Resource Allocation for Secure OFDMA Networks with Imperfect CSIT

Derrick Wing Kwan Ng*, Ernest S. Lo†, and Robert Schober*
*Department of Electrical and Computer Engineering
*The University of British Columbia
†Centre Tecnològic de Telecomunicacions de Catalunya (CTTC)

***Abstract*—In this paper, we formulate an optimization problem for resource allocation and scheduling in orthogonal frequency division multiple access (OFDMA) networks. Our problem formulation takes into account artificial noise generation to combat a passive multiple antenna eavesdropper and the effects of imperfect channel state information at the transmitter (CSIT) in slow fading. The optimization problem is solved by dual decomposition which results in an iterative resource allocation algorithm with a fast speed of convergence. The packet data rate, secrecy data rate, power, and subcarrier allocation policies are optimized to maximize the average secrecy outage capacity (bit/s/Hz securely and successfully delivered to the users). Simulation results illustrate that our proposed iterative algorithm converges to the optimal solution in a small number of iterations and guarantees a non-zero secrecy data rate for given target secrecy outage and channel outage probability requirements.**

I. Introduction

Orthogonal frequency division multiple access (OFDMA) is a promising candidate for high speed wireless communication networks including IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMAX), Long Term Evolution Advanced (LTE-A), and IEEE 802.22 Wireless Regional Area Networks (WRAN), not only because of its flexibility in resource allocation but also its robustness against multipath fading.

Recently, a large amount of work has been devoted to information-theoretic physical layer (PHY) security [1]-[6], as a complement to the traditional cryptographic encryption adopted in the application layer. The pioneering work on PHY security by Wyner [7] showed that a source and a destination can exchange perfectly secure messages with a non-zero rate if the desired receiver enjoys better channel conditions than the passive eavesdropper(s). In [1] and [2], resource allocation in multi-carrier systems with PHY security considerations were studied for the case of single-user and two-user systems, respectively. In these works, the channel state information (CSI) of the eavesdroppers is assumed to be known at the base station (BS) such that secure communication can be guaranteed. Yet, eavesdroppers are usually passive and silent in order to hide their existence. Thus, the CSI of the eavesdroppers cannot be measured at the BS by estimating handshaking signals or be obtained via feedback from the eavesdroppers. On the other hand, secure communication systems employing multiple antennas have been proposed in the absence of the eavesdropper's CSI. By exploiting the extra degrees of freedom in a multiple antenna system, artificial noise or interference is generated in the nullspace of the desired users for degrading the channels of the eavesdroppers. In [3] and [4], the authors studied the power allocation problem for maximizing the ergodic secrecy capacity in single-user single-carrier systems with artificial noise generation, assuming perfect channel state information at the transmitters (CSIT) of the desired users is available. However, the ergodic channel assumption cannot be justified for delay sensitive applications in practice since the transmitted packets of these applications experience quasi-static (slow) fading. Hence, a secrecy outage occurs whenever the scheduled secrecy data rate exceeds the secrecy capacity between the BS and the eavesdropper(s), which introduces a quality of service (QoS) concern for secrecy. In [6], the authors studied a resource allocation algorithm which takes into account the artificial noise generation and secrecy outage under the assumption of perfect CSIT of the desired users. Yet, in practice, the CSI of the desired users may be outdated at the transmitter even if the users are moving with pedestrian speeds. Imperfect CSIT introduces two kinds of performance degradations which have been overlooked in the literature [1]-[6]. First, in quasi-static fading with imperfect CSIT, a transmitted packet is corrupted whenever the transmit data rate exceeds the channel capacity between the active legitimate transceivers, despite the use of channel capacity achieving codes for error protection. Second, for imperfect CSIT, the artificial noise not only interferes the eavesdropper, but also the desired users since their nullspace is not exactly known. As a result, the optimization problem formulation changes fundamentally and the studies in the literature are not applicable. Therefore, for practical implementation, a resource allocation algorithm which takes into account secrecy outage, channel outage, and the potentially detrimental effect of artificial noise generation is needed.

II. OFDMA Downlink Network model

A. Channel Model

We consider an OFDMA downlink network which consists of a BS with N_T antennas, an eavesdropper[1] with N_E antennas, and K mobile users equipped with a single antenna, c.f. Figure 1. The BS adopts multiple-input multiple-output beamforming (MIMO-BF) to enhance the system performance. We assume that $N_T > N_E$ to enable secure communication. The eavesdropper is passive and its goal is to decode the information transmitted by the BS without causing interference to the communication channels.

The impulse responses of all channels are assumed to be time-invariant (slow fading). We consider an OFDMA system with n_F subcarriers. The received symbols at user k and the eavesdropper on subcarrier $i \in \{1, \ldots, n_F\}$ are given by, respectively,

$$y_{B,k}[i] = \mathbf{h}_{B,k}[i]\mathbf{x}_k[i] + n_k[i] \quad \text{and} \tag{1}$$

$$\mathbf{y}_{B,E}[i] = \mathbf{G}_{B,E}[i]\mathbf{x}_k[i] + \mathbf{e}[i], \tag{2}$$

where $\mathbf{x}_k[i] \in \mathbb{C}^{N_T \times 1}$ denotes the transmitted symbol vector and $\mathbb{C}^{N \times M}$ is the space of all $N \times M$ matrices with complex entries. $\mathbf{h}_{B,k}[i] \in \mathbb{C}^{1 \times N_T}$ denotes the channel matrix between the BS and user k on subcarrier i and $\mathbf{G}_{B,E}[i] \in \mathbb{C}^{N_E \times N_T}$ is the channel matrix between the BS and the eavesdropper on subcarrier i. Both variables, $\mathbf{h}_{B,k}[i]$ and $\mathbf{G}_{B,E}[i]$, include the effects of path loss and multipath fading of the associated channels. $n_k[i] \in \mathbb{C}^{1 \times 1}$ and $\mathbf{e}[i] \in \mathbb{C}^{N_E \times 1}$ are the additive white Gaussian noise (AWGN) in subcarrier i at user k and

[1] An eavesdropper with N_E antennas is equivalent to multiple eavesdroppers with a total of N_E antennas which are connected to a common processing unit.

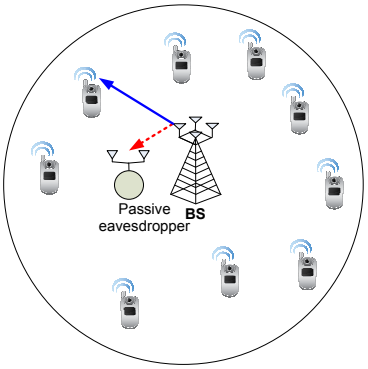

Fig. 1. Illustration of an OFDMA downlink network. There are one BS with $N_T = 4$ antennas, $K = 9$ desired users equipped with a single antenna, and one eavesdropper with $N_E = 2$ antennas. For an effective eavesdropping, the eavesdropper chooses a location closer to the BS compared to all the desired users.

the eavesdropper, respectively. Each entry in both vectors has distribution $\mathcal{CN}(0, N_0)$, where N_0 is the noise power spectral density. Here, $\mathcal{CN}(\nu, \sigma^2)$ denotes a complex Gaussian random variable with mean ν and variance σ^2. For the sake of notational simplicity and without loss of generality, a normalized noise variance of $N_0 = 1$ is assumed for all receivers in the following.

B. Channel State Information

In the following, since path loss is a slowly varying random process which changes in the order of seconds, we assume that the path loss can be estimated perfectly. Although we also assume that for signal detection purposes the users can obtain perfect estimates of the BS-to-user fading gains $\mathbf{h}_{B,k}[i]$, $i \in \{1, \ldots, n_F\}$, $k \in \{1, \ldots, K\}$, the corresponding CSI may be outdated at the BS due to the users's CSI feedback delay and the mobility of the users. To capture this effect, we model the multipath fading CSIT of the link between the BS and user k on subcarrier i as

$$\mathbf{h}_{B,k}[i] = \hat{\mathbf{h}}_{B,k}[i] + \Delta\mathbf{h}_{B,k}[i], \tag{3}$$

where $\hat{\mathbf{h}}_{B,k}[i]$ and $\Delta\mathbf{h}_{B,k}[i]$ denote, respectively, the estimated CSI vector and the CSIT error vector. $\hat{\mathbf{h}}_{B,k}[i]$ and $\Delta\mathbf{h}_{B,k}[i]$ are Gaussian random vectors and each vector has independent and identically distributed (i.i.d.) elements. Besides, the elements of vectors $\mathbf{h}_{B,k}[i]$, $\hat{\mathbf{h}}_{B,k}[i]$, and $\Delta\mathbf{h}_{B,k}[i]$ have zero means and variance $\sigma^2_{\hat{h}_{B,k}}$, $\sigma^2_{\hat{h}_{B,k}} - \sigma^2_e$, and σ^2_e, respectively. Assuming a minimum mean square error (MMSE) estimator. On the other hand, since the eavesdropper is assumed to be passive and the corresponding CSI is unavailable at the BS, in order to secure the desired wireless communication links, *artificial noise* signals are generated at the BS to degrade the channels between the BS and the eavesdropper.

C. Artificial Noise Generation

The BS chooses $\mathbf{x}_k[i]$ as the linear combination of the information bearing signal and an artificial noise signal, i.e.,

$$\mathbf{x}_k[i] = \underbrace{\hat{\mathbf{b}}_k[i]u_k[i]\sqrt{P_{B,k}[i]\alpha_{B,k}[i]}}_{\text{Desired Signal}} + \underbrace{\mathbf{V}_{B,k}[i]\mathbf{v}[i]}_{\text{Artificial Noise}}, \tag{4}$$

where $u_k[i] \in \mathbb{C}^{1\times 1}$ is the information bearing signal, $\mathbf{v}[i] \in \mathbb{C}^{N_T-1\times 1}$ is the artificial noise vector whose elements are i.i.d. complex Gaussian random variables with variance $\sigma^2_v[i]$. Since $\hat{\mathbf{h}}_{B,k}[i]$ is known at the BS, MIMO-BF can be used to maximize the received signal-to-noise (SNR) ratio at the desired receivers. The beamforming vector adopted at the BS, i.e, $\hat{\mathbf{b}}_k[i] \in \mathbb{C}^{N_T\times 1}$, is chosen to be the eigenvector corresponding to the maximum eigenvalue of $\hat{\mathbf{h}}^{\dagger}_{B,k}[i]\hat{\mathbf{h}}_{B,k}[i]$. Here, $[\cdot]^{\dagger}$ denotes the conjugate transpose operation. Furthermore, we define an orthogonal basis, $\mathbf{V}_{B,k}[i] \in \mathbb{C}^{N_T\times N_T-1}$, by using the remaining eigenvectors of $\hat{\mathbf{h}}^{\dagger}_{B,k}[i]\hat{\mathbf{h}}_{B,k}[i]$. $P_{B,k}[i]$ is the total transmitted power on subcarrier i for user k and $0 < \alpha_{B,k}[i] \leq 1$ represents the fraction of power devoted to the information bearing signal on subcarrier i for user k. The remaining power on subcarrier i is equally distributed into $N_T - 1$ dimensions for generating the artificial noise at the BS, i.e., $\sigma^2_v[i] = \frac{(1-\alpha_{B,k}[i])P_{B,k}[i]}{N_T-1}$. Hence, the received signal at user k and the eavesdropper in (1) and (2) can be rewritten as

$$\begin{aligned} y_{B,k}[i] &= \mathbf{h}_{B,k}[i]\Big(\sqrt{P_{B,k}[i]\alpha_{B,k}[i]}\hat{\mathbf{b}}_k[i]u_k[i] + \mathbf{V}_{B,k}[i]\mathbf{v}[i]\Big) \\ &\quad + n_k[i] \quad \text{and} \\ \mathbf{y}_{B,E}[i] &= \mathbf{G}_{B,E}[i]\Big(\hat{\mathbf{b}}_k[i]u_k[i]\sqrt{P_{B,k}[i]\alpha_{B,k}[i]} \\ &\quad + \mathbf{V}_{B,k}[i]\mathbf{v}[i]\Big) + \mathbf{e}[i], \end{aligned} \tag{5}$$

respectively.

III. Resource Allocation and Scheduling

A. Instantaneous Channel Capacity and Outages

Given perfect CSI at the receiver (CSIR), i.e., $\mathbf{h}_{B,k}[i]\hat{\mathbf{b}}_k[i]$, the instantaneous channel capacity based on (5) between the BS and user k on subcarrier i is given by

$$\begin{aligned} &C_{B,k}[i] \\ &= \log_2\Big(1 + \frac{\alpha_{B,k}[i]P_{B,k}[i]\hat{\mathbf{b}}^{\dagger}_k[i]\mathbf{h}^{\dagger}_{B,k}[i]\mathbf{h}_{B,k}[i]\hat{\mathbf{b}}_k[i]}{1 + (1-\alpha_{B,k})P_{B,k}[i]\sigma^2_e}\Big). \end{aligned} \tag{6}$$

On the other hand, since the BS does not have any CSI of the eavesdropper, we follow the approach in [3], [4] and consider a capacity upper bound for the eavesdropper for resource allocation purposes assuming the absence of thermal noise at the eavesdropper. Therefore, the capacity of the eavesdropper is upper bounded by

$$\begin{aligned} C_{B,E}[i] &\leq \log_2\Big(1 + \Gamma_{B,E}[i]\Big), \\ \Gamma_{B,E}[i] &= \frac{\alpha_{B,k}[i](N_T-1)}{1-\alpha_{B,k}[i]}\mathbf{g}^{\dagger}_1[i](\mathbf{G}_1[i]\mathbf{G}^{\dagger}_1[i])^{-1}\mathbf{g}_1[i], \end{aligned} \tag{7}$$

where $\mathbf{g}_1[i] = \mathbf{G}_{B,E}[i]\hat{\mathbf{b}}_k[i]$ and $\mathbf{G}_1[i] = \mathbf{G}_{B,E}[i]\mathbf{V}_{B,k}[i]$.

Hence, the maximum achievable secrecy data rate $R^{sec}_k[i]$ for perfectly secure communication between the BS and user k on subcarrier i with outage consideration can be expressed as

$$\begin{aligned} R^{sec}_k[i] \times\ & 1(R^{data}_k[i] < C_{B,k}[i]) \\ & \times 1(R^{data}_k[i] - C_{B,E}[i] > R^{sec}_k[i]), \end{aligned} \tag{8}$$

where $1(\cdot)$ denotes an indicator function which is 1 when the event is true and 0 otherwise. $R^{data}_k[i]$ is the actual packet data rate transmitted from the BS to user k. There are two types of outage measures in the considered system. The first one is known as channel outage which corresponds to the first indictor function in (8). A channel outage occurs whenever the transmit data rate exceeds the instantaneous channel capacity between two desired transceivers, i.e., $R^{data}_k[i] > C_{B,k}[i]$. If $R^{data}_k[i] > C_{B,k}[i]$, any transmitted packet between two legitimate active transceivers is corrupted even if a channel capacity achieving code is applied for error protection. Indeed, channel outage can be avoided by packet data rate adaptation when the CSIT of the desired channel is perfect. Yet, CSIT with high accuracy is difficult to obtain if the users are not static. The second type of outage measure is secrecy outage which corresponds to the

second indicator function in (8). If the CSI of the eavesdropper is available at the BS, the resource allocator can set the target secrecy data rate $R_k^{sec}[i]$ to match the channel conditions [3], i.e., $R_k^{sec}[i] < R_k^{data}[i] - C_{B,E}[i]$ and $R_k^{data}[i] > C_{B,E}[i]$, such that a packet with secrecy rate $R_k^{sec}[i]$ and packet data rate $R_k^{data}[i]$ can be securely delivered and successfully decoded by the desired user. However, here the eavesdropper is assumed to be passive and its CSI is not available at the BS, i.e., $C_{B,E}[i]$ is a random variable for the BS. Hence, a *secrecy outage* occurs whenever the target secrecy data rate $R_k^{sec}[i]$ exceeds the secrecy capacity, i.e., $R_k^{data}[i] - C_{B,E}[i]$.

In order to model the unreliability and the insecurity due to both *channel outage* and *secrecy outage*, respectively, we consider the performance in terms of the *average secrecy outage capacity*, which is defined as the total average bits/s/Hz securely and successfully delivered to the K mobile users (averaged over multiple scheduling slots) and is given by $U_{sec}(\mathcal{P},\mathcal{R},\mathcal{S}) =$

$$\sum_{k=1}^{K} w_k \sum_{i=1}^{n_F} \frac{s_k[i]}{n_F} R_k^{sec}[i] \Pr\left[R_k^{data}[i] < C_{B,k}[i] \middle| \hat{\mathbf{h}}_{B,k}[i]\right] \times \Pr\left[R_k^{data}[i] - C_{B,E}[i] > R_k^{sec}[i] \middle| \hat{\mathbf{h}}_{B,k}[i]\right], \quad (9)$$

where $\mathcal{P}$ and $\mathcal{S}$ are the power and subcarrier allocation policies, respectively. Policy $\mathcal{R}$ includes the allocation of secrecy data rate $R_k^{sec}[i]$ and packet data rate $R_k^{data}[i]$. $s_k[i] \in \{0,1\}$ is the combinatorial subcarrier allocation indicator. w_k is a positive constant provided by the upper layers, which allows the resource allocator to give different priorities to different users and to enforce certain notions of fairness such as proportional fairness and max-min fairness.

B. Optimization Problem Formulation

The optimal power allocation policy, $\mathcal{P}^*$, data rate (secrecy rate and data rate) allocation policy, $\mathcal{R}^*$, and subcarrier allocation policy, $\mathcal{S}^*$, can be obtained from

$$\begin{aligned}
&\arg \max_{\mathcal{P},\mathcal{R},\mathcal{S},\alpha_{B,k}[i]} U_{sec}(\mathcal{P},\mathcal{R},\mathcal{S}) \\
\text{s.t. C1:}\ &\Pr\left[R_k^{data}[i] \geq C_{B,k}[i] \middle| \hat{\mathbf{h}}_{B,k}[i]\right] \leq \varepsilon,\ \forall k,i, \\
\text{C2:}\ &\Pr\left[R_k^{sec}[i] \geq R_k^{data}[i] - C_{B,E}[i] \middle| \hat{\mathbf{h}}_{B,k}[i]\right] \leq \delta, \forall k,i, \\
\text{C3:}\ &\sum_{k=1}^{K}\sum_{i=1}^{n_F} P_{B,k}[i]s_k[i] \leq P_{B_T}, \\
\text{C4:}\ &\sum_{k=1}^{K} s_k[i] \leq 1, \forall i; \qquad \text{C5: } s_k[i] = \{0,1\}, \forall i,k, \\
\text{C6:}\ &P_{B,k}[i] \geq 0,\ \forall i,k; \qquad \text{C7: } 0 < \alpha_{B,k}[i] \leq 1,\ \forall i,k. \quad (10)
\end{aligned}$$

Here, C1 represents the required packet outage probability due to the imperfect CSI of the BS to user k channel on subcarrier i. In C2, δ denotes the required secrecy outage probability in the system, i.e., C2 is a QoS metric for communication security. C3 is the maximum instantaneous transmit power constraint for the BS. Constraints C4 and C5 are the subcarrier allocation constraints which guarantee that each subcarrier will serve only one user. In other words, intra-user interference is completely avoided. C6 and C7 are the boundary constraints for the power allocation variables.

IV. Solution of the Optimization Problem

A. Transformation of the Optimization Problem

For derivation of an efficient resource allocation algorithm, we replace the "$\leq$"-signs in C1 and C2 by "$=$"-signs and the resulting optimization problem may be viewed as a restricted version of the original problem (10) since replacing inequality signs by equality signs reduces the feasible set. We are now ready to introduce the following Lemma.

Lemma 1 (Equivalent Objective Function): For a given channel outage probability ε and a given secrecy outage probability δ in C1 and C2, respectively, the equivalent secrecy data rate in high SNR on subcarrier i for user k is given by

$$R_k^{sec}[i] > \left[R_k^{data}[i] - \log_2\left(1 + \frac{\alpha_{B,k}^*[i]\Lambda_E[i]}{1-\alpha_{B,k}^*[i]}\right)\right]^+ \quad (11)$$

with

$$R_k^{data}[i] = \log_2\left(1+\Gamma_{B,k}[i]\right), \quad (12)$$

$$\Gamma_{B,k}[i] = \frac{\alpha_{B,k}^*[i]P_{B,k}[i]F_{\chi_2}^{-1}(\varepsilon,i)}{1+(1-\alpha_{B,k}^*)P_{B,k}[i]\sigma_e^2},$$

$$\Lambda_E[i] = (N_T-1)F_{z_c}^{-1}(\delta,i), \alpha_{B,k}^*[i] = \frac{1}{\sqrt{\Lambda_E[i]}},$$

where $[x]^+ = \max\{0,x\}$, $F_{z_c}^{-1}(\cdot,i)$ denotes the inverse function of $F_{z_c}(z,i) = \frac{\sum_{n=0}^{N_E-1}\binom{N_T-1}{n}z^n}{(1+z)^{N_T-1}}$, and $F_{\chi_2}^{-1}(\cdot,i)$ represents the inverse cumulative distribution function (cdf) of a non-central chi-square random variable with 2 degrees of freedom and non-centrality parameter $\hat{\mathbf{h}}_{B,k}[i]\hat{\mathbf{h}}_{B,k}^{\dagger}[i]$.

Proof: Please refer to the Appendix.

There are two important observations from the above lemma. First, the asymptotically optimal $\alpha_{B,k}^*[i]$ in Lemma 1 reveals that in high SNR, the optimal fraction of power devoted to the artificial noise only depends on the statistic of the eavesdropper channel. Second, the signal-to-interference-plus-noise ratio (SINR) of the eavesdropper, $\frac{\alpha_{B,k}^*[i]}{1-\alpha_{B,k}^*[i]}\Lambda_E[i]$, approaches a constant value at high SNR. In other words, the SINR of the eavesdropper on each subcarrier is independent of the transmit power variables at the BS. This important observation will be verified in Section V via simulation.

By substituting (11) into (9), a modified objective function is obtained and the considered problem becomes an NP-hard mixed combinatorial and convex optimization problem, where the combinatorial nature comes from the binary constraints in the subcarrier assignment. Therefore, we follow the time-sharing approach in [8] and relax constraint C5 in (10) such that $s_k[i]$ is allowed to be any real value between zero and one. To facilitate the time sharing on each subcarrier, we introduce a new variable and define it as $\tilde{P}_{B,k}[i] = P_{B,k}[i]s_k[i]$. This variable is the actual transmit power of the BS on subcarrier i for user k under the time-sharing assumption. Then, problem (10) can be re-written as

Problem 1 (Transformed Optimization Problem):

$$\begin{aligned}
&\max_{\mathcal{P},\mathcal{R},\mathcal{S}} \sum_{k=1}^{K}\sum_{i=1}^{n_F} w_k s_k[i]\widetilde{R}_k^{sec}[i] \quad (13)\\
&\text{s.t.}\quad \text{C4, C6} \\
&\text{C3:} \sum_{k=1}^{K}\sum_{i=1}^{n_F} \tilde{P}_{B,k}[i] \leq P_{B_T}, \\
&\text{C5: } 0 \leq s_k[i] \leq 1 \quad \forall k,i,
\end{aligned}$$

where $\widetilde{R}_k^{sec}[i] = R_k^{sec}[i]\Big|_{P_{B,k}[i]=\tilde{P}_{B,k}[i]/s_k[i]}$ is the achievable secrecy data rate for user k on subcarrier i. Mathematically, the $[\cdot]^+$ operators in the objective function in (13) destroy the concavity of the problem. Nevertheless, as will be seen in

the Karush-Kuhn-Tucker (KKT) conditions in (18), users with negative secrecy data rate will not be considered in the subcarrier selection process, since, secure communication cannot be guaranteed for those users. Therefore, we can remove the $[\cdot]^+$ operators from $\widetilde{R}_k^{sec}[i]$ in (11), while preserving the concavity of the transformed problem. On the other hand, the constant term $\frac{1}{n_F}$ is removed from the transformed objective function for simplicity as it does not affect the values of the arguments which maximize the objective function. Besides, C7 is also removed from the optimization problem as the asymptotically optimal $\alpha_{B,k}^*[i]$ in Lemma 1 always satisfied the constraint. Now, the transformed problem is jointly concave with respect to all optimization variables and under some mild conditions [9], it can be shown that solving the dual problem is equivalent to solving the primal problem.

B. Dual Problem Formulation

In this subsection, we solve the considered problem by solving its dual. For this purpose, we first need the Lagrangian function of the primal problem. Upon rearranging terms, the Lagrangian can be written as

$$\mathcal{L}(\lambda,\boldsymbol{\beta},\mathcal{P},\mathcal{R},\mathcal{S}) = \sum_{k=1}^{K} w_k \sum_{i=1}^{n_F} s_k[i]\tilde{R}_k^{sec}[i] - \lambda\sum_{k=1}^{K}\sum_{i=1}^{n_F}\tilde{P}_k[i] - \sum_{k=1}^{K}\sum_{i=1}^{n_F}\beta[i]s_k[i] + \lambda P_{B_T} + \sum_{i=1}^{n_F}\beta[i], \quad (14)$$

where $\lambda \geq 0$ is the Lagrange multiplier corresponding to the power constraint at the BS. $\boldsymbol{\beta}$ is the Lagrange multiplier vector connected to the subcarrier usage constraints with elements $\beta[i] \geq 0$, $i \in \{1,\ldots,n_F\}$. The boundary constraints C5 and C6 will be absorbed into the KKT conditions when deriving the optimal solution in Section IV-C.

Thus, the dual problem is given by

$$\min_{\lambda,\boldsymbol{\beta}\geq 0}\ \max_{\mathcal{P},\mathcal{R},\mathcal{S}}\quad \mathcal{L}(\lambda,\boldsymbol{\beta},\mathcal{P},\mathcal{R},\mathcal{S}). \quad (15)$$

In the following sections, we solve the above dual problem iteratively by decomposing it into two parts (nested loops): the first part (inner loop) consists of n_F sub-problems with identical structure; the second part (outer loop) is the master dual problem to be solved with the gradient method.

C. Dual Decomposition and Solution

By dual decomposition, the BS first solves the subproblem

$$\max_{\mathcal{P},\mathcal{R},\mathcal{S}}\quad \mathcal{L}(\lambda,\boldsymbol{\beta},\mathcal{P},\mathcal{R},\mathcal{S}) \quad (16)$$

for a fixed set of Lagrange multipliers. Note that the above subproblem is the inner loop optimization in (15). Using standard optimization techniques, the optimal power allocation for user k on subcarrier i is given by

$$P_{B,k}^*[i] = \left[\frac{\sqrt{\Omega_{B,k}[i](\Omega_{B,k}[i]\lambda\log(2)+4\Xi_{B,k}[i]w_k)}}{2\Xi_{B,k}[i]\sqrt{\lambda}\sqrt{\log(2)}} - \frac{2(1-\alpha_{B,k}[i])\sigma_e^2+\Omega_{B,k}[i]}{2\Xi_{B,k}[i]}\right]^+, \quad (17)$$

where $\Xi_{B,k}[i] = (1-\alpha_{B,k}[i])\sigma_e^2(\Omega_{B,k}[i]+\sigma_e^2(1-\alpha_{B,k}[i]))$ and $\Omega_{B,k}[i] = F_{\chi_2}^{-1}(\varepsilon,i)\alpha_{B,k}[i]$. The optimal power allocation in (17) has the form of *multi-level* water-filling. The water level of each user depends not only on his/her priority via w_k, but also on the channel statistic of the desired channel, i.e., $F_{\chi_2}^{-1}(\varepsilon,i)\alpha_{B,k}[i]$. In order to obtain the optimal subcarrier allocation, we take the derivative of the subproblem with respect to $s_k[i]$, which yields

$$\frac{\partial\mathcal{L}(\lambda,\boldsymbol{\beta},\mathcal{P},\mathcal{R},\mathcal{S})}{\partial s_k[i]} = A_k[i]-\beta[i], \quad (18)$$

where $A_k[i] \geq 0$ is the marginal benefit [10] for allocating subcarrier i to user k and is given by

$$A_k[i] = w_k\left(\log_2\left(1+\Gamma_{B,k}^*[i]\right) - \log_2\left(1+\frac{\alpha_{B,k}^*[i]\Lambda_E[i]}{1-\alpha_{B,k}^*[i]}\right) - \frac{\Gamma_{B,k}^*[i]}{\ln(2)(1+\Gamma_{B,k}^*[i])(1+\sigma_e^2P_{B,k}^*[i](1-\alpha_{B,k}^*[i]))}\right), \quad (19)$$

where $\Gamma_{B,k}^*[i] = \Gamma_{B,k}[i]\Big|_{P_{B,k}[i]=P_{B,k}^*[i]}$. $A_k[i] \geq 0$ suggests that if user k has a negative secrecy data rate on subcarrier i, he/she will not be selected as he/she can only provide a negative marginal benefit to the system. On the contrary, if a user has good channel conditions with positive secrecy data rate on subcarrier i, he/she can provide a higher marginal benefit to the system. Thus, the optimal subcarrier selection determined by the BS on subcarrier i is given by

$$s_k^*[i] = \begin{cases} 1 & \text{if } A_k[i] = \max\limits_b A_b[i] \geq 0 \ \&\ A_b[i] \geq \beta[i] \\ 0 & \text{otherwise} \end{cases}. \quad (20)$$

The dual variable $\beta[i]$ acts as the cost in using subcarrier i in the system. Only the user who can provide a large marginal benefit to the system has a chance to be selected by the resource allocator. Note that each subcarrier will be used for serving only one user eventually. Finally, the optimal transmitted packet data rate $R_k^{*data}[i]$ and secrecy data rate $R_k^{*sec}[i]$ are obtained by substituting (17) into the equivalent packet data rate and secrecy data rate in Lemma 1 for the subcarrier with $s_k^*[i]=1$.

D. Solution of the Master Problem

Since the dual function is differentiable, the gradient method can be used to solve the master problem (outer loop) in (15) which leads to a Lagrange multiplier update equation:

$$\lambda(t+1) = \left[\lambda(t) - \xi(t)\times\left(P_{B_T} - \sum_{k=1}^{K}\sum_{i=1}^{n_F}P_{B,k}[i]s_k[i]\right)\right]^+, \quad (21)$$

where $t \geq 0$ is the iteration index and $\xi(t)$ is the positive step size. Then, the updated Lagrange multiplier in (21) is used for solving the subproblems in Section IV-C. Since the transformed problem is jointly concave with respect to all optimization variables, it is guaranteed that the iterative algorithm converges to the optimal solution if the chosen step sizes satisfy the general conditions stated in [11, Chapter 1.2]. In summary, the master problem adjusts the water-levels of (17) through the gradient update equation (21) until the power constraint of the BS is satisfied. On the other hand, updating $\beta[i]$ is not necessary as it has the same value for each user. Therefore, setting $\beta[i]=0$ in each iteration does not affect the subcarrier allocation in (20).

V. Results

In this section, we evaluate the system performance using simulations. A single cell with a radius of 1 km is considered. The number of subcarriers is $n_F = 64$ with carrier center frequency 2.5 GHz, bandwidth $\mathcal{B} = 5$ MHz, and $w_k = 1, \forall k$. Each subcarrier has a bandwidth of 78 kHz and a noise variance $N_0 = -125$ dBm. The eavesdropper is located 35 m (reference

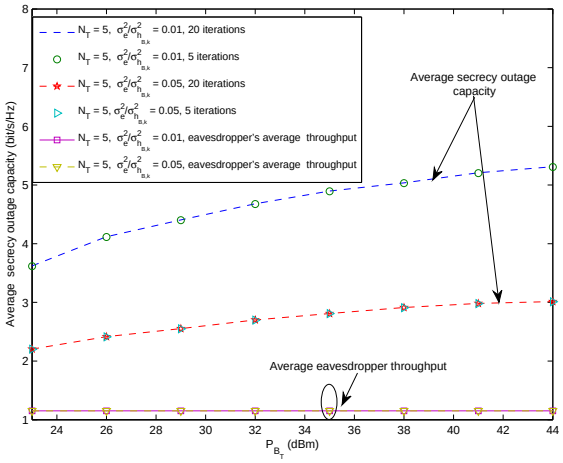

Fig. 2. Average secrecy outage capacity versus transmit power for different values of channel estimation error-to-signal ratio (ESR). The eavesdropper is equipped with $N_E = 2$ antennas and is located 35 m away from the BS.

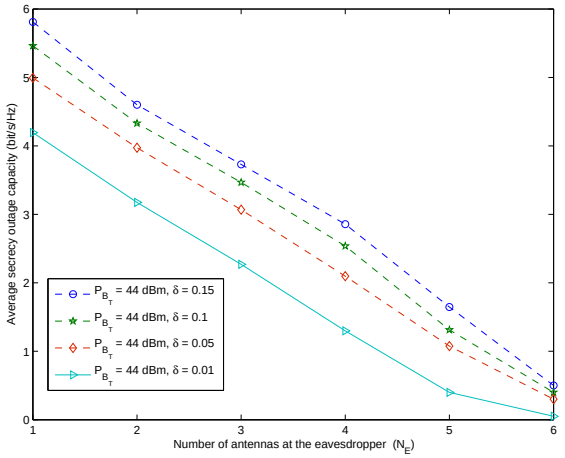

Fig. 3. Average secrecy outage capacity versus the number of eavesdropper antennas N_E for different secrecy outage requirements and $N_T = 7$ antennas at the BS.

distance) away from the BS for an effective eavesdropping. Desired users are uniformly distributed between the reference distance and the cell boundary. The 3GPP path loss model is adopted. The small scale fading coefficients of the BS-to-user and BS-to-eavesdropper links are modeled as i.i.d. Rayleigh fading. The target secrecy outage probability and channel outage probability are set to $\delta, \varepsilon = 0.05$. The channel estimation error-to-signal ratio (ESR) is set to $\frac{\sigma_e^2}{\sigma_{h_{B,k}}^2} = 0.05$, unless further specified. The average secrecy outage capacity is obtained by counting the number of packets securely delivered and decoded by the users averaged over both the macroscopic and microscopic fading.

A. Average Secrecy Outage Capacity versus Transmit Power

Figure 2 illustrates the average secrecy outage capacity and the throughput of the eavesdropper versus the total transmit power for $K = 15$ users for different values of ESRs. The eavesdropper is equipped with $N_E = 2$ antennas. The number of iterations for the proposed iterative resource allocation algorithm is 5 and 20. It can be seen that the performance for 5 and 20 iterations is virtually the same. In other words, the algorithm converges to the optimal solution in a few iterations. On the other hand, we observe that the system performance decreases as the ESR increases. This is because the nullspace information of the desired users at the transmitter becomes less accurate as the ESR increases which increases the artificial noise leakage. For a better illustration of the effectiveness of the artificial noise generation, Figure 2 also includes the performance of the eavesdropper in terms of average throughput. The average throughput between the BS and the eavesdropper does not scale with the transmit power in the high transmit power regime due to the artificial noise introduced by the BS which is in good agreement with Lemma 1. Besides, it can be observed that the artificial noise generation maintains the same effectiveness for different channel estimation error variances since an increasing ESR does not enhance the average throughput of the eavesdropper.

B. Average Secrecy Outage Capacity versus N_E

Figure 3 depicts the average secrecy outage capacity versus the number of receive antennas N_E employed at the eavesdropper for different secrecy outage requirements δ with $K = 15$ users. There are $N_T = 7$ transmit antennas at the BS. The number of iterations for the proposed algorithm is 5. It can be observed that the system performance decreases as N_E increases, since more of the transmitted power has to be devoted to the artificial noise generation for combatting the eavesdropper, which results in less transmit power for information transmission. Yet, a non-zero secrecy outage capacity can still be guaranteed as long as $N_T > N_E$ due to the artificial noise. Moreover, we observe that a more stringent secrecy outage probability requirement does not necessarily lead to a higher average secrecy outage capacity. This is because a larger fraction of power has to be allocated to the artificial noise for degrading the channel of the eavesdropper and less power is available for information transmission.

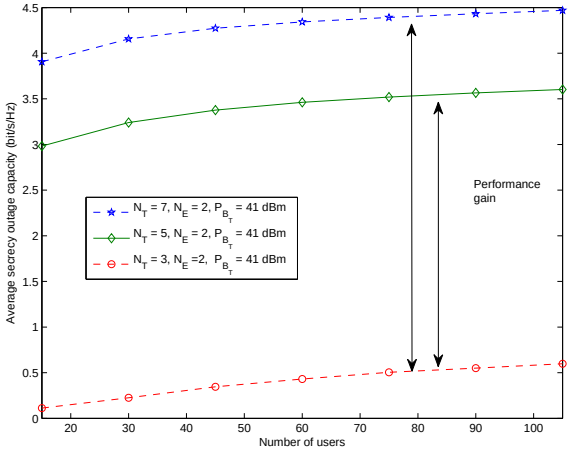

Fig. 4. Average secrecy outage capacity versus the number of desired users for different transmit antennas N_T at the BS with a total transmit power $P_{B_T} = 41$ dBm. The eavesdropper is equipped with $N_E = 2$ antennas and is located 35 m away from the BS. The double arrows demonstrate the performance gain achieved by an increasing number of transmit antennas N_T.

C. Average Secrecy Outage Capacity versus Number of Users

Figure 4 depicts the average secrecy outage capacity versus the number of users for different numbers of transmit antennas. The number of iterations is 5. The eavesdropper is equipped with $N_E = 2$ antennas. It can be observed that the average secrecy outage capacity grows with the number of users as the proposed resource allocation and scheduling algorithm is able to exploit multi-user diversity, despite the existence of the eavesdropper. Besides, it can be observed that an increasing number of transmit antennas N_T provides a substantial performance gain to the legitimate users in terms of average secrecy outage capacity. However, there is a diminishing return when N_T is large due to the *channel hardening* effect [12] in the desired channels.

VI. Conclusion

In this paper, we formulated the resource allocation and scheduling design for OFDMA systems as a non-convex and combinatorial optimization problem, where a multiple antenna eavesdropper, artificial noise generation for secure communication, and the negative effect of imperfect CSIT were taken into consideration. An efficient iterative resource allocation algorithm with closed-form power, secrecy data rate, packet data rate, and subcarrier allocation was derived by dual decomposition. Simulation results not only showed that the performance of the proposed algorithm converges to the optimal performance within a small number of iterations, but also demonstrated the achievable non-zero secrecy outage capacity for a required channel outage probability and secrecy outage probability.

Appendix-Proof of Lemma 1

The proof of Lemma 1 involves three steps. We first derive the channel outage data rate between the BS and user k on subcarrier i. By considering the channel outage probability requirement C1 in (10), we obtain

$$\begin{aligned}
&\Pr\Big[\frac{(2^{R_k^{data}[i]}-1)(1+(1-\alpha_{B,k}[i])P_{B,k}[i]\sigma_e^2)}{\alpha_{B,k}[i]P_{B,k}[i]} \geq \\
&\hat{\mathbf{b}}_k^\dagger[i]\mathbf{h}_{B,k}^\dagger[i]\mathbf{h}_{B,k}[i]\hat{\mathbf{b}}_k[i]\Big|\hat{\mathbf{h}}_{B,k}[i]\Big] \\
&= F_{\chi_2}\Big(\frac{(2^{R_k^{data}[i]}-1)(1+(1-\alpha_{B,k}[i])P_{B,k}[i]\sigma_e^2)}{\alpha_{B,k}[i]P_{B,k}[i]}, i\Big) = \varepsilon \\
&\Rightarrow R_k^{data}[i] = \log_2\Big(1+\frac{\alpha_{B,k}[i]P_{B,k}[i]F_{\chi_2}^{-1}(\varepsilon,i)}{1+(1-\alpha_{B,k})P_{B,k}[i]\sigma_e^2}\Big), \qquad (22)
\end{aligned}$$

where $F_{\chi_2}(\cdot,i)$ denotes the cdf of a non-central chi-square random variable with 2 degrees of freedom and non-centrality parameter $\hat{\mathbf{h}}_{B,k}[i]\hat{\mathbf{h}}_{B,k}^\dagger[i]$. $F_{\chi_2}^{-1}(\cdot,i)$ represents the inverse function of $F_{\chi_2}(\cdot,i)$. Then, we derive the secrecy outage data rate by calculating the secrecy outage probability in C2. Without loss of generality, we define the secrecy data rate as $R_k^{sec}[i] = \log_2(r_k^{sec}[i])$ and the data rate as $R_k^{data}[i] = \log_2(r_k^{data}[i])$. Then, the secrecy outage probability can be expressed as

$$\begin{aligned}
&\Pr\Big[R_k^{data}[i] - C_{B,E}[i] \leq R_k^{sec}[i]\Big|\hat{\mathbf{h}}_{B,k}[i]\Big] = \delta \\
\Longrightarrow &\Pr\Big[\underbrace{\Big(\frac{r_k^{data}[i]}{r_k^{sec}[i]}-1\Big)\frac{1-\alpha_{B,k}[i]}{(N_T-1)\alpha_{B,k}[i]}}_{\Theta_k[i]} \\
&\leq \underbrace{\mathbf{g}_1^\dagger[i](\mathbf{G}_2[i]\mathbf{G}_2^\dagger[i])^{-1}\mathbf{g}_1[i]}_{Z_k[i]}\Big|\hat{\mathbf{h}}_{B,k}[i]\Big] = \delta, \qquad (23)
\end{aligned}$$

where $Z_k[i]$ is an unknown random variable for the BS, $\mathbf{g}_1[i] = \mathbf{G}_{B,E}[i]\hat{\mathbf{b}}_k[i]$, and $\mathbf{G}_2[i] = \mathbf{G}_{B,E}[i]\mathbf{V}_{B,k}[i]$. Since the supermatrix $\mathbf{B}_k[i] = [\hat{\mathbf{b}}_k[i]\ \mathbf{V}_{B,k}[i]]$ is a unitary matrix, $\mathbf{B}_k[i]\mathbf{G}_{B,E}[i]$ has i.i.d. complex Gaussian entries. As a result, $Z_k[i]$ is equivalent to the signal-to-interference ratio (SIR) of a N_E-branch minimum mean square error (MMSE) diversity combiner for N_T-1 interferers. Hence, the corresponding complementary cumulative distribution function (ccdf) is given by [4], [13]

$$F_{z_c}(z,i) = \sum_{n=0}^{N_E-1}\binom{N_T-1}{n}z^n/(1+z)^{N_T-1}. \qquad (24)$$

Therefore, for a target secrecy outage probability of δ, $\Theta_k[i]$ defined in (23) can be expressed as $\Theta_k[i] = F_{z_c}^{-1}(\delta,i)$. Thus, solving $\Theta_k[i] = F_{z_c}^{-1}(\delta,i)$ for $R_k^{sec}[i]$ yields $R_k^{sec}[i] =$

$$R_k^{data}[i] - \log_2\Big(1+\frac{\alpha_{B,k}[i]}{1-\alpha_{B,k}[i]}(N_T-1)F_{z_c}^{-1}(\delta,i)\Big), \qquad (25)$$

where $F_{z_c}^{-1}(\delta,i)$ is the inverse ccdf of random variable $Z_k[i]$. Note that both inverse functions $F_{z_c}^{-1}(\delta,i)$ and $F_{\chi_2}^{-1}(\varepsilon,i)$, can be computed efficiently by numerical solvers or implemented as a look-up table for practical implementation.

The final step in deriving the lemma is to calculate the optimal $\alpha_{B,k}^*[i]$ in high SNR ($P_{B,k}[i] \to \infty$). Under such conditions and using (22) and (25), the secrecy data rate is lower bounded by

$$\begin{aligned}
R_k^{sec}[i] > \quad &\log_2\Big(1+\frac{P_{B,k}[i]F_{\chi_2}^{-1}(\varepsilon,i)\alpha_{B,k}^*[i]}{\sigma_e^2 P_{B,k}[i]}\Big) \\
&-\log_2\Big(1+\frac{\alpha_{B,k}^*[i]F_{z_c}^{-1}(\delta,i)(N_T-1)}{1-\alpha_{B,k}^*[i]}\Big). \qquad (26)
\end{aligned}$$

In fact, the term $\frac{P_{B,k}[i]F_{\chi_2}^{-1}(\varepsilon,i)\alpha_{B,k}^*[i]}{\sigma_e^2 P_{B,k}[i]}$ can be interpreted as a signal-to-interference ratio (SINR) under a virtual interferer with interference power $\sigma_e^2 P_{B,k}[i]$ for $P_{B,k}[i] \to \infty$. By standard optimization techniques, the optimal $\alpha_{B,k}^*[i]$ which maximizes the lower bound of the secrecy data rate on subcarrier i for user k in (26) is given by

$$\begin{aligned}
\alpha_{B,k}^*[i] \quad &= \quad \frac{-\Phi_k[i]+\sqrt{\Phi_k[i]\Lambda_E[i](\Phi_k[i]-\Lambda_E[i]+1)}}{\Phi_k[i](\Lambda_E[i]-1)} \\
&\overset{(a)}{\approx} \quad \frac{\sqrt{\Lambda_E[i]}-1}{\Lambda_E[i]-1} \approx \frac{1}{\sqrt{\Lambda_E[i]}} \qquad (27)
\end{aligned}$$

where $\Phi_k[i] = F_{\chi_2}^{-1}(\varepsilon,i)/\sigma_e^2$ and $\Lambda_E[i] = F_{z_c}^{-1}(\delta,i)(N_T-1)$. Note that (a) is due to $\Phi_k[i] \gg \Lambda_E[i] \gg 1$ which is always valid for reasonably small channel estimation error variance σ_e^2 (e.g. $\sigma_e^2 \ll \sigma_{h_{B,k}}^2$) and secrecy outage requirement δ (e.g. $\delta \ll 1$).

References

[1] E. A. Jorswieck and A. Wolf, "Resource Allocation for the Wire-Tap Multi-Carrier Broadcast Channel," in *Proc. International Conf. on Telecommun.*, June 2008, pp. 1 – 6.

[2] Z. Li, R. Yates, and W. Trappe, "Secrecy Capacity of Independent Parallel Channels," in *Proc. 44th Annu. Allerton Conf. Commun., Control and Computing*, Sep 2006, pp. 841–848.

[3] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180 – 2189, Jun. 2008.

[4] X. Zhou and M. R. McKay, "Secure Transmission with Artificial Noise over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Trans. Veh. Technol.*, pp. 3831 – 3842, Jul. 2010.

[5] A. Mukherjee and A. Swindlehurst, "Fixed-Rate Power Allocation Strategies for Enhanced Secrecy in MIMO Wiretap Channels," in *Proc. IEEE 10th Workshop on Signal Processing Advances in Wireless Communications* , Jun. 2009, pp. 344 –348.

[6] D. W. K. Ng and R. Schober, "Resource Allocation for Secure OFDMA Communication Systems," in *Proc. 2011 Australia Communications Theory Workshop*, Feb 2011, pp. 13 – 18.

[7] A. D. Wyner, "The Wire-Tap Channel," Tech. Rep., Oct 1975.

[8] C. Y. Wong, R. S. Cheng, K. B. Letaief, and R. D. Murch, "Multiuser OFDM with Adaptive Subcarrier, Bit, and Power Allocation," *IEEE J. Select. Areas Commun.*, vol. 17, pp. 1747–1758, Oct 1999.

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

[10] W. Yu and J. M. Cioffi, "FDMA Capacity of Gaussian Multiple-Access Channels with ISI," *IEEE Trans. Commun.*, vol. 50, pp. 102 – 111, Jan 2002.

[11] D. P. Bertsekas, *Nonlinear Programming*, 2nd ed. Athena Scientific, 1999.

[12] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, 1st ed. Cambridge University Press, 2005.

[13] H. Gao, P. J. Smith, and M. V. Clark, "Theoretical Reliability of MMSE Linear Diversity Combining in Rayleigh-Fading Additive Interference Channels," *IEEE Trans. Commun.*, vol. 46, pp. 666 – 672, May 1998.