ISIT'2013 1569720109

Capacity Bounds for Wireless Ergodic Fading Broadcast Channels with Partial CSIT

Reza K. Farsani
School of Cognitive Sciences, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran
Email: reza_khosravi@alum.sharif.ir

***Abstract*—The two-user wireless ergodic fading Broadcast Channel (BC) with partial Channel State Information at the Transmitter (CSIT) is considered. The CSIT is given by an arbitrary deterministic function of the channel state. This characteristic yields a full control over how much state information is available, from perfect to no information. A novel approach is developed to adapt and explicitly evaluate the well-known UV-outer bound for the Gaussian fading channel using the entropy power inequality. Our approach indeed sheds light on the role of broadcast auxiliaries in the fading channel. It is shown that the derived outer bound is optimal for the channel with perfect CSIT. Our bounds are also directly applicable to the case without CSIT which has been recently considered in several papers. Next, the approach is developed to analyze for the fading BC with secrecy. In the case of perfect CSIT, a full characterization of the secrecy capacity region is derived for the channel with common and confidential messages. This result completes a gap in a previous work by Ekrem and Ulukus. For the channel without common message, the secrecy capacity region is also derived when the transmitter has access only to degradedness ordering of the channel.**

I. Introduction

For the wireless ergodic fading BC the capacity region is only known when perfect channel state information is available at both the transmitter and the receivers [1]. In this paper, we consider the two-user fading BC with partial CSIT where the CSIT is given by an arbitrary deterministic function of channel state. The main benefit of such a model for CSIT is that it provides a full control over how much state information is available from perfect to no information. In literature capacity derivations for wireless ergodic channels, specifically for fading BCs, mostly rely on the analysis of channels comprising of parallel sub-channels [1-8]. By this approach the ergodic capacity region was established in [1-6] for different multi-user fading channels with perfect CSIT. In fact, this technique that fading channels are treated based on parallel channels is usually suitable for the cases where perfect state information is available at the transmitters. Moreover, it is no more applicable for analyzing scenarios such as fading interference channels that are not separable into parallel sub-channels [9-10]. In this paper, we present novel arguments to directly derive (without resorting to the analysis of parallel channels) capacity bounds for the two-user fading BC with partial CSIT with both common and private messages based on the existing bounds for the discrete channel. First, we propose a capacity inner bound for the channel by choosing an appropriate signaling scheme for the Marton's achievable rate region. We then establish an outer bound on the capacity region. We remark that one of the main challenges in analyzing the fading BC is to establish a capacity outer bound with satisfactory performance. Specifically, it has been a main focus in all the papers [11-16]. The reason is that capacity outer bounds for the BC typically include some auxiliary random variables and for the Gaussian fading channel (unlike the Gaussian channel with fixed channel gains) a naive application of the Entropy Power Inequality (EPI) fails to optimize over these auxiliaries. In [15], the authors indicate that conventional EPI is not directly applicable for analyzing the fading BC without CSIT and make use of Costa's EPI for this purpose. Also, the outer bound given in [13] for the same channel is derived using a channel enhancement technique (which creates a degraded channel) and then the relations between mutual information and minimum mean square error [17] are used to optimize over its auxiliary random variable (whose role is less clear in the Gaussian fading channel [16, Conclusion]). Nonetheless, in this paper, we develop a novel and rather simple approach to adapt and evaluate the well-known UV-outer bound [18] for the Gaussian fading BC using the EPI. Our approach indeed sheds light on the role of broadcast auxiliaries in the fading channel. We next prove that our inner and outer bounds coincide for the channel with perfect CSIT. In the special case of the fading BC without common message, the result of [1] is thus recovered with a new and concise proof. Our bounds are directly applicable to the channel without CSIT, as well.

Also, we develop our approach to analyze for the wireless ergodic fading BC with secrecy. In this scenario, a transmitter sends a common message and also two private messages to two receivers and wishes to keep each private message as secret as possible from the non-legitimate receiver. Special cases of this system have been previously considered in [2-5]. The derivations of all these papers rely on the analysis of fading channels using parallel channels. Also, all of them consider the fading channel with perfect CSIT. In this paper, we establish inner and outer bounds on the secrecy capacity region of the ergodic fading BC with partial CSIT for the general case where a common message and two confidential messages are transmitted. A key step in our analysis is to derive the outer bound. For this purpose, the outer bound established in [19] for the capacity-equivocation region of the discrete BC is exploited. We adapt this outer bound for the secrecy capacity region of the fading channel first and then optimize it over its auxiliary random variables using novel techniques. In the case of perfect CSIT, our inner and outer bounds coincide with each other, thus establishing a full characterization of the secrecy capacity region for the channel with both common and confidential messages. This result include all the ones derived in [2-5] as special cases. A gap in a previous work by Ekrem and Ulukus [4] is also completed. Clearly, in [4] Ekrem and Ulukus could find the secrecy capacity region of the parallel degraded BCs [4, Corollary 1] with both common and confidential messages, however, for the Gaussian fading channel the secrecy capacity region is given only for the channel without common message (in other words, for the Gaussian fading BC with both common and confidential messages the secrecy capacity region remains unresolved in [4]). For the channel without common message, we also establish the secrecy capacity region when the transmitter has access only to the degradedness ordering of the channel which is a more realistic assumption than perfect CSIT.

In the following section, we present preliminaries and channel model definitions. Our main results are given in Section III.

II. Preliminaries and Definitions

In this paper, the following notations are used: $\mathbb{E}[.]$ indicates the expectation operator. The set of complex numbers, real numbers, and nonnegative real numbers are denoted by $\mathbb{C}, \mathbb{R}$, and $\mathbb{R}_+$, respectively. Given a statement F, the indicator function $\mathbb{1}(F)$ is equal to one if F is true and zero otherwise. Finally, the function $\psi(x)$ is defined as: $\psi(x) \equiv \log(1+x)$, for $x \in \mathbb{R}_+$.

The Gaussian fading BC is described by the following:

$$\begin{cases} Y_{1,t} = S_{1,t}X_t + Z_{1,t} \\ Y_{2,t} = S_{2,t}X_t + Z_{2,t} \end{cases}, \qquad t \geq 1 \tag{1}$$

The sequence $\{X_t\}_{t\geq 1}$ represents complex-valued transmitted signals by the transmitter, and $\{Y_{1,t}\}_{t\geq 1}$ and $\{Y_{2,t}\}_{t\geq 1}$ represent the received signals at the first and the second receivers, respectively.

The sequences $\{Z_{1,t}\}_{t\geq 1}$ and $\{Z_{2,t}\}_{t\geq 1}$ denote additive noises each of which is an i.i.d. complex Gaussian random process with zero mean and unit variance. The state process of the channel is denoted by $\{\boldsymbol{S}_t = (S_{1,t}, S_{2,t})\}_{t\geq 1}$ where the components $S_{1,t}$ and $S_{2,t}$ are complex-valued fading coefficients at the time instant t. In general, we assume that the state process of the channel is a stationary and ergodic random process which varies in time according to any arbitrary (known) probability distribution. We consider a scenario wherein both receivers perfectly know the state information while the transmitter has access to it partially. The partial side information at each transmitter is given by a deterministic function of the channel state. Specifically, the transmitter is equipped with a deterministic function $\xi(.)$ given as follows:

$$\xi(.): \mathbb{C}^2 \to \mathcal{E}$$

where $\mathcal{E}$ is an arbitrary (potentially finite) set. At each time instant $t, t \geq 1$, the transmitter is informed of $E_t = \xi(\boldsymbol{S}_t)$ where $\boldsymbol{S}_t$ is the current state of the channel. The transmitter is subject to a power constraint: $\mathbb{E}[|X|^2] \leq P$. The details of the encoding and decoding schemes can be found in [21]. The capacity region and also the secrecy capacity region are defined as usual. By these preliminaries, we are ready to state our main results.

III. Main Results

III.A) Fading BC without Secrecy

We begin by presenting a capacity inner bound for the channel. Note that in the following analysis, the random variable $\boldsymbol{S} = (S_1, S_2) \in \mathbb{C}^2$ with a given distribution $P_{\boldsymbol{S}}(\boldsymbol{s})$ represents the channel state**,** and $E = \xi(\boldsymbol{S})$ represents the partial side information at the transmitter.

Proposition 1) *Define the rate region $\mathfrak{R}_i^{GFBC}$ as given in (3), where $\varphi(.): \mathcal{E} \to \mathbb{R}_+$ is a power allocation policy function for the transmitter with $\mathbb{E}[\varphi(E)] \leq P$ and also $\alpha(.): \mathcal{E} \to [0,1]$ and $\beta(.): \mathcal{E} \to [0,1]$ are two arbitrary deterministic functions with $\alpha(e) + \beta(e) \leq 1$ for all $e \in \mathcal{E}$. The set $\mathfrak{R}_i^{GFBC}$ constitutes an inner bound on the capacity region of the two-user Gaussian fading BC (1) with common message.*

The inner bound (3) is derived by choosing an appropriate signaling scheme for the Marton's achievable rate region [22]. The details of the derivation are given in [21, Prop. 1].

We next establish a capacity outer bound for the channel. For this purpose, we first adapt the UV-outer bound [18] to be applicable for the Gaussian fading channel (1) with stationary state process. The resultant bound is given by (See [21, Lemma 2]):

$$\bigcup_{\substack{P_{X|E}P_{UV|XS} \\ \mathbb{E}[|X|^2]\leq P}} \left\{ \begin{array}{l} (R_0, R_1, R_2) \in \mathbb{R}_+^3 : \\ R_0 + R_1 \leq I(U; Y_1|\boldsymbol{S}) \\ R_0 + R_2 \leq I(V; Y_2|\boldsymbol{S}) \\ R_0 + R_1 + R_2 \leq I(X; Y_1|V, \boldsymbol{S}) + I(V; Y_2|\boldsymbol{S}) \\ R_0 + R_1 + R_2 \leq I(X; Y_2|U, \boldsymbol{S}) + I(U; Y_1|\boldsymbol{S}) \end{array} \right\} \tag{2}$$

Then, we explicitly evaluate the bound (2) by a novel approach. This is given in the following Theorem.

Theorem 1) *Consider the two-user Gaussian fading BC (1) with common message. Define the rate region $\mathfrak{R}_o^{GFBC}$ as in (4), where $\alpha(.): \mathbb{C}^2 \to [0,1]$ and $\beta(.): \mathbb{C}^2 \to [0,1]$ are arbitrary deterministic functions; also, $\varphi(.): \mathcal{E} \to \mathbb{R}_+$ with $\mathbb{E}[\varphi(E)] \leq P$ denotes the power allocation policy for the transmitter. The set $\mathfrak{R}_o^{GFBC}$ constitutes an outer bound on the capacity region.*

Proof of Theorem 1) To derive the outer bound (4), we optimize the rate region (2) for all joint PDFs $P_{X|E}(x|e)P_{UV|XS}(u, v|x, \boldsymbol{s})$ with $\mathbb{E}[|X|^2] \leq P$. In [21], we have indicated a previous unsuccessful effort [23, 24] to solve a similar optimization problem, although for the special case with no CSIT and i.i.d. state process. It has been also remarked in [15] that the conventional EPI is not directly applicable for the fading BC. Nevertheless, in what follows we present novel arguments based on which the outer bound (2) can be still evaluated using the EPI, not only for the special case with no CSIT and i.i.d. state process but also for the general channel with any arbitrary CSIT and stationary state process.

$$\mathfrak{R}_i^{GFBC} \triangleq \bigcup_{\substack{\alpha(.),\beta(.) \\ \varphi(.)}} \left\{ \begin{array}{l} (R_0, R_1, R_2) \in \mathbb{R}_+^3 : \\ R_0 + R_1 \leq \mathbb{E}\left[\psi\left(\dfrac{|S_1|^2\big(1-\alpha(E)\big)\varphi(E)}{|S_1|^2\alpha(E)\varphi(E)+1}\right)\right], \\ R_0 + R_2 \leq \mathbb{E}\left[\psi\left(\dfrac{|S_2|^2\big(1-\beta(E)\big)\varphi(E)}{|S_2|^2\beta(E)\varphi(E)+1}\right)\right], \\ R_0 + R_1 + R_2 \leq \mathbb{E}\left[\psi\left(\dfrac{|S_1|^2\beta(E)\varphi(E)}{|S_1|^2\alpha(E)\varphi(E)+1}\right)\right] + \mathbb{E}\left[\psi\left(\dfrac{|S_2|^2\big(1-\beta(E)\big)\varphi(E)}{|S_2|^2\beta(E)\varphi(E)+1}\right)\right], \\ R_0 + R_1 + R_2 \leq \mathbb{E}\left[\psi\left(\dfrac{|S_1|^2\big(1-\alpha(E)\big)\varphi(E)}{|S_1|^2\alpha(E)\varphi(E)+1}\right)\right] + \mathbb{E}\left[\psi\left(\dfrac{|S_2|^2\alpha(E)\varphi(E)}{|S_2|^2\beta(E)\varphi(E)+1}\right)\right] \end{array} \right\} \tag{3}$$

$$\mathfrak{R}_o^{GFBC} \triangleq \bigcup_{\substack{\alpha(.),\beta(.) \\ \varphi(.)}} \left\{ \begin{array}{l} (R_0, R_1, R_2) \in \mathbb{R}_+^3 : \\ R_0 + R_1 \leq \mathbb{E}\left[\psi\left(\dfrac{|S_1|^2\big(1-\alpha(\boldsymbol{S})\big)\varphi(E)\mathbb{1}(|S_1|<|S_2|)}{|S_1|^2\alpha(\boldsymbol{S})\varphi(E)+1}\right)\right] + \mathbb{E}\big[\psi\big(|S_1|^2\varphi(E)\mathbb{1}(|S_1|\geq|S_2|)\big)\big], \\ R_0 + R_2 \leq \mathbb{E}\left[\psi\left(\dfrac{|S_2|^2\big(1-\beta(\boldsymbol{S})\big)\varphi(E)\mathbb{1}(|S_2|<|S_1|)}{|S_2|^2\beta(\boldsymbol{S})\varphi(E)+1}\right)\right] + \mathbb{E}\big[\psi\big(|S_2|^2\varphi(E)\mathbb{1}(|S_2|\geq|S_1|)\big)\big], \\ R_0 + R_1 + R_2 \leq \mathbb{E}\left[\psi\big(|S_1|^2\beta(\boldsymbol{S})\varphi(E)\mathbb{1}(|S_2|<|S_1|)\big) + \psi\left(\dfrac{|S_2|^2\big(1-\beta(\boldsymbol{S})\big)\varphi(E)\mathbb{1}(|S_2|<|S_1|)}{|S_2|^2\beta(\boldsymbol{S})\varphi(E)+1}\right)\right] \\ \qquad + \mathbb{E}\big[\psi\big(|S_2|^2\varphi(E)\mathbb{1}(|S_2|\geq|S_1|)\big)\big], \\ R_0 + R_1 + R_2 \leq \mathbb{E}\left[\psi\big(|S_2|^2\alpha(\boldsymbol{S})\varphi(E)\mathbb{1}(|S_1|<|S_2|)\big) + \psi\left(\dfrac{|S_1|^2\big(1-\alpha(\boldsymbol{S})\big)\varphi(E)\mathbb{1}(|S_1|<|S_2|)}{|S_1|^2\alpha(\boldsymbol{S})\varphi(E)+1}\right)\right] \\ \qquad + \mathbb{E}\big[\psi\big(|S_1|^2\varphi(E)\mathbb{1}(|S_1|\geq|S_2|)\big)\big] \end{array} \right\} \tag{4}$$

Note that it is only required to evaluate 1^{th} and 4^{th} constraints of (2) because the two other ones can be evaluated symmetrically. Fix a joint PDF $P_{X|E}(x|e)P_{UV|XS}(u,v|x,\boldsymbol{s})$ with $\mathbb{E}[|X|^2] \le P$. Define the deterministic function $\varphi(.)$ as follows:

$$\varphi(.): \mathcal{E} \to \mathbb{R}_+, \qquad \varphi(e) \triangleq \mathbb{E}[|X|^2|E=e] \tag{5}$$

Thereby, we have: $\mathbb{E}[\varphi(E)] \le P$. For 1^{th} and 4^{th} constraints of (2), one can write:

$$I(U;Y_1|\boldsymbol{S}) = \int_{|S_1|<|S_2|} P_{\boldsymbol{S}}(\boldsymbol{s}) I(U;Y_1|\boldsymbol{s}) + \int_{|S_1|\ge|S_2|} P_{\boldsymbol{S}}(\boldsymbol{s}) I(U;Y_1|\boldsymbol{s}) \tag{6}$$

$$\begin{aligned} &I(X;Y_2|U,\boldsymbol{S}) + I(U;Y_1|\boldsymbol{S}) \\ &\quad = \int_{|S_1|<|S_2|} P_{\boldsymbol{S}}(\boldsymbol{s})\big(I(X;Y_2|U,\boldsymbol{s}) + I(U;Y_1|\boldsymbol{s})\big) \\ &\qquad + \int_{|S_1|\ge|S_2|} P_{\boldsymbol{S}}(\boldsymbol{s})\big(I(X;Y_2|U,\boldsymbol{s}) + I(U;Y_1|\boldsymbol{s})\big) \end{aligned} \tag{7}$$

Consider the first integrals in (6) and (7). Let $\boldsymbol{s} \in \{|S_1| < |S_2|\}$. Let also $\tilde{Z}_1$ be a Gaussian virtual noise, independent of Z_1 and Z_2, with zero mean and unit variance. We have:

$$\begin{aligned} I(U;Y_1|\boldsymbol{s}) &= I\left(U; \tfrac{s_1}{s_2}Y_2 + \sqrt{1-\left|\tfrac{s_1}{s_2}\right|^2}\tilde{Z}_1 \middle| \boldsymbol{s}\right) \\ &= H\left(s_1X + \tfrac{s_1}{s_2}Z_2 + \sqrt{1-\left|\tfrac{s_1}{s_2}\right|^2}\tilde{Z}_1 \middle| \boldsymbol{s}\right) \\ &\qquad - H\left(\tfrac{s_1}{s_2}Y_2 + \sqrt{1-\left|\tfrac{s_1}{s_2}\right|^2}\tilde{Z}_1 \middle| U,\boldsymbol{s}\right) \\ &\overset{(a)}{\le} \log \pi e(|s_1|^2\mathbb{E}[|X|^2|E=e]+1) \\ &\qquad - H\left(\tfrac{s_1}{s_2}Y_2 + \sqrt{1-\left|\tfrac{s_1}{s_2}\right|^2}\tilde{Z}_1 \middle| U,\boldsymbol{s}\right) \\ &= \log \pi e(|s_1|^2\varphi(e)+1) - H\left(\tfrac{s_1}{s_2}Y_2 + \sqrt{1-\left|\tfrac{s_1}{s_2}\right|^2}\tilde{Z}_1 \middle| U,\boldsymbol{s}\right) \end{aligned} \tag{8}$$

where (a) is due to the "Gaussian maximizes the entropy" principle. Also,

$$\begin{aligned} &I(X;Y_2|U,\boldsymbol{s}) + I(U;Y_1|\boldsymbol{s}) \\ &\quad = H(Y_2|U,\boldsymbol{s}) - H(s_2X+Z_2|X,U,\boldsymbol{s}) + I(U;Y_1|\boldsymbol{s}) \\ &\quad \le H(Y_2|U,\boldsymbol{s}) - \log \pi e + \log \pi e(|s_1|^2\varphi(e)+1) \\ &\qquad - H\left(\tfrac{s_1}{s_2}Y_2 + \sqrt{1-\left|\tfrac{s_1}{s_2}\right|^2}\tilde{Z}_1 \middle| U,\boldsymbol{s}\right) \end{aligned} \tag{9}$$

Now let evaluate the term $H(Y_2|U,\boldsymbol{s}) = H(s_2X+Z_2|U,\boldsymbol{s})$ in (9). We have:

$$\begin{aligned} \log \pi e = H(Z_2) &\le H(Y_2|U,\boldsymbol{s}) = H(s_2X+Z_2|U,\boldsymbol{s}) \\ &\le H(s_2X+Z_2|\boldsymbol{s}) \le \log \pi e(|s_2|^2\varphi(e)+1) \end{aligned} \tag{10}$$

The two sides of (10) imply that there exist $0 \le \alpha(\boldsymbol{s}) \le 1$ so that:

$$H(Y_2|U,\boldsymbol{s}) = H(s_2X+Z_2|U,\boldsymbol{s}) = \log \pi e(|s_2|^2\alpha(\boldsymbol{s})\varphi(e)+1) \tag{11}$$

Then, we bound the term $H(Y_1|U,\boldsymbol{s}) = H\left(\tfrac{s_1}{s_2}Y_2 + \sqrt{1-\left|\tfrac{s_1}{s_2}\right|^2}\tilde{Z}_1 \middle| U,\boldsymbol{s}\right)$ in (8) and (9) as follows:

$$\begin{aligned} H(Y_1|U,\boldsymbol{s}) &= H\left(\tfrac{s_1}{s_2}Y_2 + \sqrt{1-\left|\tfrac{s_1}{s_2}\right|^2}\tilde{Z}_1 \middle| U,\boldsymbol{s}\right) \\ &\overset{(a)}{\ge} \log\left(2^{H\left(\frac{s_1}{s_2}Y_2|U,\boldsymbol{s}\right)} + 2^{H\left(\sqrt{1-\left|\frac{s_1}{s_2}\right|^2}\tilde{Z}_1 \middle| U,\boldsymbol{s}\right)}\right) \\ &= \log\left(\tfrac{|s_1|^2}{|s_2|^2}2^{H(Y_2|U,\boldsymbol{s})} + \pi e\left(1-\tfrac{|s_1|^2}{|s_2|^2}\right)\right) \\ &\overset{(b)}{=} \log \pi e(|s_1|^2\alpha(\boldsymbol{s})\varphi(e)+1) \end{aligned} \tag{12}$$

where (a) is due to the EPI and (b) is derived by (11). Therefore, from (8-12) we obtain:

$$\begin{aligned} &\int_{|S_1|<|S_2|} P_{\boldsymbol{S}}(\boldsymbol{s}) I(U;Y_1|\boldsymbol{s}) \\ &\quad \le \mathbb{E}\left[\psi\left(\frac{|S_1|^2\big(1-\alpha(\boldsymbol{S})\big)\varphi(E)\mathbb{1}(|S_1|<|S_2|)}{|S_1|^2\alpha(\boldsymbol{S})\varphi(E)+1}\right)\right] \end{aligned} \tag{13}$$

$$\begin{aligned} &\int_{|S_1|<|S_2|} P_{\boldsymbol{S}}(\boldsymbol{s})\big(I(X;Y_2|U,\boldsymbol{s}) + I(U;Y_1|\boldsymbol{s})\big) \\ &\quad \le \mathbb{E}\big[\psi\big(|S_2|^2\alpha(\boldsymbol{S})\varphi(E)\mathbb{1}(|S_1|<|S_2|)\big)\big] \\ &\qquad + \mathbb{E}\left[\psi\left(\frac{|S_1|^2\big(1-\alpha(\boldsymbol{S})\big)\varphi(E)\mathbb{1}(|S_1|<|S_2|)}{|S_1|^2\alpha(\boldsymbol{S})\varphi(E)+1}\right)\right] \end{aligned} \tag{14}$$

Next, consider the second integrals in (6) and (7). We have:

$$\begin{aligned} \int_{|S_1|\ge|S_2|} P_{\boldsymbol{S}}(\boldsymbol{s}) I(U;Y_1|\boldsymbol{s}) &\le \int_{|S_1|\ge|S_2|} P_{\boldsymbol{S}}(\boldsymbol{s}) I(X;Y_1|\boldsymbol{s}) \\ &\le \mathbb{E}\big[\psi\big(|S_1|^2\varphi(E)\mathbb{1}(|S_1|\ge|S_2|)\big)\big] \end{aligned} \tag{15}$$

Also,

$$\begin{aligned} &\int_{|S_1|\ge|S_2|} P_{\boldsymbol{S}}(\boldsymbol{s})\big(I(X;Y_2|U,\boldsymbol{s}) + I(U;Y_1|\boldsymbol{s})\big) \\ &\quad \overset{(a)}{\le} \int_{|S_1|\ge|S_2|} P_{\boldsymbol{S}}(\boldsymbol{s})\big(I(X;Y_1|U,\boldsymbol{s}) + I(U;Y_1|\boldsymbol{s})\big) \\ &\quad = \int_{|S_1|\ge|S_2|} P_{\boldsymbol{S}}(\boldsymbol{s}) I(X;Y_1|\boldsymbol{s}) \\ &\quad \le \mathbb{E}\big[\psi\big(|S_1|^2\varphi(E)\mathbb{1}(|S_1|\ge|S_2|)\big)\big] \end{aligned} \tag{16}$$

where inequality (a) holds because for $|s_1| \ge |s_2|$, the receiver Y_2 is a degraded version of Y_1. Note that in the last step, i.e., equation (16), it is critical to totally optimize the sum expression $I(X;Y_2|U,\boldsymbol{s}) + I(U;Y_1|\boldsymbol{s})$ because if we would independently optimize each of the mutual information functions $I(X;Y_2|U,\boldsymbol{s})$ and $I(U;Y_1|\boldsymbol{s})$ with $\boldsymbol{s} \in \{|S_1| \ge |S_2|\}$, we get $I(X;Y_2|\boldsymbol{s})$ and $I(X;Y_1|\boldsymbol{s})$, respectively. Also, note that in (15) and (16), the auxiliary random variable U is actually enhanced to X. By substituting (13)-(16) in (6) and (7), we derive the desired constraints in (4). The proof of Theorem 1 is thus complete. ■

Remark 1: The outer bound $\mathfrak{R}_o^{GFBC}$ given in (4) is applicable for all channels with arbitrary fading statistics and arbitrary amount of state information at the transmitter, specifically, for the channel with no CSIT.

In the next theorem, we prove that for the case where the transmitter has access to perfect state information, i.e., $E \equiv \boldsymbol{S}$, the rate regions (3) and (4) coincide which yield the exact capacity region.

Theorem 2) *Consider the two-user Gaussian fading BC (1) with common message wherein the transmitter knows the state perfectly, i.e., $E \equiv \boldsymbol{S}$. The inner bound $\mathfrak{R}_i^{GFBC}$ in (3) and the outer bound $\mathfrak{R}_o^{GFBC}$ in (4) coincide and result to the capacity region.*

Proof of Theorem 2) Let $\alpha^*(.):\mathbb{C}^2 \to [0,1]$ and $\beta^*(.):\mathbb{C}^2 \to [0,1]$ be two arbitrary deterministic functions. Define the deterministic functions $\alpha(.):\mathbb{C}^2 \to [0,1]$ and $\beta(.):\mathbb{C}^2 \to [0,1]$ as follows:

$$\alpha(\boldsymbol{S}) \triangleq \begin{cases} \alpha^*(\boldsymbol{S}) & \text{if } |S_1| < |S_2| \\ 0 & \text{if } |S_1| \geq |S_2| \end{cases}$$

$$\beta(\boldsymbol{S}) \triangleq \begin{cases} 0 & \text{if } |S_1| < |S_2| \\ \beta^*(\boldsymbol{S}) & \text{if } |S_1| \geq |S_2| \end{cases}$$

Thereby, we have $\alpha(\boldsymbol{s}) + \beta(\boldsymbol{s}) \leq 1$ for all $\boldsymbol{s} \in \mathbb{C}^2$. Now by substituting $\alpha(.)$ and $\beta(.)$ in the achievable rate region $\mathfrak{R}_i^{GFBC}$ in (3), one can see that it is equal to the rate region $\mathfrak{R}_o^{GFBC}$ in (4) if it is evaluated by $\alpha^*(\boldsymbol{S})$ and $\beta^*(\boldsymbol{S})$. The derivation of their equivalence is indeed interesting. ■

Remark 2: For the special case of the channel without common message, i.e., $R_0 = 0$, one can see [21, Remark 4] that Theorem 2 is reduced to the result of [1]. Note that our proof is considerably more concise than that of [1] which is based on the analysis of parallel BCs.

For the general case with partial side information at the transmitter, the inner bound (3) and the outer bound (4) may not coincide. The reason is that the functions $\alpha(.)$ and $\beta(.)$ in the inner bound (3) depend on the side information E, while they depend on the state $\boldsymbol{S}$ for the outer bound (4). Nonetheless, one may still explore for the special cases where these bounds coincide or at least have the same maximum sum-rate. We present an instance in the following theorem (the proof is given in [21]).

Theorem 3) *Consider the two-user Gaussian fading BC (1) with common message. Assume that the transmitter has access to the degradedness ordering of the channel, i.e., $E \equiv (E^*, E^\times)$ where $E^* \equiv \mathbb{1}(|S_2| < |S_1|)$ and $E^\times$ is an arbitrary deterministic function of the state $\boldsymbol{S}$. The sum-rate capacity is given below:*

$$\max_{\substack{\varphi(.):\\ \mathbb{E}[\varphi(E)]\leq P}} \begin{pmatrix} \mathbb{E}\big[\psi\big(|S_1|^2\varphi(E)\mathbb{1}(|S_1| \geq |S_2|)\big)\big] \\ +\mathbb{E}\big[\psi\big(|S_2|^2\varphi(E)\mathbb{1}(|S_2| \geq |S_1|)\big)\big] \end{pmatrix} \quad (17)$$

Some other capacity results are also derived for the channel in[21].

III.B) Fading BC with Secrecy

Next, we develop our approach to analyze for the Gaussian fading BC (1) with common and confidential messages. First, we propose an achievable rate region for the channel.

Proposition 2) *Define the rate region $\mathfrak{R}_{i\to sec}^{GFBC}$ as in (19), where $\varphi(.):\mathcal{E} \to \mathbb{R}_+$ is a power allocation policy function for the transmitter with $\mathbb{E}[\varphi(E)] \leq P$ and also $\alpha(.):\mathcal{E} \to [0,1]$ and $\beta(.):\mathcal{E} \to [0,1]$ are two arbitrary deterministic functions with $\alpha(e) + \beta(e) \leq 1$ for all $e \in \mathcal{E}$. The set $\mathfrak{R}_{i\to sec}^{GFBC}$ constitutes an inner bound on the secrecy capacity region of the two-user Gaussian fading BC (1) with common and confidential messages.*

Let remark that in equations (18) and (19) given below, the function $[x]_+$ is equal to x if x is positive and zero otherwise. The bound (19) is actually derived by adapting the achievable rate region given in [19, Th. 1] and evaluating it using Gaussian inputs, see [21, Prop. 2].

We next establish an outer bound on the secrecy capacity region of the channel. For this purpose, we make use of the outer bound given in [19, Th. 2] for the discrete BC with common and confidential messages. This outer bound can be adapted for the secrecy capacity region of the Gaussian fading channel (1) as follows:

$$\bigcup_{\substack{P_{X|E}P_{WUV|XS}\\ \mathbb{E}[|X|^2]\leq P}} \begin{Bmatrix} (R_0,R_1,R_2) \in \mathbb{R}_+^3: \\ R_0 \leq \min\{I(W;Y_1|\boldsymbol{S}), I(W;Y_2|\boldsymbol{S})\} \\ R_1 \leq [I(U;Y_1|V,W,\boldsymbol{S}) - I(U;Y_2|V,W,\boldsymbol{S})]_+ \\ R_2 \leq [I(V;Y_2|U,W,\boldsymbol{S}) - I(V;Y_1|U,W,\boldsymbol{S})]_+ \end{Bmatrix} \quad (18)$$

As we see, the outer bound (18) should be optimized over three auxiliary random variables, i.e., U, V, and W, that seems to be a challenging problem. To treat this optimization problem, by a subtle way, we actually put it in connection to the evaluation of the UV-outer bound given in Theorem 1. Clearly, we divide the state space into two events $\{|S_1| \leq |S_2|\}$ and $\{|S_2| \leq |S_1|\}$. Then, for the case of $\{|S_1| \leq |S_2|\}$, the auxiliary W is enhanced to $\bar{U} \triangleq (U,W)$ and for the case of $\{|S_2| \leq |S_1|\}$, it is enhanced to $\bar{V} \triangleq (V,W)$. As shown in [21], this is an optimal assignment, specially for the channel with perfect CSIT. By this assignment, the problem is reduced to the optimization over $\bar{U}$ and $\bar{V}$ which is treated similar to the evaluation of the UV-outer bound in Theorem 1. The resultant outer bound is given in the next theorem.

$$\mathfrak{R}_{i\to sec}^{GFBC} \triangleq \bigcup_{\substack{\alpha(.),\beta(.)\\ \varphi(.)}} \begin{Bmatrix} (R_0,R_1,R_2) \in \mathbb{R}_+^3: \\ R_0 \leq \min\left\{\mathbb{E}\left[\psi\left(\frac{|S_1|^2\big(1-\alpha(E)-\beta(E)\big)\varphi(E)}{|S_1|^2\big(\alpha(E)+\beta(E)\big)\varphi(E)+1}\right)\right], \mathbb{E}\left[\psi\left(\frac{|S_2|^2\big(1-\alpha(E)-\beta(E)\big)\varphi(E)}{|S_2|^2\big(\alpha(E)+\beta(E)\big)\varphi(E)+1}\right)\right]\right\}, \\ R_1 \leq \left[\mathbb{E}\left[\psi\left(\frac{|S_1|^2\beta(E)\varphi(E)}{|S_1|^2\alpha(E)\varphi(E)+1}\right)\right] - \mathbb{E}\big[\psi\big(|S_2|^2\beta(E)\varphi(E)\big)\big]\right]_+, \\ R_2 \leq \left[\mathbb{E}\left[\psi\left(\frac{|S_2|^2\alpha(E)\varphi(E)}{|S_2|^2\beta(E)\varphi(E)+1}\right)\right] - \mathbb{E}\big[\psi\big(|S_1|^2\alpha(E)\varphi(E)\big)\big]\right]_+ \end{Bmatrix} \quad (19)$$

$$\mathfrak{R}_{o\to sec}^{GFBC} \triangleq \bigcup_{\substack{\alpha(.),\beta(.)\\ \varphi(.)}} \begin{Bmatrix} (R_0,R_1,R_2) \in \mathbb{R}_+^3: \\ R_0 \leq \min\begin{Bmatrix} \mathbb{E}\left[\psi\left(\frac{|S_1|^2\big(1-\alpha(\boldsymbol{S})\big)\varphi(E)\mathbb{1}(|S_1|<|S_2|)}{|S_1|^2\alpha(\boldsymbol{S})\varphi(E)+1}\right)\right] + \mathbb{E}\left[\psi\left(\frac{|S_1|^2\big(1-\beta(\boldsymbol{S})\big)\varphi(E)\mathbb{1}(|S_2|\leq|S_1|)}{|S_1|^2\beta(\boldsymbol{S})\varphi(E)+1}\right)\right], \\ \mathbb{E}\left[\psi\left(\frac{|S_2|^2\big(1-\alpha(\boldsymbol{S})\big)\varphi(E)\mathbb{1}(|S_1|<|S_2|)}{|S_2|^2\alpha(\boldsymbol{S})\varphi(E)+1}\right)\right] + \mathbb{E}\left[\psi\left(\frac{|S_2|^2\big(1-\beta(\boldsymbol{S})\big)\varphi(E)\mathbb{1}(|S_2|\leq|S_1|)}{|S_2|^2\beta(\boldsymbol{S})\varphi(E)+1}\right)\right] \end{Bmatrix}, \\ R_1 \leq \mathbb{E}\left[\Big(\psi\big(|S_1|^2\beta(\boldsymbol{S})\varphi(E)\big) - \psi\big(|S_2|^2\beta(\boldsymbol{S})\varphi(E)\big)\Big)\mathbb{1}(|S_2|\leq|S_1|)\right], \\ R_2 \leq \mathbb{E}\left[\Big(\psi\big(|S_2|^2\alpha(\boldsymbol{S})\varphi(E)\big) - \psi\big(|S_1|^2\alpha(\boldsymbol{S})\varphi(E)\big)\Big)\mathbb{1}(|S_1|<|S_2|)\right] \end{Bmatrix} \quad (20)$$

Theorem 4) *Define the rate region* $\mathfrak{R}_{o\to sec}^{GFBC}$ *as in (20), where* $\varphi(.):\mathcal{E}\to\mathbb{R}_+$ *is a power allocation policy function for the transmitter with* $\mathbb{E}[\varphi(E)]\le P$ *and also* $\alpha(.):\mathbb{C}^2\to[0,1]$ *and* $\beta(.):\mathbb{C}^2\to[0,1]$ *are two arbitrary deterministic functions. The set* $\mathfrak{R}_{o\to sec}^{GFBC}$ *constitutes an outer bound on the secrecy capacity region of the two-user Gaussian fading BC (1) with common and confidential messages.*

Here, we do not provide the details of the proof for Theorem 4 due to the limited space. However, we encourage the reader to see our derivations in [21, Th. 6].

Remark 3: If we consider only the constraints given on the rates R_1 and R_2, the outer bound $\mathfrak{R}_{o\to sec}^{GFBC}$ in (20) is optimized for $\alpha(.)\equiv\beta(.)\equiv 1$.

We next prove that the inner bound (19) and the outer bound (20) coincide for some special cases which result to the exact secrecy capacity region. We have the following theorems (the proofs are given in [21]).

Theorem 5) *Consider the two-user fading BC (1) with common and confidential messages. Assume that the state information is perfectly available at the transmitter, i.e.,* $E\equiv\boldsymbol{S}$*. The bounds (19) and (20) coincide which yield the secrecy capacity region.*

The derivation of Theorem 5 is similar to Theorem 2. See [21, Th. 7] for details.

Remarks 4:

1. Theorem 5 includes all the results of [2-5] as special cases. Note that the results of all the latter papers are derived by resorting to the analysis of parallel channels. We have obtained a stronger result with a more concise proof.
2. Theorem 5 also completes a gap in the paper [4]. Clearly, in [4] Ekrem and Ulukus could find the secrecy capacity region of the parallel degraded BCs [4, Corollary 1] with both common and confidential messages, however, for the Gaussian fading channel the secrecy capacity region is given only for the channel without common message. In other words, for the Gaussian fading BC with both common and confidential messages the secrecy capacity region remains unresolved in [4].

Theorem 6) *Consider the two-user Gaussian fading BC without common message, i.e.,* $R_0=0$*. Assume that the transmitter has access to the degradedness ordering of the channel, i.e.,* $E\equiv(E^*,E^\times)$ *where* $E^*\equiv\mathbb{1}(|S_2|<|S_1|)$ *and* $E^\times$ *is an arbitrary deterministic function of the state* $\boldsymbol{S}$*. The bounds (19) and (20) coincide which result to the secrecy capacity region.*

We remark that the key to derive the capacity result in Theorem 6 is that for the channel without common message, the outer bound (20) is optimized with $\alpha(.)\equiv\beta(.)\equiv 1$, as given in Remark 3.

In this conference version, we have presented our approach for the derivation of capacity bounds. The explicit computation of the derived bounds and the optimal power allocation analysis are relegated to the journal version of the paper [21].

CONCLUSION

In this paper, we developed a new approach for analyzing wireless ergodic fading BCs with arbitrary stationary fading statistics and any arbitrary amount of CSIT. Specifically, a novel method was presented to evaluate the well-known UV-outer bound for the Gaussian fading BC using the EPI. Several new capacity results were established which include all previous results as special cases, as well. The approach is also applicable to analyze various fading network topologies regardless of that a given network is separable into parallel sub-channels or not. Specifically, in [25] by following the same approach, we derive the capacity region of the wireless ergodic fading interference channel with partial CSIT to within one bit.

REFERENCES

[1] L. Li and A. J. Goldsmith, "Capacity and optimal resource allocation for fading broadcast channels: Part I: Ergodic capacity," *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 1083–1102, Mar. 2001.

[2] 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.

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

[4] E. Ekrem and S. Ulukus, "Ergodic secrecy capacity region of the fading broadcast channel," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dresden, Germany, 2009.

[5] Y. Liang, H. V. Poor, L. Ying. "Secure communications over wireless broadcast networks: Stability and utility maximization," *IEEE Trans. on Inf. Forensics and Security,* vol. 6, no. 3, pp 682-692, July 2011.

[6] R. Liu, Y. Liang, H. V. Poor, "Fading cognitive multiple-access channels with confidential messages," *IEEE Transactions on Information Theory,* vol. 57, no. 8, pp. 4992-5005, Aug. 2011.

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

[8] A. Khisti and T. Liu, "Private broadcasting over independent parallel channels," *Submitted to IEEE Trans. on Inf. Theory*, 2012, ArXiv: 1212.6930.

[9] V. R. Cadambe and S. A. Jafar, "Parallel Gaussian interference channels are not always separable," *IEEE Trans. on Inf. Theory*, vol. 55, pp. 3983– 3990, Sep. 2009.

[10] L. Sankar, X. Shang, E. Erkip, and H. V. Poor, "Ergodic fading interference channels: Sum-capacity and separability," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2605–2626, May 2011.

[11] D. Tuninetti and S. Shamai, "On two-user fading Gaussian broadcast channels with perfect channel state information at the receivers," *In IEEE Intl. Symp. Info. Theory ISIT*, Yokohama, Japan, July 2003.

[12] A. Jafarian and S. Vishwanath, "On the capacity of one-sided two user Gaussian fading broadcast channels," *in Proc. Globecom*, Dec 2008.

[13] D. N. C. Tse and R. Yates, "Fading broadcast channels with state information at the receivers," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3453-3471, Jun. 2012.

[14] R. Yates and J. Lei, "Gaussian fading broadcast channels with CSI only at the receivers: An improved constant gap," in *Proc. IEEE Int. Symp. Inf. Theory*, Aug. 2011, pp. 2969–2973.

[15] A. Jafarian and S. Vishwanath, "The two-user Gaussian fading broadcast channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Aug. 2011, pp. 2964–2968.

[16] R. Yates and D. Tse, "K user fading broadcast channels with CSI at the receivers," in *Proc. of Information Theory and Applications Workshop (ITA 2011)*, San Diego, USA, 2011.

[17] D. Guo, S. Shamai, and S. Verdu, "Mutual information and minimum mean square error in Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 51, pp. 1261-1282, Apr. 2005.

[18] C. Nair, "A note on outer bounds for broadcast channel," in *Int. Zurich Seminar on Communications (IZS)*, Mar. 2010.

[19] Jin Xu, Yi Cao, and Biao Chen, "Capacity bounds for broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, Oct. 2009.

[20] A. Wyner, "The wire-tap channel," *Bell Systems Technical J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[21] R. K. Farsani, "Capacity bounds for wireless ergodic fading broadcast channels with partial CSIT," *IEEE Trans. Information Theory, To be submitted*, *preprint available at* ArXiv:1302.5696.

[22] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 3, pp. 306–311, May 1979.

[23] D. Tuninetti and S. Shamai (Shitz), "Gaussian broadcast channels with state information at the receivers," in *Proc. DIMACS Workshop on Network Information Theory*, Piscataway, NJ, Mar. 2003.

[24] D. Tuninetti, S. Shamai and G. Caire, "Is Gaussian input optimal for fading Gaussian broadcast channels?", in *Proc. of Information Theory and Applications Workshop (ITA 2007)*, San Diego, CA USA, January 2007.

[25] R. K. Farsani, "The capacity region of the wireless ergodic fading interference channel with partial CSIT to within one bit," *IEEE ISIT 2013*.