Power and Subcarrier Allocation for Physical-Layer Security in OFDMA-Based Broadband Wireless Networks

Xiaowei Wang, Meixia Tao, *Senior Member, IEEE*, Jianhua Mo, and Youyun Xu, *Senior Member, IEEE*

***Abstract*—Providing physical-layer security for mobile users in future broadband wireless networks is of both theoretical and practical importance. In this paper, we formulate an analytical framework for resource allocation in a downlink orthogonal frequency-division multiple access (OFDMA)-based broadband network with coexistence of secure users (SUs) and normal users (NUs). The SUs require secure data transmission at the physical layer while the NUs are served with conventional best-effort data traffic. The problem is formulated as joint power and subcarrier allocation with the objective of maximizing average aggregate information rate of all NUs while maintaining an average secrecy rate for each individual SU under a total transmit power constraint for the base station. We solve this problem in an asymptotically optimal manner using dual decomposition. Our analysis shows that an SU becomes a candidate competing for a subcarrier only if its channel gain on this subcarrier is the largest among all and exceeds the second largest by a certain threshold. Furthermore, while the power allocation for NUs follows the conventional water-filling principle, the power allocation for SUs depends on both its own channel gain and the largest channel gain among others. We also develop a suboptimal algorithm to reduce the computational cost. Numerical studies are conducted to evaluate the performance of the proposed algorithms in terms of the achievable pair of information rate for NU and secrecy rate for SU at different power consumptions.**

***Index Terms*—Dual decomposition, orthogonal frequency-division multiple access (OFDMA), physical-layer security, secrecy rate.**

I. Introduction

SECURITY is a crucial issue in wireless systems due to the broadcasting nature of wireless radio waves. It also attracts increasing attention because of the growing demand of private data transmission such as online transaction and personal medical information. Traditionally, cryptography undertakes most of security work on upper layers, which is based on computational complexity. In the standard five-layered protocol stack, security approaches are designed on every layer except the physical layer. Thus, establishing physical-layer security is of both theoretical and practical significance. In this study, we aim to provide physical-layer security for mobile users in future broadband wireless networks and formulate an analytical strategy for resource allocation to achieve this goal.

Information-theoretic security provides possibility of secure transmission in the physical layer. By exploring secrecy capacity and coding technique, messages can be sent without being decoded by any eavesdropper. Information-theoretic security originates from Shannon's notion of perfect secrecy [1]. He presented the general mathematical structure and properties of secrecy systems. The concept of information-theoretic security and wiretap channel was defined by Wyner [2] and later by Csiszár and Körner [3], who proved the existence of channel coding that makes the wiretapper to obtain no information about the transmitted data. Then the study on information-theoretic security is extended to various kinds of channels. Leung *et al.* [4] focused on Gaussian wiretap channel and showed that secrecy capacity is the difference between the capacities of the main and wiretap channels. Barros *et al.* [5] studied secrecy capacity in slow fading channels and introduced outage into secrecy issues for the first time. In [6], Li *et al.* investigated independent parallel channels and proved that the secrecy capacity of the system is the summation of the secrecy rate achieved on each independent channel. More recently, Zhu *et al.* [7] studied the cooperative power control for secret communications by using artificial noise in symmetric Gaussian interference channel.

Orthogonal frequency-division multiple access (OFDMA) has evolved as a leading technology in future broadband wireless networks, such as 3GPP Long-Term Evolution (LTE) and IEEE 802.16 WiMAX. It enables efficient transmission of a wide variety of data traffic by optimizing power, subcarrier, or bit allocation among different users. In the past decade, tremendous research results have been reported on the resource allocation of OFDMA downlink networks, such as [8]–[13], where the problem formulation differs mostly in optimization objectives and constraints. The work in [8] appeared as one of the earliest results on margin adaptation for minimizing the total transmit power with individual user rate requirements. Jang and Lee in [9] studied rate adaptation for system sum-rate maximization subject to a total transmit power constraint. In

Manuscript received September 15, 2010; revised May 24, 2011; accepted May 24, 2011. Date of publication June 09, 2011; date of current version August 17, 2011. This work was supported in part by the National Natural Science Foundation of China (60902019), in part by the Joint Research Fund for Overseas Chinese, Hong Kong and Macao Young Scholars (61028001), in part by the Shanghai Pujiang Talent Program (09PJ1406000), and in part by the Innovation Program of Shanghai Municipal Education Commission (11ZZ19). This work was presented in part at IEEE ICC'11, Kyoto, Japan, June 2011. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Wade Trappe.

X. Wang, M. Tao, and J. Mo are with the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: wangxiaowei@sjtu.edu.cn; mxtao@sjtu.edu.cn; mjh@sjtu.edu.cn).

Y. Xu is with the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China, and also with the Nanjing Institute of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China (e-mail: yyxu@vip.sina.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2011.2159206

[10], Tao *et al.* considered a heterogenous network and studied the power and subcarrier allocation problem for maximizing the sum-rate of nondelay-constrained users while satisfying the basic rate requirement of each delay-constrained user under a total transmit power constraint. Cross-layer optimizations considering utility-function and traffic arrival distribution for OFDMA networks were also studied in several works, e.g., [11]–[13]. Nevertheless, none of these works take into account the security issue, which attracts increasing attention recently in wireless networks as aforementioned.

Secrecy or private message exchanges between mobile users and the base station (BS) are generally needed in present and future wireless systems. Hence, it is essential to consider the security demand when assigning radio resources to all users. In [14], the authors made the initial attempt to find the power and subcarrier allocation in an OFDM-based broadcast channel with the objective of maximizing sum secrecy rate. However, this work is confined to two users only and does not consider the coexistence of other types of users.

In this study, we introduce two types of users according to their secrecy demands in downlink OFDMA-based broadband networks. The first type of users have physical-layer security requirements and should be served at a nonzero secrecy rate. These users are referred to as *secure users* (SUs). The other type of users have no confidential messages and do not care about security issues. Their traffic is treated in a best-effort way. These users are regarded as *normal users* (NUs). All SUs and NUs are legitimate users in the network and have their own data transmission with the BS. They are completely honest and always feedback the correct channel condition to the BS. Moreover, each of them is equipped with single antenna and only passively listens, rater than actively attacking using, for example, multiple antennas or colluding, when being a potential eavesdropper of the confidential messages for SUs. The aim of this study is to investigate the power and subcarrier allocation problem in such an OFDMA broadband network where the BS needs to simultaneously serve multiple SUs and multiple NUs.

The resource allocation problem in this paper possesses major differences compared with those without secrecy constraint, owing to the coexistence of SUs and NUs. First, the legitimate subcarriers to be assigned to an SU can only come from the subcarrier set on which this SU has the best channel condition among all the users. This is because for each SU, any other user in the same network is a potential eavesdropper. The authors in [15] showed that the secrecy capacity of a fading channel in the presence of multiple eavesdroppers is the difference between the capacities of the main channel and the eavesdropper channel with the largest channel gain among all eavesdroppers. As a result, a nonzero secrecy rate on a subcarrier is possible to achieve only if the channel gain of the SU on this subcarrier is the largest among all the users. Note that this observation is very different from that in conventional OFDMA networks where a user is still able to occupy some subcarriers and transmit signals over them even if its channel gains on these subcarriers are not the largest. Second, even if an SU has the best channel condition on a given subcarrier, assigning this subcarrier to the SU may not be the optimal solution from the system perspective when the quality of service of NUs is taken into account. This is due to the fact that the achievable secrecy rate of channels with Gaussian noise is the subtraction of two logarithmic functions [4], i.e.,

$$C_s = [\log(1 + P\alpha_M) - \log(1 + P\alpha_E)]^+ \tag{1}$$

where P is the transmit power, α_M and α_E are the channel-to-noise ratios (CNRs) of the main channel and eavesdropper channel, respectively, and $[x]^+ = \max\{0, x\}$. In the case of large P, if the gap between α_M and α_E is not large enough, the achievable secrecy rate can be rather low. In this case, it may be more beneficial for the system to assign the subcarrier to an NU for transmitting nonconfidential data traffic.

Our goal is to find an optimal power and subcarrier allocation policy to maximize the long-term aggregate information rate of all NUs while maintaining a target average secrecy rate of each individual SU under a total power constraint. Since a nonzero instantaneous secrecy rate for each SU cannot be guaranteed all the time due to channel fading, we assume that the transmission of confidential messages can wait until the channel condition of the SU becomes favorable. As a result, the average secrecy rate requirement instead of instantaneous secrecy rate requirement is considered for each SU. In addition, to make our problem more complete, both long-term average and peak total transmit power constraints at the BS are considered.

Finding the optimal power and subcarrier allocation policy with respect to channel conditions of all users in the considered system is a functional optimization problem. We solve this problem in dual domain using the decomposition method in an asymptotically optimal manner. In particular, the joint subcarrier assignment and power allocation at given dual variables can be determined on a per-subcarrier basis. Our analysis shows that for each subcarrier, if the user with the largest channel gain belongs to the category of NUs, then this subcarrier will be assigned to this NU. Otherwise if it is an SU, then this subcarrier will only be assigned to this SU when its channel gain exceeds the second-largest channel gain by a certain threshold. This analytical finding agrees with the intuition mentioned above. It is also shown that while the power allocation across the subcarriers assigned for NUs follows the standard water-filling principle, the power allocation for SUs depends on both the SUs' channel gain and the second-largest channel gain. Based on the insight derived from the optimal policy, we further propose a low-complexity suboptimal power and subcarrier allocation algorithm. First, we assign resources to only SUs as if all the NUs were pure eavesdroppers without data traffic. Then, the residual resources are allocated to NUs. The underlying mechanism of this algorithm is to decouple the joint update of the Lagrangian multipliers as required in the optimal algorithm so as to acquire a linear complexity in the numbers of users and subcarriers.

The rest of the paper is organized as follows. Section II describes the system model and problem formulation. In Section III, we introduce a dual decomposition method to solve this problem under average power constraint. The same problem under peak power constraint is solved in Section IV. An efficient suboptimal resource allocation algorithm is proposed in Section V. Section VI presents the performance of

the proposed scheme via simulation. Finally, we conclude this paper in Section VII.

II. System Model and Problem Formulation

We consider the downlink of an OFDMA broadband network with one BS and K mobile users. The first K_1 users, indexed as $k = 1, \ldots, K_1$, are SUs. Each of them has confidential messages to communicate with the BS and, therefore, demands a secrecy rate no lower than a constant C_k, for $1 \leq k \leq K_1$. The other $K - K_1$ users, indexed as $k = K_1 + 1, \ldots, K$, are NUs and demand service of best-effort traffic. NUs and SUs are all assumed to eavesdrop the legitimate channel noncooperatively and each has only one antenna. The communication link between the BS and each user is modeled as a slowly time-varying frequency-selective fading channel. The channel coefficients remain approximately unchanged during each time frame, but vary from one frame to another in a random manner. The total bandwidth is logically divided into N orthogonal subcarriers by using OFDMA with each experiencing slow fading. As a central controller, the BS knows the channel information of all users, finds the allocation policy, and then assigns power and subcarriers to mobile users at each transmission frame according to the instantaneous channel state information (CSI) of all users. The total transmit power of the BS is subject to either a long-term average or peak constraint, both denoted as power constraint P. We assume full statistical knowledge and instantaneous knowledge of CSI at the BS and that each subcarrier is occupied only by one user at each time frame to avoid multiuser interference.

Let $\alpha_{k,n}$ denote the CNR of user k on subcarrier n for all k and n. The system channel condition is denoted by the set $\boldsymbol{\alpha} = \{\alpha_{k,n}\}$, which has a joint probability density function of $f(\boldsymbol{\alpha})$. Let $\boldsymbol{\Omega}(\boldsymbol{\alpha}) = \{\Omega_1, \ldots, \Omega_K\}$ denote the subcarrier assignment policy with respect to the system channel condition $\boldsymbol{\alpha}$, where Ω_k represents the set of subcarriers assigned to user k. Furthermore, let $\boldsymbol{p}(\boldsymbol{\alpha}) = \{p_{k,n}, \forall\, k, \forall\, n\}$ denote the corresponding power allocation policy, where $p_{k,n}$ represents the transmit power allocated to user k on subcarrier n. We next present the achievable secrecy rate of SU and the achievable information rate of NU separately, under a given resource allocation policy $\{\boldsymbol{p}(\boldsymbol{\alpha}), \boldsymbol{\Omega}(\boldsymbol{\alpha})\}$.

For SU k, $1 \leq k \leq K_1$, since the subcarriers are parallel to each other, the achievable secrecy rate at a given channel realization is the summation of those achieved on each subcarrier in the presence of $K - 1$ potential eavesdroppers, and can thus be expressed as [15]

$$r_k^s = \sum_{n \in \Omega_k} r_{k,n}^s \tag{2}$$

where

$$r_{k,n}^s = \left[\log(1 + p_{k,n}\alpha_{k,n}) - \log(1 + p_{k,n}\beta_{k,n})\right]^+. \tag{3}$$

Here $\beta_{k,n} = \max\limits_{k' \neq k} \alpha_{k',n}$ denotes the largest CNR among all the users except user k on subcarrier n. The expression (3) means that nonzero instantaneous secrecy rate for SU k on a subcarrier is possible to achieve only if its CNR on this subcarrier is the largest among all the K users. On the other hand, the achievable information rate of NU k for $K_1 < k \leq K$ is given by

$$r_k = \sum_{n \in \Omega_k} r_{k,n} \tag{4}$$

where

$$r_{k,n} = \log(1 + p_{k,n}\alpha_{k,n}). \tag{5}$$

The problem is to find the optimal power and subcarrier allocation policies $\{\boldsymbol{p}(\boldsymbol{\alpha}), (\boldsymbol{\Omega}(\boldsymbol{\alpha})\}$ so as to maximize the average aggregate information rate of the $K - K_1$ NUs while satisfying the individual average secrecy rate requirement for each of the K_1 SUs. We consider both peak and average power constraints. This functional optimization problem can be expressed as

$$\max_{\{\boldsymbol{\Omega}(\boldsymbol{\alpha}), \boldsymbol{p}(\boldsymbol{\alpha})\}} \mathbb{E}\left(\sum_{k=K_1+1}^{K} \omega_k \sum_{n \in \Omega_k} r_{k,n}\right) \tag{6}$$

$$\text{subject to } \mathbb{E}\left(\sum_{n \in \Omega_k} r_{k,n}^s\right) \geq C_k,\ 1 \leq k \leq K_1 \tag{7}$$

$$\sum_{k=1}^{K} \sum_{n \in \Omega_k} p_{k,n} \leq P \tag{8}$$

$$or\ \mathbb{E}\left(\sum_{k=1}^{K} \sum_{n \in \Omega_k} p_{k,n}\right) \leq P \tag{9}$$

$$p_{k,n} \geq 0, \forall\, k, n \tag{10}$$

$$\Omega_1 \cup \cdots \cup \Omega_K \subseteq \{1, 2, \ldots, N\}$$

$$\Omega_1, \ldots, \Omega_K \text{ are disjoint} \tag{11}$$

where notation $\mathbb{E}$ represents statistical average over the joint distribution of channel conditions, i.e., $\mathbb{E}[\cdot] = \int (\cdot) f(\boldsymbol{\alpha}) d\boldsymbol{\alpha}$, and ω_k is a weighting parameter of NU k, representing its quality-of-service demand. Constraint (8) is the peak total power constraint while (9) is the average total power constraint.

In the above formulation, we impose the long-term average secrecy rate constraints because instantaneous nonzero secrecy rate cannot be guaranteed at every frame. It is possible due to channel fading that in a certain frame, an SU is the best user on none of the N subcarriers and thus obtains a zero secrecy rate. Therefore, power and subcarrier allocation should be adapted every frame to meet a long-term secrecy rate requirement.

III. Optimal Resource Allocation Under Average Power Constraint

In this section, we solve the problem with the average power constraint formulated above. It is not difficult to observe that this problem satisfies the time-sharing condition introduced in [16]. That is, the objective function is concave and constraint (7) is convex given that $r_{k,n}^s$ is concave in $p_{k,n}$ and that the integral preserves concavity. Therefore, similar to the OFDMA networks without secrecy constraint, we can use a dual approach for resource allocation and the solution is asymptotically optimal for a large enough number of subcarriers.

Define $\mathcal{P}(\boldsymbol{\alpha})$ as a set of all possible nonnegative power parameters $\{p_{k,n}\}$ at any given system channel condition $\boldsymbol{\alpha}$ satisfying that for each subcarrier n only one $p_{k,n}$ is positive.

This definition takes into account both the power constraint (10) and the exclusive subcarrier allocation constraint (11). The Lagrange dual function is thus given by

$$\begin{aligned} & g(\boldsymbol{\mu},\lambda) \\ &= \max_{\{p_{k,n}\}\in\mathcal{P}(\boldsymbol{\alpha})} \left\{ \mathbb{E}\left[\sum_{k=K_1+1}^{K}\omega_k\sum_{n=1}^{N} r_{k,n}\big(p_{k,n}(\boldsymbol{\alpha}),\boldsymbol{\alpha}\big)\right] \right. \\ &\qquad + \sum_{k=1}^{K_1}\mu_k\left(\mathbb{E}\left[\sum_{n=1}^{N} r^s_{k,n}\big(p_{k,n}(\boldsymbol{\alpha}),\boldsymbol{\alpha}\big)\right]-C_k\right) \\ &\qquad \left. + \lambda\left(P-\mathbb{E}\left[\sum_{k=1}^{K}\sum_{n=1}^{N} p_{k,n}(\boldsymbol{\alpha})\right]\right)\right\} \end{aligned} \tag{12}$$

where $\boldsymbol{\mu}=(\mu_1,\ldots,\mu_{K_1})\succeq 0$ and $\lambda\geq 0$ are the Lagrange multipliers for the constraints (7) and (9) respectively, and notation $\mathbb{E}$ stands for the statistical average over all channel conditions $\boldsymbol{\alpha}$. Then the dual problem of the original problem (6) is given by

$$\begin{aligned} &\min\ g(\boldsymbol{\mu},\lambda) \\ &s.t.\ \boldsymbol{\mu}\succeq 0,\lambda\geq 0. \end{aligned} \tag{13}$$

Observing (12), we find that the maximization in the Lagrange dual function can be decomposed into N independent subfunctions as

$$g(\boldsymbol{\mu},\lambda)=\sum_{n=1}^{N} g_n(\boldsymbol{\mu},\lambda)-\sum_{k=1}^{K_1}\mu_k C_k+\lambda P \tag{14}$$

where

$$g_n(\boldsymbol{\mu},\lambda)=\max_{\{p_{k,n}\}\in\mathcal{P}(\boldsymbol{\alpha})}\mathbb{E}\left[J_n\left(\boldsymbol{\mu},\lambda,\boldsymbol{\alpha},\{p_{k,n}\}_k\right)\right] \tag{15}$$

with

$$\begin{aligned} & J_n(\boldsymbol{\mu},\lambda,\alpha,\{p_{k,n}\}_k) \\ &= \sum_{k=K_1+1}^{K}\omega_k r_{k,n} \\ &\quad + \sum_{k=1}^{K_1}\mu_k r^s_{k,n}-\lambda\sum_{k=1}^{K} p_{k,n}. \end{aligned} \tag{16}$$

For fixed $\boldsymbol{\mu}$ and λ, the maximization problem in (15) is a single-carrier multiple-user power allocation problem. Given that the expectation $\mathbb{E}$ is over the channel condition $\boldsymbol{\alpha}$, we can obtain the maximum by directly maximizing the function (16). Based on the above subproblems, we now discuss the optimality conditions of power allocation and subcarrier assignment, respectively, in Sections III-A and III-B.

A. Optimality Condition of Power Allocation

The function in (16) is concave in $p_{k,n}$ and hence its maximum value can be found by using Karush–Kuhn–Tucker (KKT) conditions. Specifically, suppose that subcarrier n is assigned to user k; then taking the partial derivation of $J_n(\boldsymbol{\mu},\lambda,\alpha,\{p_{k,n}\}_k)$ with respect to $p_{k,n}$ and equating it to zero, we obtain the following optimality condition of power allocation:

$$\begin{aligned} & p^*_{k,n} \\ &= \frac{1}{2}\left[\sqrt{\left(\frac{1}{\alpha_{k,n}}-\frac{1}{\beta_{k,n}}\right)^2+\frac{4\mu_k}{\lambda}\left(\frac{1}{\beta_{k,n}}-\frac{1}{\alpha_{k,n}}\right)}\right. \\ &\qquad \left.-\left(\frac{1}{\alpha_{k,n}}+\frac{1}{\beta_{k,n}}\right)\right]^+ \end{aligned} \tag{17}$$

for $k=1,\ldots,K_1$, and

$$p^*_{k,n}=\left[\frac{\omega_k}{\lambda}-\frac{1}{\alpha_{k,n}}\right]^+ \tag{18}$$

for $k=K_1+1,\ldots,K$.

We can conclude from (18) that the optimal power allocation for NUs follows the conventional water-filling principle and the water level is determined by both the weight of the NU and the average power constraint. On the other hand, it is seen from (17) that the optimal power allocation for SUs has the same form as the result obtained in [17] for conventional fading wiretap channels, as expected. By observing (17) closely, it is also seen that the SU must satisfy $\alpha_{k,n}-\beta_{k,n}\geq\lambda/\mu_k$ in order to be allocated nonzero power. This means that the power allocation for SU depends on both the channel gain of the SU and the largest channel gain among all the other users. Moreover, it is nonzero only if the former exceeds the latter by the threshold λ/μ_k.

B. Optimality Condition of Subcarrier Assignment

Next, substituting (17) and (18) into (15) and comparing all the K possible user assignments for each subcarrier n, we obtain

$$g_n(\boldsymbol{\mu},\lambda)=\mathbb{E}\left[\max_{1\leq k\leq K} H_{k,n}\left(\boldsymbol{\mu},\lambda,\alpha\right)\right] \tag{19}$$

where the function $H_{k,n}(\cdot)$ is defined as

$$H_{k,n}\left(\boldsymbol{\mu},\lambda,\alpha\right)=\mu_k\log\left(\frac{1+p^*_{k,n}\alpha_{k,n}}{1+p^*_{k,n}\beta_{k,n}}\right)-\lambda p^*_{k,n} \tag{20}$$

for $1\leq k\leq K_1$ and $p^*_{k,n}$ defined in (17), and

$$H_{k,n}\left(\boldsymbol{\mu},\lambda,\alpha\right)=\omega_k\left[\log\frac{\omega_k\alpha_{k,n}}{\lambda}\right]^+-\left[\omega_k-\frac{\lambda}{\alpha_{k,n}}\right]^+ \tag{21}$$

for $K_1<k\leq K$.

From (19) it is observed that the function $H_{k,n}$ defined in (20) and (21) plays an important role in determining the optimal subcarrier assignment. Specifically, for any given dual variables $\boldsymbol{\mu}$ and λ, the subcarrier n will be assigned to the user with the maximum value of $H_{k,n}$. That is, the optimality condition for subcarrier assignment is given by

$$k^*_n=\arg\max_k H_{k,n},\quad \text{for } n=1,\ldots,N. \tag{22}$$

Note that for $k=K_1+1,\ldots,K$, $H_{k,n}$ is monotonically increasing in $\alpha_{k,n}$. Therefore, the NU with larger $\alpha_{k,n}$ is more

likely to be assigned subcarrier n. We also notice that for $k = 1, \ldots, K_1$, $H_{k,n} > 0$ only when SU k has the largest $\alpha_{k,n}$ among all the K users and satisfies $\alpha_{k,n} > \beta_{k,n} + \lambda/\mu_k$. Otherwise, $H_{k,n} = 0$. In other words, an SU becomes a candidate for subcarrier n only if its CNR is the largest and is λ/μ_k larger than the second largest.

C. Dual Update

Substituting $g_n(\boldsymbol{\mu}, \lambda)$ for $n = 1, \ldots, N$ into (14), we obtain $g(\boldsymbol{\mu}, \lambda)$. As studied in [18], the dual problem (13) is always convex and can be minimized by simultaneously updating $(\boldsymbol{\mu}, \lambda)$ using gradient descent algorithms. However, note that $g(\boldsymbol{\mu}, \lambda)$ is not differentiable due to the discontinuity of subcarrier assignment and hence its gradient does not exist. Nevertheless, we present a subgradient of $g(\boldsymbol{\mu}, \lambda)$ as follows:

$$\Delta\mu_k = \mathbb{E}\left[\sum_{n=1}^{N} r_{k,n}^{s*}\right] - C_k \tag{23}$$

$$\Delta\lambda = P - \mathbb{E}\left[\sum_{k=1}^{K}\sum_{n=1}^{N} p_{k,n}^{*}\right] \tag{24}$$

where $r_{k,n}^{s*}$ is obtained by substituting the optimal $p_{k,n}^{*}$ into (3). A brief proof is as follows.

From the expression of $g(\boldsymbol{\mu}, \lambda)$ in (12), we get

$$\begin{aligned}
&g(\boldsymbol{\mu}', \lambda') \\
&\geq \mathbb{E}\left[\sum_{k=K_1+1}^{K} \omega_k \sum_{n=1}^{N} r_{k,n}^{*}\right] + \sum_{k=1}^{K_1} \mu_k' \left(\mathbb{E}\left[\sum_{n=1}^{N} r_{k,n}^{s*}\right] - C_k\right) \\
&\quad + \lambda' \left(P - \mathbb{E}\left[\sum_{k=1}^{K}\sum_{n=1}^{N} p_{k,n}^{*}\right]\right) \\
&= g(\boldsymbol{\mu}, \lambda) + \sum_{k=1}^{K_1} (\mu_k' - \mu_k) \left(\mathbb{E}\left[\sum_{n=1}^{N} r_{k,n}^{s*}\right] - C_k\right) \\
&\quad + (\lambda' - \lambda) \left(P - \mathbb{E}\left[\sum_{k=1}^{K}\sum_{n=1}^{N} p_{k,n}^{*}\right]\right).
\end{aligned} \tag{25}$$

The results in (23) and (24) are thus proved by the definition of subgradient.

In the case when the numerical computation of statistical average is too complex, we can change to time average when the channel fading process is ergodic. Specifically,

$$\mathbb{E}\left[\sum_{n=1}^{N} r_{k,n}^{s*}\right] = \lim_{t\to\infty} \frac{1}{t} \sum_{t'=1}^{t}\sum_{n=1}^{N} r_{k,n}^{s*}(t') \tag{26}$$

$$\mathbb{E}\left[\sum_{k=1}^{K}\sum_{n=1}^{N} p_{k,n}^{*}\right] = \lim_{t\to\infty} \frac{1}{t} \sum_{t'=1}^{t}\sum_{k=1}^{K}\sum_{n=1}^{N} p_{k,n}^{*}(t'). \tag{27}$$

After finding the optimal dual variables $\{\mu_k^*\}$ and λ^*, the optimal power and subcarrier allocation policy is then obtained by substituting them into the optimality conditions (17), (18), and (22).

D. Discussion of Feasibility

To make the above optimization problem feasible, the secrecy requirement C_k for each SU must be chosen properly according to the total power constraint P. In this subsection, we will derive an upper bound of average secrecy rate each SU can obtain. If C_k is set equal or greater than this upper bound, the secrecy requirement cannot be satisfied and thus this optimization problem is not feasible.

For simplicity, we assume that the channel conditions of all the K users on each subcarrier are independently and identically distributed and follow Rayleigh distribution. Then, each SU has a probability of $1/K$ to be the best user on each subcarrier. As a result, we can write the average achievable secrecy rate of each SU k as

$$\bar{R}_k^s = \frac{N}{K}\mathbb{E}\left[r_{k,n}^{s}\right]. \tag{28}$$

Assuming that the transmit power goes to infinity, the maximum per-subcarrier secrecy rate $r_{k,n}^{s}$ can be obtained as

$$\lim_{p_{k,n}\to\infty} r_{k,n}^{s} = \left[\log\frac{\alpha_{k,n}}{\beta_{k,n}}\right]^{+}. \tag{29}$$

Therefore, an upper bound on $\bar{R}_k^s$ can be theoretically derived using order statistics as

$$\begin{aligned}
\bar{R}_k^s &\leq \frac{N}{K}\int_0^\infty\int_{\nu_2}^\infty log\frac{\nu_1}{\nu_2} f(\nu_1,\nu_2)d\nu_1 d\nu_2 \\
&= \frac{N}{K}\int_0^\infty\int_{\nu_2}^\infty N(N-1)\left(1-e^{-\nu_2/\rho}\right)^{N-2} \\
&\quad \times \frac{1}{\rho}e^{-\nu_2/\rho}\frac{1}{\rho}e^{-\nu_1/\rho}\log\frac{\nu_1}{\nu_2}d\nu_1 d\nu_2 \\
&= \frac{N}{K}\int_0^\infty\int_{\nu_2}^\infty N(N-1)\left(1-e^{-\nu_2/\rho}\right)^{N-2} \\
&\quad \times \frac{1}{\rho}e^{-\nu_2/\rho}\frac{1}{\rho}e^{-\nu_1/\rho}\log\nu_1 d\nu_1 d\nu_2 \\
&\quad - \frac{N}{K}\int_0^\infty\int_{\nu_2}^\infty N(N-1)\left(1-e^{-\nu_2/\rho}\right)^{N-2} \\
&\quad \times \frac{1}{\rho}e^{-\nu_2/\rho}\frac{1}{\rho}e^{-\nu_1/\rho}\log\nu_2 d\nu_1 d\nu_2.
\end{aligned} \tag{30}$$

In the above derivation, ν_1 and ν_2 denote the largest and second largest CNRs on a given subcarrier, $f(\nu_1, \nu_2)$ is the joint probability density function of ν_1 and ν_2, which can be obtained through order statistics. We assume Rayleigh fading and the probability distribution function of CNR is $f(x) = (1/\rho)e^{-x/\rho}$, where ρ is the mean value. Since it is difficult to further express the integrals in (30) in a closed form, we use numerical integration to get the upper limit value of secrecy rate. As an example, when the parameters are set to be $N = 64$, $K = 8$, $K_1 = 4$, and $\rho = 1$, we obtain $\bar{R}_k^s \leq 3.5$ nat/OFDMA symbol. In this case, when the secrecy rate constraint $C_k > 3.5$, the problem becomes infeasible.

IV. Optimal Resource Allocation Under Peak Power Constraint

In Section III, we solved the optimization problem under long-term average power constraint. In this section, we solve the same problem (6) but under peak power constraint. Note that the peak power constraint is more suitable for practical systems as the BS usually has a maximum radiation power. By using the similar definition of power parameter set $\mathcal{P}(\boldsymbol{\alpha})$ as in

the previous section, the associated Lagrange dual function is given by (31), shown at the bottom of the page. The difference from the dual function with average power constraint in (12) is that the dual variable $\lambda(\boldsymbol{\alpha})$ associated with the power constraint (9) is a function of the system channel condition $\boldsymbol{\alpha}$.

This dual function can be similarly decomposed into N independent subfunctions with each given by

$$g_n(\boldsymbol{\mu}, \lambda(\boldsymbol{\alpha})) = \max_{\{p_{k,n}\}\in\mathcal{P}(\boldsymbol{\alpha})} \mathbb{E}\left[J_n\left(\boldsymbol{\mu}, \lambda(\boldsymbol{\alpha}), \boldsymbol{\alpha}, \{p_{k,n}\}_k\right)\right] \quad (32)$$

with

$$J_n\left(\boldsymbol{\mu}, \lambda(\boldsymbol{\alpha}), \boldsymbol{\alpha}, \{p_{k,n}\}_k\right) = \sum_{k=K_1+1}^{K} \omega_k r_{k,n} + \sum_{k=1}^{K_1} \mu_k r_{k,n}^s - \lambda(\boldsymbol{\alpha}) \sum_{k=1}^{K} p_{k,n}. \quad (33)$$

Given that the order of expectation operation and the maximum operation can be reversed, we can obtain $g_n(\boldsymbol{\mu}, \lambda(\boldsymbol{\alpha}))$ by maximizing the function (33) for every $\alpha_{k,n}$.

Suppose that subcarrier n is assigned to user k. Taking the partial derivative of $J_n(\boldsymbol{\mu}, \lambda(\boldsymbol{\alpha}), \boldsymbol{\alpha}, \{p_{k,n}\}_k)$ with respect to $p_{k,n}$ and equating it to zero, we obtain the optimality conditions of power allocation

$$p_{k,n}^* = \frac{1}{2}\left[\sqrt{\left(\frac{1}{\alpha_{k,n}} - \frac{1}{\beta_{k,n}}\right)^2 + \frac{4\mu_k}{\lambda(\boldsymbol{\alpha})}\left(\frac{1}{\beta_{k,n}} - \frac{1}{\alpha_{k,n}}\right)} - \left(\frac{1}{\alpha_{k,n}} + \frac{1}{\beta_{k,n}}\right)\right]^+ \quad (34)$$

for $k = 1, \ldots, K_1$, and

$$p_{k,n}^* = \left[\frac{\omega_k}{\lambda(\boldsymbol{\alpha})} - \frac{1}{\alpha_{k,n}}\right]^+ \quad (35)$$

for $k = K_1 + 1, \ldots, K$.

Comparing (34) and (35) with (17) and (18), we observe that the optimal power allocations under the average power constraint and the peak power constraint have similar structure. The difference lies in the dual variable that controls total power. For average power constraint, λ is a constant for all $\alpha_{k,n}$. For peak power constraint, this variable changes with $\{\alpha_{k,n}\}$.

The rest of the algorithm is similar to the problem in the previous section. The difference is that the subgradient to update $\lambda(\boldsymbol{\alpha})$ is changed to

$$\Delta\lambda(\boldsymbol{\alpha}) = P - \sum_{k=1}^{K}\sum_{n=1}^{N} p_{k,n}^*(\boldsymbol{\alpha}). \quad (36)$$

V. Suboptimal Power and Subcarrier Allocation Algorithm

The complexity of the optimal power and subcarrier allocation policy presented in Sections III and IV mainly lies in the joint optimization of Lagrange multipliers $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_{K_1})$ and λ. If we choose the ellipsoid method, it converges in $\mathcal{O}((K_1 + 1)^2 \log(1/\epsilon))$ iterations where ϵ is the accuracy [18]. Thus, if the number of SU is large, the computational complexity may not be favorable for practical implementation. Based on the insight derived from the optimal power and subcarrier allocation policy in the previous sections, we present in this section a low-complexity and efficient suboptimal power and subcarrier allocation algorithm. For simplicity, only the average power constraint is considered. The extension to the peak power constraint is simple. The idea of this scheme is to first assign the resources to only SUs as if all the NUs were pure eavesdroppers without data transmission. After that, the residual subcarriers and power, if any, are distributed among NUs. By doing this, the joint update of the Lagrange multipliers will be decoupled as detailed below.

In this scheme, the power allocation adopts the expressions in (17) and (18) except that the parameter $\lambda/\mu_k, k = 1, \ldots, K_1$ in (17) is replaced by a new variable ν_k. Also, in (18) we define $L_k = \omega_k L_0$, for $k = K_1 + 1, \ldots, K)$ where $L_0 = 1/\lambda$. The power allocation scheme among NUs is water-filling with different water levels which are proportional to NUs' weights. Through simple observation, for SU $p_{k,n}$ is monotonically decreasing in ν_k and thus $r_{k,n}^s$ is monotonically decreasing in ν_k. Intuitively, for NU $p_{k,n}$ is monotonically increasing in water level L_0. Therefore, ν_k and L_0 can be found through two separate binary searches. We use a set of training channel realizations to compute the statistical average numerically. The set is sufficiently large to assure that their distribution converges to the statistical distribution.

The outline of this suboptimal algorithm is presented below.

Suboptimal Algorithm

Find the optimal ν_k to achieve the secrecy rate requirement C_k for $k = 1, \ldots, K_1$.

1) Set ν_k^{UB} sufficiently large, $\nu_k^{LB} = 0$ and $\nu_k = (1/2)\left(\nu_k^{LB} + \nu_k^{UB}\right)$.
2) For every training channel realization $\boldsymbol{\alpha}$
   Find $\Omega_k = \{n : \alpha_{k,n} > \max_{k'\neq k}(\alpha_{k',n}) + \nu_k\}$;
   Compute $p_k(\boldsymbol{\alpha}) = \sum_{n\in\Omega_k} p_{k,n}(\boldsymbol{\alpha})$ and $r_k^s(\boldsymbol{\alpha}) = \sum_{n\in\Omega_k} r_k^s(\boldsymbol{\alpha})$, where $p_{k,n}(\boldsymbol{\alpha})$ and $r_{k,n}^s(\boldsymbol{\alpha})$

$$g(\boldsymbol{\mu}, \lambda(\boldsymbol{\alpha})) = \max_{\{p_{k,n}\}\in\mathcal{P}(\boldsymbol{\alpha})} \left\{ \mathbb{E}\left[\sum_{k=K_1+1}^{K} \omega_k \sum_{n=1}^{N} r_{k,n}\left(p_{k,n}(\boldsymbol{\alpha}), \boldsymbol{\alpha}\right)\right] + \sum_{k=1}^{K_1} \mu_k \left(\mathbb{E}\left[\sum_{n=1}^{N} r_{k,n}^s\left(p_{k,n}(\boldsymbol{\alpha}), \boldsymbol{\alpha}\right)\right] - C_k\right) + \int_{\boldsymbol{\alpha}} \lambda(\boldsymbol{\alpha}) \left(P - \sum_{k=1}^{K}\sum_{n=1}^{N} p_{k,n}(\boldsymbol{\alpha})\right) f(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \right\} \quad (31)$$

are computed according to **(17)** and **(3)**, respectively, with λ/μ_k replaced by ν_k;
Compute $\overline{r}_k^s = \mathbb{E}\left[r_k^s(\boldsymbol{\alpha})\right]$ and $\overline{p}_k = \mathbb{E}\left[p_k(\boldsymbol{\alpha})\right]$.

3) If $\overline{r}_k^s > C_k$, $\nu_k^{LB} = \nu_k$, else $\nu_k^{UB} = \nu_k$. Set $\nu_k = (1/2)\left(\nu_k^{LB} + \nu_k^{UB}\right)$.
4) Repeat Steps 2)-3) until $|\overline{r}_k^s - C_k| \leq \epsilon C_k$, for each $k \in [1, K_1]$.
5) Compute the power consumed by SUs, $\overline{P}_{\mathrm{SU}} = \sum_{k=1}^{K_1} \overline{p}_k$. **Find the optimal water level L_0 to meet the power constraint.**
6) Set L_0^{UB} sufficiently large, $L_0^{LB} = 0$ and $L_0 = (1/2)\left(L_0^{UB} + L_0^{LB}\right)$.
7) For every training channel realization $\boldsymbol{\alpha}$
For every residual subcarrier $n \notin \bigcup_{k=1}^{K_1} \Omega_k$, i.e., not occupied by SUs
Find $k = \arg \max_{k \in (K_1, K]} H_{k,n}$ according to **(21)** with $1/\lambda$ replaced by L_0;
For the found k, compute $p_{k,n}(\boldsymbol{\alpha})$ and $r_{k,n}(\boldsymbol{\alpha})$ according to **(18)** and **(5)** with $1/\lambda$ replaced by L_0;
Compute $\overline{r}_k = \mathbb{E}\left[\sum_{n=1}^{N} r_{k,n}(\boldsymbol{\alpha})\right]$ and $\overline{P}_{\mathrm{NU}} = \mathbb{E}\left[\sum_{k=K_1+1}^{K} \sum_{n=1}^{N} p_{k,n}(\boldsymbol{\alpha})\right]$.
8) If $\overline{P}_{\mathrm{NU}} > P - \overline{P}_{\mathrm{SU}}$, $L_0^{UB} = L_0$, else $L_0^{LB} = L_0$. Set $L_0 = (1/2)\left(L_0^{UB} + L_0^{LB}\right)$.
9) Repeat Steps 7)–8) until $|\overline{P}_{\mathrm{SU}} + \overline{P}_{\mathrm{NU}} - P| < \epsilon P$.

In the algorithm, we first find the subcarrier set $\Omega_k (k = 1, \ldots, K_1)$ of SUs. The criterion is whether SUs CNR is ν_k larger than the second largest. As Ω_k's are disjoint, the optimal ν_k satisfying C_k can be obtained through K_1 independent binary searches. After getting $\{\nu_k\}$, the power allocation for the K_1 SUs is determined and the total power left for $K - K_1$ NUs is also known. The water levels of power allocation (18) for NUs can be searched until the rest of the total power for NUs is used up.

Since $\nu_k (k = 1, \ldots, K_1)$ and L_0 are obtained individually by binary search, this suboptimal algorithm converges in $\mathcal{O}(K_1 \log 1/\epsilon + \log 1/\epsilon) = \mathcal{O}((K_1+1) \log 1/\epsilon)$ iterations. Note that the optimal algorithm converges in $\mathcal{O}((K_1+1)^2 \log 1/\epsilon)$ iterations as mentioned in the beginning of this section. In addition, the computational loads in each iteration of both the optimal and suboptimal schemes are linear in $KN|\boldsymbol{\alpha}|$, where $|\boldsymbol{\alpha}|$ is the number of the training channel realizations. So the suboptimal scheme reduces the complexity by about $1/K_1 + 1$.

VI. Numerical Results

In this section, we provide some numerical results to evaluate the performance of proposed optimal and suboptimal resource allocation algorithms under both average and peak power constraints. In the simulation setup, we consider an OFDMA network with $N = 64$ subcarriers and $K = 8$ mobile users, among which $K_1 = 4$ are SUs and $K - K_1 = 4$ are NUs. For simplicity, all the weighting parameters ω_k's for NUs are set to 1 and the secrecy rate requirements C_k's for SUs are set to be identical, denoted as $C_k = R_{\mathrm{SU}}$. Let R_{NU} denote the average total information rate of the NUs. Here we use nat instead of bit as the measurement unit of data for computational convenience. The channel on each subcarrier for each user is assumed to be independent and identically distributed Rayleigh fading with unit mean-square value for illustration purpose only. Note that more sophisticated multipath broadband channel models, such as HiperLan/2 channel model A, can be easily applied since our analytical framework is general and applicable to arbitrary channel distributions. The system total transmit SNR defined in the simulation is equivalent to the average power budget P (or peak power budget if the peak power constraint is concerned) on all the N subcarriers at the base station, assuming unit noise power.

To evaluate the optimal and suboptimal power and subcarrier adaptation schemes, we introduce two nonadaptive schemes in this simulation as benchmarks. In these two nonadaptive schemes, subcarrier assignment is fixed beforehand while power allocated to the predetermined subcarrier sets conforms to (17) and (18). In the first fixed subcarrier assignment scheme, denoted as FSA-1, the 64 subcarriers are equally assigned to the eight users regardless of user type and thus each user obtains eight subcarriers. In the second scheme, denoted as FSA-2, the SUs are given higher priority and each is assigned 12 subcarriers, whereas each NU is assigned four subcarriers.

We first demonstrate the pair of achievable average total information rate of NUs and feasible average secrecy rate requirement of each individual SU $(R_{\mathrm{NU}}, R_{\mathrm{SU}})$ at a given average total power constraint. Fig. 1 shows the rate pair at fixed total transmit SNR $= 30$ dB. First it is observed that using both optimal and suboptimal algorithms, R_{NU} decreases with the increase of secrecy requirement R_{SU} and falls sharply to zero at around $R_{\mathrm{SU}} = 3.5$ nat/OFDM symbol. Recall the discussion in Section III-D where an upper bound on the secrecy rate requirement to make the problem feasible was obtained as 3.5 nat/OFDM symbol in the case of $N = 64$ subcarriers and $K = 8$ users. This explains the drastic fall of R_{NU}. It is then observed from Fig. 1 that the suboptimal algorithm only incurs less than 20% loss in R_{NU} when achieving the same R_{SU} compared with the optimal algorithm. Now comparing the optimal and suboptimal schemes with the nonadaptive ones, both of them earn great advantage over the two benchmarks FSA-1 and FSA-2. In particular, the maximum feasible points of the two fixed subcarrier assignment methods appear at around $R_{\mathrm{SU}} = 0.44$ and 0.66 nat/OFDM symbol, respectively, which are much lower than those in the optimal and suboptimal algorithms.

Figs. 2 and 3 show, respectively, the average power consumption and the average number of subcarriers assigned to all SUs with respect to different R_{SU} when the total average transmit power is fixed as 30 dB. From Fig. 2, we notice that the optimal scheme spends more power on SUs than the suboptimal one. It is observed from Fig. 3 that the number of occupied subcarriers by SUs increases with the growing of R_{SU} and reaches 32 at the feasible point of $R_{\mathrm{SU}} = 3.5$ nat/OFDM symbol for both the optimal and suboptimal schemes. Note that 32 is an expected number because when R_{SU} is very close to the feasible point, adaptive schemes tend to assign as many subcarriers as possible to SUs and on average, all SUs can occupy half of total subcarriers at most. Additionally, the optimal scheme assigns

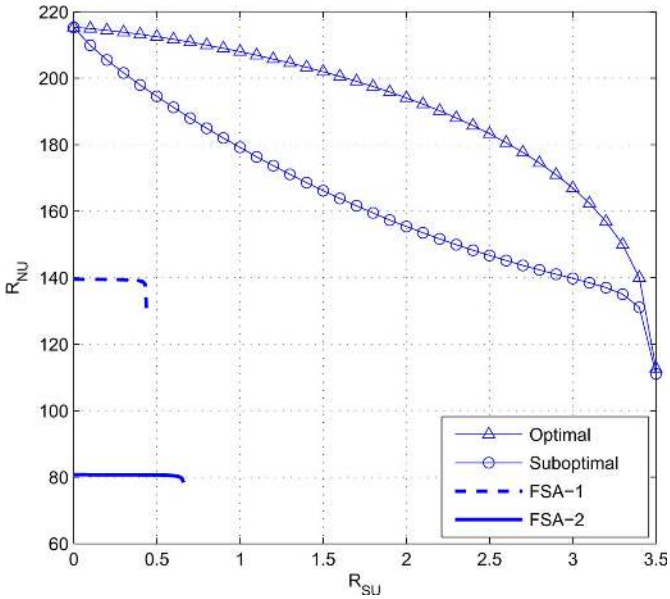


Fig. 1. Achievable $(R_{\mathrm{SU}}, R_{\mathrm{NU}})$ pair at total transmit SNR of 30 dB.

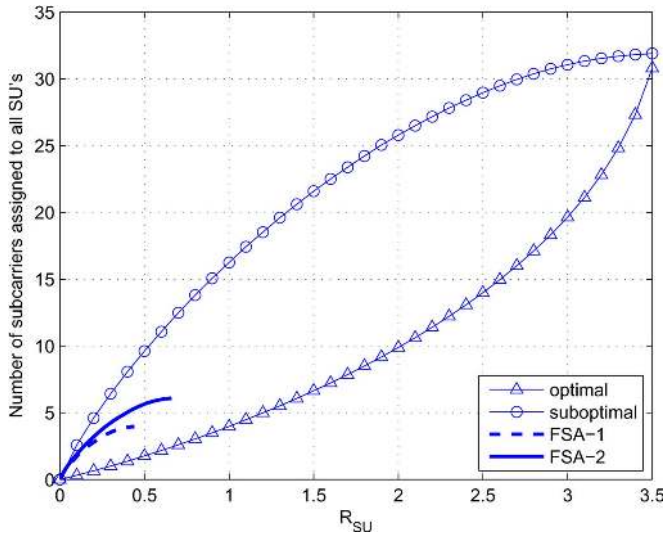


Fig. 3. Average number of subcarriers assigned to all SUs versus R_{SU} at total transmit SNR of 30 dB.

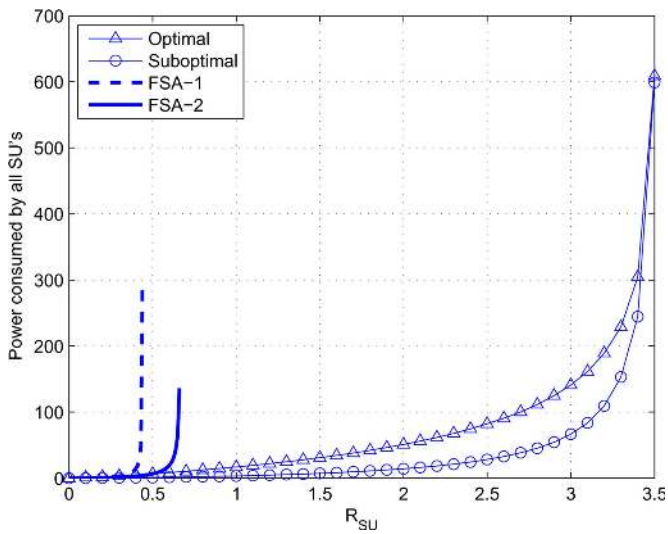


Fig. 2. Average power consumption by all SUs versus R_{SU} at total transmit SNR of 30 dB.

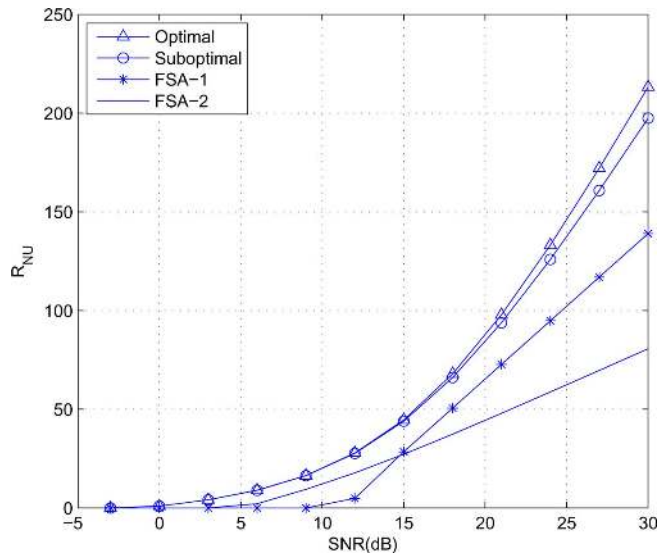


Fig. 4. R_{NU} versus total transmit SNR at $R_{\mathrm{SU}} = 0.4$ nats/OFDM symbol.

less subcarriers to SUs than the suboptimal one. For FSA-1 and FSA-2, the number of occupied subcarriers by SUs is also increasing with the feasible R_{SU} and is smaller than the number of preassigned subcarriers to SUs, i.e., 8 and 12, respectively, for FSA-1 and FSA-2. This indicates that fixed subcarrier assignments waste subcarriers compared with adaptive ones. Note that the number of subcarriers assigned to all NUs for the optimal and suboptimal schemes can be straightforwardly obtained by subtracting the numbers shown in Fig. 3 from the total number of subcarriers, 64.

We next demonstrate the relation between R_{NU} and total transmit SNR for a given $R_{\mathrm{SU}} = 0.4$ nat/OFDM symbol in Fig. 4. Note that the constraint $R_{\mathrm{SU}} = 0.4$ is feasible when SNR ≥ -2 dB for the optimal and suboptimal schemes and when SNR ≥ 3 or 9 dB, respectively, for FSA-1 and FSA-2. From Fig. 4, we first observe that at low SNR region (SNR ≤ 18 dB), the optimal and suboptimal schemes perform close to each other. As SNR becomes larger, the suboptimal scheme only incurs a marginal performance loss. It is also seen that the function curves of FSA-1 and FSA-2 intersect at about 14 dB. When the transmit SNR is lower than 14 dB, FSA-2 is superior to FSA-1 in terms of R_{NU}. This is because when power is limited, FSA-2 assigns SUs more subcarriers and thus saves more power for NUs. If transmit SNR is higher than 14 dB, FSA-2 becomes inferior to FSA-1. The reason lies in that when power is sufficient to meet secrecy rate requirements, FSA-2 wastes subcarriers on SUs and leaves NUs less to promote their information rates.

Finally, in Fig. 5, we compare the performance under average and peak power constraints and show the achieved aggregate rate of NUs at different SNR. It is observed that under the two power constraints, the two curves differ slightly in the low SNR

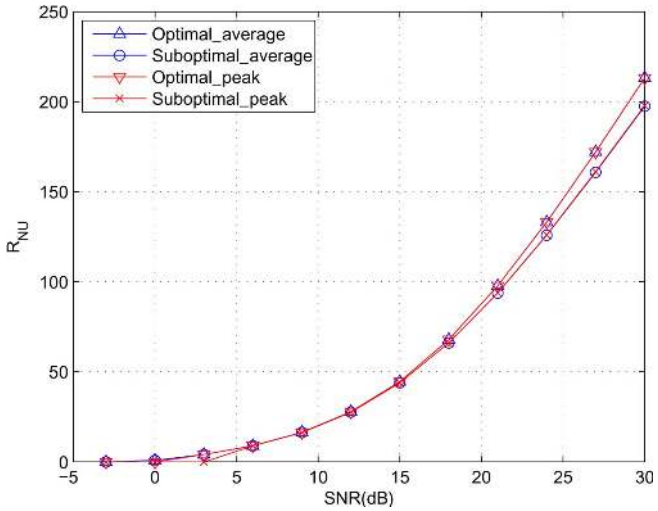


Fig. 5. R_{NU} versus total transmit SNR at $R_{\mathrm{SU}} = 0.4$ nat/OFDM symbol under both average and peak power constraints.

region and almost coincide at the high SNR region for both optimal and suboptimal schemes.

To conclude the above results, the proposed optimal and suboptimal resource allocation schemes significantly outperform those with fixed subcarrier assignment. This observation indicates the great importance of carefully coordinating the subcarrier allocation with adaptation to the system channel conditions. Moreover, the suboptimal scheme provides a good trade-off between performance and complexity.

VII. Conclusions and Discussions

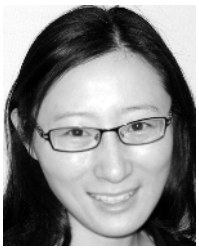
This work investigated the power and subcarrier allocation policy for OFDMA broadband networks where both SUs and NUs coexist. We formulated the problem as maximizing the average aggregate information rate of NUs while satisfying the basic average secrecy rate requirements of SUs under either an average or a peak transmit power constraint. We solved the problem asymptotically in dual domain by using decomposition method. Results show that the optimal power allocation for an SU depends on both its channel gain and the largest channel gain among others. We also observe that an SU becomes a valid candidate competing for a subcarrier only if its CNR on this subcarrier is the largest among all and larger enough than the second largest CNR. To reduce the computational cost, a suboptimal scheme with favorable performance is presented. Numerical results show that the optimal power and subcarrier allocation algorithm effectively boosts the average total information rate of NUs while meeting the basic secrecy rate requirements of SUs. It is also shown that whether it is peak or average power constraint, the system performance does not differ much given the sufficient number of subcarriers used.

Before finishing the paper, we provide some discussions. First, we assumed throughout this work that the CSI of each user obtained at the BS is accurate. If a user deliberately lies and reports a lower CNR on certain subcarriers, it would get a higher chance of eavesdropping SUs' private message and, therefore, cause secrecy rate loss. However, on the other side, its own average information rate or secrecy rate would also be reduced due to the less assigned radio resources. Hence, we argue that there is no incentive for the users to lie about their channel condition. If, however, the network contains a purely malicious eavesdropper that does not care about its own transmission, the security in the network can be circumvented by sending the BS false channel measurements. Second, if eavesdroppers can collude and exchange outputs to decode the message, the network can be regarded as a single-input multiple-output system, where there is only a single eavesdropper with multiple receive antennas. In this case, our algorithms can still apply except the change that the secrecy rate of an SU depends on the sum of the channel gains of all the eavesdroppers rather than the largest one. Furthermore, in the case where a user is equipped with multiple receive antennas, an interesting topic for future investigation is to allow the user to report only one antenna to the BS and use the remaining antennas to eavesdrop. Lastly, since the proposed resource allocation algorithm is a centralized one, full knowledge of CSI is required as commonly assumed in the literature. Taking into account practicality and system overhead, we will investigate distributed algorithms with partial or local channel knowledge in our future work.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 2009.
[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.
[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[5] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Info. Theory*, Seattle, WA, 2006, pp. 356–360.
[6] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. 41st Ann. Allerton Conf.*, Allerton House, UIUC, IL.
[7] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," *IEEE Commun. Lett.*, vol. 14, no. 10, pp. 885–887, Oct. 2010.
[8] C. Y. Wong, R. S. Cheng, K. B. Letaief, and R. D. Murch, "Multi-user OFDM with adaptive sub-carrier, bit, and power allocation," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 10, pp. 1747–1758, Oct. 1999.
[9] J. Jang and K. B. Lee, "Transmit power adaptation for multiuser OFDM systems," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 2, pp. 171–178, Feb. 2003.
[10] M. Tao, Y.-C. Liang, and F. Zhang, "Resource allocation for delay differentiated traffic in multiuser OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2190–2201, Jun. 2008.
[11] D. S. W. Hui, V. K. N. Lau, and W. H. Lam, "Cross-layer design for OFDMA wireless systems with heterogeneous delay requirements," *IEEE Trans. Wireless Commun.*, vol. 6, no. 8, pp. 2872–2880, Aug. 2007.
[12] N. Mokari, M. R. Javan, and K. Navaie, "Cross-layer resource allocation in OFDMA systems for heterogeneous traffic with imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 1011–1017, Feb. 2010.
[13] G. Song and Y. Li, "Cross-layer optimization for OFDM wireless networks: Part II: Algorithm development," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 625–634, Mar. 2005.
[14] E. Jorswieck and A. Wolf, "Resource allocation for the wire-tap multicarrier broadcast channel," in *Proc. Int. Conf. Telecommun.*, St. Petersburg, Russia.
[15] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, 2007, pp. 1301–1305.

[16] W. Yu and R. Lui, "Dual methods for nonconvex spectrum optimization of multicarrier systems," *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1310–1322, Jul. 2006.
[17] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[18] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.



Xiaowei Wang received the B.S. degree in communication engineering from Jiangsu University, Zhenjiang, China, in 2006, and the M.S. degree in control theory and engineering from Shanghai University, Shanghai, China, in 2009. She is currently working toward the Ph.D. degree with the Institute of Wireless Communication Technology, Shanghai Jiao Tong University.

Her current research interests include physical layer security, cooperative communications, resource allocation, and OFDM techniques.

Meixia Tao (S'00–M'04–SM'10) received the B.S. degree in electronic engineering from Fudan University, Shanghai, China, in 1999, and the Ph.D. degree in electrical and electronic engineering from Hong Kong University of Science and Technology in 2003.

She is currently an Associate Professor in the Department of Electronic Engineering, Shanghai Jiao Tong University, China. From Aug. 2003 to Aug. 2004, she was a Member of Professional Staff at Hong Kong Applied Science and Technology Research Institute Co. Ltd. From August 2004 to December 2007, she was with the Department of Electrical and Computer Engineering at National University of Singapore as an Assistant Professor. Her current research interests include cooperative transmission, physical layer network coding, resource allocation of OFDM networks, and MIMO techniques.

Dr. Tao is an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, an Associate Editor for the IEEE COMMUNICATIONS LETTERS, and an Editor for the *Journal Of Communications And Networks*. She served as Track/Symposium Cochair for APCC'09, ChinaCom'09, IEEE ICCCN'07, and IEEE ICCCAS'07. She has also served as Technical Program Committee member for various conferences, including IEEE GLOBECOM, IEEE ICC, IEEE WCNC, and IEEE VTC. She is the recipient of the IEEE ComSoC Asia-Pacific Outstanding Young Researcher Award in 2009, and the Publication Awards in the Institution of Engineers in Singapore in 2005.

Jianhua Mo received the B.S. degree in electronic engineering in Shanghai Jiao Tong University, Shanghai, China, in 2010. At present, he is pursuing a dual M.S. degree from Shanghai Jiao Tong University and Georgia Institute of Technology.

His research interests include application of physical-layer security, fundamental limits of secure communications, and integration of physical-layer and higher layer security.

Youyun Xu (M'02–SM'11) was born in 1966. He received the Ph.D. degree in information and communication engineering in 1999 from Shanghai Jiao Tong University (SJTU), China.

He is currently a professor with Nanjing Institute of Communication Engineering, PLA University of Science and Technology, China. He is also a part-time professor with the Institute of Wireless Communication Technologies, SJTU. He has more than 20 years of professional experience of teaching and researching in communication theory and engineering. His research interests focus on new generation wireless mobile communication system (LTE, IMT-Advanced, and Related), advanced channel coding and modulation techniques, multiuser information theory and radio resource management, wireless sensor networks, and cognitive radio networks.

Dr. Xu is a senior member of the Chinese Institute of Electronics.