Abstract—This paper deals with the problem of sum rate maximization for a multiuser orthogonal frequency-division multiple access channel with secrecy rate constraints. We consider the case of a multiple-antenna base station (BS) and several single-antenna downlink receivers; a single secure user, a single eavesdropper and several normal users (without secrecy requirements). The eavesdropper intends to wiretap the message of the secure user and the BS aims to protect its transmission by appropriately scheduling normal users and enforcing spatial multiplexing between them and the secure user. A frequency (subchannel) and power allocation problem that aims to maximize the sum rate of the normal users, while a secrecy rate constraint is ensured for the secure user, is formulated. The resulting resource allocation problem is non-convex. Based on the dual problem and some well-defined transformations, we provide an iterative resource allocation algorithm with linear complexity with respect to the number of normal users and subchannels. In addition, two low-complexity solutions that are based on the decoupling of the subchannel and the power allocation subproblems, are investigated. Numerical results are provided to illustrate the performance of all the proposed solutions.

Index Terms — Secrecy rate, user selection, resource allocation, OFDMA, zero-forcing beamforming.

I. INTRODUCTION

The issues of confidentiality and security are always critical in wireless communication systems. Since the seminal work of Wyner [1], where the fundamental notions of perfect capacity and physical-layer security have been introduced, several techniques and approaches have been proposed to guarantee security under various network configurations [2]. The main advantage of physical layer security, in comparison to cryptography-based high layer approaches, lies on the fact that it is independent of the interception and processing ability of the eavesdropper. Currently, there is a lot of interest to employ physical layer security in orthogonal frequency-division multiple access (OFDMA) systems and integrate it into the general problem of resource allocation for multuser multiantenna systems [3], [4], [5].

In [6], the authors study the optimal power allocation that maximizes a weighted secrecy sum rate for a single-input single-output (SISO)-OFDMA system with two legitimated users with confidential messages. Resource allocation for SISO-OFDMA downlink is investigated in [7], where both secure and normal users co-exist and the secure users 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 target secrecy rate constraint for the secure users. Some practical SISO-OFDMA communication scenarios are discussed in [8] under both secrecy and delay constraints. The work in [9] deals with a resource allocation 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.

All the previous studies refer to scenarios where an exclusive subchannel allocation condition holds and/or protection from the eavesdropper is achieved by jamming interference e.g transmitting onto the nullspace of the secrecy sensitive users. However, both approaches cause a significant waste of frequency and power resources that could be used in order to further improve system’s performance. The motivation herein is to explore how the coexistence of secure and normal users can be integrated to the problem of secrecy and how it can be combined with spatial multiplexing and power management to provide more efficient resource allocation solutions; ensuring secrecy without sacrificing a portion of system’s resources to protect the secure users from the eavesdropper [10]. To the best of the authors’s knowledge, such an attempt has not previously appeared in the literature.

In this paper, the model of [7] is extended to allow subchannel sharing between secure and normal users. For the sake of simplicity, it is assumed that a single secure user and a single eavesdropper exist. Moreover, that the BS has two antennas and it uses Zero Forcing Beamforming (ZFB) to spatially multiplex the transmitted signal of the secure user and the normal users. The examined problem is to maximize the sum rate of the normal users under a secrecy rate constraint (for the secure user) as well as a transmit power constraint. The novelty lies in the fact that each subchannel is forced to be shared by the secure user and a selected normal user. This coexistence is beneficial for both of them. The secure user is protected from the eavesdropper, since the transmitted power for the normal user causes jamming interference to the eavesdropper, while the selected normal user has the opportunity to occupy some system’s resources to receive its own message. The problem under consideration is stated as a combinatorial, non-convex optimization problem and two different approaches are

Throughput Maximization in Multiantenna OFDMA Downlink under Secrecy Rate Constraints

Sotiris Karachontzitis*†, Stelios Timotheou† and Ioannis Krikidis‡

* Computer Technology Institute & Press “Diophantus”, 26500, Rio-Patras, Greece
† Computer Engineering and Informatics Dept., University of Patras, 26500, Rio-Patras, Greece
‡ Department of Electrical and Computer Engineering, University of Cyprus, Cyprus
E-mail: karaxodg@ceid.upatras.gr, {timotheou.stelios, krikidis}@ucy.ac.cy
developed for its solution. In the first approach, the Lagrangian dual of the original problem is formulated in a way that allowed its iterative solution. In each iteration, the Lagrangian dual is decomposed into \( N \) independent subproblems of non-linear and combinatorial nature, where \( N \) is the number of OFDM subchannels. By using some non-trivial transformations, each one of these subproblems is solved to optimality, resulting in an iterative user assignment and power allocation algorithm that provides a lower bound to the optimal solution of the original problem. In the second approach, the subchannel and the power allocation subproblems are decoupled and heuristic rules are employed to separately solve them in an efficient and parallel across the subchannels manner.

The remainder of the paper is organized as follows: In Section II, the model under consideration is introduced and the addressed problem is described. In Section III the three proposed resource allocation schemes are presented and their computational complexity is discussed. Simulation results are presented in Section IV and conclusions in Section V.

**Notation:** In the following, lowercase bold letters denote vectors and bold uppercase denote matrices. \( \mathbb{R} \) contains the unit energy information symbols destined to the channel between the BS and the eavesdropper in subchannel \( n \). \( \mathbb{C} \) is the set of all complex numbers. \( \mathbb{Z} \) denotes the set of all integers. \( \mathbb{Z}_+ \) denotes the set of all positive integers. \( \mathbb{N} \) contains the set of all natural numbers. \( \{0,1\} \) is the binary set. \( (\quad)^T \) denotes transpose, \( (\quad)^H \) the conjugate transpose and \( \| \cdot \| \) the norm of a matrix or vector. \( \log(\cdot) \) refers to the base-2 logarithm. \( \cup \) denotes set union and \( \bullet \) denotes either set cardinality or absolute value of a complex scalar.

**II. SYSTEM MODEL & PROBLEM FORMULATION**

The downlink of an OFDMA multiuser system is considered to be consisting of a single BS, a secure user \((b)\), \( K \) normal users and one eavesdropper \( e \). The BS is equipped with two transmit antennas, whereas all the users including \( b \) and the eavesdropper have a single receive antenna. It is assumed that the BS has allocated \( N \) subchannels to serve \( b \) in a secured transmission way. Nevertheless, each one of these subchannels is also allocated to one of the normal users by using ZFB over \( b \) and the selected user. Let \( h_{n,b} \) be the wireless channel between the BS and the user \( k \) in subchannel \( n \). \( h_{n,b, e} \) is the channel between the BS and the BS and the eavesdropper in subchannel \( n \). It is assumed that all of these channels are row vectors in \( \mathbb{C}^2 \) and they are known to the BS.

Let \( k_n^b \) be the user (out of the \( K \) normal users) that has been selected for transmission within the subchannel \( n = 1, \ldots, N \). The transmitted vector within the subchannel \( n \) is written as \( x_n = W_n D_n s_n \), where \( s_n \in \mathbb{R}^2 \) contains the unit energy information symbols destined to \( \{b \cup k_n^b\} \), \( D_n \in \mathbb{R}^{2 \times 2} \) is a diagonal power matrix with the vector \( \sqrt{P_{n,b}} \), \( \sqrt{P_{n,k_n^b}} \) in the main diagonal and \( W_n = [w_{n,b}, w_{n,k_n^b}] \in \mathbb{C}^{2 \times 2} \) is the beamforming matrix. The rows of \( H_{n,k_n^b} = [h_{n,b,k_n^b}, h_{n,k_n^b}] \) and \( H_{n,b} = [h_{n,b}, h_{n,k_n^b}] \) correspond to the channels of \( \{b \cup k_n^b\} \). Under this context, \( \{b \cup k_n^b\} \) are encoded individually within subchannel \( n \) and their received signal is

\[
\begin{align*}
    y_{n,b} &= h_{n,b} W_n b \sqrt{P_n} d_n b + z_{n,b}, \\
    y_{n,k_n^b} &= h_{n,k_n^b} W_n k_n^b \sqrt{P_n} s_n k_n^b + z_{n,k_n^b},
\end{align*}
\]

where \( z_{n,k_n^b}, z_{n,b} \) denotes the independent and identically distributed (i.i.d.) samples of additive white Gaussian noise (AWGN) with variance \( \sigma_n^2 \), \( \sigma^2_z = \sigma^2 \). The secrecy rate of \( b \) and the transmission rate of user \( k_n^b \) are given as

\[
\begin{align*}
    R_n^b &= \left[ \log \left( 1 + \frac{P_n}{2} / \sigma_n^2 \right) - \log \left( 1 + \Gamma_n k_n^b / \sigma^2 \right) \right] + \\
    R_n k_n^b &= \log \left( 1 + \frac{P_n}{2} / \sigma^2 \right),
\end{align*}
\]

where \( \Gamma_n k_n^e = \frac{P_n}{\sigma^2} + \frac{\|W_n w_{n,k_n^b}\|^2}{\sigma^2} \) is the signal-to-interference-plus-noise ratio (SINR) for the link BS-\( e \). In the following analysis we set \( \sigma^2 = 1 \) for the sake of simplicity.

The aim of this paper is to maximize the throughput of the normal users under a secrecy rate constraint for \( b \) and an average power constraint per subchannel. Such a power constraint results in a more balanced power allocation across the available spectrum and it allows a simpler analysis versus a total average power constraint. Thus, the problem to be solved is the following

\[
\begin{align*}
    \max_{w_n,b, p_{n,b}} & \sum_{n,k} w_{n,k} \log \left( 1 + \frac{p_{n,k}}{\sigma^2} \right) \tag{3a} \\
    \text{s.t.} & \sum_{n,k} w_{n,k} R_{n,k}^b \geq \mathcal{R}, \tag{3b} \\
    & \sum_{k} w_{n,k} \left( p_{n,k} c_{n,k} + p_{n,b} c_{n,b} \right) \leq \frac{P_{\text{tot}}}{N}, \quad \forall n \tag{3c} \\
    & \sum_{n,k} w_{n,k} = 1, \quad n = 1, \ldots, N \tag{3d} \\
    & w_{n,k} \in \{0,1\}, \quad k = 1, \ldots, K, \quad n = 1, \ldots, N \tag{3e} \\
    & p_{n,b}, p_{n,k} \geq 0, \quad k = 1, \ldots, K, \quad n = 1, \ldots, N \tag{3f}
\end{align*}
\]

where the binary variable \( w_{n,k} \) represents the normal user that has been selected for subchannel \( n \) (e.g. \( w_{n,k} = 1 \) when the user \( k \) has been selected for subchannel \( n \), otherwise \( w_{n,k} = 0 \)). \( \mathcal{R} \) is the required secrecy rate of \( b \), \( c_{n,k} = \left( H_{n,k_n^b} H_{n,k_n^b}^H \right)^{-1} \) is the effective channel of user \( k_n^b \) in subchannel \( n \) and \( P_{\text{tot}} \) is the total available transmit power.

In the following, three different solutions for the above optimization problem are discussed expressing that the available resources of the system are exploited in a more efficient when normal users are scheduled within the \( N \) subchannels that are used for secrecy communication.

**III. THROUGHPUT MAXIMIZATION UNDER SECRECY RATE CONSTRAINT**

In this section, three different solutions of formulation (3) are discussed. The first one is based on the Lagrangian dual of (3). Specifically, the Lagrangian dual is decomposed in \( N \) independent (per subchannel), non-linear subproblems. By using some non-trivial transformations, each one of these subproblems is solved in an optimal way with linear complexity with respect to \( K \). Thus, an iterative resource

[1] Although this assumption can be naturally justified for the normal users and the secure user via a feedback channel, it may be insecure for the eavesdropper. However, there are scenarios where this assumption is reasonable such as when the eavesdropper is a legitimate user that may want unallowedly to wiretap the message of the secure user [2].
allocation algorithm is stated that provides a lower bound to the original problem. The other two solutions are based on decoupling and solving separately the subchannel and the power allocation subproblems. The subchannels are managed in a parallel way and they are allocated to users by following an exhaustive search approach (per subchannel) and a channel correlation based approach, respectively. Given the subchannel assignment, a power swapping procedure is triggered which is common for the two solutions and aims to adjust power allocation to fulfill the secrecy constraint of $b$.

### A. Dual Optimization

The partial Lagrangian dual optimization problem of (3) is

$$\max \sum_{n,b \neq 0} \sum_k w_{n,k} \left( \log (1 + p_{n,k}) + \lambda R_{n,k}^b \right)$$

where $\lambda \geq 0$ is the Lagrange multiplier of constraint (3b) and $\lambda R_{n,k}^b$ has been eliminated from objective (4a) since it is a constant term. By inspecting (4), it is clear that the overall optimization problem can be decomposed into $N$ independent subproblems, one per subchannel. The subproblem for subchannel $n$ can be written as

$$\max \sum_k w_{n,k} \left( \log (1 + p_{n,k}) + \lambda R_{n,k}^b \right)$$

with $\lambda \geq 0$ is the Lagrange multiplier of constraint (3b) and $\lambda R_{n,k}^b$ has been eliminated from objective (4a) since it is a constant term. By inspecting (4), it is clear that the overall optimization problem can be decomposed into $N$ independent subproblems, one per subchannel. The subproblem for subchannel $n$ can be written as

$$\max \sum_k w_{n,k} \left( \log (1 + p_{n,k}) + \lambda R_{n,k}^b \right)$$

The problem in (5) is still of combinatorial nature since the optimization is performed over the binary variables $w_{n,k}$ with $k = 1, \ldots, K$. Given the exclusive condition over $w_{n,k}$ (only one of them may be equal to 1), a way to solve (5) is to solve its $K$ 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 $w_{n,k} = 1$ and $w_{n,j} = 0, \forall j \neq k$. Thus, the optimization problem can be stated as

$$\max \sum_k w_{n,k} \left( \log (1 + p_{n,k}) + \lambda R_{n,k}^b \right)$$

which is linear with respect to $p_{n,b}$ and $p_{n,e}$. Thus, the problem in (6) is convex for a given $\mu$, since the objective function is concave and all the constraints are linear equations of $p_{n,b}$ and $p_{n,e}$. The following lemma is stated

**Lemma 1:** For a given $\mu$, the Karush-Kuhn-Tucker (KKT) conditions of (6) imply that the optimal power allocation $\left(p_{n,b}^\mu, p_{n,e}^\mu\right)$ is given by

$$p_{n,b}^\mu = \frac{P_{\text{tot}}/N + c_{n,b}}{c_{n,b} + \gamma_{n,b} c_{n,e}}$$

$$p_{n,e}^\mu = \frac{1}{\gamma_{n,e}}$$

where $\gamma_{n,e} = \frac{\alpha_{n,b}}{(2^{\nu - 1}) p_{n,b}^\mu}$.

**Proof:** See Appendix A.

Equation (7), gives the optimal power allocation for a given assignment as a function of parameter $\mu$. Nevertheless, back substitution of these expressions into problem (6) yields an analytical solution for $\mu$; hence, despite the fact that (6) is non-convex, it can be solved analytically to optimality.

**Lemma 2:** Let $\mu^\mu$ be the value of $\mu$ that maximizes problem (6). The range of $\mu$ is $0 < \log \left(1 + \frac{P_{\text{tot}} c_{n,e}}{N c_{n,b}}\right)$, while $\mu^\mu$ is either a real root of third degree polynomial (16) that lies in the specific range, or a boundary value that maximizes (6a).

**Proof:** See Appendix B.

Lemma 2 implies that by examining at most five values, we can obtain $\mu^\mu$, while Lemma 1 provides the optimal power allocation of problem (6) given $\mu^\mu$. Hence, based on Lemma 1, Lemma 2 and using a subgradient method to update the Lagrange multiplier $\lambda$ [12], we develop Algorithm 1 for the solution of the original problem (4).

**Algorithm 1: Subgradient Optimization Algorithm**

1. Set $\lambda^0 > 0$ and let $\delta$ be a small non-negative value.
2. Let $L$ denotes the number of iterations
3. for $i = 1, \ldots, L$ do
4. for $n = 1, \ldots, N$ do
5. for $k = 1, \ldots, K$ do
6. Solve the problem of eq. (6) for $w_{n,k} = 1$ and specify $p_{n,b}^\mu$ and $p_{n,e}^\mu$ by using Lemma 1 and Lemma 2.
7. end for
8. Set equal to 1 the variable $w_{n,k}$ that maximizes (5a).
9. end for
10. Given the subchannel and power allocation across all the subchannels, the Lagrange multiplier $\lambda$ is updated as $\lambda^{i+1} = \lambda^i - \delta \left( \sum_{n,k} w_{n,k} R_{n,k}^b - \bar{R} \right)$.
11. end for

### B. Decoupling Subchannel and Power Allocation

The main disadvantage of the dual optimization solution concerns the iterative procedure for updating the Lagrange multiplier $\lambda$, as the 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 described that aim to solve the problem in (3), without the involvement of the Lagrangian dual function. Both
schemes consist of two phases, where the subchannel and the power allocation subproblems have been decoupled. In the first phase, a subchannel assignment is performed aiming at maximizing the sum rate of normal users. To accomplish this task, an initial power allocation is also specified that is based on classic power waterfilling within each subchannel [5]. 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, and in parallel across subchannels, with the aim of adjusting power allocation to fulfill the secrecy constrain \( \bar{R} \) with equality.

In Algorithm 2, an exhaustive user search procedure is employed to allocate users in subchannels. For each subchannel, the sum \( \left( R_{n,k} + P_{n,k}^b \right) \) is calculated for each possible pair \((b,k)\) with \( k = 1, \ldots, K \), when subchannel’s power allocation follows a classic waterfilling algorithm [5]. The pair that leads to the maximum sum is selected to occupy the subchannel \( n \) and the resulting subchannel and power allocation are given as input to the power swapping procedure. In Algorithm 3, a simpler user selection rule is employed that is based on channel correlation between the eavesdropper and each user \( k \) with \( k = 1, \ldots, K \). Specifically, the user that is more aligned to the eavesdropper is selected to occupy subchannel \( n \). Again, the initial power allocation that is given as input to the power swapping procedure is based on the waterfilling algorithm.

**Algorithm 2: Maximum Sum Rate Subchannel Assignment**

1. **for** \( n = 1, \ldots, N \) **do**
2. The subchannel \( n \) is allocated to the user \( k_n^* = \arg \max_k \left( R_{n,k} + P_{n,k}^b \right) \) when \( P_{tot}/N \) is allocated by using power waterfilling over \( b \) and \( k \) [5].
3. **end for**
4. The secrecy rate of \( b \) is calculated and the Power Swapping procedure is triggered.

**Algorithm 3: Correlation-based Subchannel Assignment**

1. **for** \( n = 1, \ldots, N \) **do**
2. The subchannel \( n \) is allocated to the user \( k_n^* = \arg \max_k \left| \mathbf{h}_{n,k} \mathbf{h}_{n,e}^H \right| \).
3. The available amount of power \( (P_{tot}/N) \) is shared by using power waterfilling between \( b \) and \( k_n^* \) [5].
4. **end for**
5. The secrecy rate of \( b \) is calculated and the Power Swapping procedure is triggered.

From the above discussion, it can be seen that the proposed selection rules aim to exploit the orthogonality of ZFB transmission in order to provide a subchannel allocation that is highly probable to have high user rate and secrecy rate values. However, the two rules follow a different approach to balance between secrecy rate and user rate. By examining the quantity \( \left( R_{n,k} + P_{n,k}^b \right) \), Algorithm 1 emphasizes the role of the term \( p_{n,k} \) which specifies directly the objective function (3a) and affects the secrecy rate of \( b \) through the interference term in the denominator of \( \Gamma_{n,k,e} \). On the other hand, by aligning as much as possible the user with the eavesdropper, Algorithm 2 focuses on the role of the numerator of \( \Gamma_{n,k,e} \) and aims to control the secrecy rate firstly.

The power swapping procedure aims to fulfill the secrecy constraint of \( b \) and allocate as much as possible power to the selected users. Specifically, 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 \( \bar{R} \), the algorithm attempts to decrease (increase) \( p_{n,b} \) by an amount \( c_n \Delta P \) and increase (decrease) \( p_{n,k} \) by \( c_n \Delta P \). The secrecy rate is re-calculated and the power modification is adopted permanently if the secrecy approaches \( \bar{R} \). The process is repeated as long as the secrecy constraint is not violated.

**Algorithm 4: Power Swapping**

1. Let \( \Delta P > 0 \) be a small value and let \( S_N = \{1, \ldots, N\} \).
2. if \( \left( \sum_n R_{n,k}^b \geq \bar{R} \right) \) then
3. while \( \left( \sum_n R_{n,k}^b \geq \bar{R} \right) \) and \( S_N \neq \emptyset \) do
4. Let \( p_{n,k}^b = p_{n,k} - \Delta P c_n \) and \( p_{n,b}^t = p_{n,b} + \Delta P c_n \) \( \forall n \in S_N \). The subchannels where \( p_{n,b}^t \leq 0 \) are removed from \( S_N \).
5. The secrecy rate (let \( \bar{R} \)) is calculated by using \( (p_{n,k}^t, p_{n,b}^t) \) \( \forall n \in S_N \) and \( (p_{n,k}, p_{n,b}) \) \( \forall n \notin S_N \).
6. if \( \bar{R} \geq \bar{R} \) then
7. Set \( p_{n,k}^* = p_{n,k}^t \) and \( p_{n,b} = p_{n,b}^t \) \( \forall n \in S_N \).
8. else
9. exit while-loop.
10. **end if**
11. **end while**
12. **else**
13. while \( \left( \sum_n R_{n,k}^b \leq \bar{R} \right) \) and \( S_N \neq \emptyset \) do
14. Let \( p_{n,k}^t = p_{n,k} - \Delta P c_n \) and \( p_{n,b}^t = p_{n,b} + \Delta P c_n \) \( \forall n \in S_N \). The subchannels where \( p_{n,k}^t \leq 0 \) are removed from \( S_N \).
15. The secrecy rate (let \( \bar{R} \)) is calculated by using \( (p_{n,k}^t, p_{n,b}^t) \) \( \forall n \in S_N \) and \( (p_{n,k}, p_{n,b}) \) \( \forall n \notin S_N \).
16. if \( \bar{R} \leq \bar{R} \) then
17. Set \( p_{n,k}^* = p_{n,k}^t \) and \( p_{n,b} = p_{n,b}^t \) \( \forall n \in S_N \).
18. else
19. exit while-loop.
20. **end if**
21. **end while**
22. **end if**

**IV. Simulation Results**

In all the presented simulation examples, it is assumed that all the wireless channels follow a Rayleigh distribution. The number of subchannels is \( N = 6 \) and the secrecy constraint is set equal to \( \bar{R} = 2 \) Bits Per Channel Use (BPCU). The results are averaged over 10000 realizations.

In Fig. 1 the convergence of the subgradient optimization algorithm is shown versus the number of iterations/updates.
of Lagrange multiplier $\lambda$ for $K = 10$ and $P_{\text{tot}} = 15$ dB. Both the sum rate of the $K$ normal users and the secrecy rate of $b$ are shown. Four different step-size sequences have been used where $\delta$ has either a fixed value or 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.

Comparing maximum sum rate and correlation-based subchannel assignment, it seems that there is almost a constant gap between their performance. This happens because the first takes into consideration the normal user rate when it specifies the subchannel assignment. In the opposite, the correlation-based algorithm examines only the correlation between the user and the eavesdropper channel. The benefit of correlation-based algorithm is that it uses a simpler user selection rule that does not need a power calculation to specify subchannel assignment.

In Fig. 3 the sum rate of the normal users and the secrecy rate of $b$ are shown versus the number of normal users for $P_{\text{tot}} = 15$ dB. It can be seen, that all the three schemes exploit the multiuser diversity of the system. As before, subgradient optimization algorithm outperforms both the other two resource allocation schemes.

This paper has investigated the problem of sum rate maximization for a multiuser, multiantenna OFDMA channel when a secrecy rate constraint holds for a certain type of secure-sensitivity user. Three resource allocation algorithms have been presented. The first is based on the dual problem and it invokes some well-defined transformations to present an iterative resource allocation algorithm. The other two are based on the decoupling of the subchannel and the power allocation subproblems and the usage of heuristic rules to solve them. Numerical results show that the three solutions have different behavior with respect to optimality and they corroborate the benefits of integrating physical layer security to the general problem of resource allocation.

**APPENDIX A**

Let $\gamma_{n,\kappa} = \frac{c_{n,\kappa}}{1 + c_{n,\kappa}^2}$. By combining (6b) and (6c), the following inequalities hold

$$ p_{n,\kappa} = \gamma_{n,\kappa} p_{n,\kappa} - \frac{1}{\alpha_{n,\kappa}} \geq 0 $$

$$ 0 \leq p_{n,\kappa} \leq \frac{P_{\text{tot}}}{N + c_{n,\kappa}/\alpha_{n,\kappa}}. $$

By using (8) and eliminate the term $-\lambda \mu$ from the objective,
the problem of eq. (6) is written as
\[
\max_{p_{n,b}} \log \left( 1 + \gamma_n P_{n,b} - \frac{1}{\alpha_{n,k}} \right) + \lambda \log (1 + p_{n,b}),
\]
where maximization is performed only over \(p_{n,b}\) and \(p^b_{n,b}\) are given by
\[
p^b_{n,b} = \frac{\gamma_n}{\alpha_{n,k}}, \quad p_{n,b} = \frac{P_{\text{tot}}/N + c_{n/k}/\alpha_{n,k}}{c_{n,b} + \gamma_n c_{n,k}}.
\]
(9a)
(9b)

The Lagrangian of (9) is given as
\[
\mathcal{L} (\nu_1, \nu_2, p_{n,b}) = \log \left( 1 + \gamma_n P_{n,b} - \frac{1}{\alpha_{n,k}} \right) + \lambda \log (1 + p_{n,b}),
\]
+ \lambda \log (1 + p_{n,b}) - \nu_1 (p_{n,b} - p^b_{n,b}) + \nu_2 (p_{n,b} - p^b_{n,b}),
\]
where \(\nu_1, \nu_2 \geq 0\) are the Lagrange multipliers of the two inequalities of (9b). Let \(p^o_{n,b}\) be the optimal solution of (9) and \(\nu^o_1, \nu^o_2\) be the optimal points of its dual problem. The KKT conditions imply the following equations
\[
\nu^o_1 - \nu^o_2 = \frac{\gamma_n}{1 + \gamma_n P_{n,b} - 1/\alpha_{n,k}} + \frac{\lambda}{1 + p^o_{n,b}},
\]
(12a)
\[
p^o_{n,b} \leq p^b_{n,b} \leq \frac{p^o_{n,b}}{N c_{n,b}}.
\]
(12b)
\[
- \nu^o_1 (p^o_{n,b} - p^b_{n,b}) \leq 0
\]
(12c)
\[
\nu^o_2 (p^o_{n,b} - p^b_{n,b}) \leq 0
\]
(12d)
\[
\nu^o_1, \nu^o_2 \geq 0.
\]
(12e)

From (12c), (12d) it is clear that at most one of \(\nu_1, \nu_2\) may be nonzero, since \(p^o_{n,b} \neq p^b_{n,b}\) in a non-trivial case. Hence, the following cases should be considered
\[
1) \text{If } \nu^o_1 = \nu^o_2 = 0, \text{ then (12a) can be valid only for the trivial case of } \mu = 0.
\]
\[
2) \text{If } \nu^o_1 \neq 0 \text{ and } \nu^o_2 = 0, \text{ then the left hand of (12a) is nonpositive while the right hand is nonnegative. Thus this case is infeasible.}
\]
\[
3) \text{If } \nu^o_1 = 0 \text{ and } \nu^o_2 \neq 0, \text{ then } p^o_{n,b} = p^b_{n,b} \text{ from (12d).}
\]

\[
\text{APPENDIX B}
\]

Let us first establish the bounds of \(\mu\). From Eq. (6c), it is clear that \(\mu \geq 0\). An upper bound is established by substituting \(p^o_{n,b}\) into \(p^o_{n,k}\) in (7) and using the fact that \(p^o_{n,k} \geq 0\), yielding:
\[
\mu \leq \log \left( 1 + \frac{P_{\text{tot}}/N c_{n,k}}{c_{n,b}} \right).
\]
To obtain the optimal value of \(\mu\) in the derived range, let
\[
\beta = \frac{1}{\alpha_{n,k}}, \quad \epsilon = \alpha_{n,b} c_{n,k}/\alpha_{n,k} \quad \text{and } \delta = \beta c_{n,k} + P_{\text{tot}}/N.
\]
The \(p^o_{n,k}, p^o_{n,b}\) of (7) are written as
\[
p^o_{n,b} = \frac{x \delta}{x \epsilon + \delta}, \quad p^o_{n,k} = \frac{\alpha_{n,b} \delta}{x \epsilon + \delta}.
\]
where \(x = \log (2^\mu - 1)\). Let \(\zeta = x \epsilon + \delta\). Thus, the objective function (6a) becomes
\[
f (\mu) = \log \left( 1 + \frac{\alpha_{n,b} \delta}{\zeta} - \beta \right) + \lambda \log \left( 1 + \frac{\zeta - \epsilon}{\zeta} \right)
\]
- \lambda \log \left( 1 + \frac{\epsilon}{c_{n,b}} + \frac{\zeta}{c_{n,b}} \right).
\]
(14)

The stationary points of \(f (\mu)\) satisfy the following equation
\[
\begin{align*}
\frac{\partial f}{\partial \mu} = & - \frac{\alpha_{n,b} \delta}{\zeta (\alpha_{n,b} \delta + (1 - \beta) \zeta)} \\
& + \lambda \frac{c_{n,b}}{c_{n,b} + \alpha_{n,k} c_{n,k}} (1 + \frac{\delta}{c_{n,b}}) \\
& + \lambda \frac{\epsilon}{c_{n,b}} + \frac{\zeta}{c_{n,b}} = 0.
\end{align*}
\]
(15)

After some calculations (15) is written as a polynomial of third degree \(c_3 \zeta^3 + c_2 \zeta^2 + c_1 \zeta + c_0\), where
\[
c_3 = \lambda (1 - \beta) \left( 1 + \frac{\delta}{c_{n,b}} \right) \left( 1 + \frac{\epsilon}{c_{n,b}} \right)
\]
\[
c_2 = \alpha_{n,b} \beta \delta \left( 1 + \frac{\delta}{c_{n,b}} \right) \left( 1 + \lambda + 2 \lambda \frac{\delta}{c_{n,b}} (1 - \beta) \right)
\]
\[
c_1 = (c_{n,b} - \epsilon) \left( \alpha_{n,b} \beta \delta \left( 1 + \frac{\delta}{c_{n,b}} \right) - \lambda \frac{\delta}{c_{n,b}} \right)
\]
\[
c_0 = \alpha_{n,b} \beta \delta \left( 1 - \frac{\lambda}{c_{n,b}} \right) \left( 1 + \lambda \right).
\]

\textbf{ACKNOWLEDGMENT}

This work was supported in part by the University of Cyprus and in part by the project MIMOCORD 2.

\textbf{REFERENCES}


2The MIMOCORD research project is implemented within the framework of the Action “Supporting Postdoctoral Researchers” of the Operational Program “Education and Lifelong Learning” (Actions Beneficiary: General Secretariat for Research and Technology), and is co-financed by the European Social Fund (ESF) and the Greek State.