Optimal Power Allocation for OFDM-Based Wire-Tap Channels with Arbitrarily Distributed Inputs

Haohao Qin*, Yin Sun*, Xiang Chen, Ming Zhao, and Jing Wang

State Key Laboratory on Microwave and Digital Communications
Tsinghua National Laboratory for Information Science and Technology
Department of Electronic Engineering, Tsinghua University,
Beijing 100084, P.R. China
{haohaoqin07,sunyin02,chenxiang98,zhao.ming29}@gmail.com
wangj@mail.tsinghua.edu.cn

Abstract. In this paper, optimal power allocation is investigated for maximizing the secrecy rate of orthogonal frequency division multiplexing (OFDM) systems under arbitrarily distributed input signals. Considering the discrete inputs are used in practical systems rather than the commonly assumed Gaussian inputs, we focus on secrecy rate maximization under more practical finite discrete constellations in this paper. It is known that the secrecy rate achieved by Guassian distributed inputs is concave with respect to the transmission power. However, we prove that the secrecy rate of finite discrete constellations is non-concave, which makes traditional convex optimization methods not applicable to our problem. To address this non-concave power allocation problem, we propose an efficient power allocation algorithm. Its gap from optimality vanishes asymptotically at the rate $O(1/\sqrt{N})$, and its complexity grows in order of $O(N)$, where N is the number of sub-carriers. Numerical results are provided to illustrate the benefits and significance of the proposed algorithm.

Keywords: OFDM wire-tap channel, arbitrarily distributed inputs, duality theory, nonconvex problem, optimal power allocation.

1 Introduction

In recent years, many privacy sensitive wireless services have become more and more popular, such as pushmail, mobile wallet, Microblogging, etc. While it is convenient to access to these services through mobile phone, this also leads to more concerns of secrecy due to the easy wiretap of the subscribers' transmission signals in broadcast wireless channel. The security of wireless communications is previously guaranteed by cryptographic techniques on application layer, which recently face several challenges, such as the emergence of new cracking algorithms

* Contribute equally to this work.

P. Ren et al. (Eds.): WICON 2011, LNICST 98, pp. 192–203, 2012.

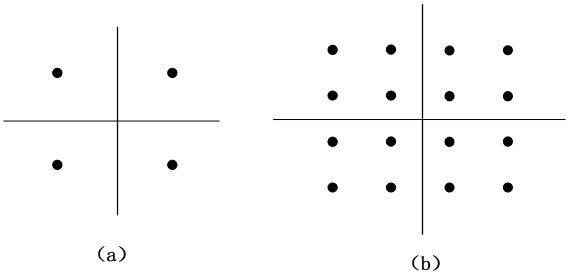

Fig. 1. (a). QPSK inputs. (b). 16QAM inputs.

and the increasing computational capability of eavesdroppers. Recently, physical layer security [1] has received considerable attentions in wireless communication communities as a complement to traditional cryptographic encryption to provide additional security mechanism.

Physical layer security was firstly studied from an information-theoretic perspective in [2], where secrecy rate was defined as the achievable data rate from a transmitter to its legitimate destination while keeping the eavesdropper completely ignorant of the secret massage. Later, the research in this field was extended to various scenes, such as Gaussian wire-tap channel [3]-[4], multiple input multiple output (MIMO) channel [5]-[7], orthogonal frequency division multiplexing (OFDM) channel [8]-[11], etc.

Recently, OFDM-based secure communications obtain much attention for its capability of countermining the dispersive of wideband wireless channels and enhance secrecy rate [8]-[9]. Optimal power allocation of secure OFDM system is investigated in [8] where the distribution of input signals is assumed to be Gaussian. However, Gaussian distributed input signals are unrealistic in practise for its infinite peak-to-average ratio. Discrete distributions, such as PSK, QAM (see Fig.1), are used in practical systems.

In this paper, we investigate optimal power allocation for OFDM-based wire-tap channels with arbitrarily distributed channel inputs. While the secrecy rate achieved by Guassian distributed inputs is concave with respect to the transmission power, we show that the secrecy rate for finite discrete constellations is non-concave. Therefore, the optimal power allocation strategy for secure communications with Gaussian distributed inputs [8]-[10] is not optimal any more to the considered problem. Following the lead of [12]-[14], we propose a low complexity power allocation algorithm which achieves asymptotic optimal performance as the number of sub-carriers increases, and its complexity grows in order of sub-carrier number. Numerical results are provided to illustrate the efficiency of the proposed algorithm.

The remainder of this paper is organized as follows: section 2 provides the system model and problem formulation. Optimal power allocation for arbitrarily distributed channel inputs is presented in Section 3. Numerical results and conclusions are given in Section 4 and Section 5.

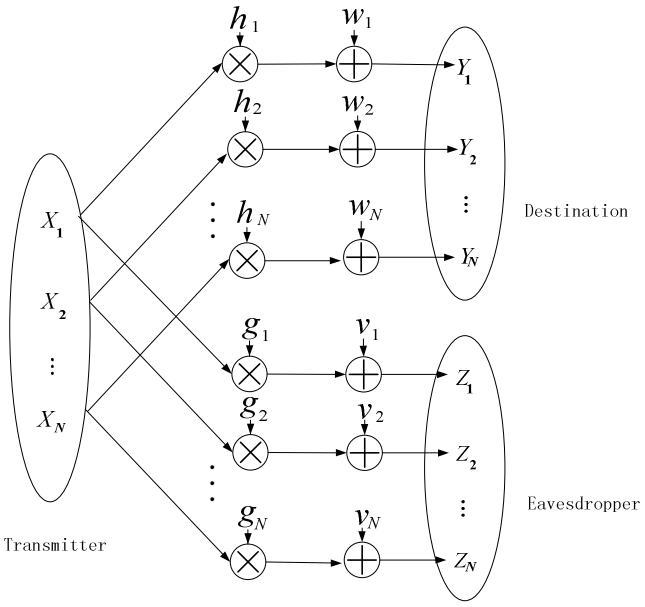

Fig. 2. System model

2 System Model and Problem Formulation

We consider wideband secure communications from a transmitter to its legitimate receiver, in the presence of an eavesdropper who intends to extract the transmitter's secret message. We assume that each node employs an OFDM air interface with N sub-carriers. The transmitter's signal in each sub-carrier follows an arbitrary but predetermined distribution, which can be either continuous constellations[1], such as Gaussian distribution, or finite discrete constellations, including PSK, QAM, etc.

The complex channel coefficients of the legitimate and eavesdropping channels for ith sub-carrier are denoted by h_i and g_i, respectively, as illustrated in Fig. 2. The transmitted signal over the ith sub-carrier is denoted as x_i, which is given by

$$x_i = \sqrt{p_i} s_i, i = 1, \ldots, N, \tag{1}$$

where p_i is the ratio between transmitting power of x_i and the noise power, and s_i represents the normalized channel input with predetermined distribution and unit variance. The power constraint of the transmitter is given by

$$\frac{1}{N} \sum_{i=1}^{N} p_i \leq P. \tag{2}$$

[1] The words "distribution" and "constellation" are used alternatively throughout the paper.

The received signals of the legitimate receiver and eavesdropper are given by

$$y_i = h_i\sqrt{p_i}s_i + w_i, i = 1, \cdots, N, \tag{3}$$
$$z_i = g_i\sqrt{p_i}s_i + v_i, i = 1, \cdots, N, \tag{4}$$

where the w_i and v_i are zero-mean complex Gasussian noises with unit-variance for ith sub-carrier. According to the information theoretical studies of [8], the secrecy rate from transmitter to its legitimate receiver is determined by

$$\sum_{i=1}^{N}[I(s_i; h_i\sqrt{p_i}s_i + w_i) - I(s_i; g_i\sqrt{p_i}s_i + v_i)]^+, \tag{5}$$

where $[x]^+ \triangleq \max\{x, 0\}$, and $I(x; y)$ denotes the mutual information between random variables x and y. The expression in (5) is quite illuminating: the secrecy rate of each sub-channel is non-negetive; if it is positive, it is exactly the difference of the data rates of the legitimate and eavesdropping channels. The total secrecy rate is simply the sum secrecy rate of all the N sub-carriers.

For fixed constellations of $\{s_i\}_{i=1}^N$, we need to optimize the power allocation to obtain the maximal secrecy rate, which is described as the following optimization problem:

$$\begin{aligned} R^* = \max_{\mathbf{p}} \quad & R_s(\mathbf{p}) \triangleq \tfrac{1}{N}\sum_{i=1}^{N}[I(s_i; h_i\sqrt{p_i}s_i + w_i) - I(s_i; g_i\sqrt{p_i}s_i + v_i)]^+ \\ \text{s.t.} \quad & \tfrac{1}{N}\textstyle\sum_{i=1}^{N} p_i \le P, \\ & \mathbf{p} \ge 0 \end{aligned} \tag{6}$$

where $\mathbf{p} \in \mathcal{R}^N$ is the vector of transmission power of the N subcarriers, i.e., $\mathbf{p} = \{p_1, p_2, ..., p_N\}$; R^* denotes the optimal value.

3 Optimal Power Allocation for Arbitrarily Distributed Channel Inputs

3.1 Non-concavity of the Secrecy Rate $R_s(\mathbf{p})$

If s_i follows Gaussian distribution, the secrecy rate $R_s(\mathbf{p})$ in (6) has explicit expression [4], i.e.,

$$R_s^G(\mathbf{p}) = \frac{1}{N}\sum_{i=1}^{N}[\ \log_2(1 + |h_i|^2 p_i) - \log_2(1 + |g_i|^2 p_i)\ ]^+. \tag{7}$$

It is worth while to mention that $R_s^G(\mathbf{p})$ is a concave function of $\mathbf{p}$. Thus, problem (6) is a convex optimization problem. Let us define

$$R_{s,i}(p_i) \triangleq [I(s_i; h_i\sqrt{p_i}s_i + w_i) - I(s_i; g_i\sqrt{p_i}s_i + v_i)]^+ \tag{8}$$

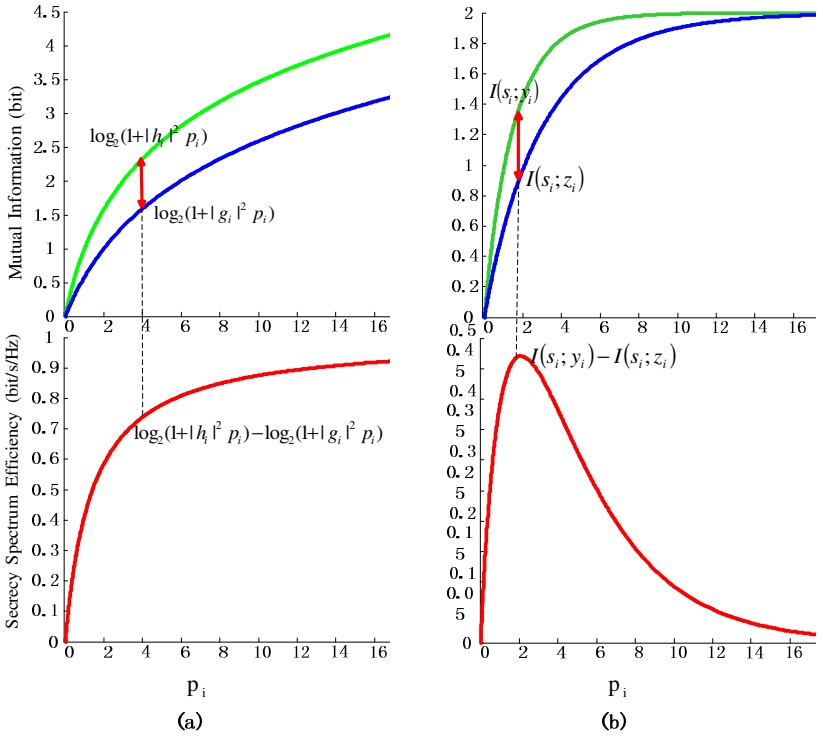

Fig. 3. (a). Secrecy rate achieved by Gaussian distributed inputs. (b). Secrecy rate achieved by discrete inputs (eg. QPSK). And p_i is the ratio of the signal power and noise power.

for the facility of latter expression. The secrecy rate for Gaussian distributed inputs is illustrated in the left part of Fig. 3. One can observe that the mutual information $\log_2(1 + |h_i|^2 p_i)$, $\log_2(1 + |g_i|^2 p_i)$ and the secrecy rate $\log_2(1 + |h_i|^2 p_i) - \log_2(1 + |g_i|^2 p_i)$ are all concave, provided that $|h_i|^2 > |g_i|^2$. In [8], [9] and [10], the authors utilized the concavity of $R_s^G(\mathbf{p})$ to obtain the optimal power allocation, i.e.,

$$p_i^* = \begin{cases} \frac{-(|h_i|^2+|g_i|^2)+\sqrt{(|h_i|^2+|g_i|^2)^2-4|h_i|^2|g_i|^2\frac{u+|g_i|^2-|h_i|^2}{u}}}{2|h_i|^2|g_i|^2} & , \text{if } \ |h_i|^2 - |g_i|^2 > u \\ 0 & , \text{others}, \end{cases} \tag{9}$$

where the Lagrange multiplier $u > 0$ is chosen to meet the power constraint:

$$\frac{1}{N}\sum_{i=1}^{N} p_i = P. \tag{10}$$

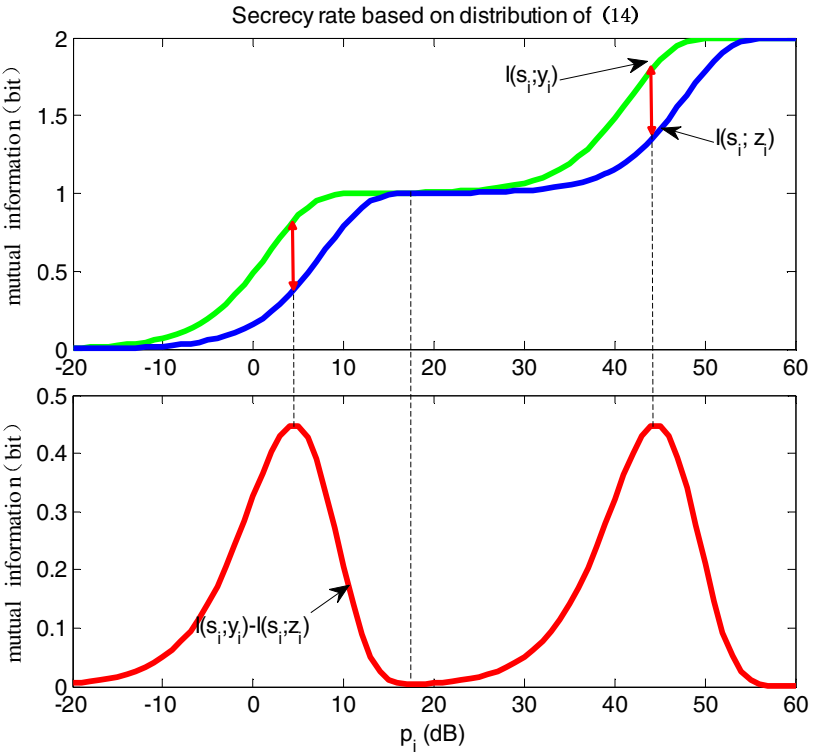

Fig. 4. Secrecy rate achieved by distribution of (14)

One may expect the concavity of $R_s(\mathbf{p})$ still holds for general input distributions. Unfortunately, our investigation shows that this is not true, which is formally described in the following proposition:

Proposition 1. *The secrecy rate function $R_s(\boldsymbol{p})$ for any discrete constellation with finite points is non-concave with respect to $\boldsymbol{p}$.*

Proof. When $p_i = 0$, one can derive $I(s_i; y_i) = I(s_i; z_i) = 0$; when $p_i = +\infty$, we have $I(s_i; y_i) = I(s_i; z_i) = H(s_i)$, where $H(x)$ is entropy of x. Therefore, $R_{s,i}(0) = R_{s,i}(+\infty) = 0$.

According to [15],

$$\frac{\partial I(s; \sqrt{p}s + n)}{\partial p} = \texttt{MMSE}(p), \tag{11}$$

where $\texttt{MMSE}(p)$ is defined as:

$$\texttt{MMSE}(p) \triangleq \mathbb{E}[|s - \mathbb{E}(s|\sqrt{p}s + n)|^2], \tag{12}$$

where $\mathbb{E}[x]$ is the expectation of random variable x; $\mathbb{E}[x|y]$ is the conditional expectation of x for given y, the derivative of $R_{s,i}(p_i)$ at $p_i = 0$ is given by[2]

[2] Only the sub-carriers that satisfy $|h_i|^2 > |g_i|^2$ are considered, as $R_{s,i}(p_i) \equiv 0$ for those sub-carriers with $|h_i|^2 \leq |g_i|^2$ which do not affect the concavity of $R_s(\mathbf{p})$.

$$R'_{s,i}(p_i)|_{p_i=0} = \left[|h_i|^2 - |g_i|^2\right]^+ > 0, \tag{13}$$

which indicates that there must exist a $\hat{p_i} > 0$ that $R_{s,i}(\hat{p_i}) > 0$. According to the Lagrange's mean value theorem [17], it must have a point $\tilde{p_i} \in [\hat{p_i}, +\infty]$ with negative slop $R'_{s,i}(\tilde{p_i}) < 0$.

If $R_{s,i}(p_i)$ is concave, then the inequality $R_{s,i}(p_i) \leq R_{s,i}(\tilde{p_i}) + R'_{s,i}(\tilde{p_i})(p_i - \tilde{p_i})$ holds [18], which indicates $R_{s,i}(+\infty) = -\infty$. This is impossible since $R_{s,i}(+\infty) = 0$. Therefore, the concavity assumption is not true, and Proposition 1 holds.

Two evidentiary examples are provided to illustrate Proposition 1:

The first example is QPSK. The curves of $I(s_i; y_i)$, $I(s_i; z_i)$ and $R_{s,i}(p_i)$ versus p_i are shown in right part of Fig. 3, and they are in accordance with the statements in the proof of Proposition 1.

The second example considers a 4 points PAM constellation with non-uniform spacing. Its probability mass function is given by:

$$P_{s_i} \sim \begin{bmatrix} -51L & -50L & 50L & 51L \\ 0.25 & 0.25 & 0.25 & 0.25 \end{bmatrix} \tag{14}$$

where L is a normalization parameter to maintain unit variance. Figure 4 shows the secrecy rate $R_{s,i}(p_i)$ of this case. It is interesting that the $R_{s,i}(p_i)$ has two peaks. Hence, it is definitely non-concave. We note that the mutual information $I(s_i; y_i)$ and $I(s_i; z_i)$ are concave with respect to p_i in linear scale [16].

3.2 Optimal Power Allocation Solution of Problem (6)

Although problem (6) is non-convex, there are still some efficient algorithms to solve it and obtain near-optimal solutions. One of them is the Lagrangian duality method [18]. Some recent studies [12]-[14] showed that asymptotic optimal performance can be achieved by this method.

The Lagrangian of problem (6) is given by

$$L(\mathbf{p}, u) = \frac{1}{N}\sum_{i=1}^{N}[I(s_i; h_i\sqrt{p_i}s_i + w_i) - I(s_i; g_i\sqrt{p_i}s_i + v_i)]^+ + u\left(P - \frac{1}{N}\sum_{i=1}^{N} p_i\right), \tag{15}$$

where u is Lagrangian dual variable. The corresponding dual function can then be written as

$$g(u) \triangleq \max_{\mathbf{p}\geq 0} \; L(\mathbf{p}, u). \tag{16}$$

Hence the dual optimization problem is expressed as

$$D^* = \min_{u\geq 0} \qquad g(u), \tag{17}$$

where D^* denotes the optimal dual value. Since the objective function of primal problem (6) is non-concave, there is a positive gap between R^* and D^*, i.e., $D^* - R^* > 0$. However, according to the recent studies of Luo and Zhang [12], [13], asymptotic strong duality holds for problem (6), i.e. the duality gap $D^* - R^*$ goes to zero as $N \to \infty$, as is expressed in the following proposition:

Table 1.

Algorithm : Lagrangian dual optimization method
Initialize u
repeat
for i=1 to N
find $p_i = \arg\max_{p_i} \left[[I(s_i; y_i) - I(s_i; z_i)]^+ - up_i \right] + uP.$
end
update u using bisection method.
until u converges.

Proposition 2. *If the channel coefficients g_i and h_i are Lipschitz continuous and bounded in the sense*

$$|h_i - h_j| \leq L_h \frac{|i-j|}{N}, \forall\ i, j \in \{1, 2, ..., N\} \tag{18}$$

$$|g_i - g_j| \leq L_g \frac{|i-j|}{N}, \forall\ i, j \in \{1, 2, ..., N\} \tag{19}$$

where $L_h, L_g > 0$ is the Lipschitz constant. Then we have

$$0 \leq D^* - R^* \leq O\left(\frac{1}{\sqrt{N}}\right). \tag{20}$$

Proof. According to (11) and (12), we have [15]

$$0 \leq \frac{\partial I(s; \sqrt{p}s + n)}{\partial p} = \texttt{MMSE}(p) \leq \mathbb{E}[|s|^2], \tag{21}$$

which implies that the derivative of $R_{s,i}(p_i)$ with respect to p_i is bounded. Then the derivative of $R_{s,i}(p_i)$ with respect to $|g_i|^2$ and $|h_i|^2$ are also bounded. Since g_i and h_i are Lipschitz continuous, according to chain rule, the secrecy rate $R_{s,i}(p_i)$ is also Lipschitz continuous. Hence according to Theorem 2 of [12], the duality gap between D^* and R^* is in the order of $1/\sqrt{N}$, which is expressed as

$$0 \leq D^* - R^* \leq O(\frac{1}{\sqrt{N}}), \tag{22}$$

and Proposition 2 holds.

The procedures to solve (16) and (17) are provided in the following.

For each fixed u, problem (16) can be decoupled into N independent subcarrier problems

$$\begin{aligned} g(u) &= \max_{p_i \geq 0}\ L(p_i, u), \\ &= \textstyle\sum_{i=1}^{N} \max_{p_i \geq 0} [[I(s_i; y_i) - I(s_i; z_i)]^+ - up_i] + uP. \end{aligned} \tag{23}$$

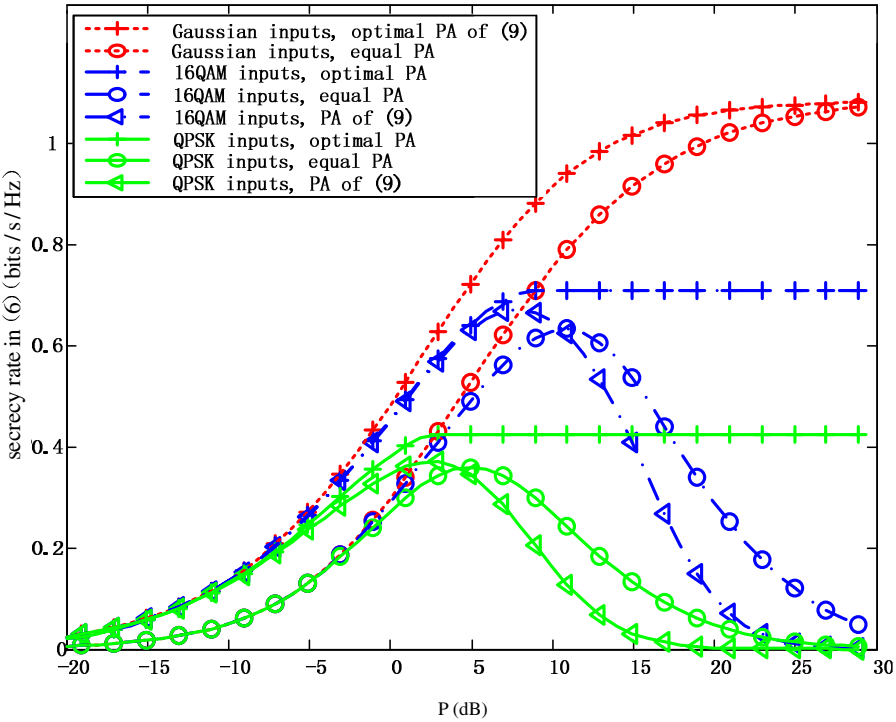

Fig. 5. The secrecy rate versus total power P

While the sub-carrier problem in (23) is still non-convex, it has only one variable p_i and can be solved by simple one dimension line search. As the dual function $g(u)$ is convex in u and its subgradient $g'(u) = P - \frac{1}{N}\sum_{i=1}^{N} p_i^*$, where p_i^* is optimal solution for problem (16) with fixed u, is an increasing function in u, bisection method can be used to solve dual problem (17), so that either $u = 0$, $P \geq \frac{1}{N}\sum_{i=1}^{N} p_i^*$ or $u > 0$, $P = \frac{1}{N}\sum_{i=1}^{N} p_i^*$ is satisfied. Table.1 summarizes the algorithm.

The complexity of this algorithm is $N\frac{1}{e_p}\log_2(\frac{1}{e_d})$, where e_p is the accuracy of one dimension exhausitive search to solve (16) and e_d is the accuracy of the bisection search to solve (17). Since its complexity is linear with respect to the number of sub-carriers N, it is quite convenient for practical large values of N, such as 64∼4096. We note that the complexity of solve (6) directly is $\frac{1}{e_p^N}$, which is exponential in N and thus unrealistic.

4 Numerical Results

In this section, we provide some simulation results to illustrate the performance of our proposed power allocation algorithm and show how different channel input distributions affect the secrecy rate and power allocation results.

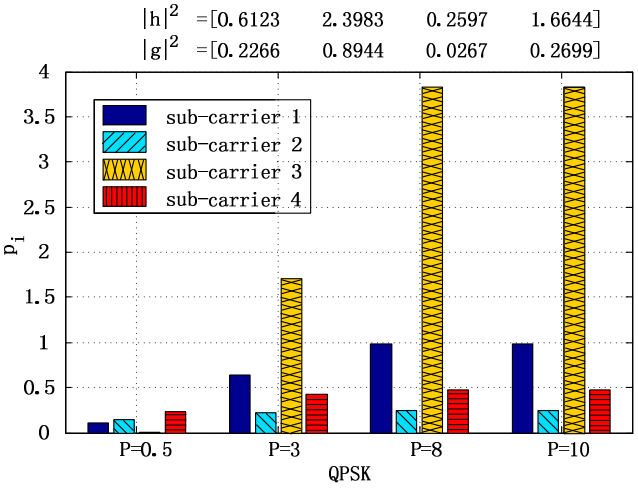

Fig. 6. Power allocation results versus P for QPSK inputs

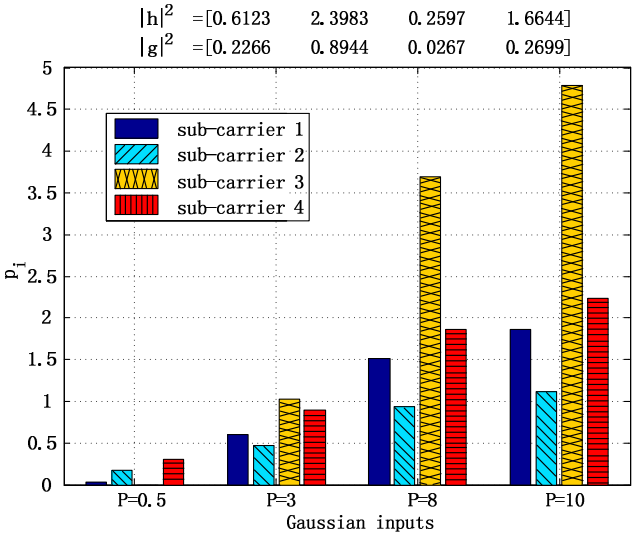

Fig. 7. Power allocation results versus P for Gaussian inputs

We first consider an OFDM-based secure system with $N = 128$ subcarriers. The secrecy rate versus total power constraint for different power allocation strategies and input distributions are illustrated in Fig. 5. Two reference strategies are considered to compare with our strategy: the optimal strategy for Gaussian inputs, i.e., (9), which is denoted by "PA of (9)" in Fig. 5; the equal power allocation strategy, which equally allocates total power among the subcarriers that satisfy $|h_i|^2 > |g_i|^2$ and is denoted by "equal PA".

Higher secrecy rate can be achieved for QPSK and 16QAM by our proposed optimal power allocation strategy, especially when the power constraint P is quite large. Equal power distribution works well for Gaussian distributed inputs. More specifically, it tends to be optimal for large value of P. Actually, when P is large, secrecy rate in (9) can be approximated by

$$\begin{aligned} R_s^G(\mathbf{p}) &= \tfrac{1}{N}\sum_{i=1}^{N}[\,\log_2(1+|h_i|^2p_i)-\log_2(1+|g_i|^2p_i)\,]^+ \\ &\approx \tfrac{1}{N}\sum_{i=1}^{N}[\,\log_2(\tfrac{|h_i|^2}{|g_i|^2})\,]^+, \end{aligned} \tag{24}$$

which is independent with power allocation p_i. However, equal power allocation can be quite bad for finite discrete constellations. The secrecy rate can drops to zero for large value of P.

The power allocation solution of the proposed algorithm is shown in Fig. 6 and Fig. 7, respectively, for QPSK and Gaussian inputs with $N = 4$. When the power constraint P is small, most transmission power is allocated to the stronger sub-channels, the channels with larger $|h_i|^2 - |g_i|^2$ (Channel 2 and Channel 4 in our simulation example). However, as P grows, the transmission power of the weak sub-channels grows quite fast. For QPSK input signals, the transmission power allocated to every sub-channels will stop increasing as P grows. But the transmission power for Guassian input signals still continues to increase.

5 Conclusion

In this paper, we have obtained the optimal power allocation for OFDM-based wire-tap channels with arbitrarily distributed inputs. While the secrecy rate achieved by Gaussian distributed channel inputs is concave with respect to the transmission power, we have found and rigorously proved that the secrecy rate is non-concave for any practical finite discrete signal constellations. A power allocation algorithm has been proposed, which is asymptotic optimal as the number of sub-carrier increases. Our numerical results show that more transmitting power may results in a huge loss in secrecy rate, which is rarely seen in previous power allocation studies. This indicates that optimal power allocation is quite essential in practical studies of physical layer security.

Acknowledgement. The authors would like to thank Dr. Tsung-Hui Chang and Prof. Shidong Zhou for valuable suggestions in this paper.

This work is supported by National S&T Major Project (2009ZX03002-002), National Basic Research Program of China (2007CB310608), National S&T Pillar Program (2008BAH30B09), National Natural Science Foundation of China (60832008) and PCSIRT, Tsinghua Research Funding-No.2010THZ02-3. This work is also sponsored by Datang Mobile Communications Equipment Co., Ltd.

References

1. Liang, Y., Poor, H.V., Shamai, S.: Information theoretic security. Found. Trends Commun. Inf. Theory 5, 355–580 (2008)
2. Wyner, A.: The wire-tap channel. Bell. Syst. Tech. J. 54(8), 1355–1387 (1975)
3. Csiszar, I., Korner, J.: Broadcast channels with confidential messages. IEEE Trans. Inf. Theory 24(3), 339–348 (1978)
4. Cheong, S.L.Y., Hellman, M.: The Gaussian wire-tap channel. IEEE Trans. Inf. Theory 24(4), 451–456 (1978)
5. Oggier, F., Hassibi, B.: The secrecy capacity of the MIMO wiretap channel. In: Proc. 45th Annu. Allerton Conf. Communication, Control and Computing, Monticello, IL, pp. 848–855 (September 2007)
6. Liu, T., Shammai, S.: A note on the secrecy capacity of the multi-antenna wiretap channel. IEEE Trans. Inf. Theory 55(6), 2547–2553 (2009)
7. Ekrem, E., Ulukus, S.: Gaussian MIMO multi-receiver wiretap channel. In: Global Telecommunications Conference, Honolulu, HI (November 2009)
8. Li, Z., Yates, R., Trappe, W.: Securecy capacity of independent parrallel channels. In: Proc. IEEE int. Symp. Information Theory(ISIT), Seattle, WA, pp. 356–360 (July 2006)
9. Liang, Y., Poor, H.V., Shamai, S.: Secure communication over fading channels. IEEE Trans. Inf. Theory 54(6), 2470–2492 (2008)
10. Jorswieck, E., Wolf, A.: Resource allocation for the wire-tap multi-carrier broadcast channel. In: Proc. International Workshop on Multiple Access Communications (MACOM), St. Petersburg, Russia (June 2008)
11. Renna, F., Laurenti, N., Poor, H.V.: Physical layer security for OFDM systems. In: European Wireless Conference, Vienna, Austria (April 2011)
12. Luo, Z., Zhang, S.: Duality Gap Estimation and Polynomial Time Approximation for Optimal Spectrum Management. IEEE Trans. Signal Processing 57(7), 2675–2689 (2009)
13. Luo, Z., Zhang, S.: Dynamic spectrum management: Complexity and duality. IEEE J. Sel.Topics Signal Process., Special Issue on Signal Process., Netw. Dyn. Spectrum Access 2(1), 57–73 (2008)
14. Yu, W., Lui, R.: Dual methods for nonconvex spectrum optimization of multicarrier systems. IEEE Trans. Commun. 54, 1310–1322 (2006)
15. Guo, D., Shamai, S., Verdu, S.: Mutual information and minimum mean-square error in Gaussian channels. IEEE Trans. Inf. Theory 51(4), 1261–1283 (2005)
16. Guo, D., Wu, Y., Shamai, S., Verdu, S.: Estimation in Gaussian noise: Properties of the minimum mean-square error. IEEE Trans. Inf. Theory 57(4), 2371–2385 (2011)
17. Jeffreys, H., Jeffreys, B.S.: Methods of Mathematical Physics, 3rd edn. Cambridge University Press, Cambridge (1988)
18. Boyd, L., Vandenberghe, S.: Convex Optimization. Cambridge University Press (2004)