doi:10.3969/j.issn.1000-436X.2012.10.011

多载波系统随机子载波加权的物理层加密算法

钟州，金梁，黄开枝
（国家数字交换系统工程技术研究中心，河南 郑州 450002）

摘 要：针对多载波传输系统中，基于载波资源分配算法在窃听者信道质量优于合法用户的条件下无法实现安全传输的问题，建立了 OFDM 系统安全传输模型并在物理层提出了一种随机子载波加权的加密算法。该算法将合法通信双方的信道状态信息作为区分不同用户的唯一特征，并以此在发端为每个子载波数据设置随机加权因子扰乱窃听用户接收的信号，而合法用户能够通过发送参考解调算法恢复数据，仿真结果表明，发端采用该算法进行加密后，合法用户的误比特率随信噪比的增加迅速下降，而窃听用户误比特率始终为 50%，系统具有一定的保密传输速率，有效实现了信息的安全传输。

关键词：正交频分复用；物理层安全；低截获概率；保密传输速率
中图分类号：TN918 **文献标识码**：A **文章编号**：1000-436X(2012)10-0086-05

Using random subcarrier weighting for multi-carrier systems physical layer security

ZHONG Zhou, JIN Liang, HUANG Kai-zhi
(National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China)

Abstract: An OFDM security model and a physical layer security transmission scheme were proposed for multi-carrier systems to achieve low probability of interception. In contrast to the resource allocation algorithm which would be disabled at the low SNR, this method designed the subcarrier transmission weighting vectors to randomize the eavesdropper's signals but not the authorized receiver's signals. The channel state information was the only character to distinguish authorized receivers and eavesdroppers, which was conducted to guide the weighting vectors design. Simulation results show that the proposed method guarantees that authorized receiver performs transmitted reference demodulation successfully, while the eavesdroppers can not detect the transmitted symbols.

Key words: orthogonal-frequency division multiplexing; wireless communication PHY-layer security; low probability of interception; security rate

1 引言

正交频分复用（OFDM, orthogonal frequency division multiplexing）作为一种多载波调制传输技术，能实现数据在多径衰落信道中的高速传输而被广泛应用于各种军事和民用无线数字宽带通信系统。然而，无线信道的开放性和电磁信号传播的广播特性使OFDM系统为用户提供高速丰富多媒体业务的同时，其信息安全问题变得日益突出和重要。

面对非法用户的高效破解算法以及计算能力的不断提升，若沿用传统的在应用层通过密钥对信

收稿日期：2011-12-05；**修回日期**：2012-06-11
基金项目：国家自然科学基金资助项目(61171108)
Foundation Item: The National Natural Science Foundation of China (61171108)

源进行加密的方法只有保证“一次一密”才能实现信息安全传输，这对无线通信系统的密钥管理与分发提出了较高要求，并不能从根本上解决无线信道开放性导致的安全问题；此外，采用扩频、跳频、超宽带等特殊体制设计信号，使其具备低截获概率的特性，能够提供一定的加密性能。然而，信号体制中特定的扩频序列或跳频图案一旦泄露，信息就会被窃听者正确解调，从而失去了安全传输的目的。为保证无线通信的信息安全，Wyner 首先建立 wire-tap 信道模型[1]，从信息论的角度提出在物理层设计编码算法能够实现“完美加密”，并定义保密容量即在窃听用户无法获取任何信息的条件下，发送端向合法用户传输信息速率的最大值，作为度量通信系统安全性能的标准。Jorswieck[2]以此推导出了多载波系统在广播信道下的保密容量，指出可以通过资源分配算法提高多载波系统的保密传输速率。文献[3,4]针对多载波系统提出了单用户及多用户通信时，在保密容量约束条件下的子载波资源分配算法。通过利用发送端与合法用户及窃听用户间的信道状态信息（CSI, channel state information）计算保密容量，并以最大化保密容量为优化目标建立凸优化模型，根据最优解为合法用户分配载波数和各子载波的发射功率实现信息安全传输。文献[5]进一步研究了在 OFDM 系统中，当输入信号服从非高斯分布条件下，采用 PSK、QAM 调制时逼近保密容量的子载波功率优化分配算法。

上述方法的本质都是发射机在已知与合法用户以及窃听用户间 CSI 条件下，从信息论的角度优化分配多载波系统的载波资源，以最大化保密传输速率为目标实现信息的安全传输。然而实际上窃听用户往往只做被动接收并不主动发射信号，因此发射机很难获取与窃听用户间的 CSI。本文针对单天线多载波系统，仅利用合法通信双方的信道特征，在发送端为每个子载波传输的数据设置随机预加权因子扰乱窃听者的接收，使得合法用户能够采用发送参考（TR, transmitted reference）解调算法恢复各子载波上的数据，而非法窃听用户接收的每个符号经过发送端预加权处理随机变化，无法还原各载波上的数据信息，满足对窃听端低截获概率的要求。

2　OFDM 系统安全传输模型

OFDM 系统安全传输主要涉及三方，如图 1 所示，Alice 作为基站端需要把信息安全传输给合法用户 Bob，而 Eve 作为窃听者只进行被动接收而不做任何主动发射。Alice 和 Bob 均使用单天线且基站端采用 OFDM 调制方式，则收发双方组成一个单输入单输出（SISO, single-input single-output）OFDM 系统。Eve 为了获得较 Bob 更好的接收信号质量，采用多天线接收保证窃听效果，因此 Alice 和 Eve 间的通信可建模为单输入多输出（SIMO, single-input multi-output）OFDM 系统。

通信时采用文献[6]的策略，即 Bob 首先向 Alice 发送未加密的请求信息，该请求信息同时包含用于信道估计的训练序列。Alice 收到请求信息后根据接收到的训练序列估计他们之间的信道。根据信道互易原理[6]，即在时分双工（TDD, time division

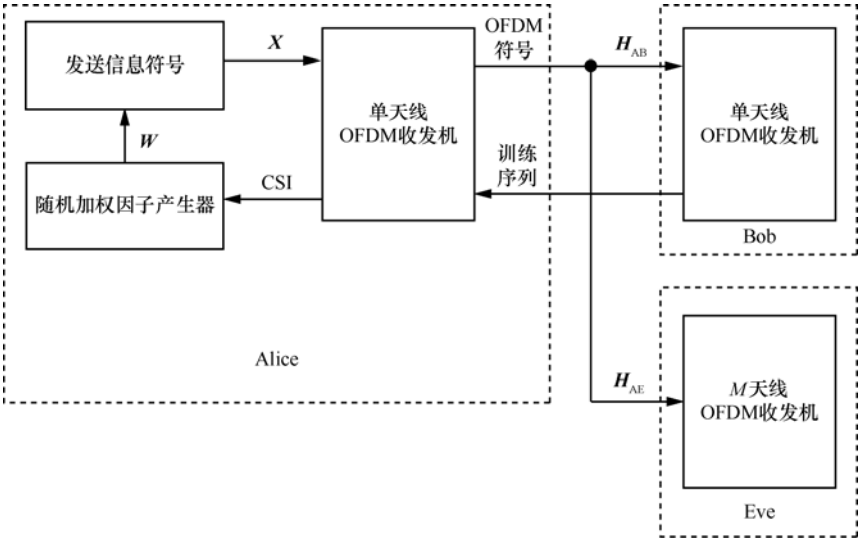


图 1　OFDM 系统安全传输模型

duplex）模式的无线通信系统中，当信道处于慢时变状态，则系统的上、下行信道具有相同的信道特征。因此可以认为 Alice 与 Bob 之间收发信道的信道特征相同，Alice 可以根据估计的信道特征对即将发送给 Bob 的信息进行加密。

根据该 OFDM 系统安全传输模型，在采用 N 个子载波传输的多载波系统中，Alice 发射的信号经过 L 径的频率选择性衰落信道传输，则 Bob 的接收机在第 k 个子载波上接收的频域信号可以表示为

$$Y_{\mathrm{B}}(k)=X(k)H_{\mathrm{AB}}(k)+N(k) \tag{1}$$

其中，$X(k)$ 是第 k 个子载波上发送的信号，$H_{\mathrm{AB}}(k)$ 表示 Alice 和 Bob 的收发天线间第 k 个子载波对应的频域信道冲击响应，$N(k)$ 为零均值单位方差的加性高斯白噪声。定义 Alice 与 Bob 间的信道为信息传输的主信道，则主信道第 k 个子载波的频域信道冲击响应为

$$H_{\mathrm{AB}}(k)=\sum_{l=1}^{L}a_{\mathrm{AB}}(l)\mathrm{e}^{-\mathrm{j}2\pi k\Delta f\tau_{\mathrm{AB}}(l)} \tag{2}$$

其中，L 表示多径数，$a_{\mathrm{AB}}(l)$ 表示第 l 径的幅度值，Δf 表示子载波间隔，$\tau_{\mathrm{AB}}(l)$ 表示第 l 径的时延。

当 Eve 采用 M 个天线进行窃听接收时，第 m $(1\leqslant m\leqslant M)$ 个天线上收到第 k 个子载波的频域信号可以表示为

$$Y_{\mathrm{E}_m}(k)=X_m(k)H_{\mathrm{AE}_m}(k)+N_m(k) \tag{3}$$

定义 Alice 与 Eve 间的信道为窃听信道，则窃听信道第 k 个子载波的频域信道冲击响应为

$$H_{\mathrm{AE}_m}(k)=\sum_{l=1}^{L}a_{\mathrm{AE}_m}(l)\mathrm{e}^{-\mathrm{j}2\pi k\Delta f\tau_{\mathrm{AE}_m}(l)} \tag{4}$$

若 Alice 为每个子载波发送数据设计加权因子，记作 $w(k)$，那么 Bob 和 Eve 接收信号的频域矩阵形式可分别表示为

$$\boldsymbol{Y}_{\mathrm{B}}=\boldsymbol{XWH}_{\mathrm{AB}}+\boldsymbol{N}_{\mathrm{B}} \tag{5}$$

$$\boldsymbol{Y}_{\mathrm{E}}=\boldsymbol{XWH}_{\mathrm{AE}}+\boldsymbol{N}_{\mathrm{E}} \tag{6}$$

该系统中由于 Eve 可能处于空间中任意不同于 Bob 的位置，并且通过多天线接收能够获得较 Bob 更高质量的信号，因此发送信息极易被窃取。

3 随机子载波加权物理层加密算法

在采用 OFDM 调制的宽带无线系统中，同一时间处于空间不同位置，不同频点子载波的信道特征差异是区分不同用户最重要的特征。为了防止信息在无线传输过程中被截获，关键是要提取并运用信道特征，为每个子载波设计随机变化的加权因子，构造快速变化的等效信道特征 $\boldsymbol{WH}_{\mathrm{AB}}$，防止 Eve 对其进行有效的跟踪。

根据上述分析，本文在 Alice 端设计发送信号时，将 N 个子载波中的第 1 个子载波用于传输导频数据，其余 $N-1$ 个子载波用于传输数据信息 $\boldsymbol{X}$。通过设计随机预编码矩阵 $\boldsymbol{W}$，对 OFDM 系统中每个子载波上的数据随机加权完成加密。算法的基本思想是利用 Alice 与 Bob、Eve 的信道特征 $\boldsymbol{H}_{\mathrm{AB}}$、$\boldsymbol{H}_{\mathrm{AE}}$ 的差异构造随机预编码矩阵 $\boldsymbol{W}$，使该矩阵中随机加权因子 $w(k)$ 满足式（7）约束。

$$w(0)\boldsymbol{H}_{\mathrm{AB}}(0)=w(k)\boldsymbol{H}_{\mathrm{AB}}(k),\quad 1\leqslant k\leqslant N-1 \tag{7}$$

记接收到的第 1 个子载波承载的导频数据为 y_{B1}，矩阵形式为 $\boldsymbol{Y}_{\mathrm{B1}}$，后 $N-1$ 个子载波承载的信息数据的矩阵形式记作 $\boldsymbol{Y}_{\mathrm{B2}}$，那么由式（1）、式（7）可将每个子信道接收到的符号表示为 $Y_{\mathrm{B2}}(k)=X(k)y_{\mathrm{B1}}+\hat{N}_{\mathrm{B}}(k)$，其中，$\hat{N}_{\mathrm{B}}(k)=N_{\mathrm{B2}}(k)-X(k)N_{\mathrm{B1}}(0)$。利用 TR 解调算法[7]，可由第一个子载波上的导频信息获得各子载波上的等效信道特征，根据式（8）的最大似然准则进行判决即可解出 Alice 发送数据 $X(k)$。

$$\hat{\boldsymbol{X}}=\arg\min_{X}\|\boldsymbol{Y}_{\mathrm{B2}}-\boldsymbol{XY}_{\mathrm{B1}}\|_F^2 \tag{8}$$

由于 Bob 与 Eve 所处位置不同，即 $H_{\mathrm{AB}}(k)\neq H_{\mathrm{AE}}(k)$，那么存在 $w(0)H_{\mathrm{AB}}(0)\neq w(k)H_{\mathrm{AE}}(k)$，$1\leqslant k\leqslant N-1$，则 Eve 将无法直接通过第一个子载波上承载的导频信息按式（8）解调出数据。另一方面，对每个子载波对应的信道特征采用随机加权处理，相当于对发给合法用户的数据进行随机预编码，主动快速改变了发送端与窃听者之间的等效信道特征，使得窃听者获取不到发送信号的统计特性，无法有效实施恒模算法等基于盲解卷积的信道盲均衡方法[8,9]解调数据。从而 Alice 发送的信息对窃听者 Eve 起到加密作用。

基于上述思想设计随机子载波加权的物理层加密算法共分为 3 个步骤。

步骤 1 信道估计。通信开始时，首先由合法接收用户 Bob 发射导频信号或训练序列，用于发送用户 Alice 估计收发双方的信道状态信息 $\boldsymbol{H}_{\mathrm{AB}}$。

步骤 2 计算随机加权因子。根据图 2 所示随机子载波加权系数产生器结构，为每个子载波构造

加权系数 w，该系数包括随机的幅度和随机的相位，设计时可以分成 w_0, w_k 这 2 部分，记

$$\begin{cases} w_0 = W(k),\ k = 0 \\ w_k = W(k),\ 1 \leqslant k \leqslant N-1 \end{cases} \tag{9}$$

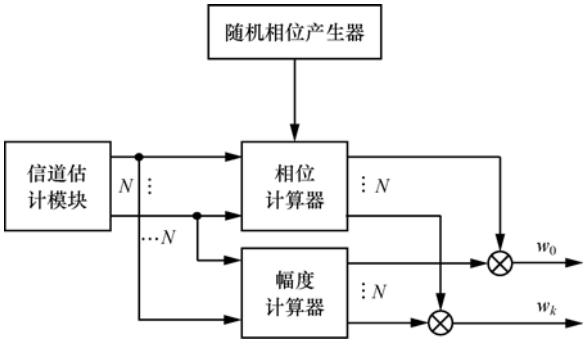


图 2　随机子载波加权系数产生器

首先将步骤 1 估计的第 1 个子载波信道状态信息 $H_{\mathrm{AB}}(0)$ 输入相位计算器和幅度计算器。随机相位产生器产生第 1 个子载波加权系数 w_0 的相位 $\theta_{w_0} \sim (0, 2\pi)_{\mathrm{rand}}$，相位计算器按式（7）的相位约束根据 θ_{w_0}，由式 $\theta_{w_k} = \theta_{H_{\mathrm{AB}}(0)} + \theta_{w_0} - \theta_{H_{\mathrm{AB}}(k)}$ 产生 N 个子载波加权系数的相位 θ_{w_k}；然后，根据幅度约束 $|w_0||H_{\mathrm{AB}}(0)| = |w_k||H_{\mathrm{AB}}(k)| = C$，幅度计算器按照 $|w_k| = C/|H_{\mathrm{AB}}(k)|$ 准则产生 N 个子载波加权系数的幅度；最后将产生的幅度与相位对应相乘即构造出每一个子载波数据的加权因子 $w_k = |w_k| \mathrm{e}^{\mathrm{j}\theta_{w_k}}$。

步骤 3　TR 解调。Bob 接收到的信号包含第 1 个子载波承载的导频数据 y_{B1}，以及后 $N-1$ 个子载波承载的信息数据 Y_{B2}，根据式（7）的约束，按式（8）进行最大似然判决完成数据解调。

上述加密算法即使在 Alice 未知与 Eve 信道特征 $\boldsymbol{H}_{\mathrm{AE}}$ 的条件下也可实现信息的安全传输，可以用最大信道转移概率近似最大后验概率给出未知 $\boldsymbol{H}_{\mathrm{AE}}$ 条件下系统的保密传输速率。

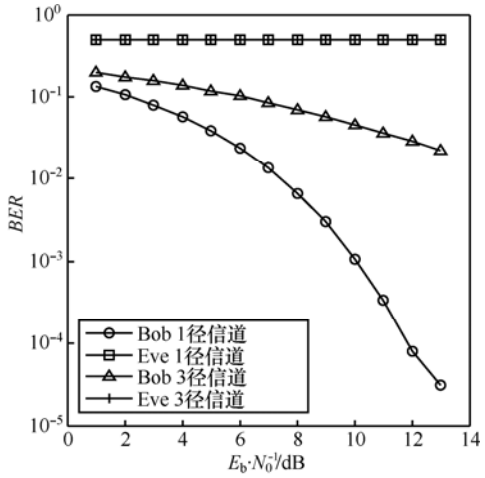
定理 1　假设输入信号服从等概分布，记 Alice 与 Bob 数据传输的误码率为 e_{AB}，Alice 与 Eve 数据传输的误码率为 e_{AE}，定义二元熵函数 $H(e) = -e\log e - (1-e)\log(1-e)$，则二进制广播信道的保密速率为 $C_s = H(e_{\mathrm{AE}}) - H(e_{\mathrm{AB}})$。

定理的证明详见附录 1。

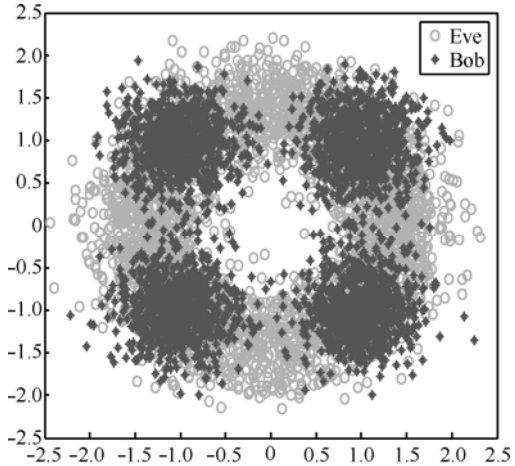
4　仿真实验

本节对随机子载波加权算法的加密效果进行仿真，为此假设系统带宽为 1MHz，在发端设置 OFDM 系统子载波数为 64，则一个 OFDM 符号长度为 64μs。为防止符号间干扰设循环前缀长度为 16μs，数据采用 QPSK 调制后分别在有直达径和多径时延为 10μs 的 3 条独立的具有相同幅度径的多径信道上叠加加性高斯白噪声（AWGN, additive white Gaussian noise）传输。

仿真在不同信噪比条件下对 Alice 发出的 1 000 个 OFDM 符号进行 100 次独立实验，统计了 Bob 和 Eve 接收信号的误比特率（BER, bit error rate），结果如图 3（a）所示。从图中可以看出采用本文提出的加密算法，合法用户 Bob 无论在有直达径还是多径信道条件下，接收信号的 BER 随信噪比的增加迅速降低，而窃听者 Eve 的 BER 始终保持在 50%，说明 Eve 即使在信道质量较好的情况下也无法获取 Alice 发出的任何信息。而在此情况下，若



(a) 直达径与多径信道下的误比特率



(b) *SNR*=10dB 时接收信号星座

图 3　合法用户与窃听用户接收信号对比

采用文献[2]中的子载波功率分配安全算法，由于窃听者的信道质量优于合法用户，那么根据最优化模型求解 Alice 所有载波分配功率值均为 0，即系统在保证信息安全传输的条件下只能选择放弃通信。图 3（b）给出了采用该算法在 *SNR*=10dB 时 Bob 和 Eve 接收信号星座，进一步说明该算法能够实现加密的原因。从图中可以看出 Bob 利用第一个子载波上发送的导频信息，通过 TR 算法解调后能够获得规则的信号星座，而 Eve 受随机预编码的影响，接收到的每个符号对应的星座都被随机置乱，难以从快速随机变化的信号中获得统计信息对信道进行盲估计，因而无法恢复接收信号。

图 4 分别给出了数据信息在只有直达径和有 3 条径的多径信道上传输时，OFDM 系统对子载波进行归一化后的保密传输速率。根据文献[1]中保密速率的定义，在 Eve 无法获取信息的条件下，系统的保密传输速率与 BER 成反比，随着信噪比的增加保密传输速率逼近信道容量，系统能够保证信息的安全传输。

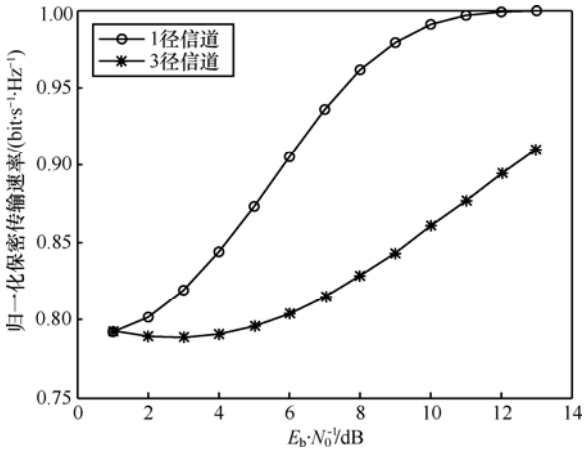


图 4 不同信道中的保密传输速率

5 结束语

本文针对时分双工多载波通信系统，建立了基于 OFDM 调制的物理层安全传输模型，通过利用合法通信双方与窃听者空间不同位置 CSI 的差异，对不同子载波传输的数据进行频域随机加权预编码，提出了一种物理层加密算法，并推导出了系统的保密容量。分析及仿真结果表明该算法在保证合法用户接收信号质量的条件下，大大降低了被非法用户截获的概率，保证了信息的安全传输。本文提出的物理层加密算法可以与传统应用层密钥加密方法相互结合，能够更加有效地解决无线通信中的安全问题，因此也具有很好的应用价值。

附录 1 定理 1 的证明

由保密速率的定义[1]可得：

$$\begin{aligned} C_s &= I(X,Y_{\mathrm{AB}}) - I(X,Y_{\mathrm{AE}}) \\ &= H(X \mid Y_{\mathrm{AE}}) - H(X \mid Y_{\mathrm{AB}}) \end{aligned} \tag{10}$$

其中，$H(X \mid Y_{\mathrm{AE}}) = H(X) - H(Y_{\mathrm{AE}}) + H(Y_{\mathrm{AE}} \mid X)$

令二元随机变量 X 的分布满足 $\begin{cases} P(x=0)=p \\ P(x=1)=1-p \end{cases}$

则 $H(X) = -p\log p - (1-p)\log(1-p) = H(p)$，那么 Eve 接收信号 Y_{AE} 的分布满足

$$\begin{cases} P(Y_{\mathrm{AE}}=0) = p(1-e_{\mathrm{AE}}) + (1-p)e_{\mathrm{AE}} = p + e_{\mathrm{AE}} - 2pe_{\mathrm{AE}} \\ P(Y_{\mathrm{AE}}=1) = 1-(p+e_{\mathrm{AE}}-2pe_{\mathrm{AE}}) \end{cases} \tag{11}$$

则 $H(Y_{\mathrm{AE}}) = H(p+e_{\mathrm{AE}}-2pe_{\mathrm{AE}})$。令 $a_1=0, a_2=1$，且 X 为等概分布时有二元条件熵

$$\begin{aligned} H(Y_{\mathrm{AE}} \mid X) &= \sum_{i=1}^{2} P(x=a_i) H(Y_{\mathrm{AE}} \mid X=a_i) \\ &= -\sum_{i=1}^{2}\sum_{j=1}^{2} P(x=a_i) P(Y_{\mathrm{AE}}=a_j \mid X=a_i) \cdot \\ &\quad \log P(Y_{\mathrm{AE}}=a_j \mid X=a_i) \\ &= H(e_{\mathrm{AE}}) \end{aligned} \tag{12}$$

所以，$H(X \mid Y_{\mathrm{AE}}) = H(p) - H(p+e_{\mathrm{AE}}-2pe_{\mathrm{AE}}) + H(e_{\mathrm{AE}})$，同理 $H(X \mid Y_{\mathrm{AB}}) = H(p) - H(p+e_{\mathrm{AB}}-2pe_{\mathrm{AB}}) + H(e_{\mathrm{AB}})$，由式（10）得

$$\begin{aligned} C_s = {} & H(e_{\mathrm{AE}}) - H(e_{\mathrm{AB}}) + \\ & H(p+e_{\mathrm{AB}}-2pe_{\mathrm{AB}}) - H(p+e_{\mathrm{AE}}-2pe_{\mathrm{AE}}) \end{aligned} \tag{13}$$

当 $p=\frac{1}{2}$ 时代入式（13），$C_s = H(e_{\mathrm{AE}}) - H(e_{\mathrm{AB}})$，证毕。

参考文献：

[1] WYNER A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.

[2] JORSWIECK E, WOLF A. Resource allocation for the wire-tap multi-carrier broadcast channel[A]. Proc International Workshop on Multiple Access Communications (MACOM)[C]. St Petersburg, Russia, 2008.

[3] FRANCESCO R, NICOLA L, VINCENT H P. Physical layer secrecy for OFDM systems[A]. Proc IEEE European Wireless Conference[C]. Lucca, Italy, 2010.782-789.

（下转第 100 页）

[5] 3GPP TSG RAN WG1 Meeting #56R1-090551. Final Report of 3GPP TSG RANWG1 #55bis v1.0.0[S]. Ljubljana, Slovenia, 2009.

[6] 3GPP TSG RAN WG1 Meeting #55bis R1-090298. Effectiveness of Discontinuous Resource Allocation for LTE-A Uplink within 20MHz[S]. Ljubljana, Slovenia, 2009.

[7] BERARDINELLI G, RUIZ De TEMINO L A, FRATTASI S, *et al*. OFDMA vs. SC-FDMA: performance comparison in local area IMT-A scenarios[J]. IEEE Wireless Communications, 2008,15(5):64-72.

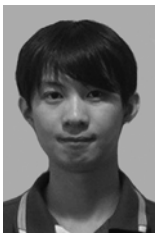
[8] FILHO D Z, LFÉTY, TERRÉ M. A hybrid single-carrier/multicarrier transmission scheme with power allocation[J]. EURASIP Journal on Wireless Communications and Networking, 2008,1(1):1-11.

[9] 李明齐, 芮赟等. 宽带无线通信多址传输技术演进[M]. 北京: 电子工业出版社, 2010.
LI M Q, RUI Y, *et al*. Evolution of Multi-access Transmission Technology based on Broadband Wireless Communication[M]. Beijing: Electronic industry press, 2010.

[10] 3GPP TSG RAN WG1 Meeting #42R1-050718. Simulation Methodology for EUTRA UL: IFDMA and DFT-Spread-OFDMA[S]. Motorola, 2005.

[11] 3GPP TSG RAN WG1 #37， R1-040642. Comparison of PAR and Cubic Metric for Power De-rating[S]. Montreal, Canada, 2004.

作者简介：



田攀（1987-），男，湖北黄冈人，中国科学院上海微系统与信息技术研究所硕士生，主要研究方向为虚拟无线电、宽带无线接入系统。

李明齐（1971-），男，江西南昌人，中国科学院上海高等研究院研究员，主要研究方向为宽带无线通信、三网融合无线技术、软件无线电。

芮赟（1983-），男，江苏溧阳人，中国科学院上海高等研究院副研究员，主要研究方向为通信中的信号处理、宽带无线接入系统等。

郑敏（1974-），男，河南新乡人，中国科学院上海微系统与信息技术研究所副研究员，主要研究方向为宽带无线通信系统移动性管理、自组织网络的自动配置技术。

卜智勇（1970-），男，安徽滁州人，中国科学院上海微系统与信息技术研究所研究员，主要研究方向为宽带无线应急通信、宽带无线多媒体。

（上接第 90 页）

[4] WANG X W, TAO M X, MO J H, *et al*. Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks[J]. IEEE Trans Information Forensics and Security, 2011, 6(3): 693-702.

[5] QIN H H, SUN Y, CHEN X, *et al*. Optimal power allocation for OFDM-based wire-tap channels with arbitrarily distributed inputs[A]. Proc International ICST Conference on Wireless Internet[C]. Xi'an, China, 2011.

[6] LI X, HWU J, RATAZZI E P. Using antenna array redundancy and channel diversity for secure wireless transmissions[J]. Journal of communications, 2007, 2(3):224-232.

[7] ZHAO S W, ORLIK P, MOLISCH A F, *et al*. Hybrid ultrawideband modulations compatible for both coherent and transmit-reference receivers[J]. IEEE Trans Wireless Communications, 2007, 6(7): 2551-2559.

[8] INOUYE Y. Criteria for blind deconvolution of multichannel linear time-invariant systems[J]. IEEE Trans Signal Processing, 1998, 46 (12): 3432-3436.

[9] LI X. Blind channel estimation and equalization in wireless sensor networks based on correlations among sensors[J]. IEEE Trans Signal Processing, 2005, 53(4): 1511-1519.

作者简介：

钟州（1982-），男，吉林省吉林市人，国家数字交换系统工程技术研究中心博士生，主要研究方向为移动通信、通信信号处理与信息安全。

金梁（1969-），男，北京人，博士，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为超宽带无线通信、通信信号处理与智能天线。

黄开枝（1973-），女，安徽来安人，博士，国家数字交换系统工程技术研究中心副教授，主要研究方向为第三代移动通信与异构无线网络安全。