Power Allocation in Multiuser Parallel Gaussian Broadcast Channels With Common and Confidential Messages

Power Allocation in Multiuser Parallel Gaussian Broadcast Channels with Common and Confidential Messages

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 over parallel channels where the transmitter sends $K+1$ messages: one common message to all users, and K confidential messages to each user which need to be kept secret from all unintended users. We assume partial channel state information at the transmitter, stemming from noisy channel estimation. Our main goal is to design a power allocation algorithm in order to maximize the weighted sum rate of common and confidential messages under a total power constraint. The resulting problem for joint encoding across channels is formulated as the cascade of two problems, the inner min problem being discrete, and the outer max problem being convex. Thereby, efficient algorithms for this kind of optimization program can be used as solutions to our power allocation problem. For the special case $K=2$, we provide an almost closed-form solution, where only two single variables must be optimized, e.g., through dichotomic searches. To reduce computational complexity, we propose three new algorithms maximizing the weighted sum rate achievable by two sub-optimal schemes that perform per-user and per-channel encoding. By numerical results, we assess the performance of all proposed algorithms as a function of different system parameters.

Index Terms

Broadcast communication, physical layer security, parallel channels, power allocation, multiuser system.

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.

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 breakthrough idea behind this approach is to exploit the characteristics of the wireless channel, in order to reinforce security in wireless communications. The basic concepts were laid out by the pioneering work of Wyner [1]. He introduced the *wiretap* channel model in which the transmitter aims at reliably sending 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 leaving the eavesdropper with no information on the message. Recently, the wiretap channel has witnessed a renewed interest and many research works have investigated the secrecy capacity of wireless fading [2]–[4], parallel [5]–[8] and multiple-input multiple-output (MIMO) channels [9]–[12]. 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 multiuser context (see [13] for a survey).

An important scenario for multiuser physical layer security is the *broadcast channel with confidential messages (BCC)* introduced in [14]. An extensive research work has been made to characterize the secrecy capacity region of fading, parallel, and MIMO BCC for a system with 2 or 3 receivers [15]–[18]. Related works about the compound wiretap channel [19]–[21] offer a general framework that captures the BCC scenario. In the last few years, many works have appeared in literature for a larger BCC with practical number of receivers. In [22]–[25], the authors attempted to characterize the complete secrecy capacity region when transmitting to an arbitrary number of legitimate receivers for different channels and various network topologies. In [26], the authors analyzed the role of multiuser diversity for secure communications in fading channel. Several works [27]–[34] have examined physical layer security in multiuser MIMO networks. Linear precoding [29], [30], [32] and non-linear Tomlinson-Harashima precoding [33] techniques have been considered for secrecy rate maximization. In [31], the beamforming and user selection problems were studied in multicast multiple-input single-output (MISO) channel, where the transmitter broadcasts a common confidential message to legitimate users and unauthorized users attempt to eavesdrop the message. The performance of low-complexity heuristic user selection algorithms in providing physical layer security was evaluated in [27]. Opportunistic scheduling was introduced in [34] to enhance physical layer security with transmit antenna selection. In [35], the authors solved the resource allocation problem in orthogonal frequency division multiple access (OFDMA) broadcast network with the objective of maximizing average communication rate to normal users while maintaining an average secrecy rate for each individual secure user in the network. A resource allocation algorithm for OFDMA broadcast system was introduced in [36] maximizing the average outage capacity in the presence of multiple eavesdroppers. In [37], a power allocation algorithm was proposed for the orthogonal frequency division multiplexing (OFDM) broadcast system, which increases the sum rate to multiple legitimate receivers in the presence of an eavesdropper, while in [38] a multicarrier multicast system with multiple multicast groups was considered where each multicast group may contain a different number of users.

In this paper, we consider parallel BCC with K receivers. This scenario can model some practical wireless systems such as an OFDMA downlink in a cellular network. The transmitter aims to reliably send a common message to all receiving users and K separate confidential messages, one for each user. The confidential messages need to be kept secret from all unintended users. All receivers are legitimate users in the network; but curious in the sense that they may attempt to learn other users' messages. We further consider the case in which only partial channel state information is available before transmission, stemming from a noisy estimate of the channels. To the best of authors' knowledge, an analysis of this generic communication scenario in multiuser setting is missing in literature. We generalize an earlier version of our work [39] that considered parallel BCC with 2 receivers. We derive the achievable rates for the common and confidential messages by joint encoding across channels, where partial channel state information is addressed by adding a margin to the estimated channel gains. The problem of interest is to design a power allocation algorithm maximizing the weighted sum rate under a total power constraint. Note that this metric is of interest for resource allocation in OFDMA systems with a fairness constraint, where the weights are selected in order to enforce the desired fairness. The power allocation increasing the weighted sum rate achieved by joint encoding is formulated as the cascade of two problems, the inner min problem being discrete, and the outer max problem being convex. In the following we denote this kind of problems as *convex discrete max-min program* problems. As a result, efficient algorithms solving this kind of program can be used as solutions to our power allocation problem. For the special case $K = 2$, we are able to provide an almost closed-form solution, where two real variables must be optimized, e.g., through dichotomic searches. Due to the heavy computational cost of power allocation for joint encoding, we propose three new algorithms with lower complexity. These sub-optimal algorithms maximize the weighted sum rate achievable by letting encoded messages span only groups of channels. For the generic case, the problem is solved using numerical tools and having a significantly lower complexity with respect to joint coding. When messages are encoded on each channel separately (i.e, groups comprise only one channel), we have an almost closed-form solution with a single variable to be optimized. The performance of all proposed algorithms is assessed in terms of achievable common and secrecy rates.

The rest of the paper is organized as follows. Section II sets up the system model and formulates the problem. Section III introduces power allocation for joint encoding. In Sections IV and V, three power allocation algorithms are proposed for per-user encoding and per-channel encoding. In Section VI, numerical results are presented. Lastly, Section VII concludes the paper.

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. For a finite set S, the cardinality of S is denoted $|S|$.

II. System Model

We consider a scenario where one transmitter aims at conveying K confidential messages to K receivers over L parallel channels (BCCs scenario) [14], [40]. The parallel channels model for example an OFDM system. As illustrated in Fig. 1, the transmitter sends a common message and K separate confidential messages. The common message M_0 is intended for all receivers, while confidential message M_k is intended only for receiver $k \in \mathcal{K} = \{1, \dots, K\}$ and needs to be kept secret from all other receivers.

The transmitter sends the complex symbol x_ℓ on channel $\ell = 1, \dots, L$.The channel input is subject to the statistical total power constraint

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

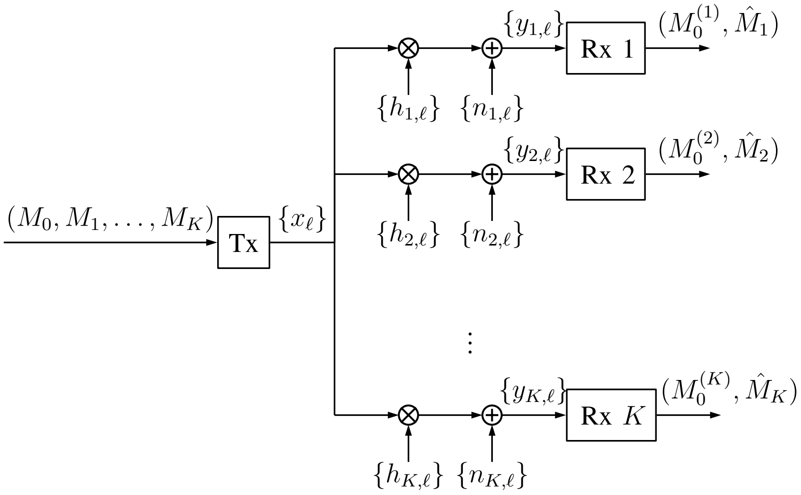


Fig. 1. BCCs with one common message M_0 and K confidential messages M_k, $k \in \mathcal{K}$, mixers and adders operate in parallel over the L channels.

The power $p_{k,\ell}$ is allocated on channel ℓ for message M_k, $k = 0, \dots, K$. Let $\boldsymbol{p}$ be the $(K+1) \times L$ matrix with entries $p_{k,\ell}$, $k = 0, \dots, K$, $\ell = 1, \dots, L$. Set $\mathcal{P}$ includes all power allocation matrices $\boldsymbol{p}$ that satisfy the power constraint (1), i.e.,

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

Moreover, we assume that channels are quasi-static, i.e., they remain constant over the entire duration of a single packet. On channel ℓ at receiver $k \in \mathcal{K}$, we obtain

$$y_{k,\ell} = h_{k,\ell}\, x_\ell + n_{k,\ell}\,, \tag{3}$$

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

$$\hat{h}_{k,\ell} = h_{k,\ell} + \eta_{k,\ell}\,, \tag{4}$$

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

$$f_{\alpha_{k,\ell}|\hat{h}_{k,\ell}}(a|b) = \frac{\int_{-\pi}^{\pi} f_\eta(b - \sqrt{a}e^{j\phi}) f_{h_{k,\ell}}(\sqrt{a}e^{j\phi})\, d\phi}{2\left[f_{h_{k,\ell}} \otimes f_\eta\right](b)} . \tag{5}$$

where $\otimes$ denotes the convolution operation.

A $(2^{nR_0}, 2^{nR_1}, \dots, 2^{nR_K}, n)$ code consists of the following:

1) $K+1$ message sets: $\mathcal{M}_k = \{1, 2, \dots, 2^{nR_k}\}$ with each message M_k uniformly distributed over the set $\mathcal{M}_k$, $k = 0, \dots, K$.
2) one stochastic encoder at the transmitter that maps each message vector $(M_0, M_1, \dots, M_K)$ to a codeword $\boldsymbol{X}^n$ representing the group of vectors $[\boldsymbol{X}[1], \dots, \boldsymbol{X}[n]]$. The vector $\boldsymbol{X}[m]$, $m = 1, \dots, n$ contains the symbols $\{x_\ell\}$ at the time index m.
3) K decoders: each at one receiver that maps a received sequence $\boldsymbol{Y}_k^n$ to a couple of messages $(M_0^{(k)}, \hat{M}_k) \in \mathcal{M}_0 \times \mathcal{M}_k$ for $k \in \mathcal{K}$. The received sequence $\boldsymbol{Y}_k^n$ represents the group of received vectors $[\boldsymbol{Y}_k[1], \dots, \boldsymbol{Y}_k[n]]$ where $\boldsymbol{Y}_k[m]$, $m = 1, \dots, n$ contains the received symbols $\{y_{k,\ell}\}$ at time index m.

The reliability condition of the confidential message M_k at the intended receiver is ensured when $\lim_{n\to\infty} P[\hat{M}_k \neq M_k] = 0$ and the reliability condition of the common message is ensured when $\lim_{n\to\infty} P[M_0^{(k)} \neq M_0] = 0$, $k \in \mathcal{K}$. The weak secrecy to the unintended user j of the confidential message M_k is guaranteed by ensuring a vanishing leakage rate as $n \to \infty$ [1], [14], i.e., we require

$$\lim_{n\to\infty} \frac{1}{n} \mathbb{I}(M_k; \boldsymbol{Y}_j^n) = 0 \tag{6}$$

for $j \neq k$. A rate vector $(R_0, R_1, \dots, R_K)$ is *achievable* if there exists a sequence of codes such that as n goes to infinity, the reliability requirement is fulfilled for all intended receivers and the secrecy requirement is fulfilled with respect to all unintended receivers.

A. Achievable Rates

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.

In particular, the transmitter can compute upper and lower bounds on the channel power gains $\alpha^+_{k,\ell}$ and $\alpha^-_{k,\ell}$ 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.,

$$\mathrm{P}\left[\alpha_{k,\ell} > \alpha^+_{k,\ell} \middle| \hat{h}_{k,\ell}\right] < \varepsilon\,, \quad \mathrm{P}\left[\alpha_{k,\ell} < \alpha^-_{k,\ell} \middle| \hat{h}_{k,\ell}\right] < \varepsilon\,. \tag{7}$$

Then, $\alpha^-_{k,\ell}$ will be considered as the channel power gain to the intended receiver, while $\alpha^+_{k,\ell}$ is the channel power gain to the unintended receiver. The probabilities in (7) can be computed using the pdf (5). Note that when perfect CSI is available $\alpha^+_{k,\ell} = \alpha^-_{k,\ell}$.

The multicast channel with multiple eavesdroppers can be seen as a compound wiretap channel [19], [20], in which the transmitter sends common message to all receivers and keeps the message secret from all eavesdroppers. When transmitting message M_k, the system can be modeled as a parallel compound wiretap channels with one receiver and $K-1$ eavesdroppers. Let us define

$$\mathcal{L}_{k/j} = \left\{\ell : \alpha^-_{k,\ell} \geq \alpha^+_{j,\ell};\ j \neq k\right\} \tag{8}$$

and

$$R_{k/j}(\boldsymbol{p}) = \sum_{\ell \in \mathcal{L}_{k/j}} \log\bigl(1 + \alpha^-_{k,\ell}\, p_{k,\ell}\bigr) - \log\bigl(1 + \alpha^+_{j,\ell}\, p_{k,\ell}\bigr)\,. \tag{9}$$

By applying the results in [19] an outer bound on the achievable secrecy rate of message M_k over the deterministic channels $\{\alpha^-_{k,\ell}, \alpha^+_{k,\ell}\}$, for a given power allocation $\boldsymbol{p}$ is

$$R^{\max}_k(\boldsymbol{p}) = \min_{j \neq k; 1 \leq j \leq K} R_{k/j}(\boldsymbol{p})\,. \tag{10}$$

From (7) we can conclude that with probability larger than $(1-\epsilon)^{KL}$ the channel gains are such that the secrecy rate is upper bounded by (10). However, since we imposed a probabilistic constraint on the channel gains rather than the secrecy rate itself, $R^{\max}_k(\boldsymbol{p})$ is not an outage bound on the secrecy rate. Al already mentioned, this approach leads to easier computations, while a comparison with an outage secrecy bound is left for future study. Moreover, in the special case of full CSI ($\epsilon = 0$), (10) is an outer bound, and we will use it extensively in Section VI.

The work [41] studied the maximum common message rate over parallel broadcast channels and showed that the expression is given by the capacity of the worst user. In our scenario, the common message is multiplexed with the confidential messages. The decoding strategy consists to reconstruct the common message first, by treating confidential messages as noise. Then, the common message is subtracted and the confidential message is decoded [15]. We define for $k \in \mathcal{K}$,

$$R_{0k}(\boldsymbol{p}) = \sum_{\ell=1}^{L} \log\bigl(1 + \alpha_{k,\ell}^{-} p_{0,\ell} + \alpha_{k,\ell}^{-} \sum_{i=1}^{K} p_{i,\ell}\bigr) - \log\bigl(1 + \alpha_{k,\ell}^{-} \sum_{i=1}^{K} p_{i,\ell}\bigr) \,. \tag{11}$$

The maximum common message rate for a given power allocation $\boldsymbol{p}$ can be expressed as [41]

$$\begin{aligned} R_0^{\max}(\boldsymbol{p}) &= \min_{k\in\mathcal{K}} \sum_{\ell=1}^{L} \log\left(1 + \frac{\alpha_{k,\ell}^{-} p_{0,\ell}}{1 + \alpha_{k,\ell}^{-} \sum_{i=1}^{K} p_{i,\ell}}\right) \\ &= \min_{k\in\mathcal{K}} \sum_{\ell=1}^{L} \log\left(\frac{1 + \alpha_{k,\ell}^{-} p_{0,\ell} + \alpha_{k,\ell}^{-} \sum_{i=1}^{K} p_{i,\ell}}{1 + \alpha_{k,\ell}^{-} \sum_{i=1}^{K} p_{i,\ell}}\right) \\ &= \min_{k\in\mathcal{K}} \; R_{0k}(\boldsymbol{p}) \,. \end{aligned} \tag{12}$$

We point out that the above communication rates are achieved by using joint encoding across the channels. Also (12) must be considered as a bound on the rate that can be achieved under constraints (7) on the channel gain, and in general is not a secrecy outage bound.

B. *Problem Statement*

We define the rate region $\mathcal{R}^{\text{outer}}$ as follows

$$\mathcal{R}^{\text{outer}} = \bigcup_{\boldsymbol{p}\in\mathcal{P}} \left\{[R_0, R_1, \ldots, R_K] \middle|\, 0 \le R_k \le R_k^{\max}(\boldsymbol{p});\; k = 0, \ldots, K\right\} \,. \tag{13}$$

The region $\mathcal{R}^{\text{outer}}$ is a convex set and any point on its boundary can be attained by maximizing a weighted sum rate. In fact, for weights $w_k \ge 0$, $k = 0, \ldots, K$, the corresponding boundary point can be obtained by solving the following optimization problem

$$\boldsymbol{p}^* = \arg\max_{\boldsymbol{p}\in\mathcal{P}} \sum_{k=0}^{K} w_k R_k^{\max}(\boldsymbol{p}). \tag{14}$$

Then, the boundary point is given by the vector $[R_0^{\max}(\boldsymbol{p}^*), R_1^{\max}(\boldsymbol{p}^*), \ldots, R_K^{\max}(\boldsymbol{p}^*)]$. Varying the weights allows to reach all the boundary points. With the above problem formulation, channel ℓ can be used to transmit multiple multiplexed confidential messages. When receiver k decodes its own confidential message, the secrecy rate of message M_k is reduced if interference from other confidential messages is present. However, with the expression (10), we ignore interference coming from multiplexed confidential messages on the same channel. Clearly, the boundary of region $\mathcal{R}^{\text{outer}}$ provides an outer bound to the set of achievable communication rates in the considered scenario.

III. Power allocation for joint encoding

Our goal is to provide a solution to the power allocation problem (14). We first observe that $R_0^{\max}(\boldsymbol{p})$ depends on the lowest channel power gain among all users. By defining the sets $\mathcal{J}_k = \{j = 1, \ldots, K;\, j \neq k\}$, for $k \in \mathcal{K}$ and

$$F_{\boldsymbol{a}}(\boldsymbol{p}) = w_0 R_{0a_0}(\boldsymbol{p}) + \sum_{k=1}^{K} w_k R_{k/a_k}(\boldsymbol{p})\,, \tag{15}$$

where $\boldsymbol{a} = [a_0, \ldots, a_K] \in \mathcal{A} = \mathcal{K} \times \mathcal{J}_1 \times \ldots \times \mathcal{J}_K$. Problem (14) can be rewritten as

$$\boldsymbol{p}^* = \arg\max_{\boldsymbol{p}\in\mathcal{P}} \min_{\boldsymbol{a}\in\mathcal{A}} F_{\boldsymbol{a}}(\boldsymbol{p})\,. \tag{16}$$

Therefore, the power allocation problem is formulated as the standard convex discrete max-min optimization problem [42] where the number of variables is $L(K+1)$ and the cardinality of the discrete space is $|\mathcal{A}| = K(K-1)^K$. Since the objective function $\min_{\boldsymbol{a}\in\mathcal{A}} F_{\boldsymbol{a}}(\boldsymbol{p})$ is not differentiable, max-min belongs to the class of non-differentiable optimization problem. However, it can be converted to a smooth constrained optimization problem as follows

$$\begin{aligned} \boldsymbol{p}^* = &\arg\max_{\boldsymbol{p}\in\mathcal{P}} \quad z \\ \text{s.t.} \qquad & F_{\boldsymbol{a}}(\boldsymbol{p}) \geq z, \quad \boldsymbol{a} \in \mathcal{A}\,. \end{aligned} \tag{17}$$

We can see from (17) that the cardinality of the discrete space is an important parameter as it translates the number of constraints which grows exponentially versus the number of users in our case.

A vast literature has investigated efficient algorithms solving the discrete max-min problem [43]–[47]. One common approach deeply studied [43]–[45] is sequential quadratic programming (SQP). Starting from an initial approximation of the solution, a quadratic programming problem is solved at each iteration, yielding a direction in the search space. To this direction, a vector is obtained in order to produce a sufficient increase of a merit function. Another common approach in literature is smoothing techniques [46], [47]. A smoothing function called the exponential penalty function or aggregate function is used to approximate the objective function. Therefore, these algorithms can be implemented as solution to our power allocation problem.

A. Power Allocation for $K = 2$

For the case of two users ($K = 2$), an almost closed-form solution to the power allocation problem (14) is provided. In fact, the max-min formulation (16) in this case is performed over a discrete space whose cardinality $|\mathcal{A}| = 2$. The max-min optimization can be solved by using an approach similar to that of [40]. The particular result is provided in the following lemma, whose proof is not reported as it follows the same steps of [40].

Lemma 1. *The solution of* (16) *when $K = 2$ also solves one of the following three sub-problems:*

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

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

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

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

$$\boldsymbol{p}^* = \begin{cases} \boldsymbol{p}^{(1)} & \textit{if}\ R_{01}(\boldsymbol{p}^{(1)}) < R_{02}(\boldsymbol{p}^{(1)}) \\ \boldsymbol{p}^{(2)} & \textit{if}\ R_{01}(\boldsymbol{p}^{(2)}) > R_{02}(\boldsymbol{p}^{(2)}) \\ \boldsymbol{p}^{(3)} & \textit{if}\ R_{01}(\boldsymbol{p}^{(3)}) = R_{02}(\boldsymbol{p}^{(3)}) \end{cases}. \tag{18}$$

We now focus on the solution of sub-problems (P1)-(P3). For $\ell = 1, \ldots, L$ and $k = 1, 2$, let $\bar{k} = 2$ if $k = 1$ and $\bar{k} = 1$ if $k = 2$, let $\delta_{k,\ell} = 1/\alpha^{+}_{\bar{k},\ell} - 1/\alpha^{-}_{k,\ell}$, let $\rho_k = \rho$ if $k = 1$ and $\rho_k = 1 - \rho$ if $k = 2$, $\lambda \geq 0$, and

$$\Omega_{k,\ell}(\lambda) = \frac{1}{2}\left[\delta_{k,\ell}\left(\delta_{k,\ell} + \frac{4w_k}{\lambda \ln 2}\right)\right]^{1/2} - \frac{1}{2}\left(\frac{1}{\alpha^{+}_{k,\ell}} + \frac{1}{\alpha^{-}_{k,\ell}}\right) \tag{19a}$$

$$\Upsilon_{k,\ell}(\lambda) = \frac{w_0}{\lambda \ln 2} - \frac{1}{\alpha^{-}_{k,\ell}} \tag{19b}$$

$$\Xi_{k,\ell} = \frac{w_k}{w_0}\delta_{k,\ell} - \frac{1}{\alpha^{+}_{\bar{k},\ell}} \tag{19c}$$

$$\omega_{k,\ell} = \left[\left(\frac{w_k}{w_0}\right)^2 + \frac{w_k}{w_0}\left(\frac{2\cdot(\frac{2}{\alpha^{-}_{\bar{k},\ell}} - \frac{1}{\alpha^{-}_{k,\ell}} - \frac{1}{\alpha^{+}_{\bar{k},\ell}})}{\frac{1}{\alpha^{+}_{\bar{k},\ell}} - \frac{1}{\alpha^{-}_{k,\ell}}}\right) + 1\right]\cdot\left[\frac{1}{\alpha^{+}_{\bar{k},\ell}} - \frac{1}{\alpha^{-}_{k,\ell}}\right]^2 \tag{19d}$$

$$\mathcal{U}_{k,\ell} = \frac{\frac{w_k}{w_0}\big(\frac{1}{\alpha^{+}_{\bar{k},\ell}} - \frac{1}{\alpha^{-}_{k,\ell}}\big) - \big(\frac{1}{\alpha^{+}_{\bar{k},\ell}} + \frac{1}{\alpha^{-}_{k,\ell}}\big) + \sqrt{\omega_{k,\ell}}}{2} \tag{19e}$$

$$\begin{aligned}\mathcal{T}_{k,\ell}(\rho) =& \big(\delta_{k,\ell}\big)^2\left(\frac{w_k}{w_0}\right)^2 + 2\frac{w_k}{w_0}\left[\delta_{k,\ell}\big(\frac{2-\rho_k}{\alpha^{-}_{\bar{k},\ell}} - \frac{\rho_{\bar{k}}}{\alpha^{-}_{k,\ell}} - \frac{1}{\alpha^{+}_{\bar{k},\ell}}\big)\right] \\ &+ \big(\delta_{k,\ell}\big)^2 + \rho_k\big(\frac{1}{\alpha^{-}_{\bar{k},\ell}} - \frac{1}{\alpha^{-}_{k,\ell}}\big)\left[\rho_k\big(\frac{1}{\alpha^{-}_{\bar{k},\ell}} - \frac{1}{\alpha^{-}_{k,\ell}}\big) - 2\big(\frac{1}{\alpha^{+}_{\bar{k},\ell}} - \frac{1}{\alpha^{-}_{\bar{k},\ell}}\big)\right]\end{aligned} \tag{19f}$$

$$\Phi_{k,\ell}(\rho) = \frac{\frac{w_k}{w_0}\delta_{k,\ell} - \big(\frac{1}{\alpha^{+}_{\bar{k},\ell}} + \frac{1}{\alpha^{-}_{k,\ell}}\big) - \rho_k\big(\frac{1}{\alpha^{-}_{\bar{k},\ell}} - \frac{1}{\alpha^{-}_{k,\ell}}\big) + \sqrt{\mathcal{T}_{k,\ell}(\rho)}}{2} \tag{19g}$$

$$\begin{aligned}\Psi_{k,\ell}(\lambda,\rho) =& \frac{1}{2}\left[\left(\frac{1}{\alpha^{-}_{\bar{k},\ell}} - \frac{1}{\alpha^{-}_{k,\ell}} - \frac{w_0}{\lambda\ln 2}\right)^2 + \frac{4w_0\rho_k}{\lambda\ln 2}\big(\frac{1}{\alpha^{-}_{\bar{k},\ell}} - \frac{1}{\alpha^{-}_{k,\ell}}\big)\right]^{1/2} \\ &- \frac{1}{2}\left(\frac{1}{\alpha^{-}_{\bar{k},\ell}} + \frac{1}{\alpha^{-}_{k,\ell}} - \frac{w_0}{\lambda\ln 2}\right).\end{aligned} \tag{19h}$$

The set $\mathcal{L}_0$ is defined by $\{1,\ldots,L\}\setminus\big(\mathcal{L}_{1/2}\cup\mathcal{L}_{2/1}\big)$. The main result for the solution of the optimization problem is provided by the following theorem.

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

(P1) *For $\ell\in\mathcal{L}_{1/2}$, if $\frac{w_1}{w_0} > \frac{\alpha^{-}_{1,\ell}}{\alpha^{-}_{1,\ell}-\alpha^{+}_{2,\ell}}$, then*

$$p^{(1)}_{0,\ell} = [\Upsilon_{1,\ell}(\lambda) - \Xi_{1,\ell}]^{+}\ ,\ p^{(1)}_{1,\ell} = [\min\{\Omega_{1,\ell}(\lambda);\Xi_{1,\ell}\}]^{+}\,. \tag{20a}$$

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

$$p^{(1)}_{0,\ell} = [\Upsilon_{1,\ell}(\lambda)]^{+}\ ,\quad p^{(1)}_{1,\ell} = 0\,. \tag{20b}$$

For $\ell\in\mathcal{L}_{2/1}$, if $\frac{w_2}{w_0} > \frac{\alpha^{-}_{1,\ell}}{\alpha^{-}_{2,\ell}-\alpha^{+}_{1,\ell}}$, then

$$p^{(1)}_{0,\ell} = [\Upsilon_{1,\ell}(\lambda) - \mathcal{U}_{2,\ell}]^{+}\ ,\ p^{(1)}_{2,\ell} = [\min\{\Omega_{2,\ell}(\lambda);\mathcal{U}_{2,\ell}\}]^{+}\,. \tag{20c}$$

Otherwise, if $\frac{w_2}{w_0} \le \frac{\alpha^-_{1,\ell}}{\alpha^-_{2,\ell} - \alpha^+_{1,\ell}}$*, then*

$$p^{(1)}_{0,\ell} = \left[\Upsilon_{1,\ell}(\lambda)\right]^+ \;, \quad p^{(1)}_{2,\ell} = 0 \,. \tag{20d}$$

For $\ell \in \mathcal{L}_0$*,*

$$p^{(1)}_{0,\ell} = \left[\Upsilon_{1,\ell}(\lambda)\right]^+ \;, \tag{20e}$$

where λ *is chosen to satisfy the total power constraint with equality.*

(P2) *Due to the symmetry (with respect to the user index) of sub-problems (P1) and (P2), solutions of (P2) and (P1) coincide, apart from an index (1 and 2) swap.*

(P3) *For* $\ell \in \mathcal{L}_{k/\bar{k}}$*, if* $\mathcal{T}_{k,\ell}(\rho) > 0$*, then*

if $\frac{w_k}{w_0} > \frac{\rho_k \alpha^-_{k,\ell} + \rho_{\bar{k}} \alpha^-_{\bar{k},\ell}}{\alpha^-_{k,\ell} - \alpha^+_{\bar{k},\ell}}$*, then*

$$p^{(3)}_{0,\ell} = \left[\Psi_{k,\ell}(\lambda,\rho) - \Phi_{k,\ell}(\rho)\right]^+ \;, \quad p^{(3)}_{k,\ell} = \left[\min\left\{\Omega_{k,\ell}(\lambda); \Phi_{k,\ell}(\rho)\right\}\right]^+ . \tag{21a}$$

Otherwise, if $\frac{w_k}{w_0} \le \frac{\rho_k \alpha^-_{k,\ell} + \rho_{\bar{k}} \alpha^-_{\bar{k},\ell}}{\alpha^-_{k,\ell} - \alpha^+_{\bar{k},\ell}}$*, then*

$$p^{(3)}_{0,\ell} = \left[\Psi_{k,\ell}(\lambda,\rho)\right]^+ \;, \quad p^{(3)}_{k,\ell} = 0 \,. \tag{21b}$$

If $\mathcal{T}_{k,\ell}(\rho) = 0$*, then*

if $\frac{w_k}{w_0} > \frac{\alpha^-_{k,\ell} + \rho_{\bar{k}} \alpha^+_{\bar{k},\ell} + \rho_k \frac{\alpha^-_{k,\ell} \alpha^+_{\bar{k},\ell}}{\alpha^-_{\bar{k},\ell}}}{\alpha^-_{k,\ell} - \alpha^+_{\bar{k},\ell}}$*, then* (21a).

Otherwise, if $\frac{w_k}{w_0} \le \frac{\alpha^-_{k,\ell} + \rho_{\bar{k}} \alpha^+_{\bar{k},\ell} + \rho_k \frac{\alpha^-_{k,\ell} \alpha^+_{\bar{k},\ell}}{\alpha^-_{\bar{k},\ell}}}{\alpha^-_{k,\ell} - \alpha^+_{\bar{k},\ell}}$*, then* (21b).

If $\mathcal{T}_{k,\ell}(\rho) < 0$*, then*

if $\frac{w_k}{w_0} > \frac{\rho_k \alpha^-_{k,\ell} + \rho_{\bar{k}} \alpha^-_{\bar{k},\ell}}{\alpha^-_{k,\ell} - \alpha^+_{\bar{k},\ell}}$*, then*

$$p^{(3)}_{0,\ell} = 0 \,, \quad p^{(3)}_{k,\ell} = \left[\Omega_{k,\ell}(\lambda)\right]^+ \;. \tag{21c}$$

Otherwise, if $\frac{w_k}{w_0} \le \frac{\rho_k \alpha^-_{k,\ell} + \rho_{\bar{k}} \alpha^-_{\bar{k},\ell}}{\alpha^-_{k,\ell} - \alpha^+_{\bar{k},\ell}}$*, then*

$$p^{(3)}_{0,\ell} = \left[\Psi_{k,\ell}(\lambda,\rho)\right]^+ \;, \quad p^{(3)}_{k,\ell} = 0 \,. \tag{21d}$$

For $\ell \in \mathcal{L}_0$*,*

$$p^{(3)}_{0,\ell} = \left[\Psi_{1,\ell}(\lambda,\rho)\right]^+ \;, \tag{21e}$$

TABLE I
POWER ALLOCATION ALGORITHM FOR 2 USERS.

```
compute $\boldsymbol{p}^{(1)}$ by (20)
 if $R_{01}(\boldsymbol{p}^{(1)})<R_{02}(\boldsymbol{p}^{(1)})$
  then $\boldsymbol{p}^* = \boldsymbol{p}^{(1)}$
 else compute $\boldsymbol{p}^{(2)}$ by (20) with user indices exchanged
  if $R_{01}(\boldsymbol{p}^{(2)})>R_{02}(\boldsymbol{p}^{(2)})$
   then $\boldsymbol{p}^* = \boldsymbol{p}^{(2)}$
  else compute $\boldsymbol{p}^* = \boldsymbol{p}^{(3)}$ by (21)
```

where $\rho \in (0,1)$ *is chosen to satisfy* $R_{01}\big(\boldsymbol{p}^{(3)}\big)=R_{02}\big(\boldsymbol{p}^{(3)}\big)$ *and* λ *is chosen to satisfy the total power constraint with equality.*

Proof. See Appendix A. □

Table I summarizes the power allocation algorithm. It includes three steps consisting of simple closed-form solutions of sub-problems (P1)-(P3). Steps 1 and 2 require the optimization of λ, while Step 3 requires the optimization of both λ and $\rho \in (0,1)$. These optimizations can be efficiently performed for instance by a dichotomic search. Moreover, the two searches can be performed in cascade.

The approach considered here to solve the problem for the case $K = 2$ can be generalized for an arbitrary number of users. For instance when $K = 3$, we should consider $2^{24} - 1$ sub-problems such as the sub-problems provided by Lemma 1. In fact, this number corresponds to all possible linear combinations of $3 \times 2^3 = 24$ objective functions. When K is large, the number of sub-problems increases super-exponentially. The extremely high number of sub-problems to consider limits the application of the approach even when $K = 3$. In addition, solving each sub-problem returns into searching the roots of a polynomial with degree K for the common message power allocation problem. It is not possible in this case to solve these sub-problems in closed-form.

IV. POWER ALLOCATION FOR PER-USER ENCODING

We remind that power allocation for joint encoding providing the outer bound to the set of achievable rates is formulated as the discrete max-min program where the cardinality of the discrete space is $|\mathcal{A}| = K(K-1)^K$. As observed, the complexity is super-exponential versus the number of users.

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

$$\begin{aligned} &\mathcal{L}_k = \left\{\ell : \alpha_{k,\ell}^- \geq \alpha_{j,\ell}^+ \, \forall j \in \mathcal{K}, j \neq k\right\}, \; k \in \mathcal{K} \\ &\mathcal{L}_0 = \{1, \ldots, L\} \setminus \cup_{k \in \mathcal{K}} \mathcal{L}_k \,. \end{aligned} \tag{22}$$

The idea behind per-user encoding is to encode the different messages jointly across channels belonging to $\mathcal{L}_k$ and independently among the different sets $\mathcal{L}_k$. In particular, message M_k is encoded jointly only across channels belonging to the set $\mathcal{L}_k$ and $p_{k,\ell} = 0$ if $\ell \notin \mathcal{L}_k$ where $k \in \mathcal{K}$. For $\ell \in \mathcal{L}_0$, $p_{k,\ell} = 0$ when $k \in \mathcal{K}$, i.e., only the common message is transmitted over channels $\ell \in \mathcal{L}_0$. Furthermore, we assign a fixed amount of power to each group of channels $\mathcal{L}_k$, in order to allow the parallel solutions of power allocation sub-problems. The resulting power allocation maximizing the weighted sum rate achieved by per-user encoding is still formulated as the discrete max-min program. However, the cardinality of the discrete space of each sub-problem is now reduced.

Let us now formally define the optimization problem for per-user encoding. For $k = 0, \ldots, K$, let us define the $(K+1) \times L$ power allocation matrix $\boldsymbol{\pi}^{(k)}$ such that

$$\pi_{i,\ell}^{(k)} = \begin{cases} p_{i,\ell} & \text{if } i \in \{0, k\} \text{ and } \ell \in \mathcal{L}_k \,, \\ 0 & \text{otherwise} \,. \end{cases} \tag{23}$$

When the messages are encoded by per-user encoding, the achievable rate of the common message for one group of channels $\mathcal{L}_k$ can be expressed as

$$R_{0k}^{(\mathrm{G})}(\boldsymbol{\pi}^{(k)}) = \min_{i \in \mathcal{K}} R_{0i}(\boldsymbol{\pi}^{(k)}) \,. \tag{24}$$

Then, the total common message rate is given by the sum over all groups of channels

$$R_0^{(\mathrm{G})}(\boldsymbol{p}) = \sum_{k=0}^{K} R_{0k}^{(\mathrm{G})}(\boldsymbol{\pi}^{(k)}) \,. \tag{25}$$

The confidential rates $R_k^{(\mathrm{G})}\big(\boldsymbol{\pi}^{(k)}\big)$ are given by (9) and (10) but with replacing $\mathcal{L}_{k/j}$ by $\mathcal{L}_k$. Furthermore, we subdivide power uniformly among groups of channels, proportionally to the number of channels per group. This can be translated into the additional constraint $(\mathcal{C}_k)$

$$(\mathcal{C}_k)\left\{\begin{array}{lll} \sum_{\ell\in\mathcal{L}_k}\left(\pi_{0,\ell}^{(k)}+\pi_{k,\ell}^{(k)}\right) & \leq & |\mathcal{L}_k|\,\frac{P}{L} \quad \text{if } k\in\mathcal{K} \\ \sum_{\ell\in\mathcal{L}_0}\pi_{0,\ell}^{(0)} & \leq & |\mathcal{L}_0|\,\frac{P}{L} \quad \text{if } k=0 \end{array}\right. . \tag{26}$$

The power allocation problem maximizing the weighted sum rate is then expressed as

$$\begin{aligned} \boldsymbol{p}^{(\mathrm{G})} = \arg\max_{\boldsymbol{p}} \quad & \sum_{k=1}^{K}\left[w_0 R_{0k}^{(\mathrm{G})}\left(\boldsymbol{\pi}^{(k)}\right)+w_k R_k^{(\mathrm{G})}\left(\boldsymbol{\pi}^{(k)}\right)\right]+w_0 R_{00}^{(\mathrm{G})}\left(\boldsymbol{\pi}^{(0)}\right) \\ \text{s.t.} \quad & \sum_{k=0}^{K}\sum_{\ell\in\mathcal{L}_k}\left(\pi_{0,\ell}^{(k)}+\pi_{k,\ell}^{(k)}\right)\leq P\,. \end{aligned} \tag{27}$$

Problem (27) can be solved by considering $K+1$ independent sub-problems where each one is reduced to channels belonging to the set $\mathcal{L}_k$. The power allocation solving the k-th sub-problem, $k\in\mathcal{K}$ consists in maximizing the weighted sum of a partial part of the common message rate and the confidential message rate of user k. While the power allocation solving the sub-problem for $k=0$ consists in maximizing a partial part of the common message rate. In formulas, the k-th sub-problem, $k\in\mathcal{K}$ is described as

$$\begin{aligned} \boldsymbol{\pi}_k^* = \arg\max_{\boldsymbol{\pi}^{(k)}} \quad & w_0 R_{0k}^{(\mathrm{G})}\left(\boldsymbol{\pi}^{(k)}\right)+w_k R_k^{(\mathrm{G})}\left(\boldsymbol{\pi}^{(k)}\right) \\ \text{s.t.} \quad & (\mathcal{C}_k)\,. \end{aligned} \tag{28}$$

For $k=0$, the sub-problem is described as

$$\begin{aligned} \boldsymbol{\pi}_0^* = \arg\max_{\boldsymbol{\pi}^{(0)}} \quad & R_{00}^{(\mathrm{G})}\left(\boldsymbol{\pi}^{(0)}\right) \\ \text{s.t.} \quad & (\mathcal{C}_0)\,. \end{aligned} \tag{29}$$

With this formulation, sub-problem (28) is a convex discrete max-min problem, where the number of unknowns is $2\,|\mathcal{L}_k|$ and the cardinality of the discrete space is $K(K-1)$. Meanwhile, sub-problem (29) is a convex discrete max-min problem, where the number of unknowns is $|\mathcal{L}_0|$ and the cardinality of the discrete space is K. Again, standard algorithms for discrete max-min program can be used. Therefore, the proposed algorithm consists in the solutions of $K+1$ independent sub-problems. As a result, the complexity of the algorithm is cubic versus the number of users. Compared to the outer bound provided by joint encoding, the complexity is significantly reduced.

TABLE II
POWER ALLOCATION FOR PER-USER ENCODING WITH MODIFIED COMMON MESSAGE POWER ALLOCATION.

```
solve the $K$ independent sub-problems (28)
  $p_{k,\ell}^{(MG)} = \pi_{k,\ell}^{*}$, for $k \in \mathcal{K}$ and $\ell \in \mathcal{L}_k$
compute constraint $(\mathcal{D})$ by (30)
solve problem (31) given constraint $(\mathcal{D})$
  $p_{0,\ell}^{(MG)} = p_{0,\ell}^{*}$, for $\ell = 1, \dots, L$
```

A. Modified Common Message Power Allocation

The idea is to exploit the allocated powers obtained by (27) and then perform joint encoding for the common message, thus achieving common message rate (12) instead of (25). Therefore, we can further increase the common message rate by optimizing the common message rate, while not changing the power allocation of the confidential messages.

In particular, the power of the common message is allocated in order to maximize the common message rate given by (12). Let $\boldsymbol{p}_0 = \{p_{0,\ell}\}$ denote the $1 \times L$ power allocation vector for the common message to be optimized. Once power allocation for confidential messages is fixed, the total available power for the common message is

$$(\mathcal{D}): \quad \sum_{\ell=1}^{L} p_{0,\ell} = P - \sum_{i=1}^{K} \sum_{\cup_{k \in \mathcal{K}} \mathcal{L}_k} p_{i,\ell}^{(\mathrm{G})} \,. \tag{30}$$

Then, the optimization problem is expressed as

$$\begin{aligned} \boldsymbol{p}_{\boldsymbol{0}}^{*} = & \arg\max_{\boldsymbol{p}_0} \min_{k \in \mathcal{K}} \quad \sum_{\ell=1}^{L} \log \left(1 + \alpha_{k,\ell}^{-} p_{0,\ell} + \alpha_{k,\ell}^{-} \sum_{i=1}^{K} p_{i,\ell}^{(\mathrm{G})} \right) \\ & \text{s.t.} \qquad\qquad (\mathcal{D})\,. \end{aligned} \tag{31}$$

Problem (31) is a convex discrete max-min program, where the number of unknowns is L and the cardinality of the discrete space is K. The steps of the new algorithm are summarized in Table II.

The proposed modification requires to solve an additional discrete max-min program with cardinality K. The complexity of this modification is still small when compared to the complexity of power allocation for per-user encoding which is cubic versus the number of users.

V. Power allocation for per-channel encoding

We now consider further simplification of the power allocation problem by considering a separate encoding for both the confidential and the common messages on a per-channel basis. In other words, the common message and the confidential messages are split into sub-messages, and a separate encoder is used on each channel. This is clearly a further sub-optimal approach with respect to the joint encoding, but it allows a simple implementation and significantly simplify the power allocation problem, as detailed in the following.

Let us start by assessing the achievable rates of this scheme with a given power allocation. We define $\beta_{k,\ell} = \max_{j\neq k} \alpha^{+}_{j,\ell}$ and $\gamma_\ell = \min_k \alpha^{-}_{k,\ell}$. The achievable confidential message rate for user k is

$$R_k^{(\mathrm{C})}(\boldsymbol{p}) = \sum_{\ell\in\mathcal{L}_k} \left[\log\big(1+\alpha^{-}_{k,\ell}p_{k,\ell}\big) - \log\big(1+\beta_{k,\ell}p_{k,\ell}\big)\right] \,, \tag{32}$$

while, the common message rate can be expressed as

$$R_0^{(\mathrm{C})}(\boldsymbol{p}) = \sum_{\ell=1}^{L} \left[\log\big(1+\gamma_\ell p_{0,\ell} + \gamma_\ell \sum_{i=1}^{K} p_{i,\ell}\big) - \log\big(1+\gamma_\ell \sum_{i=1}^{K} p_{i,\ell}\big)\right] \,. \tag{33}$$

The power allocation problem maximizing the weighted sum rate is now

$$\boldsymbol{p}^{(C)} = \arg\max_{\boldsymbol{p}\in\mathcal{P}} \sum_{k=0}^{K} w_k R_k^{(C)}(\boldsymbol{p}). \tag{34}$$

Before providing its solution, for $\ell = 1,\dots,L$, $k\in\mathcal{K}$ and $\lambda \geq 0$, we define

$$\Lambda_{k,\ell}(\lambda) = \frac{1}{2}\left[\big(\frac{1}{\beta_{k,\ell}} - \frac{1}{\alpha^{-}_{k,\ell}}\big)\big(\frac{1}{\beta_{k,\ell}} - \frac{1}{\alpha^{-}_{k,\ell}} + \frac{4w_k}{\lambda\ln 2}\big)\right]^{1/2} - \frac{1}{2}\big(\frac{1}{\beta_{k,\ell}} + \frac{1}{\alpha^{-}_{k,\ell}}\big) \tag{35a}$$

$$\mathcal{Z}_\ell(\lambda) = \frac{w_0}{\lambda\ln 2} - \frac{1}{\gamma_\ell} \tag{35b}$$

$$\Delta_{k,\ell} = \left(\frac{1}{\beta_{k,\ell}} - \frac{1}{\alpha^{-}_{k,\ell}}\right)^2 \left[\big(\frac{w_k}{w_0}\big)^2 + 2\cdot\frac{w_k}{w_0}\cdot\frac{\frac{2}{\gamma_\ell} - \frac{1}{\alpha^{-}_{k,\ell}} - \frac{1}{\beta_{k,\ell}}}{\frac{1}{\beta_{k,\ell}} - \frac{1}{\alpha^{-}_{k,\ell}}} + 1\right] \tag{35c}$$

$$\Theta_{k,\ell} = \frac{1}{2}\left[\frac{w_k}{w_0}\big(\frac{1}{\beta_{k,\ell}} - \frac{1}{\alpha^{-}_{k,\ell}}\big) - \big(\frac{1}{\beta_{k,\ell}} + \frac{1}{\alpha^{-}_{k,\ell}}\big) + \sqrt{\Delta_{k,\ell}}\right] \,. \tag{35d}$$

The main result is provided by the following theorem.

Theorem 2. *For $\ell \in \mathcal{L}_k$ and $k \in \mathcal{K}$, the solution of power allocation* (34) *is:*

if $\alpha^-_{k,\ell} - \beta_{k,\ell} > \frac{\gamma_\ell w_0}{w_k}$, then

$$p^{(\mathrm{C})}_{0,\ell} = \left[\mathcal{Z}_\ell(\lambda) - \Theta_{k,\ell}\right]^+ \ , \quad p^{(\mathrm{C})}_{k,\ell} = \left[\min\left\{\Lambda_{k,\ell}(\lambda); \Theta_{k,\ell}\right\}\right]^+ \ , \tag{36a}$$

otherwise,

$$p^{(\mathrm{C})}_{0,\ell} = \left[\mathcal{Z}_\ell(\lambda)\right]^+ \ , \quad p^{(\mathrm{C})}_{k,\ell} = 0\,. \tag{36b}$$

For $\ell \in \mathcal{L}_0$,

$$p^{(\mathrm{C})}_{0,\ell} = \left[\mathcal{Z}_\ell(\lambda)\right]^+ \ , \tag{36c}$$

and λ is chosen to satisfy the total power constraint (1) with equality.

Proof. See Appendix B. □

The theorem provides an almost closed-form solution to the problem where only one positive real variable λ should be optimized numerically. Note that the total power is a decreasing function versus λ, therefore the optimization of λ can be performed efficiently by a dichotomic search as it only scales with the number of channels L. From the theorem, we also conclude that no power is allocated to the confidential message when the difference between the channel power gains of the intended receiver and the strongest unintended receiver is below a certain threshold. On the other hand, in this case power allocation for the common message follows the conventional water-filling principle, where the water level is determined by the weight w_0 and the total available power through λ. Finally, we highlight that the complexity of the proposed algorithm is independent of the number of users.

VI. Numerical Results

This section offers the performance evaluation of the proposed sub-optimal algorithms and comparison to the outer bound. We consider Rayleigh fading channel, i.e., $h_{k,\ell}$ are zero-mean Gaussian with variance that coincides with the average signal-to-noise ratio (SNR), $\Gamma_k = \mathbb{E}[\alpha_{k,\ell}]$. The number of channels and the total power are both set to $L = P = 16$. Unless otherwise specified, we consider perfect CSI and $\alpha^+_{k,\ell} = \alpha^-_{k,\ell}$. The discrete max-min optimization problem is solved using MATLAB optimization toolbox which implements the goal attainment method of

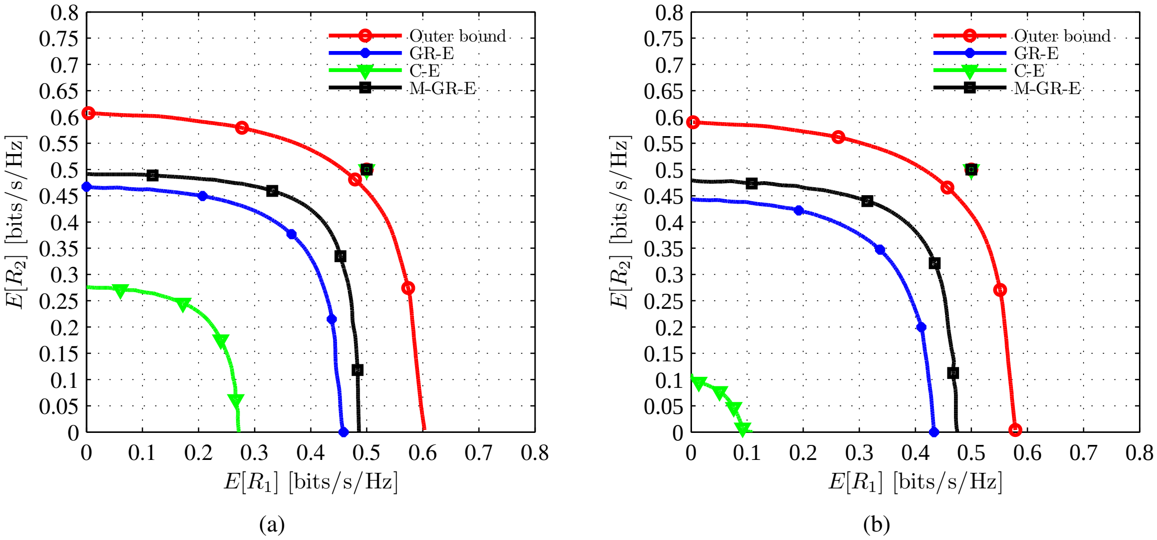


Fig. 2. Achievable secrecy rate region $(\mathbb{E}[R_1], \mathbb{E}[R_2])$ comparison: $\Gamma_k = 10$ dB, $\mathbb{E}[R_0] = 1.5$ bits/s/Hz, and (a) $\mathbb{E}[R_3] = 0.33$ bits/s/Hz (b) $\mathbb{E}[R_3] = 0.4$ bits/s/Hz .

Gembicki [43]. We use the notation GR-E, M-GR-E, C-E and UNI to denote respectively per-user encoding, per-user encoding with modified common message power allocation, per-channel encoding schemes and uniform power allocation.

A. System With 3 *Users*

a) Secrecy Rates: Fig. 2 shows the average confidential message rate region for the first two users ($\mathbb{E}[R_1]$ and $\mathbb{E}[R_2]$) achieved by the four power allocation algorithms. The average common message rate is fixed to 1.5 bits/s/Hz and the average rate of the confidential message of the third user is 0.33 and 0.4 bits/s/Hz in Figs. 2a and 2b respectively. The region is obtained by suitably varying the barycentric weights $w_0, \ldots, w_3$. We assume that all users have the same average SNR, $\Gamma_1 = \Gamma_2 = \Gamma_3 = 10$ dB. Although the sub-optimal algorithms do not approach the outer bound in this case, we remark that M-GR-E still allows a significant performance improvement over GR-E. C-E achieves a secrecy rate region substantially smaller than the other algorithms. As expected, we also notice that by increasing $\mathbb{E}[R_3]$ we shrink the achievable regions.

b) Users With the Same SNR*:* Fig. 3 shows the average sum rate with all equal weights versus $\Gamma_k = \Gamma$ ($k = 1, \ldots, 3$) for the five power allocation algorithms. As expected, the average sum rate grows logarithmically with Γ. The uniform power allocation shows the worst performance. M-GR-E allows to achieve a performance level close to the outer bound (gap less

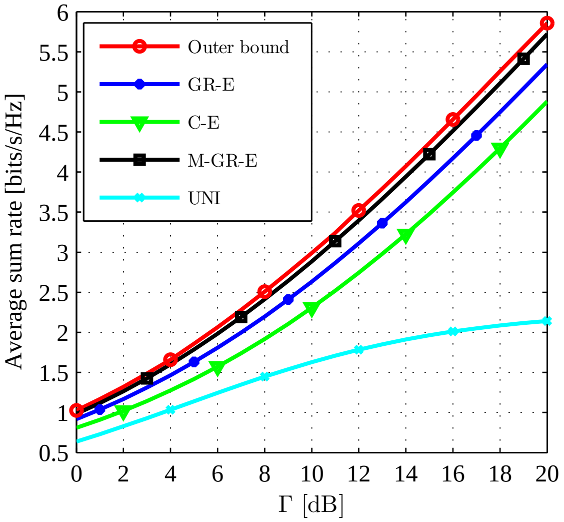
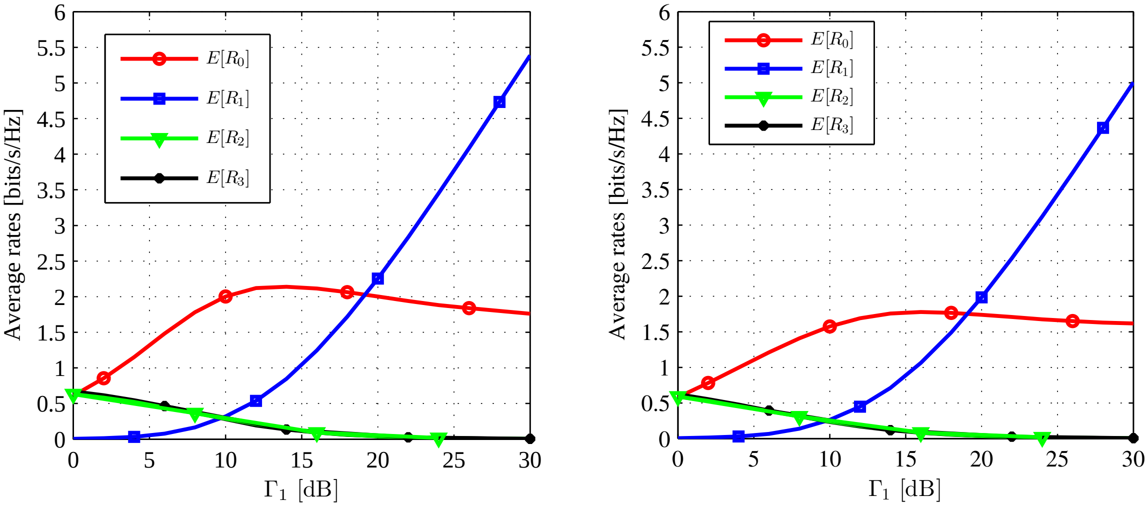


Fig. 3. Average sum rate comparison versus Γ.

than 0.02 bits/s/Hz). The performance gap between the algorithms is distinguishable mainly at the high SNR regime.

c) Unequal SNR*s Among Users:* Fig. 4 shows the average messages rates versus Γ_1 for M-GR-E and C-E when Γ_2 and Γ_3 are both fixed to 10 dB. We observe that the average confidential messages rates cross at $\Gamma_1 = 10$ dB when all users have the same average SNR, while $\mathbb{E}[R_1] > \mathbb{E}[R_2], \mathbb{E}[R_3]$ for $\Gamma_1 > 10$ dB. $\mathbb{E}[R_2]$ and $\mathbb{E}[R_3]$ are similar as both users 2 and 3 have equal SNRs. At the high Γ_1 regime, $\mathbb{E}[R_1]$ grows unbounded while $\mathbb{E}[R_2]$ and $\mathbb{E}[R_3]$ converge to 0. $\mathbb{E}[R_0]$ increases rapidly for $\Gamma_1 < 10$ dB and reaches a fixed value different from 0 at the high Γ_1 regime. This may be counter-intuitive as, when a user has a significantly higher average SNR than the others, we would expect that the power devoted to the common message would be vanishing and $\mathbb{E}[R_0]$ converging to 0.

To understand the behavior of $\mathbb{E}[R_0]$ at high Γ_1 regime, we propose to consider a simplified degraded deterministic scalar channel with one transmitter and two receivers whose channel power gains are respectively α and β, with $\alpha > \beta$. The transmitter sends one common message to both receivers and one confidential message to receiver 1. The power allocated to the confidential message is P_s and the power allocated to the common message is P_c such that $P = P_c + P_s$. The



(a)

(b)

Fig. 4. Average messages rates versus Γ_1, $\Gamma_2 = \Gamma_3 = 10$ dB, (a) M-GR-E (b) C-E.

common message rate $R_c(P_s)$ and confidential message rate $R_s(P_s)$ can be expressed as [41]

$$R_c(P_s) = \log\big(1 + \beta P\big) - \log\big(1 + \beta P_s\big)\,; \tag{37}$$

$$R_s(P_s) = \log\big(1 + \alpha P_s\big) - \log\big(1 + \beta P_s\big)\,. \tag{38}$$

Our goal is to determine $\bar{P}_c^*$ maximizing the sum rate $R_c(P_s) + R_s(P_s)$ at the high SNR regime when $\alpha \to \infty$. A simple computation allows to show that

$$\bar{P}_c^* = \begin{cases} P - \frac{P}{\beta} & \text{if } \beta \geq 1 \\ 0 & \text{else} \end{cases}. \tag{39}$$

We deduce that P_c^* converges to a fixed value $\bar{P}_c^* = P - \frac{P}{\beta}$ when β is larger than a certain threshold equal to 0 dB and $\bar{P}_c^* = 0$ otherwise. We conclude that the power devoted to the common message is vanishing only if β is lower than a certain threshold. In Fig. 5, we show $\mathbb{E}[R_0]$ versus Γ_1 achieved by C-E for some values of Γ_2 and Γ_3. The conclusion drawn from the simplified case is confirmed: $\mathbb{E}[R_0]$ tends to a fixed value different from 0 when $\Gamma_2 = \Gamma_3 \in \{5, 10\}$ dB and $\mathbb{E}[R_0]$ tends to 0 when $\Gamma_2 = \Gamma_3 \in \{-5, -10\}$ dB at the high Γ_1 regime.

In Fig. 6, we compare $\mathbb{E}[R_0]$ and $\mathbb{E}[R_1]$ versus Γ_1 between the four power allocation algorithms; $\Gamma_2 = \Gamma_3 = 10$ dB. We remark that GR-E and M-GR-E achieve very close secrecy rate as the

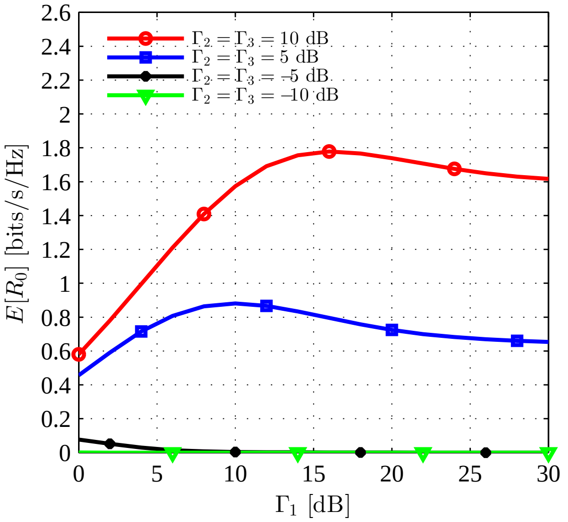


Fig. 5. $\mathbb{E}[R_0]$ versus Γ_1 for some values of Γ_2 and Γ_3, C-E.

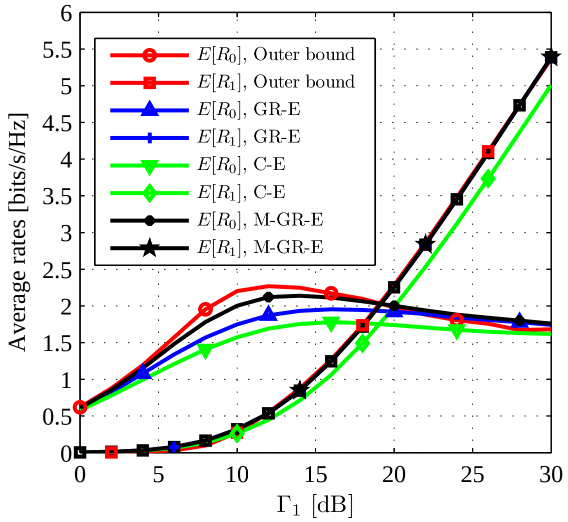


Fig. 6. $\mathbb{E}[R_0]$ and $\mathbb{E}[R_1]$ versus Γ_1 comparison between the four algorithms, $\Gamma_2 = \Gamma_3 = 10$ dB.

outer bound. The loss in performance of GR-E and M-GR-E compared to the outer bound is observed mainly for the common message rate. Nevertheless, $\mathbb{E}[R_0]$ tends to close values for all power allocation algorithms at the high Γ_1 regime.

d) Imperfect CSI : To investigate the impact of imperfect CSI, we show in Fig. 7 $\mathbb{E}[R_0]$ and $\mathbb{E}[R_1]$ versus the outage probability ε with $\sigma = 0.01$ for joint encoding providing the outer bound and M-GR-E. We notice that as ε is less than a cutoff ($\approx 5 \cdot 10^{-2}$), $\mathbb{E}[R_0]$ and $\mathbb{E}[R_1]$ are

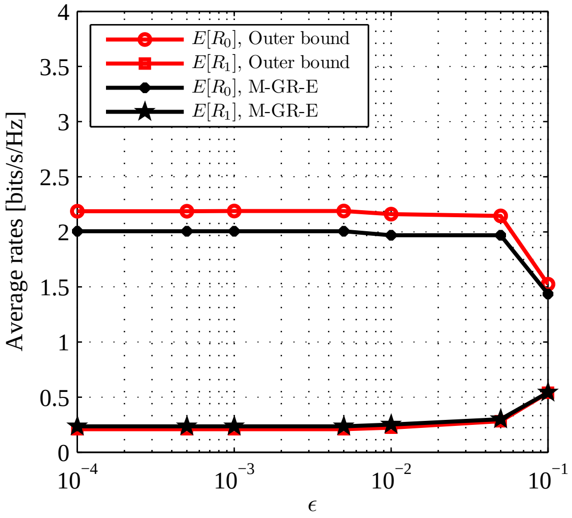


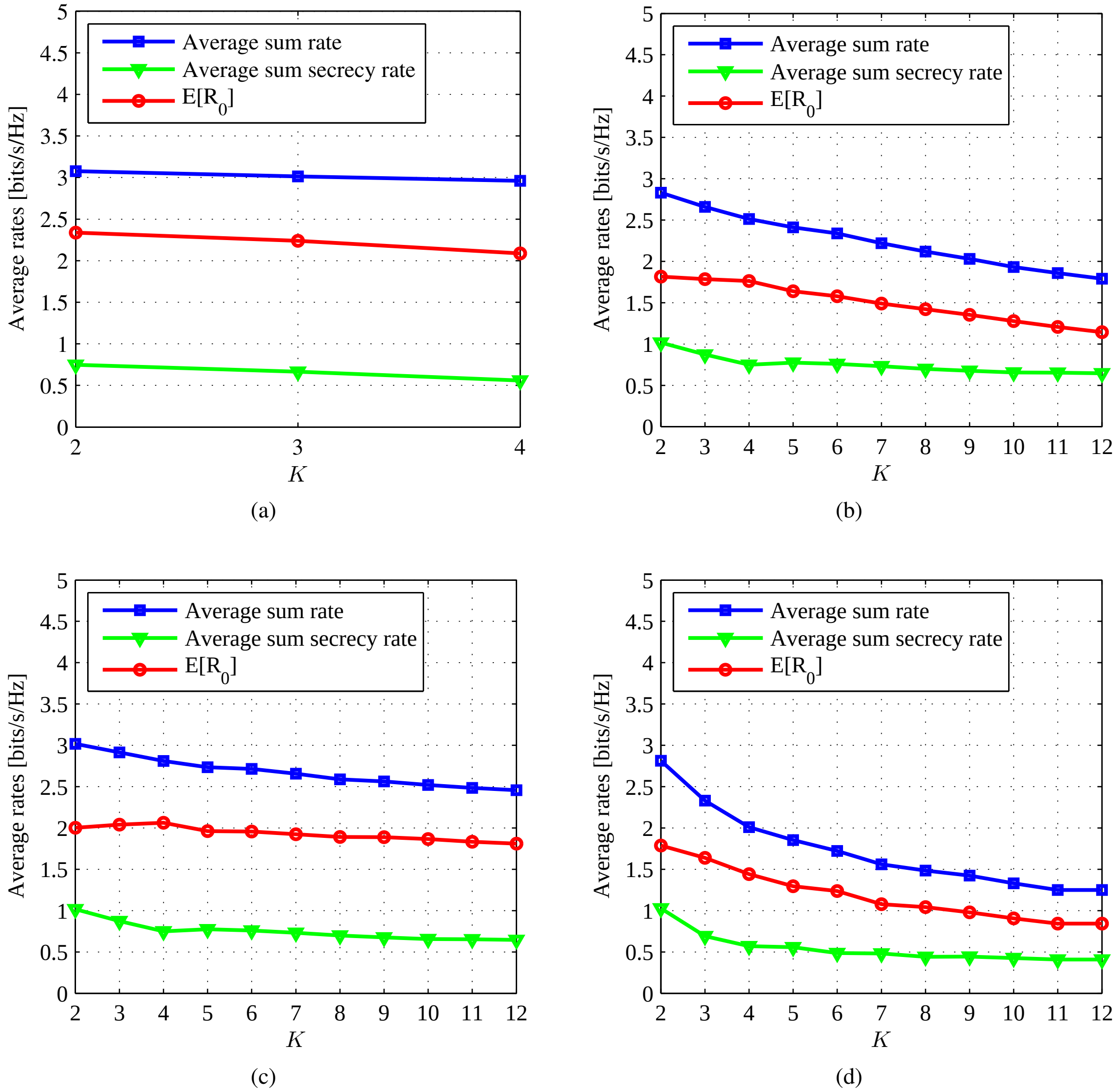
Fig. 7. $\mathbb{E}[R_0]$ and $\mathbb{E}[R_1]$ versus ε for J-E and M-GR-E.

both constant. While for $\varepsilon >$ the cutoff, the secrecy rate increases, as we are less restrictive on the illegitimate receiver. On the other hand, the average rate of the common message decreases.

B. Multiuser System

e) Impact of the Number of Users: Fig. 8 shows the average sum secrecy rate and the average common message rate versus K for all power allocation algorithms. We do not go beyond $K = 4$ for the outer bound due to the heavy computational complexity of the power allocation algorithm in this case. All users in the system are assumed to have the same $\Gamma_k = 10$ dB and we consider equal weights, $w_k = 1$, for $k = 0, \ldots, K$. We observe that the average rates are decreasing functions versus K. In fact, the number of eavesdroppers increases with K, which reduces the individual secrecy rate. As a result, the sum secrecy rate decreases too. The common message rate depends on the capacity of the worst user, which decreases as K increases thus $\mathbb{E}[R_0]$ is reduced too.

Fig. 9 shows the average sum rate for the five solutions as a function of K. We observe that we have same order as for the case of three users (see Fig. 3), except for the UNI power allocation that as $K > 3$ outperforms the C-E solution. This is due to the fact that coding per subchannel is in general suboptimal, although may provides some advantage in terms of computational complexity.



(a)

(b)

(c)

(d)

Fig. 8. Average sum rate, sum secrecy rate and $\mathbb{E}[R_0]$ versus K, (a) Outer bound (b) GR-E (c) M-GR-E (d) C-E.

f) Computational Complexity Comparison: The computational complexity of the proposed algorithms is related to the number of channels L and the number of users K. The complexity depends mainly on the number of users K via the cardinality of the discrete space in the max-min program. Table III reports the cardinality of the discrete space and the number of variables for all algorithms. In fact, the solution of the outer bound has an exponential complexity, while GR-E and M-GR-E reduce complexity from exponential to cubic and also reduce the number of variables. On the other hand, the complexity of C-E is independent of K.

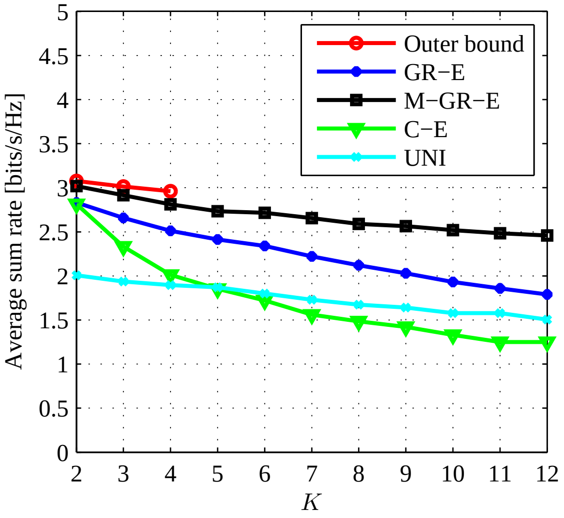


Fig. 9. Average sum rate versus K comparison.

TABLE III
COMPUTATIONAL COMPLEXITY COMPARISON BETWEEN POWER ALLOCATION ALGORITHMS

Algorithm	Cardinality of the max-min space			Number of variables
	general K	$K = 3$	$K = 12$	
Outer bound	$K(K-1)^K$	24	$3.76 \cdot 10^{13}$	$L(K+1)$
GR-E	$K^2(K-1)$	18	1584	$2L$
M-GR-E	$K^2(K-1)+K$	21	1596	$3L$
C-E	1	1	1	$2L$

VII. Conclusion

We proposed four power allocation algorithms with the objective of maximizing the weighted sum rate achievable by different encoding schemes. Moreover, we offered performance evaluation and computational complexity comparison for all proposed algorithms. Numerical results have shown the merit of power allocation for per-user encoding with modified common message power allocation as it reaches close performance to the outer bound provided by joint encoding at much lower complexity (cubic versus exponential function of the number of users). The performance gap of power allocation for per-user encoding grows large when the number of users K increases for a fixed number of channels L. The variant with modified common message power allocation enables to correct this behavior and considerably reduces the gap. However, the correction may not be as effective when power is over-allocated to confidential messages. Although power allocation for per-channel encoding has a poor performance, it can offer suitable solution for computational constrained devices as the complexity is independent of the number of users. We conclude also from the analysis that the growing number of users becomes detrimental to performance for the studied communication scenario.

APPENDIX

A. Proof of Theorem 1

Solutions of (P1), (P2) and (P3) follow the same steps. We present only the solution of (P1) for the sake of conciseness. (P1) is a convex optimization with concave objective function and affine constraint. We solve the optimization by a technique based on deriving an upper bound on the Lagrangian dual and establishing power allocations that achieve the upper bound.

The Lagrangian dual $\mathcal{G}(\boldsymbol{p},\lambda)$ of (P1) is given by

$$\begin{aligned}\mathcal{G}(\boldsymbol{p},\lambda) = &\sum_{\ell=1}^{L} w_0 \log\big(1+\frac{\alpha^-_{1,\ell}p_{0,\ell}}{1+\alpha^-_{1,\ell}[p_{1,\ell}+p_{2,\ell}]}\big)\\ &+\sum_{\ell\in\mathcal{L}_1} w_1\log\big(1+\alpha^-_{1,\ell}p_{1,\ell}\big) - w_1\log\big(1+\alpha^+_{2,\ell}p_{1,\ell}\big)\\ &+\sum_{\ell\in\mathcal{L}_2} w_2\log\big(1+\alpha^-_{2,\ell}p_{2,\ell}\big) - w_2\log\big(1+\alpha^+_{1,\ell}p_{2,\ell}\big)\\ &-\lambda\sum_{\ell=1}^{L}\big[p_{0,\ell}+p_{1,\ell}+p_{2,\ell}\big] \end{aligned} \tag{40}$$

where $\lambda \geq 0$ is the Lagrange multiplier. For $\ell \in \mathcal{L}_{1/2}$, we have $p_{2,\ell}=0$. In this case, $p^{(1)}_{0,\ell}$ and $p^{(1)}_{1,\ell}$ need to maximize :

$$\begin{aligned}\mathcal{G}_1(p_{0,\ell},p_{1,\ell},\lambda) = &\, w_0\log\big(1+\frac{\alpha^-_{1,\ell}p_{0,\ell}}{1+\alpha^-_{1,\ell}p_{1,\ell}}\big) + w_1\log\big(1+\alpha^-_{1,\ell}p_{1,\ell}\big)\\ &- w_1\log\big(1+\alpha^+_{2,\ell}p_{1,\ell}\big) - \lambda(p_{0,\ell}+p_{1,\ell}). \end{aligned} \tag{41}$$

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

$$u_{0,\ell}(x) = \frac{w_0}{\ln 2}\frac{\alpha^-_{1,\ell}}{1+\alpha^-_{1,\ell}x} - \lambda \tag{42}$$

$$u_{k,\ell}(x) = \frac{w_k}{\ln 2}\left(\frac{\alpha^-_{k,\ell}}{1+\alpha^-_{k,\ell}x} - \frac{\alpha^+_{k,\ell}}{1+\alpha^+_{k,\ell}x}\right) - \lambda. \tag{43}$$

Then, (41) can be rewritten as

$$\mathcal{G}_1(p_{0,\ell}, p_{1,\ell}, \lambda) = \int_{p_{1,\ell}}^{p_{1,\ell}+p_{0,\ell}} u_{0,\ell}(x)\,dx + \int_0^{p_{1,\ell}} u_{1,\ell}(x)\,dx \tag{44}$$

and upper bounded as

$$\mathcal{G}_1(p_{0,\ell}, p_{1,\ell}, \lambda) \leq \int_0^{+\infty} [\max\{u_{0,\ell}(x), u_{1,\ell}(x)\}]^+\,dx. \tag{45}$$

The root of $u_{0,\ell}(x)$ is $\Upsilon_{1,\ell}(\lambda)$ defined in (19b) while the largest root of $u_{1,\ell}(x)$ is $\Omega_{1,\ell}(\lambda)$ defined in (19a). $u_{0,\ell}(x)$ and $u_{1,\ell}(x)$ intersect at the point $\Xi_{1,\ell}$ given by (19c). 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., $\Xi_{1,\ell}$ 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 (45) is achieved by $p^{(1)}_{0,\ell} = 0$ and $p^{(1)}_{1,\ell} = 0$.

   b) If $u_{1,\ell}(0) \geq 0$ and $\Upsilon_{1,\ell}(\lambda) < \Xi_{1,\ell}$, then (45) is achieved by $p^{(1)}_{0,\ell} = 0$ and $p^{(1)}_{1,\ell} = \Omega_{1,\ell}(\lambda)$.

   c) If $\Upsilon_{1,\ell}(\lambda) \geq \Xi_{1,\ell}$, then (45) is achieved by $p^{(1)}_{0,\ell} = \Upsilon_{1,\ell}(\lambda) - \Xi_{1,\ell}$ and $p^{(1)}_{1,\ell} = \Xi_{1,\ell}$.

   In summary, we obtain (20a).

2) $\frac{w_1}{w_0} \leq \frac{\alpha^-_{1,\ell}}{\alpha^-_{1,\ell}-\alpha^+_{2,\ell}}$, i.e., $\Xi_{1,\ell}$ is negative.

   In this case, $u_{0,\ell}(0) \geq u_{1,\ell}(0)$.

   a) If $u_{0,\ell}(0) \leq 0$, then (45) is achieved by $p^{(1)}_{0,\ell} = 0$ and $p^{(1)}_{1,\ell} = 0$.

   b) If $u_{0,\ell}(0) > 0$, then (45) is achieved by $p^{(1)}_{0,\ell} = \Upsilon_{1,\ell}(\lambda)$ and $p^{(1)}_{1,\ell} = 0$.

   In summary, we obtain (20b).

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

$$\begin{aligned}\mathcal{G}_2(p_{0,\ell}, p_{2,\ell}, \lambda) =& w_0 \log\big(1 + \frac{\alpha^-_{1,\ell}p_{0,\ell}}{1+\alpha^-_{1,\ell}p_{2,\ell}}\big) + w_2 \log\big(1+\alpha^-_{2,\ell}p_{2,\ell}\big) \\ &- w_2 \log\big(1+\alpha^+_{1,\ell}p_{2,\ell}\big) - \lambda(p_{0,\ell}+p_{2,\ell}).\end{aligned} \tag{46}$$

Then, we obtain, analogously to (45)

$$\mathcal{G}_2(p_{0,\ell}, p_{2,\ell}, \lambda) \le \int_0^{+\infty} \big[\max\{u_{0,\ell}(x), u_{2,\ell}(x)\}\big]^+ \, dx. \tag{47}$$

The largest root of $u_{2,\ell}(x)$ is $\Omega_{2,\ell}(\lambda)$ given by (19a). $u_{0,\ell}(x)$ and $u_{2,\ell}(x)$ intersect at two points. The largest point $\mathcal{U}_{2,\ell}$ is given by (19e). 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 (47) is achieved by $p_{0,\ell}^{(1)} = 0$ and $p_{2,\ell}^{(1)} = 0$.

   b) If $u_{2,\ell}(0) \ge 0$ and $\Upsilon_{1,\ell}(\lambda) < \mathcal{U}_{2,\ell}$, then (47) is achieved by $p_{0,\ell}^{(1)} = 0$ and $p_{2,\ell}^{(1)} = \Omega_{2,\ell}(\lambda)$.

   c) If $\Upsilon_{1,\ell}(\lambda) \ge \mathcal{U}_{2,\ell}$, then (47) is achieved by $p_{0,\ell}^{(1)} = \Upsilon_{1,\ell}(\lambda) - \mathcal{U}_{2,\ell}$ and $p_{2,\ell}^{(1)} = \mathcal{U}_{2,\ell}$.

   In summary, we obtain (20c).

2) $\frac{w_2}{w_0} \le \frac{\alpha_{1,\ell}^-}{\alpha_{2,\ell}^+ - \alpha_{1,\ell}^+}$, *i.e.*, the two intersection points are negative.

   In this case, $u_{0,\ell}(0) \ge u_{2,\ell}(0)$. There are two possibilities to consider.

   a) If $u_{0,\ell}(0) \le 0$, then (47) is achieved by $p_{0,\ell}^{(1)} = 0$ and $p_{2,\ell}^{(1)} = 0$.

   b) If $u_{0,\ell}(0) > 0$, then (47) is achieved by $p_{0,\ell}^{(1)} = \Upsilon_{1,\ell}(\lambda)$ and $p_{2,\ell}^{(1)} = 0$.

   In summary, we obtain (20d).

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

For $\ell \in \mathcal{L}_0$, $p_{0,\ell}^{(1)}$ need to maximize

$$\mathcal{G}_0(p_{0,\ell}, \lambda) = w_0 \log\big(1 + \alpha_{1,\ell}^- p_{0,\ell}\big) - \lambda\, p_{0,\ell}. \tag{48}$$

$\mathcal{G}_0(p_{0,\ell}, \lambda)$ can be upper bounded by

$$\mathcal{G}_0(p_{0,\ell}, \lambda) = \int_0^{p_{0,\ell}} u_{0,\ell}(x)\, dx \le \int_0^{+\infty} [u_{0,\ell}(x)]^+ \, dx. \tag{49}$$

If $u_{0,\ell}(0) < 0$, then the upper bound on $\mathcal{G}_0(p_{0,\ell}, \lambda)$ is achieved by $p_{0,\ell}^{(1)} = 0$. If $u_{0,\ell}(0) \ge 0$, the upper bound is achieved in this case by $p_{0,\ell}^{(1)} = \Upsilon_{1,\ell}(\lambda)$. In summary, we obtain (20e).

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

B. Proof of Theorem 2

Problem (34) is a convex optimization with concave objective function and affine constraint. We solve this problem analytically by deriving an upper bound on the Lagrangian dual and establishing power allocations that achieve this upper bound. The Lagrangian dual $\mathcal{G}(\boldsymbol{p}, \lambda)$ of the problem is given by

$$\begin{aligned}\mathcal{G}(\boldsymbol{p}, \lambda) =& w_0 \sum_{\ell=1}^{L} \log\left(1 + \frac{\gamma_\ell\, p_{0,\ell}}{1 + \gamma_\ell [p_{1,\ell} + \ldots p_{K,\ell}]}\right) \\ &+ \sum_{k=1}^{K} w_k \sum_{\ell\in\mathcal{L}_k} \log\bigl(1 + \alpha^{-}_{k,\ell} p_{k,\ell}\bigr) - \log\bigl(1 + \beta_{k,\ell} p_{k,\ell}\bigr) \\ &- \lambda \sum_{k=1}^{K}\sum_{\ell=1}^{L} \bigl[p_{0,\ell} + p_{k,\ell}\bigr] \end{aligned} \tag{50}$$

where $\lambda \geq 0$ is the Lagrange multiplier.

For $\ell \in \mathcal{L}_k$, $k \in \mathcal{K}$, the transmitter sends the common message M_0 and the confidential message M_k. In this case, $p^{(\mathrm{C})}_{0,\ell}$ and $p^{(\mathrm{C})}_{k,\ell}$ need to maximize:

$$\begin{aligned}\mathcal{G}_k(p_{0,\ell}, p_{k,\ell}, \lambda) =& w_0 \log\left(1 + \frac{\gamma_\ell\, p_{0,\ell}}{1 + \gamma_\ell\, p_{k,\ell}}\right) + w_k \log\bigl(1 + \alpha^{-}_{k,\ell}\, p_{k,\ell}\bigr) \\ &- w_k \log\bigl(1 + \beta_{k,\ell}\, p_{k,\ell}\bigr) - \lambda[p_{0,\ell} + p_{k,\ell}]\,. \end{aligned} \tag{51}$$

We denote by $\mathcal{M}_{0,\ell}(\cdot)$ and $\mathcal{M}_{k,\ell}(\cdot)$ the partial derivative of $\mathcal{G}_k(p_{0,\ell}, p_{k,\ell}, \lambda)$ with respect to $p_{0,\ell}$ and $p_{k,\ell}$, i.e.,

$$\mathcal{M}_{0,\ell}(x) = \frac{w_0}{\ln 2}\,\frac{\gamma_\ell}{1 + \gamma_\ell\, x} - \lambda \tag{52}$$

$$\mathcal{M}_{k,\ell}(x) = \frac{w_k}{\ln 2}\left(\frac{\alpha^{-}_{k,\ell}}{1 + \alpha^{-}_{k,\ell}\, x} - \frac{\beta_{k,\ell}}{1 + \beta_{k,\ell}\, x}\right) - \lambda\,. \tag{53}$$

Then, (51) can be rewritten as

$$\mathcal{G}_k(p_{0,\ell}, p_{k,\ell}, \lambda) = \int_{p_{k,\ell}}^{p_{k,\ell}+p_{0,\ell}} \mathcal{M}_{0,\ell}(x)\, dx + \int_0^{p_{k,\ell}} \mathcal{M}_{k,\ell}(x)\, dx \tag{54}$$

and upper bounded by

$$\mathcal{G}_k(p_{0,\ell}, p_{k,\ell}, \lambda) \leq \int_0^{+\infty} \left[\max\{\mathcal{M}_{0,\ell}(x), \mathcal{M}_{k,\ell}(x)\}\right]^+ dx\,. \tag{55}$$

The root of $\mathcal{M}_{0,\ell}(\cdot)$ is $\mathcal{Z}_\ell(\lambda)$ defined in (35b) and the largest root of $\mathcal{M}_{k,\ell}(\cdot)$ is $\Lambda_{k,\ell}(\lambda)$ defined in (35a). As the discriminant $\Delta_{k,\ell}$ given by (35c) is strictly positive, $\mathcal{M}_{0,\ell}(\cdot)$ and $\mathcal{M}_{k,\ell}(\cdot)$ intersect at two points. The largest one is $\Theta_{k,\ell}$ defined in (35d). We consider two cases depending on the sign of both points.

1) $\alpha^-_{k,\ell} - \beta_{k,\ell} > \frac{\gamma_l w_0}{w_k}$, i.e., one point is negative and the other is positive.

   In this case, $\mathcal{M}_{k,\ell}(0) > \mathcal{M}_{0,\ell}(0)$. There are three possibilities to consider depending on the value of λ.

   a) If $\mathcal{M}_{k,\ell}(0) < 0$, then both $\mathcal{M}_{0,\ell}(x)$ and $\mathcal{M}_{k,\ell}(x)$ are negative for $x > 0$. The upper bound (55) is achieved by $p^{(\mathrm{C})}_{0,\ell} = 0$ and $p^{(\mathrm{C})}_{k,\ell} = 0$.

   b) If $\mathcal{M}_{k,\ell}(0) \geq 0$ and $\mathcal{Z}_\ell(\lambda) < \Theta_{k,\ell}$, then (55) is achieved by $p^{(\mathrm{C})}_{0,\ell} = 0$ and $p^{(\mathrm{C})}_{k,\ell} = \Lambda_{k,\ell}(\lambda)$.

   c) If $\mathcal{Z}_\ell(\lambda) \geq \Theta_{k,\ell}$, then (55) is achieved by $p^{(\mathrm{C})}_{0,\ell} = \mathcal{Z}_\ell(\lambda) - \Theta_{k,\ell}$ and $p^{(\mathrm{C})}_{k,\ell} = \Theta_{k,\ell}$.

   In summary, we obtain (36a).

2) $\alpha^-_{k,\ell} - \beta_{k,\ell} \leq \frac{\gamma_l w_0}{w_k}$, i.e., both intersection points are negative.

   In this case, $\mathcal{M}_{0,\ell}(0) \geq \mathcal{M}_{k,\ell}(0)$. There are two possibilities to consider.

   a) If $\mathcal{M}_{0,\ell}(0) \leq 0$, then (55) is achieved by $p^{(\mathrm{C})}_{0,\ell} = 0$ and $p^{(\mathrm{C})}_{k,\ell} = 0$.

   b) If $\mathcal{M}_{0,\ell}(0) > 0$, then (55) is achieved by $p^{(\mathrm{C})}_{0,\ell} = \mathcal{Z}_\ell(\lambda)$ and $p^{(\mathrm{C})}_{k,\ell} = 0$.

   In summary, we obtain (36b).

The case that both intersection points are positive is not possible.

For $\ell \in \mathcal{L}_0$, $p^{(\mathrm{C})}_{0,\ell}$ needs to maximize

$$\mathcal{G}_0(p_{0,\ell}, \lambda) = w_0 \log\bigl(1 + \gamma_l \, p_{0,\ell}\bigr) - \lambda \, p_{0,\ell}\,. \tag{56}$$

$\mathcal{G}_0(p_{0,\ell}, \lambda)$ can be upper bounded by

$$\mathcal{G}_0(p_{0,\ell}, \lambda) = \int_0^{p_{0,\ell}} \mathcal{M}_{0,\ell}(x)\, dx \leq \int_0^{+\infty} [\mathcal{M}_{0,\ell}(x)]^+ \, dx\,. \tag{57}$$

If $\mathcal{M}_{0,\ell}(0) < 0$, then the upper bound (57) is achieved by $p^{(\mathrm{C})}_{0,\ell} = 0$. If $\mathcal{M}_{0,\ell}(0) \geq 0$, (57) is achieved in this case by $p^{(\mathrm{C})}_{0,\ell} = \mathcal{Z}_\ell(\lambda)$. In summary, we obtain (36c).

The KKT (Karush-Kuhn-Tucker) conditions impose that the Lagrange multiplier λ must be chosen to satisfy the power constraint with equality.

REFERENCES

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

[2] J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wireless channels,” in *Proc. IEEE Inter. Symp. Inf. Theory*, Seattle, WA, USA, July 2006, pp. 356–360.

[3] Z. Li, R. Yates, and W. Trappe, “Secret communication with a fading eavesdropper channel,” in *Proc. IEEE Inter. Symp. Inf. Theory*, Nice, France, June 2007, pp. 1296–1300.

[4] 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.

[5] 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.

[6] 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.

[7] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, M. Zhao, and J. Wang, “Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs,” *IEEE Trans. on Wireless Commun.*, vol. 12, no. 6, pp. 2717–2729, Jun. 2013.

[8] H. Qin, Y. Sun, X. Chen, M. Zhao, and J. Wang, “Optimal power allocation for OFDM-based wire-tap channels with arbitrarily distributed inputs,” in *Wireless Internet*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, P. Ren, C. Zhang, X. Liu, P. Liu, and S. Ci, Eds. Springer Berlin Heidelberg, 2012, vol. 98, pp. 192–203. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-30493-4_20

[9] 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.

[10] ——, “Secure transmission with multiple antennas II: The MIMOME wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[11] S. Tomasin, “Resource allocation for secret transmissions over MIMOME fading channels,” in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Atlanta, Georgia, USA, Dec. 2013.

[12] 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.

[13] 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. 1550–1576, 2014.

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

[15] 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.

[16] R. Liu, T. Liu, H. V. Poor, and S. Shamai, “Multiple-input multiple-output Gaussian broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[17] ——, “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.

[18] Y. K. Chia and A. ElGamal, “Three-receiver broadcast channels with common and confidential messages,” *IEEE. Trans. Inf. Theory*, vol. 58, no. 5, pp. 2748–2765, May 2012.

[19] T. Liu, V. Prabhakaran, and S. Vishwanath, “The secrecy capacity of a class of parallel Gaussian compound wiretap channels,” in *Proc. IEEE Inter. Symp. Inf. Theory*, Toronto, Canada, July 2008, pp. 116–120.

[20] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, “Compound wire-tap channels,” *EURASIP Journal on Wireless Commun. and Netw., Special Issue on Wireless Physical Layer Security*, vol. 2009, no. 142374, 2009.

[21] R. F. Schaefer and H. Boche, “Robust broadcasting of common and confidential messages over compound channels,” *IEEE. Trans. Inf. Forensics and Security*, vol. 9, no. 10, pp. 1720–1732, Oct. 2014.

[22] 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.

[23] A. Khisti and T. Liu, “Private broadcasting over independent parallel channels,” *IEEE. Trans. Inf. Theory*, vol. 60, no. 9, pp. 5173–5187, Sep. 2014.

[24] Y. Liang, H. V. Poor, and L. Ying, “Secure communications over wireless broadcast networks: stability and utility maximization,” *IEEE. Trans. Inf. Forensics and Security*, vol. 6, no. 3, pp. 682–690, Sep. 2011.

[25] 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.

[26] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, “On multiuser secrecy rate in flat fading channel,” in *Proc. IEEE Military Commun. Conf.*, Boston, USA, Oct. 2009, pp. 1–7.

[27] A. Mukherjee and A. L. Swindlehurst, “User selection in multiuser MIMO systems with secrecy considerations,” in *Proc. IEEE Asilomar Conf. Sig., Sys. and Comp.*, California, USA, Nov. 2009, pp. 1479–1482.

[28] I. Krikidis and B. Ottersten, “Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling,” *IEEE Sig. Processing Letters*, vol. 20, no. 2, pp. 141–144, Feb. 2013.

[29] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, “Large system analysis of linear precoding in MISO broadcast channels with confidential messages,” *IEEE Journal Selected Areas Commun.*, vol. 31, no. 9, pp. 1660–1671, Sep. 2013.

[30] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, “Secrecy rates in broadcast channels with confidential messages and external eavesdroppers,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931–2943, May 2014.

[31] X. Liu, F. Gao, G. Wang, and X. Wang, “Joint beamforming and user selection in multicast downlink channel under secerecy-outage constraint,” *IEEE Commun. Letters*, vol. 18, no. 1, pp. 82–85, Jan. 2014.

[32] M. F. Hanif, L. N. Tran, M. Juntti, and S. Glisic, “On linear precoding strategies for secrecy rate maximization in multiuser multiantenna wireless networks,” *IEEE Trans. Sig. Processing*, vol. 62, no. 14, pp. 3536–3551, July 2014.

[33] X. Lu, K. Zu, and R. C. de Lamare, “Lattice-reduction aided successive optimization Tomlinson-Harashima precoding strategies for physical-layer security in wireless networks ,” in *Proc. IEEE Sensor Sig. Processing for Defense (SSPD)*, Edinburgh, UK, Sep. 2014, pp. 1–5.

[34] A. P. Shrestha and K. S. Kwak, “Performance of opportunistic scheduling for physical layer security with transmit antenna selection,” *EURASIP Journal on Wireless Commun. and Netw.*, vol. 2014, no. 33, pp. 1–9, 2014.

[35] X. Wang, M. Tao, J. Mo, and Y. Xu, “Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks,” *IEEE Trans. Inf. Forensics and Security*, vol. 6, no. 3, pp. 693–702, 2011.

[36] X.-M. Ran, Y.-Q. Mo, and Y.-L. Chen, “A resource allocation algorithm for physical-layer security for OFDMA system under non-ideal condition,” *Commun. and Netw.*, vol. 2013, pp. 204–210, 2013.

[37] H. Qin, X. Chen, X. Zhong, F. He, M. Zhao, and J. Wang, “Joint power allocation and artificial noise design for multiuser

wiretap OFDM channels," in *Proc. IEEE Commun. and Inf. Sys. Security Symp.*, Budapest, Hungary, June 2013, pp. 2193–2198.

[38] T. Lin, K. Zhi, and W.-Y. Luo, "A multicarrier-based physical layer security scheme for the multicast systems," in *Proc. IEEE Conf. Inf. Science and Tech.*, Jiangsu, China, March 2013, pp. 1584–1587.

[39] A. Benfarah, S. Tomasin, and N. Laurenti, "Parallel BCC with one common and two confidential messages and imperfect CSIT," in *Proc. IEEE Globecom second Workshop on trusted Commun. with Physical Layer Security (TCPLS 2014)*, Austin, TX USA, Dec. 2014. [Online]. Available: http://arxiv.org/abs/1403.6982

[40] 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.

[41] V. L. Nir and B. Scheers, "Distributed power allocation for parallel broadcast channels with only common information in cognitive tactical radio networks," *EURASIP Journal Wireless Commun. and Netw.*, vol. 2010, no. 172013, pp. 1–10, 2010.

[42] V. F. Demyanov and V. N. Malozemov, *Introduction to Minimax.* John Wiley, New York, 1974.

[43] F. W. Gembicki and Y. Y. Haimes, "Approach to performance and sensitivity multiobjective optimization: the goal attainment method ," *IEEE Trans. Automatic Control*, vol. 20, no. 6, pp. 769–771, Dec. 1975.

[44] E. R. Panier and A. L. Tits, "Superlinearly convergent feasible method for the solution on inequality constrained optimization problems," *SIAM Journal on Control and Optimization*, vol. 25, no. 4, pp. 934–950, 1987.

[45] L. Wang and Z. Luo, "A simple SQP algorithm for constrained finite minimax problems," *The Scientific World Journal*, vol. 2014, no. 159754, pp. 1–9, 2014.

[46] D. P. Bertsekas, "A new algorithm for solution of nonlinear resistive networks involving diodes," *IEEE Trans. Circ. Sys.*, vol. 23, no. 10, pp. 599–608, 1976.

[47] X. S. Li, "An aggregate function method for nonlinear programming," *Science in China (A)*, vol. 34, pp. 1467–1473, 1991.

Answer to Editor Comments

Point 1

While I am ok with your explanation of how the bound in [19] is applied, the resulting expression cannot be considered an outer bound as it is based on a thresholding scheme of channel gains in Eq. (7). I feel that it is important to clarify this in your paper so that the readers do not get confused with how the outer bound is derived. Please think of a suitable way of presenting the results that you claim are outer bounds on the problem.

Ans: We agree with the Editor that the definition of (10) as maximum outage achievable secrecy rate may be misleading. Therefore we have replaced it with the following sentences:

By applying the results in [19] an outer bound on the achievable secrecy rate of message M_k over the deterministic channels $\{\alpha^-_{k,\ell}, \alpha^+_{k,\ell}\}$, for a given power allocation $\boldsymbol{p}$ is

$$R_k^{\max}(\boldsymbol{p}) = \min_{j\neq k; 1\leq j\leq K} R_{k/j}(\boldsymbol{p})\,. \tag{10}$$

From (7) we can conclude that with probability larger than $(1-\epsilon)^{KL}$ the channel gains are such that the secrecy rate is upper bounded by (10). However, since we imposed a probabilistic constraint on the channel gains rather than the secrecy rate itself, $R_k^{\max}(\boldsymbol{p})$ is not an outage bound on the secrecy rate. Al already mentioned, this approach leads to easier computations, while a comparison with an outage secrecy bound is left for future study. Moreover, in the special case of full CSI ($\epsilon = 0$), (10) is an outer bound, and we will use it extensively in Section VI.

At the end of the same sub-section, with reference to the common rate again we added the following sentence:

Also (12) must be considered as a bound on the rate that can be achieved under constraints (7) on the channel gain, and in general is not a secrecy outage bound.