Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Resource allocation for physical-layer security in OFDMA downlink with imperfect CSI*

Wei YANG†1, Jing MAO†1, Chen CHEN†‡1, Xiang CHENG1, Liu-qing YANG†2, Hai-ge XIANG1

[1]*State Key Laboratory of Advanced Optical Communication Systems and Networks,*
Peking University, Beijing 100871, China

[2]*Department of Electrical & Computer Engineering, Colorado State University, Fort Collins, CO 80523, USA*

†E-mail: youngwei@pku.edu.cn; maojing@pku.edu.cn; c.chen@pku.edu.cn; lqyang@engr.colostate.edu

Received Jan. 9, 2017; Revision accepted Apr. 8, 2017; Crosschecked Mar. 15, 2018

Abstract: We investigate the problem of resource allocation in a downlink orthogonal frequency-division multiple access (OFDMA) broadband network with an eavesdropper under the condition that both legitimate users and the eavesdropper are with imperfect channel state information (CSI). We consider three kinds of imperfect CSI: (1) noise and channel estimation errors, (2) feedback delay and channel prediction, and (3) limited feedback channel capacity, where quantized CSI is studied using rate-distortion theory because it can be used to establish an information-theoretic lower bound on the capacity of the feedback channel. The problem is formulated as joint power and subcarrier allocation to optimize the maximum-minimum (max-min) fairness criterion over the users' secrecy rate. The problem considered is a mixed integer nonlinear programming problem. To reduce the complexity, we propose a two-step suboptimal algorithm that separately performs power and subcarrier allocation. For a given subcarrier assignment, optimal power allocation is achieved by developing an algorithm of polynomial computational complexity. Numerical results show that our proposed algorithm can approximate the optimal solution.

Key words: Resource allocation; Orthogonal frequency-division multiple access (OFDMA); Imperfect channel state information (CSI); Physical layer security
https://doi.org/10.1631/FITEE.1700026 **CLC number:** TN92

1 Introduction

Orthogonal frequency-division multiple access (OFDMA) is a leading multi-access technique that provides high spectral efficiency and flexibility in resource allocation for existing and future wireless networks such as 4G long-term evolution (LTE), IEEE 802.16 WiMAX, and 5G networks. In the past several years, the problem of assigning powers, subcarriers, and rates to different users in the OFDMA system has been an active research area (Wong et al., 1999; Jang and Lee, 2003; Shen et al., 2005; Song and Li, 2005). These studies considered various formulations under different optimization objectives and constraints. In recent years, with the increasing data rate demand for local area services and dramatically increasing spectrum congestion, resource allocation in device-to-device (D2D) communications underlaying cellular networks has been a hot topic due to the advantages of resource utilization improvement, cell capacity enhancement, energy efficiency increase, and transmission delay decrease among local users (Cheng et al., 2015; Zhang RQ et al., 2015, 2016).

Security is a crucial issue for wireless communication systems due to its broadcasting nature.

‡ Corresponding author

* Project supported by the National Natural Science Foundation of China (Nos. 61471008, 61622101, and 61571020) and the National Key Research and Development Program of China (No. 2016YFE0123100)

ORCID: Chen CHEN, http://orcid.org/0000-0001-5058-6749

Physical layer security is an information-theoretic approach that achieves secrecy by using channel codes and advanced signal processing techniques. The concept of information-theoretic security was defined by Wyner (1975), and then extended to scalar Gaussian (Cheong and Hellman, 1978) and broadcast channels (Csiszár and Korner, 1978). Barros and Rodrigues (2006) studied secrecy capacity in slow fading channels and introduced outage into secrecy issues for the first time.

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 integrate physical layer security into the resource allocation problem in multiuser OFDMA systems. Li et al. (2006) investigated independent parallel channels and proved that the secrecy rate of the system is the summation of the secrecy capacity achieved on each independent channel. Jorswieck and Wolf (2008) tried to investigate power and subcarrier allocation in an OFDM-based broadband system with the objective of maximizing the sum secrecy rate. Wang et al. (2011) considered the problem of secure communications in OFDMA networks in which there are two groups of users: secure users and ordinary users. Their objective is to maximize the ordinary users' data rate under the individual secrecy rate constraint for secure users and the total transmit power of the BS. In Karachontzitis et al. (2015), the authors' objective is to assign subcarriers and allocate the transmit power to optimize the maximum-minimum (max-min) secrecy rate among all legitimate users. However, traditional physical layer security approaches based on single antenna systems are hampered by channel conditions. Some recent approaches have been proposed to overcome this limitation by taking advantage of relays. Relay nodes can achieve cooperative diversity by forwarding information or act as cooperative jammers to degrade eavesdroppers' channel conditions (Wang et al., 2015), and thus improve the security of legitimate transmission (Wang and Wang, 2015; Huang et al., 2016). In an effort to further improve physical layer security, a number of studies have suggested incorporating the multiple antenna technique into wireless communication systems (Yang et al., 2013; Huang et al., 2015). Zhang M et al. (2016) and Zhang and Liu (2016) studied physical layer security for simultaneous wireless information and power transfer (SWIPT) in OFDMA systems.

In most studies, it is assumed that the channel state information (CSI) of both legitimate links and the eavesdropper link is perfectly known at the BS. This assumption is quite unrealistic due to channel estimation errors, and more importantly, channel feedback delay and the limited feedback rate. Motivated by these observations, in this study we focus on the case where only imperfect (partial) CSI is available. We consider the resource allocation problem for optimizing the max-min criterion over the user's secrecy rate under an average total transmit power constraint with imperfect CSI. To the best of our knowledge, no work has considered the max-min security rate with imperfect CSI of both legitimate users and the eavesdropper in OFDMA systems. We discuss three different kinds of partial CSI: (1) partial CSI with noise and channel estimation errors, (2) partial CSI with feedback delay and channel prediction errors, and (3) limited feedback channel capacity, where we employ the rate-distortion theory to find the relationship between quantization errors and feedback channel capacity. In our previous research (Wu et al., 2010, 2011; Chen *et al.*, 2011), spectral efficiency optimization has been addressed with predicted CSI and quantized CSI. Once the conditional probability density function (PDF) of real channel gain is established for the partial channel gain, we can formulate the security-aware resource allocation problem with partial CSI. We solve the optimization problem through a two-step suboptimal algorithm. This algorithm breaks the problem into two subproblems, subcarrier allocation and power allocation, and solves each subproblem with less complexity. We introduce a greedy method to assign the subcarriers. For the assignment of a given subcarrier, we obtain the optimal power allocation policy in semi-closed form using the Karush-Kuhn-Tucker (KKT) conditions. Using this algorithm, we can evaluate the maximum achievable secrecy rate under different partial CSI assumptions.

Notations: Vectors and matrices are presented in bold, and the $(i,j)^{\mathrm{th}}$ entry of matrix $\boldsymbol{A}$ is denoted by $A_{i,j}$. $\boldsymbol{A}^{\mathrm{T}}$ and $\boldsymbol{A}^{\mathrm{H}}$ denote the transpose and conjugate transpose of $\boldsymbol{A}$, respectively. The Kronecker product is denoted as $\otimes$, and $E[\cdot]$ denotes the statistical expectation. In particular, $E_X[\cdot]$ denotes this expectation with respect to X.

2 System model and problem formulation

In this section, we first outline three different kinds of imperfect CSI and introduce the downlink OFDMA system model, and then formulate the max-min secrecy rates problem under the condition of imperfect CSI.

2.1 Downlink channel model

The downlink channel is modeled as a multipath fading channel. The baseband channel gain from the BS to the k^{th} user on the n^{th} subcarrier can be written as

$$H_{n,k}=\sum_{l=1}^{L_k} a_{k,l}\mathrm{e}^{-\mathrm{j}2\pi\tau_{k,l}(n-\frac{N+1}{2})\Delta f}, \tag{1}$$

where L_k is the number of multipath taps, Δf is the subcarrier spacing, and $a_{k,l}$ and $\tau_{k,l}$ denote the attenuation factor and the propagation delay of the l^{th} multipath tap at the k^{th} user's channel, respectively. The multipath channel taps at the k^{th} user $[a_{k,1}, a_{k,2}, \ldots, a_{k,l}]^{\mathrm{T}}$ can be modeled as a zero-mean circularly symmetric complex Gaussian (ZMCSCG) vector with independent entries $a_{k,l}\sim\mathcal{CN}(0,\sigma^2_{a_{k,l}})$. Then, $\boldsymbol{H}_k=[H_{1,k}, H_{2,k}, \ldots, H_{N,k}]^{\mathrm{T}}$ satisfies $\boldsymbol{H}_k\sim\mathcal{CN}(\boldsymbol{0},\boldsymbol{\varSigma}_{\boldsymbol{H}_k})$, where the $(n_1,n_2)^{\mathrm{th}}$ entry of $\boldsymbol{\varSigma}_{\boldsymbol{H}_k}$ is

$$(\varSigma_{\boldsymbol{H}_k})_{n_1,n_2}=\sum_{l=1}^{L_k}\sigma^2_{a_{k,l}}\mathrm{e}^{-\mathrm{j}2\pi\tau_{k,l}(n_1-n_2)\Delta f}. \tag{2}$$

We assume that the downlink OFDMA system employs frequency division duplex (FDD) and that the BS obtains the downlink CSI from users' feedback. The CSI obtained by the BS usually has errors, which can be caused by noise or estimation errors, feedback delay, and quantization errors.

2.2 Noise and estimation errors

In this subsection, we consider the CSI errors $\boldsymbol{\epsilon}_k$ caused by noise and estimation errors, which can be modeled as a zero-mean complex Gaussian vector with independent entries $\epsilon_{n,k}\sim\mathcal{CN}(0,\sigma^2_{n,k})$, where $\sigma^2_{n,k}$ is the mean variance of channel estimation errors. Thus, we have

$$\boldsymbol{H}_k=\hat{\boldsymbol{H}}_k+\boldsymbol{\epsilon}_k, \tag{3}$$

where $\hat{\boldsymbol{H}}_k$ denotes the estimate of $\boldsymbol{H}_k$. Thus, when $\hat{H}_{n,k}$ is estimated, the conditional PDF of $H_{n,k}$ is $(H_{n,k}|\hat{H}_{n,k})\sim\mathcal{CN}(H_{n,k},\sigma^2_{n,k})$.

2.3 Feedback delay and channel prediction

In this subsection, we consider the feedback delays and channel prediction errors of the downlink CSI. Each user estimates the CSI of the downlink channel and sends its channel estimate to the BS. Based on the finite number of past observations of feedback estimates, the BS performs an δm_k-step-ahead prediction for the CSI of user k, where δm_k is equal to the feedback delay of user k.

We use $H_{n,k}(m)$ to denote the baseband channel gain of the k^{th} user on the n^{th} subcarrier at time index m, and it can be modeled as Eq. (1). The identically normalized temporal autocorrelation function of the attenuation factors satisfies the Jakes model:

$$\phi_k(t)=\mathrm{cov}(\alpha_{k,l}(m+t),\alpha_{k,l}(m))=\mathrm{J}_0(2\pi v_k\frac{f_{\mathrm{c}}}{c_0}T_{\mathrm{s}}t), \tag{4}$$

where $\alpha_{k,l}(m)$ is the k^{th} user's channel attenuation factor of the l^{th} multipath tap at time index m, $\mathrm{J}_0(\cdot)$ is the 0^{th}-order Bessel function of the first kind, v_k is the velocity of user k, f_{c} is the carrier frequency, and c_0 is the speed of light in vacuum. We assume that the channel estimate of user k at time index $m-\delta m_k$ is $\widetilde{\boldsymbol{H}}_k(m-\delta m_k)=\left[\widetilde{H}_{1,k},\widetilde{H}_{2,k},\ldots,\widetilde{H}_{N,k}\right]^{\mathrm{T}}$ and that it satisfies $\widetilde{\boldsymbol{H}}_k(m-\delta m_k)=\boldsymbol{H}_k(m-\delta m_k)+\boldsymbol{e}_k(m-\delta m_k)$, where $\boldsymbol{e}_k(m-\delta m_k)\sim\mathcal{CN}(\boldsymbol{0}_N,\sigma^2_{\mathrm{e}}\boldsymbol{I}_N)$ is the spectral and temporal white estimation error with estimation error variance σ^2_ϵ and uncorrelated with $\boldsymbol{H}_k(m-\delta m_k)$. Based on the finite number of past feedbacks of channel estimations $\widetilde{\boldsymbol{H}}_k(m-\delta m_k)$, the BS predicts the channel gain of user k through a linear regressive approach with order Q. Assuming the use of a minimum mean square error (MMSE) channel prediction scheme at BS, we can write the perfect CSI vector $\boldsymbol{H}_k(m)$ as the sum of the predicted channel $\hat{\boldsymbol{H}}_k(m)$ and the prediction error $\boldsymbol{\epsilon}_k(m)$, which are uncorrelated with each other (Wu et al., 2010):

$$\boldsymbol{H}_k(m)=\hat{\boldsymbol{H}}_k(m)+\boldsymbol{\epsilon}_k(m), \tag{5}$$

where $\hat{\boldsymbol{H}}_k(m)\sim\mathcal{CN}(\boldsymbol{0}_N,\boldsymbol{\varSigma}_{\boldsymbol{H}_k}-\boldsymbol{\varSigma}_k)$, $\boldsymbol{\epsilon}_k(m)\sim\mathcal{CN}(\boldsymbol{0}_N,\boldsymbol{\varSigma}_k)$, $\boldsymbol{\varSigma}_k=\boldsymbol{\varSigma}_{\boldsymbol{H}_k}-(\boldsymbol{\varPhi}_k\otimes\boldsymbol{\varSigma}_{\boldsymbol{H}_k})(\boldsymbol{\varGamma}_k\otimes\boldsymbol{\varSigma}_{\boldsymbol{H}_k}+\sigma^2_{\mathrm{e}}\boldsymbol{I})^{-1}(\boldsymbol{\varPhi}_k\otimes\boldsymbol{\varSigma}_{\boldsymbol{H}_k})^{\mathrm{H}}$ is the error covariance matrix, $\boldsymbol{\varGamma}_k$ is an $N\times N$ matrix with $(\varGamma_k)_{i,j}=\phi(j-i)$, and $\boldsymbol{\varPhi}_k=[\phi(\delta m_k),\phi(\delta m_k+1),\ldots,\phi(\delta m_k+Q-1)]$. Therefore, the conditional PDF of $H_{n,k}$ for a given $\hat{H}_{n,k}$ is $(H_{n,k}|\hat{H}_{n,k})\sim\mathcal{CN}(H_{n,k},\sigma^2_{n,k})$, where $\sigma^2_{n,k}$ is the n^{th} diagonal component of $\boldsymbol{\varSigma}_k$.

2.4 Finite-rate feedback of downlink CSI

According to the assumption in Section 2.1 that the system employs FDD, the BS can obtain only the quantized CSI through the finite-rate feedback channel. In this subsection, we consider the CSI errors caused by quantization errors. We characterize the minimum distortion of the quantized CSI for a given capacity of the feedback channel using rate-distortion theory. We use $R_k(D_k)$ to denote the information rate-distortion function (RDF) of $\boldsymbol{H}_k$ with squared-error distortion $d(\boldsymbol{H}_k,\hat{\boldsymbol{H}}_k)=\sum_{n=1}^{N}|H_{n,k}-\hat{H}_{n,k}|^2$, defined as

$$R_k(D_k)=\min_{E[d(\boldsymbol{H}_k,\hat{\boldsymbol{H}}_k)]\le D_k} I(\boldsymbol{H}_k;\hat{\boldsymbol{H}}_k), \tag{6}$$

where $\hat{\boldsymbol{H}}_k=[\hat{H}_{1,k},\hat{H}_{2,k},\ldots,\hat{H}_{N,k}]^{\mathrm{T}}$ is the quantized description of $\boldsymbol{H}_k$, D_k denotes an upper bound on the quantization error, and $I(\boldsymbol{H}_k;\hat{\boldsymbol{H}}_k)$ denotes the mutual information between $\boldsymbol{H}_k$ and $\hat{\boldsymbol{H}}_k$. According to rate-distortion theory, we know that RDF gives a minimum number of bits that can describe $\boldsymbol{H}_k$ without exceeding the quantization error D_k. In other words, quantization error D_k is achievable if and only if the feedback channel's capacity of user k satisfies $C_k>R_k(D_k)$ (Cover and Thomas, 2012). Then we have the following statement (Chen *et al.*, 2011):

Theorem 1 Suppose that the autocorrelation of a ZMCSCG vector $\boldsymbol{H}_k$ is given in Eq. (2). Let the eigenvalue decomposition of $\boldsymbol{\Sigma}_{\boldsymbol{H}_k}$ be

$$\boldsymbol{\Sigma}_{\boldsymbol{H}_k}=\boldsymbol{U}_k\boldsymbol{\Psi}_k\boldsymbol{U}_k^{\mathrm{H}}, \tag{7}$$

where $\boldsymbol{U}_k$ is an $N\times N$ unitary matrix and $\boldsymbol{\Psi}_k$ is an $N\times N$ diagonal matrix with $(\Psi_k)_{n,n}=\psi_{n,k}$. Then the RDF of $\boldsymbol{H}_k$ is given by

$$R_k(D_k)=\sum_{n=1}^{N}\log\max\left\{\frac{\psi_{n,k}}{\theta_k},1\right\}, \tag{8}$$

where $D_k=\sum_{n=1}^{N}\min\{\theta_k,\psi_{n,k}\}$ and θ_k is the Lagrangian multiplier which can be decided for a given D_k. The corresponding test channel that achieves the RDF is given by

$$\boldsymbol{H}_{n,k}=\hat{\boldsymbol{H}}_{n,k}+\boldsymbol{\epsilon}_k,\boldsymbol{\epsilon}_k\sim\mathcal{CN}(\boldsymbol{0}_N,\boldsymbol{\Sigma}_k), \tag{9}$$

where $\boldsymbol{\Sigma}_k=\boldsymbol{U}_k\mathrm{diag}(\min\{\theta_k,\psi_{k,1}\},\min\{\theta_k,\psi_{k,2}\},\ldots,\min\{\theta_k,\psi_{k,N}\})\boldsymbol{U}_k^{\mathrm{H}}$. Therefore, the conditional PDF of $H_{n,k}$ for a given $\hat{H}_{n,k}$ is $(H_{n,k}|\hat{H}_{n,k})\sim\mathcal{CN}(H_{n,k},\sigma_{n,k}^2)$, where $\sigma_{n,k}^2$ is the n^{th} diagonal component of $\boldsymbol{\Sigma}_k$.

In the above three cases of imperfect CSI conditions, the conditional PDFs of $H_{n,k}$ for a given $\hat{H}_{n,k}$ are the same in form $(H_{n,k}|\hat{H}_{n,k})\sim\mathcal{CN}(H_{n,k},\sigma_{n,k}^2)$. Thus, with a given white Gaussian noise σ_v^2, the channel-gain-to-noise ratio (CNR) $\gamma_{n,k}=\frac{|H_{n,k}|^2}{\sigma_v^2}$ conditioned on $\hat{\gamma}_{n,k}=\frac{|\hat{H}_{n,k}|^2}{\sigma_v^2}$ is a non-central Chi-squared (NC_{χ^2}) distributed random variable with two degrees of freedom with a PDF of

$$f(\gamma_{n,k}|\hat{\gamma}_{n,k})=\frac{1}{\alpha_{n,k}}\mathrm{e}^{-\frac{\gamma_{n,k}+\hat{\gamma}_{n,k}}{\alpha_{n,k}}}\mathrm{I}_0\left(\frac{2}{\alpha_{n,k}}\sqrt{\gamma_{n,k}\hat{\gamma}_{n,k}}\right), \tag{10}$$

where $\alpha_{n,k}=\frac{\sigma_{n,k}^2}{\sigma_v^2}$ is the ratio of channel estimation error variance to noise variance and $\mathrm{I}_0(\cdot)$ is the 0^{th}-order modified Bessel function of the first kind.

2.5 System model and problem formulation

The system setup is shown in Fig. 1. We consider an OFDMA broadband system that consists of K active users and N used subcarriers indexed by sets $\mathcal{K}=\{1,2,\ldots,K\}$ and $\mathcal{N}=\{1,2,\ldots,N\}$. An eavesdropper who is passive aims to wiretap the transmitted signal within each data-bearing subcarrier. We assume that this system employs FDD, and that the BS obtains the downlink CSI from users' feedback. The eavesdropper is an honest, but curious, legitimate user who illegally starts wiretapping the messages of the authorized and serviced users. Thus, the BS anticipates the existence of the eavesdropper and can obtain its partial CSI just as it does with other legitimate users. The channel response between user $k\in\mathcal{K}$ and the BS in subcarrier $n\in\mathcal{N}$ is denoted as $H_{n,k}$, while the channel response between the eavesdropper and the BS in subcarrier $n\in\mathcal{N}$ is denoted as $H_{n,\mathrm{e}}$. We use $\hat{H}_{n,k}$ and $\hat{H}_{n,\mathrm{e}}$ to denote the prior information of $H_{n,k}$ and $H_{n,\mathrm{e}}$ that the BS obtains through users' feedback, respectively.

We have obtained the conditional PDF of both the CNR of the k^{th} user $\gamma_{n,k}=\frac{|H_{n,k}|^2}{\sigma_v^2}$ on $\hat{\gamma}_{n,k}=\frac{|\hat{H}_{n,k}|^2}{\sigma_v^2}$ and the CNR of eavesdropper $\gamma_{n,\mathrm{e}}=\frac{|H_{n,\mathrm{e}}|^2}{\sigma_v^2}$

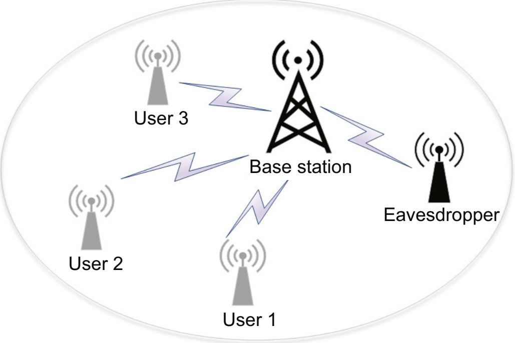

Fig. 1 System model

on $\hat{\gamma}_{n,\mathrm{e}} = \frac{|\hat{H}_{n,\mathrm{e}}|^2}{\sigma_v^2}$. With the knowledge of the feedback CSI, the ergodic capacity for user k on subcarrier n is given by

$$\begin{aligned} R_{n,k}&(p_{n,k}, \hat{\gamma}_{n,k}) \\ &= E_{\gamma_{n,k}}\{\log_2(1+p_{n,k}\gamma_{n,k})|\hat{\gamma}_{n,k}\} \\ &= \int_0^{+\infty} \log_2(1+p_{n,k}\gamma_{n,k})\frac{1}{\alpha_{n,k}} \\ &\quad \cdot \mathrm{e}^{-\frac{\gamma_{n,k}+\hat{\gamma}_{n,k}}{\alpha_{n,k}}} \mathrm{I}_0\left(\frac{2}{\alpha_{n,k}}\sqrt{\gamma_{n,k}\hat{\gamma}_{n,k}}\right)\mathrm{d}\gamma_{n,k}, \end{aligned} \tag{11}$$

where $p_{n,k}$ is the transmit power of user k on subcarrier n. We assume an exclusive subcarrier assignment, in which each subcarrier is assigned exactly to one user. Let the binary variables $\rho_{n,k}, n \in \mathcal{N}, k \in \mathcal{K}$ denote the subcarrier assignment, with $\rho_{n,k} = 1$ if subcarrier n is assigned to user k. Moreover, let $\boldsymbol{P} = (p_{n,k})_{N\times K}$ denote the power allocation matrix, with $P_{\mathrm{T}} > 0$ denoting the available amount of power at the BS and σ_v^2 denoting the ambient noise variance. Regarding Eq. (11), the following proposition can be stated:

Proposition 1 Under the condition of a given $\alpha_{n,k}$, $R_{n,k}(p_{n,k}, \hat{\gamma}_{n,k})$ is an increasing function of $\hat{\gamma}_{n,k}$.

Proof See Appendix.

Accordingly, the ergodic secrecy rate (Chen et al., 2016) of user k within n is given by

$$\begin{aligned} C_{n,k}(p_{n,k}) = \{&E_{\gamma_{n,k}}[\log_2(1+p_{n,k}\gamma_{n,k})|\hat{\gamma}_{n,k}] \\ &-E_{\gamma_{n,\mathrm{e}}}[\log_2(1+p_{n,k}\gamma_{n,\mathrm{e}})|\hat{\gamma}_{n,\mathrm{e}}]\}^+, \end{aligned} \tag{12}$$

where $[x]^+ = \max\{0, x\}$. With the conclusion we have obtained in Proposition 1 and the assumption $\alpha_{n,k} = \alpha_{n,\mathrm{e}}$ where $\alpha_{n,\mathrm{e}}$ is the eavesdropper's ratio of quantization error variance to noise variance, we have

$$C_{n,k} = \begin{cases} E_{\gamma_{n,k}}[\log_2(1+p_{n,k}\gamma_{n,k})|\hat{\gamma}_{n,k}], \\ -E_{\gamma_{n,\mathrm{e}}}[\log_2(1+p_{n,k}\gamma_{n,\mathrm{e}})|\hat{\gamma}_{n,\mathrm{e}}], \quad \hat{\gamma}_{n,k} > \hat{\gamma}_{n,\mathrm{e}}, \\ 0, \quad \hat{\gamma}_{n,k} < \hat{\gamma}_{n,\mathrm{e}}. \end{cases} \tag{13}$$

Therefore, the problem of maximizing the minimum secrecy rate among all users under the total transmit power and exclusive subcarrier assignment constraints is formulated as

$$\begin{aligned} \max_{\rho_{n,k},p_{n,k}} \min_k &\sum_{n\in\mathcal{N}} \rho_{n,k}C_{n,k}(p_{n,k}) \\ \text{s.t.} &\sum_{k\in\mathcal{K},n\in\mathcal{N}} \rho_{n,k}p_{n,k} \le P_{\mathrm{T}}, \\ &\sum_{k\in\mathcal{K}} \rho_{n,k} = 1, n\in\mathcal{N}, \\ &\rho_{n,k}\in\{0,1\}, n\in\mathcal{N}, k\in\mathcal{K}, \\ &0 \le p_{n,k} \le P_{\mathrm{T}}, n\in\mathcal{N}, k\in\mathcal{K}. \end{aligned} \tag{14}$$

From a practical point of view, problem (14) is important mainly for two reasons. First, compared with the max-sum criterion over the total secrecy rate, the max-min criterion can guarantee fairness in the sense that it provides a secrecy rate balancing across the different users as it does not allow one or more privileged users (i.e., users with a channel much stronger than the eavesdropper's channel) to monopolize the available resources. Second, the capacity of the feedback channel is limited in practical communication systems, so the BS can obtain only quantized CSI. As a result, the performance of resource allocation schemes is degraded due to imperfect CSI. Analyzing the effect of finite feedback rates in OFDMA systems turns out to be a crucial problem. Problem (14) is a mixed integer nonlinear programming problem due to the existence of binary variables $\rho_{n,k}$ and the integration of logarithm functions $C_{n,k}(p_{n,k})$. Hence, we can find that problem (14) is NP-hard. In the following section, we propose a suboptimal algorithm with an acceptable complexity by breaking the problem into two subproblems: subcarrier allocation and power allocation.

3 Resource allocation algorithm

3.1 Optimal power allocation algorithm when subcarrier assignment is fixed

In this section, we aim to specify optimal power allocation when subcarrier assignment is given. Let $\mathcal{N}_k$ denote the set of subcarriers that have been assigned to user $k \in \mathcal{K}$. In most cases, we assume that $C_{n,k}(p_{n,k}) > 0$, $n \in \mathcal{N}_k$, $k \in \mathcal{K}$, as it is not beneficial to assign channels with $C_{n,k}(p_{n,k}) = 0$ to user k. The original problem can be rewritten as

$$\max_{p_{n,k},r} \quad r \tag{15a}$$

$$\text{s.t.} \quad 0 \le r \le \sum_{n\in\mathcal{N}_k} C_{n,k}(p_{n,k}), k \in \mathcal{K}, \tag{15b}$$

$$\sum_{k\in\mathcal{K},n\in\mathcal{N}_k} p_{n,k} \le P_{\mathrm{T}}. \tag{15c}$$

For problem (15), we have the following proposition:
Proposition 2 Problem (15) is convex.
Proof The objective in problem (15) is linear with respect to secrecy rate r. Moreover, the constraints in Eq. (15c) are linear functions of $p_{n,k}$. Thus, we focus on the secrecy constraint as given by Eq. (15b). The second derivative of $C_{n,k}(\cdot)$ with respect to $p_{n,k}$ is given as

$$\frac{\partial^2 C_{n,k}}{\partial p_{n,k}^2} = \frac{1}{\ln 2}\left\{ E_{\gamma_{n,k}}\left[\frac{-\gamma_{n,k}^2}{(1+p_{n,k}\gamma_{n,k})^2}\middle|\hat{\gamma}_{n,k}\right] - E_{\gamma_{n,\mathrm{e}}}\left[\frac{-\gamma_{n,\mathrm{e}}^2}{(1+p_{n,k}\gamma_{n,\mathrm{e}})^2}\middle|\hat{\gamma}_{n,\mathrm{e}}\right]\right\}. \tag{16}$$

When $\alpha_{n,k}$ is fixed, $E_{\gamma_{n,k}}\left\{\frac{-\gamma_{n,k}^2}{(1+p_{n,k}\gamma_{n,k})^2}\middle|\hat{\gamma}_{n,k}\right\}$ is a decreasing function of $\hat{\gamma}_{n,k}$. Therefore, $\frac{\partial^2 C_{n,k}}{\partial p_{n,k}^2}$ is always negative for $\hat{\gamma}_{n,k} > \hat{\gamma}_{n,\mathrm{e}}$. Thus, $C_{n,k}(p_{n,k})$ is a concave function of $p_{n,k}$. Therefore, problem (15) is a convex problem, and we can use any standard convex optimization tool to obtain the unique optimal solution. In what follows, we use a bisection method to derive the optimal solution in a semi-closed form.

Assume a fixed value r_f such that $0 < r_f \le \max_k \sum_{n\in\mathcal{N}_k} \mathrm{RA}_{n,k}(p_{n,k})$, where $\mathrm{RA}_{n,k}(p_{n,k})$ denotes the secrecy rate under the assumption that the transmit power is monopolized by exactly one user and distributed equally to its selected subcarriers. Clearly, the secrecy rate r_f can be guaranteed to any user $k \in \mathcal{K}$ if there is a sufficient (possibly higher than P_{T}) amount of power at the BS. Nevertheless, we need to solve the new optimization problem as follows to obtain the optimal power allocation that guarantees secrecy rate r_f across all the users:

$$\begin{aligned} &\min_{p_{n,k}} \sum_{k\in\mathcal{K},n\in\mathcal{N}} p_{n,k} \\ &\text{s.t. } r_f \le \sum_{n\in\mathcal{N}_k} C_{n,k}(p_{n,k}), k \in \mathcal{K}, \\ &\quad p_{n,k} \ge 0, n \in \mathcal{N}, k \in \mathcal{K}. \end{aligned} \tag{17}$$

The Lagrangian multiplexer function for problem (17) is given by (Boyd and Vandenberghe, 2004)

$$\begin{aligned} &L(\boldsymbol{P}, \boldsymbol{\lambda}, \boldsymbol{\mu}) \\ &= \sum_{k\in\mathcal{K}}\sum_{n\in\mathcal{N}} p_{n,k} + \sum_{k\in\mathcal{K}} \lambda_k \left[r_f - \sum_{n\in\mathcal{N}_k} C_{n,k}(p_{n,k})\right] \\ &- \sum_{k\in\mathcal{K}}\sum_{n\in\mathcal{N}} \mu_{n,k} p_{n,k}, \end{aligned} \tag{18}$$

where $\boldsymbol{\lambda} = [\lambda_1, \lambda_2, \ldots, \lambda_K]$ are the Lagrangian multipliers. Based on the KKT condition, we have

$$\begin{cases} \dfrac{\partial L(\boldsymbol{P}, \boldsymbol{\lambda}, \boldsymbol{\mu})}{\partial p_{n,k}}|_{p_{n,k}^*,\lambda_k^*,\mu_{n.k}^*} = 0, n \in \mathcal{N}, k \in \mathcal{K}, \\ \lambda_k^* \left[r_f - \sum\limits_{n\in\mathcal{N}_k} C_{n,k}(p_{n,k}^*)\right] = 0, k \in \mathcal{K}, \\ \mu_{n,k}^* p_{n,k}^* = 0, \\ p_{n,k}^* \ge 0, \lambda_k^* \ge 0, \mu_{n,k}^* \ge 0, \end{cases} \tag{19}$$

where $p_{n,k}^*$ is the optimal power allocation, and λ_k^* and $\mu_{n,k}^*$ are the optimal Lagrange multipliers. Note that $\mu_{n,k}^*$ acts as a slack variable, which can be eliminated (Boyd and Vandenberghe, 2004). The optimal power allocation on the n^{th} subcarrier, which is assigned to user k at the given λ_k, is

$$\overline{p}_{n,k} = \begin{cases} \widetilde{p}_{n,k}, \{E_{\gamma_{n,k}}[\gamma_{n,k}|\hat{\gamma}_{n,k}] - E_{\gamma_{n,\mathrm{e}}}[\gamma_{n,\mathrm{e}}|\hat{\gamma}_{n,\mathrm{e}}]\} > \dfrac{\ln 2}{\lambda_k}, \\ 0, \quad \{E_{\gamma_{n,k}}[\gamma_{n,k}|\hat{\gamma}_{n,k}] - E_{\gamma_{n,\mathrm{e}}}[\gamma_{n,\mathrm{e}}|\hat{\gamma}_{n,\mathrm{e}}]\} < \dfrac{\ln 2}{\lambda_k}, \end{cases} \tag{20}$$

where $\widetilde{p}_{n,k}$ satisfies

$$E_{\gamma_{n,k}}\left[\frac{\gamma_{n,k}}{1+p_{n,k}\gamma_{n,k}}\middle|\hat{\gamma}_{n,k}\right] - E_{\gamma_{n,e}}\left[\frac{\gamma_{n,\mathrm{e}}}{1+p_{n,k}\gamma_{n,\mathrm{e}}}\middle|\hat{\gamma}_{n,\mathrm{e}}\right] = \frac{\ln 2}{\lambda_k}. \tag{21}$$

We use a Gamma distribution to approximate the NC_{χ^2} distribution of Eq. (10) to reduce the computational complexity:

$$f(\gamma_{k,n}|\hat{\gamma}_{k,n}) \approx \frac{\beta^{\alpha}}{\Gamma(\alpha)}\gamma_{k,n}^{\alpha-1}\exp(-\beta\gamma_{k,n}), \tag{22}$$

where $\alpha = (\kappa_{n,k}+1)^2/(2\kappa_{n,k}+1)$ is the Gamma PDF shape parameter with $\kappa_{k,n}/\alpha_{k,n}$ and $\beta = \alpha/(\hat{\gamma}_{k,n} + \alpha_{k,n})$ is the Gamma PDF rate parameter. Using this PDF, we can derive the closed-form expression of Eq. (21) according to Gradshteyn and Ryzhik (2014):

$$\begin{aligned}&E_{\gamma_{n,k}}\left\{\frac{\gamma_{n,k}}{1+p_{n,k}\gamma_{n,k}}\middle|\hat{\gamma}_{n,k}\right\}\\ &\approx\frac{\alpha}{p_{n,k}}\left(\frac{\beta}{p_{n,k}}\right)^{\alpha}\mathrm{e}^{\frac{\beta}{p_{n,k}}}\Gamma\left(-\alpha,\frac{\beta}{p_{n,k}}\right),\end{aligned} \tag{23}$$

where $\Gamma(a,x)$ is the incomplete Gamma function. This approximation has been shown to be fully accurate in Wong and Evans (2009). Substituting Eq. (23) into Eq. (21), a bisection method is used to calculate the power allocation problem for each given λ_k. To find the optimal multiplier λ_k that can satisfy $r_f = \sum_{n\in\mathcal{N}_k} C_{n,k}(\overline{p}_{n,k})$ under the given r_f, we can use the bisection method as well. Clearly, when the available power at the BS is P_{T}, the secrecy rate r_f can be supported by the system only when $\sum_{n,k}\overline{p}_{n,k} \le P_{\mathrm{T}}$. To arrive at a final solution to problem (17), we can use a bisection method to find the optimal r_f.

For each iteration of the bisection method, problem (16) is solved and the total power consumption is calculated. When the total power consumption is higher (lower) than P_{T}, r_f is decreased (increased) and the process is repeated. Such a decrease (increase) in r_f is interpreted as a decrease (increase) in the multipliers λ_k, and thus more (less) power is allocated to each user. By appropriately setting the lower and upper values for the bisection over r, $r_{\min}$ and $r_{\max}$, respectively, the process is repeated until the total power consumption to P_{T} is achieved. The whole procedure to solve the power allocation problem for fixed subcarrier assignment is described in Algorithm 1.

Algorithm 1 Optimal power allocation for fixed subcarrier assignment

```
Set $r_{\min} = 0, r_{\max} = \max_k \sum_{n\in\mathcal{N}_k} \mathrm{RA}_{n,k}(p_{n,k})$
repeat
    Set $r_f = (r_{\min} + r_{\max})/2$
    Solve problem (17) using Eq. (20), and the power allocation is denoted as $\overline{p}_{n,k},\ k \in \mathcal{K}, N \in \mathcal{N}$
    The total power consumption is calculated as $P_{\mathrm{c}} = \sum_{n,k}\overline{p}_{n,k}$
    if $P_{\mathrm{c}} < P_{\mathrm{T}}$ then
        Set $r_{\min} = r_f$ and $p^*_{n,k} = \overline{p}_{n,k}, k \in \mathcal{K}, n \in \mathcal{N}_k$
    else
        Set $r_{\max} = r_f$
    end if
until $|r_{\max} - r_{\min}| \le \epsilon$
Output $p^*_{n,k}, k \in \mathcal{K}, n \in \mathcal{N}$
```

3.2 Suboptimal subcarrier allocation algorithm

Assuming the transmit power is equally split across all subcarriers, $p_{n,k} = P_{\mathrm{T}}/N$, the original problem (14) becomes

$$\begin{aligned}&\max_{\rho_{n,k},R}\ R\\ &\text{s.t.}\ \sum_{n\in\mathcal{N}}\rho_{n,k}C_{n,k}(p_{n,k}) \ge R,\ \forall k,\\ &\qquad\sum_{k\in\mathcal{K},n\in\mathcal{N}}\rho_{n,k}p_{n,k} \le P_{\mathrm{T}}.\end{aligned} \tag{24}$$

Problem (24) is an integer programming problem. Thus, finding the optimal solution to Eq. (24) is still very complex. We propose a greedy subcarrier assignment algorithm that finds a suboptimal solution to problem (24). In each iteration, the user with the currently lowest secrecy rate is enforced to occupy one more subcarrier from the available ones. The subcarrier assigned to this user is the one that can give the user the maximum secrecy rate. Denote $\mathcal{S}$ as the set of subcarriers that have not been assigned to users, and C_k as the secrecy rate of user k. The resulting algorithm is described in Algorithm 2.

Note that in step 4, according to the assumption $\alpha_{n,k} = \alpha_{n,\mathrm{e}}$, the expression in Eq. (25) (on the next page) becomes

$$(k^*, n^*) = \arg\max_{k\in\mathcal{U},n\in\mathcal{S}}(\hat{\gamma}_{n,k} - \hat{\gamma}_{n,\mathrm{e}}). \tag{26}$$

The subcarrier assigned to the user with the minimum secrecy rate is the one that has the highest difference in estimation channel gain with respect to the eavesdropper.

Algorithm 2 Greedy subcarrier assignment

```
Set $\mathcal{S}$ as the set of available subcarriers. Initially, $\mathcal{S} = \{1, 2, \ldots, N\}$, $C_1 = C_2 = \cdots = C_K = 0$ and $\rho_{n,k} = 0$, $\forall k$, $\forall n$
while $\mathcal{S} \neq \varnothing$ do
    Determine the set of users with the minimum secrecy rate, $\mathcal{U} = \{k : C_k \leq C_{k'}, \forall k' \neq k\}$
    Find the best user–subcarrier pair in the set $\mathcal{S} \times \mathcal{U}$:
        $(k^*, n^*) = \arg \max_{k \in \mathcal{U}, n \in \mathcal{S}} C_{n,k}(P_{\mathrm{T}}/N, \hat{\gamma}_{n,k}) \quad (25)$
    Assign subcarrier $n^*$ to user $k^*$, $\rho_{n^*,k^*} = 1$
    Remove $n^*$ from the set $\mathcal{S}$, $\mathcal{S} = \mathcal{S} \setminus \{n^*\}$
    Update $C_{k^*} = C_{k^*} + C_{n^*,k^*}(P_{\mathrm{T}}/N, \hat{\gamma}_{n,k})$
end while
```

If the OFDMA system employs time-division duplex (TDD), the BS estimates the uplink channel and obtains the downlink CSI according to the channel reciprocity. If the baseband channel gain from the BS to the k^{th} user on the n^{th} subcarrier satisfies $H_{n,k} = \hat{H}_{n,k} + \epsilon_{n,k}$, where $\hat{H}_{n,k}$ denotes the estimate of $H_{n,k}$ and $\epsilon_{n,k}$ denotes the estimation error that satisfies $\epsilon_{n,k} \sim \mathcal{CN}(0, \sigma_{n,k}^2)$, and $\sigma_{n,k}^2$ is the mean variance of the channel estimation error, our proposed algorithm will still be valid.

3.3 Complexity

The complexity of a bisection method is approximately $\log \frac{1}{\epsilon}$, where ϵ is the required accuracy. In Algorithm 1, an external bisection is required to adjust the value of r, while we use the bisection method per user to search for the Lagrangian multiplier λ_k ($k = 1, 2, \ldots, K$) and calculate the optimal power policy per user across the selected subcarrier for a given λ_k. Therefore, the complexity of Algorithm 1 is $\mathcal{O}(KN \log^3(1/\epsilon))$. In Algorithm 2, two maximum/minimum search operations are performed in each subcarrier assignment iteration. Thus, the complexity of Algorithm 2 is $\mathcal{O}(N(K + N))$, and the overall complexity of our proposed algorithm is $\mathcal{O}(KN^2 \log^3(1/\epsilon)(K + N))$. If we use an exhaustive search method to find the optimal subcarrier assignment, we need K^N searches. Hence, the complexity will be $\mathcal{O}(KN \log^3(1/\epsilon)K^N)$, which is quite high. Therefore, our algorithm has polynomial complexity and is more feasible for practical implementations.

4 Simulation results

We present several simulation results to demonstrate the security rate performance of the OFDMA system under different imperfect CSI conditions using our proposed algorithm. We assume that the transmit power is $P_{\mathrm{T}} = 20$ W, and that the channel is modeled as a frequency-selective Rayleigh fading channel with $E[|h_{n,k}|^2] = E[|h_{n,\mathrm{e}}|^2] = 1$. To simulate imperfect CSI, we generate an independent realization of $\hat{\boldsymbol{H}}_k$, $\hat{\boldsymbol{H}}_{\mathrm{e}}$ and $\boldsymbol{\epsilon}_k$, $\boldsymbol{\epsilon}_{\mathrm{e}}$ according to different imperfect CSI assumptions and then generate $\boldsymbol{H}_k$, which is equal to the sum of them.

In Fig. 2, we test the optimality of our proposed algorithm. We assume that there are $N = 8, 10$ subcarriers with independent and identical distribution and $K = 2$ legitimate users. We use the imperfect CSI assumption discussed in Section 2.3 with simulation parameters summarized in Table 1 and assume that the feedback delays of all users are equal, $\delta m_k = 1$. We compare the secrecy rates of our algorithm with the upper bounds. To obtain the upper bounds, we use an exhaustive search method to search for the maximum secrecy rate among all possible subcarrier allocations. For each subcarrier allocation, we assign the transmit power using the algorithm given in Section 3.1. Fig. 2 shows that the secrecy rate of our algorithm is nearly the same as the optimal value. The gap between the secrecy rate of the proposed algorithm and the optimum does not change as the number of subcarriers increases.

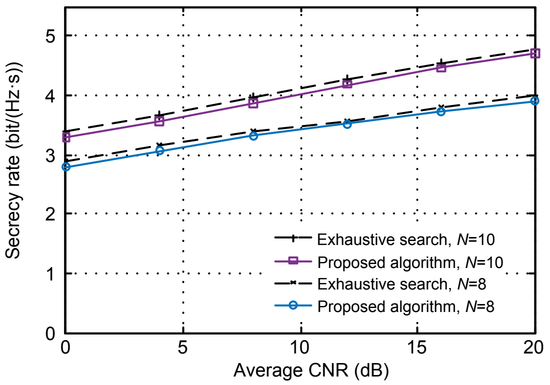

Fig. 2 Comparison of the proposed suboptimal algorithm and the optimal algorithm

Then, we compare the performance of our proposed resource allocation algorithm under different feedback delays, i.e., $\delta m_e = \delta m_k = 1, 5, 8$. We use the imperfect CSI assumption discussed in Section

Table 1 Simulation parameters

Parameter	Value
Carrier frequency, f_c	2.6 GHz
Speed, v_k	50 km/h
Subcarrier spacing, Δf	45 kHz
Maximum transmit power, P_T	20 W
Estimation error of users, σ_e^2	1
Prediction order, Q	5
Channel model	i.i.d.

i.i.d.: independent and identical distribution

2.3 with simulation parameters summarized in Table 1. We also consider the case in which the CSI is perfectly known at the BS. In all of the aforementioned cases, we assume that there are $N = 32$ subcarriers with independent and identical distribution and $K = 4$ legitimate users.

Fig. 3 plots the achieved minimum secrecy rate versus the CNR. The simulation results show that the achieved minimum secrecy rate decreases as the feedback delay δm_k increases. The performance gap between the proposed algorithm and the perfect CSI case increases as CNR increases.

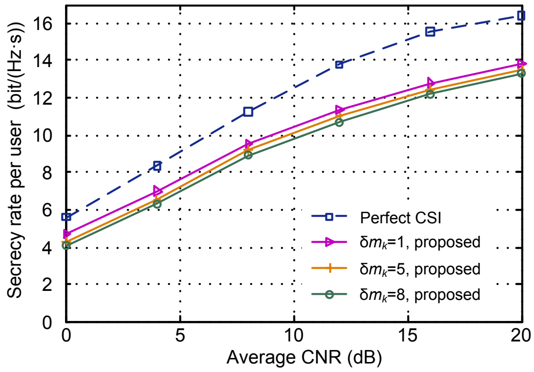

Fig. 3 Comparison of the achieved secrecy rate under different feedback delays

In Fig. 4, we show the secrecy rate per user of different algorithms against feedback channel capacity under the imperfect CSI assumption discussed in Section 2.4. We also consider the case in which the BS can obtain perfect CSI, where the user with the largest power gain gap between the legitimate user and the eavesdropper is chosen to each subcarrier. Then we use the power allocation algorithm given in Section 3.1. We assume that there are $N = 16$ subcarriers with independent and identical distribution and $K = 4$ users. We can see that the secrecy rate per user with imperfect CSI increases as the feedback channel capacity increases and that our proposed algorithm can obtain higher secrecy rates than the algorithms in which the power is distributed equally to each subcarrier. We can also see that the secrecy rate is near the one with perfect CSI when the capacity of the feedback channel is high.

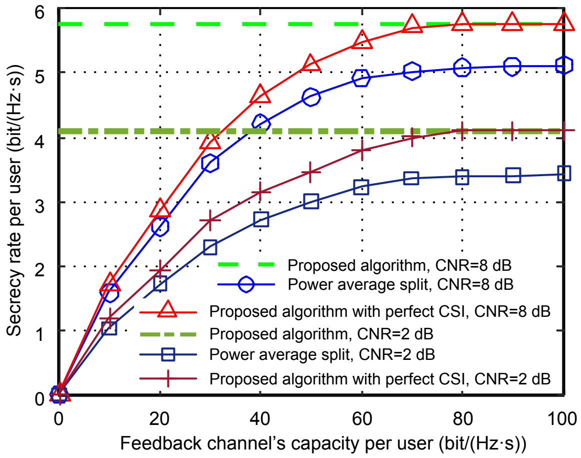

Fig. 4 Secrecy rate versus the capacity of the feedback channel

5 Conclusions

In this paper, we investigated the problem of resource allocation in a security-aware FDD-OFDMA system with partial CSI constraints. We discussed three kinds of imperfect CSI, and established a unified mathematical model of imperfect CSI for the OFDMA system. We formulated the max-min secrecy rate problem under the condition in which the CSI of both legitimate users and the eavesdropper are partially obtained at the BS. Since the optimal algorithm has exponential complexity, an effective algorithm was proposed with acceptable complexity that is more feasible. We proposed a low-complexity suboptimal algorithm that breaks the problem into two subproblems: subcarrier allocation and power allocation. First we solved the power allocation problem for fixed subcarrier assignment using a bisection method; then, we obtained a suboptimal subcarrier allocation solution through the greedy algorithm. Numerical results showed that the performance of the proposed algorithm is close to the optimum. The secrecy rate per user with a limited feedback rate can be very close to the rate with perfect CSI as the feedback rate increases.

References

Barros J, Rodrigues MRD, 2006. Secrecy capacity of wireless channels. IEEE Int Symp on Information Theory, p.356-360. https://doi.org/10.1109/ISIT.2006.261613

Boyd S, Vandenberghe L, 2004. Convex Optimization. Cambridge University Press, New York, USA.

Chen C, Bai L, Wu B, *et al.*, 2011. Downlink throughput maximization for OFMDA systems with feedback channel capacity constraints. *IEEE Trans Signal Process*, 59(1):441-446. https://doi.org/10.1109/TSP.2010.2080270

Chen XM, Chen J, Zhang HZ, et al., 2016. On secrecy performance of multiantenna-jammer-aided secure communications with imperfect CSI. *IEEE Trans Veh Technol*, **65**(10):8014-8024. https://doi.org/10.1109/TVT.2015.2510502

Cheng X, Yang LQ, Shen X, 2015. D2D for intelligent transportation systems: a feasibility study. *IEEE Trans Intell Transp Syst*, 16(4):1784-1793. https://doi.org/10.1109/TITS.2014.2377074

Cheong SKLY, Hellman ME, 1978. The Gaussian wire-tap channel. *IEEE Trans Inform Theory*, 24(4):451-456. https://doi.org/10.1109/TIT.1978.1055917

Cover TM, Thomas JA, 2012. Elements of Information Theory. John Wiley & Sons.

Csiszár I, Korner J, 1978. Broadcast channels with confidential messages. *IEEE Trans Inform Theory*, 24(3):339-348. https://doi.org/10.1109/TIT.1978.1055892

Gradshteyn IS, Ryzhik IM, 2014. Table of Integrals, Series, and Products. Academic Press.

Huang YZ, Al-Qahtani FS, Duong TQ, et al., 2015. Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI. *IEEE Trans Commun*, 63(8):2959-2971. https://doi.org/10.1109/TCOMM.2015.2442248

Huang YZ, Wang JL, Zhong CJ, et al., 2016. Secure transmission in cooperative relaying networks with multiple antennas. *IEEE Trans Wirel Commun*, 15(10):6843-6856. https://doi.org/10.1109/TWC.2016.2591940

Jang J, Lee KB, 2003. Transmit power adaptation for multiuser OFMDA systems. *IEEE J Sel Areas Commun*, 21(2):171-178. https://doi.org/10.1109/JSAC.2002.807348

Jorswieck EA, Wolf A, 2008. Resource allocation for the wiretap multi-carrier broadcast channel. Proc Int Conf on Telecommunications, p.1-6. https://doi.org/10.1109/ICTEL.2008.4652697

Karachontzitis S, Timotheou S, Krikidis I, et al., 2015. Security-aware max–min resource allocation in multiuser OFMDA downlink. *IEEE Trans Inform Forens Secur*, 10(3):529-542. https://doi.org/10.1109/TIFS.2014.2384392

Li Z, Yates R, Trappe W, 2006. Secrecy capacity of independent parallel channels. In: Liu RH, Trappe W (Eds.), Securing Wireless Communications at the Physical Layer. Springer, New York, p.1-18. https://doi.org/10.1007/978-1-4419-1385-2_1

Shen ZK, Andrews JG, Evans BL, 2005. Adaptive resource allocation in multiuser OFDM systems with proportional rate constraints. *IEEE Trans Wirel Commun*, 4(6):2726-2737. https://doi.org/10.1109/TWC.2005.858010

Song GC, Li Y, 2005. Cross-layer optimization for OFDM wireless networks—part II: algorithm development. *IEEE Trans Wirel Commun*, 4(2):625-634. https://doi.org/10.1109/TWC.2004.843067

Wang C, Wang HM, 2015. Robust joint beamforming and jamming for secure AF networks: low-complexity design. *IEEE Trans Veh Technol*, 64(5):2192-2198. https://doi.org/10.1109/TVT.2014.2334640

Wang HM, Wang C, Ng DWK, 2015. Artificial noise assisted secure transmission under training and feedback. *IEEE Trans Signal Process*, 63(23):6285-6298. https://doi.org/10.1109/TSP.2015.2465301

Wang XW, Tao MX, Mo JH, et al., 2011. Power and subcarrier allocation for physical-layer security in OFMDA-based broadband wireless networks. *IEEE Trans Inform Forens Secur*, 6(3):693-702. https://doi.org/10.1109/TIFS.2011.2159206

Wong CY, Cheng RS, Letaief KB, et al., 1999. Multiuser OFDM with adaptive subcarrier, bit, and power allocation. *IEEE J Sel Areas Commun*, 17(10):1747-1758. https://doi.org/10.1109/49.793310

Wong IC, Evans BL, 2009. Optimal resource allocation in the OFMDA downlink with imperfect channel knowledge. *IEEE Trans Commun*, 57(1):232-241. https://doi.org/10.1109/TCOMM.2009.0901.060546

Wu B, Chen C, Bai L, et al., 2010. Resource allocation for OFMDA systems with guaranteed outage probabilities. Proc 6th Int Wireless Communications and Mobile Computing Conf, p.731-735. https://doi.org/10.1145/1815396.1815564

Wu B, Bai L, Chen C, et al., 2011. Resource allocation for maximizing outage throughput in OFMDA systems with finite-rate feedback. *EURASIP J Wirel Commun Netw*, 2011:1-10. https://doi.org/10.1186/1687-1499-2011-56

Wyner A, 1975. The wire-tap channel. *Bell Syst Techn J*, 54(8):1355-1387. https://doi.org/10.1002/j.1538-7305.1975.tb02040.x

Yang N, Yeoh PL, Elkashlan M, et al., 2013. Transmit antenna selection for security enhancement in MIMO wiretap channels. *IEEE Trans Commun*, 61(1):144-154. https://doi.org/10.1109/TCOMM.2012.12.110670

Zhang M, Liu Y, 2016. Energy harvesting for physical-layer security in OFDMA networks. *IEEE Trans Inform Forens Secur*, 11(1):154-162. https://doi.org/10.1109/TIFS.2015.2481797

Zhang M, Liu Y, Zhang R, 2016. Artificial noise aided secrecy information and power transfer in OFDMA systems. *IEEE Trans Wirel Commun*, 15(4):3085-3096. https://doi.org/10.1109/TWC.2016.2516528

Zhang RQ, Cheng X, Yang LQ, et al., 2015. Interference graph based resource allocation (InGRA) for D2D communications underlaying cellular networks. *IEEE Trans Veh Technol*, 64(8):3844-3850. https://doi.org/10.1109/TVT.2014.2356198

Zhang RQ, Cheng X, Yang LQ, 2016. Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks. *IEEE Trans Wirel Commun*, 15(8):5651-5663. https://doi.org/10.1109/TWC.2016.2565579

Appendix: Proof of Proposition 1

According to the conditional PDF obtained in Eq. (10), we can rewrite Eq. (11) as follows:

$$\begin{aligned}&E_{\gamma_{n,k}}[\log_2(1+p_{n,k}\gamma_{n,k})|\hat{\gamma}_{n,k}]\\ =&\int_0^{+\infty}\log_2(1+ax)\mathrm{e}^{-(t+x)}\mathrm{I}_0(2\sqrt{tx})\mathrm{d}x \\ =&F(t),\end{aligned} \tag{A1}$$

where $x=\frac{\gamma_{n,k}}{\alpha_{n,k}}$, $t=\frac{\hat{\gamma}_{n,k}}{\alpha_{n,k}}$, $a=p_{n,k}\alpha_{n,k}$. We rewrite $\mathrm{I}_0(\cdot)$ in the form of Taylor series:

$$\mathrm{I}_0(z)=\sum_{i=0}^{+\infty}\frac{1}{i!i!}\left(\frac{z}{2}\right)^{2i}. \tag{A2}$$

Thus, we have

$$F(t)=\mathrm{e}^{-t}\sum_{i=0}^{+\infty}\frac{t^i}{i!i!}\int_0^{+\infty}\log_2(1+ax)\mathrm{e}^{-x}x^i\mathrm{d}x. \tag{A3}$$

The derivative of $F(t)$ is

$$\begin{aligned}F'(t)=&\mathrm{e}^{-t}\sum_{i=0}^{+\infty}\frac{t^i}{i!(i+1)!}\int_0^{+\infty}\log_2(1+ax)\\ &\cdot\mathrm{e}^{-x}[x^{i+1}-(i+1)x^i]\mathrm{d}x\\ =&\frac{\mathrm{e}^{-t}}{\ln 2}\sum_{i=0}^{+\infty}\frac{t^i}{i!(i+1)!}G_i,\end{aligned} \tag{A4}$$

where $G_i=\int_0^{+\infty}\ln(1+ax)\mathrm{e}^{-x}[x^{i+1}-(i+1)x^i]\mathrm{d}x$. In addition, we have

$$\begin{aligned}G_i=&\int_0^{+\infty}\ln(1+ax)\mathrm{e}^{-x}x^{i+1}\mathrm{d}x\\ &-(i+1)\int_0^{+\infty}\ln(1+ax)\mathrm{e}^{-x}x^i\mathrm{d}x\\ =&-\int_0^{+\infty}\ln(1+ax)x^{i+1}\mathrm{d}\mathrm{e}^{-x}\\ &-(i+1)\int_0^{+\infty}\ln(1+ax)\mathrm{e}^{-x}x^i\mathrm{d}x\\ =&-\ln(1+ax)\mathrm{e}^{-x}x^{i+1}|_{x=0}^{x=+\infty}\\ &+\int_0^{+\infty}\mathrm{e}^{-x}\mathrm{d}[\ln(1+ax)x^{i+1}]\\ &-(i+1)\int_0^{+\infty}\ln(1+ax)\mathrm{e}^{-x}x^i\mathrm{d}x\\ =&\int_0^{+\infty}\mathrm{e}^{-x}\left[\frac{a}{1+ax}x^{i+1}+(i+1)\ln(1+ax)x^i\right]\mathrm{d}x\\ &-(i+1)\int_0^{+\infty}\ln(1+ax)\mathrm{e}^{-x}x^i\mathrm{d}x\\ =&\int_0^{+\infty}\mathrm{e}^{-x}\frac{a}{1+ax}x^{i+1}\mathrm{d}x>0.\end{aligned} \tag{A5}$$

Thus, $F'(t)>0$, $F(t)$ is an increasing function of t, and we obtain Proposition 1.