一种提高 OFDM 系统安全传输的载波功率分配算法*

陈玉磊，季新生，黄开枝，吉　江
（国家数字交换系统工程技术研究中心，郑州 450000）

摘　要：现有的 OFDM 安全传输技术无法满足无线通信系统对安全性能的需求，针对这一问题，提出了一种旨在提高 OFDM 系统安全传输速率的载波功率分配算法。考虑 OFDM 各载波信道存在的衰落差异性，基于 OFDM 窃听信道模型推导出窃听端与授权接收端平均信噪比不同的系统安全传输速率；在总功率受限的条件下，以安全传输速率最大化为目标，利用 K-T 条件对各载波功率进行优化分配，从而提高 OFDM 系统安全传输性能。仿真结果表明，当选用 128 个载波时，优化分配的安全传输速率比平均分配的安全传输速率最多可以提升 6.109 bit/s/Hz，并且随着载波数的不断增加，安全传输速率的提升也越来越明显。

关键词：物理层安全；正交频分复用系统；功率分配；安全传输速率
中图分类号：TN929.53　　**文献标志码**：A　　**文章编号**：1001-3695(2012)06-2236-04
doi:10.3969/j.issn.1001-3695.2012.06.062

Carriers power allocation algorithm to enhance security of OFDM system transmission

CHEN Yu-lei, JI Xin-sheng, HUANG Kai-zhi, JI Jiang
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450000, *China*)

Abstract: In order to protect OFDM wireless communication systems to transmit information safety major use encryption protocol on high-level, however it has very limited space to improve its safety performance. For this problem, this paper presented a carriers power allocation algorithm to improve the secrecy rate. First, considering each OFDM carrier channel fading coefficient exist differences, based on OFDM wire-tap model it derived the secrecy rate under the authorized receiver and eavesdropper had different average SNR; Then, it used K-T conditions to optimize the carriers power allocation for the target to maximize secrecy rate under the total power limited, 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 6.109 bit/s/Hz at most when the system uses 128 carriers. And with the increasing number of carrier the secrecy rate upgrade more obvious.

Key words: physical layer security; OFDM system; power allocation; secrecy rate

正交频分复用(OFDM)技术由于其频谱利用率高、抗多径衰落强等优越特性，被广泛应用于各种无线通信系统。为提高 OFDM 系统的安全性，传统的方法是利用密钥加密机制对信息进行加密。但是随着终端处理能力的提升，传统密钥加密机制对密钥的分发和管理变得更加困难，实现难度越来越大。因此，通过在物理层为 OFDM 系统提供安全保障具有十分重要的意义。

目前，有少量文献对 OFDM 系统的物理层安全进行了研究。文献[1]提出了一种差分编码方案使 OFDM 系统的信息传输具有低截获概率；文献[2,3]分析了窃听端采用不同接收机时的 OFDM 系统保密容量，但都没有提出可行的提高 OFDM 系统安全传输速率的方案。文献[4]讨论了功率分配对 OFDM 安全传输速率的影响，但并没有提出具体的提升系统安全传输速率的算法，而且文中假设窃听端平均信噪比与授权接收端平均信噪比相同，这与实际情况不符。近些年的研究表明，通过衰落信道的资源分配可以提高系统的安全传输性能。文献[5]分析了在平坦衰落信道下，根据不同时刻的衰落程度调整发射功率可以使系统获得更高的安全传输速率。文献[6,7]在非各态历经衰落信道下也得到了相似的结论，这为在频率选择性衰落信道下，通过合理的分配载波功率提高 OFDM 系统安全传输速率提供了很好的思路。

基于此，本文利用 OFDM 各载波信道的衰落差异，提出一种可以提高 OFDM 系统安全传输速率的载波功率优化分配算法。

1　OFDM 窃听信道模型

图 1 为 OFDM 窃听信道模型，发送端采用 N 点的 IFFT 对输入数据进行 OFDM 调制，授权接收端与窃听端都通过 N 点的 FFT 对接收数据进行 OFDM 解调，不考虑系统的符号间干扰和载波间干扰，可认为系统有 N 个相互独立的载波信道。设输入信号为 $X=[x_1,\cdots,x_N]$，其各载波输入信号独立同分布，第 n 个载波的输入信号 x_n 为均值为零、方差为 p_n 的高斯

收稿日期：2011-10-31；**修回日期**：2011-12-02　　**基金项目**：国家自然科学基金资助项目(61171108)

作者简介：陈玉磊(1987-)，男，吉林九台人，硕士研究生，主要研究方向为移动无线通信(yuleiaiyanan@126.com)；季新生(1968-)，男，教授，主要研究方向为移动通信网络技术；黄开枝(1973-)，女，安徽来安人，副教授，主要研究方为第三代移动通信；吉江(1983-)，山西人，博士研究生，主要研究方向为移动通信.

变量。定义发送端与授权接收端之间的信道为主信道,其信道特征矢量为 $\boldsymbol{H}_b=[h_{b1},\cdots,h_{bN}]$,发送端与窃听端之间的信道为窃听信道,其信道特征矢量为 $\boldsymbol{H}_e=[h_{e1},\cdots,h_{eN}]$,其中 h_{bn}、h_{en} 分别为主信道与窃听信道第 n 个载波的频域特性。$N_b=[n_{b1},\cdots,n_{bN}]$ 和 $N_e=[n_{e1},\cdots,n_{eN}]$ 分别为主信道与窃听信道的加性噪声,其中 n_{bn}、n_{en} 是第 n 个载波上均值为零、方差为 σ_{bn}^2、σ_{en}^2 的加性高斯白噪声。授权接收端与窃听端接收的信号分别为 $\boldsymbol{Y}_b=[y_{b1},\cdots,y_{bN}]$,$\boldsymbol{Y}_e=[y_{e1},\cdots,y_{eN}]$,其中 y_{bn}、y_{en} 分别为授权接收端与窃听端第 n 个载波的接收信号:

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

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

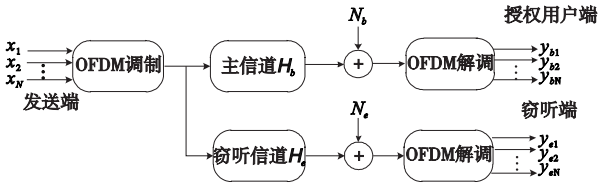


图1　OFDM窃听信道模型

各子载波信道与载波输入信号都相互独立,则 OFDM 系统的安全传输速率[8]可表示为

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

其中:$I(x_n;y_{bn})$ 为第 n 个载波上的发送信号与授权接收端接收信号的互信息,$I(x_n;y_{en})$ 为第 n 个载波上的发送信号与窃听端接收信号的互信息。符号 $[x]^+=\max\{0,x\}$。

由于授权接收端与窃听端的各载波噪声分量与 X 中各分量都服从高斯分布,则由信息论的最大互信息条件可以得到

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

同理得到

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

其中:$\alpha_n=|h_{bn}|^2$ 与 $\beta_n=|h_{en}|^2$ 表示第 n 个载波的信道增益系数;$p_n=E[x_n^2]$ 为第 n 个载波上的发射功率。在实际中,可以认为授权接收端与窃听端各载波信道的噪声方差相同,即 $\sigma_b^2=\sigma_{b1}^2=\cdots=\sigma_{bn}^2$,$\sigma_e^2=\sigma_{e1}^2=\cdots=\sigma_{en}^2$。那么 OFDM 系统的安全传输速率可表示为

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

2　最大化安全传输速率的功率分配算法

在实际传输中,考虑总功率受限的情况,有 $\sum_{n=1}^{N}p_n\leqslant P$,$P$ 为给定的总功率;又由于各载波分配的功率应该为非负值,故 $\forall p_n\geqslant 0$。因此将式(6)作为目标函数,根据上述系统存在的约束条件,通过对各载波功率进行优化分配,实现系统安全传输速率最大化。最大化安全传输速率描述可为一个有约束的非线性规划问题:

$$\max_{p} C_s(p)\ \text{s.t.}\ \sum_{n=1}^{N}p_n\leqslant P,p_n\geqslant 0,n=1,\cdots,N \tag{7}$$

其中,$\boldsymbol{p}=[p_1,\cdots p_N]$。根据 K-T 定理[9],构造拉格朗日函数:

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

其中:$\lambda_1,\cdots,\lambda_n$ 和 μ 为拉格朗日算子。由于在约束条件的梯度线性无关情况下,最优点必定是满足 K-T 条件的 K-T 点,因此首先求解式(8)的 K-T 点,然后从 K-T 点中选取满足 C_s 值最大的点,该点即为最优的功率分配。此时的 K-T 条件为

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

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

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

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

令 $\gamma_n=\sigma_e^2\alpha_n-\sigma_b^2\beta_n$,定义为载波功率分配因子,则可将式(9)变换为

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

从式(13)中不难看出,当 $\gamma_n<0$ 时会有 $\mu-\lambda_n<0$,则由式(11)(12)可知此时 p_n 必为零。因此,在分配功率之前,首先判断各载波的功率分配因子是否小于零,若 $\gamma_n\leqslant 0$,则不考虑给该载波分配功率;然后将 $\gamma_n>0$ 的载波根据 K-T 定理,由 K-T 条件式(9)~(12)再加上本身的约束条件

$$P-\sum_{n=1}^{N}p_n\geqslant 0\quad p_n\geqslant 0 \tag{14}$$

求解 K-T 点。从 γ_n 的定义式中可以看出,当 $\sigma_b^2=\sigma_e^2$ 时,功率分配因子的正负只由增益系数决定,而当 $\sigma_b^2\neq\sigma_e^2$ 时,功率分配因子不仅与增益系数有关,而且还与各接收端的背景噪声有关。

为求解 K-T 点,下面分以下几种情况考虑:

a)若式(14)第一项等号不成立,则由式(10)可知此时 $\mu=0$;又由于 $\gamma_n>0$,那么式(13)中的 λ_n 必然小于零,这和式(11)矛盾。因此式(14)第一项的等号必成立。

b)若式(14)第二项的等号成立,即存在 $p_i=0,i\in[1,2,\cdots,N]$,这时只要满足 $P-\sum_{n\neq i}^{N}p_n=0(n=1,\cdots,N)$ 就已经满足上述的 K-T 条件,故此时的 K-T 点有无穷多个。由式(8)可知此时的 λ_i、μ 应满足 $\frac{\alpha_i}{\sigma_b^2}-\frac{\beta_i}{\sigma_e^2}+\lambda_i-\mu=0$。

c)若式(14)第二项的等号不成立,则由式(11)可知此时的 $\lambda_n=0$;又由于 $\gamma_n>0$,则通过式(13)可知 $\mu>0$,将 $\lambda_n=0$ 代入式(13)可解得

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

故由式(14)(15)可解得 K-T 点。如果所求解中出现 $p_i<0$,其中 $i\in[1,2,\cdots,N]$,这与前面假设相矛盾,说明在该条件下将不存在 K-T 点,通过式(15)还可以获知此时会有 $\gamma_n\leqslant\mu\sigma_e^2\sigma_b^2$。

综上所述,可确定最终的功率分配算法,如图 2 所示。

算法主要步骤:首先判断各载波的功率分配因子的正负,若 $\gamma_n\leqslant 0$ 则不考虑给该载波分配功率,然后利用 $\gamma_n>0$ 的载波构造 K-T 条件求解 K-T 点。如果所求解的 K-T 点 p_n 都为正值,则将此时的 p_n 作为最终的最优分配结果,此时 OFDM 系统的安全传输速率达到最大;如果所求解的 p_n 中存在负值,由于与实际条件不符,将不考虑该载波的功率分配,利用 $p_n>0$ 的载波重新构造 K-T 条件求解 K-T 点,直到 p_n 都为正值时作为最终的分配结果。

3　仿真与性能分析

仿真过程中不考虑具体的调制方式,α_n、β_n 在[0,2]服从

均匀分布。a)验证优化分配的安全性,系统采用 128 个子载波,分别在不同信噪比下对比了优化分配与平均分配的安全传输速率;b)取 16 个子载波分析不同信噪比对功率分配的影响,并验证了文献[7]中结论与本文分析结果的一致性;c)在相同信噪比下取不同子载波数,分析载波数对系统安全速率的影响。

3.1 优化分配与平均分配的系统安全性能对比

图 3 为取载波数 $N=128$ 时优化分配的 C_s 与平均分配的 C_s 差值。从图 3 中可以看出,优化分配的 C_s 始终不低于平均分配的 C_s,而且在授权接收端与窃听端平均信噪比在 -5 dB ~ 5 dB 左右时,通过优化分配提高安全传输速率幅度较大,相比平均分配最高可提高 6.109 bit/s/Hz。但随着授权接收端与窃听端平均信噪比的升高,优化分配的安全传输速率提升幅度越来越小。这是由于此时 $\sigma_b^2\to 0,\sigma_e^2\to 0$,通过式(6)可以得到 C_s 将趋于 $\sum_{n=1}^{N}[\log(\frac{\alpha_n}{\beta_n})]^+$,说明通过调整载波功率分配提升 C_s 的空间越来越小。然而在平均信噪比达到 25 dB 时,优化分配的安全传输速率仍然可以提高 0.4521 bit/s/Hz,说明只要接收端的平均信噪比不是非常高,优化分配还是可以提升系统安全性的。从图 3 中还可以看出,在授权接收端与窃听端平均信噪比相差很大时,优化分配的 C_s 相比平均分配的 C_s 几乎得不到提高。这是由于此时系统处于一种极端状态,导致优化功率分配算法提高系统的安全性能下降。

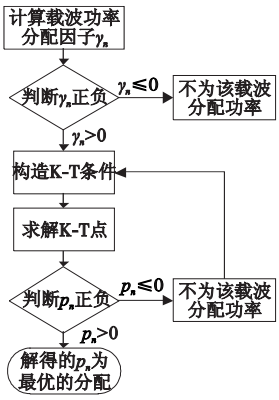


图2 功率分配算法流程

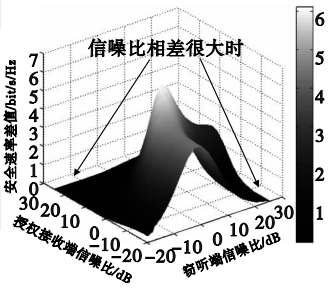


图3 优化分配与平均分配的安全传输速率差值

3.2 不同信噪比对功率分配的影响

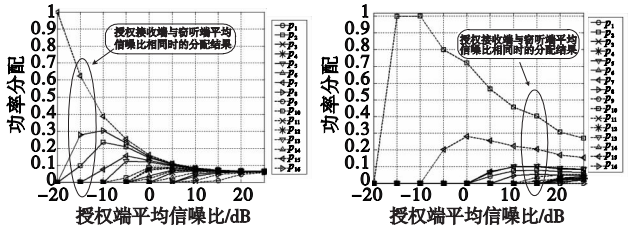
取载波个数 $N=16$ 随机产生一组载波信道增益系数,如表 1 所示。

表 1 授权接收端与窃听端的增益系数

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

图 4(a)是窃听端平均信噪比取 -15 dB 时,载波功率随授权接收端平均信噪比变化的分配结果。在授权接收端平均信噪比为 -15 dB 左右时,从图 4(a)和表 1 中可以看出功率分配主要与 $\alpha_n-\beta_n$ 有关,这与文献[7]中的结论一致。随着授权接收端平均信噪比的不断增加,各载波分配的功率向同一值趋近,当达到 20 dB 左右时分配结果趋于平均,即授权接收端平均信噪比远高于窃听端平均信噪比时,平均分配就是最优的功率分配。这是由于此时可认为 $\sigma_b^2 \ll \alpha_n,\beta_n \ll \sigma_e^2$,那么由式(15)近似可得到 $p_n\approx -\frac{\sigma_e^2}{2}+\sqrt{\frac{\sigma_e^4}{4}+\frac{\sigma_e^2}{\mu}}=c(\mu)$。可以看出,衰落系数将不影响载波的功率分配,各载波得到同一功率分配结果 $c(\mu)$。由于在总功率不变时,μ 的大小由载波数决定,因此载波分配的功率值大小也将由载波数决定。这就印证了图 3 的仿真结果,当窃听端平均信噪比在 -15 dB、授权接收端平均信噪比在 20 dB 时,优化分配的安全传输速率相比平均分配没有明显提升。

图 4(b)是窃听端平均信噪比取 15 dB 时,载波功率随授权接收端平均信噪比变化的分配结果。在授权接收平均信噪比为 15 dB 左右时,从图 4(b)和表 1 中可以看出功率分配主要与$\frac{\alpha_n}{\beta_n}$有关,这与文献[7]中的结论一致。随着 σ_e^2 的逐渐减小或 σ_b^2 的逐渐增大,会有越来越多的载波功率分配因子小于零,能够提供安全传输的载波数越来越少。当窃听端平均信噪比远大于授权接收端平均信噪比时,所有载波的功率分配因子均小于零,将没有载波能够提供安全传输,此时无论如何进行功率分配,系统的安全传输速率都将为零。这说明当授权接收端处信噪比非常低时,实现安全传输的可能性微乎其微,这也印证了图 3 的仿真结果。当窃听端平均信噪比在 20 dB、授权接收端平均信噪比在 -15 dB 时,系统的安全传输速率几乎为零,优化分配无法提升系统的安全性。但从图 4(b)中可以看出,在授权接收端平均信噪比低于窃听端平均信噪比的一定范围内,采用优化分配可以进行安全传输,说明只要授权接收端的条件不是很恶劣,优化分配可以提升系统安全传输性能。



(a)窃听端信噪比为-15 dB (b)窃听端信噪比为15 dB

图4 载波功率随授权接收端信噪比变化的分配结果

3.3 载波数对安全传输速率的影响

图 5 描述了不同载波数的系统安全传输速率。当授权接收端与窃听端平均信噪比为 10 dB 时,子载波数取 $N=8$ 的安全传输速率为 1.006 bit/s/Hz,子载波数取 $N=128$ 的安全传输速率为 26.75 bit/s/Hz,这表明通过增加载波数可以提高系统安全性。其原因可从式(6)得出,由于在 $\gamma_n\leqslant 0$ 时 $p_n=0$,则对任意的 $n\in[1,N]$ 都会有 $\log(1+\frac{\alpha_n p_n}{\sigma_b^2})-\log(1+\frac{\beta_n p_n}{\sigma_e^2})\geqslant 0$,因此随着 N 的不断增加,C_s 必然呈不断上升的趋势。从图 5 中还可以看出,在授权接收端与窃听端平均信噪比为 -15 dB 时,子载波数取 $N=8$ 和 $N=128$ 的安全传输速率分别为 0.1159 bit/s/Hz、1.865 bit/s/Hz,说明在信噪比低的情况下载波数的增加对系统安全性能也是有提升的。这是由于信噪比的降低,σ_b^2、σ_e^2 逐势,使增加载波数提升的系统安全性不断损失,但在信噪比不是非常低时,载波数的增加还是可以提高系统安全性的。

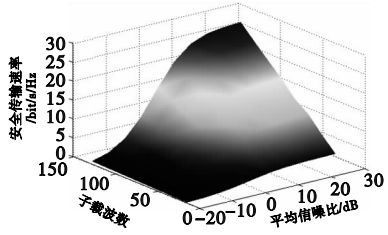


图5　载波数对安全传输速率的影响

4　结束语

针对 OFDM 系统的安全传输问题,本文提出了一种提高 OFDM 安全传输速率的载波功率分配算法。首先在总发射功率一定的条件下,考虑各载波信道衰落不同,以安全传输速率最大化为目标,利用 K-T 条件对各载波进行功率分配,分配结果在很大程度上提高了 OFDM 系统的安全传输性能。仿真结果表明,当授权接收端与窃听端平均信噪比在 -5 dB ~ 5 dB 内,优化分配的系统安全传输速率相比平均分配提升较为显著。在载波数取 $N=128$ 时,最高可提高 6.109 bit/s/Hz,并且随着信噪比的变化,优化分配的趋势将会有明显的改变。虽然系统采用的载波数可以影响系统的安全传输速率,但在信噪比很低的情况下,安全传输速率提升幅度也非常有限。

参考文献:

[1] LI Zheng, XIA Xiang-gen. A distributed differentially encoded OFDM scheme for asynchronous cooperative systems with low probability of interception[J]. IEEE Trans on Wireless Communication, 2009, 8(7): 3372-3379.

[2] RENNA F, LAURENTI N, POOR H V. Physical layer secrecy for OFDM systems[C]//Proc of IEEE European Wireless Conference. 2010: 782-789.

[3] RENNA F, LAURENTI N, POOR H V. High SNR secrecy rates with OFDM signaling over fading channels[C]//Proc of the 21th IEEE International Symposium on Personal Indoor and Mobile Radio Communications. 2010: 2692-2697.

[4] JORSWIECK E, WOLF A. Resource allocation for the wire-tap multi-carrier broadcast channel[C]//Proc of International Workshop on Multiple Access Communications. 2008.

[5] BLOCH M, BARROS J, RODRIGUES M R S. Wireless information theoretic security[J]. IEEE Trans on Information Theory, 2008, 54(6): 2515-2534.

[6] GOPALA P K, CAI L, GAMAL H E. On the secrecy capacity of fading channels[C]//Proc of IEEE International Symposium on Information. 2007.

[7] LIANG Ying-bin, POOR H V. Secure communication over fading channels[J]. IEEE Trans on Information Theory, 2008, 54(6): 2470-2492.

[8] CSISZAR I, KONER J. Broadcast channels with confidential messages[J]. IEEE Trans on Information Theory, 1978, 24(3): 339-348.

[9] 施光艳,钱伟懿,庞丽萍. 最优化方法[M]. 2 版. 北京:高等教育出版社,2010.