Communications and Network, 2013, 5, 204-210
http://dx.doi.org/10.4236/cn.2013.53B2039 Published Online September 2013 (http://www.scirp.org/journal/cn)

A Resource Allocation Algorithm of Physical-Layer Security for OFDMA System under Non-ideal Condition

Xiao-min Ran, You-quan Mo, Yu-lei Chen
National Digital Switching System Engineering & Technological Research Center, Zhengzhou, China
Email: hongyinghunan@126.com

Received June, 2013

ABSTRACT

In this paper, a resource allocation scheme based on physical layer security under non-ideal condition for OFDMA system is introduced. Firstly, the program uses the information security constructing an OFDMA system Wiretap Channel Model under non-ideal condition. Based on this model, artificial noise is generated for secure communications combatting passive multiple eavesdroppers. In order to maximize the average secrecy outage capacity without channel state information of eavesdroppers, we use dual decomposition method to implement subcarriers and power allocation in joint optimization. Simulation results show that the average secrecy outage capacity can achieve 7.81 bit/s/Hz while secrecy outage probability is 0.05 with 50 dB mtransmitpower and 64 sub-carrier for 8 authorized users.

Keywords: OFDMA System; Physical Layer Security; Secrecy Outage Capacity; Resource Allocation

1. Introduction

With many good characteristics, OFDM (Orthogonal Frequency Division Multiplexing) not only has the resistance to multipath fading, but also the allocation of resources can be flexible depending on the constraints. It has been chosen as an important candidate technology by Wireless communication standards such as 3GPP LTE, IEEE802.16WiMAX and IEEE802.22 WRAN.

In recent years, there are many researches about physical layer security of OFDM system, unlike traditional channel encryption method, the new method takes advantages of the channel characteristics differences between the communicating parties, it achieves the secure transmission in wireless signal while ensure the communication quality of a legitimate user by increasing the difficulty of the eavesdropper to intercept or restore the signal and measure the security of the system by Confidential capacity[1,2]. Csiszar[3]proposes a differential encoding method to lower the probability of interception in OFDM system; Renna[4,5] analyze the Confidential capacity of OFDM system with different receiver. Jorswieck[6] and Li[7] discuss how to deal with the allocation of power to maximize the confidential rate in single-user and multi-user OFDM system.

Existing literatures about physical resource allocation in multi-user OFDMA(Orthogonal Frequency Division Multiple Access) system are always based on the ideal condition that authorized user`s channel quality is better than the eavesdropper`s, and lack of attention on the physical resource allocation methods to obtain higher safety in bad communication environment. In this paper, an algorithm about OFDMA physical resource allocation for non-ideal environment is proposed. First, we construct an OFDMA network security model. Then, the concept of system average confidential capacity is putted forward as an index to measure the safety of system when the state of wiretap channel is unknown. Finally, the joint optimization distribution of subcarrier and power is realized by dual decomposition to maximize the average confidential interrupt capacity.

2. OFDMA System Network Model

Assume that there are K authorized users, N_E eavesdroppers in OFDM network. Each eavesdropper shares the received message (equally, one eavesdropper with N_E antenna), as shown in **Figure 1**. Because there are many eavesdroppers in the system, In order to guarantee that the system can secure communication, the sender need to use multi-antenna, and the number of antenna $N_A > N_E$. Assume that each authorized user uses single antenna when receiving. And there are N_F subcarriers in OFDMA system, consider that all the carrier channels are slow fading channels, in a short time the channel impulse response remains unchanged. The signal that the $k\ th \in \{1,\cdots,K\}$ user and eavesdropper received on the $i\ th \in \{1,\cdots,N_F\}$ carrier can be written as

$$y_{k,i} = \mathbf{h}_{k,i}\mathbf{x}_{k,i} + n_i \quad (1)$$

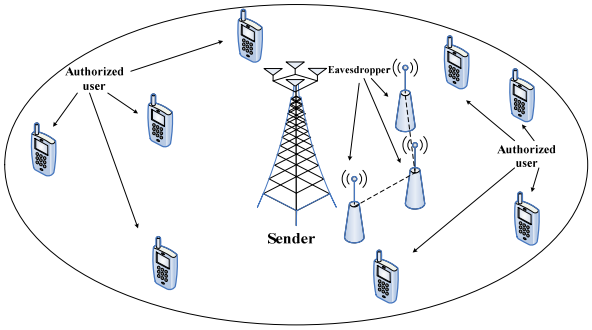

Figure 1. OFDMA network model.

$$\mathbf{y}_{E,i} = \mathbf{G}_{E,i}\mathbf{x}_{k,i} + \mathbf{e}_i \tag{2}$$

where $\mathbf{x}_{k,i} \in C^{N_A \times 1}$ is the signal vector sent by authorized user k on carrier i, $C^{N\times M}$ is a $N \times M$ matrix. $\mathbf{h}_{k,i} \in C^{1\times N_A}$ is the CSI vector of the sender and the authorized user k on the i-thcarrier, $\mathbf{G}_{E,i} \in C^{N_E \times N_A}$ is the CSI matrix of the sender and eavesdropper on the i-th carrier, $\mathbf{h}_{k,i}$, $\mathbf{G}_{E,i}$ contains the influence of path loss and the multipath fading. n_i is the AWGN (Additive White Gaussian Noise) of legitimate user k on the i-th carrier, andit submitsGaussian distribution with mean of 0 and variance of N_0, $\mathbf{e}_i \in C^{N_E \times 1}$ is the AWGN vector of eavesdropper on i-th carrier, and it obeys Gaussian distribution with mean of 0 and variance of N_0. Normalize all the noise variance at the receiver, set $N_0 = 1$. Assume that the sender can fully know the CSI(Channel State Information) of each authorized user, namely $\mathbf{h}_{k,i}$ is already known. Because of the passive interception of the eavesdropper, the sender can't learn the CSI of the eavesdropper, namely $\mathbf{G}_{E,i}$ is unknown, where

$$i \in \{1, \cdots, N_F\}, \text{ and } k \in \{1, \cdots K\}.$$

Giving that the sender can't acquire the accurate number and position of eavesdroppers，so let us image a poor situation, set $N_E = N_A - 1$. In order to achieve safe transmission while the sender and eavesdropper are very near, we can use artificial noise[8] to guarantee security, namely, let the sending signal $\mathbf{x}_{k,i}$ contains the two parts of useful signal $u_{k,i}$ and noise signal $\mathbf{v}_{k,i}$

$$\mathbf{x}_{k,i} = \mathbf{b}_{k,i}u_{k,i} + \mathbf{W}_{k,i}\mathbf{v}_{k,i} \tag{3}$$

where, $\mathbf{v}_{k,i}$ is an independent and identically distributed complex Gaussian random variable with the variance of σ_i^2, $\mathbf{W}_{k,i}$ is the orthogonal basis on the null space of $\mathbf{h}_{k,i}$, namely $\mathbf{W}_{k,i}^{\mathrm{H}}\mathbf{W}_{k,i} = \mathbf{I}_{k,i}$ and $\mathbf{h}_{k,i}\mathbf{W}_{k,i}\mathbf{v}_{k,i} = 0$. $\mathbf{I}_{k,i}$ is a $(N_A - 1)\times(N_A - 1)$ unit matrix. In order to maximize the signal-to-noise ratio of authorized user k, we can use the method of specific maximum beam forming, so the received signal can be written as

$$y_{k,i} = \mathbf{h}_{k,i}\mathbf{b}_{k,i}u_{k,i} + n_i \tag{4}$$

$$\mathbf{y}_{E,i} = \mathbf{G}_{E,i}\mathbf{b}_{k,i}u_{k,i} + \mathbf{G}_{E,i}\mathbf{W}_{k,i}\mathbf{v}_{k,i} + \mathbf{e}_i \tag{5}$$

Assume that the total transmitting power of the *k-th* user on the i-th carrier is $P_{k,i}$, the power of useful signal is $p_{k,i}$, so $P_{k,i} = p_{k,i} + (N_A - 1)\sigma_i^2$. $\alpha_{k,i}$ is defined as the power ratio of useful signal, then there will be

$$p_{k,i} = \alpha_{k,i}P_{k,i} \tag{6}$$

$$\sigma_i^2 = \frac{(1-\alpha_{k,i})P_{k,i}}{N_A - 1} \tag{7}$$

According to the CSI between the sender and the authorized user, we can achieve the channel capacity of user *k* on carrier *i*

$$C_{k,i} = \log_2\left(1 + p_{k,i}\left\|h_{k,i}\right\|^2\right) \tag{8}$$

while the channel capacity of eavesdropper on carrier *i* can be indicated as

$$C_{E,i} = \log_2\left|\mathbf{I} + \frac{p_{k,i}\boldsymbol{\psi}_i\boldsymbol{\psi}_i^{\mathrm{H}}}{\sigma_i^2\boldsymbol{\Phi}_i\boldsymbol{\Phi}_i^{\mathrm{H}} + 1}\right| \tag{9}$$

where, $\boldsymbol{\psi}_i = \mathbf{G}_{E,i}\mathbf{b}_{k,i}$, $\boldsymbol{\Phi}_i = \mathbf{G}_{E,i}\mathbf{W}_{k,i}$. Thus, (9) can be converted to:

$$\begin{aligned} C_{E,i} &= \log_2\left|\mathbf{I} + \frac{p_{k,i}\boldsymbol{\psi}_i\boldsymbol{\psi}_i^{\mathrm{H}}}{\sigma_i^2\boldsymbol{\Phi}_i\boldsymbol{\Phi}_i^{\mathrm{H}}}\right| \\ &= \log_2\left(1 + \frac{\alpha_{k,i}(N_A - 1)}{1-\alpha_{k,i}}\boldsymbol{\psi}_i^{\mathrm{H}}\left(\boldsymbol{\Phi}_i\boldsymbol{\Phi}_i^{\mathrm{H}}\right)^{-1}\boldsymbol{\psi}_i\right) \end{aligned} \tag{10}$$

So the secrecy capacity of user k achieved on carrier *i* can be shown as

$$\begin{aligned} C_{k,i}^s &= \left[C_{k,i} - C_{E,i}\right]^+ \\ &= \left[\log_2\left(1 + p_{k,i}\left\|h_{k,i}\right\|^2\right)\right. \\ &\quad \left. - \log_2\left(1 + \frac{\alpha_{k,i}(N_A - 1)}{1-\alpha_{k,i}}\boldsymbol{\psi}_i^{\mathrm{H}}\left(\boldsymbol{\Phi}_i\boldsymbol{\Phi}_i^{\mathrm{H}}\right)^{-1}\boldsymbol{\psi}_i\right)\right]^+ \end{aligned} \tag{11}$$

3. The Resource Allocation Algorithm of Physical Layer Security in Non-ideal Environment

The concept of average confidential outage capacity is the general average security bits from the sender to all the authorized users per secondindicate, it can be described as

$$C_{out} = \sum_{k=1}^{K}\sum_{i=1}^{N_F}\rho_{k,i}R_{i,k}^s \Pr\left[R_{i,k}^s < C_{k,i} - C_{E,i}|\mathbf{h}_{k,i}\right] \tag{12}$$

Among them, $\rho_{k,i}$ is the indication of sub-carrier's allocation, when user k employ in sub-carrier *i*, $\rho_{k,i}$=1, otherwise $\rho_{k,i}$=0. In order to make the security of the system reaching a maximum, in the conditions of total

power constraint, the optimization problem of making the confidential outage capacity maximization is established. Assuming that the authorized users can meet their needs of confidential outage probability, so the mathematical problems are as follows

$$\max_{p_{k,i},\rho_{k,i},\alpha_{k,i}} C_{out}\left(p_{k,i},\rho_{k,i},\alpha_{k,i}\right)$$

$$\begin{aligned}
&\text{Subject,}\ \ \Pr\left[R_{i,k}^{s} \ge C_{k,i} - C_{E,i}|\mathbf{h}_{k,i}\right] \le \varepsilon_k,\ \ \forall k,i,\\
&\sum_{k=1}^{K}\sum_{i=1}^{N_F}\rho_{k,i}P_{k,i} \le P_t,\ \ and\ \ P_{k,i} \ge 0, \forall k,i,\\
&\sum_{k=1}^{K}\rho_{k,i} \le 1,\ \ and\ \ \rho_{k,i} = \{0,1\}, \forall k,i,\\
&0 < \alpha_{k,i} \le 1,\ \ \forall k,i.
\end{aligned} \tag{13}$$

The essence of the problem is to complete the maximization of system performance through rational allocation of each user's carrier and power, using channel state information and the added artificial noise which have been achieved. (13) Indicates that, constraint conditions that exist in the form of probability. In order to simplify the problem, the constraint conditions can be transformed into objective function. Then it can be solved through dual decomposition method.

3.1. The Transformation of Optimization Problem

In order to make the design of resource allocation algorithm not be effected by the CSI of eavesdropper' schannel, the following lemma can be given firstly.

Lemma: For a given security outage probability ε_k, the security rate of authorized user k in carrier i is equivalent to the following form

$$R_{i,k}^{s} = \left[\begin{array}{l}\log_2\left(1+\alpha_{k,i}P_{k,i}\left\|h_{k,i}\right\|^2\right)\\ -\log_2\left(1+\dfrac{\alpha_{k,i}\left(N_A-1\right)F_z^{-1}\left(\varepsilon_k\right)}{1-\alpha_{k,i}}\right)\end{array}\right]^{+} \tag{14}$$

Among them, $F_z^{-1}\left(\varepsilon_k\right)$ is the inverse function of $F_z\left(z\right) = \dfrac{\sum_{n=0}^{N_E-1}\mathbf{C}_{N_A-1}^{n}z^n}{\left(1+z\right)^{N_A-1}} = \varepsilon_k$, the proof is given in Appendix. The lemma uses the interference characteristics of multiple antenna, computes the security outage probability by tapping channel information of the probability distribution function to express the security rate.

When $P_{k,i}$ is fixed, in order to make the security outage capacity achieve the maximum, let $\dfrac{\partial R_{i,k}^{s}}{\alpha_{k,i}} = 0$. Then the optimum solution of $\alpha_{k,i}$ is:

$$\alpha_{k,i}^{*} = \frac{-P_{k,i}\left\|h_{k,i}\right\|^2 + \sqrt{\begin{array}{l}\left(N_A-1\right)P_{k,i}\left\|h_{k,i}\right\|^2 F_z^{-1}\left(\varepsilon_k\right)\\ \left[P_{k,i}\left\|h_{k,i}\right\|^2 - \left(N_A-1\right)F_z^{-1}\left(\varepsilon_k\right)+1\right]\end{array}}}{P_{k,i}\left\|h_{k,i}\right\|^2\left[\left(N_A-1\right)F_z^{-1}\left(\varepsilon_k\right)-1\right]} \tag{15}$$

With the increase of transmission power, $-P_{k,i}\left\|h_{k,i}\right\|^2$ will continue growing, but $\left(N_A-1\right)F_z^{-1}\left(\varepsilon_k\right)$ maintain a fixed value of constant. So (15) can be predigested as

$$\alpha_{k,i}^{*} \approx \frac{\sqrt{\left(N_A-1\right)F_z^{-1}\left(\varepsilon_k\right)}-1}{\left(N_A-1\right)F_z^{-1}\left(\varepsilon_k\right)-1} \approx \frac{1}{\sqrt{\left(N_A-1\right)F_z^{-1}\left(\varepsilon_k\right)}} \tag{16}$$

Combining (16) with (14)

$$R_{i,k}^{s} = \left[\log_2\left(1+P_{k,i}\Gamma_{k,i}\right) - \log_2\left(1+\Lambda_{k,i}\right)\right]^{+} \tag{17}$$

where

$$\Gamma_{k,i} = \frac{\left\|h_{k,i}\right\|^2}{\sqrt{\left(N_A-1\right)F_z^{-1}\left(\varepsilon_k\right)}},$$

$$\Lambda_{k,i} = \frac{\left(N_A-1\right)F_z^{-1}\left(\varepsilon_k\right)}{\sqrt{\left(N_A-1\right)F_z^{-1}\left(\varepsilon_k\right)}-1}$$

So when the SNR is high, the SINR of eavesdropper is a fixed value, and is never influenced by the transmitted power P_t.

Taking (17) into (13), the optimization problem is still a NP-hard problem. Using the method of literature[10] to relax $\rho_{k,i}$, the problem can be converted to a convex optimization problems. Literature[11]indicates that when the system's sub-carriers are enough, the error caused by relaxation will be close to zero. In order to simply (13) further, the constraint conditions of ε_k can narrow the range only an equality. Let $\rho_{k,i} \in [0,1]$, $\tilde{P}_{k,i} = P_{k,i}\rho_{k,i}$, then (13) can be converted to the below

$$\max_{\tilde{P}_{k,i},\rho_{k,i}} \sum_{k=1}^{K}\left(1-\varepsilon_k\right)\sum_{i=1}^{N_F}\rho_{k,i}\tilde{R}_{i,k}^{s}$$

$$\begin{aligned}
&\text{Subject,}\ \ \sum_{k=1}^{K}\sum_{i=1}^{N_F}\tilde{P}_{k,i} \le P_t,\ \ \text{and}\ \ \tilde{P}_{k,i} \ge 0, \forall k,i,\\
&\sum_{k=1}^{K}\rho_{k,i} \le 1,\ \ and\ \ \rho_{k,i} \in [0,1], \forall k,i,
\end{aligned} \tag{18}$$

where $\tilde{R}_{i,k}^{s} = R_{i,k}^{s}\left|_{P_{k,i}=\tilde{P}_{k,i}/\rho_{k,i}}\right.$. Because $R_{i,k}^{s}\left|_{P_{k,i}=\tilde{P}_{k,i}}\right.$ is a concave function to $\tilde{P}_{k,i}$, and $\rho_{k,i}\tilde{R}_{i,k}^{s}$ is the perspective function of $R_{i,k}^{s}\left|_{P_{k,i}=\tilde{P}_{k,i}}\right.$, according to literature[12], $\rho_{k,i}\tilde{R}_{i,k}^{s}$ is also aconcave function of $\tilde{P}_{k,i}$, then(18) is a convex optimization problem. For the optimization vari-

ables of above-mentioned problem are coupling, the dual decomposition method of convex optimization theory can be used to solve the problem.

3.2. The Optimization Problem Solved by Dual Method

3.2.1. Dual Transformation and Decomposition

Dual decomposition method [13] can decompose the original complex optimization problem into main problem and sub-problem which can be solved easily. We can get the final results of the original problem by solving the main problem and the sub-problem. At first, structure the Lagrangiandual of (18).

$$\begin{aligned} L\left(\boldsymbol{\rho},\mathbf{P},\vec{\lambda}_1,\lambda_2\right) = &\sum_{k=1}^{K}\left(1-\varepsilon_k\right)\sum_{i=1}^{N_F}\rho_{k,i}\tilde{R}_{i,k}^{s} \\ &+\sum_{i=1}^{N_F}\lambda_{1i}\left(1-\sum_{k=1}^{K}\rho_{k,i}\right) \\ &+\lambda_2\left(P_T-\sum_{k=1}^{K}\sum_{i=1}^{N_F}\tilde{P}_{k,i}\right) \end{aligned} \tag{19}$$

where $\boldsymbol{\rho}$ is the sum of allocation instruction of each carrier, P is the sum of allocation power of each carrier. $\vec{\lambda}_1=\left[\lambda_{11},\lambda_{12},\cdots,\lambda_{1N_F}\right]$, λ_2 is the Lagrange multiplier of each constraint condition. The dual problem is to solve the original problem through tight upper bound. Therefore, the dual problem of (18) can be expressed as $\min_{\vec{\lambda}_1,\lambda_2}\max_{\boldsymbol{\rho},\mathbf{p}} L\left(\boldsymbol{\rho},\mathbf{p},\vec{\lambda}_1,\lambda_2\right)$. Solving the dual problem is divided into two layers, a main problem to be solved at a higher level; K independent sub-problems to be solved at a lower level, each sub-problem correspond to a user. Therefore, the sub-problem k can be described as

$$\begin{aligned} &\max_{\rho_{k,i},\tilde{P}_{k,i}}\left(1-\varepsilon_k\right)\sum_{i=1}^{N_F}\rho_{k,i}\left(\tilde{R}_{i,k}^{s}-\lambda_{1i}\right)-\lambda_2\sum_{i=1}^{N_F}\tilde{P}_{k,i} \\ &\text{Subject}\quad \rho_{k,i}\in[0,1]\ \ and\ \ \tilde{P}_{k,i}\ge 0,\forall i \end{aligned} \tag{21}$$

The main problem can be described as

$$\begin{aligned} &\min_{\lambda_{1i},\lambda_2}\sum_{k=1}^{K}G_k\left(\vec{\lambda}_1,\lambda_2\right)+\sum_{i=1}^{N_F}\lambda_{1i}+\lambda_2 P_T \\ &\text{Subject}\ \ \lambda_{1i}\ge 0,\forall i\ \ \text{and}\ \ \lambda_2\ge 0. \end{aligned} \tag{22}$$

where $G_k(\cdot)$ is the optimal value of the objective function in sub-problem, which can be obtained by solving-sub-problem.

3.2.2. The Solving of Main Problem and Sub-problems

When the Lagrange coefficient in (21) is a fixed value, K-T conditions can deduce the optimal power allocation of user k on carrier i.

$$\tilde{P}_{k,i}^{*}=\rho_{k,i}P_{k,i}^{*}=\rho_{k,i}\left[\frac{1-\varepsilon_k}{\lambda_2\ln(2)}-\frac{\sqrt{\left(N_F-1\right)F_z^{-1}\left(\varepsilon_k\right)}}{\left\|h_{k,i}\right\|^2}\right]^{+} \tag{23}$$

According the above formula， the optimal power allocation can be observed as water injection in a multi-horizontal surface, different users have different water lines $\frac{1-\varepsilon_k}{\lambda_2\ln(2)}$. To obtain the allocating power of each user's sub-carrier, we should find the partial derivative of $\rho_{k,i}$ using 21. According to the K-T conditions

$$\frac{\partial G_k}{\partial\rho_{k,i}}=A_{k,i}-\lambda_{1i}\begin{cases}=0 & 0<\rho_{k,i}<1\\ >0 & \rho_{k,i}=1\end{cases} \tag{24}$$

where

$$A_{k,i}=\left(1-\varepsilon_k\right)\left(\log_2\left(1+P_{k,i}^{*}\Gamma_{k,i}\right)-\log_2\left(1+\Lambda_{k,i}\right)-\frac{P_{k,i}^{*}\Gamma_{k,i}}{\ln(2)\left(1+P_{k,i}^{*}\Gamma_{k,i}\right)}\right)$$

it can be seen from the above formula that when $0<\rho_{k,i}\le 1$, there is $A_{k,i}\ge\lambda_{1i}$, in order to be able to get the integer value of $\rho_{k,i}$, $\rho_{k,i}$ can be defined as

$$\rho_{k,i}=\begin{cases}1, & A_{k,i}\ge\lambda_{1i}\\ 0, & otherwise\end{cases} \tag{25}$$

For each of the sub-carriers there is no more than one nonzero $\rho_{k,n}$. The above formula is equivalent to allocate sub-carrier i to the user of the sub-carrier which has the maximum $A_{k,i}$. The optimal power allocation of the carrier can be written as

$$\rho_{k,i}^{*}=\begin{cases}1, & A_{k,i}=\max_j A_{k,j}\ \ and\ \ A_{k,j}\ge 0\\ 0, & otherwise\end{cases} \tag{26}$$

After the solving of the sub-problem, we need to solve the λ_{1i}, λ_2 in main problem. From (25) it can be deduced that λ_{1i} in the optimal solution can take any one value between the largest and the second largest $A_{k,i}$ of sub-carrier i. The value of λ_2 can be obtained by sub-gradientiterative algorithm

$$\lambda_2(t+1)=\left[\lambda_2(t)-\alpha(t)\left(P_t-\sum_{k=1}^{K}\sum_{i=1}^{N_F}\tilde{P}_{k,i}^{*}\right)\right]^{+} \tag{27}$$

where t is the number of iterations, $\alpha(t)$ is the iterative step. As long as iteration step meets certain conditions, you can guarantee iterations to converge to the optimal solution. Therefore, performing loop iteration on solving process of the main problem until all parameters convergence, we will get the optimal solution of the original problem.

3.3. Process of Resource Allocation Algorithms and Complexity Analysis

The algorithm processes can be expressed as **Table 1**. The calculation amount of the proposed algorithm is mainly focused on the dual decomposition algorithm. The total computational complexity can be approximated as $O(KN)$, which is greatly less compared to the computational complexity $O(K^N)$ of the exhaustive search. In the same time, the sender does not participate in solving each sub-problem, only according λ_{1i}, λ_2 to control the resource allocation of each user, so the calculation complexity for the sender is reduced greatly.

4. Simulation and Analysis

4.1. Simulation Conditions

It is assumed that the carrier number of OFDMA network $N_F = 64$, the number of authorized users $K = 8$, the secrecy outage probability which is required by each user $\varepsilon_k = 0.05, \forall k$. It is assumed that the coverage of transmission signal is 1 km, the distance between the eavesdropper and the sender should be closer than that between authorized user and the sender, path loss uses the modified Hata path loss model, shadowing takes log-normal shadow fading. Small scale fading takes Cost 231 model [14], the noise power spectral density takes-120 dBm. And set the iteration step $\alpha(t) = a/t$, where a is a constant. Perform simulation of the proposed algorithm through Monte Carlo method, take the average of the 200 times Channel implementation result as the final simulation results.

Comparing the performance of the two basic OFDMA resource allocation method, method 1 considers to allocate carrier evenly to all authorized users, in this case, each user will get 8 subcarriers, each user gets the same power $P_T/8$, we use the method in article[6] to complete the carrier power allocation within each user. Method 2 considers to allocate subcarrier to user with the largest channel gain, then carriers power is allocated equally, the power obtained by each carrier is $P_T/64$.

Table 1. Resource allocation algorithm.

It is known that sender can get all the channel state information $\mathbf{h}_{k,i}$ of each authorized user, the total transmit poweris P_t.
First, initialization: λ_{1i}, λ_2 will be initialized to random positive number.
Second, the iterative process:
Step1: calculate the allocating power value for each carrier by (23), and the negative value to be zero.
Step2: $A_{k,i}$ is calculated by (24), execution on any sub-carrier i: $k^* = \arg\max_k A_{k,i}$ carrier i is allocated to the users with the largest $A_{k,i}$. If more than one user has the same $A_{k,i}$ value, we randomly choose one of them to make the optional user's serial number as k^*; judge $A_{k,i}$ is positive or not , if all $A_{k,i}$ are negative, the carrier i will not be assigned.
Step3: according to (27) update λ_2, let $A'_{k,i}$ be a second largest value in $A_{k,i}$, then λ_{1i} can be $\left(A'_{k,i} + A^*_{k,i}\right)/2$.
Step4: If λ_2 don't convergence, continue step1, 2, 3; Otherwise, the algorithm terminates.

4.2. Comparison of Secrecy Outage Capacity of Different Allocation Methods

Take the number of eavesdroppers $N_E = 2$, compare achievable throughput of eavesdropper and secrecy outage capacity of each allocation method in different transmit power. As shown in **Figure 2**, it can be clearly seen from the figure. The average secrecy outage capacity of this allocation method system is far higher than that of the other two allocation method systems in the same transmit power, and with the increasing of transmit power, the rise of secrecy outage capacity of this allocation method is obviously higher than that of the other two allocation methods. In addition, it can also be seen that when carrier allocation is equivalent, secrecy outage capacity of the system is the lowest. This shows that the optimal allocation of the carrier is more important than the optimal allocation of power and therefore has a greater impact on the security of the system. It can be found from the figure, the number of transmit antennas will influence the size of secrecy outage capacity. Com-

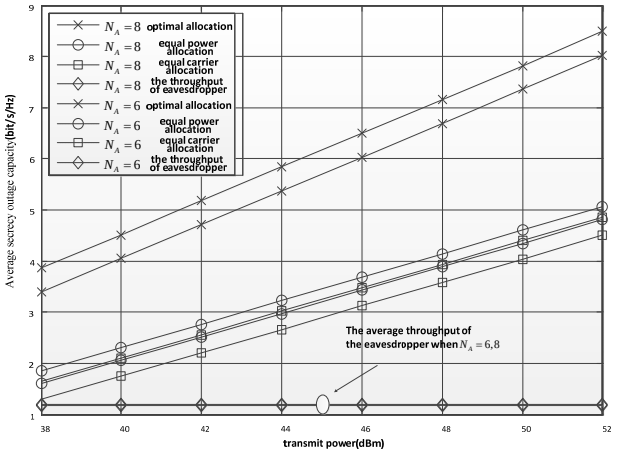

Figure 2. The comparison of Secrecy outage capacity of different allocation methods.

pared to $N_A = 6$, when $N_A = 8$, secrecy outage capacity improves. This is because when the number of emission antennas increases, the overall signal-to-noise ratio of the system will also increase. For the eavesdropper, proportion of artificial noise will also increase. Therefore, secrecy outage capacity of the system will increase. It can be seen from the figure that when the eavesdropper through put is the same, the artificial noise has a great influence on the eavesdropper. Although the total transmit power is increasing, the average throughput of the eavesdropper is always maintained at a very low pos

4.3. The Influence of the Number of Eavesdroppers on Secrecy outage capacity

Define the number of transmit antennas $N_A = 8$. As shown in **Figure 3**, with increasing number of eavesdroppers, secrecy outage capacity is sustained declining. This is due to when the number of the eavesdroppers increase, the suppression of increase in throughput will need more power to produce artificial noise, in case that the total power is constant, the share of the power of the useful signal is bound to reduce, thereby the average secrecy outage capacity will decline. It can also be seen from the figure that although the increasing number of the eavesdroppers will decrease the secrecy outage capacity of the system, as long as $N_A > N_E$, the secrecy outage capacity of this method does not tend to 0, for two other allocation methods when $N_E = 7$, the secrecy outage capacity of the system has dropped to a very low level, which further illustrates that the method has certain advantages in protecting the security of the system.

4.4. The Influence of Outage Probability on Secrecy outage capacity

Take the transmission power $P_t = 44\text{dBm}$, the number of transmitting antennas $N_A = 8$, and the number of the eavesdroppers $N_E = 2$, we analyze the influence of outage probability on the secrecy outage capacity. As shown in **Figure 4**, with the increasing of selected outage probability, the average secrecy outage capacity which system can achieve will slightly upgrade. This shows that when the user is able to endure high outage probability, the secrecy outage capacity which system can achieve will increase, but as artificial noise shares more power, the power of useful signal is relatively small, so the level of increase is not large. It can also be seen from the figure that when the number of authorized users $K = 16$, the secrecy outage capacity which system can achieve is higher than that when the number of authorized users $K = 8$. This illustrates that the method can take advantage of the diversity of multi-user to achieve the effect of diversity, but for the other two allocation methods, this effect is not very obvious.

5. Conclusions

In this paper, a resource allocation algorithm for OFDMA physical layer security under a non-ideal environmentis proposed to solve the problem of secure transmission of OFDM system. Firstly, we build the security model of OFDMA system network based on artificial noise, in the presence of multiple eavesdroppers. Then, average secrecy outage capacity of the system is defined as the optimal goal without eavesdropper channel state. Finally, to further simplify the optimization problem, the joint optimal allocation of subcarrier and power is realized via dual decomposition method. Simulation results show that, total transmit power of the system is 50 dBm, 64 subcarriers are chosen to provide services for eight authorized users, when the secrecy outage capacity of each user is 0.05, the average secrecy outage capacity can be up to 7.81 bit/s/Hz.

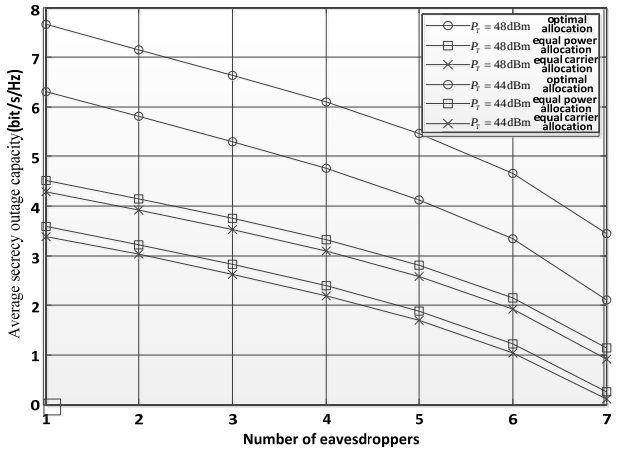

Figure 3. The influence of the number of eavesdroppers on Secrecy outage capacity.

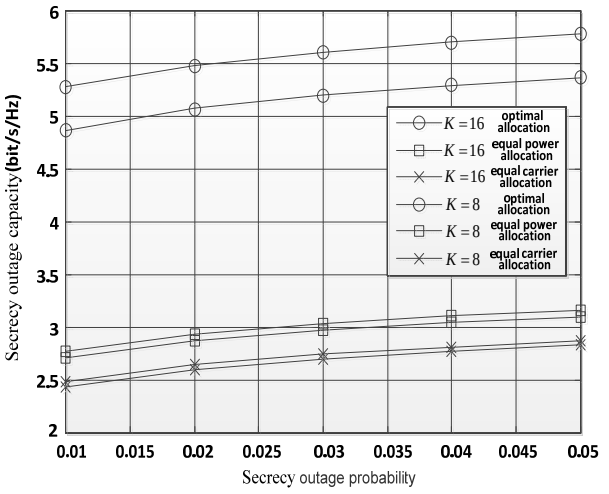

Figure 4. The influence of outage probability on secrecy-outage capacity.

REFERENCES

[1] A. D. Wyner, "The Wire-tap Channel," *The Bell System Technical Journal*, Vol. 54, No. 8, 1975, pp. 1355-1387. doi:10.1002/j.1538-7305.1975.tb02040.x

[2] I. Csiszar and J. Koner, "Broadcast Channels with Confidential Messages," *IEEE Transactions on Information Theory*, Vol. 24, No. 3, 1978, pp. 339-348. doi:10.1109/TIT.1978.1055892

[3] Z. Li and X. G. Xia, "A Distributed Differentially Encoded OFDM Scheme for Asynchronous Cooperative Systems with Low Probability of Interception," *IEEE Transactions on Wireless Communication*, Vol. 8, No. 7, 2009, pp. 3372-3379. doi:10.1109/TWC.2009.080365

[4] F. Renna, N. Laurenti and H. V. Poor, "Physical Layer Secrecy for OFDM Systems," in Proceedings of the IEEE European Wireless Conference, Lucca, Italy, 2010, pp. 782-789.

[5] F. Renna, N. Laurenti and H. V. Poor, "High SNR Secrecy Rates with OFDM Signaling over Fading Channels," in Proceedings of the IEEE 21thInternational Symposium on Personal Indoor and Mobile Radio Communications,Istanbul, Turkey, 2010, pp. 2692-2697.

[6] E. Jorswieck and A. Wolf, "Resource Allocation for the Wire-tap Multi-carrier Broadcast Channel," in Proceedings of International Workshop on Multiple Access Communications, Petersburg, Russia, 2008.

[7] Z. Li, R. Yates and W. Trappe, "Secrecy Capacity ofIndependent Parallel Channels," in Proceedings of Allerton Conference on Communications, 2006, pp. 841-848.

[8] X. Zhou and M. R. McKay, "Secure Transmission with Artificial Noiseover Fading Channels: AchievableRate and Optimal Power Allocation," *IEEE Transactions on Vehicular Technology*, 2010, pp. 3831-3842. doi:10.1109/TVT.2010.2059057

[9] M. Bloch, J. Barros, M. R. S. Rodrigues and S. W. McLaughlin, "Wireless Information Theoretic Security," *IEEE Transactions on Information Theory*, Vol. 54, No. 6, 2008, pp. 2515-2534. doi:10.1109/TIT.2008.921908

[10] D. W. K. Ng and R. Schober, Cross-layer Scheduling for Ofdma Amplify and Forward Relay Networks," *IEEE Transactions on Vehicular Technology*, Vol. 59, No. 3, 2010, pp. 1443-1458. doi:10.1109/TVT.2009.2039814

[11] W. Yu and R. Liu, "Dual Methods for Non-convex Spectrum Optimization of Multicarrier Systems," *IEEE Transactions on Communications*, Vol. 54, No. 7, 2006, pp. 1310- 1322. doi:10.1109/TCOMM.2006.877962

[12] S. Boyd and L. Vandenberghe, Convex Optimization, Cambridge University Press, 2004. doi:10.1017/CBO9780511804441

[13] D. P. Palomar and M. Chiang, "Chiang Tutorial on Decomposition Methods for Network Utility Maximization," *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 8, 2006, pp. 1439-1451. doi:10.1109/JSAC.2006.879350

[14] 3GPP TR25.996 V9.0.0, Spatial Channel Model for Multiple Input Multiple Output Simulations [S]. 3GPP, 2009:

[15] H. Gao, P. J. Smith and M. V. Clark, "Theoretical Reliability of MMSE Linear Diversity Combining in Rayleigh Fading Additive Interference Channels," *IEEE Transaction Communications*, 1998, Vol. 46, pp. 666-672.

