# Resource Allocation & Physical Layer Security in Wireless Communication Systems

**Sotiris Karachontzitis**

Department of Computer Engineering & informatics

University of Patras

This dissertation is submitted for the degree of
Doctor of Philosophy
at the
University of Patras

University of Patras July 2015

# Acknowledgements

First of all, I would like to sincerely thank my advisor Professor Kostas Berberidis for his leading and his generous support and encouragement during my PhD course. I will always be deeply indebted to him for the opportunity to pursue my doctoral dissertation and to grow up as a research scientist. I am also grateful to my co-advisor Professor Ioannis Krikidis for his constant guidance and his invaluable contribution in time, motivation and ideas, without of which it would be impossible for me to finish this work. I would like to express my special thanks to Professor Anastasios Dagiuklas and Dr. Stelios Timotheou for their valuable guidance and contributions during our collaborative research. Both of them are considered not only as brilliant professionals and colleagues but also as best friends. Further, I would like to thank my committee members, Professor Angeliki Alexiou, Professor Theodore Antonakopoulos, Professor Emmanouel Psarakis and Professor Emmanouel Varvarigos for their precious time and their valuable comments and suggestions. Also, I thank the members of the Signal Processing and Communications Lab, past and present, for all the time we shared together during my stay at the Lab. Finally, I would like to thank my parents for their unconditional support in my life and my sweet Angel for her continuous understanding and love. Thank you all!

# Abstract

In this thesis, the problem of resource allocation is investigated in multiuser, multi-antenna downlink wireless systems in which spatial multiplexing is employed in the physical layer. The thesis consists of two main parts; in the first, the interest is focused on optimizing system's performance in terms of users' transmission rate. Under this context, a low-complexity but highly performing user selection algorithm is presented for the flat-fading channel, when zero-forcing beamforming is employed at the BS and the aim is to maximize system's throughput. For the more interesting case where the transmission is performed simultaneously over a number of parallel subchannels, two fairness-aware resource allocation problems are investigated in the sense that certain QoS constraints are considered. Typically, this kind of problems fall within the NP class because of the integer nature of the involved user selection procedure. Hence, several near-optimal and heuristic solutions are proposed. In the second part of the thesis, the concept of physical layer security is integrated into the resource allocation procedure and the secrecy rate becomes the critical quantity of the considered problems. The considered setup consists of a multiuser downlink system in which a passive eavesdropper tries to wiretap the message of one or more users. First, the problem of secrecy rate balancing is investigated for a SISO downlink system in which transmission is performed over a set of parallel subchannels. Under the assumption that each subchannel is occupied exactly by one user, several optimal, near-optimal and heuristic solutions are proposed for several different problem settings. By assuming a multiantenna BS, the resource allocation problem is further enriched with spatial multiplexing within each subchannel. Thus, the thesis is completed with the investigation of two such problems in which secrecy-rate QoS constraints are also taken into consideration.

# Table of contents

# List of figures

# List of tables

# List of Algorithms

# Chapter 1

# Introduction

## 1.1 Precoding in multiantenna downlink channel

Precoding at the transmitter, *i.e.* spatial multiplexing of several independent data streams, is an effective way to increase spectral efficiency in multiuser, multiantenna downlink system [1]. In this section, we establish the fundamentals of the downlink precoding signal model which is under consideration in the following chapters.

Let assume a single-cell wireless system with a base station (BS) that is equipped with $T_x$ antenna elements and $U$ single antenna users, the set of which is denoted as $\mathscr{U} = \{1, \ldots, U\}$. In principle, precoding at the transmitter side requires the channels to be known and constant over some time period, which is high enough to send back the channel state information (CSI) from users to the BS. Under this assumption, the vector $\mathbf{h}_u(t) \in \mathbb{C}^{T_x}$ is used to denote the flat fading channel between the BS and the user $u \in \mathscr{U}$ at time instance $t$. Moreover, it is assumed that each one of these channels follows a circularly symmetric complex Gaussian distribution with zero mean and covariance matrix $\Sigma_{\mathbf{h}_u}, u \in \mathscr{U}$. Thus, the discrete time, baseband input-output model for user $u \in \mathscr{U}$ is

$$y_u(t) = \mathbf{h}_u^T(t)\,\mathbf{x}(t) + z_u(t), \qquad u \in \mathscr{U}, \tag{1.1}$$

where $y_u(t) \in \mathbb{C}$ is the received signal at time $t$, $\mathbf{x}(t) \in \mathbb{C}^{T_x}$ is the transmitted signal vector at time $t$ and $z_k(t) \in \mathbb{C}$ denotes the complex, additive white Gaussian noise (AWGN) with zero mean and variance $\sigma^2$ at time $t$[1]. In the most common case, the transmitted signal is subject to an average power constraint, *e.g* $Tr(\mathbf{R}_x) \leq P_T$, where $\mathbf{R}_x = \mathbb{E}\left\{\mathbf{x}\mathbf{x}^H\right\}$ and $P_T$ is the bound on average transmitted power.

[1] Without loss of generality, the time-index $t$ is omitted in the follow.

In literature, a number of different precoding schemes have been proposed of both linear and nonlinear nature [2]. In the following subsections, we briefly describe the precoding techniques which will be mentioned and be employed in the later chapters.

### 1.1.1 Beamforming transmission

Beamforming is a linear processing technique to spatially multiplex the independent data streams of a number of users. Let $\mathscr{K} = \{1,\ldots,K\} \subseteq \mathscr{U}$ denotes the subset of the users which are spatially multiplexed. In beamforming transmission, it holds that $|\mathscr{K}| \leq T_x$ and the transmitted signal vector from the BS over one symbol period is of the form [3]

$$\mathbf{x} = \sum_{k=1}^{K} \mathbf{w}_k \sqrt{p_k} s_k, \tag{1.2}$$

where $s_k$ is a complex scalar denoting the information symbol of user $k \in \mathscr{K}$, $\mathbf{w}_k \in \mathbb{C}^{T_x}$ is the corresponding beamforming column-vector and $p_k \in \mathbb{R}_+$ is the corresponding power loading. Without loss of generality, we assume that $\mathbb{E}\left\{|s_k|^2\right\} = 1, k \in \mathscr{K}$. The received signal of user $k \in \mathscr{K}$ is given as

$$y_k = \sum_{i\in\mathscr{K}} \mathbf{h}_k^T \mathbf{w}_i \sqrt{p_i} s_i + z_k = \mathbf{h}_k^T \mathbf{w}_k \sqrt{p_k} s_k + \sum_{i\in\mathscr{K}, i\neq k} \mathbf{h}_k^T \mathbf{w}_i \sqrt{p_i} s_i + z_k, \qquad k \in \mathscr{K}. \tag{1.3}$$

The signal to interference plus noise ratio (SINR) of user $k \in \mathscr{K}$ is equal to

$$SINR_k = \frac{|\mathbf{h}_k^T \mathbf{w}_k|^2 p_k}{\sum_{i\neq k} |\mathbf{h}_k^T \mathbf{w}_i|^2 p_i + \sigma^2}, \qquad k \in \mathscr{K}. \tag{1.4}$$

The transmission rate, in bits per channel usage (bpcu), is determined by the SINR as

$$R_k = \log_2(1 + SINR_k), \qquad k \in \mathscr{K}. \tag{1.5}$$

As can be seen by (1.4), the inter-user interference term in the denominator of SINR is mainly controlled by the beamforming design and the user selection procedure, *i.e.* which $K$ out of $U$ users are multiplexed in $\mathscr{K}$. In a multiuser system, the design of both these aspects may be a challenging issue since adaptation to one user potentially affects the transmission to the other users too.

### Zero Forcing Beamforming

In the case where zero forcing beamforming (ZFB) is used to multiplex the transmitted symbols, the inter-user interference term in (1.4) is completely eliminated at the transmitter side. The beamforming vectors are selected such that the zero interference condition be valid, meaning $\mathbf{h}_i^T \mathbf{w}_j = 0$, $\forall i, j \in \mathscr{K}, i \neq j$. The transmitted signal vector over one symbol period is written as

$$\mathbf{x} = \mathbf{W}\mathbf{D}\mathbf{s} \tag{1.6}$$

where $\mathbf{W} = [\mathbf{w}_1 \dots \mathbf{w}_K] = \mathbf{H}_{\mathscr{K}}^H \left(\mathbf{H}_{\mathscr{K}} \mathbf{H}_{\mathscr{K}}^H\right)^{-1} \in \mathbb{C}^{T_x \times K}$ is the beamforming matrix, $\mathbf{D} \in \mathbb{R}^{K \times K}$ is a diagonal power loading matrix with the vector $\left[\sqrt{p_1}, ..., \sqrt{p_K}\right]$ in the main diagonal and $\mathbf{s} = [s_1 \dots s_K] \in \mathbb{C}^K$ contains the unit energy information symbols destined to users in $\mathscr{K}$. Note that the matrix $\mathbf{H}_{\mathscr{K}} \in \mathbb{C}^{K \times T_x}$ contains as row vectors the channels of the users within set $\mathscr{K}$. In the special case where just a single user is contained within $\mathscr{K}$, ZFB coincides with maximum ratio transmission (MRT) to that user [3].

## 1.1.2 Nonlinear techniques

It is well known, that dirty paper coding (DPC) achieves the full capacity region in the multiantenna downlink channel [4, 5]. In DPC, the transmitted signal vector is written as $\mathbf{x} = \mathbf{W}\mathbf{s}$, where $\mathbf{W} \in \mathbb{C}^{T_x \times |\mathscr{U}|}$ denotes the precoding matrix and the column vector $\mathbf{s} \in \mathbb{C}^{|\mathscr{U}|}$ contains the unit energy information symbols of users within $\mathscr{U}$, which are generated by successive dirty-paper encoding with a predefined order [6]. The precoded channel yields the following input-output equation

$$y_u = \mathbf{h}_u^T \mathbf{w}_u s_u + \sum_{u,j \in \mathscr{K}, j<u} \mathbf{h}_u^T \mathbf{w}_j s_j + \sum_{u,j \in \mathscr{K}, j>u} \mathbf{h}_u^T \mathbf{w}_j s_j + z_u, \qquad u \in \mathscr{U}. \tag{1.7}$$

where $\mathbf{w}_u \in \mathbb{C}^{T_x}$ is the $u$-th column of the precoding matrix $\mathbf{W}$. In DPC, it is possible to spatially multiplex up to all the users of the system; by predefining an encoding order, the $u$-th symbol is encoded considering as known the interference caused by the users that have been preceded in the encoding order [6, 7]. At the receiver side, the $u$-th symbol is decoded considering as additive noise the transmission to the users that follow in the encoding order. As a result, the transmission rate of $u \in \mathscr{U}$ is given as

$$R_u = \log_2 \left(1 + \frac{\left|\mathbf{h}_u^T \mathbf{w}_u\right|^2}{\sigma^2 + \sum_{u,j \in \mathscr{K}, j>u} \left|\mathbf{h}_u^T \mathbf{w}_j\right|^2}\right), \qquad u \in \mathscr{U}. \tag{1.8}$$

Note that the transmission rate of each individual user depends on both the precoding matrix $\mathbf{W}$ and the encoding/decoding order of the users.

### Tomlinson-Harashima Precoding with Zero Forcing

As it was mentioned above, DPC is difficult to be implemented due to the highly complex multidimensional vector quantization process which is required. Tomlinson-Harashima Precoding (THP) is a well known, one-dimensional approach to apply DPC. In THP, interference elimination is achieved by adding a feedback filter at the transmitter side and using a modulo operation at both communicating ends [2]. Specifically, let $\mathscr{K} = \{1,\ldots,K\} \subseteq \mathscr{U}$ denotes the set of users which are multiplexed and that the natural order $1,\ldots,K$ is assumed as the encoding order. The information symbols of the selected users are encoded sequentially and a feedback filter $\mathbf{B}-\mathbf{I}$ is used at the transmitter side to eliminate the interference from the previously encoded symbols, where $\mathbf{B} \in \mathbb{C}^{K\times K}$ is a unit triangular matrix, *i.e* a triangular matrix with ones on the main diagonal. Moreover, a processing matrix $\mathbf{F} \in \mathbb{C}^{T_x\times K}$ is used to eliminate the residual interference [2]. In total, the transmitted signal vector is written as

$$\mathbf{x} = \mathbf{F}\mathbf{B}^{-1}\mathbf{D}\mathbf{v}, \tag{1.9}$$

where $\mathbf{D}$ is a $K\times K$ diagonal power loading matrix with vector $\left[\sqrt{p_1},...,\sqrt{p_K}\right]$ in the main diagonal and $\mathbf{v} \in \mathbb{C}^K$ is the effective data vector that is created by a modulo-based procedure over the information bearing vector $\mathbf{s} \in \mathbb{C}^K$ [8]. Stacking together all the received signals in the column vector $\mathbf{y} \in \mathbb{C}^K$, the system model of (1.1) becomes

$$\mathbf{y} = \mathbf{G}\mathbf{H}_{\mathscr{K}}\underbrace{\mathbf{F}\mathbf{B}^{-1}\mathbf{D}\mathbf{v}}_{=\mathbf{x}}+\mathbf{G}\mathbf{z}, \tag{1.10}$$

where $\mathbf{H}_{\mathscr{K}}$ is the $K\times T_x$ channel matrix of users in $\mathscr{K}$ and $\mathbf{G} \in \mathbb{R}^{K\times K}$ is a diagonal scaling matrix for the receiving symbols. When zero forcing condition is combined with THP, the interference term in (1.10) is eliminated, *i.e.* $\mathbf{G}\mathbf{H}_{\mathscr{K}}\mathbf{F}\mathbf{B}^{-1} = \mathbf{I}$. The matrices $\mathbf{F},\mathbf{B}$ and $\mathbf{G}$ can be obtained by performing the QR factorization $\mathbf{H}_{\mathscr{K}}^H = \mathbf{Q}\mathbf{R}$, where $\mathbf{R}$ is an $T_x\times K$ upper triangular matrix with real diagonal elements $r_{kk}, k = 1,\ldots,K$, and $\mathbf{Q}$ is an $T_x\times T_x$ unitary matrix. In such a case, $\mathbf{B} = \mathbf{G}\mathbf{R}^H$, $\mathbf{F} = \mathbf{Q}$ and $\mathbf{G} = \left[r_{11}^{-1},\ldots,r_{KK}^{-1}\right]$, *i.e.* the matrix $\mathbf{G}$ consists of the inverses of the diagonal elements of $\mathbf{R}$. Equation (1.10) yields the following input/output equation

$$\mathbf{y} = \mathbf{D}\mathbf{v}+\mathbf{G}\mathbf{z}, \tag{1.11}$$

where the variance of the $k$-th element of the noise $\mathbf{G}\mathbf{z}$ is given by $\sigma^2/r_{kk}^2$, $k = 1,\ldots,K$. As can be seen from (1.11), the spatial interference caused to the user $k \in \mathscr{K}$ by all the other users has been removed completely. Moreover, its signal to noise ratio (SNR) is given by

$\Gamma_k = \frac{r_{kk}^2 p_k}{\sigma^2}$, where the variable $r_{kk}^2$ follows a central chi-square distribution with $2\,(T_x - k + 1)$ degrees of freedom[2] [8].

[2] It is important to note that the degrees of freedom of the user's effective channel increases as long as it is placed earlier in the encoding order.

## 1.2 Transmission over parallel channels

In broadband wireless systems, transmission over parallel channels is widespread adopted as an efficient and simple implemented method to improve spectral efficiency and to provide flexibility in the resource allocation process. Commonly, the parallel channels are created by employing orthogonal frequency-division multiplexing (OFDM) transmission at both communicating ends [9]. In single user OFDM transmission, the total bandwidth of the system is divided into $N$ parallel, flat fading channels, called subchannels, and the single high-data-rate stream is divided into a number of lower rate streams that are transmitted simultaneously over the narrower subchannels. In multiuser case, orthogonal frequency-division multiple access (OFDMA) is a frequency modulation technique which also provides a (frequency-division) multiple access mechanism. In contrast to the static OFDM where a single user uses all the available bandwidth, in OFDMA a number of users is allowed to transmit simultaneously on the different subchannels, per OFDM symbol. This way, the inherent multiuser diversity of the system can be exploited and the overall spectral efficiency can be notably improved; given that the probability that all users experience a deep fade in a particular subchannels is very low, spectral efficiency is improved by assuring that subchannels are assigned to the users who have better channels. In addition, OFDMA is naturally combined with multiantenna transmission [10]. In the following chapters, we adopt the MISO-OFDM block fading model, where each subchannel remains constant for a large enough block of symbols to perform resource allocation and varies independently across blocks[3]. In each block, one codeword is transmitted spanning the length of the whole block. The codeword is generated using an encoder chosen for the particular block based on the channel gains. Assuming, further, perfect synchronization in all communicating ends, the following compact and simple signal model results for the received signal of user $u \in \mathscr{U}$ within the subchannel $n \in \mathscr{N}$

$$y_{n,u} = \mathbf{h}_{n,u}^T \mathbf{x}_n + z_{n,u}, \qquad n \in \mathscr{N},\ u \in \mathscr{U}, \tag{1.12}$$

where $\mathscr{N} = \{1, \ldots, N\}$ denotes the set of subchannels, the vector $\mathbf{x}_n \in \mathbb{C}^{T_x}$ denotes the transmitted signal and the vector $\mathbf{h}_{n,u} \in \mathbb{C}^{T_x}$ denotes the channel of user $u \in \mathscr{U}$ within $n \in \mathscr{N}$, respectively. In the most common case, the transmitted signal is subject to either an overall average power constraint across all the subchannels or individual power bounds per subchannel. The general MISO-OFDMA resource allocation problem consists of determining which subchannels are assigned to which users, which possible spatial multiplexing technique will be used and what will be the power allocation per subchannel and/or user. In general, solving such a problem in an optimal way is often an intractable task [11].

[3] The block fading model allows the application of information theoretic results in each block separately

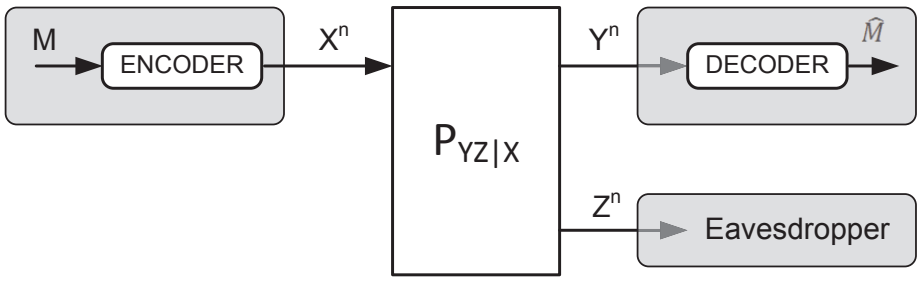



Fig. 1.1 Wiretap channel model.

## 1.3 Physical layer security

In a secret communication scenario, a sender wishes to reliably and confidentially transmit a secret message to an intended receiver in the presence of a passive eavesdropper. The fundamentals of physical layer security and the information-theoretic notion of secrecy capacity are defined in [12] using the model illustrated in Fig. 1.1. The objective for the transmitter is to send a message (represented by the random variable $M$) at rate $R$ by encoding it into a codeword of length $n$ (noted as $X^n$) and transmit the symbols over a noisy memoryless broadcast channel, characterized by the transition probability $P_{Y,Z|X}$. The legitimate receiver observes the signal $Y^n$ and should be able to make a correct estimation of the transmitted message with high probability. The eavesdropper observes $Z^n$ and should obtain no information about the message $M$. A code for this communication problem is called a wiretap code. A secret communication $R$ rate is achievable if there exists a sequence of wiretap codes with increasing block length $n$, such that

$$\lim_{n\to\infty} P_r\left(M \neq \widehat{M}\right) = 0 \quad \text{(reliability)} \quad \text{and} \quad \lim_{n\to\infty} I(M;Z^n) = 0 \quad \text{(secrecy)} \tag{1.13}$$

where $\widehat{M}$ is the estimation of $M$ made by the legitimate receiver and $I(M;Z^n)$ is the mutual information between $M$ and $Z^n$.

In general, it is not a-priori obvious that wiretap codes exist with nontrivial rates. In fact, the reliability requirement in reception calls for the introduction of redundancy in the encoder to fight the effect of the noise. On the other hand, the secrecy requirement for Eve would intuitively call for limiting such redundancy to avoid leaking information. Perhaps surprisingly, it turns out that simultaneously satisfying both requirements is sometimes possible. In particular, one can characterize the secrecy capacity, defined as the supremum of all achievable rates with wiretap codes. In other words, it is defined as the maximum achievable rate such that perfect secrecy is maintained, in the sense that the receiver can decode the secret message with negligible decoding error probability while the eavesdropper cannot decode the secret message. The secrecy capacity can be viewed as the counterpart of the

traditional channel capacity, when a secrecy requirement is imposed. It can be shown that it is given by[4] [13, 14]

$$C^{sc} = \max_{V \to X \to YZ} \left( I(V;Y) - I(V;Z) \right) \tag{1.14}$$

where $V$ is an auxiliary random variable and $V \to X \to YZ$ denotes a Markov chain between variables $V, X$ and $YZ$. Note that the secrecy capacity is positive provided $I(V;Y) - I(V;Z)$ is positive; in particular, if $Y = Z$, then the secrecy capacity is zero.

Recently, there is a lot of interest to integrate physical layer security into the problem of resource allocation in multiuser, multiantenna channels. In this section, we develop the secret communication signal model that is used in the following chapters. A multiuser downlink channel is considered in which the BS has $T_x$ antenna elements and all the users and the eavesdropper have a single antenna. The case of passive eavesdropping is considered in which one or more eavesdroppers aim to wiretap the message of one or more communicating users. Let the vector $\mathbf{h}_u \in \mathbb{C}^{T_x}$ denotes the channel between the BS and the user $u \in \mathscr{U}$. As previously, a slow-varying block fading model is assumed, meaning that all the channels remain constant over a block of large number of symbols and they vary independently across the blocks. When the BS transmits only to the user $u \in \mathscr{U}$, its received signal is given by (1.1). The corresponding signal received by the eavesdropper is given as

$$y_e = \mathbf{h}_e^T \mathbf{x} + z_e, \tag{1.15}$$

where the row-vector $\mathbf{h}_e \in \mathbb{C}^{T_x}$ denotes the channel between the BS and the eavesdropper and $z_e \in \mathbb{C}$ is the complex AWGN with zero mean and variance $\sigma^2$. The secrecy capacity of user $u \in \mathscr{U}$, under an average transmit power bound constraint, is defined as [15–17]

$$C_u^{sc} = \left[ \max_{\mathbf{x}: \mathbb{E}\{\mathbf{x}^H \mathbf{x}\} \le P_T} \left( \log_2 \left( 1 + \frac{|\mathbf{h}_u^T \mathbf{x}|^2}{\sigma^2} \right) - \log_2 \left( 1 + \frac{|\mathbf{h}_e^T \mathbf{x}|^2}{\sigma^2} \right) \right) \right]^+, \quad u \in \mathscr{U}. \tag{1.16}$$

where $[a]^+$ stands for the maximum between $a \in \mathbf{R}$ and 0, *i.e.* $[a]^+ = \max\{a, 0\}$. Note that the secrecy capacity $C^{sc}$ is nonzero, when user's SNR is higher than the SNR of the eavesdropper, *i.e.* when $|\mathbf{h}_u^T \mathbf{x}| > |\mathbf{h}_e^T \mathbf{x}|$.

In single user transmission, it has be shown that $C_u^{sc} = [\log_2 \lambda_{max}]^+$ and that the secrecy capacity is achieved by beamforming along the direction of $\psi_{max}$, where $(\lambda_{max}, \psi_{max})$ denotes the generalized eigenvalue-eigenvector pair of matrices $\left(\mathbf{I} + P_T \mathbf{h}_u^H \mathbf{h}_u\right)$ and $\left(\mathbf{I} + P_T \mathbf{h}_e^H \mathbf{h}_e\right)$ that corresponds to the maximum eigenvalue [16]. In the multiuser case, the notion of secrecy capacity region is defined as the $|\mathscr{U}|$-space volume in which the simultaneous transmission to the several users of the system is completely secured and error free. Again, (1.16)

[4] The memoryless discrete-time fading channel is an important example for which the secrecy capacity is completely known

quantifies the difference between each user and the eavesdropper's capacity. In principle, secrecy capacity achieving transmission is based on DPC-like processing which is difficult to be implemented in practice [18–20]. Thus, the interest is also focused on exploring the performance of low-complexity precoding schemes such that discussed in Section 1.1. Finally, the concept of secrecy capacity is extended in an straightforward manner for systems that transmit over a number of parallel independent channels. In such case, the overall resource allocation problem is refreshed to integrate also secrecy-oriented objectives and constraints. A comprehensive technical guide covering basic concepts, recent advancements, and open issues in providing communication security at the physical layer is [21].

## 1.4 Thesis outline

In this thesis, we initially investigate the problem of resource allocation in multiuser, multiantenna downlink in order to optimize throughput-aware metrics of the system's performance. Then, we integrate the notion of secrecy rate into the considered resource allocation problem and we seek for solutions that provide also physical-layer security. The organization of the rest of the thesis is as follows:

In Chapter 2, the problem of resource allocation in multiantenna, multiuser downlink channel is considered when zero-forcing beamforming is used at the BS to spatially multiplex several users at the same time. The interest is focused on optimizing system's performance in terms of users' transmission rate. First, a greedy user selection algorithm is proposed for the problem of throughput maximization in MISO flat fading channel. The algorithm approaches closely to the optimal spectral efficiency using zero-forcing beamforming, while it has a notable less computational complexity from other proposed solutions. Later, the problem of resource allocation when the transmission is performed over a number of parallel channels is investigated. Typically, this kind of problems fall within the NP-hard class. Thus, several near-optimal and heuristic resource allocation schemes are proposed when fairness-aware optimization criteria and QoS constraints are considered. Finally, the effect of chunk-based resource allocation over the system's throughput is investigated and an efficient user selection algorithm is presented, which exploit both spatial and frequency diversity of the system. This chapter, as conference papers, appeared in Proceedings of IEEE International Conference on Multimedia and Expo (ICME), 2011, IEEE Symposium on Computers and Communications (ISCC) in 2011 and IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC) in 2009.

In Chapter 3, we study a setup in which a BS transmits over a number of data-bearing parallel channels, each of which is assigned to exactly one user but it is also wiretapped by a passive eavesdropper. The eavesdropper is a "honest-but-curious" legitimate user which illegally starts wiretapping the messages of the other authorized users. The aim is to maximize the minimum secrecy rate over the users and it is formulated as a mixed integer nonlinear program (MILNP). Thus, a number of resource allocation schemes are developed for different parameter settings of the setup. This chapter appeared in IEEE Transactions on Information Forensics & Security in 2015 as a journal paper and in part in the Proceedings of International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) in 2014 as a conference paper.

In Chapter 4, we study two resource allocation problems which consider physical layer security in multiantenna, multiuser downlink system; in the first one, we aim to solve a user selection and power allocation problem in order to maximize the worst sum secrecy rate in a MISO flat fading setup, in the sense that a passive eavesdropper is able to decode the message of all the spatially multiplexed users. In the second, we assume a multiantenna system that transmits over a number of parallel channels and serves both conventional and

secured sensitive users, *i.e* users that should be protected by passive eavesdropping. The aim is to exploit the additional degrees of freedom offered by the multiple antennas to maximize system's throughput under a secrecy rate constraint for the secured sensitive users. This chapter, as conference papers, appeared in Proceedings of IEEE Wireless Communications and Networking Conference (WCNC) in 2014 and IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC) 2013.

In Chapter 5, the conclusions and two future research directions are briefly discussed related with the material of this thesis.

## 1.5 Author's publication list

**Publications which are included in this thesis**

- S. Karachontzitis, S. Timotheou, I. Krikidis and K. Berberidis, "Security-aware max-min resource allocation in multiuser OFDMA downlink," in *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 529–542, Mar. 2015.

- S. Karachontzitis, S. Timotheou, I. Krikidis and K. Berberidis, "Fair resource allocation in multiuser OFDMA downlink with passive eavesdropping," in *IEEE* $10^{th}$ *International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Larnaca, Oct. 2014, pp. 622–627.

- S. Karachontzitis, S. Timotheou and I. Krikidis, "Throughput maximization in multiantenna OFDMA downlink under secrecy rate constraints," in *IEEE Wireless Communications and Networking Conference (WCNC)*, Constantinople, Apr. 2014, pp. 410–415.

- S. Karachontzitis, I. Krikidis and K. Berberidis, "User selection schemes for multiuser MISO downlink with eavesdropping," in *IEEE* $14^{th}$ *Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Darmstadt, Jun. 2013, pp. 280–284.

- S. Karachontzitis, T. Dagiuklas and L. Dounis, "Novel cross-layer scheme for video transmission over LTE-based wireless systems," in *IEEE International Conference on Multimedia and Expo (ICME), Workshop on Streaming and Media Communications (StreamComm)*, Barcelona, Jul. 2011, pp. 1–6.

- S. Karachontzitis and T. Dagiuklas, "A chunk-based resource allocation scheme for downlink MIMO-OFDMA channel using linear precoding," *IEEE Symposium on Computers and Communications (ISCC)*, Corfu, Jul. 2011, pp. 931–936.

- S. Karachontzitis and D. Toumpakaris, "Efficient and low-complexity user selection for the multiuser MISO downlink," *IEEE* $20^{th}$ *International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Tokyo, Sep. 2009, pp. 3094–3098.

**Other publications**

- S. Timotheou, I. Krikidis, S. Karachontzitis and K. Berberidis, "Spatial domain simultaneous information and power transfer for MIMO channels," in *IEEE Trans. Wireless Commun.*, vol. 14, pp. 4115–4128, Aug. 2015.

- S. Karachontzitis, T. Dagiuklas and L. Dounis, "Fair cross-layer scheme for heterogeneous H.264/AVC video streams over LTE-based broadband systems," in *International Wireless Communications & Mobile Computing Conference (IWCMC)*, Lemessos, Aug. 2012, pp. 1006–1010.

- A. Stavridis, S. Karachontzitis and K. Berberidis, "Bezout-based robust precoding for MIMO frequency selective channel using imperfect channel knowledge," *European Signal Processing Conference (EUSIPCO)*, Barcelona, Sep. 2011, pp. 649–653.

- H. Zhu, S. Karachontzitis and D. Toumpakaris, "Low-complexity resource allocation and its application to distributed antenna systems," *IEEE Wireless Commun. Mag.* , vol. 57, pp. 44–50, Jun., 2010.

- V.U. Prabhu, S. Karachontzitis and D. Toumpakaris, "Performance comparison of limited feedback codebook based downlink beamforming schemes for distributed antenna systems," *Wireless VITAE 2009*, Aalborg, Sep. 2009, pp. 171–176.

# Chapter 2

# Resource Allocation in multiuser, multiantenna downlink channel using SDMA

## 2.1 Introduction

In multiuser downlink MISO, DPC is the optimal transmission technique to maximize system's throughput [4], [22]. However, practical implementation of DPC still remains a challenging task, mainly because it requires sophisticated random and interference-dependent coding/decoding. Under this perspective, linear-based space-division multiple access (SDMA) is a very promising way to overcome this drawback and to provide notable spectral efficiency improvement at the same time [23], [24], [25]. A practical constraint imposed by a linear processing transmission is that the number of simultaneously serviced users can be up to a specific number. Otherwise, users' signal separation is not possible. As a result, in a multiuser system, linear processing transmission is always in a bind with a user selection policy which aims to specify the subset of users that will be serviced simultaneously. Clearly, the design of a user selection policy depends heavily on the condition of the system, *e.g.* current users' channels quality. Nevertheless, it also depends on the considered design objectives and QoS constraints. In a system that transmits over a set of parallel channels, *e.g.* by employing OFDMA transmission, the linear processing design and the problem of user selection are enriched further with an extra dimension that dictates which user (or group of users) is serviced within each one of the parallel channels. The overall problem, referred as resource allocation problem, is of combinatorial nature and falls within the NP-class of problems. Thus, in principle, it is intractable to be solved in an optimal way, especially as its size scales with respect to the number of users, the number of parallel channels and the number of antennas at the BS [11]. As a result, it is of high interest to present heuristic

solutions with high efficiency in terms of both performance and computational complexity [1], [26].

### State of the art

In multiuser, multiantenna downlink wireless communication systems, the problem of throughput maximization has been extensively investigated in terms of precoding and user selection design. In [27], an optimal algorithm is presented based on uplink-downlink duality which is extended to the case of weighted throughput maximization in [28]. Several reduced-complexity suboptimal variations for throughput maximization have been presented in [29], [30], where nonlinear, DPC-based transmission is combined with user scheduling. Interestingly, they achieve optimality in scaling laws with respect to the number of users and users' SINR. Other nonlinear precoding schemes are presented in [31], [32]. However, the real time implementation of nonlinear processing algorithms is still a difficult and complex task, especially when the number of users and the number of antennas are large. Under this scope, ZFB-based transmission is a promising alternative. In [33–37], ZFB is combined with low-complexity user selection policies to present efficient transmission schemes in terms of throughput which achieves a large portion of the optimal performance, with significantly lower computational complexity [25]. Several other low-complexity designs which aim to optimize a variety of objective criteria and QoS constraints are proposed in [26, 38–40]. For a thorough discussion of the subject, the interest reader may refer to [41].

In wireless systems that transmit over a number of parallel channels (subchannels), a typical resource allocation problem considers not only the subchannel-group of users binding but also the design of the beamforming matrices within subchannels, the adjustment of allocated power per subchannel and user, QoS guarantees etc. One common assumption that simplifies the resource allocation problem is to allow the transmission to only one user per subchannel. In [42–45], several solutions are presented for a variety of optimization objectives under the assignment assumption of a single user per subchannel. However, in multiuser, multiantenna systems it is beneficial to employ spatial multiplexing within each one subchannel. Towards this direction, [46–48] have focused on allocating resources to maximize systems' throughput, while [49–55] have focused on optimizing several fairness-aware constrained problems. In general, the problem of jointly finding the optimal beamforming and subchannel-user binding is a non-linear, nonconvex one. In [56], the problem of throughput maximization is considered under the assumption that ZFB is employed within the subchannels. In [57–59], several other objectives are studied under the same assumption. For a thorough discussion, the reader may refer to [53], [60].

In a system that transmit simultaneously over a number of subchannels, the correlation between adjacent subchannels can be exploited to reduce the signal overhead and computational complexity of the resource allocation procedure. Towards this direction, one approach is to combine a set of contiguous subchannels (called chunk) into one entity and

perform resource allocation on chunk basis [61]. Clearly, chunk-based resource allocation may achieve just a portion of the performance of the subchannel-based resource allocation. In the majority of existed works, chunk-based resource allocation is performed using a single, representative value for each chunk, *e.g.*, the mean value of subchannels' quality within the chunk or the quality of the median subchannel [53], [62]. However, this way the frequency selectivity of the system is ignored and the benefits that come from the inherent frequency diversity gain are missed. In broadband wireless systems, it is not uncommon, the coherence bandwidth to exceed the subchannel bandwidth and to be comparable to the chunk-size. Hence, there is a high probability for a user to have high (low) channel quality in a portion of the chunk and low (high) in another one portion. By taking this feature into consideration in the chunk-based resource allocation it is possible to further close the performance gap with respect to the subchannel-based resource allocation and to reduce the signal overhead and the computational complexity at the same time [63], [64].

### Contribution

In this chapter, the problem of resource allocation in multiantenna, multiuser downlink channel is considered when ZFB is used to spatially multiplex several users at the same time. The interest is focused on optimizing system's performance in terms of users' transmission rate. Specifically, the contribution in this chapter is as follows:

- A greedy user selection algorithm is proposed for the problem of throughput maximization in flat fading channel. The algorithm approaches the optimal performance in terms of spectral efficiency when ZFB is employed, while it has a notable less computational complexity from other proposed solutions.
- A number of near-optimal and heuristic resource allocation schemes are proposed for the problem of resource allocation over parallel subchannels when fairness-aware optimization criteria and QoS constraints are considered. Typically, this kind of problems fall within the NP-hard class. Thus, emphasis it is given to present highly-performing solutions with polynomial computational complexity.
- The effect of chunk-based resource allocation over the system's throughput is investigated and an efficient user selection algorithm is presented which exploit both spatial and frequency diversity of the system.

The organization of the rest of the chapter is as follows. In Section 2.2, a polynomial complexity user selection algorithm is presented for the problem of throughput maximization in flat fading channel. In Section 2.3, we investigate two fairness-aware resource allocation problems when the transmission is performed over a number of parallel channels and present several solutions. Finally, in Section 2.4, chunk-based resource allocation is investigated in order to maximize system's throughput.

## 2.2 A low-complexity user selection algorithm for maximizing throughput

In this section, the objective is to specify the subset of the users which maximizes the throughput (sum rate) of a multiuser, multiantenna system when ZFB is employed and an average transmit power constraint holds. Let $\mathscr{U}$ denotes the set of the users in the system and $\mathscr{K} \subset \mathscr{U}$ denotes the subset of multiplexed users. Specifically, the problem to be solved is the following

$$\begin{aligned} \max_{\mathscr{K}\subseteq\mathscr{U},p_k} \quad & \sum_{k\in\mathscr{K}} R_k(p_k) \\ s.t. \quad & Tr(\mathbb{E}\left\{\mathbf{x}\mathbf{x}^H\right\}) \leq P_T, \\ & |\mathscr{K}| \leq T_x, \end{aligned} \tag{2.1}$$

where $P_T$ is the total available amount of power, $R_k(p_k) = \log_2\left(1+p_{n,k}\right)$ is the transmission rate of user $k \in \mathscr{K}$ and $\mathbf{x}$ is the transmitted signal vector. Let $\mathbf{H}_{\mathscr{K}} \in \mathbb{C}^{|\mathscr{K}|\times T_x}$ denotes the channel matrix which has as row-vectors the channels of the users within $\mathscr{K}$. Given the set $\mathscr{K}$, the optimal power allocation in terms of throughput is given as [3]

$$p_k = c_k(\mathscr{K})\left[\frac{\lambda}{\ln 2} - \frac{1}{c_k(\mathscr{K})}\right]^+, \qquad k \in \mathscr{K}, \tag{2.2}$$

where $\lambda \geq 0$ is the Lagrange multiplier of the power constraint in (2.1) and $c_k(\mathscr{K})$ is the effective channel of the user $k \in \mathscr{K}$, which is given by the inverse of the diagonal element of the matrix $\left(\mathbf{H}_{\mathscr{K}}\mathbf{H}_{\mathscr{K}}^H\right)^{-1}$ that corresponds to the user $k$. The system's throughput is

$$R_{ZFB}^{thr}(\mathscr{K}) = \sum_{k\in\mathscr{K}} \left[\log_2(\mu c_k(\mathscr{K}))\right]^+, \tag{2.3}$$

and the Lagrange multiplier $\lambda$ is calculating by solving the water-filling equation

$$\sum_{k\in\mathscr{K}}\left[\frac{\lambda}{\ln 2} - \frac{1}{c_k(\mathscr{K})}\right]^+ = P_T.$$

When the set $\mathscr{K}$ is unknown, the problem in (2.1) is a combinatorial one. The optimal solution can be obtained by employing an exhaustive search policy over all different possible groups of users with cardinality up to $T_x$. Let $S = \sum_{i=1}^{T_x}\binom{|\mathscr{U}|}{i}$ denotes this number. Clearly, the computational complexity of the exhaustive search approach becomes prohibitive when the $\mathscr{U}$ contains a large number of users. In the following, a low-complexity user selection al-

gorithm is presented which is based on the metric of normalized spatial correlation between the channels of the users.

The normalized spatial correlation between the channels of any two users $i, j \in \mathscr{U}$, is given as

$$\rho_{i,j}\left(\mathbf{h}_i, \mathbf{h}_j\right) \triangleq \frac{\left|\mathbf{h}_i^H \mathbf{h}_j\right|}{\|\mathbf{h}_i\|_2 \left\|\mathbf{h}_j\right\|_2} = \left|\cos\left(\theta_{i,j}\right)\right|, \qquad i, j \in \mathscr{U}, \tag{2.4}$$

where $0 \leq \theta_{i,j} \leq 2\pi$ is the angular between the channels of the users $i$ and $j$ and $0 \leq \rho_{i,j}(.) \leq 1$. The user selection algorithm, called Correlation-based User Selection Algorithm (CUSA), is described in Algorithm 1. In principle, orthogonalization and interference elimination between two strongly correlated users requires a significant amount of power to be spent by ZFB. Thus, a smaller portion of the available power remains to be used for throughput maximization. The CUSA takes advantage of the inherent multiuser diversity of the system to output a group of simultaneously transmitting users with low average mutual correlation. In CUSA, the user transmission group $\mathscr{K}$ is built in an iterative manner by using the normalized spatial correlation metric defined in (2.4). The user with the strongest channel gain is selected in the first iteration, while up to $T_x - 1$ more iterations may follow. In each iteration, one more user is added to the transmission group, if its insertion increases the throughput. In each one of these iterations, a set of users (denoted as $\mathscr{A}$), is formulated which contains the unselected users with the $L$ smallest values of average spatial correlation to the users that have been already inserted in $\mathscr{K}$. The value of $L$ is given as an input parameter to the algorithm. The justification of using the set $\mathscr{A}$ is based on the fact that the throughput of a transmission group is affected by both the correlation between its users and the strength of their channels; formulating the set $\mathscr{A}$ is a way to balance the role of correlation and channel gain and enrich the essential multiuser diversity in the selection options per iteration. One-by-one the elements of $\mathscr{A}$ are examined for possible addition in $\mathscr{K}$; each element is temporary added to $\mathscr{K}$ and the new throughput is calculated. The element that leads to the maximum increase in throughput (if there is such) is permanently inserted into $\mathscr{K}$ and the next iteration begins. Otherwise, the transmission group remains the same and the procedure terminates.

In each iteration of CUSA, the average correlation between each unselected user and the users in $\mathscr{K}$ must be calculated. This procedure requires $\mathscr{O}(UT_x)$ since the calculation of $\rho_{i,j}(.)$, $i, j \in \mathscr{U}$, is done in $\mathscr{O}(T_x)$. In step 9), the throughput $R_{ZFB}^{thr}(\mathscr{K} \cup a)$ is calculated for each element of $\mathscr{A}$. To complete each one of these calculations, the effective channels of users in $\{\mathscr{K} \cup a\}$ and the Lagrange multiplier $\lambda$ must be determined. The first can be done in $\mathscr{O}\left(m^2\right)$, $m \leq T_x$, by using matrix inversion lemma and the effective channels from the previous iteration [65]. The Lagrange multiplier can be specified in $\mathscr{O}\left(\log_2 \varepsilon^{-1}\right)$ by using a bisection method over it with predefined required accuracy $\varepsilon > 0$. Given that

**Algorithm 1:** Correlation-based user selection algorithm (CUSA)

Input: channels $\mathbf{h}_u, u \in \mathscr{U}$ and parameter $L$.
Set $\mathscr{K} = \emptyset$, $\mathscr{A} = \emptyset$ and $m = 1$.
Specify user $k^* = \arg\max_{k \in \mathscr{U}} \|\mathbf{h}_k\|$.
Set $\mathscr{K} = \{k^*\}$.
**while** $m < T_x$ **do**
  Set $m = m + 1$.
  Let $Cor_i = \sum_{k \in \mathscr{K}} \rho_{k,i}(\mathbf{h}_k, \mathbf{h}_i)$, $i \in \mathscr{U} \setminus \mathscr{K}$, where $\rho_{k,i}(\bullet)$, $k \in \mathscr{K}$, $i \in \mathscr{U} \setminus \mathscr{K}$, is given by (2.4).
  Let $\mathscr{A}$ denotes the set of users in $\mathscr{U} \setminus \mathscr{K}$ which have the $L$ lowest values $Cor_i$.
  Specify user $a^* = \arg\max_{a \in \mathscr{A}} R_{ZFB}^{thr}(\mathscr{K} \cup a)$.
  **if** $R_{ZFB}^{thr}(\mathscr{K} \cup a^*) > R_{ZFB}^{thr}(\mathscr{K})$ **then**
    Set $\mathscr{K} = \{\mathscr{K} \cup a^*\}$.
  **else**
    $m = T_x$.
  **end if**
**end while**
Calculate system's throughput by using $\mathscr{K}$ and (2.2) and (2.3).

up to $T_x$ iterations may be performed, the overall computation complexity of CUSA is $\mathscr{O}\left(\left(UT_x + LT_x^2 \log \varepsilon^{-1}\right) T_x\right)$.

### Numerical results

In Fig. 2.1a, the average throughput of CUSA is depicted as a function of $P_T$ and it is compared with DPC and ZFB with exhaustive search over each possible transmission group (ZFB-Exh). The throughput of DPC is calculated by the iterative algorithm presented in [27] using 50 iterations and it is included in the Fig. 2.1a to reveal the throughput loss by using ZFB for spatial multiplexing. As can be seen, CUSA performs very close to the best that can be achieved by using ZFB. For instance, it achieves more than 95% of the ZFB-Exh throughput for $T_x = 4$ and $P_T = 10$dB. In Fig. 2.1b, the effect of cardinality of set $\mathscr{A}$ (parameter $L$) is shown over the system's throughput. Clearly, the value of $L$ affects both the throughput and the computational complexity of the algorithm. Nevertheless, there is no significant improvement in throughput by the increase of $L$ beyond a certain point.

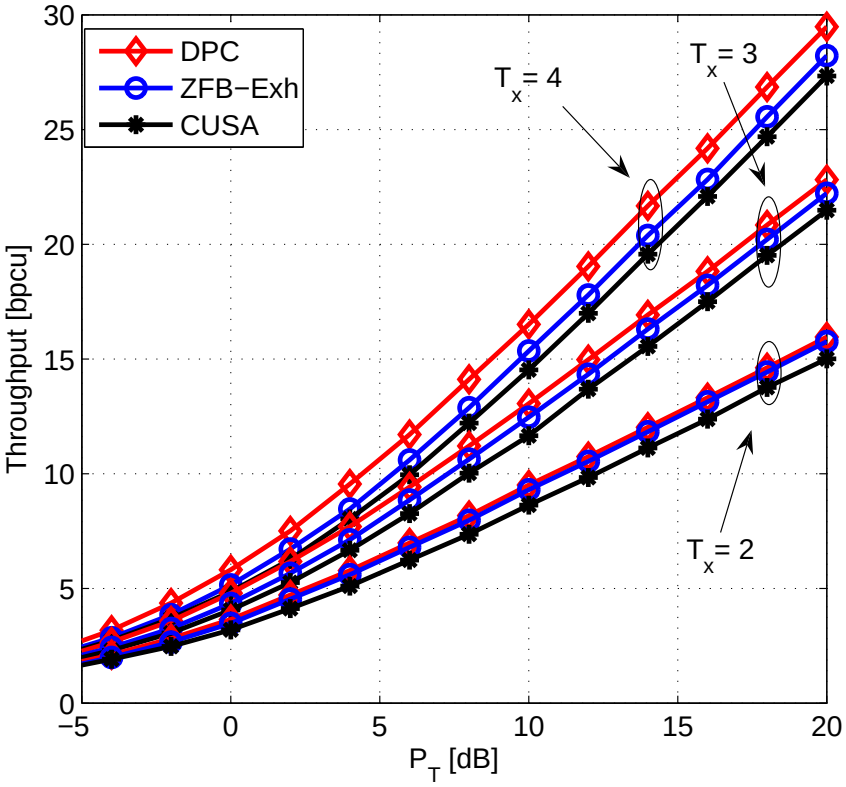
In Fig. 2.2a, the throughput of CUSA is compared to other three ZFB-based user selection algorithms, namely zero forcing scheduling (ZFS) proposed in [33], semi-orthogonal user scheduling (SUS) proposed in [35] and greedy correlated scheduling (GCS) proposed in [66]. All the three algorithms are of greedy nature, in the sense that iteratively built the transmission group based on some well-defined grouping metric. As can be seen, CUSA, ZFS and SUS perform very close to each other with a slight superiority of ZFS over the other two. Moreover, all three of them are superior than GCS. Nevertheless, the complex-

Table 2.1 Percentage of times the user with $l^{th}$ lowest average spatial correlation (to the already selected users) is selected, $L = T_x = 4$.

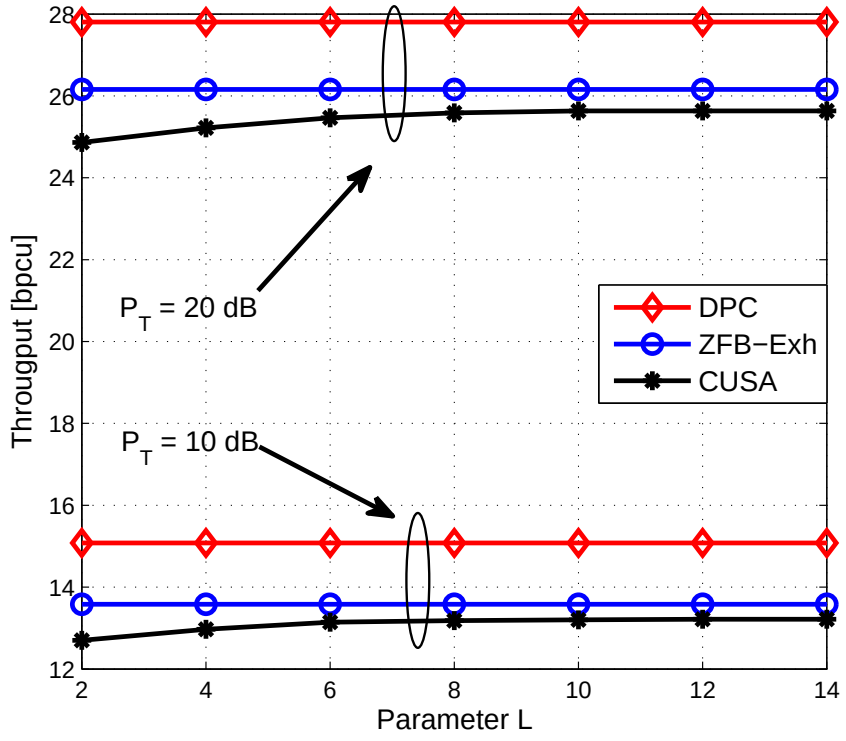
| $P_T$ | 0 $dB$ | 5 $dB$ | 10 $dB$ | 20 $dB$ |
|---|---|---|---|---|
| $1^{st}$ iteration | [27, 26, 24, 23] | [26, 26, 25, 23] | [26, 26, 25, 23] | [27, 26, 24, 23] |
| $2^{nd}$ iteration | [33, 26, 20, 17] | [33, 27, 22, 18] | [32, 27, 22, 19] | [31, 27, 22, 20] |
| $3^{rd}$ iteration | [09, 04, 02, 02] | [36, 18, 12, 8] | [44, 25, 17, 13] | [44, 25, 18, 13] |

ity of ZFS and SUS is one order of magnitude higher than the complexity of CUSA with respect to $T_x$. This is because ZFS updates its transmission group by examining all the unselected users for possible addition per iteration, while the transmission group in SUS is built in parallel with a semi-orthogonal basis in which the channels of the selected users are projected. The throughput of all the above mentioned algorithms versus the number of users $U$ is depicted in Fig. 2.2b for $P_T = 10$dB and $T_x = 4$. Again, it can be noticed that CUSA, ZFS and SUS exploit almost identical the inherent multiuser diversity that is available in the system.

In GCS, the average spatial correlation criterion (2.2) is used to formulate the transmission group, similar to CUSA, but only the unselected user with the lowest average correlation is examined for possible addition per iteration. As a result, the performance is degraded by a constant gap versus CUSA. In order to emphasize the benefits from using the set $\mathscr{A}$, the percentage of the times the user with the $l^{th}, l = 1, \ldots, |\mathscr{A}|$, lowest average correlation is selected per iteration of CUSA is shown in Table 2.1. As can be seen, there is almost equal probability to select any user from $\mathscr{A}$ in the first iteration. For instance, the vector $[27, 26, 24, 23]$ for $P_T = 0dB$ dictates that the lowest average correlated user is selected 27% of times, the second lowest 26% of times, the third lowest 24% of times and the forth lowest 23% of times. The same behavior is noted for other values of $P_T$. This explains the improvement in performance compared to the GCS, since not always the lowest correlated user leads to the maximum throughput increase. As can be seen, the lowest correlated user is selected more frequently as the iterations evolve.

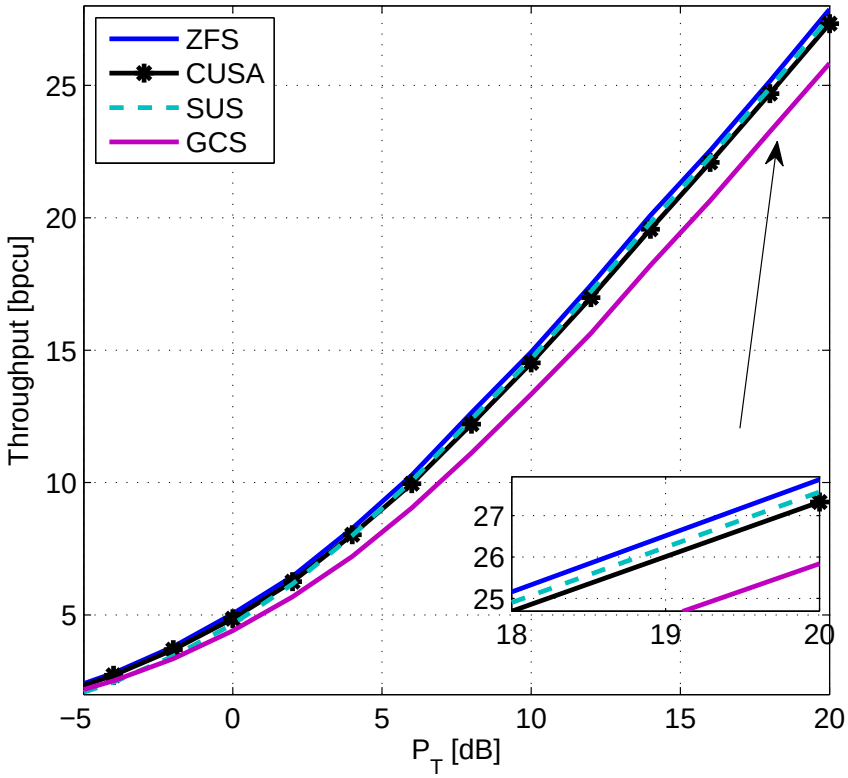



(a) Throughput vs $P_T$ for $U = 20$ and $L = T_x$.

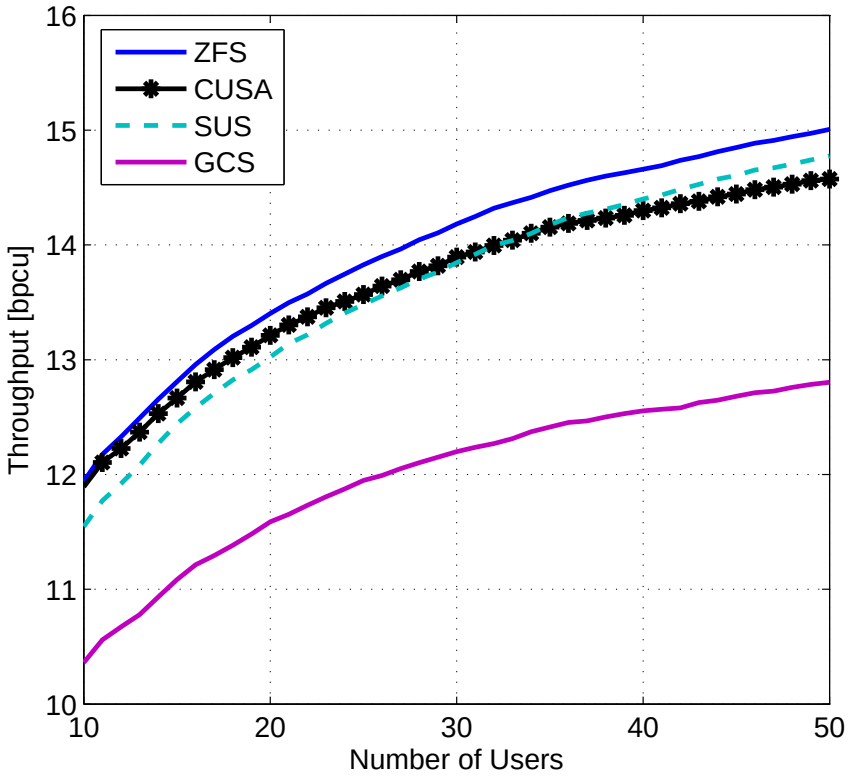



(b) Throughput of CUSA vs $L$ for $U = 20$ and $T_x = 4$.

Fig. 2.1 Throughput of CUSA.




(a) Throughput vs $P_T$ for $U = 20$.




(b) Throughput vs number of users for $P_T = 10dB$, $T_x = 4$.

Fig. 2.2 Comparison of throughput between CUSA and other user selection algorithms.

## 2.3 Resource allocation schemes in systems that transmit over parallel suchannels

When the transmission is performed over a number of parallel subchannels, the problem of resource allocation is enriched with an additional dimension which dictates the binding between users and subchannels. Let $\mathcal{N} = \{1,\ldots,N\}$ denotes the set of the subchannels of the system. Given that ZFB is employed within each subchannel, up to $T_xN$ spatial resources are opened, called spatial slots. The resource allocation algorithm has to decide which one of the different possible group of users is assigned to each subchannel, where $S = \sum_{l=1}^{T_x} \binom{|\mathcal{U}|}{l}$ denotes the number of different possible user sets with cardinality up to $T_x$. Clearly, the problem of resource allocation is NP-hard and it may become intractable as the problem's size increases, *i.e.* the number of users, subchannels and antennas increases. In the following subsections, we discuss two special resource allocation problems and we are interest to state near-optimal solutions of polynomial computational complexity with respect to the set optimization criteria.

### 2.3.1 Throughput maximization under individual user rate constraints

In this subsection, the objective is to assign spatial slots and allocate the available power in order to maximize the throughput, under guarantee individual rate constraints per user and a transmit power constraint. Let the binary variable $\omega_{n,\Phi_i}$ be equal to 1 when the subchannel $n \in \mathcal{N}$ is assigned to the set $\Phi_i$, where $\Phi_i \subseteq \{1,\ldots,U\}$, $i = 1,\ldots,S$, denotes a set of users with cardinality up to $T_x$ (otherwise $\omega_{n,\Phi_i} = 0$). The considered problem is

$$\max \sum_{n\in\mathcal{N}} \sum_{i=1}^{S} \omega_{n,\Phi_i} \sum_{k\in\Phi_i} R_{n,k}\left(p_{n,k}\right) \tag{2.5a}$$

$$s.t. \sum_{n\in\mathcal{N}} \sum_{i=1}^{S} \omega_{n,\Phi_i} \sum_{k\in\Phi_i} \frac{p_{n,k}}{c_{n,k}\left(\Phi_i\right)} \leq P_T \tag{2.5b}$$

$$\sum_{n\in\mathcal{N}} \sum_{i=1}^{S} \omega_{n,\Phi_i} R_{n,k}\left(p_{n,k}\right) \geq \overline{R}_k, \qquad k \in \mathcal{U}, \tag{2.5c}$$

$$\sum_{i=1}^{S} \omega_{n,\Phi_i} = 1, \qquad n \in \mathcal{N}, \tag{2.5d}$$

$$p_{n,k} \geq 0, \qquad k \in \mathcal{U}, n \in \mathcal{N}, \tag{2.5e}$$

$$\omega_{n,\Phi_i} \in \{0,1\}, \qquad n \in \mathcal{N}, i = 1,\ldots,S.$$

where $R_{n,k}\left(p_{n,k}\right)=\log_2\left(1+p_{n,k}\right)$ is the rate of user $k\in\mathscr{U}$ within $n\in\mathscr{N}$ when power $p_{n,k}$ is allocated to it. Moreover, $c_{n,k}\left(\Phi_i\right)$ denotes the effective channel of the user $k\in\Phi_i$ (the diagonal element of the $|\Phi_i|\times|\Phi_i|$ matrix $\left(\mathbf{H}_{\Phi_i}\mathbf{H}_{\Phi_i}^H\right)^{-1}$ that corresponds to that user), $\overline{R}_k$ denotes the transmission rate constraint of the user $k\in\mathscr{U}$ and $P_T$ denotes the total available power. The problem (2.5) is a MINLP since the functions $R_{n,k}\left(.\right),n\in\mathscr{N},k\in\mathscr{U}$ are logarithm-based. In general, MINLP falls within the class of NP-hard problems which are difficult to be solved in an optimal way.

### Optimal power allocation for fixed subchannel assignment

Let $\mathscr{K}_n$ denotes the set of users that have been selected to transmit within the subchannel $n\in\mathscr{N}$. For a fixed $\mathscr{K}_1\ldots\mathscr{K}_N$, the power allocation problem (2.5) is convex since the objective is the sum of a number of concave functions and all the constraints are either linear or convex functions of $p_{n,k}$. The following proposition can be stated:

***Proposition 2.1***: The Karush-Kuhn-Tucker conditions for the (convex) power allocation problem, results by (2.5) for fixed $\mathscr{K}_1\ldots\mathscr{K}_N$, dictate that the optimal power allocation satisfy the following equations

$$p_{n,k}^*\left(\lambda^*,\mu_k^*\right)=\left[\frac{c_{n,k}\left(\mathscr{K}_n\right)\left(1+\mu_k^*\right)}{\lambda^*\ln 2}-1\right]^+,\qquad n\in\mathscr{N},k\in\mathscr{K}_n,\tag{2.6a}$$

$$\sum_{n\in\mathscr{N}}\sum_{k\in\mathscr{K}_n}\left[\frac{1+\mu_k^*}{\lambda^*\ln 2}-\frac{1}{c_{n,k}\left(\mathscr{K}_n\right)}\right]^+=P_T,\tag{2.6b}$$

$$\prod_{n\in\mathscr{N}}\left(1+\left[\frac{c_{n,k}\left(\mathscr{K}_n\right)\left(1+\mu_k^*\right)}{\lambda^*\ln 2}-1\right]^+\right)=2^{\overline{R}_k},\qquad k\in\mathscr{U},\tag{2.6c}$$

where $\lambda^*>0$ is the optimal value of the Lagrange multiplier of (2.5b) and $\mu_k^*\geq 0,k\in\mathscr{U}$, is the optimal value of the Lagrange multiplier of (2.5c).

The optimal values $p_{n,k}^*,\lambda^*,\mu_k^*$ can be calculated by the Algorithm 2, called Optimal Power Allocation for Fixed Subchannel Assignment (OPA/FSA). The algorithm is based on a bisection method to calculate the Lagrange multiplier of the power constraint $\lambda$. In each iteration of the bisection method, $|\mathscr{U}|$ nested bisections are taking place in parallel mode to calculate the Lagrange multipliers $\mu_k,k\in\mathscr{U}$, in order to satisfy the constraints (2.6c). The output of OPA/FSA is a feasible solution of (2.6a), if the transmission rate constraint is guaranteed for every user. The overall computational complexity of OPA/FSA is $\mathscr{O}\left(UNT_x^3\log_2^2\left(\varepsilon^{-1}\right)\right)$, given that the effective channels of the selected users are calculated in $\mathscr{O}\left(T_x^3\right)$ and the predefined accuracy of all used bisections is $\varepsilon,\varepsilon>0$.

**Algorithm 2:** Optimal power allocation for fixed subchannel assignment (OPA/FSA)

**Input:** $\mathscr{K}_1,\ldots,\mathscr{K}_N$ and precision $\varepsilon$.
Set appropriate $\lambda_{min},\lambda_{max}>0$, $\mu_{k,min},\mu_{k,max}>0, k\in\mathscr{U}$.
**repeat**
  Set $\lambda=(\lambda_{min}+\lambda_{max})/2$.
  **for all** $k\in\mathscr{U}$ **do**
    Calculate $\mu_k$ and $p_{n,k}(\lambda,\mu_k)$ by employing a bisection method on $\mu_k$ to satisfy (2.6c) and by using (2.6a).
  **end for**
  The total power consumption is calculated as $P_c=\sum_{n\in\mathscr{N}}\sum_{k\in\mathscr{K}_n}\frac{p_{n,k}(\lambda,\mu_k)}{c_{n,k}(\mathscr{K}_n)}$.
  **if** $P_c<P_T$ **then**
    Set $\lambda_{max}=\lambda$ and $p^*_{n,k}=p_{n,k}(\lambda,\mu_k)$, $n\in\mathscr{N},k\in\mathscr{K}_n$.
  **else**
    Set $\lambda_{min}=\lambda$.
  **end if**
**until** $|\lambda_{min}-\lambda_{max}|\leq\varepsilon$
**if** The constraint (2.5c) is satisfied for every user in $\mathscr{U}$ **then**
  The problem is feasible and the optimal solution is $p^*_{n,k}, n\in\mathscr{N},k\in\mathscr{U}$.
**else**
  The problem is infeasible.
**end if**

In principle, the optimal solution in (2.5) can be derived by an exhaustive subchannel assignment policy in which OPA/FSA is triggered for each examined, possible assignment snapshot $\mathscr{K}_1\ldots\mathscr{K}_N$. The optimal assignment is the one with the highest throughput among them which result to feasible solutions in the power allocation subproblem. Given that there are $S^N$ different assignment snapshots, the computational complexity of such a policy is $\mathscr{O}\left(S^N N T_x^3 \log_2^2 \varepsilon^{-1}\right)$.

### A near-optimal solution using piecewise linear approximation

In this subsection, a piecewise linear approximation (PLA) procedure is developed over the functions $R_{n,k}(.), n\in\mathscr{N},k\in\mathscr{U}$, and the mixed integer nonlinear program (MINLP) (2.5) is transformed to a (mixed integer linear program (MILP). Despite that MILP is still an NP-complete problem, there are significantly more efficient solvers for this kind of problems compared to MINLP, where the original problem in (2.5) belongs [67].

Let $f(w)$ be a continuous, logarithmic and increasing function of $w\in\mathbb{R}_+$. In PLA, the function $f(w)$ is approximated by an appropriate series of linear segments as it is depicted in Fig. 2.3. Let $\mathscr{L}=\{1,\ldots,L\}$ denotes the set of linear segments that is used in the approximation. Each segment $l\in\mathscr{L}$, is specified by its slope $c^l$ and its lower and upper breakpoints $b^{l-1}$ and $b^l$, respectively. Moreover, it is bound with a continuous variable $\xi^l$,

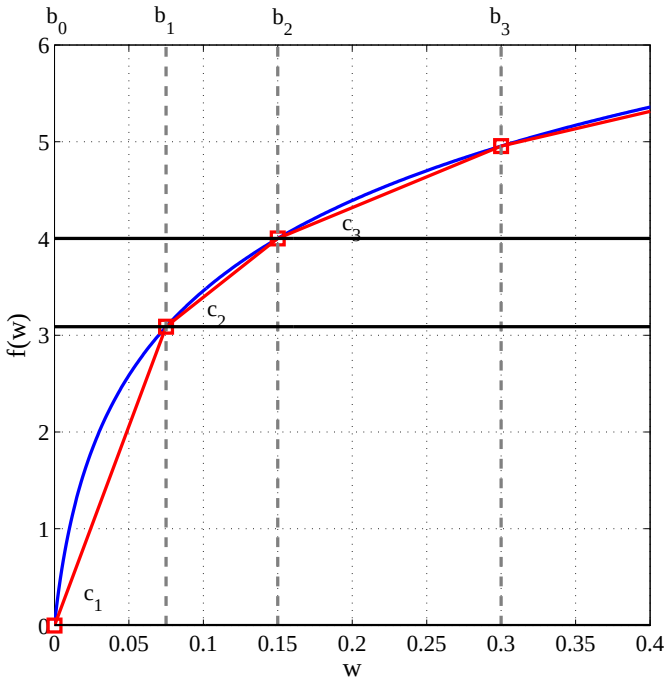



Fig. 2.3 Piecewise linear approximation of a logarithmic function $f(w)$.

$b^{l-1} \leq \xi^l \leq b^l$, which is called segment's load. A segment is characterized as *full*, when its load takes the maximum possible value. By using segments' loads, any value $w \in \mathbb{R}_+$ can be composed as $w = \sum_{l \in \mathscr{L}} \xi^l$, under the assumption that the load of $(l+1)$-*th* segment is zero unless $l$-*th* segment is *full*. Thus, $f(w)$ can be approximated as $f(w) = \sum_{l \in \mathscr{L}} c^l \xi^l$, under the constraint that $w = \sum_{l \in \mathscr{L}} \xi^l$ and $0 \leq \xi^l \leq b^l - b^{l-1}, l \in \mathscr{L}$ [68]. Clearly, as the number of segments increases, the linear approximation of $f(w)$ becomes more accurate.

Let $r_{n,k,\Phi_i} \in \mathbb{R}_+$ denotes a power variable defined as $r_{n,k,\Phi_i} = \omega_{n,\Phi_i} p_{n,k}$, $n \in \mathscr{N}, k \in \mathscr{U}$, $i = 1, \ldots, S$. Clearly, $R_{n,k}\left(r_{n,k,\Phi_i}\right) = 0$ if $k \notin \Phi_i$. Moreover, $R_{n,k}\left(r_{n,k,\Phi_i}\right) = R_{n,k}\left(p_{n,k}\right)$ if $\omega_{n,\Phi_i} = 1$ and $R_{n,k}(0) = 0$ if $\omega_{n,\Phi_i} = 0$. Using variables $r_{n,k,\Phi_i}$, the problem in (2.5) is written as

$$\max \sum_{n \in \mathscr{N}} \sum_{i=1}^{S} \sum_{k \in \Phi_i} R_{n,k}\left(r_{n,k,\Phi_i}\right) \tag{2.7a}$$

$$s.t. \sum_{n \in \mathscr{N}} \sum_{i=1}^{S} \sum_{k \in \Phi_i} \frac{r_{n,k,\Phi_i}}{c_{n,k}(\Phi_i)} \leq P_T, \tag{2.7b}$$

$$\sum_{n \in \mathscr{N}} \sum_{i=1}^{S} R_{n,k}\left(r_{n,k,f\Phi_i}\right) \geq \overline{R}_k, \qquad k \in \mathscr{U}, \tag{2.7c}$$

$$\sum_{i=1}^{S} \omega_{n,\Phi_i} = 1, \qquad n \in \mathscr{N}, \tag{2.7d}$$

$$r_{n,k,\Phi_i} \geq 0, \qquad k \in \mathscr{U}, n \in \mathscr{N}, \tag{2.7e}$$

$$\omega_{n,\Phi_i} \in \{0,1\}, \qquad n \in \mathscr{N}, i = 1,\ldots,S. \tag{2.7f}$$

The MINLP (2.7) can be transformed to the following MILP by employing the previously described PLA over the function $R_{n,k}(.), n \in \mathscr{N}, k \in \mathscr{K}$.

$$\max_{\omega_{n,\Phi_i}, r_{n,k,\Phi_i}, \xi^l_{n,k,\Phi_i}} \quad \sum_{n\in\mathscr{N}} \sum_{i=1}^{S} \sum_{k\in\Phi_i} \sum_{l\in\mathscr{L}} c^l \xi^l_{n,k,\Phi_i} \tag{2.8a}$$

$$s.t. \sum_{n\in\mathscr{N}} \sum_{i=1}^{S} \sum_{l\in\mathscr{L}} c^l \xi^l_{n,k,\Phi_i} \geq \overline{R}_k, \qquad k \in \mathscr{U}, \tag{2.8b}$$

$$\sum_{n\in\mathscr{N}} \sum_{i=1}^{S} \sum_{k\in\Phi_i} \frac{r_{n,k,\Phi_i}}{c_{n,k}(\Phi_i)} \leq P_T, \tag{2.8c}$$

$$\sum_{i=1}^{S} \omega_{n,\Phi_i} = 1, \qquad n \in \mathscr{N}, \tag{2.8d}$$

$$\omega_{n,\Phi_i} \in \{0,1\}, \qquad n \in \mathscr{N}, i = 1,\ldots,S, \tag{2.8e}$$

$$0 \leq r_{n,k,\Phi_i} \leq \omega_{n,\Phi_i} P_T, \qquad n \in \mathscr{N}, k \in \mathscr{U}, i = 1,\ldots,S, \tag{2.8f}$$

$$0 \leq \xi^l_{n,k,\Phi_i} \leq b^l - b^{l-1}, \qquad n \in \mathscr{N}, k \in \mathscr{U}, l \in \mathscr{L}, i = 1,\ldots,S, \tag{2.8g}$$

$$r_{n,k,\Phi_i} = \sum_{l\in\mathscr{L}} \xi^l_{n,k,\Phi_i}, \qquad n \in \mathscr{N}, k \in \mathscr{U}, i = 1,\ldots,S, \tag{2.8h}$$

where the constraints (2.8b)–(2.8f) are inherited by (2.7) with the only difference that function $R_{n,k}\left(r_{n,k,\Phi_i}\right)$ has been replaced by its linear approximation $\sum_{l\in\mathscr{L}} c^l \xi^l_{n,k,\Phi_i}, n \in \mathscr{N}, k \in \mathscr{U}, i = 1,\ldots,S$. Moreover, the constraints (2.8g)–(2.8h) are imposed by the used PLA model. Note that just one linear approximation of $R_{n,k}(.)$ is necessary, irrespectively to the specific value of $n$ and $k$. As a result, the sense that the same number of segments, positions of breakpoints and slopes are used to approximate $R_{n,k}(.)$, $n \in \mathscr{N}, k \in \mathscr{U}$, and $i = 1,\ldots,S$. Typically, the MILP (2.8) is an NP-complete problem and it is commonly solved by a branch and bound algorithm which decomposes it into an integer program (IP) and a series of subordinated linear programs (LPs). Nevertheless, there are powerful solvers for this class of problems, based on which a benchmark for the optimal solution of (2.5) can be obtained.

**Relaxation and subchannel reassignment to fulfill individual rate constraints**

In [56], a resource allocation scheme is presented for the problem of throughput maximization without constraints on the users' transmission rate, *i.e.* the problem in (2.5) without the constraints (2.5c). The presented scheme, called Throughput Maximization using

**Algorithm 3:** Relaxation and subchannel reassignment algorithm (RSRA)

An initial subchannel assignment, $\mathscr{K}_1,\ldots,\mathscr{K}_N$, is obtained by solving the unconstrained problem of maximizing throughput using (2.9), (2.10a) and (2.10b).
Let $\mathscr{A}$ denotes the set of users which do not occupy any subchannel.
**for all** $k \in \mathscr{A}$ **do**
  Let $\mathscr{N}_A$ denotes the set of subchannels that have free spatial slots, *i.e* the subchannels which have less than $T_x$ users.
  **if** $|\mathscr{N}_A| \geq 1$ **then**
    Specify $n^* = \min_{n\in\mathscr{N}_A} \sum_{j\in\mathscr{K}_n} \rho_{k,j}\left(\mathbf{h}_{n,k},\mathbf{h}_{n,j}\right)$. Set $\mathscr{K}_{n^*} = \{\mathscr{K}_{n^*} \cup k\}$.
  **else**
    Let $\mathscr{B}$ denotes the set of users who occupy the most subchannels (more than one subchannel) and $\mathscr{N}_s$ denotes the set of subchannels occupied by the user $s, s \in \mathscr{B}$.
    Specify $(s^*,n^*) = \arg\min_{s\in\mathscr{B}} \min_{n\in\mathscr{N}_s} \sum_{j\in\mathscr{K}_n\setminus s} \rho_{k,j}\left(\mathbf{h}_{n,k},\mathbf{h}_{n,j}\right)$. Set $\mathscr{K}_{n^*} = \{\mathscr{K}_{n^*} \cup k\} - \{s^*\}$.
  **end if**
**end for**

Relaxation Algorithm (TMRA), is based on relaxing the binary variables $\omega_{n,\Phi_i}, n \in \mathscr{N}, i = 1,\ldots,S$, to take values in $[0,1]$ and decomposing the resulting problem across the subchannels by using dual space optimization. Overall, an iterative procedure is defined that outputs a (near) optimal subchannel assignment and power allocation solution. Each iteration corresponds to an update operation of the Lagrange multiplier of the power constraint using a bisection method. The subchannel assignment per iteration is specified as

$$\mathscr{K}_n^* = \arg\max_{i=1,\ldots,S} \; H_n^{\Phi_i}(\lambda), \qquad n \in \mathscr{N}, \tag{2.9}$$

where the $H_n^{\Phi_i}(\lambda)$ and the corresponding power allocation are given as

$$H_n^{\Phi_i}(\lambda) = \sum_{k\in\Phi_i} \log_2\left(1+p_{n,k}(\lambda)\right) - \frac{\lambda\, p_{n,k}(\lambda)}{\ln 2\, c_{n,k}(\Phi_i)}, \qquad n \in \mathscr{N}, i = 1,\ldots,S, \tag{2.10a}$$

$$p_{n,k}(\lambda) = c_{n,k}(\Phi_i)\left[\frac{1}{\lambda\ln 2} - \frac{1}{c_{n,k}(\Phi_i)}\right]^+, \qquad n \in \mathscr{N}, k \in \Phi_i, \tag{2.10b}$$

and the Lagrange multiplier of the total power constraint $\lambda > 0$ is calculated in order to satisfy $\sum_{n\in\mathscr{N}} \sum_{k\in\mathscr{K}_n^*} \frac{p_{n,k}(\lambda)}{c_{n,k}^{\mathscr{K}_n^*}} = P_T$. The computational complexity of TMRA is $\mathscr{O}\left(SNT_x^3 \log_2 \varepsilon^{-1}\right)$, where $\varepsilon > 0$ is the predefined required accuracy in the bisection method over the Lagrange multiplier $\lambda$. Note that the computational complexity is remarkably reduced compared to an exhaustive search approach over each different possible subchannel assignment instance.

Table 2.2 Feasibility of the presented resource allocation schemes.

| $P_T$ | $T_x = 2$ | | | $T_x = 3$ | | |
|---|---|---|---|---|---|---|
| | TMRA | MILP-OPA/FSA | RSRA-OPA/FSA | TMRA | MILP-OPA/FSA | RSRA-OPA/FSA |
| 4 dB | 0.001 | 0.006 | 0.002 | 0.036 | 0.525 | 0.141 |
| 6 dB | 0.006 | 0.455 | 0.088 | 0.080 | 0.951 | 0.528 |
| 8 dB | 0.028 | 0.927 | 0.374 | 0.142 | 0.972 | 0.787 |
| 10 dB | 0.053 | 0.956 | 0.643 | 0.221 | 0.999 | 0.879 |
| 12 dB | 0.109 | 0.982 | 0.834 | 0.315 | 0.999 | 0.927 |
| 14 dB | 0.134 | 0.997 | 0.933 | 0.380 | 0.999 | 0.958 |

Inspired by the near-optimal performing TMRA scheme, a heuristic subchannel assignment policy is proposed herein and it is combined with OPA/FSA, presented in Algorithm 2, to state a resource allocation scheme for the case in which individual rate constraints are also considered. In the proposed scheme, an initial subchannel assignment is obtained by optimally solving the problem of maximizing throughput using (2.9), (2.10a) and (2.10b). In the next step, the OPA/FSA algorithm is triggered using as input the initial assignment. Nevertheless, there is a possibility for some users to not occupy any spatial slot in the initial subchannel assignment obtained by TMRA. In such a case, the proposed algorithm ensures that at least one subchannel is assigned to every such user before OPA/FSA is triggered. For each one such user, the assigned subchannel is the one in which it faces the less sum normalized spatial correlation with respect to the users that already have been assigned therein. In the case where there isn't any available spatial slot in the initial assignment, the subchannels which are occupied by the users who posses the most subchannels are considered as available and the same rule is applied. Nevertheless, a user swapping is also performed in this case. The overall subchannel assignment algorithm, called Relaxation and Subchannel Reassignment Algorithm (RSRA), is described in detail in Algorithm 3. Its computational complexity consists of two parts; the first corresponds to the complexity of TMRA, which is $\mathscr{O}\left(SNT_x^3 \log_2 \varepsilon^{-1}\right)$, while the second corresponds to subchannel reassign phase. Even if the complexity of this phase cannot be defined precisely, each reassignment procedure takes $\mathscr{O}\left(NT_x^2\right)$ and the need of such reassignments may be up to $T_xN-1$. The combined scheme of RSRA and OPA/FSA is called RSRA-OPA/FSA.

### Numerical results

In Fig. 2.4, the performance of RSRA-OPA/FSA is shown versus $P_T$ in terms of system's throughput for $N = 4, K = 6$, $T_x = 2,3$ and equal rate constraints for all users, *i.e.* $\overline{R}_k = 1$ bpcu, $k \in \mathscr{U}$. It is assumed that all the wireless channels follow a Rayleigh distribution and the results are averaged over 1000 feasible realizations. The performance of RSRA-

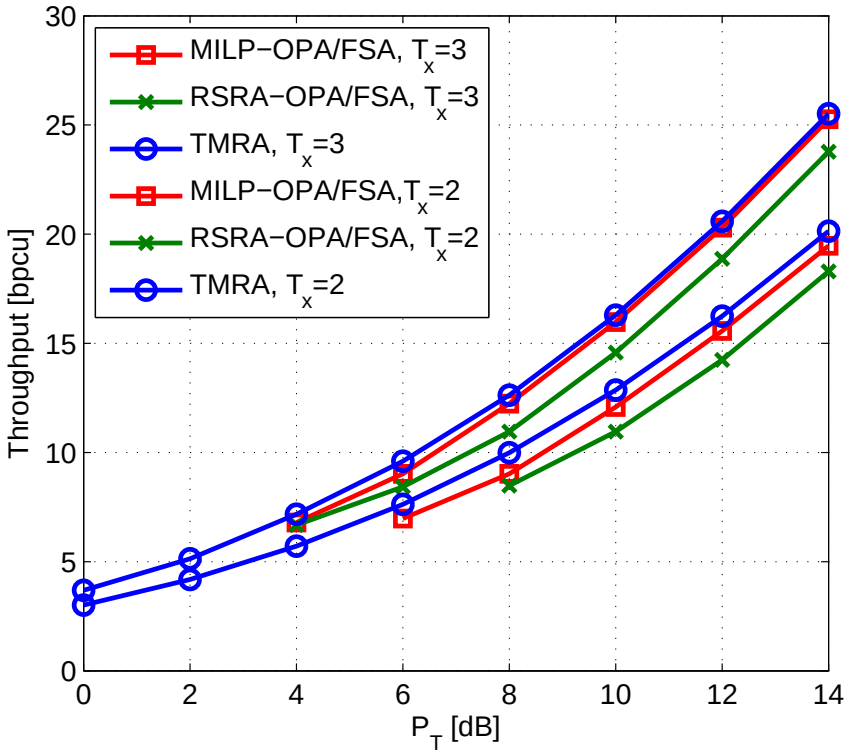



Fig. 2.4 Throughput of RSRA-OPA/FSA vs $P_T$ for $N = 4$ and $U = 6$.

OPA/FSA is compared with that of MILP-OPA/FSA. In MILP-OPA/FSA, the MILP (2.8) is firstly solved and the OPA/FSA is later executed by using as input the MILP's output subchannel assignment. As PLA in MILP becomes more dense, the MILP-OPA/FSA performs near to optimal and it can be used as benchmark to evaluate the performance of any other proposed scheme. Note that RSRA-OPA/FSA achieves more than 90% of the MILP-OPA/FSA performance for every $P_T$. A similar relative behavior was noticed for other transmission rate constraints, both uniform and non-uniform. As an upper bound for the system's throughput, the performance of TMRA is also shown [56]. Note that none individual rate constraints (2.5c) is guaranteed by the TMRA, opposite to RSRA-OPA/FSA and MILP-OPA/FSA.

In Table 2.2, the feasibility of the above discussed resource allocation schemes is shown for 10000 realizations. For low values $P_T$, the problem is infeasible since there is not enough resources to ensure users' transmission rate constraints. The feasibility of all schemes is improved as there are more system resources, *e.g.* as $T_x$ and/or $P_T$ increase.

### 2.3.2 Maximize users' rate balancing

In this subsection, the considered problem is to maximize the minimum user rate of the system under an average power constraint (rate balancing). Rate balancing is a widely-used optimization criterion of system's performance in multiuser systems, since it considers fairness in the resource allocation process in the sense that all the users are able to occupy adequate resources and be serviced in an almost uniform way. The addressed problems is

$$\max_{p_{n,k},\omega_{n,\Phi_i}} \min_{k} \quad \sum_{n\in\mathscr{N}}\sum_{i=1}^{S}\omega_{n,\Phi_i}\sum_{k\in\Phi_i}R_{n,k}\left(p_{n,k}\right) \tag{2.11a}$$

$$s.t. \sum_{n\in\mathscr{N}}\sum_{i=1}^{S}\omega_{n,\Phi_i}\sum_{k\in\Phi_i}\frac{p_{n,k}}{c_{n,k}\left(\Phi_i\right)} \leq P_T, \tag{2.11b}$$

$$\sum_{i=1}^{S}\omega_{n,\Phi_i} = 1, \qquad n\in\mathscr{N}, \tag{2.11c}$$

$$p_{n,k} \geq 0, \qquad n\in\mathscr{N}, k\in\mathscr{U}, \tag{2.11d}$$

$$\omega_{n,\Phi_i} \in \{0,1\}, \qquad n\in\mathscr{N}, i=1,\ldots,S. \tag{2.11e}$$

where the same notation is used as in the previous subsection. The problem (2.11) is combinatorial and it is composed of a set selection and a power allocation subproblem. By introducing the auxiliary variable $x \geq 0$, (2.11) is written in the following typical form

$$\max_{p_{n,k},\omega_{n,\Phi_i}} \quad x \tag{2.12a}$$

$$s.t. \quad x \leq \sum_{n\in\mathscr{N}}\sum_{i=1}^{S}\omega_{n,\Phi_i}R_{n,k}\left(p_{n,k}\right), \qquad k\in\mathscr{U}, \tag{2.12b}$$

$$\sum_{n\in\mathscr{N}}\sum_{i=1}^{S}\omega_{n,\Phi_i}\sum_{k\in\Phi_i}\frac{p_{n,k}}{c_{n,k}\left(\Phi_i\right)} \leq P_T, \tag{2.12c}$$

$$\sum_{i=1}^{S}\omega_{n,\Phi_i} = 1, \qquad n\in\mathscr{N}, \tag{2.12d}$$

$$p_{n,k} \geq 0, \qquad n\in\mathscr{N}, k\in\mathscr{U}, \tag{2.12e}$$

$$\omega_{n,\Phi_i} \in \{0,1\}, \qquad n\in\mathscr{N}, i=1,\ldots,S. \tag{2.12f}$$

The problem (2.12) is a MINLP. For fixed sets $\mathscr{K}_1,\ldots,\mathscr{K}_N$, the resulting power allocation (sub)problem is convex. Specifically, the following proposition can be stated:

**Algorithm 4:** Rate balanced - optimal power allocation for fixed subchannel assignment (RB-OPA/FSA)

**Input:** $\mathscr{K}_1,\ldots,\mathscr{K}_N$.
Set $x_{min}=0$ and an appropriate value $x_{max}>0$.
**repeat**
  Set $x_f=(x_{min}+x_{max})/2$.
  **for all** $k\in\mathscr{U}$ **do**
    Let $\theta_k=\frac{\mu_k}{\lambda}$. Calculate $p_{n,k}(\theta_k)$, $n\in\mathscr{N}$, by using (2.13a) and by employing a bisection method over $\theta_k$ to satisfy (2.13c).
  **end for**
  The total power consumption is calculated as $P_c=\sum_n\sum_{k\in\mathscr{K}_n}\frac{p_{n,k}(\theta_k)}{c_{n,k}(\mathscr{K}_n)}$.
  **if** $P_c<P_T$ **then**
    Set $x_{min}=x$ and $p^*_{n,k}=p_{n,k}(\theta_k)$, $n\in\mathscr{N},k\in\mathscr{K}_n$.
  **else**
    Set $x_{max}=x$.
  **end if**
**until** $|x_{min}-x_{max}|\leq\varepsilon$

***Proposition 2.2***: The Karush-Kuhn-Tucker conditions for the (convex) power allocation problem, results by (2.12) for fixed $\mathscr{K}_1\ldots\mathscr{K}_N$, dictate that the optimal power allocation satisfy the following equations

$$p^*_{n,k}(\lambda^*,\mu^*_k)=\left[\frac{c_{n,k}(\mathscr{K}_n)\,\mu^*_k}{\lambda^*\ln 2}-1\right]^+,\qquad n\in\mathscr{N},k\in\mathscr{K}_n,\tag{2.13a}$$

$$\sum_{n\in\mathscr{N}}\sum_{k\in\mathscr{K}_n}\left[\frac{\mu^*_k}{\lambda^*\ln 2}-\frac{1}{c_{n,k}(\mathscr{K}_n)}\right]^+=P_T,\tag{2.13b}$$

$$\prod_{n\in\mathscr{N}}\left(1+\left[\frac{c_{n,k}(\mathscr{K}_n)\,\mu^*_k}{\lambda^*\ln 2}-1\right]^+\right)=2^x,\qquad k\in\mathscr{U},\tag{2.13c}$$

$$\sum_{k\in\mathscr{U}}\mu^*_k=1,\tag{2.13d}$$

where $\lambda^*>0$ is the optimal value of the Lagrange multiplier of (2.12c) and $\mu^*_k\geq 0,k\in\mathscr{K}$, are the optimal values for the Lagrange multipliers of (2.12b).

The values $p^*_{n,k},\lambda^*,\mu^*_k$ can be calculated by the Algorithm 4, called Rate Balanced Optimal Power Allocation for Fixed Subchannel Assignment (RB-OPA/FSA). In RB-OPA/FSA, the variable $x$ is controlled by a bisection method in order to satisfy (2.12c) with equality. For each value of this variable, the ratio $\theta_k=\frac{\mu_k}{\lambda},k\in\mathscr{U}$, is calculated by a nested bisection method to satisfy (2.13c). The overall computational complexity of RB-OPA/FSA is $\mathscr{O}\left(UNT_x^3\log_2^2\left(\varepsilon^{-1}\right)\right)$, where $\varepsilon>0$ is the predefined required accuracy in Lagrange multi-

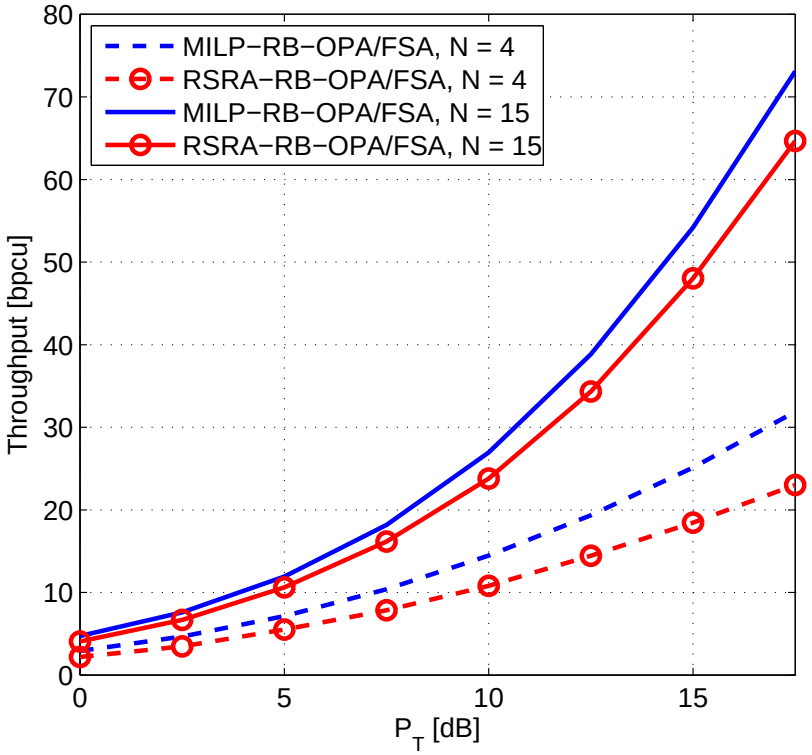



Fig. 2.5 Throughput RSRA-RB-OPA/FSA vs $P_T$ for $U = 6$ and $T_x = 3$.

pliers' calculation. In principle, the optimal solution in (2.11) can be derived by an exhaustive subchannel assignment policy in which RB-OPA/FSA is triggered for each examined, possible assignment snapshot. Given that there are $S^N$ different assignment snapshots, the computational complexity of such a policy is $\mathcal{O}\left(S^N N T_x^3 \log_2^2 \varepsilon^{-1}\right)$.

A low-complexity resource allocation scheme for the problem (2.12) results by combining RSRA with RB-OPA/FS. Specifically, the scheme consists of two phases; in the first phase, the RSRA is executed, described in Algorithm 3. In the second phase, the RB-OPA/FSA is triggered given the output subchannel assignment of RSRA and, thus, users' rate balancing is perfectly guaranteed. The overall algorithm is called RSRA-RB-OPA/FSA and its computational complexity is formed by the sum of the complexities of the two individual algorithms, namely RSRA and RB-OPA/FSA.

**Numerical results**

In Fig. 2.5 the throughput versus $P_T$ is shown for $K = 6$, $T_x = 3$ and $N = 4, 15$. For the sake of comparison, the performance of MILP-RB-OPA/FSA is also shown which can be considered as benchmark for the optimal solution. In MILP-RB-OPA/FSA, a PLA of $R_{n,k}(.)$ is employed and the problem (2.12) is transformed to a MILP, similar to what described in subsection 2.3.1. The subchannel output of this MILP is combined with RB-OPA/FSA.

## 2.4 Throughput maximization by performing resource allocation on chunk basis

In this section, the problem of throughput maximization is considered for a system that transmits over a number of parallel channels when resource allocation is performed on chunk-basis. Let $\mathscr{U} = \{1,\ldots,U\}$ denotes the set of users in the system, $\mathscr{N} = \{1,\ldots,N\}$ denotes the set of parallel channels and $\mathscr{C} = \{1,\ldots,C\}$ denotes the set of chunks. Moreover, $\mathscr{N}_c \subseteq \mathscr{N}$ denotes the set of subchannels that belong to the chunk $c \in \mathscr{C}$ and $\mathscr{K}_c \subseteq \mathscr{U}$ denotes the users transmission group that has been selected for chunk $c \in \mathscr{C}$. The aim is to maximize the throughput of the system under an average power constraint per chunk. Specifically, the addressed problem is

$$\begin{aligned} &\max_{\mathscr{K}_c, p_{n,k}} \sum_{c\in\mathscr{C}} \sum_{n\in\mathscr{N}_c} \sum_{k\in\mathscr{K}_c} R_{n,k}\left(p_{n,k}\right) && (2.14)\\ &s.t. \sum_{n\in\mathscr{N}_c} \sum_{k\in\mathscr{K}_c} p_{n,k} \le P_T, && c\in\mathscr{C}\\ &|\mathscr{K}_c| \le T_x, && c\in\mathscr{C}. \end{aligned}$$

where $P_T$ is the bound on the average transmitted power per chunk. A power bound per chunk is a quite common assumption in chunk-based resource allocation because of the relative large size of the chunk. Nevertheless, the considered problem can be set in a similar way under a total power bound over the chunks.

The problem (2.14) is a combinatorial one. The optimal solution can be specified by exhaustively search over all the different sets of users with cardinality up to $T_x$. For each candidate set, the throughput is specified by a waterfilling power loading over the effective channels of each user in the set. The transmission rate of the user $k \in \mathscr{K}_c$ within the chunk $c \in \mathscr{C}$ is

$$R_k^c(\mathscr{K}_c) = \sum_{n\in\mathscr{N}_c} \left[\log_2\left(\mu_c c_{n,k}(\mathscr{K}_c)\right)\right]^+, \qquad k\in\mathscr{K}_c, c\in\mathscr{C}, \qquad (2.15)$$

where $c_{n,k}(\mathscr{K}_c)$ denotes its effective channel and the value of $\mu_c \ge 0$ is calculated by

$$\sum_{n\in\mathscr{N}_c} \sum_{k\in\mathscr{K}_c} \left[\frac{\mu_c}{\ln 2} - \frac{1}{c_{n,k}(\mathscr{K}_c)}\right]^+ = P_T, \qquad c\in\mathscr{C}, \qquad (2.16)$$

However, the computational complexity of an exhaustive search policy is prohibitive, especially as the number of users increases. In the following subsection, a low-complexity

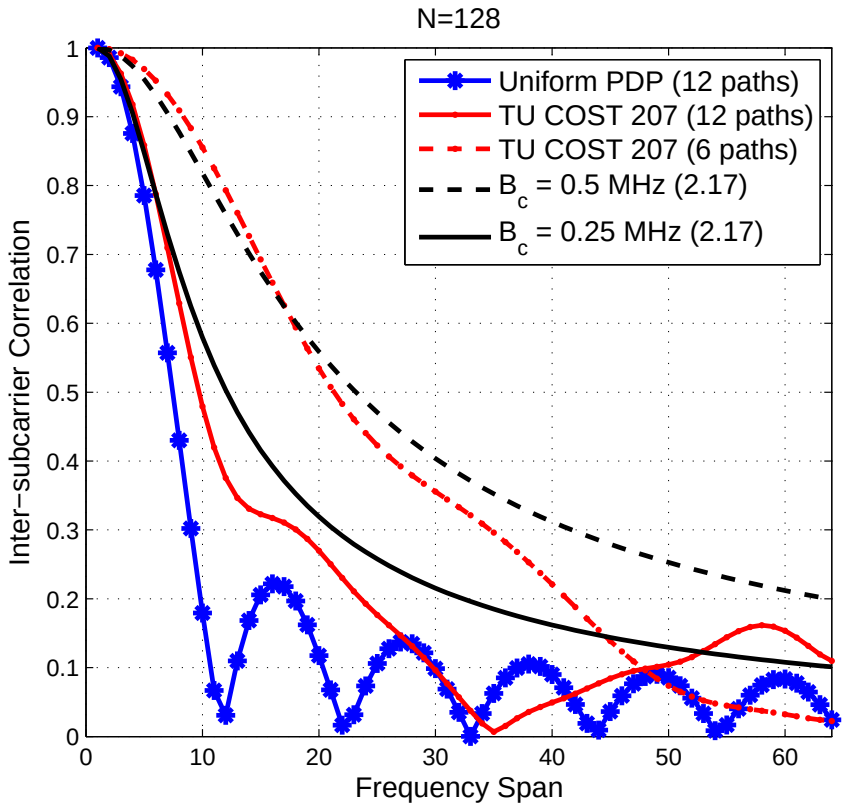



Fig. 2.6 Inter-subchannel correlation profile in a system which transmits over a number of parallel subchannels.

heuristic for (2.14) is presented inspired by CUSA, described in Section 2.2, which aims to exploit the inter-subchannel correlation and frequency diversity of the system in order to reduce the computational complexity.

In broadband wireless systems, inter-subchannel correlation depends primarily on the physical characteristics of the wireless medium, *i.e.* the delay spread $T_d$ and the (inverse related) coherence bandwidth $B_c \approx \frac{1}{T_d}$. In Fig. 2.6, three inter-subchannel correlation profiles are illustrated which correspond to a uniform 12-path power delay profile (PDP) and two practically consisted 6-path and 12-path Typical Urban PDPs of COST model [69]. Moreover, the inter-subchannel correlation profile results by (2.17) is depicted, which is a commonly used mathematical formula to model the inter-subchannel correlation [9],

$$r_{m,n} = \frac{1}{\sqrt{1+\left(\frac{d(m-n)Df}{B_c}\right)^2}}, \qquad m,n \in \mathcal{N}, \tag{2.17}$$

**Algorithm 5:** Frequency-space correlation-based user selection algorithm (FS-CUSA)

Set $\mathscr{K}_c = \emptyset$, $c \in \mathscr{C}$.
**for** $c \in \mathscr{C}$ **do**
  Specify user $u^* = \arg\max_{k \in \mathscr{U}} R_k^c(u)$.
  Set $\mathscr{K}_c = \{u^*\}$ and $m = 1$.
  **while** $m < T_x$ **do**
    Set $\mathscr{A} = \emptyset$, $m = m + 1$.
    **for** $n \in \mathscr{N}_c$ **do**
      Specify $i_n^* = \min_{i \in \mathscr{U} \setminus \mathscr{K}_c} \sum_{k \in \mathscr{K}_c} \rho_{k,i} \left(\mathbf{h}_{n,k}, \mathbf{h}_{n,i}\right)$
      Set $\mathscr{A} = \{\mathscr{A} \cup i_n^*\}$
    **end for**
    Formulate set $\mathscr{A} = \{i_n^*\}, n \in \mathscr{N}_c$.
    Specify user $a^* = \arg\max_{a \in \mathscr{A}} \sum_{k \in \{\mathscr{K}_c \cup a\}} R_k^c(\{\mathscr{K}_c \cup a\})$.
    **if** $\sum_{k \in \{\mathscr{K}_c \cup a^*\}} R_k^c(\{\mathscr{K}_c \cup a^*\}) > \sum_{k \in \mathscr{K}_c} R_k^c(\mathscr{K}_c)$ **then**
      set $\mathscr{K}_c = \{\mathscr{K}_c \cup a^*\}$.
    **else**
      $m = T_x$.
    **end if**
  **end while**
**end for**
**return** $\mathscr{K}_c$, $c \in \mathscr{C}$.

In (2.17), $Df$ is the frequency separation between two consecutive subchannels and the decay factor $d$ specifies how correlation is smoothing across them. By tuning appropriately these parameters, the inter-subchannel correlation can be accordingly adjusted to a desired profile. The two black-colored curves in Fig. 2.6 hold for $N = 128$ and $d = 2$; the solid one corresponds to a strong inter-subchannel correlation profile ($B_c = 0.5$ MHz), while the other corresponds to a medium inter-subchannel correlation profile ($B_c = 0.25$ MHz).

### Frequency-space correlation-based user selection algorithm

In the proposed resource allocation scheme, the key idea is to exploit multiuser diversity in frequency domain rather than in spatial domain as in CUSA. The algorithm, called Frequency Space Correlation-based User Selection Algorithm (FS-CUSA), is described in Algorithm 5. Similar to CUSA, the transmission group in FS-CUSA is iteratively formed by appending users with low average spatial correlation to the already selected ones. Nevertheless, the group of users from which the new member of the transmission group will result, *i.e* set $\mathscr{A}$, is built over the frequency dimension by embody only the lowest correlated user per chunk's subchannel. Such a policy preserves multiuser diversity while decreases the computational complexity at the same time. In principle, two users with low spatial correlation within a subchannel of a given chunk will have low spatial correlation within the

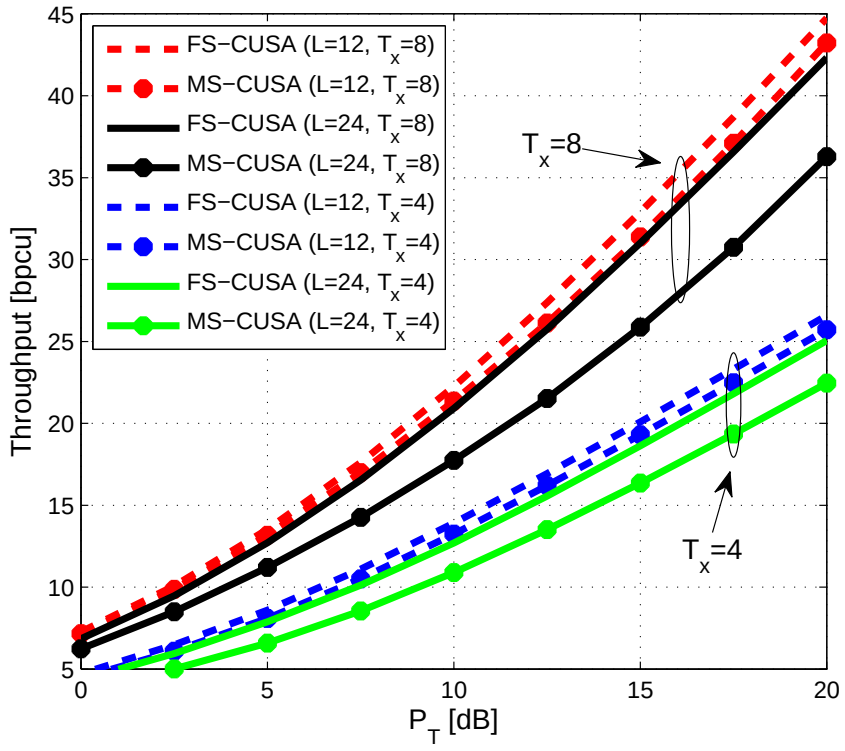



Fig. 2.7 Throughput vs $P_T$ for $B_c = 0.5$ MHz, $U = 100$ and $T_x = 4, 8$.

adjacent subchannels of the same chunk with high probability. Thus, it may be beneficial to multiplex them in a sequence of subchannels. Nevertheless, this characteristic will gradually fade-away, as the frequency distance between the subchannels increases. Thus, the necessary multiuser diversity of the selection process is guaranteed by searching for low correlated users within all the subchannels of the chunk. The computational complexity of FS-CUSA is $\mathscr{O}\left(\left(UT_x + LT_x^2 \log_2 \varepsilon^{-1}\right) T_x\right)$ per chunk, where $\varepsilon > 0$ is the predefined required accuracy in calculation of $\mu_c, c \in \mathscr{C}$.

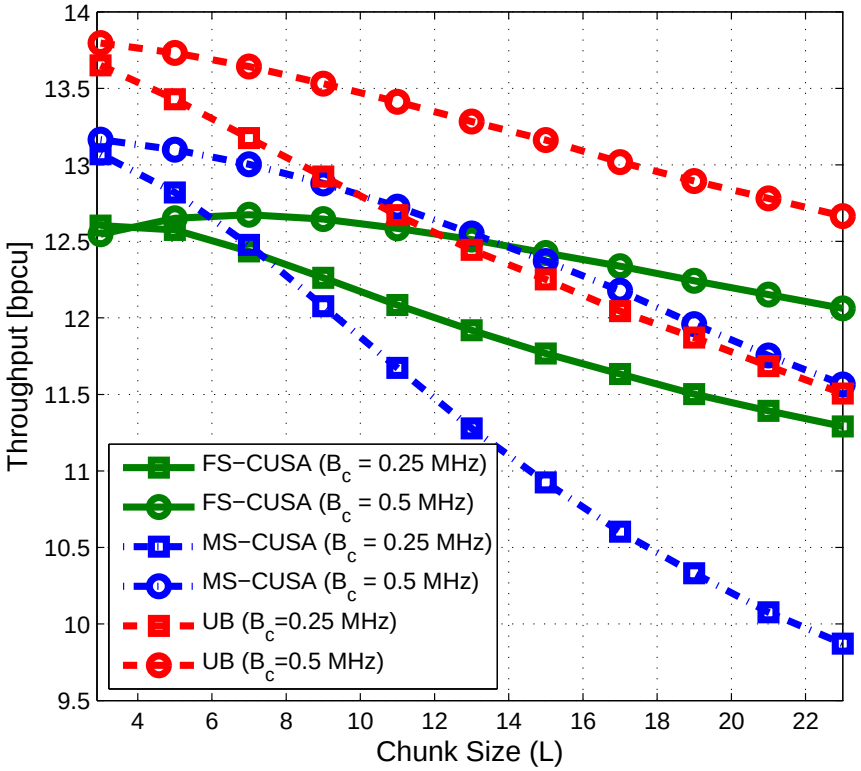
### Numerical results

In Fig. 2.7, the performance of FS-CUSA is depicted versus $P_T$ for $U = 100$, $B_c = 0.25$ MHz and $T_x$ equal to 4 and 8. The available bandwidth is 2.5 MHz, decay factor is $d = 2$, $N = 128$ (thus, subchannel spacing is approximately 20 kHz) and the results are averaged over 10000 experiments. For comparison reasons, the performance of a chunk-based resource allocation scheme that follows a typical strategy is also depicted; the resource allocation scheme, called Middle Subchannel Correlation-based User Selection Algorithm (MS-CUSA), employs CUSA within the middle subchannel of each chunk to specify the user transmission

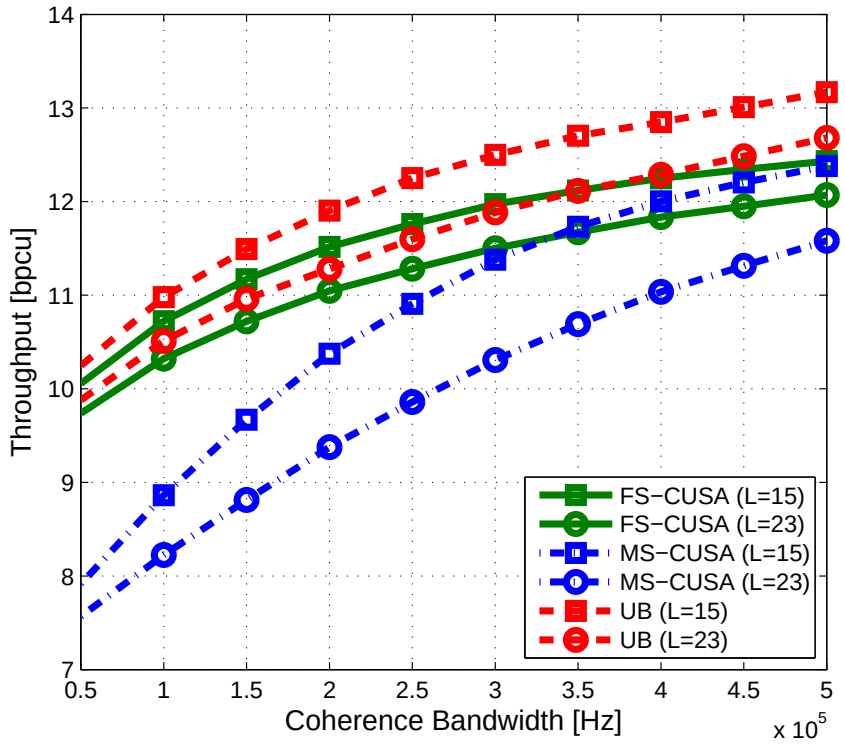
set within all the chunk. As can be seen in Fig. 2.7, the performance of FS-CUSA outperforms MS-CUSA, especially as the chunk size increases.

In Fig. 2.8a, the throughput of FS-CUSA versus chunk size ($L$) is depicted when $P_T$ is 10 dB, $B_c = 250,500KHz$, $T_x = 4$ and $U = 20$. Its performance is compared to that of MS-CUSA and an Upper Bound (UB), which results by employing an exhaustive search policy for user selection. It can be seen that FS-CUSA performs closely to the Upper Bound, achieving more than 95% of its performance for chunk sizes with practical interest, *e.g.* $L \geq 13$. Typical chunk sizes for WiMAX and LTE are $L = 24$and $L = 12$, respectively [70], [71]. Similar behavior was observed for other values in system parameter setup. Even if MS-CUSA performs better than FS-CUSA for small chunk sizes (where strong inter-subchannel correlation exists), its performance is degraded rapidly as $L$ increases since multiuser diversity is exploited only within a small portion of the chunk and not over its entire spectrum. In the opposite, the performance of FS-CUSA is smoothly degraded as the chunk size increases since both frequency (inter-subchannel) and multiuser diversity are exploited more efficiently.

In Fig. 2.8b, the influence of the coherence bandwidth is depicted over the throughput FS-CUSA and MS-CUSA. As it was mentioned earlier, $B_c$ varies according to the channel model but typically it is not higher than a few hundreds of KHz [71]. For that area, FS-CUSA achieves significant performance benefits versus MS-CUSA, under the cost of limited increase in complexity. For instance, when $L = 15$ and $B_c = 0.3$ MHz, FS-CUSA achieves a 0.6 bps/Hz improvement over MS-CUSA.




(a) Throughput vs chunk size for $T_x = 4$ and $U = 20$.




(b) Throughput vs coherence bandwidth for $T_x = 4$ and $U = 20$.

Fig. 2.8 Throughput of chunk-based resource allocation schemes.

# Chapter 3

# Secrecy rate balancing over parallel channels in the presence of passive eavesdropping

## 3.1 Introduction

As the issues of confidentiality and security become more critical in communication systems, physical layer security appears to be an attractive technique to provide security against attacks over the wireless medium [15]. In essence, physical layer security is an information-theoretic approach that achieves secrecy by using channel codes and advanced signal processing techniques. Its main advantage over the cryptography-based traditional approaches lies in the fact that it is independent of the interception and processing ability of the eavesdroppers. Recently, there is a lot of interest to integrate physical layer security into the problem of resource allocation in multiuser orthogonal frequency-division multiple access (OFDMA) broadband systems. From this perspective, physical layer security turns out to be an excellent prospect to provide both security and quality of service (QoS) guarantees [72].

### State of the art

The principles of physical layer security and the definition of the secrecy capacity have been determined in the seminal works [12–14]. Recently, there is a lot of interest to integrate physical layer security into the problem of resource allocation in multiuser orthogonal frequency-division multiple access (OFDMA) broadband systems [73–84].

The secrecy capacity region for a parallel broadcast channel is investigated in [73] and it is shown that it is simply the summation of the secrecy capacities of the individual channels. Moreover, the optimal power allocation strategy is derived for a broadcast system with parallel Gaussian channels subject to a total power constraint. The optimal input distribution

of the parallel broadcast channel with two receivers is derived in [74], for the case where the source has a common information for both receivers and some confidential information intended to only one of them. The same setup is studied in [75], [76] and the optimal power allocation that maximizes the weighted secrecy sum rate is obtained when a different confidential message is sent to each receiver.

Resource allocation in a multiuser OFDMA downlink is investigated in [78] for a setup where conventional users co-exist with secure-sensitive users *i.e.*, users that are served at a nonzero secrecy rate. The goal therein is to find a subchannel and a power allocation policy that maximizes the sum rate of the normal users, while maintaining a targeted secrecy rate for each secure-sensitive user. In [77], [79] a more generic utility function is studied that takes into account both system's power consumption and users' secrecy rate outage probability and an interesting tradeoff is revealed between energy efficiency and secure communication. In [85], a similar objective is investigated in a relay-aided setup where the base station (BS) communicates with each user through a half-duplex decode-and-forward relay. Further discussion is provided in [80], where flow control and resource allocation are jointly optimized in a cross-layer fashion under both delay and security QoS constraints. Physical layer security in cooperative OFDMA networks is discussed in [81], [82], where several power allocation strategies are proposed to inject interference to the eavesdropper by using friendly jammers. The case of jointly optimized artificial noise, subchannel assignment and power allocation in order to maximize the instantaneous sum secrecy rate of a multiuser wiretap OFDMA downlink is studied in [83, 84].

### Contribution

In this chapter, we consider the case where each one of the available data-bearing subchannel is occupied by exactly one user and is wiretapped by a passive eavesdropper. The eavesdropper is a "honest-but-curious" legitimate user which illegally starts wiretapping the messages of the authorized, serviced users [86]. Thus, the BS anticipates the existence of the eavesdropper and perfectly knows its channel state information [81–84, 87, 88]. The problem aims to maximize the minimum secrecy rate over the users of the system. From a practical point of view, the considered problem is important mainly because of two reasons; it incorporates physical layer security into the process of frequency, power and user management and it is built over a system performance measure that considers fairness in the transmission design. The considered problem is formulated as a mixed integer nonlinear program (MILNP) which is hard to be solved because of its combinatorial and nonlinear nature. Thus, several resource allocation schemes are developed which are based on optimal, near-optimal or heuristics solutions. Specifically, the contribution in this chapter is as follows:

- For a fixed subchannel assignment, the optimal power allocation is derived in semi-closed form by using the Karush-Kuhn-Tucker (KKT) conditions.

- In the case of more users than subchannels, the optimal resource allocation scheme is obtained in polynomial computational complexity under the additional assumption that the number of serviced users at a given time instant would be equal to the number of subchannels. To achieve this, an appropriate sequence of linear sum assignment problems (LSAPs) is developed in which a standard algorithm is used to solve each LSAP to optimality [89].
- In the case of less users than subchannels, the optimal solution is generally hard to find. Hence,
  - We use piecewise linear approximation for the logarithm-based secrecy rate functions to formulate a mixed integer linear program (MILP). Although MILP belongs to the NP-complete class, the resulting structure is quite solvable by using a branch-and-bound algorithm, at least for a moderate number of subchannels. This way, a near-optimal solution is obtained which can be used as a benchmark to evaluate the performance of any other solution.
  - Optimality is discussed in the two special cases where the available power tends to infinity and to zero, respectively. In the first case, a high power approximation of the secrecy rate is used and the optimal solution is obtained by formulating a MILP. In the second case, the optimal solution is obtained in polynomial complexity by solving a series of LSAPs. Interestingly, each special case gives rise to a resource allocation scheme with competitive performance in a wide range of system setup.
  - Two heuristic resource allocation schemes of linear computational complexity are proposed by decoupling the original problem into a subchannel assignment and a power allocation subproblem.

The organization of the rest of the chapter is as follows. In Section 3.2, we describe the system model and we obtain the optimal power allocation for fixed subchannel assignment. In Section 3.3, the case in which the number of users is higher than the number of subchannels is discussed and the optimal resource allocation solution is derived. Finally, several resource allocation schemes are presented in Section 3.4 for the case in which the number of users is less than the number of subchannels.

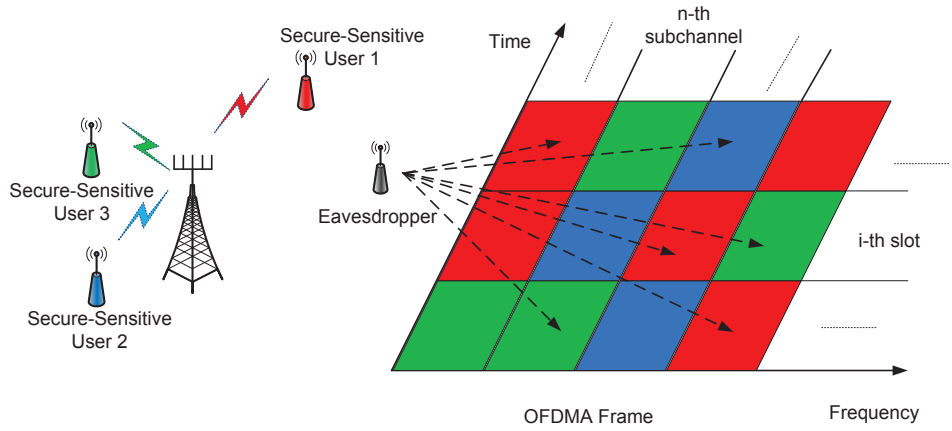



Fig. 3.1 System setup; the eavesdropper wiretaps the transmitted message within each data-bearing subchannel.

## 3.2 The problem of secrecy rate balancing

The downlink of a multiuser OFDMA-based system is considered, consisting of a single BS, $K$ users and one passive eavesdropper. It is assumed that the BS uses $N$ subchannels to transmit and the eavesdropper aims to wiretap the transmitted signal within all the data-bearing subchannels. An exclusive subchannel assignment is assumed, in which each subchannel is assigned exactly to one user. The considered setup is shown in Fig. 3.1.

Let $\mathscr{N} = \{1,\ldots,N\}$ denotes the set of the subchannels that are available for data transmission and $\mathscr{K} = \{1,\ldots,K\}$ denotes the set of users. Moreover, let $h_{n,k}$ denotes the channel response between user $k \in \mathscr{K}$ and the BS in subchannel $n \in \mathscr{N}$ and $h_{n,e}$ denotes the channel response between the eavesdropper and the BS in $n \in \mathscr{N}$. The secrecy rate of user $k \in \mathscr{K}$ within $n \in \mathscr{N}$ is given as

$$R^{sr}_{n,k}\left(p_{n,k}\right) = \left[\log\left(1+\frac{a_{n,k}p_{n,k}}{\sigma^2}\right) - \log\left(1+\frac{a_{n,e}p_{n,k}}{\sigma^2}\right)\right]_+, \tag{3.1}$$

where $p_{n,k}$ is the allocated power, $a_{n,k} = \left\|h_{n,k}\right\|^2$, $a_{n,e} = \left\|h_{n,e}\right\|^2$ and $\sigma^2$ is the noise variance (which is equal to one in what follows). Note that $R^{sr}_{n,k}(.)$, is zero when $a_{n,k} \leq a_{n,e}$. Let the binary variables $\omega_{n,k} = \{0,1\}, n \in \mathscr{N}, k \in \mathscr{K}$ denote the subchannel assignment, with $\omega_{n,k} = 1$ if subchannel $n$ is assigned to user $k$. The considered problem is to maximize the minimum secrecy rate across all the users under total transmitted power. Specifically, the problem is formulated as

$$\max_{\omega_{n,k},p_{n,k}} \min_{k} \sum_{n\in\mathscr{N}} \omega_{n,k} R^{sr}_{n,k}\left(p_{n,k}\right) \tag{3.2}$$

$$
\begin{aligned}
s.t. \quad & \sum_{k\in\mathscr{K},n\in\mathscr{N}} \omega_{n,k}p_{n,k} \leq P_T, \\
& \sum_{k\in\mathscr{K}} \omega_{n,k} = 1, && n\in\mathscr{N}, \\
& \omega_{n,k} \in \{0,1\}, && n\in\mathscr{N}, k\in\mathscr{K}, \\
& 0 \leq p_{n,k} \leq P_T, && n\in\mathscr{N}, k\in\mathscr{K},
\end{aligned}
$$

where $P_T > 0$ denotes the available amount of power at the BS. Note that $R^{sr}_{n,k}(.)$, $n\in\mathscr{N}$, $k\in\mathscr{K}$ in (3.2) is selected prior to the solution of the problem either as 0 or nonzero value, according to the known values $a_{n,k}$ and $a_{n,e}$. By introducing the non-negative power variables $s_{n,k} = \omega_{n,k}p_{n,k}$, $n\in\mathscr{N}, k\in\mathscr{K}$ and appropriately transforming the max-min objective in (3.2), the following maximization problem yields

$$
\begin{aligned}
& \max_{\omega_{n,k},s_{n,k},x} && x && && (3.3a)\\
s.t. \quad & 0 \leq x \leq \sum_{n\in\mathscr{N}} R^{sr}_{n,k}\left(s_{n,k}\right), && k\in\mathscr{K}, && (3.3b)\\
& \sum_{k\in\mathscr{K},n\in\mathscr{N}} s_{n,k} \leq P_T, && && (3.3c)\\
& \sum_{k\in\mathscr{K}} \omega_{n,k} = 1, && n\in\mathscr{N}, && (3.3d)\\
& \omega_{n,k} \in \{0,1\}, && n\in\mathscr{N},\ k\in\mathscr{K}, && (3.3e)\\
& 0 \leq s_{n,k} \leq \omega_{n,k}P_T, && n\in\mathscr{N}, k\in\mathscr{K}. && (3.3f)
\end{aligned}
$$

In (3.3), the scalar value $x$ defines the secrecy rate of system. Note that $\omega_{n,k}$ do not appear in the right-hand side of (3.3b) because $R^{sr}_{n,k}\left(s_{n,k}\right) = \omega_{n,k}R^{sr}_{n,k}\left(p_{n,k}\right)$ for any $\omega_{n,k}\in\{0,1\}$. The assignment policy is implicitly applied by the variables $s_{n,k}$, $n\in\mathscr{N}$, $k\in\mathscr{K}$ since the substitution $s_{n,k} = \omega_{n,k}p_{n,k}$ forces $s_{n,k} = 0$ when $\omega_{n,k} = 0$.

The problem in (3.3) is a mixed integer nonlinear program (MINLP) due to the existence of the binary variables $\omega_{n,k}$ and the logarithm-based functions $R^{sr}_{n,k}\left(s_{n,k}\right)$. Hence, in the general case it is NP-hard to solve. In the following sections, several optimal and suboptimal resource allocation schemes are presented that aim to solve it in an efficient manner.

### 3.2.1 Optimal power allocation for fixed subchannel assignment

Assume that each user $k\in\mathscr{K}$ achieves a nonzero secrecy rate and that $\mathscr{N}_k$ denotes the set of subchannels that have been assigned to the user $k\in\mathscr{K}$. Clearly, $\mathscr{N}_k\bigcap\mathscr{N}_j = \emptyset\ \forall(k,j)\in\mathscr{K}$ and $\mathscr{N}_1\bigcup\ldots\bigcup\mathscr{N}_K = \mathscr{N}$. The problem in (3.2) is written as

$$\max_{p_{n,k},x} \quad x \tag{3.4a}$$

$$s.t.\ \ 0 \le x \le \sum_{n\in\mathscr{N}_k} R^{sr}_{n,k}\left(p_{n,k}\right), \qquad k \in \mathscr{K}, \tag{3.4b}$$

$$0 \le p_{n,k} \le P_T, \qquad n \in \mathscr{N},\ k \in \mathscr{K}. \tag{3.4c}$$

For the above problem, the following proposition can be stated.

***Proposition 3.1***: The optimization problem (3.4) is convex.

*Proof.* The objective in (3.4) is linear with respect to the secrecy rate $x$. Moreover, the constraints in (3.4c) are linear functions of $p_{n,k}, n \in \mathscr{N}, k \in \mathscr{K}$. Thus, we focus on the secrecy constraint (3.4b) and especially in the right side. The second derivative of $R^{sr}_{n,k}(\bullet)$ with respect to $p_{n,k}$ is given as

$$\frac{\partial^2 R^{sr}_{n,k}}{\partial p^2_{n,k}} = \frac{\left(a_{n,e}-a_{n,k}\right)\left(a_{n,k}+a_{n,e}+2a_{n,k}a_{n,e}p_{n,k}\right)}{\left(1+a_{n,k}p_{n,k}\right)^2\left(1+a_{n,e}p_{n,k}\right)^2},$$

which is always negative for $a_{n,k} > a_{n,e}$. Thus, each term of the summation in the right side of (3.4b) is a concave function of $p_{n,k}$. Overall, the whole summation is a concave function as a sum of concave functions. □

In what follows, an algorithm is developed to derive the optimal solution in (3.4) in a semi-closed form, *i.e.* a form where bisection is used. Lets assume a fixed value $x_f$ such that $0 < x_f \le \min_k \sum_{n\in\mathscr{N}_k} \log\frac{a_{n,k}}{a_{n,e}}$. Clearly, the secrecy rate $x_f$ can be guaranteed to any user $k \in \mathscr{K}$ if there is sufficient (possible higher than $P_T$) amount of power at the BS. Nevertheless, the optimal power allocation that guarantees secrecy rate $x_f$ across all the users is the solution of the following problem

$$\min_{p_{n,k}} \quad \sum_{k\in\mathscr{K},n\in\mathscr{N}} p_{n,k}, \tag{3.5a}$$

$$s.t.\ \ x_f \le \sum_{n\in\mathscr{N}_k} R^{sr}_{n,k}\left(p_{n,k}\right), \qquad k \in \mathscr{K}, \tag{3.5b}$$

$$p_{n,k} \ge 0, \qquad n \in \mathscr{N}, k \in \mathscr{K}. \tag{3.5c}$$

For the problem (3.5), the following Theorem can be stated:

***Theorem 3.1***: In the optimal solution of (3.5), the power allocation of user $k \in \mathscr{K}$ over the subchannel $n \in \mathscr{N}_k$ is given as

$$\overline{p}_{n,k} = \begin{cases} \widetilde{p}_{n,k} & \text{if } \lambda_k > \frac{1}{a_{n,k}-a_{n,e}} \\ 0 & \text{if } \lambda_k \leq \frac{1}{a_{n,k}-a_{n,e}} \end{cases} \tag{3.6}$$

where the function $\widetilde{p}_{n,k}$ is given as

$$\widetilde{p}_{n,k} = -\frac{\left(a_{n,k}+a_{n,e}\right)}{2a_{n,k}a_{n,e}} + \frac{\sqrt{\left(a_{n,k}-a_{n,e}\right)^2 + 4\left(a_{n,k}-a_{n,e}\right)a_{n,k}a_{n,e}\lambda_k}}{2a_{n,k_n}a_{n,e}} \tag{3.7}$$

and $\lambda_k \geq 0$ is the Lagrange multiplier in (3.5b), $k \in \mathscr{K}$. Each one of the Lagrange multipliers $\lambda_k, k \in \mathscr{K}$ is calculated by (3.6), (3.7) and a bisection method to satisfy

$$x_f = \sum_{n \in \mathscr{N}_k} \log\left(\frac{1+\alpha_{n,k}\overline{p}_{n,k}}{1+\alpha_{n,e}\overline{p}_{n,k}}\right), \qquad k \in \mathscr{K}. \tag{3.8}$$

*Proof.* By Proposition 3.1, the problem in (3.5) is convex. Thus, its optimal solution can be specified by using the KKT conditions. Let $p^*_{n,k}$ be the optimal power allocation and $\lambda^*_k, \nu^*_{n,k}$ be the optimal Lagrange multipliers of (3.5b) and (3.5c), respectively. The *KKT* conditions for the problem in (3.5) are the following

$$\nabla_{p_{n,k}} L\left(p_{n,k}, \lambda_k, \nu_{n,k}\right)|_{p^*_{n,k}, \lambda^*_k, \nu^*_{n,k}} = 0, \qquad n \in \mathscr{N}, k \in \mathscr{K}, \tag{3.9a}$$

$$\begin{cases} \lambda^*_k \left(x_f - \sum_{n \in \mathscr{N}_k} \log\left(\frac{1+\alpha_{n,k}p^*_{n,k}}{1+\alpha_{n,e}p^*_{n,k}}\right)\right) = 0, & k \in \mathscr{K}, \\ \nu^*_{n,k} p^*_{n,k} = 0, & n \in \mathscr{N}, k \in \mathscr{K}, \end{cases} \tag{3.9b}$$

$$\begin{cases} \lambda^*_k \geq 0, & k \in \mathscr{K}, \\ \nu^*_{n,k} \geq 0, & n \in \mathscr{N}, k \in \mathscr{K}, \end{cases} \tag{3.9c}$$

$$\begin{cases} x_f - \sum_{n \in \mathscr{N}_k} \log\left(\frac{1+\alpha_{n,k}p^*_{n,k}}{1+\alpha_{n,e}p^*_{n,k}}\right) \leq 0, & k \in \mathscr{K}, \\ p^*_{n,k} \geq 0 & n \in \mathscr{N}, k \in \mathscr{K}, \end{cases} \tag{3.9d}$$

where $L(.)$ is the Lagrangian of (3.5), which is given as

$$L\left(p_{n,k}, \lambda_k, \nu_{n,k}\right) = \sum_{k \in \mathscr{K}} \sum_{n \in \mathscr{N}} p_{n,k} + \sum_{k \in \mathscr{K}} \lambda_k \left(x - \sum_{n \in \mathscr{N}_k} C_{n,k}\left(p_{n,k}\right)\right) - \sum_{n \in \mathscr{N}} \sum_{k \in \mathscr{K}} \nu_{n,k} p_{n,k}.$$

For $k \in \mathcal{K}, n \in \mathcal{N}$, the second legs in (3.9b), (3.9c) and (3.9d) dictate that either $\nu_{n,k}^* \geq 0$ and $p_{n,k}^* = 0$ or $\nu_{n,k}^* = 0$ and $p_{n,k}^* > 0$. The first case is trivial. In the most interesting case where $\nu_{n,k}^* = 0$ and $p_{n,k}^* > 0$, the following equation holds by (3.9a)

$$\lambda_k^* \left( \frac{\alpha_{n,k}}{1+\alpha_{n,k} p_{n,k}^*} - \frac{\alpha_{n,e}}{1+\alpha_{n,e} p_{n,k}^*} \right) = 1. \tag{3.10}$$

Equation (3.10) can be written in the following quadratic form

$$\alpha_{n,k}\alpha_{n,e} {p_{n,k}^*}^2 + \left(\alpha_{n,k} + \alpha_{n,e}\right) p_{n,k}^* - \lambda_k^* \left(\alpha_{n,k} - \alpha_{n,e}\right) + 1 = 0,$$

which for any $\lambda_k^* \in \mathbb{R}$ has the following two solutions in $\mathbb{R}$

$$\widetilde{p}_{n,k} = -\frac{\left(a_{n,k} + a_{n,e}\right)}{2a_{n,k}a_{n,e}} \pm \frac{\sqrt{\left(a_{n,k} - a_{n,e}\right)^2 + 4\left(a_{n,k} - a_{n,e}\right) a_{n,k} a_{n,e} \lambda_k^*}}{2a_{n,k_n}a_{n,e}} \tag{3.11}$$

Clearly, only the solution with the positive sign before the square root in the right hand of (3.11) may result to positive value. This is true when $\lambda_k^* > \frac{1}{a_{n,k}-a_{n,e}}$ and, thus, $p_{n,k}^* = \widetilde{p}_{n,k}$. In the opposite case where $\lambda_k^* \leq \frac{1}{a_{n,k}-a_{n,e}}$, then $p_{n,k}^* = 0$. Given these power allocation rules, the Lagrange multiplier $\lambda_k^*$, $k \in \mathcal{K}$, can be calculated by any Newton-based method in order to satisfy the first leg in (3.9b). Note that $\lambda_k^*$, $k \in \mathcal{K}$, is strictly positive when (3.9) is feasible. This is true since in the case where $\lambda_k^* = 0$ for a user $k \in \mathcal{K}$, its secrecy rate is zero by (3.11), *i.e.* $p_{n,k}^* = 0, n \in \mathcal{N}_k$, and (3.11) is feasible only in the trivial case where $x_f = 0$. Thus, in the non-trivial case where $x_f > 0$, it must hold that $\lambda_k^* > 0, k \in \mathcal{K}$ and the Lagrange multipliers are calculated to satisfy equality in the first leg of (3.9d).

□

The usage of bisection to calculate $\lambda_k, k \in \mathcal{K}$ is possible since the right hand in (3.8) is an increasing function of $\lambda_k$. This is true because the power allocation in (3.7) is an increasing function of $\lambda_k$, $k \in \mathcal{K}$ and $R_{n,k}^{sr}(.)$ in (3.2) is an increasing function of $p_{n,k}$. Thus, it turns out that each nonzero term in the summation in the right hand in (3.8) is also an increasing function of $\lambda_k$. One interesting observation regarding the power allocation in (3.6) is that it may result to a power transmission policy where power is allocated only to a subset of $\mathcal{N}_k$, $k \in \mathcal{K}$. This is more obvious if we consider that the elements in $\mathcal{N}_k$ are sorted in a decreasing order with respect to $\left(\frac{1}{a_{n,k}-a_{n,e}}\right)$. It turns out from (3.6), that $\lambda_k$ constitutes a threshold that points out which of the elements in $\mathcal{N}_k$ will have nonzero power. An increase (decrease) in the value of $\lambda_k$ transposes this threshold accordingly and may result to allocate power in more (less) channels in $\mathcal{N}_k$.

Clearly, when the available power at the BS is $P_T$, the secrecy rate $x_f$ can be supported by the system only when $\sum_{k\in\mathcal{K}, n\in\mathcal{N}} \overline{p}_{n,k} \leq P_T$. To arrive to a final solution in (3.4), the power policy described by Theorem 3.1 for a given $x_f$ is combined with a bisection method

**Algorithm 6:** Optimal power allocation for fixed subchannel assignment (OPA/FSA).

Set $x_{min} = 0$, $x_{max} = \min_k \sum_{n \in \mathcal{N}_k} \log \frac{a_{n,k}}{a_{n,e}}$.
**repeat**
  Set $x_f = (x_{min} + x_{max})/2$.
  The problem in (3.5) is solved using Theorem 3.1. Let $\overline{p}_{n,k}$ be the resulting power allocation $k \in \mathcal{K}, n \in \mathcal{N}$.
  The total power consumption is calculated as $P_c = \sum_{n,k} \overline{p}_{n,k}$.
  **if** $P_c < P_T$ **then**
    Set $x_{min} = x_f$ and $p^*_{n,k} = \overline{p}_{n,k}, k \in \mathcal{K}, n \in \mathcal{N}_k$.
  **else**
    Set $x_{max} = x_f$.
  **end if**
**until** $|x_{min} - x_{max}| \leq \varepsilon$
Output $p^*_{n,k}, k \in \mathcal{K}, n \in \mathcal{N}$.

over $x$. For each iteration of the bisection method, the problem in (3.5) is solved and the total power consumption is calculated. In the case where the total power consumption is lower (higher) than $P_T$, $x_f$ is increased (decreased) and the process is repeated. Such an increase (decrease) in $x_f$ is interpreted as an increase (decrease) in the multipliers $\lambda_k, k \in \mathcal{K}$, and, thus, more (less) power is allocated per user. By appropriately setting the lower and upper values for the bisection over $x$, $x_{min}$ and $x_{max}$ respectively, the process is repeated until a predefined convergence of the total power consumption to $P_T$ is achieved. Thus, both the optimal power allocation per subchannel and the maximum value of secrecy rate that can be supported without violating the total power constraint are specified. The resulting algorithm, called Optimal Power Allocation for Fixed Subchannel Assignment (OPA/FSA), is described in Algorithm 6. Its computational complexity is $\mathcal{O}\left(N \log_2^2 (1/\varepsilon)\right)$, where $\varepsilon > 0$ is the predefined required accuracy in the involved bisections.

## 3.3 Optimal resource allocation in the case of more users than subchannels

In the case where the number of users is higher than the number of subchannels, the optimal resource allocation scheme can be specified by using a special case of assignment problem which is called linear sum assignment problem (LSAP) [90]. In general, an assignment problem deals with the question of how to assign a set of $N$ different jobs, (*i.e.* subchannels), to $K$ different servers, (*i.e.* users) in an optimal way. The output of an assignment algorithm can be described by a $N \times K$ binary assignment matrix $W$, where $W_{n,k} = 1$ when subchannel $n$ is occupied by user $k$, otherwise $W_{n,k} = 0$. In an LSAP, a value is defined for each possible binding $(n,k)$, which reflects the cost of assign subchannel $n$ to the user $k$. The aim is to specify a mapping $W$ that minimizes the total cost value under the assumption that each subchannel is strictly assigned to one user and each user occupies up to one subchannel.

Consider a fixed value of secrecy rate $x = x_f$ such that $0 < x_f \leq \max_{n,k} \log \frac{a_{n,k}}{a_{n,e}}$. Let $P$ denotes an $N \times K$ power cost matrix, where the element $P_{n,k}$ reflects the power that is required by user $k$ to achieve secrecy rate $x_f$ when it occupies (only) the subchannel $n$. The value of $P_{n,k}$ is obtained by setting $R^{sr}_{n,k}\left(P_{n,k}\right) = x_f$ as

$$P_{n,k} = \frac{2^{x_f} - 1}{a_{n,k} - a_{n,e}2^{x_f}}, \qquad n \in \mathcal{N}, k \in \mathcal{K}, \tag{3.12}$$

The non-positive values $P_{n,k}$ that result from (3.12) are set equal to $\infty$ reflecting the fact that secrecy $x_f$ cannot be achieved by assigning $n$ to user $k$. Based on the matrix $P$ and the specific value of $x_f$, the LSAP in (3.13) is formulated, where the aim is to specify the mapping of minimum overall power cost between the $N$ subchannels and exactly $N$ (out of $K$) users

$$\min_{W} \sum_{k\in\mathcal{K}} \sum_{n\in\mathcal{N}} W_{n,k} P_{n,k} \tag{3.13a}$$

$$s.t. \sum_{k\in\mathcal{K}} W_{n,k} = 1, \qquad n \in \mathcal{N}, \tag{3.13b}$$

$$\sum_{n\in\mathcal{K}} W_{n,k} \leq 1, \qquad k \in \mathcal{K}, \tag{3.13c}$$

$$W_{n,k} \in \{0,1\}, \qquad n \in \mathcal{N}, k \in \mathcal{K}. \tag{3.13d}$$

Given the LSAP's solution in (3.13), the fixed value $x_f$ is guaranteed across all the users only when the total power cost is less than $P_T$. Thus, the solution of the original problem in (3.2) can be obtained by solving a series of LSAPs in the form of (3.13) that are controlled by a bisection method over the value of $x$. The procedure is optimal since the secrecy rate $x$ is directly proportional to the available power $P_T$. The overall algorithm, called Optimal Resource Allocation (ORA), is described in Algorithm 7. It is well known that rectangular

**Algorithm 7:** Optimal resource allocation (ORA)

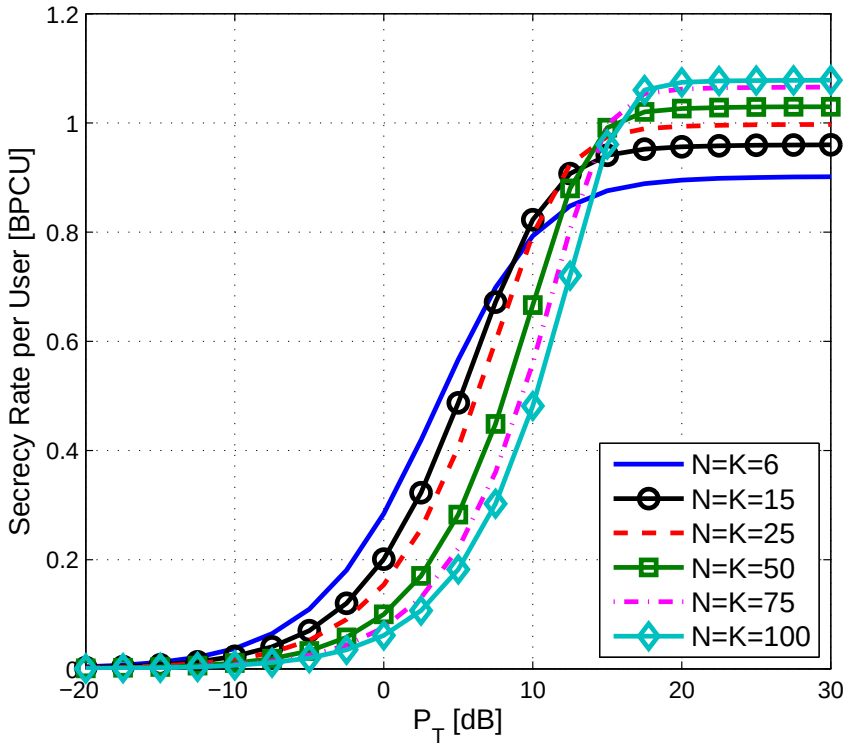
Set $x_{min} = 0$ and $x_{max} = \max_{n,k} \log \frac{a_{n,k}}{a_{n,e}}$.
**repeat**
  Set $x_f = (x_{min} + x_{max})/2$.
  Given $x_f$, the elements of the $N \times K$ power cost matrix $P$ are calculated based on (3.12).
  The LSAP in (3.13) is solved to obtain the $N \times K$ binary assignment matrix $\overline{W}$.
  The total power consumption $P_c$ is calculated as $P_c = \sum_{n,k} \overline{W}_{n,k} P_{n,k}$.
  **if** $P_c < P_T$ **then**
    Set $x_{min} = x_f$ and $W^* = \overline{W}$.
  **else**
    Set $x_{max} = x_f$.
  **end if**
**until** $|x_{min} - x_{max}| \leq \varepsilon$
Output $W^*$.

LSAP can be solved by extending it to a square LSAP using dummy variables, which is optimally solved in $\mathcal{O}\left(K^3\right)$ (or even less depending on the structure of the cost matrix) [89, 90]. Thus, the computational complexity of the Algorithm 7 is $\mathcal{O}\left(K^3 \log\left(1/\varepsilon\right)\right)$.

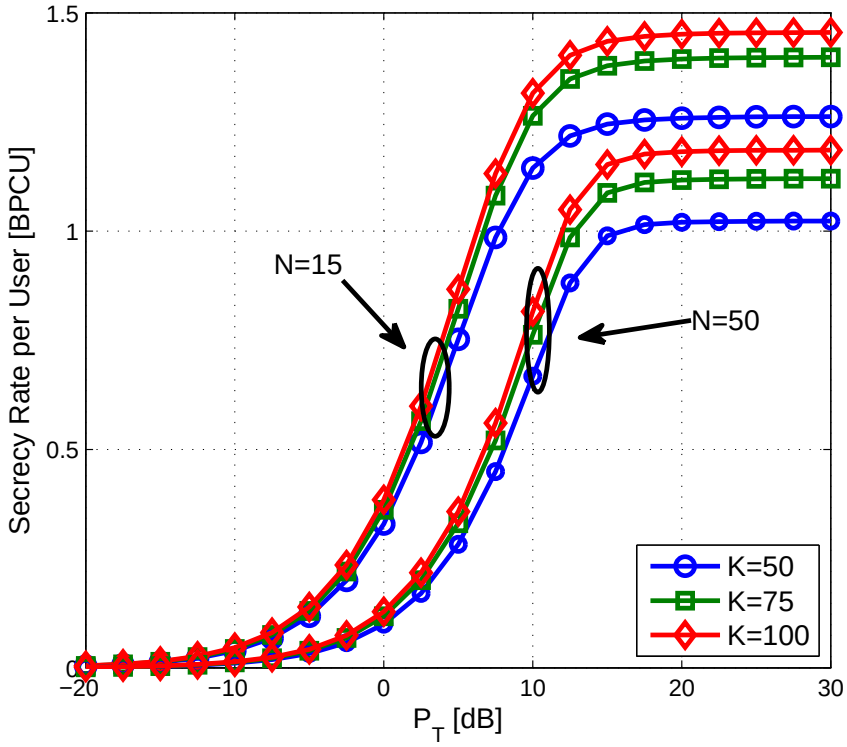
### Numerical results

In Fig. 3.2a and Fig. 3.2b, the secrecy rate per user of ORA is evaluated for the case where $K \geq N$. Note that ORA is the optimal solution to (3.3). The number of subchannels is selected from the set $\{6, 15, 25, 50, 75, 100\}$, which are the values that are defined in Long-Term Evolution (LTE) specifications (subchannels are referred as Resource Blocks in LTE's terminology) [91]. Both figures are characterized by an "error floor" phenomenon as $P_{Tot}$ increases, which reflects the fact that secrecy rate per subchannel $R^{sr}_{n,k}\left(p_{n,k}\right)$ approximates a constant value as the power $p_{n,k}$ increases. In Fig. 3.2a, the performance of ORA is evaluated for $N = K$. As shown, the secrecy is affected in a different way by $N$. For lower values of $P_T$, a smaller number of subchannels results in a higher secrecy rate per user, while the opposite is true for increasing $P_T$. Such a behavior is justified since the same amount of power is split to fewer users in the first case. Hence, a higher secrecy rate can be guaranteed for all of them. As $P_T$ increases, the system gradually starts to benefit from the additional frequency diversity that is offered by the existence of a higher number of subchannels. Thus, for moderate to high values of $P_T$, both a higher secrecy rate per user and a higher number of serviced users may be achieved.

In Fig. 3.2b, the performance of ORA is evaluated for the the case where $K > N$ and $N = \{15, 50\}$. As the number of users increases, the multiuser diversity of the system also increases. Thus, a more efficient subset of serviced users is specified in terms of secrecy




(a) Secrecy rate per user of ORA vs $P_T$ for $K = N$.




(b) Secrecy rate per user of ORA vs $P_T$ for $K \geq N$.

Fig. 3.2 Secrecy rate of Optimal Resource Allocation Algorithm.

rate. However, it is clear that multiuser diversity saturates as $K$ increases since the support of channel fading (across the users) is bounded [92].

## 3.4 Resource allocation schemes in the case of less users than subchannels

In the case of less users than subchannels, the original problem in (3.3) is hard to solve. In this section, we develop a MILP form of (3.3) by performing PLA in $R_{n,k}^{sr}\left(p_{n,k}\right)$. As the number of linear segments increases, the resulting MILP model becomes more accurate and its solution converges to the optimal one [93]. Thus, MILP's performance can be used as a benchmark for the performance of any other resource allocation scheme that is mentioned in this section. Apart from PLA, the original problem is examined for two special cases, namely when $P_T \to \infty$ and $P_T \to 0$, respectively. Inspired by the optimal solutions in these cases, two resource allocation schemes are proposed of competitive performance in the non-limit power area too. Finally, two low-complexity, heuristics are presented in order to provide a better tradeoff between performance and computational complexity.

### 3.4.1 Optimality in two special cases

In this subsection, the optimal solution in (3.3) is derived for two special cases, namely the case where $P_T \to \infty$ and the case where $P_T \to 0$. Interestingly, each solution gives rise to a resource allocation scheme that has competitive performance in the non limit power regime compared to the near-optimal MILP–OPA/FSA scheme of the previous subsection.

#### Optimality in high-power regime

Consider a specific subchannel $n \in \mathcal{N}$ and let $k_n \in \mathcal{K}$ denotes the user that occupies the subchannel $n$. When $p_{n,k_n} \to \infty$ also holds, where $k_n \in \mathcal{K}$ is the user that occupies the subchannel $n$. Hence, the secrecy rate within subchannel $n$ takes the following form

$$f_{n,k_n} = \lim_{p_{n,k_n}\to\infty} R_{n,k_n}^{sr}\left(p_{n,k_n}\right) = \log_2\left(\frac{a_{n,k_n}}{a_{n,e}}\right) \tag{3.14}$$

Merging (3.14) into the original problem (3.3), yields the following MILP

$$\max_{\omega_{n,k},x} \quad x \tag{3.15a}$$

$$s.t.\ \ 0 \le x \le \sum_{n\in\mathcal{N}} \omega_{n,k} f_{n,k}, \qquad k \in \mathcal{K}, \tag{3.15b}$$

$$\sum_{k\in\mathcal{K}} \omega_{n,k} = 1, \qquad n \in \mathcal{N}, \tag{3.15c}$$

$$\omega_{n,k} \in \{0,1\}, \qquad n \in \mathcal{N},\ k \in \mathcal{K}. \tag{3.15d}$$

Clearly, the optimal solution in (3.15) coincides with the optimal solution in (3.3) as $P_T \to \infty$. Nevertheless, the idea of using (3.14) and solving the problem in (3.14) may be extended to the non-limit range of $P_T$ values. In Fig. 3.3, the behavior of $R_{n,k}^{sr}(.)$ is depicted for two

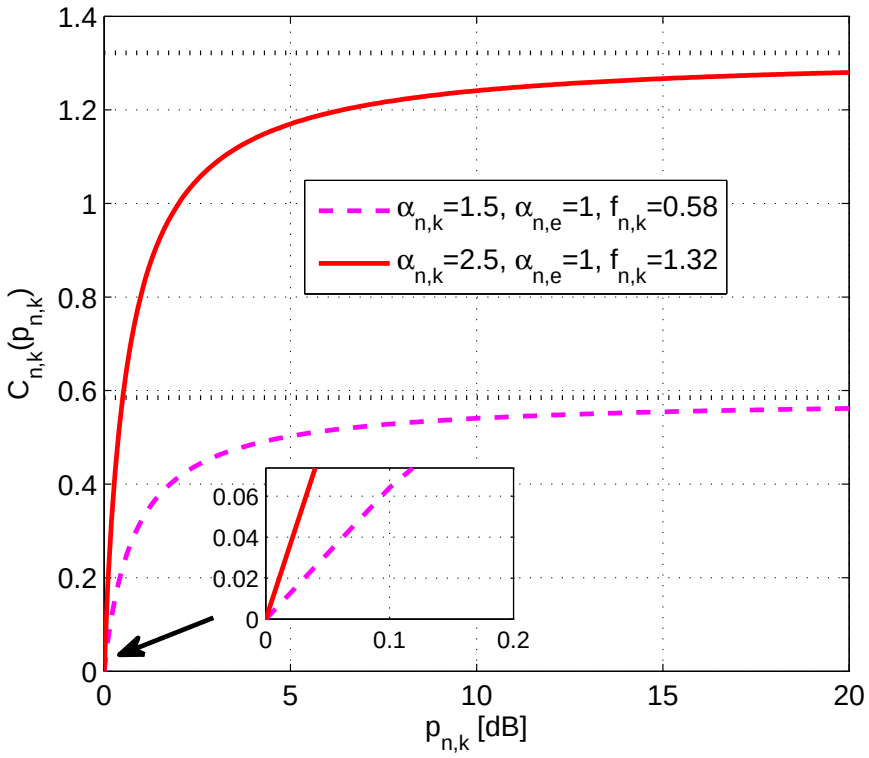



Fig. 3.3 Approximation of secrecy rate formula in high power regime.

different pairs $(a_{n,k}, a_{n,e})$. As it is shown, the convergence of $R^{sr}_{n,k_n}(.)$ to the $f_{n,k_n}$ is observed even for relatively small values of $p_{n,k}$. Thus, the approximation in (3.14) and the MILP in (3.15) can be set even for large but finite $P_T$ values. In such a case, the resulting subchannel assignment in (3.15) can be combined with the OPA/FSA algorithm. The resulting resource allocation scheme, called Optimal Infinity Power with OPA/FSA (OIP–OPA/FSA), is the optimal solution of the original problem in (3.3) as $P_T \to \infty$.

### Optimality in low-power regime

Let assume a fixed subchannel assignment over the $K$ users. As $P_T \to 0$, it is natural to assume that the amount of power that is allocated per user also tends to zero, *i.e.* $P_k = \sum_{n \in \mathcal{N}_k} p_{n,k} \to 0, k \in \mathcal{K}$. In this case, each user allocates power only to one of the subchannels that have been assigned to it, which is the subchannel with the largest derivative in $R^{sr}_{n,k}(.)$ at $p_{n,k} = 0$. An intuitive explanation can be deduced by Fig. 3.3. Assume that the two curves in Fig. 3.3 denote the secrecy rate over two subchannels that have been assigned to the same user. Since both of them have almost linear behavior in the origin, the curve with the largest derivative at $p_{n,k} = 0$ yields the highest secrecy rate as $P_k \to 0$. Thus, for small enough $P_k$, each user will have nonzero secrecy rate only within one of the subchannels that

have been assigned to it. Hence, the optimal subchannel assignment and power allocation can be specified by setting up a series of rectangular LSAPs, similar to the Section 3.3.

Consider a fixed value of secrecy rate $x = x_f$ such that $0 < x_f \leq \max_{n,k} \log \frac{a_{n,k}}{a_{n,e}}$ and the power cost matrix $P$ which is calculated by (3.12), similar to the Section 3.3. Assume the following LSAP

$$\min_{W} \quad \sum_{k\in\mathscr{K},n\in\mathscr{N}} W_{n,k}P_{n,k} \tag{3.16a}$$

$$s.t. \quad \sum_{n\in\mathscr{N}} W_{n,k} = 1, \qquad k \in \mathscr{K}, \tag{3.16b}$$

$$\sum_{k\in\mathscr{K}} W_{n,k} \leq 1, \qquad n \in \mathscr{N}, \tag{3.16c}$$

$$W_{n,k} \in \{0,1\}, \qquad n \in \mathscr{N}, k \in \mathscr{K}, \tag{3.16d}$$

where (3.16b) guarantees that each user will occupy strictly one subchannel and (3.16c) states that that it is possible for any subchannel not to be assigned at all. Given the optimal solution in (3.16), the secrecy rate $x_f$ is guaranteed for the problem (3.3), only if the total power cost is up to $P_T$. Under this scope, the maximum possible secrecy rate for the initial problem in (3.3) can be obtained by solving a series of LSAPs in the form of (3.16), which is controlled by a bisection method over the value of $x_f$. The overall resource allocation scheme, called Optimal Near-zero Power (ONZP), is the optimal solution of the original problem in (3.3) as $P_T \to 0$. Its computational complexity is $\mathscr{O}\left(N^3 \log\left(1/\varepsilon\right)\right)$ since a similar argument to the Algorithm 7 can be stated, where the roles of input sizes $K$ and $N(N > K)$ are interchanged.

### 3.4.2 A near-optimal solution based on linear piecewise approximation

By employing PLA on the continuous, logarithmic and increasing functions $R^{sr}_{n,k}\left(s_{n,k}\right)$ in (3.3), it turns out that it is approximated as

$$R^{sr}_{n,k}\left(s_{n,k}\right) = \sum_{l\in\mathscr{L}} c^l_{n,k}\xi^l_{n,k}, \qquad n \in \mathscr{N}, k \in \mathscr{K}, \tag{3.17}$$

where $\xi^l_{n,k}$ is the load variable and $c^l_{n,k}$ is the slope of segment $l \in \mathscr{L}$ and $s_{n,k} = \sum_{l\in\mathscr{L}} \xi^l_{n,k}$ where $0 \leq \xi^l_{n,k} \leq b^l_{n,k} - b^{l-1}_{n,k}, l \in \mathscr{L}$[1]. By integrate (3.17) into (3.3), a MILP results since the objective and all the constraints are linear functions while both binary and continuous variables are involved, as it is shown in (3.18)

[1]For simplicity reasons, it is assumed that the same number of linear segments is used to approximate $R^{sr}_{n,k}\left(s_{n,k}\right)$ for all different possible pairs $(n,k)$.

$$\max_{\omega_{n,k},s_{n,k},\xi^l_{n,k},x} \quad x \qquad s.t. \tag{3.18a}$$

$$0 \le x \le \sum_{n\in\mathcal{N},l\in\mathcal{L}} c^l_{n,k}\xi^l_{n,k}, \qquad k\in\mathcal{K}, \tag{3.18b}$$

$$\sum_{k\in\mathcal{K},n\in\mathcal{N}} s_{n,k} \le P_T, \tag{3.18c}$$

$$\sum_{k\in\mathcal{K}} \omega_{n,k} = 1, \qquad n\in\mathcal{N}, \tag{3.18d}$$

$$\omega_{n,k} \in \{0,1\}, \qquad n\in\mathcal{N},k\in\mathcal{K}, \tag{3.18e}$$

$$0 \le s_{n,k} \le \omega_{n,k}P_T, \qquad n\in\mathcal{N},k\in\mathcal{K}, \tag{3.18f}$$

$$0 \le \xi^l_{n,k} \le b^l_{n,k} - b^{l-1}_{n,k}, \qquad n\in\mathcal{N},k\in\mathcal{K},l\in\mathcal{L}, \tag{3.18g}$$

$$s_{n,k} = \sum_{l\in\mathcal{L}} \xi^l_{n,k}, \qquad n\in\mathcal{N},k\in\mathcal{K}, \tag{3.18h}$$

where the constraints (3.18b)–(3.18f) are inherited by the original problem (3.13) with the only difference that $R^{sr}_{n,k}\left(s_{n,k}\right)$ has been replaced by its linear approximation $\sum_{l\in\mathcal{L}} c^l_{n,k}\xi^l_{n,k}$. Moreover, the constraints (3.18g) and (3.18h) are imposed by the used linear approximation model. The subchannel assignment obtained by solving (3.18) can be combined with the OPA/FSA policy, presented in Algorithm 6. The whole resource allocation scheme, called MILP–OPA/FSA, performs near to optimal (especially as the linear approximation of the logarithmic functions becomes more dense) and it can be used as benchmark to evaluate the performance of any other proposed scheme.

### 3.4.3 Low-complexity heuristics

In this subsection, two resource allocation schemes are presented which are inspired by two corresponding existing methods that has been suggested in the literature for different problems. In both, the inherent subchannel assignment and power allocation subproblems in (3.3) are decoupled. In the first scheme, a greedy subchannel assignment is adopted while the second, assignment is inspired by the special case of Subsection 3.4.1 and appropriately solving the problem in (3.15). Given subchannel assignment, power allocation is solved by using OPA/FSA in both schemes.

#### Greedy subchannel assignment

The problems of subchannel assignment and power allocation are decoupled and the first is solved in an iterative manner in which the subchannels are assigned to users one-by-one. In each iteration, the user with the currently lowest secrecy rate is enforced to occupy one more subchannel from the available ones. The subchannel that is assigned to it is the one

**Algorithm 8:** Greedy subchannel assignment (GSA)

1: Let $\mathscr{N}_A$ denotes the set of the available subchannels. Initially, $\mathscr{N}_A = \{1,2,\ldots,N\}$.
2: **for** $n = 1,\ldots,N$ **do**
3: Find $k^o = arg\min_k \sum_{n\in\mathscr{N}_k} R^{sr}_{n,k}\left(\frac{P_T}{N-|\mathscr{N}_A|}\right)$.
4: The subchannel $n^o = arg\max_{n\in\mathscr{N}_A}\left(\alpha_{n,k}-\alpha_{n,e}\right)$ is inserted into $\mathscr{N}_{k^o}$ and it is removed from the set $\mathscr{N}_A$.
5: The secrecy rate of all users is updated assuming that $P_T$ is equally split across the subchannels that have been assigned so far.
6: **end for**
7: Output $\mathscr{N}_k, k\in\mathscr{K}$.

that has the highest difference in channel gain with respect to the eavesdropper. In each iteration, the users update their secrecy rate under the assumption that the available power is equally split across the assigned subchannels. The process is repeated up to the point where all subchannels have been assigned to users. The overall procedure, called Greedy Subchannel Assignment (GSA), is described in Algorithm 8. Its computational complexity is $\mathscr{O}(N(K+N))$ since just two maximum/minimum search operations are performed per subchannel assignment iteration. Using the resulting subchannel assignment, OPA/FSA is triggered to allocate power in an optimal way and guarantee secrecy rate equality across users. The overall resource allocation scheme is called as GSA–OPA/FSA.

### Relaxation, roundup and subchannel swapping

In this heuristic approach, (3.15) is considered again but the binary variables $\omega_{n,k}$ are relaxed to take values within $[0,1]$. Thus, the resulting problem is an LP that can be solved in polynomial complexity by any standard LP solver. As it is known, the solution of the particular LP produces at least $N-K+1$ (out of $NK$) variables $\omega_{n,k}$ which are equal to one [94]. Based on these variables, a partial subchannel assignment can be derived and, thus, a subset of $\mathscr{N}$ is assigned to the users. For each one of the remaining (unassigned) subchannels, the values $\omega_{n,k}$ are compared across all the users and the subchannel is assigned to the user that corresponds to the highest value. Hence, a complete initial subchannel assignment is obtained and is used by (3.14) to calculate an initial secrecy rate across the users. Clearly, in this stage not all the users will have the same secrecy rate. Both the assignment and the users' secrecy rates are given as inputs to the subchannel swapping phase that follows. The subchannel swapping phase is of greedy, iterative nature and aims to present a final assignment output that is at least as efficient as the initial one. At each iteration, the user with the lowest secrecy rate is specified and a candidate set of subchannels is generated that contains subchannels which may be re-assigned to it. The decision whether a subchannel will be inserted into the re-assignment set or not, depends on the amount of secrecy rate reduction for the user that losses it. Specifically, the updated secrecy rate of that user (after a possible

**Algorithm 9:** Relaxation, roundup and subchannel swapping (RRSS)

1: The problem in (3.15) is relaxed, *i.e.* by setting $0 \leq \omega_{n,k} \leq 1, n \in \mathcal{N}, k \in \mathcal{K}$. Let $\overline{\omega}_{n,k}$ be the solution of the resulting LP.
2: Let $\mathcal{N}_k$ denotes the set of subchannels assigned to user $k$. Initially $\mathcal{N}_k = \emptyset, k \in \mathcal{K}$.
3: **for** $n \in \mathcal{N}$ **do**
4: Subchannel $n$ is inserted into $\mathcal{N}_{k_n}$, where $k_n = \arg\max_{k \in \mathcal{K}} \overline{\omega}_{n,k}$.
5: **end for**
6: **repeat**
7: Find $k^o = \arg\min_{k \in \mathcal{K}} \sum_{n \in \mathcal{N}_k} \log f_{n,k}$ and set $R^{k^o} = \sum_{n \in \mathcal{N}_k^o} \log f_{n,k^o}$.
8: Let $\mathcal{N}_{SS}$ denotes the set of candidate subchannels for possible re-assignment to $k^o$. Initially $\mathcal{N}_{SS} = \emptyset$.
9: **for** $m \in \mathcal{N} \setminus \mathcal{N}_{k^o}$ **do**
10: Subchannel $m$ is inserted in $\mathcal{N}_{SS}$, if its re-assignment to $k^o$ doesn't reduce the secrecy rate of the user that currently occupies it to become less than $R^{k^o}$.
11: **end for**
12: **if** $\mathcal{N}_{SS} \neq \emptyset$ **then**
13: The subchannel $m^o$ is inserted into $\mathcal{N}_{k^o}$, where $m^o = \arg\max_{m \in \mathcal{N}_{SS}} f_{m,k^o}$.
14: **end if**
15: The secrecy rates of the users involved in the swapping of $m^o$ are updated.
16: **until** $\mathcal{N}_{SS} \neq \emptyset$
17: Output $\mathcal{N}_k, k \in \mathcal{K}$.

re-assignment) must be no less than the secrecy rate of the user that currently has the lowest value. When the candidate set is finalized, the subchannel giving the largest increase in the secrecy rate of the user with the currently lowest secrecy rate is assigned to it and the secrecy rates of the users that have been involved in the swapping are re-calculated. The process is repeated in a similar way until an empty candidate set results at some iteration. The overall procedure, called as Relaxation, Roundup and Subchannel Swapping (RRSS), is described in Algorithm 9. In general, an LP can be solved in $\mathcal{O}\left((KN)^{3.5}\right)$ computational complexity, where $KN$ is the number of unknown variables [95]. Assuming that the number of performed iterations in the swapping phase is $N_{iter}$, the overall complexity of Algorithm 9 is $\mathcal{O}\left((KN)^{3.5} + KNN_{iter}\right)$, as the complexity of one swapping iteration is $\mathcal{O}(KN)$. Using the resulting subchannel assignment, the convex problem of power allocation is solved to optimality to obtain a complete resource allocation solution, called as RRSS–OPA/FSA.

### Numerical results

The performance of MILP–OPA/FSA and the effect of piecewise linear approximation are shown in Fig. 3.4, where the relative error in secrecy rate of the system is shown with respect to the number of segments ($L$) for three different values of $P_T$. The relative error is defined with respect to the performance of an exhaustive subchannel assignment policy

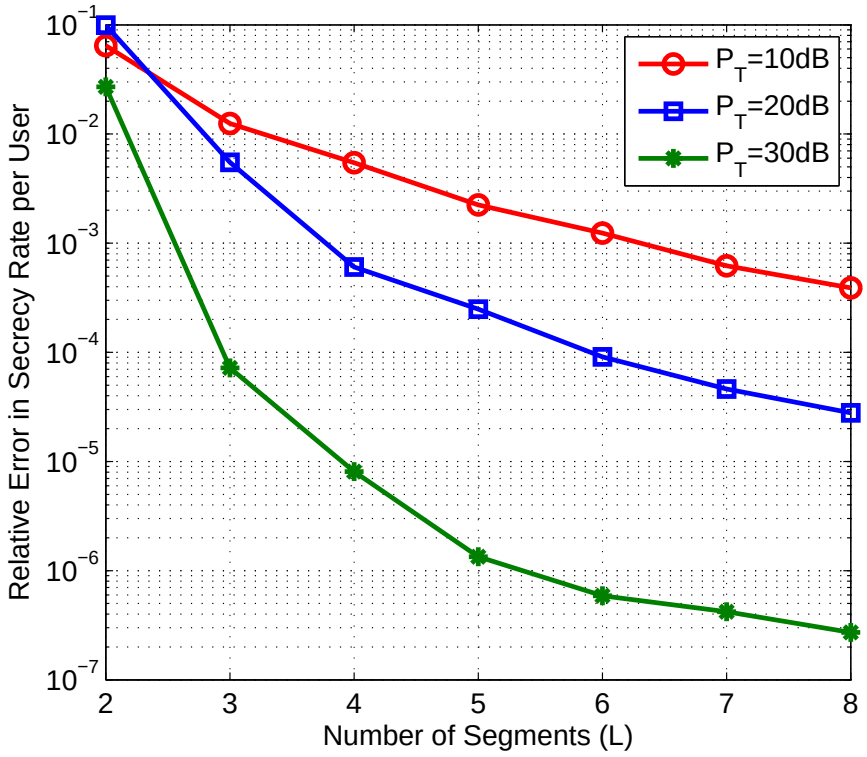



Fig. 3.4 Secrecy rate per user of MILP-OPA/FSA versus the number of segments in linear approximation of secrecy formula, $N = 6$ and $K = 5$.

that provides the optimal solution to the considered problem. Given the demanding computational complexity of an exhaustive assignment policy, the number of subchannels is set equal to $N = 6$. In linear approximation of $R^{sr}_{n,k}(.)$, $n \in \mathcal{N}, k \in \mathcal{K}$, the first breakpoint is set to $b_0 = 0$, while the rest are set by using an exponential rule over the inter-point distance[2]. Thus, a denser segmentation results at the beginning of each logarithmic function $R^{sr}_{n,k}(.)$. In general, MILP–OPA/FSA provides a very tight approximation to the optimal solution in (3.3), while in the most cases it achieves the optimal. As shown in Fig. 3.4, this is substantially achieved even for small number of linear segments. It should be noted that an increase in the number of segments implies a proportional increase in the computational complexity of the MILP formulation in (3.18).

Figure 3.5a depicts the secrecy rate per user versus $P_T$ for all the proposed algorithms, $N = 15$ and $K = 6$. The performance of MILP–OPA is used as benchmark to evaluate the performance of the two low-complexity resource allocation schemes presented in Section 3.4.3, namely the GSA–OPA/FSA and the RRSS–OPA/FSA, respectively. Finally, the performance of OIP–OPA/FSA and ONZP is shown, which are the optimal resource allocation

[2]Specifically, the rest breakpoints are set by using the formula $[b_1,\ldots,b_L] = \frac{P_T}{2^w}$, where $w = linspace(10,0,L)$.

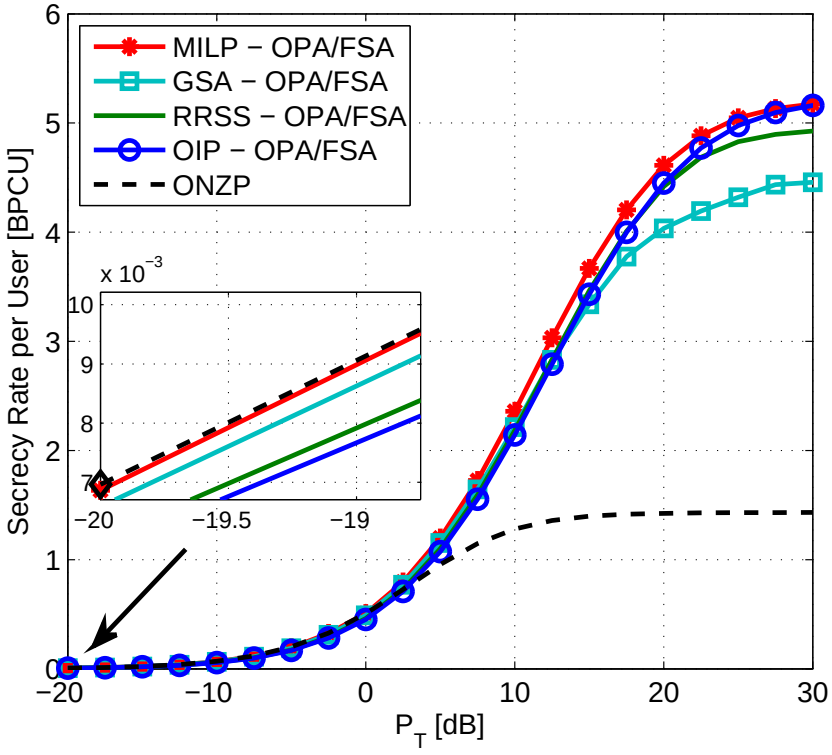
Table 3.1 Relative secrecy rate of the presented schemes over MILP–OPA/FSA.

| $P_T$ | GSA-OPA/FSA | RRSS-OPA/FSA | OIP-OPA/FSA | ONZP |
|---|---|---|---|---|
| -20 dB | 96.02 | 88.10 | 85.33 | **99.99** |
| -10 dB | 96.18 | 88.41 | 85.76 | **99.99** |
| 0 dB | 96.76 | 90.84 | 89.02 | **99.75** |
| 10 dB | **93.88** | 92.63 | 90.80 | 54.32 |
| 20 dB | 87.48 | 95.83 | **96.49** | 30.80 |
| 30 dB | 86.13 | 95.20 | **99.77** | 27.68 |

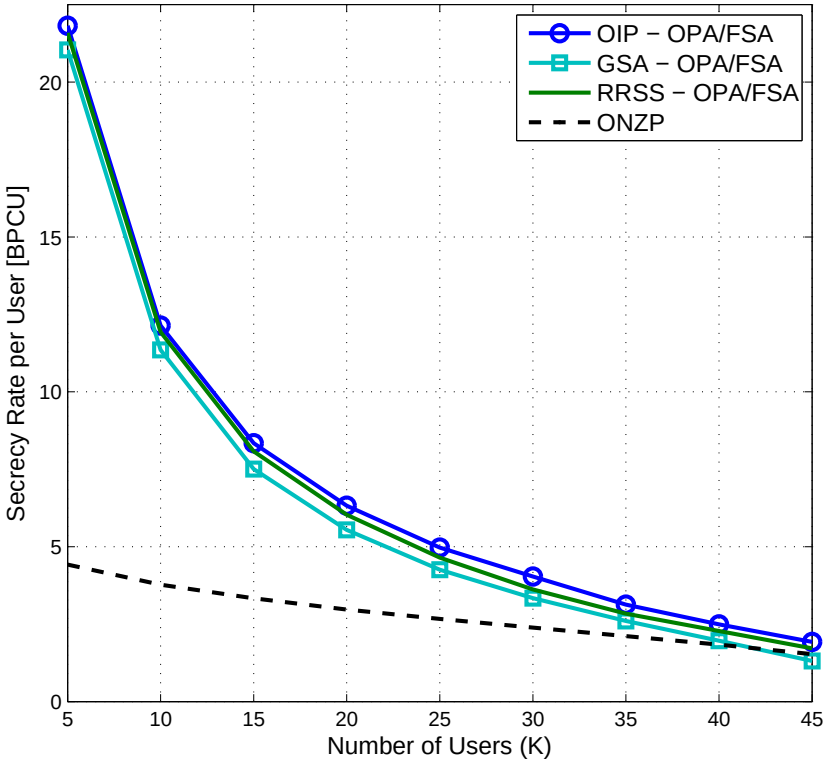
schemes for $P_T \to \infty$ and $P_T \to 0$, respectively. As shown in Fig. 3.5a, both schemes perform competitively for moderate to high and low to moderate $P_T$ values, respectively.

The relative performance of each resource allocation scheme versus the MILP–OPA/FSA is shown in Table 3.1. Regarding the performance of RRSS, it is remarkable that it closely follows the performance of OIP since it is based on the same high power approximation in (3.14). The advantage of RRSS over OIP is that it solves a much simpler LP problem than the MILP formulation of the second. Comparing the performance of the two low-complexity solutions, it seems that GSA performs better in low power regime while RRSS it is superior than GSA as $P_T$ increases. It should be noted that these schemes along with ONZP are characterized by polynomial computational complexity. Thus, depending on the value of $P_T$, an appropriate handling between the three of them achieves more than 93% of the PLA–MILP performance in any case.

Finally, in Fig. 3.5b, the scaling behavior of the secrecy rate per user is shown as the number of users increases, $N = 50$ and $P_T = 30$ dB. OIP–OPA/FSA is used as benchmark for the other solutions since it is almost optimal for $P_T = 30$ dB. As can be seen, the relative performance of OIP–OPA/FSA, GSA–OPA/FSA and RRSS–OPA/FSA is nearly independent of the number of users, while there is a gap in ONZP's performance since it is a low power inspired algorithm. However, its behavior is improved as $N/K \to 1$ where one subchannel is approximately assigned for each user.




(a) Secrecy rate per user vs $P_T$ for $N = 15, K = 6$.




(b) Secrecy rate per user vs the number of users for $N = 15, P_T = 30$dB.

Fig. 3.5 Secrecy rate per user of the presented resource allocation schemes.

# Chapter 4

# Throughput maximization in multiantenna systems under secrecy rate constraints

## 4.1 Introduction

In multiantenna systems, the integration of physical layer security into the resource allocation procedure results to quite challenging optimization problems; the existed degrees of freedom can be used to provide both secrecy and conventional rate benefits. In principle, the resource allocation problems in the field are difficult to be solved in an optimal way. This is mainly due to their integer, combinatorial nature but also on the fact that secrecy rate formula is a more complex function than the conventional transmission rate function.

### State of the art

In the last years, a considerable research effort has been devoted towards developing secrecy techniques for multiuser multiple-input multiple-output (MIMO) networks. In [96], the idea of masked beamforming is presented, which sacrifices a portion of the transmitted power to broadcast an artificial interference (jamming signal) in the user channel's null space; this jamming signal confuses the eavesdropper about the legitimate information signal. In [97], [98], [99] the authors investigate robust masked beamforming techniques that minimize the transmitted power subject to per-user quality-of-service (QoS) constraints, under an imperfect channel state information (CSI). In [100], [101] the idea of artificial interference is extended to cooperative jamming, where a friendly helper is introduced to provide the jamming signal. Beamforming strategies for cooperative jamming are further investigated in [102].

In practical communication systems, a large number of users require to be served at any resource allocation epoch and a user selection procedure is necessary to be applied before any transmission design is employed. In [103], multiuser MIMO secrecy sum-rate is examined under a worst-case eavesdropping scenario where each user is wiretapped by all the other users of the system. In [104], the authors investigate simple user selection strategies to minimize transmitted power under some well-defined secrecy oriented constraints. The protection against the eavesdropper is based on sacrificing a portion of the available power to create jamming interference. In [79], resource allocation is considered problem for a multiple-input single-output (MISO)-OFDMA downlink with a multiantenna eavesdropper and partial channel state information (CSI) at the BS. The aim is to maximize an energy efficiency utility function, which takes into account both power consumption and secrecy outage capacity. An exclusive subchannel allocation policy is assumed and artificial noise is created to protect the transmission against the eavesdropper. The authors present an iterative resource allocation solution that is based on relaxing the exclusive subchannel allocation constraint. The motivation in this chapter is to explore how the coexistence of conventional users and users that should be protected by eavesdropping affects the problem of resource allocation; how this coexistence can be exploited through spatial multiplexing and power management to provide more efficient resource allocation solutions.

### Contribution

In this chapter, we investigate two resource allocation problems which consider physical layer security in multiantenna, multiuser downlink system; in the first, we aim to solve a user selection and power allocation problem in order to maximize the worst sum secrecy rate in a flat fading setup, in the sense that a passive eavesdropper is able to decode the message of all the spatially multiplexed users. Since the problem is combinatorial, we propose two low-complexity user selection schemes in which the spatial channel correlation metric is used. The key idea is to integrate the protection of the information signal (by the eavesdropper) into the user selection process. In the second considered problem, we assume a multiantenna system that uses a number of parallel channels to serve a special user that should be protected by passive eavesdropping. The novelty of the presented approach lies in the fact that each channel is forced to be spatially shared by the special user and another one without any secrecy constraint. This coexistence is beneficial for both of them. The secure user is protected from the eavesdropper, since the transmitted power which allocated to the other user causes jamming interference to the eavesdropper, while the selected user has the opportunity to occupy some system's resources for its own transmission. The aim is to maximize its throughput under a secrecy rate constraint for the special user. Specifically, the contribution in this chapter is as follows

- For the first considered problem, two heuristics of low-complexity are proposed in which the subproblems of user selection and power allocation have been decoupled;

in the first heuristic, user selection is performed in the null space of the eavesdropper's channel by using the metric of spatial correlation to group users. The power allocation subproblem is solved by an iterative procedure which is developed based on KKT conditions. In the second heuristic, the eavesdropper is treated as an authorized user of the system and it is placed in the transmission group. Moreover, the power allocation is performed by a classical waterfilling policy in which the allocated power to the eavesdropper is forced to be zero.

- For the second considered problem, three solutions are presented; the first is based on working on the Lagrangian dual space, in which the problem can be decomposed per subchannel into a number of non-linear subproblems. By using some non-trivial transformations, each such subproblem is solved in an optimal way with linear computational complexity. The other two solutions are based on decoupling of the subchannel and the power allocation subproblems.

The organization of the rest of the chapter is as follows. In Section 4.2, we investigate the problem of user selection and power allocation in multiuser flat fading MISO downlink to maximize sum secrecy rate. In Section 4.3, we study the problem of maximizing the throughput in a multiuser, multiantenna downlink system in which a set of parallel channels has been devoted to provide secrecy to a special user.

## 4.2 User selection to maximize secrecy throughput under passive eavesdropping

In this section we aim to maximize the secrecy throughput of a multiuser, multiantenna system under in the presence of a passive eavesdropper. Let $\mathscr{U}$ denotes the set of the users in the system and $\mathscr{K} \subseteq \mathscr{U}$ the set of the users which are spatially multiplexed. It is assumed that the eavesdropper potentially wiretaps all of them *i.e* a worst-case wiretapping scenario is assumed. The problem to be solved is the following

$$\begin{aligned} \max_{\mathscr{K}\subseteq\mathscr{U},p_k} \quad & \sum_{k\in\mathscr{K}} [R_k(\mathscr{K}) - R_{ek}(\mathscr{K})]^+ \\ s.t. \quad & Tr(\mathbb{E}\left\{\mathbf{x}\mathbf{x}^H\right\}) \leq P_T, \\ & |\mathscr{K}| \leq T_x, \end{aligned} \tag{4.1}$$

where $\mathbf{x}$ is the transmitted signal vector to the users in $\mathscr{K}$, $R_k(\mathscr{K})$ is the transmission rate of user $k \in \mathscr{K}$ and $R_{ek}(\mathscr{K})$ is the rate of the eavesdropper when it wiretaps the message of user $k \in \mathscr{K}$. In the following, it is assumed that either ZFB or THP/ZF is used to spatially multiplex the users in $\mathscr{K}$. Thus, the transmitted signal $\mathbf{x}$ is given by (1.6) and (1.9), respectively. Let $\Gamma_k(\mathscr{K})$ denotes the SINR of the user $k \in \mathscr{K}$. This SINR is given as

$$\Gamma_k(\mathscr{K}) = \frac{p_k}{\sigma^2}, \qquad \text{in ZFB}, \tag{4.2a}$$

$$\Gamma_k(\mathscr{K}) = \frac{r_k^2 p_k}{\sigma^2}, \qquad \text{in THP/ZF}, \tag{4.2b}$$

where $p_k$ is the power loading for $k \in \mathscr{K}$ and $r_k^2, k \in \mathscr{K}$ denotes the scaling random variable used in THP/ZF reception[1]. Let $\Gamma_{ek}(\mathscr{K})$ denotes the SINR of the eavesdropper when it wiretaps the message of the user $k \in \mathscr{K}$. This SINR is given as

$$\Gamma_{ek}(\mathscr{K}) = \frac{p_k |\mathbf{h}_e^T \mathbf{w}_k|^2}{\sigma^2 + \sum_{j\in\mathscr{K}, j\neq k} p_j |\mathbf{h}_e^T \mathbf{w}_j|^2} \qquad \text{in ZFB}, \tag{4.3a}$$

$$\Gamma_{ek}(\mathscr{K}) = \frac{p_k |\mathbf{h}_e^T \left(\mathbf{F}\mathbf{B}^{-1}\right)_k|^2}{\sigma^2 + \sum_{j\in\mathscr{K}, j\neq k} p_j |\mathbf{h}_e^T \left(\mathbf{F}\mathbf{B}^{-1}\right)_j|^2}, \qquad \text{in THP/ZF}, \tag{4.3b}$$

where $\left(\mathbf{F}\mathbf{B}^{-1}\right)_k$ is the $k$-th column of the precoding matrix $\mathbf{F}\mathbf{B}^{-1}$ (see Section 1.1.2). Using (4.2) and (4.3), the problem (4.1) can be written as

[1] It is also assumed that the natural order $1 \ldots, |\mathscr{K}|$ is used in THP/ZF encoding process

$$\begin{aligned}\max_{\mathscr{K}\subseteq\mathscr{U},p_k} \quad & \sum_{k\in\mathscr{K}} \left[\log_2\left(1+\Gamma_k\left(\mathscr{K}\right)\right)-\log_2\left(1+\Gamma_{ek}\left(\mathscr{K}\right)\right)\right]^+ \\ s.t. \quad & \sum_{k\in\mathscr{K}} \frac{p_k}{c_k\left(\mathscr{K}\right)} \leq P_T, \\ & \left|\mathscr{K}\right| \leq T_x, \\ & p_k \geq 0,\end{aligned} \tag{4.4}$$

where $c_k\left(\mathscr{K}\right)$ is the effective channel of the user $k\in\mathscr{K}$. In ZFB, $c_k\left(\mathscr{K}\right)$ is given by the inverse of the diagonal element of the matrix $\left(\mathbf{H}_{\mathscr{K}}\mathbf{H}_{\mathscr{K}}^H\right)^{-1}$ which corresponds to the user $k$. In THP/ZF, it holds $c_k\left(\mathscr{K}\right)=1$, $k\in\mathscr{K}$.

### 4.2.1 Power allocation for fixed transmission group of users

Let assume a fixed transmission group $\mathscr{K}$. If the operator $[.]^+$ is omitted, the following power allocation problem results

$$\begin{aligned}\max_{p_k} \quad & \sum_{k\in\mathscr{K}} \log_2\left(1+\Gamma_k\left(\mathscr{K}\right)\right)-\log_2\left(1+\Gamma_{ek}\left(\mathscr{K}\right)\right) \\ s.t. \quad & \sum_{k\in\mathscr{K}} \frac{p_k}{c_k\left(\mathscr{K}\right)} \leq P_T, \\ & p_k \geq 0,\end{aligned} \tag{4.5}$$

The problem (4.5) is non-convex with respect to the power variables since each term in the summation of the objective function is the difference of two concave functions. Nevertheless, the following Lemma can be stated

***Lemma 4.1***: The Karush-Kuhn-Tucker (KKT) conditions in (4.5) imply that (a possible local) optimal power loading can be derived by solving a system of $|\mathscr{K}|$ polynomial equations in which each equation has up to $(|\mathscr{K}|+1)$ order.

*Proof.* Let $a_k=\left|\mathbf{h}_e^T\mathbf{w}_k\right|^2$ and $\widetilde{\sigma}_k^2=\sigma^2$ in the case of ZFB, while $a_k=\left|\mathbf{h}_e^T\left(\mathbf{F}\mathbf{B}^{-1}\right)_k\right|^2$ and $\widetilde{\sigma}_k^2=\sigma^2/r_k^2$, $k\in\mathscr{K}$, in the case of THP/ZF. The Lagrangian of (4.5) is given by

$$\begin{aligned}L(p_k,\mu)=&\sum_{k\in\mathscr{K}}\left[\log_2\left(1+p_k/\widetilde{\sigma}_k^2\right)-\log_2\left(1+\frac{a_kp_k}{\sigma^2+\sum_{j\in\mathscr{K},j\neq k}a_jp_j}\right)\right] \\ &-\mu\left(\sum_{k\in\mathscr{K}}\frac{p_k}{c_k\left(\mathscr{K}\right)}-P_T\right)\end{aligned} \tag{4.6}$$

$$= \sum_{k\in\mathscr{K}} \left[ \log\left(1+p_k/\widetilde{\sigma}_k^2\right) - \log_2\left(\sigma^2 + \sum_{j\in\mathscr{K}} a_j p_j\right) + \log_2\left(\sigma^2 + \sum_{j\in\mathscr{K}, j\neq k} a_j p_j\right)\right]$$
$$- \mu\left(\sum_{k\in\mathscr{K}} \frac{p_k}{c_k(\mathscr{K})} - P_T\right).$$

where $\mu \geq 0$ is the Lagrange multiplier of the power constraint and $c_k = c_k(\mathscr{K})$. The partial derivative of (4.6) with respect to $p_k, k \in \mathscr{K}$ is given as

$$\begin{aligned}\frac{\partial L}{\partial p_k} &= \left(\frac{1}{\widetilde{\sigma}_k^2 + p_k} - \frac{a_k}{\sigma^2 + \sum_{j\in\mathscr{K}} a_j p_j}\right)\frac{1}{\ln 2} \\ &+ \frac{1}{\ln 2}\sum_{i\in\mathscr{K}, i\neq k,}\left[-\frac{a_k}{\sigma^2+\sum_{j\in\mathscr{K}} a_j p_j} + \frac{a_k}{\sigma^2+\sum_{j\in\mathscr{K}, j\neq i} a_j p_j}\right] - \frac{\mu}{c_k} \\ &= \frac{1}{\ln 2}\left(\frac{1}{\widetilde{\sigma}_k^2 + p_k} - \frac{a_k}{\sigma^2 + \sum_{j\in\mathscr{K}} a_j p_j}\right) - \frac{\mu}{c_k} \\ &+ \frac{a_k}{\ln 2}\sum_{i\in\mathscr{K}, i\neq k}\left[-\frac{1}{\sigma^2+\sum_{j\in\mathscr{K}, j\neq k} a_j p_j + a_k p_k} + \frac{1}{\sigma^2+\sum_{j\in\mathscr{K}, j\neq k} a_j p_j - a_i p_i + a_k p_k}\right].\end{aligned} \tag{4.7}$$

Let $\beta_k = \left(\sigma^2 + \sum_{j\in\mathscr{K}, j\neq k} a_j p_j\right), k \in \mathscr{K}$. From (4.7), the $\partial L/\partial p_k$ is written as

$$\begin{aligned}\frac{\partial L}{\partial p_k} =& \frac{1}{\ln 2}\left(\frac{1}{\widetilde{\sigma}_k^2 + p_k} - \frac{a_k}{\beta_k + a_k p_k}\right) - \frac{\mu}{c_k} + \\ &+ \frac{a_k}{\ln 2}\sum_{i\in\mathscr{K}, i\neq k}\left[\frac{1}{\beta_k - a_i p_i + a_k p_k} - \frac{1}{\beta_k + a_k p_k}\right].\end{aligned} \tag{4.8}$$

Note that each term in the summation of the right hand of (4.8) is nonnegative, since $a_i p_i > 0, i \in \mathscr{K}$. Thus, $\frac{\partial L}{\partial p_k}$ can be written as the ratio of two polynomials of $p_k$, with a strictly positive polynomial in the denominator. Let $p_k^*, k \in \mathscr{K}$ denotes a (possibly local) optimal solution in (4.5). Given that KKT conditions imply that $\partial L/\partial p_k^* = 0, k \in \mathscr{K}$, a system of $|\mathscr{K}|$ polynomial equations results by setting the numerator of each such ratio equal to zero. Clearly, each one of these $|\mathscr{K}|$ polynomials has order up to $(|\mathscr{K}|+1)$ and it depends on all the power loading variables $p_k^*, k \in \mathscr{K}$. □

In Algorithm 10, an iterative procedure is presented to solve the system of power equations in *Lemma 4.1*, called Iterative Power Allocation Algorithm (IPAA). In IPAA, a bisection method is used to update the Lagrange multiplier of the total power constraint $(\mu)$ to satisfy the overall power bound. In each iteration step (fixed value of $\mu$), the $\frac{\partial L}{\partial p_k}, k \in \mathscr{K}$, in (4.8) is set equal to zero and the roots of the resulting polynomial are calculated. This calculation is performed in parallel over all the users in $\mathscr{K}$ by employing an iterative man-

**Algorithm 10:** Iterative power allocation algorithm (IPAA)

Input: $\alpha_k, k \in \mathscr{K}$, and small positive value $\varepsilon$.
Let $p_k^0, k \in \mathscr{K}$, be an initial power allocation. Set $\mu > 0$ and $\mu_l = 0$.
**repeat**
  Set $i = 0$.
  **repeat**
    Set $i = i+1$.
    **for** $k \in \mathscr{K}$ **do**
      Calculate the roots by setting $\partial L / \partial p_k = 0$ in (4.8) and by using the values $p_j^i = p_j^{(i-1)}, j \in \mathscr{K}, j \neq k$. Set $p_k^i$ equal to the minimum positive root.
    **end for**
  **until** $\max_{k \in \mathscr{K}} \left| p_k^i - p_k^{i-1} \right| \leq \varepsilon$
  Calculate the overall transmit power consumption as $P_{cons} = \sum_{k \in \mathscr{K}} \frac{p_k^i}{c_k(\mathscr{K})}$.
  **if** $P_{cons} < P_T$ **then**
    $\mu_l = \mu$ and $\mu = 2\mu$.
    Set $p_k^* = p_k^i, k \in \mathscr{K}$.
  **else**
    $\mu = (\mu + \mu_l)/2$.
  **end if**
**until** $|P_{cons} - P_T| \leq \varepsilon$
**return** $p_k^*, k \in \mathscr{K}$.

ner; for the $k^{th}$ polynomial, the values $p_j$, $j \in \mathscr{K}, j \neq k$ of the previous iteration are used to update the value of $p_k$ in the current iteration. For polynomial-order less than five, there are closed form solutions which produce all the roots of the polynomial [105]. In the case of polynomials with higher order, roots could be obtained by using any Newton's based numerical method [106]. The computational complexity of the Algorithm 10 can not be accurately specified. It is mainly dependent on the initial starting point guess for variable $\mu$, the number of update iterations while solving the set of $|\mathscr{K}|$ polynomial equations (for each specific value of $\mu$) and the complexity of the used root-finding algorithm. Nevertheless, the overall complexity is linear with respect to the $|\mathscr{K}|$, since the roots of $|\mathscr{K}|$ uni-variate polynomials need to be found in each iteration of the bisection method.

Let $p_k^a, k \in \mathscr{K}$, denotes a solution of the $|\mathscr{K}|$ polynomial equations derived by Algorithm 10. In the case where one ore more values of $p_k^a$ are negative, the secrecy rate of the corresponding users will be zero because of the $[.]^+$ operator. Nevertheless, their channels affect the secrecy rate of all the users in $\mathscr{K}$ because of the beamforming matrix which depends on the channels of all the users in $\mathscr{K}$. One way to have a feasible solution for the problem (4.5) based on $p_k^a, k \in \mathscr{K}$, is to set the negative values of power equal to zero and resolve a set of fewer equations. By repeating this policy if necessary, it is always guaranteed that a feasible solution in (4.5) can be obtained.

### 4.2.2 Low complexity resource allocation schemes

The throughput of the system increases as the users within the set $\mathscr{K}$ have high channel gain and they are as much as possible orthogonal to each other and the channel of the eavesdropper. Based on this remark, two user selection algorithms are presented in the following paragraphs which aim to group users with as much as possible jointly orthogonal to each other and to the eavesdropper.

#### User selection within the nullspace of eavesdropper's channel

In this scheme, the channels of all the legitimate users are projected onto the null space of the eavesdropper's channel and the process of user selection is performed by CUSA (Section 2.2) by using the projected channels. The details of the algorithm, called Secrecy Correlation-based User Selection Algorithm (S/CUSA), are described in Algorithm 11. Note that power allocation is performed by IPAA in line 10 of S/CUSA, where the transmission group is considered for a possible update. If $\mathscr{C}_{IPAA}$ denotes the computational complexity of the IPAA, the complexity of S/CUSA is $\mathscr{O}\left(UT_x^3 + (UT_x + L\mathscr{C}_{IPAA})\,T_x\right)$, where the first term is due to the channel projection process and the second term due to the selection process.

#### The eavesdropper within the transmission group

In this selection scheme, the eavesdropper is forced to be within the transmission group $\mathscr{K}$, as it was a regular (authorized) user of the system. Nevertheless, the power that is allocated to it is set equal to zero. This way the eavesdropper cannot decode the symbol of any of the users in $\mathscr{K}$ since the transmission to the users in $\mathscr{K}$ is orthogonal in space. Moreover, $R_{ek} = 0$ irrespectively of the user which is wiretapped by the eavesdropper. Apart from the eavesdropper, the rest users in $\mathscr{K}$ are specified by CUSA (Section 2.2). Given the set $\mathscr{K}$, power waterfilling is used to allocate the available power over the (up to $T_x - 1$) selected users. The overall selection algorithm is called CUSA with Eave. It should be noted that in the case where THP/ZF is used, the eavesdropper is forced to be the last encoded member of $\mathscr{K}$, since user encoding order affects both the overall secrecy throughput and the individual secrecy rates. The computational complexity of the whole process is equal to the complexity of the CUSA, *i.e.* $\mathscr{O}\left(\left(UT_x + cT_x^2\right)T_x\right)$, where $c$ is a constant.

#### Numerical results

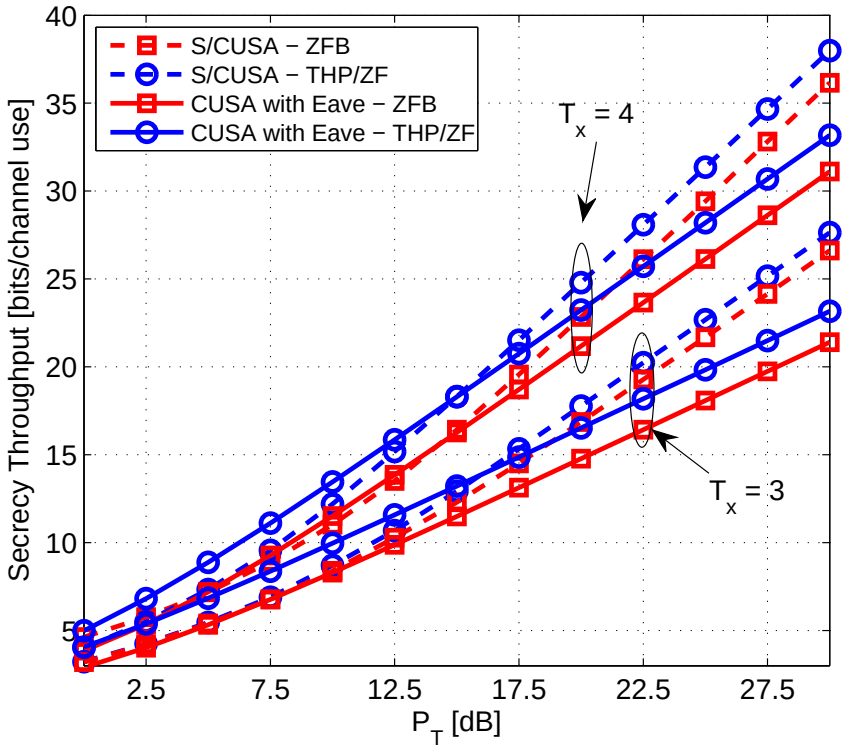
The performance of the two proposed user selection algorithms is evaluated in Figs. 4.1a, 4.1b for Rayleigh-distributed wireless channels of legitimate users and the eavesdropper. In Fig. 4.1a, the secrecy throughput versus the overall power $P_T$ is shown when $U = 50$ users and $T_x = 3,4$ antennas. As can be seen, THP/ZF outperforms ZF for both the proposed

**Algorithm 11:** Secrecy correlation-based user selection algorithm (S/CUSA)

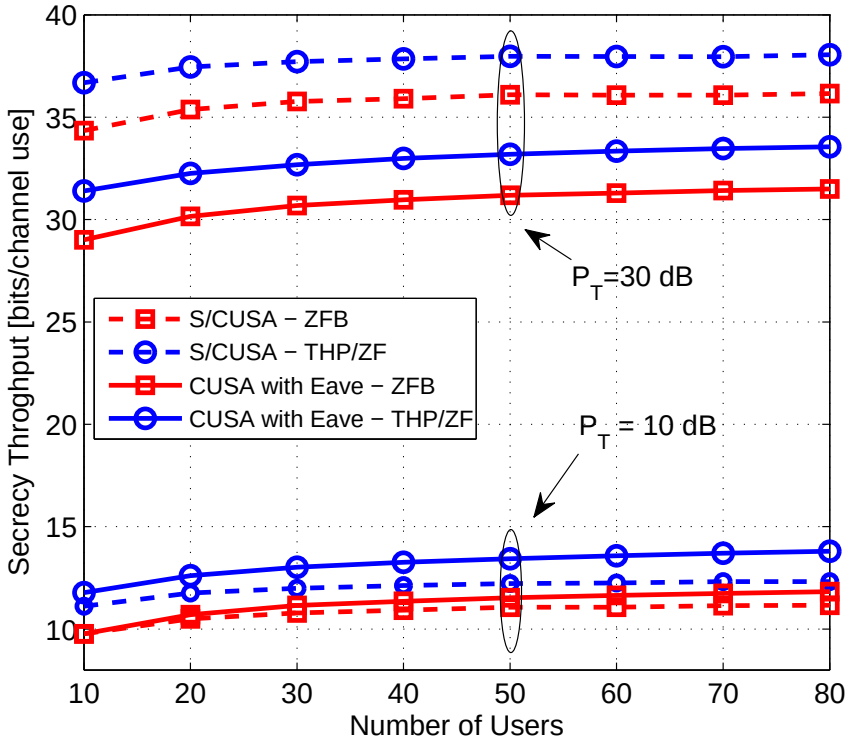
Input: channels $\mathbf{h}_u, u \in \mathscr{U}$, and parameter $L$.
Set $\mathscr{K} = \emptyset$, $\mathscr{A} = \emptyset$ and $m = 1$.
Let $\mathscr{N}(\mathbf{h}_e)$ denotes the null space of the eavesdropper's channel and $\widetilde{\mathbf{h}}_k, k \in \mathscr{K}$, be the projection of the user's $k$ channel onto the $\mathscr{N}(\mathbf{h}_e)$.
Specify user $k^* = \arg\max_{k \in \mathscr{U}: R_k(k) > R_{ek}(k)} \left\| \widetilde{\mathbf{h}}_k \right\|$.
Set $\mathscr{K} = \{k^*\}$.
**while** $m < T_x$ **do**
    $m = m + 1$
    Let $Cor_i = \sum_{k \in \mathscr{K}} \rho_{k,i} \left( \widetilde{\mathbf{h}}_k, \widetilde{\mathbf{h}}_i \right)$, $i \in \mathscr{U} \setminus \mathscr{K}$.
    Let $\mathscr{A}$ denotes the users in $\mathscr{U} \setminus \mathscr{K}$ which have the $L$ lowest values $Cor_i$.
    Specify user $a^* = \arg\max_{a \in \mathscr{A}} \sum_{k \in \{\mathscr{K} \cup a\}} \left[ R_k(\mathscr{K} \cup a) - R_{ek}(\mathscr{K} \cup a) \right]^+$ by using Algorithm 10 to calculate power loading for each one candidate set $\{\mathscr{K} \cup a\}$.
    **if** $\sum_{k \in \{\mathscr{K} \cup a^*\}} \left[ R_k(\mathscr{K} \cup a^*) - R_{ek}(\mathscr{K} \cup a^*) \right]^+ > \sum_{k \in \mathscr{K}} \left[ R_k(\mathscr{K}) - R_{ek}(\mathscr{K}) \right]^+$ **then**
        set $\mathscr{K} = \{\mathscr{K} \cup a^*\}$.
    **else**
        $m = T_x$.
    **end if**
**end while**
**return** Set $\mathscr{K}$

schemes, especially as the number of transmitting antennas and the $P_T$ increase. Comparing the performance between the two selection schemes, it can be seen that CUSA with Eave outperforms S/CUSA as $P_T$ decreases for both ZF and THP/ZF. This is justified since fewer users are multiplexed, as $P_T$ decreases. Hence, it is more efficient to use (some of) the available degrees of freedom to completely eliminate eavesdropping rather than to improve the array gain. On the other hand, as $P_T$ increases S/CUSA outperforms CUSA with Eave since spatial multiplexing becomes the critical factor in terms of secrecy throughput and user selection should be able to accommodate as many as possible users.

In Fig. 4.1b, the secrecy throughput versus the number of users is shown for $P_T = 10$ dB and $P_T = 30$ dB. All the transmission techniques exploit multiuser diversity as the number of users increases. As before, S/CUSA is superior at high SNRs, while CUSA with Eave dominates in low SNR regime.




(a) Secrecy throughput vs $P_T$ for $U = 50$.




(b) Secrecy throughput vs number of users for $T_x = 4$.

Fig. 4.1 Secrecy throughput of S/CUSA and CUSA with eavesdropper selected.

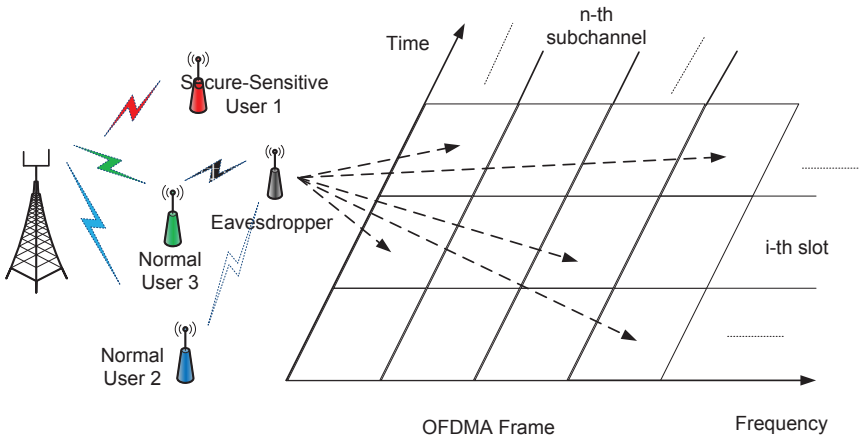



Fig. 4.2 System setup; spatial multiplexing between a normal and a secure sensitive user.

## 4.3 Simultaneous secrecy and throughput maximization using SDMA

Consider the transmission scenario depicted in Fig. 4.2. The scenario consists of a single BS, a set of users $\mathscr{U}$ (called normal users), a secure user (denoted as $b$) and a passive eavesdropper. The BS is equipped with two transmit antennas, whereas all the users (including the user $b$) and the eavesdropper have a single receive antenna. It is assumed that the BS has assigned the set of subchannels $\mathscr{N} = \{1,\ldots,N\}$ to serve the user $b$ in a secured transmission way. Nevertheless, each one of these subchannels is also assigned to one of the users in $\mathscr{U}$ and ZFB is employed between the $b$ and the selected user.

Let $k_n^* \in \mathscr{U}$ denotes the user that has been selected for transmission within the subchannel $n \in \mathscr{N}$. The transmitted signal vector within the subchannel $n$ is written as $\mathbf{x}_n = \mathbf{W}_n\mathbf{D}_n\mathbf{s}_n$, where $\mathbf{s}_n \in \mathbb{R}^2$ contains the (unit energy) information symbols destined to $\{b \cup k_n^*\}$, $\mathbf{D}_n \in \mathbb{R}^{2\times 2}$ is a diagonal power loading matrix with the vector $\left[\sqrt{p_{n,b}}, \sqrt{p_{n,k_n^*}}\right]$ in the main diagonal and $\mathbf{W}_n = [\mathbf{w}_{n,b}, \mathbf{w}_{n,k_n^*}] = \mathbf{H}_{n,\{b\cup k_n^*\}}^H \left(\mathbf{H}_{n,\{b\cup k_n^*\}}\mathbf{H}_{n,\{b\cup k_n^*\}}^H\right)^{-1} \in \mathbb{C}^{2\times 2}$ is the beamforming matrix. The rows of $\mathbf{H}_{n,\{b\cup k_n^*\}} = [\mathbf{h}_{n,b}^T, \mathbf{h}_{n,k_n^*}^T]^T \in \mathbb{C}^{2\times 2}$ correspond to the channels of $\{b \cup k_n^*\}$. The received signal of $k_n^*$ and $b$ within the subchannel $n$ are given as

$$y_{n,b} = \mathbf{h}_{n,b}^T \mathbf{w}_{n,b}\sqrt{p_{n,b}}s_{n,b} + z_{n,b}, \qquad n \in \mathscr{N} \tag{4.9a}$$

$$y_{n,k_n^*} = \mathbf{h}_{n,k_n^*}^T \mathbf{w}_{n,k_n^*}\sqrt{p_{n,k_n^*}}s_{n,k_n^*} + z_{n,k_n^*}, \qquad n \in \mathscr{N}, \tag{4.9b}$$

where $z_{n,k_n^*}$ and $z_{n,b}$ denote the independent and identically distributed samples of complex Gaussian additive white noise with variance $\sigma^2_{z_{n,k_n^*}} = \sigma^2_{z_{n,b}} = \sigma^2$. In what follows it is as-

sumed that $\sigma^2 = 1$. The secrecy rate of $b$ and the transmission rate of user $k_n^*$ are given as

$$R_{n,k_n^*}^{sr-b} = \left[\log\left(1+p_{n,b}\right) - \log\left(1+\Gamma_{n,k_n^*,e}\right)\right]^+, \qquad n \in \mathscr{N}, \tag{4.10a}$$

$$R_{n,k_n^*} = \log\left(1+p_{n,k_n^*}\right), \qquad n \in \mathscr{N}, \tag{4.10b}$$

where $\Gamma_{n,k_n^*,e} = \frac{p_{n,b}|\mathbf{h}_{n,e}^T \mathbf{w}_{n,b}|^2}{1+p_{n,k_n^*}|\mathbf{h}_{n,e}^T \mathbf{w}_{n,k_n^*}|^2}$ is the SINR for the link between the BS and the eavesdropper. The problem to be solved aims to maximize the throughput of the users in $\mathscr{U}$ under a secrecy rate constraint for $b$ and an average power constraint per subchannel. Specifically,

$$\max_{w_{n,k}p_{n,k},p_{n,b}} \quad \sum_{n\in\mathscr{N}}\sum_{k\in\mathscr{K}} w_{n,k}\log\left(1+p_{n,k}\right) \tag{4.11a}$$

$$\sum_{n\in\mathscr{N}}\sum_{k\in\mathscr{K}} w_{n,k}R_{n,k}^{sr-b} \geq \overline{R}, \tag{4.11b}$$

$$\sum_{k\in\mathscr{K}} w_{n,k}\left(p_{n,k}/c_{n,k} + p_{n,b}/c_{n,b}\right) \leq P_N, \qquad n \in \mathscr{N}, \tag{4.11c}$$

$$\sum_{k\in\mathscr{K}} w_{n,k} = 1, \qquad n \in \mathscr{N}, \tag{4.11d}$$

$$w_{n,k} \in \{0,1\}, \qquad k \in \mathscr{U},\ n \in \mathscr{N}, \tag{4.11e}$$

$$p_{n,b},\ p_{n,k} \geq 0, \qquad k \in \mathscr{U}, n \in \mathscr{N}, \tag{4.11f}$$

where the binary variables $w_{n,k}, n \in \mathscr{N}, k \in \mathscr{K}$ denote the normal user that has been selected for subchannel $n$, *i.e.* $w_{n,k} = 1$ when the user $k$ has been selected for subchannel $n$, otherwise $w_{n,k} = 0$, $\overline{R}$ is the required secrecy rate of the user $b$, $c_{n,k}$ and $c_{n,b}$ are the effective channels of the user $k$ and the user $b$ in subchannel $n$, respectively, and $P_N$ is the available transmit power per subchannel. The problem in (4.11) is a MINLP. In the following subsections, three resource allocation schemes are discussed. The first is based on optimization in the dual space while the rest two are based on decoupling the subchannel assignment and the power allocation subproblems.

### 4.3.1 A resource allocation scheme based on dual optimization

The partial Lagrangian dual optimization of (4.11) is as follows [106]

$$\max_{w_{n,k}p_{n,k},p_{n,b}} \sum_{n\in\mathscr{N}} \left[\sum_{k\in\mathscr{K}} w_{n,k}\left(\log\left(1+p_{n,k}\right) + \lambda R_{n,k}^{sr-b}\right)\right] \tag{4.12a}$$

$$\sum_{k\in\mathscr{U}} w_{n,k}\left(p_{n,k}c_{n,k}^{-1}+p_{n,b}c_{n,b}^{-1}\right)\leq P_N, \qquad n\in\mathscr{N}, \tag{4.12b}$$

$$\sum_{k\in\mathscr{U}} w_{n,k}=1, \qquad n\in\mathscr{N}, \tag{4.12c}$$

$$w_{n,k}\in\{0,1\}, \qquad k\in\mathscr{U},\ n\in\mathscr{N}, \tag{4.12d}$$

$$p_{n,b},\ p_{n,k}\geq 0, \qquad k\in\mathscr{U},n\in\mathscr{N}, \tag{4.12e}$$

where $\lambda\geq 0$ is the Lagrange multiplier of constraint (4.11b) and $\lambda\overline{R}$ has been eliminated from objective (4.12a) since it is a constant term. By inspecting (4.12), it is clear that the overall optimization problem can be decomposed into $N$ independent subproblems, one per subchannel. The subproblem for subchannel $n\in\mathscr{N}$ can be written as

$$\max_{w_{n,k}p_{n,k},p_{n,b}} \quad \sum_{k} w_{n,k}\left(\log\left(1+p_{n,k}\right)+\lambda R_{n,k}^{sr-b}\right) \tag{4.13a}$$

$$\sum_{k\in\mathscr{K}} w_{n,k}\left(p_{n,k}c_{n,k}^{-1}+p_{n,b}c_{n,b}^{-1}\right)\leq P_N, \tag{4.13b}$$

$$\sum_{k\in\mathscr{K}} w_{n,k}=1, \tag{4.13c}$$

$$w_{n,k}\in\{0,1\}, \qquad k\in\mathscr{U}, \tag{4.13d}$$

$$p_{n,b},\ p_{n,k},\geq 0 \qquad k\in\mathscr{U}. \tag{4.13e}$$

The problem (4.13) is still a combinatorial one since the optimization is performed over the binary variables $w_{n,k},k\in\mathscr{U},n\in\mathscr{N}$. Given the exclusive condition over $w_{n,k}$ (only one of them may be equal to 1), a way to solve (4.13) is to solve its $U$ different instances, where a different $w_{n,k}$ is set equal to 1, and select the solution that maximizes the objective function. Consider such an instance in which $w_{n,\kappa}=1$ and $w_{n,j}=0, j,\kappa\in\mathscr{U},j\neq\kappa$. The following optimization problem can be stated

$$\max_{p_{n,\kappa},p_{n,b}} \quad \log\left(1+p_{n,\kappa}\right)+\lambda\left(\log\left(1+p_{n,b}\right)-\mu\right) \tag{4.14a}$$

$$p_{n,\kappa}c_{n,\kappa}^{-1}+p_{n,b}c_{n,b}^{-1}\leq P_N, \tag{4.14b}$$

$$\log\left(1+\frac{\alpha_{n,b}p_{n,b}}{1+\alpha_{n,\kappa}p_{n,\kappa}}\right)=\mu, \tag{4.14c}$$

$$p_{n,\kappa}\geq 0,\ p_{n,b}>0, \tag{4.14d}$$

where $\alpha_{n,b}=|\mathbf{h}_{n,e}^T\mathbf{w}_{n,b}|^2$ and $\alpha_{n,\kappa}=|\mathbf{h}_{n,e}^T\mathbf{w}_{n,\kappa}|^2$. For constant $\mu$, constraint (4.14c) takes the following linear form

$$\alpha_{n,b}p_{n,b}-\left(2^{\mu}-1\right)\alpha_{n,\kappa}p_{n,\kappa}=\left(2^{\mu}-1\right),$$

which is linear with respect to $p_{n,b}$ and $p_{n,\kappa}$. Under this assumption, the problem (4.14) is convex for a given $\mu$; the objective function is concave and all the constraints are linear equations of $p_{n,b}$ and $p_{n,\kappa}$. Thus, the following lemma is stated

***Lemma 4.2***: For a given $\mu$, the Karush-Kuhn-Tucker (KKT) conditions of (4.14) imply that the optimal power allocation $\left(p_{n,b}^{o}, p_{n,\kappa}^{o}\right)$ is given by

$$p_{n,b}^{o} = \frac{P_N + c_{n,\kappa}^{-1}/\alpha_{n,\kappa}}{c_{n,b}^{-1} + \gamma_{n,\kappa} c_{n,\kappa}^{-1}} \quad \text{and} \quad p_{n,\kappa}^{o} = \gamma_{n,\kappa} p_{n,b}^{o} - \frac{1}{\alpha_{n,\kappa}}, \tag{4.15}$$

where $\gamma_{n,\kappa} \triangleq \frac{\alpha_{n,b}}{(2^{\mu}-1)\alpha_{n,\kappa}}$.

*Proof.* Let $\gamma_{n,\kappa} = \frac{\alpha_{n,b}}{(2^{\mu}-1)\alpha_{n,\kappa}}$. By combining (4.14b) and (4.14c), the following inequalities hold

$$p_{n,\kappa} = \gamma_{n,\kappa} p_{n,b} - \frac{1}{\alpha_{n,\kappa}} \geq 0 \quad \text{and} \quad 0 \leq p_{n,b} \leq \frac{P_N + c_{n,\kappa}^{-1}/\alpha_{n,\kappa}}{c_{n,b}^{-1} + \gamma_{n,\kappa} c_{n,\kappa}^{-1}}. \tag{4.16}$$

By using (4.16), the problem of eq. (4.14) is written as

$$\max_{p_{n,b}} \ \log\left(1 + \gamma_{n,\kappa} p_{n,b} - \frac{1}{\alpha_{n,\kappa}}\right) + \lambda \log\left(1 + p_{n,b}\right), \tag{4.17a}$$

$$p_{n,b}^{lb} \leq p_{n,b} \leq p_{n,b}^{ub}, \tag{4.17b}$$

where the term $-\lambda\mu$ has been eliminated from the objective and $p_{n,b}^{lb}, p_{n,b}^{ub}$ are given by

$$p_{n,b}^{lb} = \frac{1}{\gamma_{n,\kappa}\alpha_{n,\kappa}} \ \text{ and } \ p_{n,b}^{ub} = \frac{P_N + c_{n,\kappa}^{-1}/\alpha_{n,\kappa}}{c_{n,b}^{-1} + \gamma_{n,\kappa} c_{n,\kappa}^{-1}}. \tag{4.18}$$

Note that maximization in (4.17) is performed only over $p_{n,b}$. The Lagrangian of (4.17) is given as

$$\begin{aligned} \mathscr{L}\left(\nu_1, \nu_2, p_{n,b}\right) = & \log_2\left(1 + \gamma_{n,\kappa} p_{n,b} - \frac{1}{\alpha_{n,\kappa}}\right) + \lambda \log_2\left(1 + p_{n,b}\right) \\ & - \nu_1\left(p_{n,b} - p_{n,b}^{lb}\right) + \nu_2\left(p_{n,b} - p_{n,b}^{ub}\right), \end{aligned} \tag{4.19}$$

where $\nu_1, \nu_2 \geq 0$ are the Lagrange multipliers of the two inequalities of (4.17b). Let $p_{n,b}^o$ be the optimal solution of (4.17) and $\nu_1^o, \nu_2^o$ be the optimal points of its dual problem. The KKT conditions imply the following equations

$$\ln 2\,(\nu_2^o - \nu_1^o) = \frac{\gamma_n}{1+\gamma_{n,\kappa} p_{n,b}^o - 1/\alpha_{n,\kappa}} + \frac{\lambda}{1+p_{n,b}^o} \tag{4.20a}$$

$$p_{n,b}^{lb} \leq p_{n,b}^o \leq p_{n,b}^{ub}, \tag{4.20b}$$

$$-\nu_1^o \left(p_{n,b}^o - p_{n,b}^{lb}\right) \leq 0, \tag{4.20c}$$

$$\nu_2^o \left(p_{n,b}^o - p_{n,b}^{ub}\right) \leq 0, \tag{4.20d}$$

$$\nu_1^o, \nu_2^o \geq 0. \tag{4.20e}$$

From (4.20c), (4.20d) it is clear that at most one of $\nu_1, \nu_2$ may be nonzero, since $p_{n,b}^{lb} \neq p_{n,b}^{ub}$ in a non-trivial case. Hence, the following cases should be considered:

1. If $\nu_1^o = \nu_2^o = 0$, then (4.20a) can be valid only in the trivial case where $\mu = 0$.
2. If $\nu_1^o \neq 0$ and $\nu_2^o = 0$, then the left hand of (4.20a) is non-positive, while the right hand is non-negative. Thus this case is infeasible.
3. If $\nu_1^o = 0$ and $\nu_2^o \neq 0$, then $p_{n,b}^o = p_{n,b}^{ub}$ from (4.20d).

□

In (4.15), the optimal power allocation $\left(p_{n,b}^o, p_{n,k}^o\right)$ is given as a function of parameter $\mu$. Nevertheless, back substitution of these expressions into (4.14) yields an analytical solution for $\mu$; hence, despite the fact that (4.14) is non-convex, it can be solved analytically to find the optimal solution. Thus, the following Lemma can be stated:

***Lemma 4.3***: Let $\mu^o$ be the value of $\mu$ that maximizes problem (4.14). The range of $\mu$ is $\left[0, \log\left(1+\frac{P_N \alpha_{n,b}}{c_{n,b}^{-1}}\right)\right]$. Moreover, $\mu^o$ is either a real root of the third degree polynomial with coefficients given by (4.22) that lies in the specific range, or the boundary value that maximizes (4.14a).

*Proof.* Let us first establish the bounds of $\mu$. From (4.14c), it is clear that $\mu \geq 0$. An upper bound for $\mu$ is established by substituting $p_{n,b}^o$ into $p_{n,\kappa}^o$ in (4.15) and using the fact that $p_{n,\kappa}^o \geq 0$, *i.e.*

$$\mu \leq \log\left(1 + P_N \alpha_{n,b} c_{n,b}\right).$$

To obtain the optimal value of $\mu$ in the derived range, we follow the follow procedure; let $\beta = 1/\alpha_{n,\kappa}$, $\varepsilon = \frac{\alpha_{n,b}}{c_{n,\kappa}\alpha_{n,\kappa}}$ and $\delta = \beta c_{n,\kappa}^{-1} + P_N$. The $p_{n,b}^o, p_{n,\kappa}^o$ in (4.15) are written as

**Algorithm 12:** Subgradient optimization algorithm (SOA)

Set $\lambda^0 > 0$ and let $\varepsilon$ be a small non-negative value.
**repeat**
  $i = i+1$.
  **for** $n \in \mathscr{N}$ **do**
    **for** $k \in \mathscr{U}$ **do**
      Solve the problem in (4.14) for $w_{n,k} = 1$, $w_{n,j} = 0, j \neq k$ and using *Lemma 4.2* and *Lemma 4.3*. Let $f_k$ be the resulting value of the objective (4.14a).
    **end for**
    Set $w_{n,k^*} = 1$ and $w_{n,j} = 0, j \neq k^*, j, k^* \in \mathscr{U}$ where $k^* = \arg\max_{k\in\mathscr{U}} f_k$.
  **end for**
  Given the subchannel assignment (and the corresponding power allocation) across all the subchannels, update $\lambda$ as $\lambda^i = \left[\lambda^{i-1} - \delta\left(\sum_{n\in\mathscr{N}}\sum_{k\in\mathscr{U}} w_{n,k} R_{n,k}^{sr-b} - \overline{R}\right)\right]_+$.
**until** $\left|\lambda^i - \lambda^{i-1}\right| \leq \varepsilon$

$$p_{n,b}^o = \frac{x\delta}{xc_{n,b}^{-1}+\varepsilon}, \text{ and } p_{n,\kappa}^o = \frac{\alpha_{n,b}\beta\delta}{xc_{n,b}^{-1}+\varepsilon} - \beta,$$

where $x = \log(2^\mu - 1)$. Let $\zeta = xc_{n,b}^{-1} + \varepsilon$. Thus, the objective function (4.14a) becomes

$$f(\mu) = \log\left(1 + \frac{\alpha_{n,b}\beta\delta}{\zeta} - \beta\right) + \lambda\log\left(1 + \frac{(\zeta-\varepsilon)\delta c_{n,b}}{\zeta}\right) - \lambda\log\left(1 - c_{n,b}(\varepsilon-\zeta)\right).$$

The stationary points of $f(\mu)$ satisfy the following equation

$$\partial f/\partial\mu = -\frac{\zeta^{-1}\alpha_{n,b}\beta\delta}{(\alpha_{n,b}\beta\delta + (1-\beta)\zeta)}\frac{\zeta^{-1}\lambda\varepsilon\delta c_{n,b}}{(\zeta(1+\delta c_{n,b}) - \varepsilon\delta c_{n,b})} - \frac{\lambda}{c_{n,b}-\varepsilon+\zeta} = 0. \quad (4.21)$$

After some calculations in (4.21), $\partial f/\partial\mu$ is written as a polynomial of third degree $c_3\zeta^3 + c_2\zeta^2 + c_1\zeta^1 + c_0$, where the coefficients are given as

$$\begin{aligned}
c_3 &= \lambda(1-\beta)\left(1+\delta c_{n,b}^{-1}\right)\\
c_2 &= \alpha_{n,b}\beta\delta\left(1+\delta c_{n,b}^{-1}\right)(1+\lambda) - 2\lambda\varepsilon\delta c_{n,b}^{-1}(1-\beta)\\
c_1 &= \left(c_{n,b}^{-1}-\varepsilon\right)\left(\alpha_{n,b}\beta\delta\left(1+\delta c_{n,b}^{-1}\right) - \lambda\varepsilon\delta c_{n,b}^{-1}\right) - \alpha_{n,b}\beta\varepsilon\delta^2 c_{n,b}^{-1}(1+2\lambda)\\
c_0 &= \alpha_{n,b}\beta\varepsilon\delta^2\left(1-\varepsilon c_{n,b}^{-1}\right)(1+\lambda).
\end{aligned} \quad (4.22)$$

□

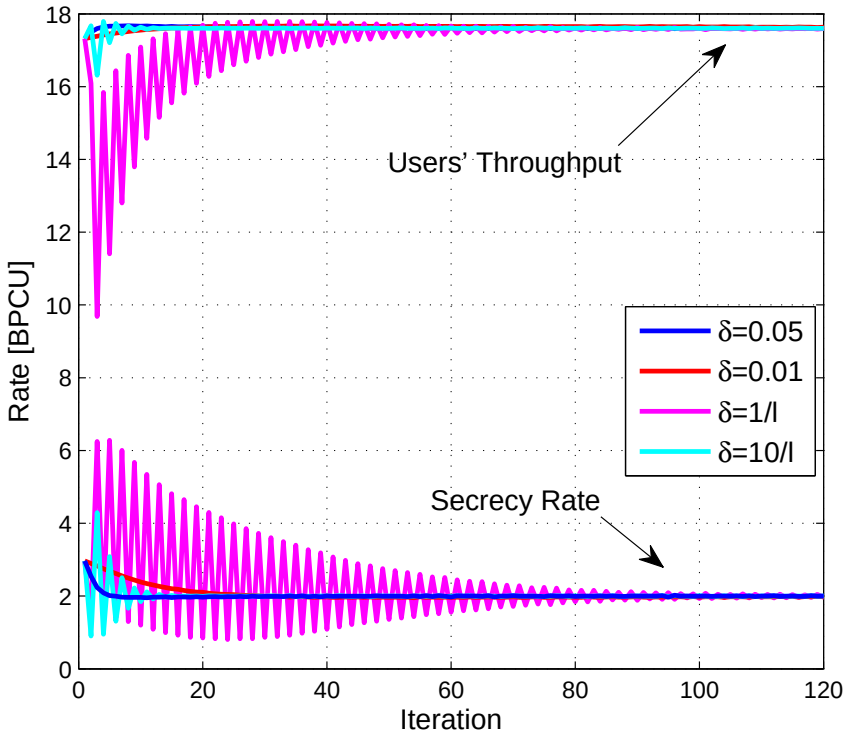



Fig. 4.3 Convergence behavior of SOA.

In Lemma 4.3, it is stated that $\mu^o$ can be obtained by examining at most five values. Given $\mu^o$, Lemma 4.2 can be used to provide the optimal power allocation in (4.14). Based on these two Lemmas, the subgradient method in Algorithm 12 is developed, called Subgradient Optimization Algorithm (SOA), to solve the original problem (4.12). If $M$ denotes the number of iterations (updates) in the subgradient process, tts computational complexity is $\mathcal{O}(NUM)$.

In Fig. 4.3, the convergence of SOA is shown versus the number of iterations/updates of the Lagrange multiplier $\lambda$ for $U = 10$ and $P_N = 15$ dB. Both the throughput of the selected users and the secrecy rate of the user $b$ are shown. Two different models are used for the step-size $\delta$; in the first $\delta$ has a fixed value while in the second it is decreased proportionally to the number of iterations $l$. Clearly, the convergence speed of the dual decomposition algorithm is heavily dependent on the step size. A small stepsize value may lead to slow convergence while a higher value may lead to higher fluctuations.

### 4.3.2 Decoupling the subproblems of subchannel assignment and power allocation

The drawback of the dual optimization solution described in the previous subsection is due to the iterative updating procedure of the Lagrange multiplier $\lambda$, since its convergence rate is dependent on the stepsize $\delta$ and the parameters of the problem. In this subsection, two suboptimal, low-complexity resource allocation schemes are presented that aim to solve the problem in (4.11). Both schemes consist of two phases, where the subchannel and the power allocation subproblems are decoupled. In the first phase, a subchannel assignment is specified that aims to maximize the throughput of the selected users. To accomplish this task, an initial power allocation is also required that results by a classic power waterfilling formula within each subchannel [33]. It should be noted that the secrecy constraint is only implicitly taken into consideration in this phase. In the second phase, which is common for both schemes, power swapping is performed within each subchannel between $b$ and the selected user. Power swapping is performed iteratively within each subchannel (in parallel across all the subchannels) aiming to adjust power allocation in order to fulfill the secrecy constraint with equality.

#### Subchannel assignment subproblem

The first subchannel assignment policy is based on a mixed rate-secrecy rate criterion to decide the user that will occupy each one of the available subchannels. The algorithm, called Maximum Throughput Subchannel Assignment (MTSA), uses an exhaustive search procedure to bind users with subchannels. For each subchannel, the sum $\left(R_{n,k}+R_{n,k}^{sr-b}\right)$ is calculated for each possible pair $(b,k)$, $k\in\mathscr{U}$ by using waterfilling to allocate $P_N$ over $b$ and $k$ [33]. The pair that leads to the maximum value is selected to occupy the subchannel $n$. The procedure is described in detail in Algorithm 13. The second subchannel assignment policy, called Correlation-based Subchannel Assignment (CSA), uses a simpler user selection rule that is based on spatial channel correlation between the eavesdropper and the users. Specifically, the user that is more aligned to the eavesdropper is selected to occupy the subchannel $n\in\mathscr{N}$. Since the ZFB orthogonalizes the channels between $b$ and the selected user, such a policy selection will make the effective channel of the $b$ almost vertical to the channel of the eavesdropper. The procedure is described in detail in Algorithm 14. In both algorithms, the activated user selection rule takes $\mathscr{O}(U)$ per subchannel while the initial power allocation is performed in constant cost. Thus, the computational complexity of the first phase of each algorithm is $\mathscr{O}(NU)$. Nevertheless, it should be noted that the Algorithm 14 has lower execution time since it uses a simpler user selection metric than Algorithm 13.

#### Power allocation subproblem

The Power Swapping Procedure (PSP), described in Algorithm 15, aims to fulfill the secrecy constraint of $b$. Given the subchannel assignment of the previous phase, the secrecy rate of

**Algorithm 13:** Maximum throughput subchannel assignment (MTSA)

1: **for** $n \in \mathcal{N}$ **do**
2: The subchannel $n$ is allocated to the user $k_n^* = \arg\max_{k \in \mathcal{U}} \left( R_{n,k} + R_{n,k}^{sr-b} \right)$ when $P_N$ is allocated by using power waterfilling over $b$ and $k$.
3: **end for**
4: The secrecy rate of $b$ is calculated and the power swapping procedure, described in Algorithm 15, is triggered.

**Algorithm 14:** Correlation-based subchannel assignment (CSA)

1: **for** $n = \in \mathcal{N}$ **do**
2: The subchannel $n$ is allocated to the user $k_n^* = \arg\max_{k \in \mathcal{U}} \left\| \mathbf{h}_{n,k} \mathbf{h}_{n,e}^H \right\|$,
3: The available amount of power $P_N$ is shared by using power waterfilling between $b$ and $k_n^*$.
4: **end for**
5: The secrecy rate of $b$ is calculated and the power swapping procedure, described in Algorithm 15, is triggered.

the user $b$ may be much less or much higher than the threshold $\overline{R}$. Thus, the first task of the power swapping is to calculate the secrecy rate of $b$ based on the subchannel allocation and the initial power allocation. If this value is higher (lower) than $\overline{R}$, the algorithm attempts to decrease (increase) $p_{n,b}$ by an amount $c_{n,b}\Delta P$ and increase (decrease) $p_{n,k}$ by $c_{n,k}\Delta P$. The secrecy rate is re-calculated and the power modification is adopted permanently if the secrecy approaches $\overline{R}$. The process is repeated as long as the secrecy constraint is not violated. The complexity of the power swapping procedure can not be accurately specified, since it depends on factors such as the initial value of secrecy rate, the value of $\Delta P$, the value of $P_T$ etc. However, it involves only scalar operations per iteration and it is performed in parallel across the subchannels. Empirically, it was observed that just a few number of iterations were enough. If $M$ denotes this number, the overall complexity of both algorithms is $\mathcal{O}(NU + M)$.

### Numerical results

In Fig. 4.4, the feasibility ratio is illustrated as a function of $P_N$ for the two resource allocation policies described above and the SOA described in the previous subsection. Feasibility is measured as the ratio of the instances where the secrecy constraint is guaranteed over the total number of problem instances that are set, that is 10000. It can be observed that the dual decomposition method and the MTSA-PSP scheme have almost the same behavior for moderate to high $P_N$ values. However, MTSA-PSP is superior in terms of feasibility for lower values of $P_N$.

**Algorithm 15:** Power swapping procedure (PSP)

Let $\Delta P > 0$ be a small value and let $\mathscr{S} = \{1, \ldots, N\}$.
**if** $\left(\sum_{n \in \mathscr{N}} R_{n,k_n^*}^{sr-b} \geq \overline{R}\right)$ **then**
  **while** $\left(\sum_{n \in \mathscr{N}} R_{n,k_n^*}^{sr-b} \geq \overline{R}\right)$ and $\mathscr{S} \neq \emptyset$ **do**
    Let $p_{n,k_n^*}^t = p_{n,k_n^*} + \Delta P c_{n,k_n^*}$ and $p_{n,b}^t = p_{n,b} - \Delta P c_{n,b}$, $n \in \mathscr{S}$. The subchannels in which $p_{n,b}^t \leq 0$ are removed from $\mathscr{S}$.
    The secrecy rate is re-calculated by using $\left(p_{n,k_n^*}^t, p_{n,b}^t\right)$, $n \in \mathscr{S}$, and $\left(p_{n,k_n^*}, p_{n,b}\right)$, $n \notin \mathscr{S}$. Let $\widetilde{R}_{n,k_n^*}^{sr-b}$ denotes the new secrecy rate of $b$.
    **if** $\widetilde{R}_{n,k_n^*}^{sr-b} \geq \overline{R}$ **then**
      Set $p_{n,k_n^*} = p_{n,k_n^*}^t$ and $p_{n,b} = p_{n,b}^t$ $n \in \mathscr{S}$.
    **else**
      exit while-loop.
    **end if**
  **end while**
**else**
  **while** $\left(\sum_{n \in \mathscr{N}} R_{n,k_n^*}^{sr-b} \leq \overline{R}\right)$ and $\mathscr{S} \neq \emptyset$ **do**
    Let $p_{n,k_n^*}^t = p_{n,k_n^*} - \Delta P c_{n,k_n^*}$ and $p_{n,b}^t = p_{n,b} + \Delta P c_{n,b}$, $n \in \mathscr{S}$. The subchannels in which $p_{n,k_n^*}^t \leq 0$ are removed from $\mathscr{S}$.
    The secrecy rate of $b$ is re-calculated by using $\left(p_{n,k_n^*}^t, p_{n,b}^t\right)$, $n \in \mathscr{S}$, and $\left(p_{n,k_n^*}, p_{n,b}\right)$ $n \notin \mathscr{S}$. Let $\widetilde{R}_{n,k_n^*}^{sr-b}$ denotes the new secrecy rate of $b$.
    **if** $\widetilde{R}_{n,k_n^*}^{sr-b} \leq \overline{R}$ **then**
      Set $p_{n,k_n^*} = p_{n,k_n^*}^t$ and $p_{n,b} = p_{n,b}^t$ $n \in \mathscr{S}$.
    **else**
      exit while-loop.
    **end if**
  **end while**
**end if**

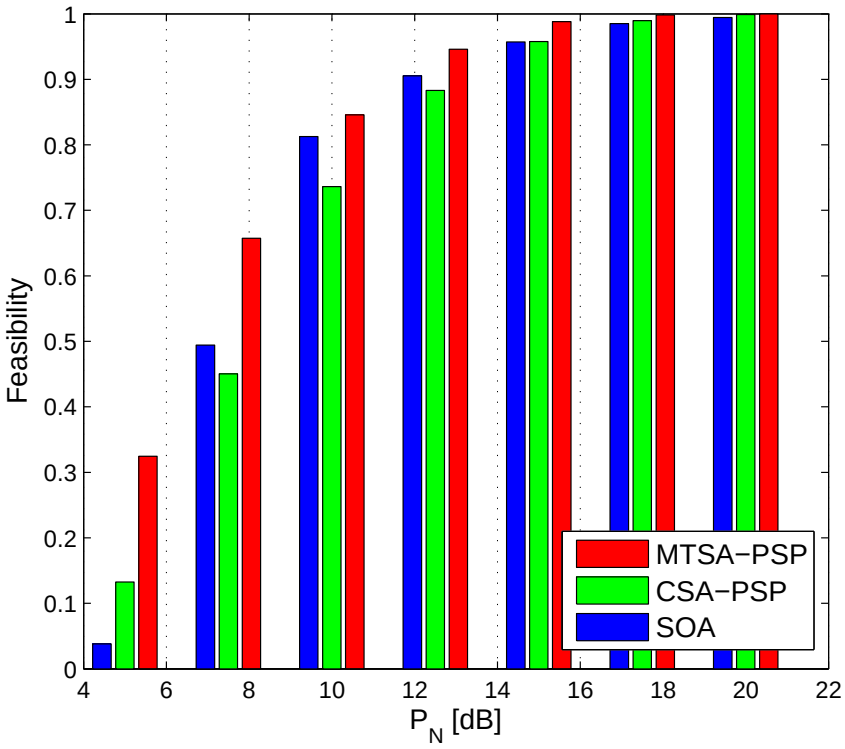
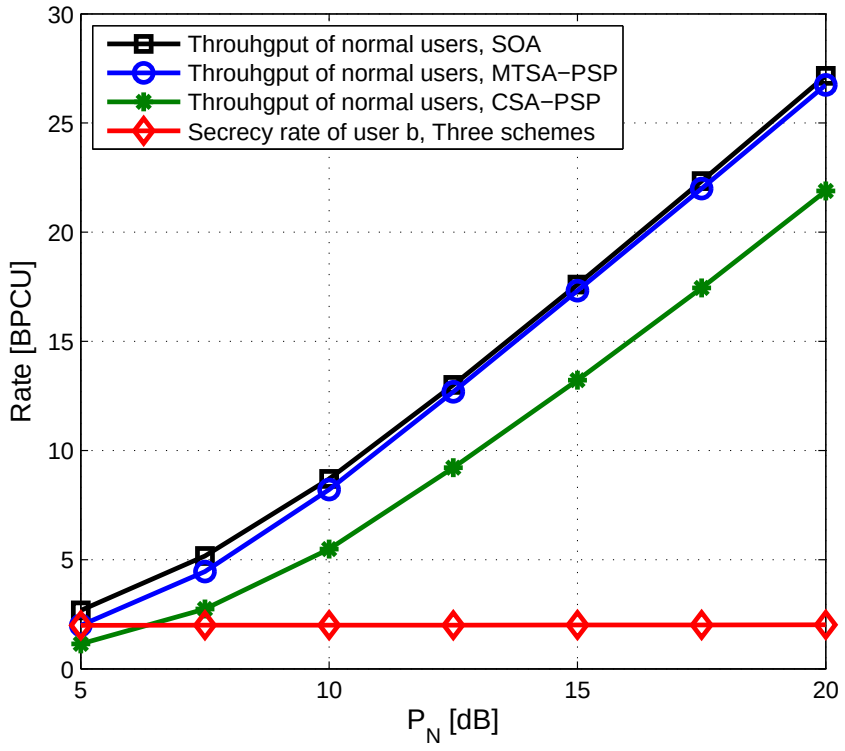
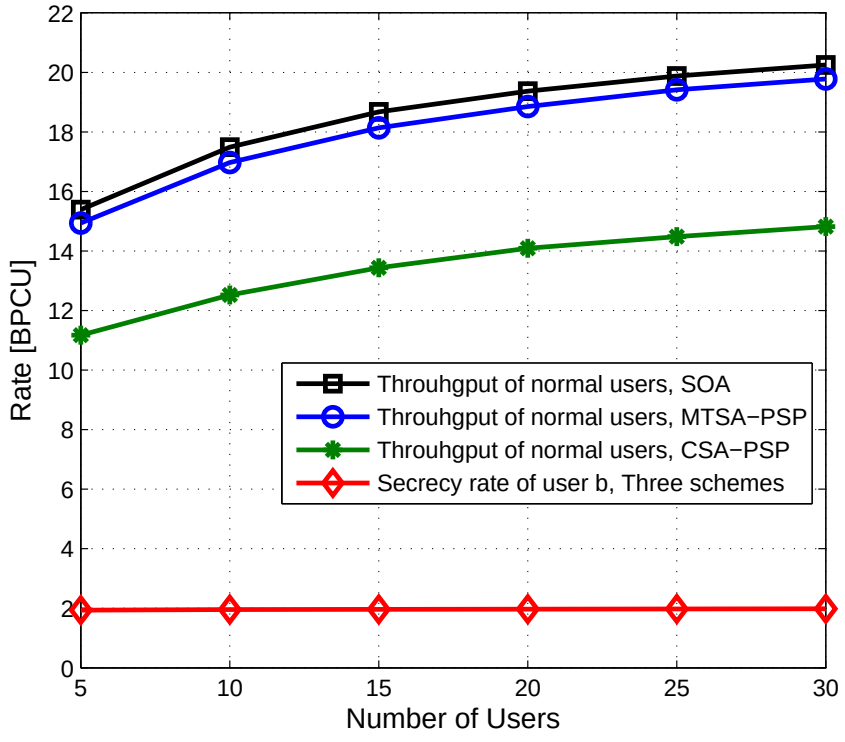



Fig. 4.4 Feasibility of the presented resource allocation schemes.

In Fig. 4.5a, the throughput of the selected users and the secrecy rate of the user $b$ are shown versus $P_N$ for MTSA-PSP, CSA-PSP and SOA. In SOA, the step-size is set equal to $\delta = 1/l$ and 500 iterations/updates of multiplier $\lambda$ are performed. In PSP, $\Delta P$ is set equal to $0.001P_N$. As can be seen, SOA outperforms the other two resource allocation solutions. However, MTSA-PSP becomes competitive to the subgradient optimization algorithm as $P_N$ increases. Moreover, it is advantageous in the sense that it is not affected by slow convergence issues as it happens with the subgradient optimization algorithm. Comparing MTSA-PSP and CSA-PSP, it seems that there is almost a constant gap between their performance. The better performance of MTSA-PSP is due to the explicit transmission rate calculations which are performed in the subchannel assignment phase. In the opposite, in CSA-PSP only channel spatial correlation calculations are performed. Nevertheless, the advantage of CSA is the less computational effort that is required since it doesn't need to perform any power allocation and rate calculations. In Fig. 4.5b the throughput of the selected users and the secrecy rate of $b$ are shown versus the number of the users for $P_N = 15$ dB. It can be seen, that all the three schemes exploit the multiuser diversity. As before, SOA outperforms the other two resource allocation schemes.




(a) Throughput & secrecy rate vs $P_N$, for $U = 10$.




(b) Throughput & secrecy rate vs number of users for $P_N = 15dB$.

Fig. 4.5 Throughput of the presented resource allocation schemes.

# Chapter 5

# Summary & future work

## 5.1 Summary

In this thesis, we have studied resource allocation problems in PHY layer of multiuser, multiantenna downlink systems. In particular, our focus was on two specific topics: user selection procedure and physical layer security aspects. In general, the problems that dealing with user selection are NP-complete. Thus, it is difficult to be solved in an optimal way. Physical layer security focuses on exploiting the physical layer properties of the wireless channels, such as multi-path fading and interference, to protect the confidential information transmission against eavesdropping.

In the first part, we present a low-complexity user selection algorithm to maximize throughput for the MISO-flat fading case under the assumption that ZFB is used to multiplex data streams of several users. As compared with other solutions, it reduces the computational complexity at the cost of a slight degradation in throughput. Moreover, we study the problem of resource allocation when the system transmits over a number of parallel channels. The problem primarily consists of deciding the user-channel binding and the corresponding power allocation procedure and it is investigated from the perspective of maximizing throughput under two different criteria of QoS; a) when each user is serviced with a guaranteed transmission rate and b) when a max-min criterion over users' rates is set as objective. For both considered problems, a near-optimal solution is derived by applying PLA of the logarithm-based formula of user transmission rate and solving the resulting MILPs. Also, a heuristic solution is presented that decouples the problems of channel assignment and power allocation and performs close to the optimal but with polynomial computational complexity. In broadband wireless systems that transmit over a number of parallel channels, resource allocation is commonly performed on chunk-basis. Thus, in the last section of this part we explore how the frequency diversity emanates from this aspect can be exploited to simplify the user selection process.

In the second part, we study the problem of secrecy rate balancing in a SISO, multiuser downlink that transmits over a number of parallel channels which are wiretapped by a passive eavesdropper. The considered problem is formulated as a MILNP which is hard to be solved because of its combinatorial and nonlinear nature. Thus, the study progresses towards two directions depending on whether the number of users is higher or less than the number of the available channels. In the first case, the optimal resource allocation scheme is obtained in polynomial computational complexity, under the additional assumption that the number of serviced users at a given time instant would be equal to the number of subchannels. In the case of less users than subchannels, optimality is derived in the two special cases where the available power tends to infinity and to zero, respectively. Nevertheless, each special case gives rise to a resource allocation scheme with competitive performance in a wide range of system setup. Moreover, two heuristic of linear computational complexity are proposed by decoupling the original problem into a subchannel assignment and a power allocation subproblem. The performance of all the presented schemes is evaluated by using as benchmark the MILP that results by employing PLA over the logarithm-based secrecy rate functions.

In the third part, we explore how spatial multiplexing can be employed in a multiantenna, multiuser downlink to improve system's spectral efficiency and also to provide wireless security. In general, the optimization problems that can be set when spatial multiplexing is combined with secrecy-oriented constraints are intractable. Herein, we employ ZFB and we focus on investigation two special problems; in the first, we aim to solve the user selection and power allocation problem in order to maximize the worst sum secrecy rate in a flat fading setup, where a passive eavesdropper wiretaps the messages of all the spatially multiplexed users. In the second, we assume a scenario in which a number of parallel channels are used to serve a special user that should be protected by passive eavesdropping and explore how the available spatial and channel resources can be simultaneously used by other users to enhance both system's spectral efficiency and wireless protection for the special users. For both problems we present several low-complexity solutions that exploit spatial multiplexing to appropriately create interference to the passive eavesdropper in a controlled manner.

## 5.2 Future work

Resource management will remain an important topic in the near and distant future wireless systems since its main task is to avoid wastage of the available resources and allocating them over a short period of time in order to providing the targeted QoS. Nevertheless, as the next generation wireless systems become available, it is of critical importance to explore the impact of their distinctive features into the resource management and planning procedure.

### 5.2.1 Resource allocation in massive MIMO systems

Massive MIMO systems have the potential to be a key technology in future wireless systems [107, 108]. In a massive MIMO system, the spatial signatures of the users to be scheduled might play a fundamental role thanks to the very large number of antennas and an excess of degrees of freedom. The multiuser diversity along with the high array gains might be exploited by resource allocation algorithm along with timely CSI. Since the total number of users would be much higher than the number of transmit antennas, the system needs efficient resource allocation algorithms to select best set of users according to a chosen criterion. In particular, the problem of user selection corresponds to a combinatorial problem. Hence, strategies based on heuristic, low-cost and discrete optimization methods would be very promising since they could reduce the overall computational cost of the procedure [109, 110].

### 5.2.2 Physical layer security in heterogeneous cellular networks

A promising way to face up the demanding data traffic requirements in the upcoming, next generation cellular networks is the deployment of a hybrid topology where macro base station (MBS) coexist with femtocell access points (FAPs), *i.e.* small, inexpensive and low-power cell entities which operate in the same frequency bands with MBS. Under this framework, the objective of the resource allocation problem, consisting of MIMO precoders at the MBS and FAPs, spectrum sharing, power control etc., has to be updated to integrate the special characteristics of the deployed scenario in terms of energy efficiency, interference management, relay-aided & cooperative transmission etc. [111–113]. Actually, the ad-hoc nature of FAPs and the limited back-haul infrastructure makes the problem of resource allocation to be highly affected by the contaminated CSI, which will be very hard to be obtained in instantaneous, perfect mode. Under this scope, integration of physical layer security is currently a more or less unexplored aspect [114].

# List of Abbreviations

| | |
|---|---|
| AWGN | Additive White Gaussian Noise |
| BS | Base Station |
| CSI | Channel State Information |
| DPC | Dirty Paper Coding |
| IP | Integer Program |
| KKT | Karush-Kuhn-Tucker |
| LSAP | Linear Sum Assignment Problem |
| MILP | Mixed Integer Linear Program |
| MIMO | Multiple Input Multiple Output |
| MINLP | Mixed Integer Non-Linear Program |
| MISO | Multiple Input Single Output |
| MRT | Maximum Ration Transmission |
| NP | Nondeterministic Polynomial |
| OFDM | Orthogonal Frequency Division Multiplexing |
| OFDMA | Orthogonal Frequency Division Multiple Access |
| PDP | Power Delay Profile |
| PLS | Physical Layer Security |
| PLA | Piecewise Linear Approximation |
| QoS | Quality of Service |
| SDMA | Space Division Multiple Access |
| SINR | Signal-to-Interference-plus-Noise Ratio |
| SISO | Single Input Single Output |
| SNR | Signal to Noise Ratio |
| ZFB | Zero-Forcing Beamforming |

# References


[1] H. Huang, C. Papadias, and S. Venkatesan, *MIMO Communication for Cellular Networks*. Springer, 2012.

[2] C. Windpassinger, R. F. H. Fischer, T. Vencel, and J. B. Huber, "Precoding in multiantenna and multiuser communications," *IEEE Trans. Wireless Commun.*, vol. 3, pp. 1305–1316, Jul. 2004.

[3] D. Tse and P. Viswanath, *Fundamentals of Wireless Communications*. Cambridge University Press, 2004.

[4] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 53, pp. 3936–3964, Sep. 2006.

[5] M. Mohseni, R. Zhang, and J. Cioffi, "Optimized transmission for fading multiple-access and broadcast channels with multiple antennas," *IEEE J. Sel. Areas Commun.*, vol. 24, pp. 1627–1639, Aug. 2006.

[6] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. 29, pp. 439–441, May 1983.

[7] U. Erez and S. ten Brink, "A closed-to-capacity dirty paper coding scheme," *IEEE Trans. Inf. Theory*, vol. 51, pp. 3417–3432, Oct. 2005.

[8] J. Liu and A. Krzymien, "A novel nonlinear precoding algorithm for the downlink of multiple antenna multi-user systems," in *Proc. IEEE VTC-Spring*, 2005, pp. 887–891.

[9] R. Prasad, *OFDM for Wireless Communications Systems*. Artech House, 2004.

[10] H. Yang, "A road to future broadband wireless access: MIMO-OFDM-based air interface," *IEEE Commun. Mag.*, vol. 43, pp. 53–60, Jan. 2005.

[11] W. W. L. Ho and Y.-C. Liang, "Optimal resource allocation for multiuser MIMO-OFDM systems with user rate constraints," *IEEE Trans. Veh. Technol.*, vol. 58, pp. 1190–1203, Mar. 2009.

[12] A. D. Wyner, "The wire–tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1367, 1975.

[13] S. L. Y. Cheong and M. Hellman, "The gaussian wire–tap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, Jul. 1978.

[14] I. Csiszar and J. Korner, "Broadcast channels with confidentials messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–349, May 1978.

[15] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security Part I: theoretical aspects," *IEEE Trans. Inf. Theory, Special Issue on Information-Theoretic Security*, vol. 54, pp. 693–702, 2008.

[16] A. Khisti and G. Wornell, "Secure transmission with multiple antennas I: the MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 3088–3104, Jul. 2010.

[17] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, pp. 4961–4972, Aug. 2011.

[18] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna gaussian bc with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, pp. 1235–1249, Mar. 2009.

[19] 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, pp. 4215–4227, Sep. 2010.

[20] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, pp. 2083–2114, Apr. 2011.

[21] L. S. X. Zhou and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2014.

[22] S. Vishwanath, N. Jindal, and A. Goldsmith, "Duality, achievable rates and sum-rate capacity of gaussian MIMO broadcast channels," *IEEE Trans. Inf. Theory*, vol. 49, pp. 2658–2668, Oct. 2003.

[23] N. Jindal and A. Goldsmith, "Dirty-paper coding versus TDMA for MIMO broadcast hannels," *IEEE Trans. Inf. Theory*, vol. 51, pp. 1783–1794, May 2005.

[24] J. Lee and N. Jindal, "Dirty paper coding vs. linear precoding for MIMO broadcast channels," in *Proc. Asilomar*, 2006, pp. 779–783.

[25] M. Sharif and B. Hassibi, "A comparison of time-sharing, DPC and beamforming for MIMO broadcast channels with many users," *IEEE Trans. Commun.*, vol. 55, pp. 11–15, Jan. 2007.

[26] S. Sigdel and W. A. Krzymien, "Simplified fair scheduling and antenna selection algorithms for multiuser MIMO orthogonal space-division multiplexing downlink," *IEEE Trans. Veh. Technol.*, vol. 58, pp. 1329–1344, Mar. 2009.

[27] N. Jindal, W. Ree, S. Vishwanath, S. A. Jafar, and A. Goldsmith, "Sum power iterative water-filling for multi-antenna Gaussian broadcast channels," *IEEE Trans. Inf. Theory*, vol. 51, pp. 1570–1580, Apr. 2005.

[28] M. Kobayashi and G. Caire, "An iterative water-filling algorithm for maximum weighted sum-rate of gaussian MIMO-BC," *IEEE J. Sel. Areas Commun.*, vol. 24, pp. 1640–1646, Aug. 2006.

[29] G. Caire and S. Shamai, "On the achievable throughput of a multiantenna gaussian broadcast channel," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1691–1706, Jul. 2003.

[30] Z. Tu and R. Blum, "Multiuser diversity for a dirty paper approach," *IEEE Commun. Lett.*, vol. 7, pp. 370–372, Aug. 2003.

[31] W. Y. C-H. F. Fung and T. J. Lim, "Precoding for the multiantenna downlink: multiuser SNR gap and optimal user ordering," *IEEE Trans. Commun.*, vol. 55, pp. 188–197, Jan. 2007.

[32] K. Zu, R. C. D. Lamare, and M. Haardt, "Multi-branch tomlinson-harashima precoding design for MU-MIMO systems: theory and algorithms," *IEEE Trans. Commun.*, vol. 62, pp. 939–951, Mar. 2014.

[33] G. Dimic and N. D. Sidiropoulos, "On downlink beamforming with greedy user selection: performance analysis and a simple new algorithm," *IEEE Trans. Signal Process.*, vol. 53, pp. 3857–3868, Oct. 2005.

[34] B. M. H. C. B. Peel and A. L. Swindlehurst, "A vector-perturbation technique for near-capacity multiantenna multiuser communication – Part I: channel inversion and regularization," *IEEE Trans. Commun.*, vol. 53, pp. 195–202, Jan. 2005.

[35] T. Yoo and A. Goldsmith, "On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming," *IEEE J. Sel. Areas Commun.*, vol. 24, pp. 528–541, Mar. 2006.

[36] Z. Wang and W. Chen, "Regularized zero-forcing for multiantenna broadcast channels with user selection," *IEEE Wireless Commun. Lett.*, vol. 2, pp. 129–132, Apr. 2012.

[37] Z. Shen, R. Chen, J. G. Andrews, R. W. H. Jr., and B. L. Evans, "Low complexity user selection algorithms for multiuser MIMO systems with block diagonalization," *IEEE Trans. Signal Process.*, vol. 54, pp. 3658–3663, Sep. 2006.

[38] M. Fuchs, G. D. Galdo, and M. Haardt, "Low complexity space-time-frequency scheduling for MIMO systems with SDMA," *IEEE Trans. Veh. Technol.*, vol. 56, pp. 2775–2784, Sep. 2007.

[39] X. Wang and X.-D. Zhang, "Linear transmission for rate optimization in MIMO broadcast channels," *IEEE Trans. Wireless Commun.*, vol. 9, pp. 3247–3257, Oct.2010.

[40] R. Chen, Z. Shen, J. Andrews, and R. H. Jr., "Multimode transmission for multiuser MIMO systems with block diagonalization," *IEEE Trans. Signal Process.*, vol. 56, pp. 3294–3302, Jul. 2008.

[41] H.-C. Yang and M.-S. Alouini, *Order Statistics in Wireless Communications Diversity, Adaptation, and Scheduling in MIMO and OFDM Systems*. Cambridge University Press, 2011.

[42] C. Y. Wong, R. S. Cheng, K. B. Letaief, and R. D. Murch, "Multiuser OFDM with adaptive subcarrier, bit, and power allocation," *IEEE J. Sel. Areas Commun.*, vol. 10, pp. 1747–1758, Oct. 1999.

[43] W. Rhee and J. M. Cioffi, "Increase in capacity of multiuser OFDM system using dynamic subchannel allocation," in *Proc. IEEE VTC-Spring*, 2000, pp. 1085–1089.

[44] W. Xu, C. Zhao, P. Zhou, and Y. Yang, "Efficient adaptive resource allocation for multiuser OFDM systems with minimum rate constraints," in *Proc. IEEE ICC*, 2007, pp. 5226–5231.

[45] E. S. Lo, P. Chan, V. Lau, R. Cheng, K. B. Letaief, R. Murch, and W. H. Mow, "Adaptive resource allocation and capacity comparison of downlink multiuser MIMO-MC-CDMA and MIMO-OFDMA," *IEEE Trans. Wireless Commun.*, vol. 6, pp. 1083–1093, Mar. 2007.

[46] P. Tejera, W. Utschick, G. Bauch, and J. Nossek, "Subchannel allocation in multiuser multiple-input-multiple-output systems," *IEEE Trans. Inf. Theory*, vol. 52, pp. 4721–4733, Oct. 2006.

[47] J. Tang, K. Cumanan, and S. Lambotharan, "Sum-rate maximization technique for spectrum-sharing MIMO OFDM broadcast channels," *IEEE Trans. Veh. Technol.*, vol. 60, pp. 1960–1964, May 2011.

[48] G. Zheng, K.-K. Wong, and T.-S. Ng, "Throughput maximization in linear multiuser MIMO-OFDM downlink systems," *IEEE Trans. Veh. Technol.*, vol. 57, pp. 1993–1998, May 2008.

[49] S. Shi, M. Schubert, and H. Boche, "Rate optimization for multiuser MIMO systems with linear processing," *IEEE Trans. Signal Process.*, vol. 56, pp. 4020–4030, Aug. 2008.

[50] C. Pan, Y. Cai, and Y. Xu, "Adaptive subcarrier and power allocation for multiuser MIMO-OFDM systems," in *Proc. IEEE ICC*, 2005, pp. 2631–2635.

[51] H. Karaa, R. Adve, and A. Tenenbaum, "Linear precoding for multiuser MIMO-OFDM systems," in *Proc. IEEE ICC*, 2007, pp. 2797–2802.

[52] H. Karaa and R. Adve, "User assignment for MIMO-OFDM systems with multiuser linear precoding," in *Proc. IEEE WCNC*, 2008, pp. 952–957.

[53] T. F. Maciel and A. Klein, "On the performance, complexity and fairness of suboptimal resource allocation for multiuser MIMO-OFDMA systems," *IEEE Trans. Veh. Technol.*, vol. 59, pp. 406–419, Jan. 2010.

[54] P. Henarejos, A. Perez-Neira, V. Tralli, and M. Lagunas, "Low-complexity resource allocation with rate balancing for the MISO-OFDMA broadcast channel," *Elsevier Signal Processing*, vol. 92, pp. 2975–2989, 2012.

[55] J. Chen and A. Swindlehurst, "Applying bargaining solutions to reduce allocation in multiuser MIMO-OFDMA broadcast systems," *IEEE J. Sel. Topics Signal Process.*, vol. 6, pp. 127–139, Apr. 2012.

[56] P. Chan and R. Cheng, "Capacity maximization for zero-forcing MIMO-OFDMA downlink systems with multiuser diversity," *IEEE Trans. Wireless Commun.*, vol. 6, pp. 1880–1889, May 2007.

[57] F. Jiang, J. Zhu, G. Hu, Y.Wang, G. Liu, and P. Zhang, "Joint space-frequency-power scheduling algorithm for real time service in cellular MIMO-OFDM system," in *Proc. IEEE VTC-Spring*, 2008, pp. 2461–2466.

[58] P. Tejera, W. Utschick, J. Nossek, and G. Bauch, "Rate balancing in multiuser MIMO OFDM systems," *IEEE Trans. Commun.*, vol. 57, pp. 1370–1380, May 2009.

[59] D. Perea-Vega, A. Girard, and J-F.Frigon, "Dual-based bounds for resource allocation in zero-forcing beamforming OFDMA-SDMA systems," *EURASIP Journal onWireless Communications and Networking*, vol. 51, pp. 1–16, 2013.

[60] F. Shams, G. Bacci, and M. Luise, "A survey on resrouce allocation techniques in OFDM(A) networks," *Elsevier, Computer Networks*, vol. 65, pp. 129–150, Mar. 2014.

[61] H. Zhu and J. Wang, "Chunk-based resource allocation in OFDMA systems - Part I: chunk allocation," *IEEE Trans. Commun.*, vol. 57, pp. 2734–2744, Sep. 2009.

[62] C. Tsai, C. Chang, F. Ren, and C. Yen, "Adaptive radio resource allocation for downlink OFDMA/SDMA systems with multimedia traffic," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 1734–1743, May 2008.

[63] N. Gao and X. Wang, "Optimal subcarrier-chunk scheduling for wireless OFDMA systems," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 2116–2123, Jul. 2011.

[64] Z. Ren, S. Chen, C. Bo, and W. Ma, "Proportional resource allocation with subcarrier grouping in OFDM wireless systems," *IEEE Commun. Lett.*, vol. 17, pp. 868–871, May 2013.

[65] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge University Press, 1990.

[66] T. Ji, C. Zhou, S. Zhou, and Y. Yao, "Low complex user selection strategies for multiuser MIMO downlink scenario," in *Proc. IEEE WCNC*, 2007, pp. 1534–1538.

[67] I. Gurobi Optimization, "Gurobi optimizer reference manual," 2015. [Online]. Available: http://www.gurobi.com

[68] A. B. Keha, I. R. de Farias, and G. L. Nemhauser, "Models for representing piecewise linear cost functions," *Operations Research Letters*, vol. 32, pp. 44–48, 2004.

[69] "Digital land mobile radio communications-COST 207," *Commission of the European Communities, Final Report, Office for Official Publications of the European Communities*, 1989.

[70] A. Biagioni, R. Fantacci, D. Marabissi, and D. Tarchi, "Adaptive subcarrier allocation schemes for wireless OFDMA systems in WiMAX networks," *IEEE J. Sel. Areas Commun.*, vol. 27, pp. 217–225, Feb. 2009.

[71] E. Dahlman, S. Parkvall, J. Skold, and P. Beming, *3G Evolution – HSPA and LTE for Mobile Broadband*. Academinc Press, 2008.

[72] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[73] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. 44th Annu. Allerton Conf.*, 2006, pp. 841–848.

[74] Y. Liang, H. V. Poor, and S. Shamai, "Secrecy capacity region of parallel broadcast channels," in *Proc. ITW*, 2007, pp. 240–250.

[75] E. Jorswieck and A. Wolf, "Resource allocation for the wire-tap multicarrier broadcast channel," in *Proc. Int. Conf. Telecommun.*, 2008, pp. 1–6.

[76] E. Jorswieck and S. Gerbracht, "Secrecy rate region of downlink OFDM systems: efficient resource allocation," in *Proc. IEEE Int. OFDM Workshop*, 2009, pp. 1–6.

[77] D. W. K. Ng, E. S. Lo, and R. Schober, "Resource allocation for secure OFDMA networks with imperfect CSIT," in *Proc. IEEE Globecom*, 2011, pp. 1–6.

[78] 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 Security*, vol. 6, pp. 693–702, Sept. 2011.

[79] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation for secure OFDMA systems," *IEEE Trans. Veh. Technol.*, vol. 61, pp. 2572–2585, Jul. 2012.

[80] X. Zhu, B. Yang, and X. Guan, "Cross-layer scheduling with secrecy demands in delay-aware OFDMA network," in *Proc. IEEE WCNC*, 2013, pp. 1339–1344.

[81] A. Wang, J. Chen, Y. Cai, C. Cai, W. Yang, and Y. Cheng, "Joint subcarrier and power allocation for physical layer security in cooperative OFDMA networks," *EURASIP Journal onWireless Communications and Networking*, vol. 193, pp. 1–10, 2013.

[82] M. Ara, H. Reboredo, F. Renna, and M. Rodrigues, "Power allocation strategies for OFDM gaussian wiretap channels with a friendly jammer," in *Proc. IEEE ICC*, Jun. 2013, pp. 3413–3417.

[83] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, M. Zhao, and J. Wang, "Power allocation and artificial noise design for wiretap OFDM with arbitrary inputs," *IEEE Trans. Wireless Commun.*, vol. 12, pp. 2717–2729, Jul. 2013.

[84] 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 ICC*, 2013, pp. 786–791.

[85] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 3528–3540, Oct. 2011.

[86] R. Bassily, E. Ekrem, H. Xiang, E. Takin, X. Jianwei, M. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer," *IEEE Signal Process. Mag.*, vol. 30, pp. 16–28, Sep. 2013.

[87] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4687–4698, Oct. 2008.

[88] A. Chorti, S. M. Perlaza, Z. Han, and H. Poor, "Physical layer security in wireless networks with passive and active eavesdroppers," in *Proc. IEEE Globecom*, Dec. 2012, pp. 4868–4873.

[89] A. Volgenant, "Linear and semi-assignment problems: A core oriented approach," *Computers & OR*, vol. 23, pp. 917–932, 1996.

[90] R. Burkard, M. Dell'Amico, and S. Martello, *Assignment Problems*. SIAM, 2009.

[91] A. Ghosh, J. Zhang, J. Andrews, and R. Muhamed, *Fundamentals of LTE*. Prentice Hall, 2011.

[92] A. Lozano and N. Jindal, "Are yesterday-s information-theoretic fading models and performance metrics adequate for the analysis of today's wireless systems?" *IEEE Commun. Mag.*, vol. 50, pp. 210–217, Nov. 2012.

[93] D. Bertsekas, *Nonlinear Programing*. Athens Scientific, 2004.

[94] Y. K. Lin, M. E. Pfund, and J. W. Fowler, "Heuristics for minimizing regular performance measures in unrelated parallel machine scheduling problems," *Computers & OR*, vol. 38, pp. 901–916, 2011.

[95] N. Karmarkar, "A new polynomial-time algorithm for linear programming," *Combinatorica*, vol. 4, pp. 373–395, 1984.

[96] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, Jun. 2008.

[97] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser mimo wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 544–549, Feb. 2012.

[98] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Sign. Proc.*, vol. 59, pp. 351–361, Jan. 2011.

[99] Z. Ding, K. K. Leung, and H. V. Poor, "Interference masking for secure wireless broadcast communications," *IET Communications, Special issue on Secure Physical Layer Communications*, vol. 8, pp. 1184–1187, May 2014.

[100] L. Dong, H. Zhu, A. Petropulu, and H. Poor, "Cooperative jamming for wireless physical layer security," in *Proc. IEEE Statist. Sign. Proc.*, 2009, pp. 417–420.

[101] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. L. Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, pp. 1833–1847, May 2015.

[102] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Sign. Proc.*, vol. 60, pp. 1696–1707, Apr. 2012.

[103] C. Geraci, M. E. M., Y. Jinhong, A. Razi, and I. Collings, "Secrcecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, pp. 3472–3482, Nov. 2012.

[104] A. Mukherjee and A. L. Swindlehurst, "User selection in multiuser MIMO systems with secrecy considerations," in *Proc. Asimolar Conf. Sign. Syst. Comp.*, 2009, pp. 1479–1482.

[105] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions: With Formulas, Graphs, and Mathematical Tables*. Courier Dover Publications, 1964.

[106] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[107] F. Rusek, D. Persson, B. Lau, E. Larsson, T. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: opportunities, and challenges with very large arrays," *IEEE Signal Processing Mag.*, vol. 30, pp. 40–60, Jan. 2013.

[108] L. Lu, G. Y. Li, A. Swindlehurst, A. Ashikhmin, and R. Zhang, "An overview of massive MIMO: benefits and challenges," *IEEE J. Sel. Topics Signal Process.*, vol. 8, pp. 742–758, Oct. 2014.

[109] R. C. de Lamar, "Massive MIMO systems: signal processing challenges and research trends," *arXiv:i3i0*, Oct. 2013.

[110] V. Jungnickel, K. Manolakis, W. Zirwas, B. Panzner, V. Braun, M. Lossow, M. Sterna, R. Apelfrojd, and T. Svensson, "The role of small cells, coordinated multipoint, and massive MIMO in 5G," *IEEE Commun. Mag.*, vol. 52, pp. 44–51, May 2014.

[111] R. Xie, F. R. Yu, and H. Ji, "Energy-efficient spectrum sharing and power allocation in cognitive radio femtocell networks," in *Proc. IEEE INFOCOM*, 2012, p. 1665–1673.

[112] Z. Lu, T. Bansal, and P. Sinha, "Achieving user-level fairness in open-access femtocell based architecture," *IEEE Trans. Mobile Com.*, vol. 12, p. 1943–1954, Oct. 2013.

[113] H. V. Nguyen and L. L. Bao, "Fair resource allocation for OFDMA femtocell networks with macrocell protection," *IEEE Trans. Veh. Technol.*, vol. 63, pp. 3528–3540, Mar. 2014.

[114] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, pp. 1154–1170, Mar. 2015.