Parallel BCC with One Common and Two Confidential Messages and Imperfect CSIT

Ahmed Benfarah, Stefano Tomasin and Nicola Laurenti
Department of Information Engineering, University of Padova
via Gradenigo 6/B, 35131 Padova, Italy. Email: firstname.lastname@dei.unipd.it

***Abstract*—We consider a broadcast communication system over parallel sub-channels where the transmitter sends three messages: a common message to two users, and two confidential messages to each user which need to be kept secret from the other user. We assume partial channel state information at the transmitter (CSIT), stemming from noisy channel estimation. The first contribution of this paper is the characterization of the secrecy capacity region boundary as the solution of weighted sum-rate problems, with suitable weights. Partial CSIT is addressed by adding a margin to the estimated channel gains. The second paper contribution is the solution of this problem in an almost closed-form, where only two single real parameters must be optimized, e.g., through dichotomic searches. On the one hand, the considered problem generalizes existing literature where only two out of the three messages are transmitted. On the other hand, the solution finds also practical applications into the resource allocation of orthogonal frequency division multiplexing (OFDM) systems with both secrecy and fairness constraints.**

***Index Terms*—Broadcast communication, orthogonal frequency division multiplexing (OFDM), parallel channels, physical layer security, power allocation.**

I. Introduction

With the widespread adoption of wireless networks, security becomes an inherent issue of nowadays communications. In this context, *physical layer security* arises as a promising tool to complement traditional cryptographic solutions. The basic concepts of this approach were founded by the pioneering work of Wyner [1]. He introduced the *wiretap* channel model in which the transmitter aims at sending reliably a confidential message to the legitimate receiver in presence of an eavesdropper. The *secrecy capacity* measures the maximum information rate at which the transmitter can reliably communicate a secret message to the receiver, while the eavesdropper left with no information on the message. Recently, the wiretap channel witnessed a renewed interest and many research works investigated the secrecy capacity of wireless fading [2], parallel [3], [4] and multiple-input multiple-output (MIMO) channels [5], [6]. All of these works deal with the point-to-point wiretap channel model. There has been also an effort to generalize physical layer security to the multi-user context (see [7] for a survey).

An important scenario of multi-user physical layer security is the *broadcast channel with confidential messages* (BCC) [8]. In [9], the authors established the secrecy capacity region of parallel sub-channels where a source node has a common message for two receivers and a confidential message is intended only for one receiver. Extensive research work was made to characterize the secrecy capacity region of Gaussian MIMO BCC [10] [11]. In all these works, the communication scenario consists of a source node communicating with two receiving users maliciously eavesdropping on each other. Secure broadcasting to multiple receivers was analyzed in [12], [13] when the eavesdropper is external to the group of users. For an overview of the different considered BCC scenarios, the reader can see [14].

In this paper, we consider a parallel BCC with two receivers, where the transmitter aims at sending three independent messages with a total power constraint: one common message to both users and two confidential messages, one for each user. We further consider the case in which only partial channel state information at the transmitter (CSIT) is available before transmission, stemming from a noisy estimate of the channels. We first characterize the secrecy capacity region of the considered system where partial CSIT is addressed by adding a margin to the estimated channel gains. Then, an almost closed-form solution to the weighted sum-rate maximization problem is derived, where two real variables must be optimized, e.g., through dichotomic search. Our contribution generalizes some related work which considered only two out of the three possible messages: in [15], [16], the authors derived the optimal power allocation in presence of two confidential messages without a common while in [9], the optimal power allocation for the case of one common message and one confidential message was established.

II. System Model

We consider[1] parallel BCC (e.g., OFDM) with L sub-channels, one transmitter and two receiving users. Note that we consider real-valued signals. The transmitter sends the real-valued symbol x_ℓ on sub-channel ℓ. The channel input is

This work was partly supported by the Italian Ministry of Education and Research (MIUR) under project ESCAPADE (Grant RBFR105NLC) in the "FIRB-Futuro in Ricerca 2010" funding program.

[1]*Notation:* Vectors and matrices are written in bold letters. $\log$ and $\ln$ denote the base-2 and natural-base logarithms, respectively. We indicate the positive part of a real quantity x as $[x]^+ = \max\{x; 0\}$. $\mathbb{E}[X]$ denotes the expectation of the random variable X, $\mathbb{I}(X;Y)$ denotes the mutual information between variables X and Y. $\mathrm{tr}(\boldsymbol{X})$ denotes the trace of a square matrix $\boldsymbol{X}$. For two positive semi-definite matrices $\boldsymbol{X}$ and $\boldsymbol{Y}$, we write $\boldsymbol{X} \preceq \boldsymbol{Y}$ whenever $\boldsymbol{Y} - \boldsymbol{X}$ is a positive semi-definite matrix.

subject to the statistical total power constraint

$$\sum_{\ell=1}^{L} \mathbb{E}\{x_\ell^2\} \leq P. \tag{1}$$

We assume that the channel is quasi-static, i.e., it remains constant over the entire duration of a single packet. At sub-channel ℓ of receiver $i = 1, 2$ we obtain

$$y_{i,\ell} = h_{i,\ell} x_\ell + n_{i,\ell}\,, \tag{2}$$

where $n_{i,\ell}$ is the real-valued zero-mean unit variance additive white Gaussian noise (AWGN) term. Noise components for different sub-channels are independent. $h_{i,\ell}$ is the real-valued channel coefficient. Let $\alpha_{i,\ell} = h_{i,\ell}^2$ be the channel power gain. We assume that the transmitter has some partial channel state information. It knows the channel statistical distribution and possesses estimates $\hat{h}_{i,\ell}$ of the channel coefficients, that are corrupted by noise

$$\hat{h}_{i,\ell} = h_{i,\ell} + \eta_{i,\ell}\,, \tag{3}$$

where $\eta_{i,\ell}$ are iid real-valued zero-mean Gaussian noise with variance σ^2. The conditional probability density function (pdf) of the channel gain $\alpha_{i,\ell}$ given the channel coefficient estimate $\hat{h}_{i,\ell}$ can be computed from the *a priori* pdf of the channel coefficient $f_{h_{i,\ell}}$ and that of the estimation noise f_η as

$$f_{\alpha_{i,\ell}|\hat{h}_{i,\ell}}(a|b) = \frac{f_\eta(b-\sqrt{a}) f_{h_{i,\ell}}(\sqrt{a}) + f_\eta(b+\sqrt{a}) f_{h_{i,\ell}}(-\sqrt{a})}{2\sqrt{a}\left[f_{h_{i,\ell}} \otimes f_\eta\right](b)}. \tag{4}$$

where $\otimes$ denotes the convolution operation.

As illustrated in Fig. 1, we consider a BCC where the transmitter aims at reliably delivering a common message M_0 with information rate R_0 and two separate confidential messages M_1 and M_2 with information rates R_1 and R_2, respectively [17]. The common message M_0 is intended for both receivers, while confidential message M_i is intended for receiver i and needs to be kept secret from the other receiver. The transmitter allocates power $p_{i,\ell}$ on sub-channel ℓ for the confidential message M_i, and power $p_{0,\ell}$ for the common message M_0.

In order to have *reliable transmissions* to the intended receiver, vanishing error probabilities must be obtained as the codeword length n grows to infinity. *Secrecy* is measured in terms of the information leakage rate to the non-intended receiver (aka *weak* information theoretic secrecy) [1], [8], i.e., defining $\boldsymbol{Y}_i^n = [\boldsymbol{y}_i(1), \ldots, \boldsymbol{y}_i(n)]$, we require

$$\frac{1}{n}\mathbb{I}(M_1; \boldsymbol{Y}_2^n) \to 0 \quad ; \quad \frac{1}{n}\mathbb{I}(M_2; \boldsymbol{Y}_1^n) \to 0, \tag{5}$$

as $n \to \infty$.

A. Secrecy Capacity Region

Since the transmitter does not know the exact channel realization, secrecy outage may occur, i.e., the transmitted message is either not secret or not decoded by the receiver. However, computing the secrecy outage probability is an involved task, therefore we consider here a simpler approach where we add some margin to the channel estimates in order to keep the outage probability under control.

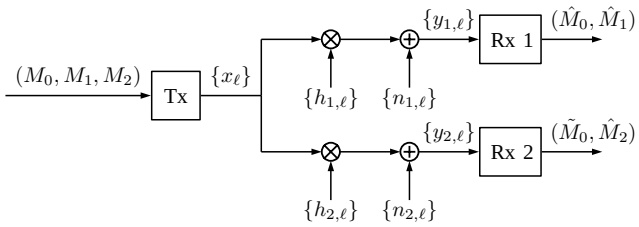


Fig. 1. Parallel BCC with common and two confidential messages.

In particular, the transmitter can compute upper and lower bounds on the channel gains $\alpha_{i,\ell}^+$ and $\alpha_{i,\ell}^-$ that provide the desired outage probability. We consider here a simpler approach where the same probability threshold ε is used on each channel, i.e.,

$$\mathrm{P}\left[\alpha_{i,\ell} > \alpha_{i,\ell}^+ \middle| \hat{h}_{i,\ell}\right] < \varepsilon\,, \quad \mathrm{P}\left[\alpha_{i,\ell} < \alpha_{i,\ell}^- \middle| \hat{h}_{i,\ell}\right] < \varepsilon\,. \tag{6}$$

Then, $\alpha_{i,\ell}^-$ will be considered as the channel gain to the intended receiver, while $\alpha_{i,\ell}^+$ is the channel gain to the unintended receiver. The probabilities in (6) can be computed using the pdf (4). Note also that when perfect CSIT is available $\alpha_{i,\ell}^- = \alpha_{i,\ell}^+$.

The secrecy capacity region $\mathcal{C}_s$ is defined as the closure of all rate triples (R_0, R_1, R_2) that can be achieved by any coding scheme while maintaining both reliability and secrecy requirements. Let $\boldsymbol{K}_x$ be the covariance matrix of $\{x_\ell\}_{\ell=1,\ldots,L}$, the secrecy capacity region of the Gaussian MIMO BCC under a covariance constraint (i.e., $\boldsymbol{K}_x \preceq \boldsymbol{K}$) was characterized in [10], [11]. The secrecy capacity region $\mathcal{C}_s$ under the total power constraint (1) is obtained by the union over all covariance matrices which satisfy $\mathrm{tr}(\boldsymbol{K}) \leq P$. Moreover, the parallel channels can be seen as a special case of MIMO channels. Having independent inputs for each sub-channel is optimal for the parallel BCC [9]. Consequently, it is sufficient to have diagonal input covariance matrices [11], [10] for the parallel BCC. We define the power allocation vector $\boldsymbol{p} = [p_{0,1}, \ldots, p_{0,L}, p_{1,1}, \ldots, p_{1,L}, p_{2,1}, \ldots, p_{2,L}]$. The set $\mathcal{P}$ includes all power allocation vectors $\boldsymbol{p}$ that satisfy the total power constraint (1), i.e.,

$$\mathcal{P} = \left\{ \boldsymbol{p} : \sum_{\ell=1}^{L} (p_{0,\ell} + p_{1,\ell} + p_{2,\ell}) \leq P \right\}. \tag{7}$$

Let us partition the channel index set $\{1, \ldots, L\}$ into

$$\begin{aligned} &S_1 = \{\ell : \alpha_{1,\ell}^- > \alpha_{2,\ell}^+\}\,, \quad S_2 = \{\ell : \alpha_{2,\ell}^- > \alpha_{1,\ell}^+\}\,, \\ &S_3 = \{1, \ldots, L\} \setminus (S_1 \cup S_2)\,. \end{aligned} \tag{8}$$

By combining the results of [10] and [9], the secrecy capacity region of the parallel BCC with common and two confidential messages can be written as

$$\mathcal{C}_s = \bigcup_{\boldsymbol{p}\in\mathcal{P}} \left\{ \begin{array}{l} (R_0, R_1, R_2): \\ 0 \le R_0 \le R_0^{\max}(\boldsymbol{p}) \\ \\ 0 \le R_i \le R_i^{\max}(\boldsymbol{p}) \end{array} \right. \tag{9}$$

where

$$R_0^{\max}(\boldsymbol{p}) = \min\{R_{01}^{\max}(\boldsymbol{p}), R_{02}^{\max}(\boldsymbol{p})\} \tag{10}$$

$$\begin{aligned} R_{01}^{\max}(\boldsymbol{p}) = \frac{1}{2}\sum_{\ell=1}^{L} &\log\big(1+\alpha_{1,\ell}^{-}[p_{0,\ell}+p_{1,\ell}+p_{2,\ell}]\big) \\ &- \log\big(1+\alpha_{1,\ell}^{-}[p_{1,\ell}+p_{2,\ell}]\big) \end{aligned} \tag{11}$$

$$\begin{aligned} R_{02}^{\max}(\boldsymbol{p}) = \frac{1}{2}\sum_{\ell=1}^{L} &\log\big(1+\alpha_{2,\ell}^{-}[p_{0,\ell}+p_{1,\ell}+p_{2,\ell}]\big) \\ &- \log\big(1+\alpha_{2,\ell}^{-}[p_{1,\ell}+p_{2,\ell}]\big) \end{aligned} \tag{12}$$

$$R_1^{\max}(\boldsymbol{p}) = \frac{1}{2}\sum_{\ell\in S_1} \log(1+\alpha_{1,\ell}^{-}p_{1,\ell}) - \log(1+\alpha_{2,\ell}^{+}p_{1,\ell}) \tag{13}$$

$$R_2^{\max}(\boldsymbol{p}) = \frac{1}{2}\sum_{\ell\in S_2} \log(1+\alpha_{2,\ell}^{-}p_{2,\ell}) - \log(1+\alpha_{1,\ell}^{+}p_{2,\ell}). \tag{14}$$

The expression of the secrecy capacity region states that the receivers decode the common message first, by treating the confidential messages as noise. Then, each receiver decodes its own confidential message.

Note that the expressions of the secrecy capacity region hold also for perfect CSIT by letting $\alpha_{i,\ell}^{-} = \alpha_{i,\ell}^{+}$.

III. Power Allocation Algorithm

First note that the secrecy capacity region (9) is convex. Therefore, for each triplet $(R_0^{\max}(\boldsymbol{p}^*), R_1^{\max}(\boldsymbol{p}^*), R_2^{\max}(\boldsymbol{p}^*))$ on the region boundary, there exists a weight triplet $w_0, w_1, w_2 > 0$ satisfying

$$\boldsymbol{p}^* = \arg\max_{\boldsymbol{p}\in\mathcal{P}} \left[w_0 R_0^{\max}(\boldsymbol{p}) + w_1 R_1^{\max}(\boldsymbol{p}) + w_2 R_2^{\max}(\boldsymbol{p})\right]. \tag{15}$$

By solving (15) all points of the secrecy capacity region boundary are obtained. Note also that the weighted sum rate problem is also of interest for resource allocation in OFDM systems with a fairness constraint, where the weights are selected in order to enforce the desired fairness.

Now, the optimization problem (15) together with (10) is a max-min optimization, and can be solved by using an approach similar to that of [18]. The particular result is provided in the following lemma, whose proof is not reported as it follows the same steps of [18].

Lemma 1. *The solution of (15) also solves one of the following three problems:*

(P1) $\boldsymbol{p}^{(1)} = \arg\max_{\boldsymbol{p}\in\mathcal{P}} \left[w_0 R_{01}^{\max}(\boldsymbol{p}) + w_1 R_1^{\max}(\boldsymbol{p}) + w_2 R_2^{\max}(\boldsymbol{p})\right]$

(P2) $\boldsymbol{p}^{(2)} = \arg\max_{\boldsymbol{p}\in\mathcal{P}} \left[w_0 R_{02}^{\max}(\boldsymbol{p}) + w_1 R_1^{\max}(\boldsymbol{p}) + w_2 R_2^{\max}(\boldsymbol{p})\right]$

(P3) $\boldsymbol{p}^{(3)} = \arg\max_{\boldsymbol{p}\in\mathcal{P}} \left[w_0(\mu R_{01}^{\max}(\boldsymbol{p}) + (1-\mu) R_{02}^{\max}(\boldsymbol{p})) + w_1 R_1^{\max}(\boldsymbol{p}) + w_2 R_2^{\max}(\boldsymbol{p})\right]$

for some $\mu \in (0,1)$ in (P3). In particular,

$$\boldsymbol{p}^* = \begin{cases} \boldsymbol{p}^{(1)} & \text{if } \mathrm{R}_{01}^{\max}(\mathrm{p}^{(1)}) < \mathrm{R}_{02}^{\max}(\mathrm{p}^{(1)}) \\ \boldsymbol{p}^{(2)} & \text{if } \mathrm{R}_{01}^{\max}(\mathrm{p}^{(2)}) > \mathrm{R}_{02}^{\max}(\mathrm{p}^{(2)}) \\ \boldsymbol{p}^{(3)} & \text{if } \mathrm{R}_{01}^{\max}(\mathrm{p}^{(3)}) = \mathrm{R}_{02}^{\max}(\mathrm{p}^{(3)}) \end{cases}. \tag{16}$$

We now focus on the solution of problems (P1)-(P3). Before introducing the result, we define the following terms, with $\ell = 1, \ldots, L$ and $i = 1, 2$. Let $\bar{\imath} = 2$ if $i = 1$ and $\bar{\imath} = 1$ if $i = 2$, let $\mu_i = \mu$ if $i = 1$ and $\mu_i = 1-\mu$ if $i = 2$. Denote by $\delta_{i,\ell} = 1/\alpha_{\bar{\imath},\ell}^{+} - 1/\alpha_{i,\ell}^{-}$, and let $\lambda \ge 0$ be a real valued parameter. Then, denote

$$\beta_{i,\ell} = \frac{1}{2}\left[\delta_{i,\ell}\left(\delta_{i,\ell} + \frac{2w_i}{\lambda \ln 2}\right)\right]^{1/2} - \frac{1}{2}\left(\frac{1}{\alpha_{\bar{\imath},\ell}^{+}} + \frac{1}{\alpha_{i,\ell}^{-}}\right) \tag{17a}$$

$$\gamma_{i,\ell} = \frac{w_0}{2\lambda\ln 2} - \frac{1}{\alpha_{i,\ell}^{-}}, \quad \zeta_{i,\ell} = \frac{w_i}{w_0}\delta_{i,\ell} - \frac{1}{\alpha_{\bar{\imath},\ell}^{+}} \tag{17b}$$

$$\begin{aligned} \nu_{i,\ell} = \frac{1}{2}\Bigg[&\left(\frac{1}{\alpha_{\bar{\imath},\ell}^{-}} - \frac{1}{\alpha_{i,\ell}^{-}} - \frac{w_0}{2\lambda\ln 2}\right)^2 \\ &+ \frac{2w_0\mu_i}{\lambda\ln 2}\left(\frac{1}{\alpha_{\bar{\imath},\ell}^{-}} - \frac{1}{\alpha_{i,\ell}^{-}}\right)\Bigg]^{1/2} \\ &- \frac{1}{2}\left(\frac{1}{\alpha_{\bar{\imath},\ell}^{-}} + \frac{1}{\alpha_{i,\ell}^{-}} - \frac{w_0}{2\lambda\ln 2}\right) \end{aligned} \tag{17c}$$

$$\begin{aligned} \Delta_{i,\ell} = &\left[\left(\frac{w_i}{w_0}\right)^2 + \frac{w_i}{w_0}\left(\frac{2\cdot\left(\frac{2}{\alpha_{\bar{\imath},\ell}^{-}} - \frac{1}{\alpha_{i,\ell}^{-}} - \frac{1}{\alpha_{\bar{\imath},\ell}^{+}}\right)}{\frac{1}{\alpha_{\bar{\imath},\ell}^{+}} - \frac{1}{\alpha_{i,\ell}^{-}}}\right) + 1\right] \\ &\cdot \left[\frac{1}{\alpha_{\bar{\imath},\ell}^{+}} - \frac{1}{\alpha_{i,\ell}^{-}}\right]^2 \end{aligned}$$

$$\theta_{i,\ell} = \frac{\frac{w_i}{w_0}\left(\frac{1}{\alpha_{\bar{\imath},\ell}^{+}} - \frac{1}{\alpha_{i,\ell}^{-}}\right) - \left(\frac{1}{\alpha_{\bar{\imath},\ell}^{+}} + \frac{1}{\alpha_{i,\ell}^{-}}\right) + \sqrt{\Delta_{i,\ell}}}{2} \tag{17d}$$

$$\begin{aligned} \Lambda_{i,\ell} = &\left(\delta_{i,\ell}\right)^2\left(\frac{w_i}{w_0}\right)^2 + 2\frac{w_i}{w_0}\left[\delta_{i,\ell}\left(\frac{2-\mu_i}{\alpha_{\bar{\imath},\ell}^{-}} - \frac{\mu_{\bar{\imath}}}{\alpha_{i,\ell}^{-}} - \frac{1}{\alpha_{\bar{\imath},\ell}^{+}}\right)\right] \\ &+ \left(\delta_{i,\ell}\right)^2 + \mu_i\left(\frac{1}{\alpha_{\bar{\imath},\ell}^{-}} - \frac{1}{\alpha_{i,\ell}^{-}}\right)\left[\mu_i\left(\frac{1}{\alpha_{\bar{\imath},\ell}^{-}} - \frac{1}{\alpha_{i,\ell}^{-}}\right) - 2\left(\frac{1}{\alpha_{\bar{\imath},\ell}^{+}} - \frac{1}{\alpha_{i,\ell}^{-}}\right)\right] \end{aligned}$$

$$\xi_{i,\ell} = \frac{\frac{w_i}{w_0}\delta_{i,\ell} - \left(\frac{1}{\alpha_{\bar{\imath},\ell}^{+}} + \frac{1}{\alpha_{i,\ell}^{-}}\right) - \mu_i\left(\frac{1}{\alpha_{\bar{\imath},\ell}^{-}} - \frac{1}{\alpha_{i,\ell}^{-}}\right) + \sqrt{\Lambda_{i,\ell}}}{2}. \tag{17e}$$

The main result for the solution of the optimization problem (15) is provided by the following theorem.

Theorem 1. *The solutions of problems (P1)-(P3) are:*

(P1) *For $\ell \in S_1$, if $\frac{w_1}{w_0} > \frac{\alpha_{1,\ell}^{-}}{\alpha_{1,\ell}^{-} - \alpha_{2,\ell}^{+}}$, then*

$$p_{0,\ell}^{(1)} = \left[\gamma_{1,\ell} - \zeta_{1,\ell}\right]^{+}, \; p_{1,\ell}^{(1)} = \left[\min\left\{\beta_{1,\ell}; \zeta_{1,\ell}\right\}\right]^{+}. \tag{18a}$$

Otherwise, if $\frac{w_1}{w_0} \leq \frac{\alpha_{1,\ell}^-}{\alpha_{1,\ell}^- - \alpha_{2,\ell}^+}$, *then*

$$p_{0,\ell}^{(1)} = [\gamma_{1,\ell}]^+ \,, \quad p_{1,\ell}^{(1)} = 0 \,. \tag{18b}$$

For $\ell \in S_2$, *if* $\frac{w_2}{w_0} > \frac{\alpha_{1,\ell}^-}{\alpha_{2,\ell}^- - \alpha_{1,\ell}^+}$, *then*

$$p_{0,\ell}^{(1)} = [\gamma_{1,\ell} - \theta_{2,\ell}]^+ \,, \; p_{2,\ell}^{(1)} = [\min\{\beta_{2,\ell}; \theta_{2,\ell}\}]^+ \,. \tag{18c}$$

Otherwise, if $\frac{w_2}{w_0} \leq \frac{\alpha_{1,\ell}^-}{\alpha_{2,\ell}^- - \alpha_{1,\ell}^+}$, *then*

$$p_{0,\ell}^{(1)} = [\gamma_{1,\ell}]^+ \,, \quad p_{2,\ell}^{(1)} = 0 \,. \tag{18d}$$

For $\ell \in S_3$,

$$p_{0,\ell}^{(1)} = [\gamma_{1,\ell}]^+ \tag{18e}$$

where λ *is chosen to satisfy the total power constraint (7).*

(P2) *Due to the symmetry (with respect to the user index) of problems (P1) and (P2), solution (P2) is the same as that of (P1) where user indices 1 and 2 are swapped.*

(P3) *For* $\ell \in S_i$, *if* $\Lambda_{i,\ell} > 0$, *then*

if $\frac{w_i}{w_0} > \frac{\mu_i \alpha_{i,\ell}^- + \mu_{\bar{\imath}} \alpha_{\bar{\imath},\ell}^-}{\alpha_{i,\ell}^- - \alpha_{\bar{\imath},\ell}^+}$, *then*

$$p_{0,\ell}^{(3)} = [\nu_{i,\ell} - \xi_{i,\ell}]^+ \,, \quad p_{i,\ell}^{(3)} = [\min\{\beta_{i,\ell}; \xi_{i,\ell}\}]^+ \,. \tag{19a}$$

Otherwise, if $\frac{w_i}{w_0} \leq \frac{\mu_i \alpha_{i,\ell}^- + \mu_{\bar{\imath}} \alpha_{\bar{\imath},\ell}^-}{\alpha_{i,\ell}^- - \alpha_{\bar{\imath},\ell}^+}$, *then*

$$p_{0,\ell}^{(3)} = [\nu_{i,\ell}]^+ \,, \quad p_{i,\ell}^{(3)} = 0 \,. \tag{19b}$$

If $\Lambda_{i,\ell} = 0$, *then*

if $\frac{w_i}{w_0} > \frac{\alpha_{i,\ell}^- + \mu_{\bar{\imath}} \alpha_{\bar{\imath},\ell}^+ + \mu_i \frac{\alpha_{i,\ell}^- \alpha_{\bar{\imath},\ell}^+}{\alpha_{\bar{\imath},\ell}^-}}{\alpha_{i,\ell}^- - \alpha_{\bar{\imath},\ell}^+}$, *then*

$$p_{0,\ell}^{(3)} = [\nu_{i,\ell} - \xi_{i,\ell}]^+ \,, \quad p_{i,\ell}^{(3)} = [\min\{\beta_{i,\ell}; \xi_{i,\ell}\}]^+ \,. \tag{19c}$$

Otherwise, if $\frac{w_i}{w_0} \leq \frac{\alpha_{i,\ell}^- + \mu_{\bar{\imath}} \alpha_{\bar{\imath},\ell}^+ + \mu_i \frac{\alpha_{i,\ell}^- \alpha_{\bar{\imath},\ell}^+}{\alpha_{\bar{\imath},\ell}^-}}{\alpha_{i,\ell}^- - \alpha_{\bar{\imath},\ell}^+}$, *then*

$$p_{0,\ell}^{(3)} = [\nu_{i,\ell}]^+ \,, \quad p_{i,\ell}^{(3)} = 0 \,. \tag{19d}$$

If $\Lambda_{i,\ell} < 0$, *then*

if $\frac{w_i}{w_0} > \frac{\mu_i \alpha_{i,\ell}^- + \mu_{\bar{\imath}} \alpha_{\bar{\imath},\ell}^-}{\alpha_{i,\ell}^- - \alpha_{\bar{\imath},\ell}^+}$, *then*

$$p_{0,\ell}^{(3)} = 0 \,, \quad p_{i,\ell}^{(3)} = [\beta_{i,\ell}]^+ \,. \tag{19e}$$

Otherwise, if $\frac{w_i}{w_0} \leq \frac{\mu_i \alpha_{i,\ell}^- + \mu_{\bar{\imath}} \alpha_{\bar{\imath},\ell}^-}{\alpha_{i,\ell}^- - \alpha_{\bar{\imath},\ell}^+}$, *then*

$$p_{0,\ell}^{(3)} = [\nu_{i,\ell}]^+ \,, \quad p_{i,\ell}^{(3)} = 0 \,. \tag{19f}$$

For $\ell \in S_3$,

$$p_{0,\ell}^{(3)} = [\nu_{1,\ell}]^+ \tag{19g}$$

where λ *is chosen to satisfy the total power constraint (7), and* μ *is chosen to satisfy* $R_{01}^{\max}\big(\boldsymbol{p}^{(3)}\big) = R_{02}^{\max}\big(\boldsymbol{p}^{(3)}\big)$.

Proof: See the Appendix. ∎

Table I summarizes the power allocation algorithm solving (15). The algorithm includes three steps consisting of simple closed-form solutions of problems (P1)-(P3). Steps 1 and 2 require the optimization of λ, while Step 3 requires the optimization of both λ and $\mu \in (0,1)$. As $R_{01}^{\max}(\boldsymbol{p}^{(3)})$ and $R_{02}^{\max}(\boldsymbol{p}^{(3)})$ are monotonous functions versus both λ and μ, these optimizations can be performed efficiently for instance by a dichotomic search. Moreover, the two searches can be performed in cascade.

TABLE I
POWER ALLOCATION ALGORITHM.

Step 1	Compute $\boldsymbol{p}^{(1)}$ by (18). If $R_{01}^{\max}(\boldsymbol{p}^{(1)}) < R_{02}^{\max}(\boldsymbol{p}^{(1)})$, then $\boldsymbol{p}^* = \boldsymbol{p}^{(1)}$. Otherwise, go to *Step 2*.
Step 2	Compute $\boldsymbol{p}^{(2)}$ by (18) with user indices exchanged. If $R_{01}^{\max}(\boldsymbol{p}^{(2)}) > R_{02}^{\max}(\boldsymbol{p}^{(2)})$, then $\boldsymbol{p}^* = \boldsymbol{p}^{(2)}$. Otherwise, go to *Step 3*.
Step 3	Compute $\boldsymbol{p}^{(3)}$ by (19). Then $\boldsymbol{p}^* = \boldsymbol{p}^{(3)}$.

Note that the power allocation algorithm can be used also for perfect CSIT by letting $\alpha_{i,\ell}^- = \alpha_{i,\ell}^+$.

IV. Numerical Results

In this section, we validate the analytical results by considering a system where the number of sub-channels L and the total power P are both fixed to 64. Each sub-channel is Rayleigh fading, thus, the powers of the sub-channel gains $h_{1,\ell}^2$ and $h_{2,\ell}^2$ are exponentially distributed with means $\mathrm{SNR}_1 = \mathbb{E}\{\mathrm{h}_{1,\ell}^2\}$ and $\mathrm{SNR}_2 = \mathbb{E}\{\mathrm{h}_{2,\ell}^2\}$.

Fig. 2 shows a contour plot of the boundary surface for the three dimensional secrecy capacity averaged over the channel realizations with $\mathrm{SNR}_1 = \mathrm{SNR}_2 = 10$ dB and perfect CSIT. We remark that the surface of the secrecy capacity gets smaller as $\mathbb{E}[R_0]$ increases. Moreover, the secrecy capacity region is symmetric for the same average SNR values of both users.

We then compare the algorithm with two other schemes. The first one is uniform power allocation over the sub-channels and over the three messages. The second scheme is the power allocation algorithm proposed in [15] which maximizes the sum secrecy-rate in the presence of two confidential messages but without a common message. In order to compare [15] with our approach, we first assign power $P/3$ to transmit the common message and then we split the remaining power $2\,P/3$ between the two confidential messages according to the algorithm of [15]. Fig. 3.a compares the average weighted sum-rate (with $w_0 = w_1 = w_2$) of our algorithm with the average sum-rate of the two schemes versus $\mathrm{SNR} = \mathrm{SNR}_1 = \mathrm{SNR}_2$. The optimal algorithm provides a significant advantage mainly at high SNR range.

Lastly, in Fig. 3.b we show the rates when imperfect CSIT is available with $\sigma = 0.01$, as function of ϵ. We note that as ϵ increases the secret rates increases, as we are less restrictive on the illegitimate channel, while on the other hand the rate of the common message decreases.

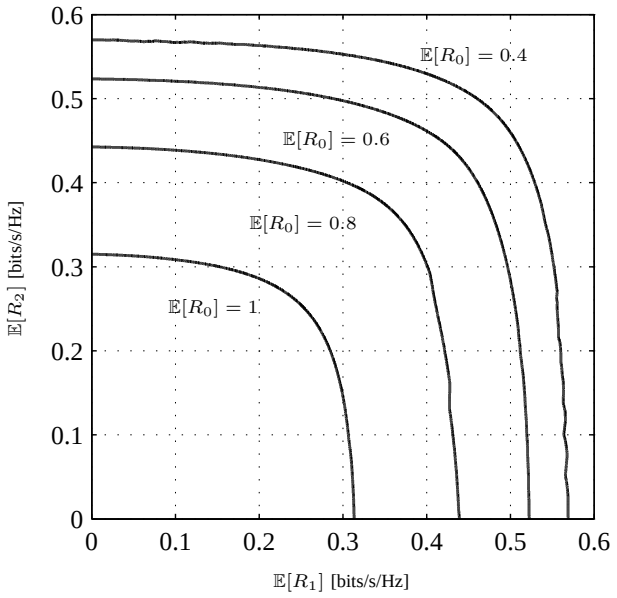
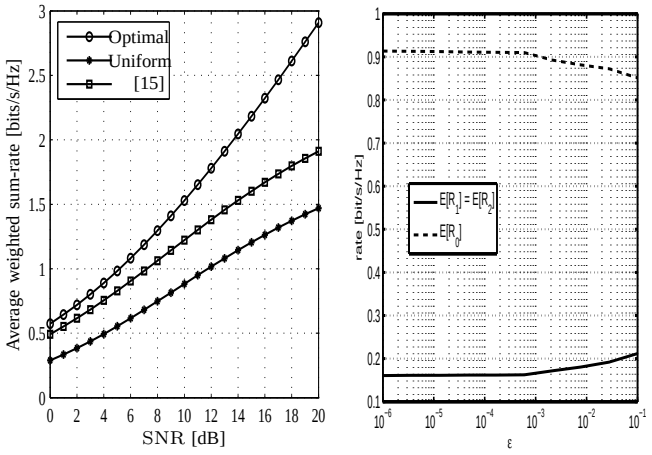


Fig. 2. Contour plot of the boundary surface of the secrecy capacity region.



a) b)

Fig. 3. a) Average weighted sum-rate ($w_0 = w_1 = w_2 = 1$) versus $\mathrm{SNR} = \mathrm{SNR}_1 = \mathrm{SNR}_2$ of some power allocation algorithms.

V. Conclusions

We have provided a characterization of the boundary for the secrecy capacity region of a parallel BCC with two confidential and one common messages by converting it into a power allocation problem. An almost closed-form solution to the problem has been provided, which can also be exploited in practical scenarios for resource allocation in OFDM systems with secrecy and fairness constraints. Comparison with existing power allocation schemes highlights the significant advantage of the optimal algorithm.

Appendix

We solve problems (P1)-(P3) by a technique based on deriving an upper bound on the Lagrangian operator and establishing power allocations that achieve the upper bound.

(P1) The Lagrangian $\mathcal{L}$ of (P1) is given by

$$\begin{aligned}\mathcal{L} = &\sum_{\ell=1}^{L} \frac{w_0}{2}\log\big(1+\frac{\alpha_{1,\ell}^{-}p_{0,\ell}}{1+\alpha_{1,\ell}^{-}[p_{1,\ell}+p_{2,\ell}]}\big)\\ &+\sum_{\ell\in S_1}\frac{w_1}{2}\log\big(1+\alpha_{1,\ell}^{-}p_{1,\ell}\big)-\frac{w_1}{2}\log\big(1+\alpha_{2,\ell}^{+}p_{1,\ell}\big)\\ &+\sum_{\ell\in S_2}\frac{w_2}{2}\log\big(1+\alpha_{2,\ell}^{-}p_{2,\ell}\big)-\frac{w_2}{2}\log\big(1+\alpha_{1,\ell}^{+}p_{2,\ell}\big)\\ &-\lambda\sum_{\ell=1}^{L}\big[p_{0,\ell}+p_{1,\ell}+p_{2,\ell}\big] \qquad (20)\end{aligned}$$

where $\lambda \geq 0$ is the Lagrange multiplier. For $\ell \in S_1$, the transmitter merely sends the common and the confidential messages M_1 (i.e., $p_{2,\ell}$=0). For $\ell \in S_2$, the transmitter sends the common and the confidential message M_2, (i.e. $p_{1,\ell}$=0). While, for $\ell \in S_3$, the transmitter sends only the common message. For $\ell \in S_1$, $p_{0,\ell}^{(1)}$ and $p_{1,\ell}^{(1)}$ need to maximize :

$$\begin{aligned}\mathcal{L}_1 = &\frac{w_0}{2}\log\big(1+\frac{\alpha_{1,\ell}^{-}p_{0,\ell}}{1+\alpha_{1,\ell}^{-}p_{1,\ell}}\big)+\frac{w_1}{2}\log\big(1+\alpha_{1,\ell}^{-}p_{1,\ell}\big)\\ &-\frac{w_1}{2}\log\big(1+\alpha_{2,\ell}^{+}p_{1,\ell}\big)-\lambda(p_{0,\ell}+p_{1,\ell}). \qquad (21)\end{aligned}$$

We denote by $u_{0,\ell}(\cdot)$ and $u_{1,\ell}(\cdot)$ the partial derivative of $\mathcal{L}_1$ with respect to $p_{0,\ell}$ and $p_{1,\ell}$, respectively:

$$u_{0,\ell}(x) = \frac{w_0}{2\ln 2}\frac{\alpha_{1,\ell}^{-}}{1+\alpha_{1,\ell}^{-}x}-\lambda \qquad (22)$$

$$u_{i,\ell}(x) = \frac{w_i}{2\ln 2}\left(\frac{\alpha_{i,\ell}^{-}}{1+\alpha_{i,\ell}^{-}x}-\frac{\alpha_{i,\ell}^{+}}{1+\alpha_{i,\ell}^{+}x}\right)-\lambda. \qquad (23)$$

Then, (21) can be rewritten as

$$\mathcal{L}_1 = \int_{p_{1,\ell}}^{p_{1,\ell}+p_{0,\ell}} u_{0,\ell}(x)\,dx + \int_{0}^{p_{1,\ell}} u_{1,\ell}(x)\,dx \qquad (24)$$

and upper bounded as

$$\mathcal{L}_1 \leq \int_{0}^{+\infty}\left[\max\{u_{0,\ell}(x), u_{1,\ell}(x)\}\right]^{+}\,dx. \qquad (25)$$

The root of $u_{0,\ell}(x)$ is $\gamma_{1,\ell}$ defined in (17b) while the largest root of $u_{1,\ell}(x)$ is $\beta_{1,\ell}$ defined in (17a). $u_{0,\ell}(x)$ and $u_{1,\ell}(x)$ intersect at the point $\zeta_{1,\ell}$ given by (17b). In the following, we consider two cases.

1) $\frac{w_1}{w_0} > \frac{\alpha_{1,\ell}^{-}}{\alpha_{1,\ell}^{-}-\alpha_{2,\ell}^{+}}$, i.e., $\zeta_{1,\ell}$ is positive.
   In this case, $u_{1,\ell}(0) > u_{0,\ell}(0)$. There are three possibilities to consider depending on the value of λ.
   a) If $u_{1,\ell}(0) < 0$, then both $u_{0,\ell}(x)$ and $u_{1,\ell}(x)$ are negative for $x > 0$, and (25) is achieved by $p_{0,\ell}^{(1)} = 0$ and $p_{1,\ell}^{(1)} = 0$.
   b) If $u_{1,\ell}(0) \geq 0$ and $\gamma_{1,\ell} < \zeta_{1,\ell}$, then (25) is achieved by $p_{0,\ell}^{(1)} = 0$ and $p_{1,\ell}^{(1)} = \beta_{1,\ell}$.
   c) If $\gamma_{1,\ell} \geq \zeta_{1,\ell}$, then (25) is achieved by $p_{0,\ell}^{(1)} = \gamma_{1,\ell} - \zeta_{1,\ell}$ and $p_{1,\ell}^{(1)} = \zeta_{1,\ell}$.

In summary, we obtain (18a).

2) $\frac{w_1}{w_0} \leq \frac{\alpha^-_{1,\ell}}{\alpha^-_{1,\ell}-\alpha^+_{2,\ell}}$, i.e., $\zeta_{1,\ell}$ is negative.
In this case, $u_{0,\ell}(0) \geq u_{1,\ell}(0)$.
   a) If $u_{0,\ell}(0) \leq 0$, then (25) is achieved by $p^{(1)}_{0,\ell} = 0$ and $p^{(1)}_{1,\ell} = 0$.
   b) If $u_{0,\ell}(0) > 0$, then (25) is achieved by $p^{(1)}_{0,\ell} = \gamma_{1,\ell}$ and $p^{(1)}_{1,\ell} = 0$.

   In summary, we obtain (18b).

For $\ell \in S_2$, $p^{(1)}_{0,\ell}$ and $p^{(1)}_{2,\ell}$ need to maximize :

$$\mathcal{L}_2 = \frac{w_0}{2}\log\big(1+\frac{\alpha^-_{1,\ell}p_{0,\ell}}{1+\alpha^-_{1,\ell}p_{2,\ell}}\big) + \frac{w_2}{2}\log\big(1+\alpha^-_{2,\ell}p_{2,\ell}\big) - \frac{w_2}{2}\log\big(1+\alpha^+_{1,\ell}p_{2,\ell}\big) - \lambda(p_{0,\ell}+p_{2,\ell}). \quad (26)$$

Then, we obtain, analogously to (25)

$$\mathcal{L}_2 \leq \int_0^{+\infty} \big[\max\big\{u_{0,\ell}(x), u_{2,\ell}(x)\big\}\big]^+ \, dx. \quad (27)$$

The largest root of $u_{2,\ell}(x)$ is $\beta_{2,\ell}$ given by (17a). $u_{0,\ell}(x)$ and $u_{2,\ell}(x)$ intersect at two points. The largest point $\theta_{2,\ell}$ is given by (17d). We consider two cases depending on the sign of the two points.

1) $\frac{w_2}{w_0} > \frac{\alpha^-_{1,\ell}}{\alpha^+_{2,\ell}-\alpha^+_{1,\ell}}$, *i.e.*, one point is negative and the other is positive.
In this case, $u_{2,\ell}(0) > u_{0,\ell}(0)$. There are three possibilities to consider.
   a) If $u_{2,\ell}(0) < 0$, then both $u_{0,\ell}(x)$ and $u_{2,\ell}(x)$ are negative for $x > 0$, and (27) is achieved by $p^{(1)}_{0,\ell} = 0$ and $p^{(1)}_{2,\ell} = 0$.
   b) If $u_{2,\ell}(0) \geq 0$ and $\gamma_{1,\ell} < \theta_{2,\ell}$, then (27) is achieved by $p^{(1)}_{0,\ell} = 0$ and $p^{(1)}_{2,\ell} = \beta_{2,\ell}$.
   c) If $\gamma_{1,\ell} \geq \theta_{2,\ell}$, then (27) is achieved by $p^{(1)}_{0,\ell} = \gamma_{1,\ell} - \theta_{2,\ell}$ and $p^{(1)}_{2,\ell} = \theta_{2,\ell}$.

   In summary, we obtain (18c).

2) $\frac{w_2}{w_0} \leq \frac{\alpha^-_{1,\ell}}{\alpha^+_{2,\ell}-\alpha^+_{1,\ell}}$, *i.e.*, the two intersection points are negative.
In this case, $u_{0,\ell}(0) \geq u_{2,\ell}(0)$. There are two possibilities to consider.
   a) If $u_{0,\ell}(0) \leq 0$, then (27) is achieved by $p^{(1)}_{0,\ell} = 0$ and $p^{(1)}_{2,\ell} = 0$.
   b) If $u_{0,\ell}(0) > 0$, then (27) is achieved by $p^{(1)}_{0,\ell} = \gamma_{1,\ell}$ and $p^{(1)}_{2,\ell} = 0$.
      In summary, we obtain (18d).

   The case that the two points are positive is not possible.

For $\ell \in S_3$, $p^{(1)}_{0,\ell}$ need to maximize

$$\mathcal{L}_3 = \frac{w_0}{2}\log\big(1+\alpha^-_{1,\ell}p_{0,\ell}\big) - \lambda\, p_{0,\ell}. \quad (28)$$

$\mathcal{L}_3$ can be upper bounded by

$$\mathcal{L}_3 = \int_0^{p_{0,\ell}} u_{0,\ell}(x)\, dx \leq \int_0^{+\infty} [u_{0,\ell}(x)]^+ \, dx. \quad (29)$$

If $u_{0,\ell}(0) < 0$, then the upper bound on $\mathcal{L}_3$ is achieved by $p^{(1)}_{0,\ell} = 0$. If $u_{0,\ell}(0) \geq 0$, the upper bound is achieved in this case by $p^{(1)}_{0,\ell} = \gamma_{1,\ell}$. In summary, we obtain (18e).

The Lagrange parameter λ is chosen to satisfy the power constraint with equality.

The solution of (P2) and (P3) is obtained in a similar fashion to that of (P1) and is not reported here for the sake of conciseness.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] P. K. Gopala, L. Lai, and H. ElGamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[3] N. Laurenti, S. Tomasin, and F. Renna, "Resource allocation for secret transmissions on parallel Rayleigh channels," in *Proc. IEEE Int. Conf. on Commun. (ICC)*, Sydney, Australia, June 2014.

[4] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Foren. Sec.*, vol. 7, no. 4, pp. 1354–1367, Aug. 2012.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[6] F. Renna, N. Laurenti, and S. Tomasin, "Achievable secrecy rates over MIMOME Gaussian channels with GMM signals in low-noise regime," in *Proc. Global Wireless Summit (GWS'14)*, Aalborg, Denmark, May 2014.

[7] A. Mukherjee, S. Ali., A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

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

[9] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[10] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5669–5680, Sep. 2012.

[11] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.

[12] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.

[13] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, April 2011.

[14] ——, "Secure broadcasting using multiple antennas," *Journal of Commun. and Networks*, vol. 12, no. 5, pp. 411–432, Oct. 2010.

[15] E. Jorswieck and S. Gerbracht, "Secrecy rate region of downlink OFDM systems: Efficient resource allocation," in *Proc. 14th Int. OFDM-Workshop (InOWo)*, Hamburg, Germany, Sep. 2009.

[16] E. Ekrem and S. Ulukus, "Ergodic secrecy capacity region of the fading broadcast channel," in *IEEE Int. Conf. Commun. (ICC'09)*, Dresden, Germany, June 2009, pp. 1–5.

[17] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4529–4542, Oct. 2009.

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