第 43 卷 第 2 期 计 算 机 工 程 2017 年 2 月
Vol. 43 No. 2 Computer Engineering February 2017

·移动互联与通信技术· 文章编号:1000-3428(2017)02-0171-05 文献标志码:A 中图分类号:TN911

考虑频谱感知错误的多载波认知无线电资源分配算法

庄 陵,马 龙

(重庆邮电大学 移动通信技术重点实验室,重庆 400065)

摘 要: 认知无线电(CR)资源分配中二级用户对主用户造成的干扰源于两方面,即带外频谱泄露和频谱感知错误。滤波器组多载波(FBMC)技术和正交频分复用(OFDM)技术相比,FBMC 带外泄露较小,频谱利用率较高。FBMC 技术考虑干扰来源,可以降低二级用户对主用户的干扰,提高 CR 系统吞吐量。为此,提出考虑频谱感知错误的 CR 资源分配算法,建立干扰模型,将资源分配分步简化为载波分配和功率分配,在干扰约束和功率约束条件下对二级用户进行功率分配。基于 FBMC 和 OFDM 系统的仿真结果表明,该算法对主用户造成的干扰更小,CR 系统可以获得更大的吞吐量,FBMC 的干扰和吞吐量性能均优于 OFDM。

关键词: 频谱感知错误;认知无线电;滤波器组;资源分配;正交频分复用;多载波技术

中文引用格式: 庄 陵,马 龙. 考虑频谱感知错误的多载波认知无线电资源分配算法[J]. 计算机工程,2017,43(2):171-175,182.

英文引用格式: Zhuang Ling, Ma Long. Resource Allocation Algorithm of Multicarrier Cognitive Radio Considering Spectrum Sensing Error[J]. Computer Engineering,2017,43(2):171-175,182.

Resource Allocation Algorithm of Multicarrier Cognitive Radio Considering Spectrum Sensing Error

ZHUANG Ling, MA Long

(Key Laboratory of Mobile Communication Technology,
Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

【Abstract】 The interference in Cognitive Radio(CR) resource allocation introduced by the Secondary User(SU) to the Primary User(PU) derives from two aspects: Out-of-Band Leakage(OOBL) and Spectrum Sensing Error(SSE). Filter Bank Multicarrier (FBMC) has small OOBL and high spectral efficiency in comparison with Orthogonal Frequency Division Multiplexing(OFDM). Full consideration of interference sources can reduce the interference from SU to PU and improve CR system throughput. So this paper proposes a resource allocation algorithm considering SSE in CR network, establishes the interference model, decomposes resource allocation into subcarrier allocation and power allocation, and allocates the power to SU under both interference constraint and power constraint. Simulation results based on FBMC and OFDM show that the proposed algorithm causes less interference to PU. The CR system can obtain greater throughput, and the performance of FBMC in interference and throughput is better than that of OFDM.

【Key words】 spectrum sensing error; Cognitive Radio (CR); filter bank; resource allocation; Orthogonal Frequency Division Multiplexing(OFDM); multicarrier technology

DOI: 10.3969/j.issn.1000-3428.2017.02.028

0 概述

近年来,由于数字技术和移动计算能力的高速发展,多媒体移动终端数量快速增长,需要更多的频谱资源,以保证移动宽带的实现和传输速率。无线频谱资源越见稀缺,现有的频谱管理与分配策略是造成频谱资源稀缺的重要原因[1]。认知无线电(Cognitive Radio,CR)技术的出现,被认为是解决无线频谱资源匮乏的有效手段之一[2]。

正交频分复用(Orthogonal Frequency Division

基金项目: 重庆市教委科学技术研究项目(KJ1500435,KJ1500147)。

作者简介: 庄 陵(1978—),女,副教授、博士,主研方向为宽带无线通信;马 龙,硕士研究生。

收稿日期: 2016-01-13 **修回日期:** 2016-02-22 **E-mail:** zhuangling@cqupt.edu.cn

Multiplexing,OFDM)[3]技术的抗多径衰落能力较强、频谱利用率较高,信道均衡技术也较为简单,当前多数 CR 资源分配方案基于 OFDM。但是 OFDM 技术存在的缺点,如较大的带外泄漏(Out-of-Band Leakage,OOBL)、较高的峰均比,由于循环前缀造成频谱利用率不高,特别是较大的带外频谱泄漏,严重影响了系统的频谱效率。

滤波器组多载波(Filter Bank Multicarrier,FBMC)[4-5]技术的带外频谱泄露较小,可以不插入循环前缀,频谱利用率高于 OFDM,非常适用于 CR 系统。由于 FBMC 的诸多优点,该技术已成为 5G 物理层重要的一个候选方案[6-7]。

CR 系统资源分配过程中二级用户(Secondary User,SU)对主用户(Primary User,PU)的干扰不能超过干扰门限,以保证 PU 的正常通信。当前多数研究基于 CR 完全正确的频谱感知信息,但在实际通信环境中,由于传播损耗、阴影衰落、多径衰落、CR 接收器灵敏度等因素,频谱感知并非完全正确,会产生误差,由此造成对 PU 的干扰。因而,SU 对 PU 的干扰来源于 2 个方面:1)带外泄露干扰;2)频谱感知错误(Spectrum Sensing Error,SSE)。

目前 CR 资源分配问题已有一些相关文献可以参考。文献[8]在干扰约束和功率约束条件下,根据比例公平的原则对认知用户进行资源分配。文献[9]把资源分配当作一维问题,基于单用户的系统模型,提出一种 Max-Min 算法,利用背包问题模型解决资源分配问题。文献[10]以认知用户服务质量需求为优化目标,采用贪婪算法实现多目标优化。文献[11]提出保证认知用户最小速率需求的资源分配算法,保证认知用户需求的同时也降低了系统的吞吐量。

上述文献研究的均是基于频谱感知完全正确的系统模型。然而实际通信环境中频谱感知总是有错误的,对 PU 的干扰源于 OOBL 及 SSE。不考虑 SSE 会降低分配给子载波的功率,影响 CR 系统的吞吐量。为了全面考虑干扰的来源,降低 SU 对 PU 的干扰,提高 CR 系统吞吐量,本文基于 FBMC 多载波技术,提出考虑频谱感知错误的资源分配算法,并与基于 OFDM 的 CR 系统作对比仿真分析。

1 系统模型

图 1 为 CR 网络的系统构架图。PU 和 SU 共存于同一个地理通信环境,认知基站(Cognitive Base Station,CBS)向 SU 发送信息时会对 PU 造成干扰,同时 PU 与主用户基站之间的通信也会对 SU 的通信产生干扰。

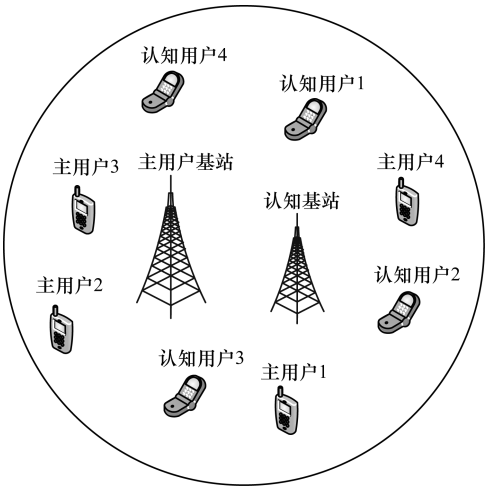

图 1 CR 网络系统构架

PU 授权频段的子载波分布情况如图 2 所示。PU 频段有 N 个子载波,CR 系统通过频谱感知确定 PU 频段中未被占用的子载波,这些子载波构成集合 N_v。SU 使用集合 N_v 中的子载波进行数据传输,剩余的子载波被确定为 PU 占用的子载波,这些子载波构成集合 N_o。集合 N_o 中的子载波被认为是正在被 PU 占用,不能被 SU 使用。

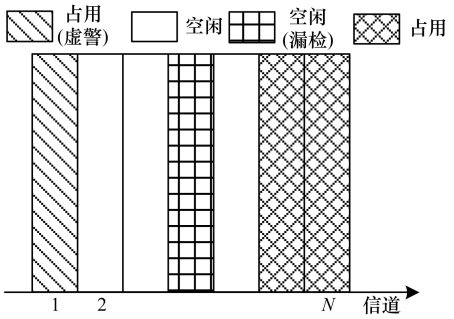

图 2 频谱感知错误接入模型

如图 2 所示,有些子载波被认为是 PU 占用的,但实际是空闲的,即虚警错误,用虚警概率 Q_{fa} 表示;有些子载波被 PU 占用,感知结果却是空闲的,即漏检错误,用漏检概率 Q_{md} 表示。在 CR 系统通信过程中,除了 OOBL 对 PU 造成的干扰外,SSE 也会引发 SU 对 PU 的数据传输造成干扰。

2 干扰模型

2.1 数学表达式

第 k 个 SU 在子载波 n 上传输数据对第 l 个 PU 造成的干扰表示为:

$$I_{kn}^{l}=p_{kn}\psi_{n}^{l} \tag{1}$$

其中,p_{kn} 是 SU 在子载波 n 上的发送功率;ψ_{n}^{l} 是 SU 在子载波 n 上以单位功率进行数据传输时对 PU 造成的干扰,ψ_{n}^{l} 的表达式为[12]:

$$\psi_{n}^{l}=|g_{n}^{l}|^{2}\int_{d_l-B_l'/2}^{d_l+B_l'/2}\varphi_{n}(f)\,\mathrm{d}f \tag{2}$$

其中,g_{n}^{l} 是第 n 个子载波和第 l 个 PU 间的信道增

益;d_l 是第 l 个 PU 的中心频率;B_l 是第 l 个 PU 的带宽;$\varphi_n(f)$ 是第 n 个子载波的功率谱密度(Power Spectrum Density,PSD),可表示为:

$$\varphi_n(f)=\frac{T_s\,|h_n(f)|^2}{T} \tag{3}$$

其中,$-\frac{f_s}{2}+(n-1)\Delta f\leqslant f\leqslant\frac{f_s}{2}+(n-1)\Delta f$;$T_s$ 为采样间隔;$f_s=1/T_s$ 为采样频率;T 是第 n 个子载波上的脉冲成型滤波器 $h_n(m)$ 的长度;$h_n(f)$ 是第 n 个子载波上的脉冲成型滤波器 $h_n(m)$ 的频率响应,$h_n(f)$ 的表达式取决于 CR 系统采用的多载波技术类型。

如果 CR 系统采用 FBMC 多载波技术,原型滤波器可以表示为 $h(m)$,$m=0,1,\cdots,T-1$。其中,$T=MN$,M 为重叠因子,假设 $h(0)=0$,且 $h(m)$ 关于 $h(T/2)$ 偶对称,则[13]:

$$|h_n(f)|=\left|h\left(\frac{T}{2}\right)+2\sum_{r=1}^{T/2-1}h\left(\frac{T}{2}-r\right)\cdot\cos\left(\frac{2\pi r(f-(n-1)\Delta f)}{N\Delta f}\right)\right| \tag{4}$$

如果 CR 系统采用 OFDM 多载波技术,则原型滤波器 $h(m)$ 为矩形窗函数,此时,$T=N+C$。其中,N 为子载波的数目;C 为循环前缀的长度,那么:

$$|h_n(f)|^2=\left|T+2\sum_{r=1}^{T/2-1}(T-r)\cdot\cos\left(\frac{2\pi r(f-(n-1)\Delta f)}{N\Delta f}\right)\right| \tag{5}$$

2.2　考虑 SSE 的干扰模型

由系统模型部分的讨论可知,频谱感知过程中存在的 SSE 会引起 SU 对 PU 的干扰,基于此定义以下条件概率:

α_j:子载波 $j\in N_o$ 被 PU 占用(事件 O_j),频谱感知检测子载波 j 被 PU 占用(事件 $\tilde{O}_j$)的概率。使用贝叶斯公式和全概率公式,α_j 可以表示为

$$\begin{aligned}\alpha_j&=P\{O_j\mid\tilde{O}_j\}\\&=\frac{P\{\tilde{O}_j\mid O_j\}P\{O_j\}}{P\{\tilde{O}_j\mid O_j\}P\{O_j\}+P\{\tilde{O}_j\mid V_j\}P\{V_j\}}\\&=\frac{(1-Q_j^{md})Q_j^{pu}}{(1-Q_j^{md})Q_j^{pu}+Q_j^{fa}(1-Q_j^{pu})}\end{aligned} \tag{6}$$

事件 V_j 表示子载波 j 处于空闲状态,Q_j^{pu} 表示子载波 j 被 PU 占用的概率。

β_m:子载波 $m\in N_v$ 被 PU 占用,频谱感知子载波 m 处于空闲状态的概率。

$$\begin{aligned}\beta_m&=P\{O_m\mid\tilde{V}_m\}\\&=\frac{P\{\tilde{V}_m\mid O_m\}P\{O_m\}}{P\{\tilde{V}_m\mid O_m\}P\{O_m\}+P\{\tilde{V}_m\mid V_m\}P\{V_m\}}\\&=\frac{Q_m^{md}Q_m^{pu}}{Q_m^{md}Q_m^{pu}+(1-Q_m^{fa})(1-Q_m^{pu})}\end{aligned} \tag{7}$$

事件 $\tilde{V}_m$ 表示频谱感知确定子载波 m 处于空闲状态。

ω_n:子载波 $n\in N_v$ 处于空闲状态,频谱感知子载波 n 未被 PU 占用的概率为

$$\begin{aligned}\omega_n&=P\{V_n\mid\tilde{V}_n\}=1-\beta_n\\&=\frac{(1-Q_n^{fa})(1-Q_n^{pu})}{(1-Q_n^{fa})(1-Q_n^{pu})+Q_n^{md}Q_n^{pu}}\end{aligned} \tag{8}$$

条件概率 α_j 表征由于 OOBL 引起的干扰在子载波 j 上出现的可能性大小,β_m 表征由于 SSE 引起的干扰在子载波 m 上出现的可能性大小,ω_n 表征子载波 n 处于空闲状态的可能性大小。

由上述条件概率可得第 k 个 SU 在子载波 $n\in N_v$ 上传输数据,对第 l 个 PU 造成的干扰:

$$\begin{aligned}I_{kn}&=\sum_{j\in N_o}I_{kn}^{j,o}+\sum_{m\in N_v}I_{kn}^{m,v}\\&=p_{kn}\Big(\sum_{j\in N_o}\alpha_j\psi_n^j+\sum_{m\in N_v}\beta_m\psi_n^m\Big)\\&=p_{kn}\tilde{I}_n\end{aligned} \tag{9}$$

式(9)括号中的第 1 项表示由 OOBL 引起的对 PU 的干扰,第 2 项表示由 SSE 引起的对 PU 的干扰,I_{kn} 表示 SU 对 PU 造成的总干扰。

3　资源分配算法

由信息论香农公式可知,子载波 n 的传输速率可以表示为:

$$r_n=\Delta f_n\,\mathrm{lb}\left(1+\frac{p_n\,|h_n|^2}{\sigma_n^2}\right) \tag{10}$$

其中,r_n 表示传输速率;Δf_n 表示子载波带宽;p_n 表示发送功率;$\frac{|h_n|^2}{\sigma_n^2}$ 表示子载波的信噪比。

假设每个子信道都近似经历平衰落,CBS 完全获知 CR 系统中子载波的信道信息。资源分配问题表述如下:

$$R1:\ \max_{p_{kn},v_{kn}}\sum_{k=1}^{K}\sum_{n\in N_v}v_{kn}\omega_n\Delta f_n\,\mathrm{lb}\left(1+\frac{p_{kn}\,|h_n|^2}{\sigma_n^2}\right) \tag{11}$$

subject to:

$$\sum_{k=1}^{K}\sum_{n\in N_v}v_{kn}p_{kn}\leqslant P_t \tag{12}$$

$$\sum_{k=1}^{K}\sum_{n\in N_v}v_{kn}I_{kn}\leqslant I_{th} \tag{13}$$

$$\sum_{k=1}^{K}v_{kn}\leqslant 1,\ \forall\, n\in N_v \tag{14}$$

$$p_{kn}\geqslant 0,\ \forall\, n\in N_v,\ \forall\, k \tag{15}$$

$$v_{kn}\in\{0,1\},\ \forall\, n\in N_v,\ \forall\, k \tag{16}$$

问题 $R1$ 中的 v_{kn} 是子载波分配标识,假设子载波 n 被分配给用户 k,那么 $v_{kn}=1$,否则为 0。

式(14)确定每个子载波只能被分配给一个用户,式(12)为 CR 系统总功率约束条件,式(13)为 PU 干扰门限约束条件,PU 根据自身容忍干扰能力设置干扰门限,SU 对 PU 造成的干扰需在干扰门限之下。问题 $R1$ 的目标是实现 CR 系统吞吐量最大化,$R1$ 的求解复杂度随着输入数据的增加呈指数增长,将此问题分步求解:首先进行子载波的分配,其次进行功率分配。这将大大减小求解复杂度。

按照最大信道增益原则把子载波分配给各 SU。完成子载波分配后,给每个子载波分配功率。SU 对 PU 的干扰大部分是由临近 PU 的子载波引起的,基于此,假设对每个 PU 的干扰只源于距离 PU 最近的子载波。则问题 $R1$ 可以表示为:

$$R2:\max_{p_n}\sum_{n\in N_v}\omega_n\Delta f_n\mathrm{lb}\left(1+\frac{p_n|h_n|^2}{\sigma_n^2}\right) \tag{17}$$

subject to:

$$\sum_{n=1}^{N}p_n\leqslant P_t,\ \forall\, n\in N_v \tag{18}$$

$$\sum_{n=1}^{N}p_n\tilde{I_n}\leqslant I_{th},\ \forall\, n\in N_v \tag{19}$$

$$p_n\geqslant 0\ ,\ \forall\, n\in N_v \tag{20}$$

利用拉格朗日乘子法可以得到 $R2$ 的解为:

$$p_n=\left[\frac{\omega_n}{a\tilde{I_n}+b}-\frac{\sigma_n^2}{h_n^2}\right]^+ \tag{21}$$

其中,$[x]^+=\max(0,x)$。式(21)中的 a,b 分别表示式(18)、式(19)的拉格朗日乘子。$R2$ 的求解复杂度仍较高,继续分解此问题,首先满足干扰约束条件式(19),忽略 $R2$ 中的总功率约束条件式(18),求解可得:

$$p'_n=\left[\frac{\omega_n}{a\tilde{I_n}}-\frac{\sigma_n^2}{h_n^2}\right]^+ \tag{22}$$

式(22)保证了 SU 对 PU 造成的干扰满足条件式(19),即对每个子载波分配的功率不能超过 p'_n,也即每个子载波所能获得的最大功率 $p_n^{\max}=p'_n$,同时还要保证所有子载波的功率之和不超过总功率约束式(18),满足干扰约束条件的总功率约束问题可以表述为:

$$R3:\max_{p_n}\sum_{n\in N_v}\omega_n\Delta f_n\mathrm{lb}\left(1+\frac{p_n^f|h_n|^2}{\sigma_n^2}\right) \tag{23}$$

subject to:

$$\sum_{n=1}^{N}p_n^f\leqslant P_t,\ \forall\, n\in N_v \tag{24}$$

$$0\leqslant p_n^f\leqslant p_n^{\max},\ \forall\, n\in N_v \tag{25}$$

优化问题 $R1,R2,R3$ 的目标函数中都含有权重因子 ω_n,$R3$ 的解 p_n^f 满足 PU 的干扰约束条件,且所有子载波的 p_n^f 之和也满足总功率约束,在进行子载波功率分配时,需要按照每个子载波的权重因子进行分配。使用几何注水法[14]求解问题 $R3$,得到分配给 SU 的子载波的最终功率,进而使 CR 系统的吞吐量最大化。

4 仿真及分析

使用 Matlab7.8.0 软件对本文的资源分配算法进行仿真。在仿真参数设置上,使用 2 个 PU,3 个 SU,Q_{md},Q_{fa},Q_{pu} 分别在区间[0.01,0.05],[0.05,0.01],[0,1]上服从均匀分布,PU 干扰门限 $I_{th}^1=I_{th}^2=I_{th}$,具体的参数设置如表 1 所示。仿真中使用的滤波器组原型函数是欧洲 PHYDYAS 项目组设计的原型滤波器[15],重叠因子为 4,并与 OFDM 系统做比较分析。

表 1 仿真参数

仿真参数	参数值
主用户数	1
认知用户数	3
子载波数	32
子载波带宽/MHz	0.312 5
信道增益	均值为 1 的瑞利随机变量
AWGN 方差	10^{-6}

图 3 给出了不同干扰门限值下 SU 对 PU 造成的干扰,CR 系统总功率为 1 W。从图中可以看出,在 FBMC 与 OFDM 系统中,SU 对 PU 造成的干扰始终处于 PU 的干扰门限之下,即满足优化问题 $R1$ ~ $R3$ 中的干扰约束条件,保证了 SU 在接入空闲载波的时刻 PU 的正常通信不受影响。随着 PU 干扰门限的增大,考虑 SSE 的资源分配算法对 PU 的干扰小于未考虑 SSE 的资源分配算法的干扰,且 FBMC 系统中 SU 对 PU 的干扰明显小于 OFDM 系统中 SU 对 PU 的干扰。

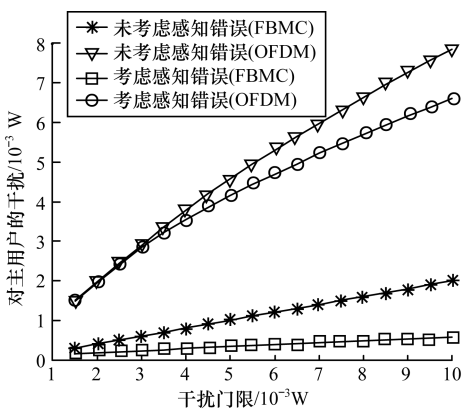

图 3 不同干扰门限下 SU 对 PU 的干扰

图 4 给出了不同干扰门限值条件下,CR 系统吞吐量的仿真图,仿真中 CR 系统总功率为 1 W。从图中可以看到,本文算法与未考虑 SSE 的算法相比,OFDM 系统吞吐量提高约 3 Mb/s,FBMC 系统吞吐量提高约 1 Mb/s,其中考虑 SSE 的 FBMC 系统比未考虑 SSE 的 OFDM 系统吞吐量高出 4 Mb/s ~ 16 Mb/s。

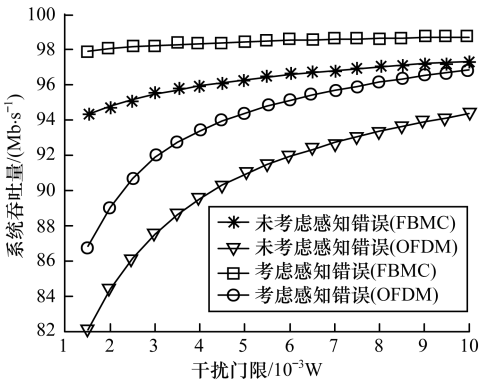

图 4　不同干扰门限下 CR 系统的吞吐量

在 FBMC 和 OFDM 系统中,考虑 SSE 的资源分配算法的吞吐量均高于未考虑 SSE 的资源分配算法的吞吐量,且采用本文算法的 FBMC 系统的吞吐量是最大的,其吞吐量曲线增长较慢。这是因为 FBMC 的旁瓣小,带外泄露比 OFDM 小很多,加之考虑 SSE 引起的干扰比未考虑 SSE 引起的干扰小,所以采用本文算法的 FBMC 引起的干扰最小,分配给每个子载波的功率接近于最大值,曲线增长较慢,图 3中的干扰曲线和图 4 中的吞吐量曲线验证了此结论。其他 3 个 CR 系统的吞吐量,随着干扰门限的增大,每个系统的子载波获得的功率相应增加,吞吐量曲线都相应增大。但 OFDM 系统的吞吐量始终小于 FBMC 系统的吞吐量,且未考虑 SSE 算法的 OFDM 系统的吞吐量最小。

图 5 是不同的系统总功率约束条件下,CR 系统的吞吐量,仿真中干扰门限设定为 0.01 W。从图中可以看出,FBMC 系统吞吐量提高约 2 Mb/s ~ 3 Mb/s,OFDM 系统吞吐量提高约 4 Mb/s,且 FBMC 系统的吞吐量高于 OFDM 的吞吐量。OFDM 系统的吞吐量在总功率门限 5 W 后基本不再增加,这是因为 OFDM 系统中 SU 对 PU 的干扰已经接近干扰门限,即便增大总功率,系统的吞吐量也无多大改善,而 FBMC 系统的吞吐量则随着总功率的增大而增大,这也验证了 FBMC 系统中 SU 对 PU 的干扰更小,FBMC 多载波技术相较于 OFDM 更适用于 CR 网络。

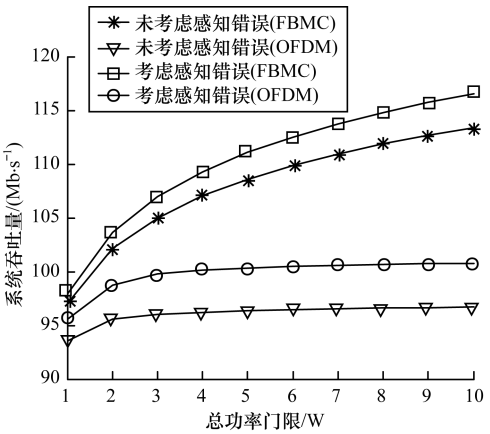

图 5　不同总功率门限下 CR 系统的吞吐量

5　结束语

本文从多载波技术在 CR 网络中的资源分配问题出发,考虑了资源分配中的干扰来源,提出考虑频谱感知错误的 CR 资源分配算法,并基于 FBMC 和 OFDM 系统进行实验仿真。结果表明,该算法对 PU 造成的干扰更小,认知系统可以获得更大的吞吐量,FBMC 在干扰和吞吐量方面的性能均优于 OFDM,相较于 OFDM,FBMC 在认知无线电资源分配问题上更具优势,下一步将深入研究 FBMC 在 5G 中的应用。

参考文献

[1] Slam M H,Koh C L,Oh S W,et al. Spectrum Survey in Singapore:Occupancy Measurements and Analyses[C]// Proceedings of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications. Washington D. C., USA: IEEE Press, 2008: 1-7.

[2] Mitola J, Maguire G Q. Cognitive Radio: Making Software Radios More Personal[J]. IEEE Personal Communications,1999,6(4):13-18.

[3] 佟学检,罗　涛. OFDM 移动通信技术原理与应用[M]. 北京:人民邮电出版社,2003.

[4] Farhang-Boroujeny B. OFDM Versus Filter Bank Multicarrier[J]. IEEE Signal Processing Magazine, 2011, 28(3):92-112.

[5] 王光宇. 多速率数字信号处理和滤波器组理论[M]. 北京:科学出版社,2013.

[6] Andrews J G,Buzzi S,Choi W,et al. What Will 5G be[J]. IEEE Journal on Selected Areas in Communications,2014, 32(6):1065-1082.

[7] Schellmann M,Zhao Zhao,Lin Hao,et al. FBMC-based Air Interface for 5G Mobile: Challenges and Proposed Solutions[C]//Proceedings of the 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications. Washington D.C., USA: IEEE Press,2014:102-107.

(下转第 182 页)

6 结束语

基于云存储中密钥追踪问题,本文结合外包解密和白盒追踪属性加密方案,提出一种安全、高效、可追踪和监控的属性加密方案。通过安全分析和实验验证,该方案数据拥有者端的追踪性能明显得到提高,有助于解决资源受限用户追踪的性能瓶颈,能满足云存储中密钥管理安全、高效、可追踪的要求。由于方案涉及的算法步骤较多,因此,后期需要对实际应用场景下密钥管理的高效性进行研究。

参考文献

[1] Chu C K, Chow S S M, Tzeng W G, et al. Key-aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.

[2] 杨小东,王彩芬. 基于属性群的云存储密文访问控制方案[J]. 计算机工程, 2012, 38(11): 20-22, 26.

[3] Sahai A, Waters B. Fuzzy Identity-based Encryption[C]//Proceedings of Cryptology-EUROCRYPT' 05. Berlin, Germany: Springer, 2005: 457-473.

[4] Goyal V, Pandey O, Sahai A, et al. Attribute-based Encryption for Fine-grained Access Control of Encrypted Data[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2006: 89-98.

[5] Bethencourt J, Sahai A, Waters B. Ciphertext-policy Attribute-based Encryption[C]//Proceedings of 2007 IEEE Symposium on Security and Privacy. Piscataway, USA: IEEE Press, 2007: 321-334.

[6] 邓宇乔. 基于动态属性的加密方案[J]. 计算机工程, 2014, 40(4): 136-140.

[7] 解 理,任艳丽. 隐藏访问结构的高效基于属性加密方案[J]. 西安电子科技大学学报, 2015, 42(3): 97-102.

[8] Green M, Hohenberger S, Waters B. Outsourcing the Decryption of ABE Ciphertexts[C]//Proceedings of the 20th USENIX Security Symposium. Sanfrancisco, USA: USENIX Association Press, 2011: 1-16.

[9] Lai Junzuo, Robert D H, Guan Chaowen, et al. Attribute-based Encryption with Verifiable Outsourced Decryption[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(8): 1343-1354.

[10] Qin Baodong, Deng Robert H, Liu Shengli, et al. Attribute-based Encryption with Efficient Verifiable Outsourced Decryption[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(7): 1384-1393.

[11] Rouselakis Y, Waters B. Practical Constructions and New Proof Methods for Large Universe Attribute-based Encryption[C]//Proceedings of ACM SIGSAC Conference on Computer & Communications Security. New York, USA: ACM Press, 2013: 463-474.

[12] Li Jin, Huang Qiong, Chen Xiaofeng, et al. Multi-authority Ciphertext-policy Attribute-based Encryption with Accountability[C]//Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. New York, USA: ACM Press, 2011: 386-390.

[13] Ning Jianting, Dong Xiaolei, Cao Zhenfu, et al. White-box Traceable Ciphertext-policy Attribute-based Encryption Supporting Flexible Attributes[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(6): 1274-1288.

[14] Beimel A. Secure Schemes for Secret Sharing and Key Distribution[D]. Haifa, Isral: Israel Institute of Technology, 1996.

[15] Wang Zhiwei, Chen Feng, Xia Aidong. Attribute-based Online/Offline Encryption in Smart Grid[C]//Proceedings of the 24th International Conference on Computer Communication and Networks. Washington D. C., USA: IEEE Press, 2015: 1-5.

[16] Fan Chun, Vincent S M, Ruan Heming. Arbitrary-state Attribute-based Encryption with Dynamic Membership[J]. IEEE Transactions on Computers, 2014, 63(8): 1951-1961.

[17] 张 宇,陈 晶,杜瑞颖,等. 一个适用于云计算环境的高效属性加密方案[J]. 武汉大学学报(理学版), 2015, 61(4): 375-383.

[18] 彭开锋,张 席. 适应性安全且支持属性撤销的 CP-ABE 方案[J]. 计算机工程, 2015, 41(4): 151-155.

编辑 刘 冰

(上接第 175 页)

[8] 卢云波,唐 亮,郝李欣,等. 多用户认知无线电 OFDM 系统的资源分配算法[J]. 计算机工程, 2015, 41(7): 111-114, 119.

[9] Zhang Yonghong, Leng C. Resource Allocation in an OFDM-based Cognitive Radio System[J]. IEEE Transactions on Communications, 2009, 57(7): 1928-1931.

[10] 赵知劲,赖海超,尚俊娜. 基于 QoS 需求的认知无线电资源分配算法[J]. 计算机工程, 2013, 39(2): 85-89.

[11] Zhuang Ling, Liu Lu, Shao Kai, et al. Efficient Resource Allocation Algorithm with Rate Requirement Consideration in Multicarrier-based Cognitive Radio Networks[J]. Journal of Communications, 2015, 10(1): 16-23.

[12] Weiss T, Hillenbrand J, Krohn A, et al. Mutual Interference in OFDM-based Spectrum Pooling Systems[C]//Proceedings of the 59th Vehicular Technology Conference. Washington D. C., USA: IEEE Press, 2004: 1873-1877.

[13] Baltar L G, Waldhauser D S, Nossek J A. Multi-carrier Spread Spectrum[M]. Berlin, Germany: Springer, 2007.

[14] He P, Zhao Lian, Zhou Sheng, et al. Water-filling: A Geometric Approach and Its Application to Solve Generalized Radio Resource Allocation Problems[J]. IEEE Transactions on Wireless Communications, 2013, 12(7): 3637-3647.

[15] Bellanger M, LeRuyet D, Roviras D, et al. FBMC Physical Layer: A Primer[EB/OL]. (2010-05-27). http://www.ict-phydyas.org/teamspace/internal-folder/FBMC-Primer_06-2010.pdf.

编辑 顾逸斐