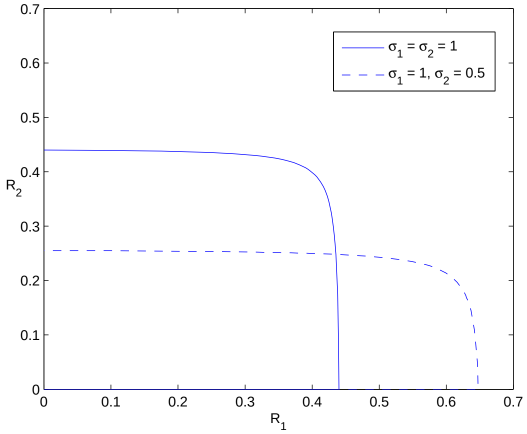

Fig. 1. Ergodic secrecy capacity region for different mean values of the fading distribution. The average power, P, is 5 dB.

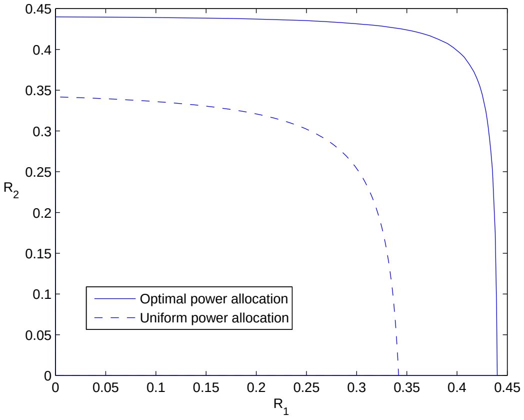

Fig. 2. Comparison of the ergodic secrecy capacity region and an achievable secrecy region obtained by using a uniform power allocation. The average power, P, is 5 dB.

References

[1] A. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, Jan. 1975.

[2] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, IT-24(3):339–348, May 1978.

[3] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory*, 54(12):5747–5755, Dec. 2008.

[4] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inf. Theory*, 54(6):2493–2507, Jun. 2008.

[5] Y. Oohama. Relay channels with confidential messages. Submitted to *IEEE Trans. Inf. Theory*. Also available at [arXiv:0611125].

[6] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory*, 54(9):4005–4019, Sep. 2008.

[7] Y. Liang and H. V. Poor. Generalized multiple access channels with confidential messages. *IEEE Trans. Inf. Theory*, 54(3):976–1002, Mar. 2008.

[8] Z. Li, R. Yates, and W. Trappe. Secrecy capacity of independent parallel channels. In *44th Annual Allerton Conf. Commun., Contr. and Comput.*, pages 841–848, Sep. 2006.

[9] Y. Liang, H. V. Poor, and S. Shamai. Secure communication over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2470 – 2492, Jun. 2008.

[10] P. Gopala, L. Lai, and H. El Gamal. On the secrecy capacity of fading channels. *IEEE Trans. Inf. Theory*, 54(10):4687–4698, Oct. 2008.

[11] Z. Li, R. Yates, and W. Trappe. Secret communication with a fading eavesdropper channel. In *IEEE ISIT*, pages 1296 – 1300, Jun. 2007.

[12] A. Khisti, A. Tchamkerten, and G. W. Wornell. Secure broadcasting over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2453–2469, Jun. 2008.

[13] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin. Wireless information-theoretic secrecy. *IEEE Trans. Inf. Theory*, 54(6):2515–2534, Jun. 2008.

[14] P. Parada and R. Blahut. Secrecy capacity of SIMO and slow fading channels. In *IEEE ISIT*, pages 2152–2155, Sep. 2005.

[15] G. Caire, G. Taricco, and E. Biglieri. Optimal power control over fading channels. *IEEE Trans. Inf. Theory*, 45(5):1468–1489, Jul. 1999.

[16] Y. Liang, H. V. Poor, and L. Ying. Wireless broadcast networks: reliability, security and stability. In *3rd Information Theory and Applications Workshop*, Jan. 2008.

[17] R. Liu and H. V. Poor. Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages. *IEEE Trans. Inf. Theory*, 55(3):1235–1249, Mar. 2009.

[18] S. K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, Jul. 1978.