A Power Allocation Algorithm for Enhancing the Security of OFDM System

Hui Zhu, Kaizhi Huang, Wenyue Luo, and Ying Hong

Abstract—**In order to protect OFDM wireless communication systems, information encryption protocol on high-layer is always used. However, it has very limited space to improve its safety performance. For this problem, we present a carrier power allocation algorithm to improve the secrecy rate. Firstly, the difference of each OFDM carrier channel fading coefficient is considered. Secondly, K-T condition is used to optimize the carrier power allocation to maximize secrecy rate with the limited total power, thereby enhancing the transmission security performance of OFDM system. Simulation results show that compared to the average allocation the secrecy rate of optimal allocation can be enhanced to 6.109bit/s/Hz at most with 128 carriers.**

Index Terms—**Physical layer security, OFDM system, Power allocation, secrecy rate.**

I. Introduction

Recently, OFDM (orthogonal frequency division multiplexing) technology has been widely used in various wireless communication systems for its superior characteristics of high spectrum efficiency and strong anti-multi-path fading [1]. Traditionally, the key encryption mechanism is used to encrypt the information to improve the security of the OFDM system. However, with the upgrading of the terminal handling capacity, key distribution and management of encryption mechanism has become more and more difficult to achieve.

There are a small amount of literatures on the OFDM physical layer security. A differential encoding scheme is proposed in [2] to enable the information transmission of OFDM system with a low probability of intercept. In [3], [4], the confidential capacity of the OFDM system using different receivers in the eavesdropper is analysed, but did not put forward feasible program to improve the security transfer rate of OFDM system.

It assumed that the average SNR of the receiver and eavesdropper, which does not match with the actual situation. Recent studies show that the safety of the system transmission can be improved through the resource allocation of fading channel [5]. In [6], the content of adjusting transmit power is analysed to achieve higher security transfer rate under flat fading channel. The similar conclusions in the non-ergodic fading channel are obtained in [7], [8], which provides a good idea to improve the security transfer rate of OFDM system through the rational allocation of carrier power under frequency selective fading channel.

Based on this, we use fading differences of OFDM carrier channel and propose a carrier power optimization allocation algorithm which can improve the security transfer rate of OFDM system. Firstly, in the case of the known information of channel state, we deduce the security transmission rate of the system with different average SNR of eavesdroppers to receiver by using broadcast eavesdropping OFDM channel model [9]. Secondly, to maximize the safe transfer rate, the power of each carrier according to KT condition with optimizing theory is allocated when the total transmit power is limited. Then, we use the optimized power allocation algorithm to enhance the security transmission performance of OFDM system. Also, the paper gives a detailed analysis of the influence of the number of carriers on the security transmission rate of the system as well as the influence of different average SNR on power distribution. Simulation results show that when the system uses 128 carriers, the security transfer rate of system with optimization distribution can be raised to 6.109bit/s/Hz compared with the average distribution. With the increasing number of carriers, the secure transmission rate is also increased.

II. OFDM Wiretap Channel Model

An OFDM wiretap channel model is shown in Fig. 1. The transmitter uses N-point IFFT to perform OFDM modulation on the input data. Authorized receiver and eavesdropper both use the N-point FFT to perform OFDM demodulation on the received data. Without considering inter-symbol interference and inter-carrier interference in the system, it can be considered that the system has N mutually independent carrier channel. We assume that the input signal is $X=[x_1,\cdots x_N]$, which are independent and identically distributed. The input signal of the *n*-th carrier is Gaussian variables with zero mean and variance of p_n. The channel between transmitter and legitimate user is defined as the main channel, its feature vector is $H_b=[h_{b1},...,h_{bN}]$ .The channel between the transmitter and eavesdropper is defined as the eavesdropping channel, its feature vector is $H_e=[h_{e1},...,h_{eN}]$, where h_{bn}, h_{en} are the frequency domain characteristics of the main channel and the eavesdropping channel of the n-th carrier respectively. $N_b=[n_{b1},\cdots,n_{bN}]$ and $N_e=[n_{e1},\cdots,n_{eN}]$ are respectively the additive noise of main channel and the eavesdropping channel. n_{bn} n_{en} are additive white Gaussian noise of the n-th carrier with zero mean and variance of σ_{bn}^2 and σ_{en}^2. The received signals of Receiver and eavesdropper are respectively $Y_b=[y_{b1},\cdots,y_{bN}]$, $Y_e=[y_{e1},\cdots,y_{eN}]$,

Manuscript received May 29, 2013; revised August 10, 2013.

Hui Zhu is with the Beijing University of Post&Telecommunication, Beijing, China (e-mail: huangkaizhi@tsinghua.org.cn).

DOI: 10.7763/IJEEEE.2014.V4.306

where y_{bn} y_{en} are the reception signal of the n-th carrier to the legitimate receiver and eavesdropper respectively.

$$y_{bn} = h_{bn} x_n + n_{bn} \tag{1}$$

$$y_{en} = h_{en} x_n + n_{en} \tag{2}$$

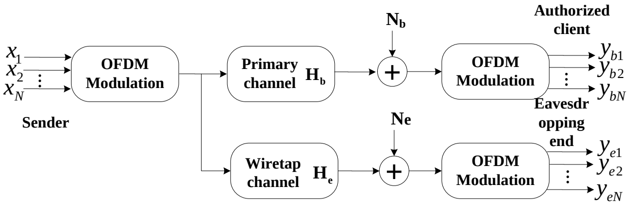


Fig. 1. OFDM wiretap channel model.

Each sub-carrier and input signals of the carrier are mutually independent. The security transmission rate of OFDM system [9] can be expressed as

$$C_s = \sum_{n=1}^{N} \left[I\left(x_n; y_{bn}\right) - I\left(x_n; y_{en}\right) \right]^+ \tag{3}$$

$I\left(x_n; y_{bn}\right)$ is the mutual information of sending and authorized to receive signals of the n-th carrier. $I\left(x_n; y_{en}\right)$ is the mutual information of sending signal and received signal of eavesdropper of the n-th carrier. Where $\left[x\right]^+ = \max\left\{0, x\right\}$. Thus, we can deduce from Maximum mutual information condition from information theory

$$I\left(x_n; y_{bn}\right) = h(y_{bn}) - h\left(y_{bn} \mid x_n\right) = \frac{1}{2}\log\left(1 + \frac{\alpha_n p_n}{\sigma_{bn}^2}\right) \tag{4}$$

Similarly,

$$I\left(x_n; y_{en}\right) = \frac{1}{2}\log\left(1 + \frac{\beta_n p_n}{\sigma_{en}^2}\right) \tag{5}$$

$\alpha_n = \left|h_{bn}\right|^2$ and $\beta_n = \left|h_{en}\right|^2$ represent the channel gain coefficient of the n-th carrier. $p_n = E[x_n^2]$ is the transmit power on the n-th carrier. In the actual situation, the noise variances of the receiver and eavesdropper are the same. So, $\sigma_b^2 = \sigma_{b1}^2 = \cdots = \sigma_{bn}^2, \sigma_e^2 = \sigma_{e1}^2 = \cdots = \sigma_{en}^2$. Then the secure transmission rate of the OFDM system can be expressed as

$$C_s = \sum_{n=1}^{N} \left[\log\left(1 + \frac{\alpha_n p_n}{\sigma_b^2}\right) - \log\left(1 + \frac{\beta_n p_n}{\sigma_e^2}\right) \right]^+ \tag{6}$$

III. The Power Allocation Algorithm to Maximize the Security Transmission Rate

Considering the total power is limited in the actual transmission, $\sum_{n=1}^{N} p_n \le P$, where P is a given total power. The allocated power of each carrier should be non-negative. Therefore, (6) is the objective function. The optimum allocation method of the carrier power to achieve maximum system security transfer rate is proposed. The maximization of security transfer rate can be described as the problems of constrained nonlinear programming

$$\max_{\mathbf{p}} C_s\left(\mathrm{p}\right) \text{ s.t. } \sum_{\mathrm{n}=1}^{N} p_n \le P, \quad p_n \ge 0, \quad n = 1, \cdots N, \tag{7}$$

$p = \left[p_1, \cdots p_N\right]$. According to the K-T theorem [10], construct Lagrange function:

$$L(p, \lambda, \mu) = C_s\left(p\right) + \sum_{n=1}^{N} p_n \lambda_n + \mu(P - \sum_{n=1}^{N} p_n), n = 1, \cdots N, \tag{8}$$

Therefore, firstly, we solve the K-T point in formula (8). Then selecting the maximum point from KT points, which is the optimal power allocation. The K-T condition can be written as

$$\frac{\partial L(p_n, \lambda_n, \mu)}{\partial p_n} = \frac{\alpha_n}{\sigma_b^2 + \alpha_n p_n} - \frac{\beta_n}{\sigma_e^2 + \beta_n p_n} + \lambda_n - \mu = 0 \tag{9}$$

$$\mu(P - \sum_{n=1}^{N} p_n) = 0 \tag{10}$$

$$p_n \lambda_n = 0 \tag{11}$$

$$\lambda_n \ge 0, \mu \ge 0 \tag{12}$$

Define $\gamma_n = \sigma_e^2 \alpha_n - \sigma_b^2 \beta_n$ as the carrier power allocation factor. Then formula (9) can be converted into

$$\frac{\gamma_n}{\left(\sigma_b^2 + \alpha_n p_n\right)\left(\sigma_e^2 + \beta_n p_n\right)} = \mu - \lambda_n \tag{13}$$

Obviously, when $\gamma_n < 0$, there will be $\mu - \lambda_n < 0$. We can deduce from (11), (12), p_n must be zero. Therefore, we first determine whether the power allocation for each carrier factor is less than zero. If $\gamma_n \le 0$, the carrier would not be assigned. According to the conditions of K-T and

$$P - \sum_{n=1}^{N} p_n \ge 0 \text{, } p_n \ge 0 \tag{14}$$

As can be seen from the definition of γ_n, the power distribution factor is not only related with the gain coefficient when $\sigma_b^2 \ne \sigma_e^2$, but also with the background noise of each receiver.

For solving the KT point, we consider the following situations

1) If the first equal sign in formula (14) is not met. We can see from the formula (10) that $\mu = 0$, $\gamma_n > 0$, λ_n in formula (13) must to be less than zero, which is in contradiction with the formula(11). Therefore the first equal sign in formula (14) must be met.
2) If the second equal sign in formula (14) is set up. There exists $p_i = 0$, $i \in \left[1, 2, \cdots, N\right]$. Then as long as $P - \sum_{n \ne i}^{N} p_n = 0$, $n = 1, \cdots, N$, the K-T conditions have

already been met. Therefore, at this time there are infinite many K-T points. According to formula (8), λ_i, μ should meet $\frac{\alpha_i}{\sigma_b^2} - \frac{\beta_i}{\sigma_e^2} + \lambda_i - \mu = 0$.

3) If the second equal sign in formula (14) is not met. We can see from the formula (11) that at this time $\lambda_n = 0$. Since $\gamma_n > 0$, we can see from the formula (13) that $\mu > 0$.Put $\lambda_n = 0$ into formula (13), we can get

$$p_n = -\frac{1}{2}\frac{\left(\sigma_e^2\alpha_n + \sigma_b^2\beta_n\right)}{\alpha_n\beta_n} + \sqrt{\frac{\gamma_n^2}{4\alpha_n^2\beta_n^2} + \frac{\gamma_n}{\mu\alpha_n\beta_n}} \qquad (15)$$

If $p_i < 0$, this is in contradiction with the hypothesis before. It means there will be no K-T point in this condition. From (15), it can be seen $\gamma_n \le \mu\sigma_e^2\sigma_b^2$. In summary, we can determine the final power allocation algorithm, as shown in Fig. 2.

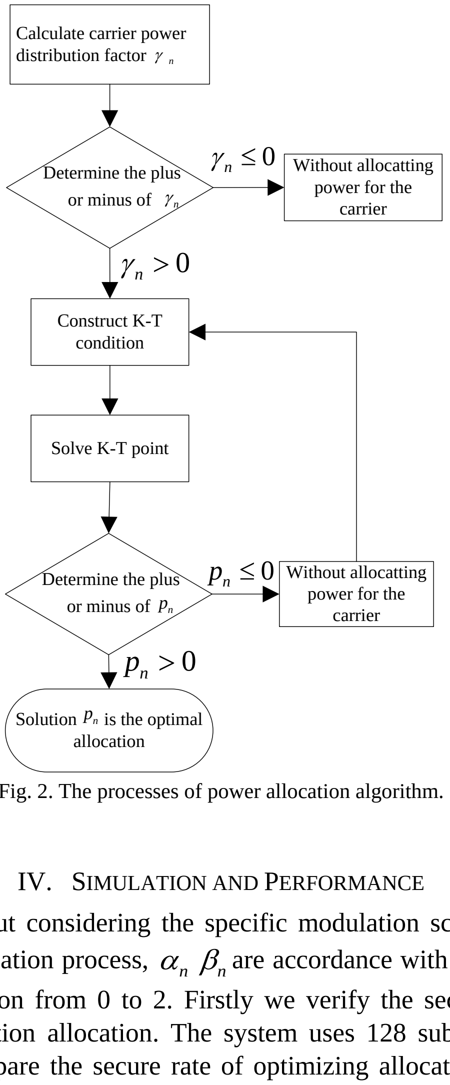

Calculate carrier power distribution factor γ_n
Determine the plus or minus of γ_n
$\gamma_n \le 0$
Without allocatting power for the carrier
$\gamma_n > 0$
Construct K-T condition
Solve K-T point
Determine the plus or minus of p_n
$p_n \le 0$
Without allocatting power for the carrier
$p_n > 0$
Solution p_n is the optimal allocation

Fig. 2. The processes of power allocation algorithm.

IV. Simulation and Performance

Without considering the specific modulation scheme in the simulation process, α_n β_n are accordance with uniform distribution from 0 to 2. Firstly we verify the security of optimization allocation. The system uses 128 subcarriers. We compare the secure rate of optimizing allocation with that of average allocation under different SNR. Then we take 16 subcarriers to analyse the influence of different SNR on power distribution. We verify the consistency of conclusion in literature [8] and the results analyzed in this paper. Finally, we choose different number of subcarriers under the same SNR and analysis the effect of the number of carriers on the rate of system security.

A. Comparison of System's Safety Performance Between Optimal Allocation And Average Allocation

Fig. 3 shows the difference between C_5 of optimal allocation and average allocation when the number of carriers N = 128. It can be seen from the figure that C_5 of optimal allocation is always not less than that of average allocation. The average SNR of receiver and eavesdropper is from- 5dB to 5dB. After improving the magnitude of the secure rate through the optimal allocation, the secure rate can be increased to a maximum 6.109bit/s/Hz compared to the average allocation. The rise of security transmission rate of optimization allocation is getting smaller and smaller when the average SNR of receiver and eavesdropper increasing. It is $\sigma_b^2 \to 0, \sigma_e^2 \to 0$, (6) shows that at this time C_5 will tend to $\sum_{n=1}^{N}\left[\log\left(\frac{\alpha_n}{\beta_n}\right)\right]^+$, the carrier improving space is getting smaller and smaller with the adjustment of carrier power. However, when average SNR reaches 25dB, secure transmission rate of optimizing allocation can still increase 0.4521bit/s/Hz. It means that as long as the average SNR of receiver is not very high, the optimal allocation can improve system security performance. We can also see from the figure that when the average SNR difference of receiver and eavesdropper is very big, C_5 of even distribution are almost not able to improve compared to that of optimal allocation. It is because at this point the system is in an extreme state, resulting in the decline of system security performance.

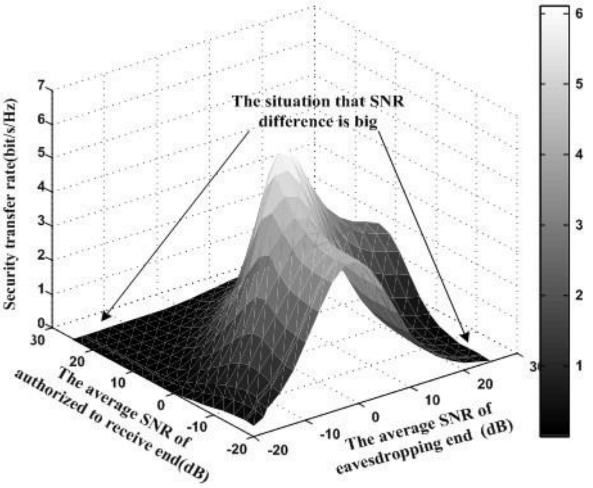


Fig. 3. The security transfer rate difference of optimal allocation and average allocation.

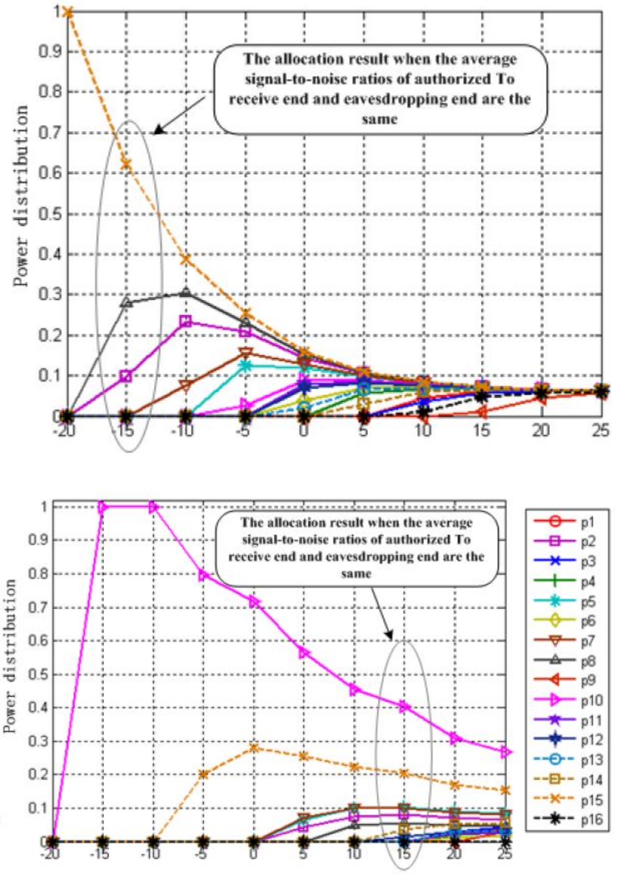
B. The Influence of Different SNR on Power Distribution

Define the carrier number N = 16 to randomly generate a set of carrier channel gain coefficient, such as shown in Table I.

TABLE I: THE GAIN COEFFICIENT OF RECEIVER AND EAVESDROPPER

	1	2	3	4	5	6	7	8
α	0.1520	1.3791	0.1207	0.3334	0.8641	0.4599	1.0052	1.7387
β	0.2908	0.0989	0.2056	0.5531	0.0535	1.0679	0.0580	0.2081
	9	10	11	12	13	14	15	16
α	0.0314	0.5998	0.6095	0.5499	0.3806	0.2168	1.9399	0.0859
β	0.1734	0.0003	0.6227	0.4403	0.3830	0.1346	0.0103	1.1502

Fig. 4 (a) shows that when average SNR of eavesdropper takes -15dB, the allocation results of carrier power change according to the average SNR change of receiver. When the average SNR of receiver is around -15dB, we can see from the figure and table1 that power distribution is mainly relevant with $\alpha_n - \beta_n$, which is consistent with the conclusions in literature [8]. With the increasing average SNR of the receiver, the power allocation of each carrier is approaching to the same value. The allocation result tends to average when it reaches about 20dB. The average SNR of receiver is far higher than that of eavesdropper, the average allocation is the optimal power allocation. This is due to we can consider $\sigma_b^2 \ll \alpha_n, \beta_n \ll \sigma_e^2$ this time, then approximation can be obtained from formula (15) $p_n \approx -\frac{\sigma_e^2}{2} + \sqrt{\frac{\sigma_e^4}{4} + \frac{\sigma_e^2}{\mu}} = c(\mu)$,it can be seen that the fading coefficient will not affect the power allocation of carrier , each carrier gets the same power allocation results $c(\mu)$. Since μ is determined by the number of carriers when the total power is constant, the size of power value of carrier allocation is also decided by the number of carriers. This confirms the simulation results of Fig. 3, when average SNRs of eavesdropper and receiver are respectively -15dB and 20dB. Optimal allocation has not improved significantly compared to the security transfer rate of average allocation.



(a) The SNR of receiver is -15db; (b) The SNR of eavesdropper is 15dB.
Fig. 4. The change of allocation results of carrier power according to the average SNR change of receiver.

Fig. 4 (b) shows that when average SNR of eavesdropper takes -15dB, the allocation results of carrier power change according to the average SNR change of receiver. When the average SNR of receiver is around 15dB, we can see from the figure and table1 that power distribution is mainly relevant with $\frac{\alpha_n}{\beta_n}$, which is consistent with the conclusions in literature [8]. With the decreasing of σ_e^2 or increasing of σ_b^2, there will be more and more allocation factors of carrier power which are less than zero, fewer number of carriers is capable of providing secure transmission. When the average SNR of eavesdropper is far higher than that of receiver, all power allocation factors of carriers is less than zero, no carrier can provide secure transmission. No matter how to allocate power at this time, the security transmission rate of the system will be zero. This shows that it is extremely unlikely to perform secure transmission when the SNR of receiver is very low. This confirms the simulation results of Fig. 3, when average SNRs of eavesdropper and receiver are respectively -15dB and 20dB, the security transmission rate of the system is almost zero, optimal allocation is impossible to increase the security of the system. We can see from Fig. 4(b) that it is possible to perform security transmission by optimal allocation when the average SNR of receiver is below that of eavesdropper, this explains that as long as the conditions of receiver are not very bad, optimal allocation can improve the security transmission performance of the system.

C. The Influence of the Number of Carriers on the Secure Transmission Rate

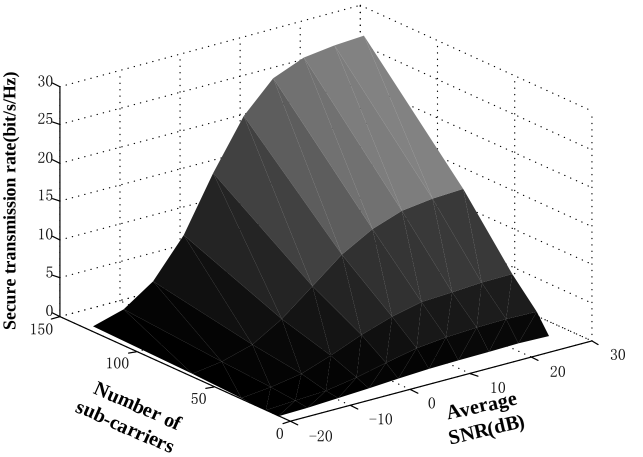


Fig. 5. The influence of the number of carriers on the secure transmission rate.

Fig. 5 describes the security transmission rate of the system with different number of carrier. In the condition that the average SNR of receiver and eavesdropper is 10dB, when the number of sub-carriers is *N*=8, the secure transmission rate is 1.006bit/s/Hz, when the number of sub-carriers is *N*=8, the secure transmission rate is 26.75bit/s/Hz, this indicates that we can improve the security of system by increasing the number of carriers. The reason can be derived from the formula (6), since when $\gamma_n \le 0$, $p_n = 0$, Then for any $n \in [1, N]$,there will be $\log\left(1+\frac{\alpha_n p_n}{\sigma_b^2}\right) - \log\left(1+\frac{\beta_n p_n}{\sigma_e^2}\right) \ge 0$, therefore, with the increasing of N, C_5 certainly show a rising trend. It can be seen from the figure that in the condition that the average SNR of receiver and eavesdropper is -15dB, when the number of sub-carriers is N=8, the secure transmission rate is 0.1159bit/s/Hz, when the number of sub-carriers is N=8, the secure transmission rate is 1.865bit/s/Hz, this explains that in low SNR condition, the increasing number of carrier wave can improve the security performance of system. This is due to the decrease of the SNR, $\sigma_b^2 = \sigma_e^2$, σ_e^2 gradually increases, it can be seen from formula (6) that C_5 is in a declining trend, which causes the loss of security of the system, however, when the SNR is not very low, the increase in the number of carriers can still improve the security of the system.

V. Conclusion

A carrier allocation algorithm is proposed for improving secure rate of OFDM. Firstly, channel fading of each carrier is different with constant total transmit power. Then, we use K-T conditions to optimize the carrier power allocation for maximizing secrecy rate, thereby enhancing the security performance of OFDM system. Simulation results show that the secrecy rate of optimal allocation can be enhanced to 6.109bit/s/Hz at most with 128 carriers. Although the number of carriers used by the system that can affect the security of the system, the rise of secure rate is also very limited with very low SNR.

References

[1] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal.*, vol. 54, no. 8, pp. 767-782, October 1975.

[2] 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, pp. 3372-3379, 2009.

[3] F. Renna, N. Laurenti, and H. V. Poor, “Physical layer secrecy for OFDM systems,” in *Proc. The IEEE European Wireless Conference*, Lucca, Italy, 2010, pp. 782-789.

[4] F. Renna, N. Laurenti, and H. V. Poor, “High SNR secrecy rates with OFDM signaling over fading channels,” in *Proc. The IEEE 21th International Symposium on Personal Indoor and Mobile Radio Communications.*, Istanbul, Turkey, 2010, pp. 2692-2697.

[5] E. Jorswieck and A. Wolf, “Resource allocation for the wire-tap multi-carrier broadcast channel,” in *Proc. International Workshop on Multiple Access Communications*, Petersburg, Russia.

[6] 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, pp. 2515-2534, 2008.

[7] P. K. Gopala, L. Cai, and H. E. Gamal, “On the secrecy capacity of fading channels,” in *Proc. The IEEE International Symposium on Information*, Nice, France, 2007.

[8] Y. Liang and H. V. Poor, “Secure communication over fading channels,” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470-2492, 2008.

[9] I. Csiszar and J. Koner, “Broadcast channels with confidential messages,” *IEEE Transactions on Information Theory*, vol. 24, pp. 339-348, 1978.

[10] N. Kawasaki, “Parametric study of thermal and chemical nonequilibrium nozzle flow,” M.S. thesis, Dept. Electron. Eng., Osaka Univ., Osaka, Japan, 1993.

Hui Zhu was born in 1971. During 1990-1994, he studied at the Dept. of Electronic Engineering, Tianjin University, Tianjin, China, and received bachelor degree. During 1994-1997, he studied at Dept of Information & Electronic Engineering, Zhejiang University, Zhejiang, China, as post graduate student. Since 2005, he has got his Doctor’s degree at School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China. His major field of study is Mobile communications, information security. From 1997, he is working in China Academy of Telecommunications Technology, Beijing, China.