动态频谱管理中频谱机会发现与授权用户保护的折中优化研究

田家强[1,2] 陈 勇[2] 张建照[2]
(中国人民解放军理工大学通信工程学院 南京 210007)[1] (南京电讯技术研究所 南京 210007)[2]

摘 要 在基于认知无线电的动态频谱管理中,频谱感知需要发现更多的频谱机会,同时尽量减少对授权用户的干扰。文中研究了能量感知中这两个性能指标的折中优化问题,建立了以两个指标的加权作为优化目标函数、感知时间和感知门限作为优化变量的联合优化模型,并证明了该问题属于双凹优化问题。提出了基于迭代凸优化搜索的优化算法,该算法在不依赖预置感知门限或感知时间的情况下,能够快速获得近似最优解。仿真表明,相比于单参数优化方法,所提联合优化算法的性能平均提高了32%和85.9%。

关键词 能量感知,感知时间,感知门限,联合优化,双凸优化
中图法分类号 TN929.5 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.03.016

Tradeoff Optimization of Spectrum Opportunity Discovery and Licensed User Protection in Dynamic Spectrum Management

TIAN Jia-qiang[1,2] CHEN Yong[2] ZHANG Jian-zhao[2]
(Institute of Communications Engineering, PLA University of Science & Technology, Nanjing 210007, China)[1]
(Nanjing Telecommunication Technology Institute, Nanjing 210007, China)[2]

Abstract In dynamic spectrum management based on cognitive radio, spectrum sensing is desired to explore more spectrum opportunity while incurring less interference to licensed users. This paper investigated the tradeoff optimization of the two performance metrics, and constructed a joint optimization model in which the weighted sum of two metrics is regarded as objective function, and sensing duration and sensing threshold are regarded as variables. This problem is proved to be in the form of biconcave optimization problem (BOP). An optimization algorithm based on alternative convex search was proposed, which can quickly find the near optimal solutions without relying on the predefined sensing parameters. Simulation results demonstrate that the joint parameters optimization scheme generates 32.0% and 85.9% promotion over single parameter optimization schemes on average.

Keywords Energy sensing, Sensing duration, Sensing threshold, Joint optimization, Biconvex optimization

基于认知无线电的动态频谱管理被认为是无线通信中解决频谱稀缺和已分配频谱未充分利用共存问题的有效方法[1]。在认知无线网络中,频谱机会的获取是认知无线网络的前提条件和关键步骤,次级用户在对授权主用户不产生极大干扰的情况下寻求短暂的频谱机会来进行通信。与其他可用的方法如频谱数据库和频谱预测相比,频谱感知是获取频谱机会最基本和最普遍的方法。目前已被提出的频谱感知方法包括能量感知、匹配滤波器检测和特征检测等[2]。基于显著的低复杂度和对目标信号特征无要求的特点,能量感知成为目前应用得最为广泛的频谱感知技术[3]。

频谱感知的两个常用性能指标是检测概率和虚警概率。更高的检测概率意味着对主用户更多的保护,同时在一个较低的虚警概率下可获取更多的频谱机会。给定一个具有采样能力的能量检测器,频谱感知的性能大部分取决于感知门限和感知时间的设定。因此,能量检测的研究集中于感知门限和/或感知时间,以最优化检测概率和/或虚警概率。感知门限是能量检测器的最大相关参数。文献[4]通过获得不同主用户占用概率下的自适应感知门限来最小化检测错误概率。文献[5]在相同的目标下获得超瑞利衰落信道的闭式最优感知门限。给定一个由检测概率或虚警概率约束得出的感知门限,感知时间的确定便是认知无线网络性能的关键。文献[6]在检测概率的约束下,得出了最大化吞吐量的最优感知时间。对于感知能量消耗和次用户吞吐量的折中,文献[7]对频谱感知做了最优化设计。由于单个参数的设定问题通常是凸的,因此联合优化感知门限和感知时间的最优化问题更可取且更具有挑战性,因为它具有非凸性。对于多时隙感知问题,以最小化感知时间和最大化吞吐量为目标,文献[8]提出了一种联合感知门限和感知时间的最优化方案。

到稿日期:2016-12-20 返修日期:2017-02-14 本文受国家自然科学基金(61301161,61471395),江苏省自然科学基金(BK20141070,20161125)资助。

田家强(1991-),男,硕士生,主要研究方向为动态频谱管理,E-mail:491812048@qq.com;**陈 勇**(1975-),男,硕士,研究员,主要研究方向为电磁频谱技术、通信抗干扰技术等,E-mail:chy63s@126.com(通信作者);**张建照**(1985-),男,博士,工程师,主要研究方向为电磁频谱技术等。

本文主要研究单时隙能量感知中的频谱机会利用和主用户保护的折中问题，其中前者利用成功获取的频谱机会长度来评估，后者利用对主用户的干扰来衡量。将两个指标的加权和作为效用函数，同时通过优化感知门限和感知时间来最大化效用函数。本文证明了这是一个双凹优化问题并且提出了一种联合选择算法来获得最优参数。虽然在不改变算法复杂度的前提下，很容易获得联合检测概率和虚警概率限制，但是提出的方案本身不依赖于约束来确定参数。另外，通过改变频谱机会利用和主用户保护的性能权重来获得最优的参数设计是比较容易实现的。

1　系统模型

1.1　系统架构

对于单信道接入条件下一个次用户在传输之前进行感知的情况，其对应的时隙结构如图 1 所示。次用户在传输之前执行感知以判断信道中是否有主用户存在，这种情况是由每一时隙开端处的主用户决定且在整个时隙中保持不变[9]。假定对于一个单位长度的时隙，感知时间表示为 $\rho\in(0,\rho_{\max})$。$\rho_{\max}\in(0,1)$是感知时间的上界，因为如果感知之后的剩余时间不能被利用，则过长时间的频谱感知将毫无意义。感知过程之后，如果信道感知结果为空闲，则一个次用户将会接入进行传输，否则在剩余的 $1-\rho$ 时隙里它将保持静默以避免对主用户产生干扰。假定次用户具有较好的干扰识别能力，当感知到主用户重新进入信道时，它能够在短时间内空出占用的信道并在剩余的时隙里保持空闲，因此在一个时隙内其不会对主用户产生多次干扰。

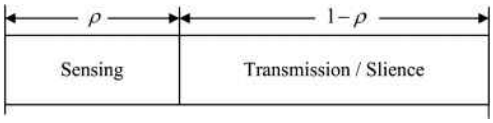

图 1　时隙结构

Fig. 1　Time-slot structure

1.2　能量检测器

假定次用户采用能量检测器来进行频谱感知。感知决策为一个二元假设检验，观测到的信号可表示为：

$$y(n)=\begin{cases}w(n), & H_0\\ s(n)+w(n), & H_1\end{cases} \tag{1}$$

其中，H_0 和 H_1 分别代表主用户不存在和存在时的假设，$w(n)$表示均值为 0、方差为 σ_n^2 的加性高斯独立同分布随机噪声，$s(n)$表示均值为 0、方差为 σ_s^2 的独立同分布随机过程的主用户信号。给定样本数为 N，检验的统计数据为：

$$Y=\frac{1}{N}\sum_{n=1}^{N}|y(n)|^2 \tag{2}$$

如果 N 足够大，那么检测概率 P_d 可近似表示为：

$$P_d=P(Y>\lambda|H_1)=Q\left(\frac{\lambda-\sigma_n^2(1+\gamma)}{\sigma_n^2(1+\gamma)/\sqrt{f_s\rho/2}}\right) \tag{3}$$

虚警概率 P_f 可近似表示为：

$$P_f=P(Y>\lambda|H_0)=Q\left(\frac{\lambda-\sigma_n^2}{\sigma_n^2/\sqrt{f_s\rho/2}}\right) \tag{4}$$

其中，λ 为感知门限，ρ 为感知时间，f_s 为样本速率，$\gamma=\frac{\sigma_s^2}{\sigma_n^2}$ 为信噪比(SNR)，且 Q 函数 $Q(\cdot)$可表示为：

$$Q(x)=\frac{1}{\sqrt{2\pi}}\int_x^{\infty}e^{-t^2/2}\,dt \tag{5}$$

在实际的感知设计中，P_d 越大，对主用户的保护就越好；P_f 越小，就能获取越多可用的频谱机会。

1.3　性能指标

由于只考虑单时隙感知，因此感知的最优化问题与频谱机会利用和对主用户的保护均相关。从 1.1 节介绍的网络模型很容易得出，对主用户的干扰最多只有一次。由于频谱具有灵活性的特点，因此对主用户的不利影响可用干扰概率(Interference Ratio，IR)来量化，表示为：

$$P_{IR}=1-P_d=1-Q\left(\frac{\lambda-(\sigma_n^2+\sigma_s^2)}{(\sigma_n^2+\sigma_s^2)/\sqrt{f_s\rho/2}}\right) \tag{6}$$

对于频谱机会利用，需要寻求更小的虚警概率 P_f 来减少频谱机会的丢失。然而从式(4)可推断 P_f 由感知时间部分 ρ 决定，要获得更小的 P_f，可通过增大 ρ 同时减小可用传输时间来实现。制定一个对策，实际的频谱机会利用可表示为：

$$A_u=(1-P_f)(1-\rho)=\left(1-Q\left(\frac{\lambda-\sigma_n^2}{\sigma_n^2/\sqrt{f_s\rho/2}}\right)\right)(1-\rho) \tag{7}$$

2　联合优化算法的设计

2.1　效用函数与问题的形成

为充分利用频谱机会，且对主用户造成较少的干扰，P_{IR} 较小和 A_u 较大的感知决策更为可取。为解决这个双目标最优化问题，引入一个系数 $\theta(\theta>0)$，构建效用函数为：

$$\begin{aligned}u(\lambda,\rho)&=A_u-\theta P_{IR}\\&=\left(1-Q\left(\frac{\lambda-\sigma_n^2}{\sigma_n^2/\sqrt{f_s\rho/2}}\right)\right)(1-\rho)-\\&\quad\theta\left(1-Q\left(\frac{\lambda-\sigma_n^2(1+\gamma)}{\sigma_n^2(1+\gamma)/\sqrt{f_s\rho/2}}\right)\right)\end{aligned} \tag{8}$$

其中，σ_n^2，γ 和 f_s 是给定的反映感知环境和次用户感知能力的参数，λ 和 ρ 为变量。很显然，增大 $u(\lambda,\rho)$等同于增大 A_u 且减小 P_{IR}，然而这两个指标的偏好取决于参数 θ。

根据此效用函数，联合感知门限和感知时间的最优化问题可表示为：

$$\begin{aligned}&\max_{\lambda,\rho}\ u(\lambda,\rho)\\&\text{subject to (6),(7),(8)}\\&\sigma_n^2>0,\gamma>0,f_s>0,\lambda>0,\rho\in(0,\rho_{\max})\end{aligned} \tag{9}$$

很容易看出问题(9)是一个非凹问题。下一节中将会介绍如果可用的变量空间定义为 $\lambda\in(\sigma_n^2,\sigma_n^2(1+\gamma))$，那它就可以转化为一个双凹优化问题，这在能量检测器的设计中是一个合理且常用的假设。事实上，从式(3)－式(5)可得问题(9)的解将会导致 $P_d\leqslant 0.5$ 或 $P_f\geqslant 0.5$ 而不满足$(\sigma_n^2,\sigma_n^2(1+\gamma))$的约束，这在频谱感知设计中是多余的。

2.2　问题的双凹性

由于双凹优化问题可被有效解决，因此如果能够证明一个问题是双凹的形式，那么就可以研究相应的有效算法。在证明之前，首先引入双凸集合和双凹函数的定义[10]。

定义 1　令 $X\subseteq R^n$，$Y\subseteq R^m$，如果对于 $\forall x\in X$，$B_x=\{y\in Y|(x,y)\in B\}$为凸且 $\forall y\in Y$，$B_y=\{x\in X|(x,y)\in B\}$也为凸，则可称集合 $B\subseteq X\times Y$ 为 $X\times Y$ 上的一个双凸集合，简称双凸。

定义 2 如果对于 $\forall y\in Y, f_x:B_y\to R$ 是一个凹函数且 $\forall x\in X, f_y:B_x\to R$ 也是一个凹函数，则可称双凸集合 B 上的 $f(x,y):B\to R$ 为一个双凹函数。

定义 3 如果 B 是一个双凸集合，f 是一个双凹函数，则 $\max\{f(x,y):B\to R\}$ 是一个双凹优化问题(Biconcave Optimization Problem，BOP)。

一般来说，尽管双凹优化问题仍然是非凹的，但其在变量的双凸结构和双凹目标函数的利用方面比一般的非凹问题更高效。应用于解决双凹优化问题的大量有效算法已被提出且其有效性在应用中得到了证明。下一节中将证明问题(9)是一个双凹优化问题的形式且服从合理的 λ 约束，并提出一种联合优化算法。

定理 1 问题(9)是一个服从附加约束 $\lambda\in(\sigma_n^2,\sigma_n^2(1+\gamma))$ 的双凹优化问题。

显然，候选解集 $\Omega=\{(\lambda,\rho)\mid\lambda\in(\sigma_n^2,\sigma_n^2(1+\gamma)),\rho\in(0,\rho_{\max})\}$ 是双凸的，因此仅需要通过证明 Ω 中 $u(\lambda,\rho)$ 的双凹性来证明定理 1。

引理 1 令 $\Omega_\lambda=\{\lambda\mid(\lambda,\rho)\in\Omega\}$，那么 $u_\lambda:\Omega_\lambda\to R$ 是一个凹函数。

证明：对于任意给定的 $\rho\in(0,\rho_{\max})$，函数 u_λ 的导数为：

$$u_\lambda'=\frac{\sqrt{f_s\rho}}{2\sqrt{\pi}\sigma_n^2}(1-\rho)\exp\left(-\frac{1}{2}\left(\frac{\lambda-\sigma_n^2}{\sqrt{2}\sigma_n^2}\sqrt{f_s\rho}\right)^2\right)-\theta\frac{\sqrt{f_s\rho}}{2\sqrt{\pi}\sigma_n^2(1+\gamma)}\exp\left(-\frac{1}{2}\left(\frac{\lambda-\sigma_n^2(1+\gamma)}{2\sqrt{\pi}\sigma_n^2(1+\gamma)}\sqrt{f_s\rho}\right)^2\right)\tag{10}$$

给定 $Q(x)$，对于 $x>0$ 单调递减和约束 $\lambda\in(\sigma_n^2,\sigma_n^2(1+\gamma))$，从式(10)很容易得出公式中的第一项和第二项(包括负号)随 λ 的增加而递减，u_λ' 是关于 λ 的单调减函数。因为 $u_\lambda''<0$，所以 u_λ' 是一个凹函数。

引理 2 令 $\Omega_\rho=\{\rho\mid(\lambda,\rho)\in\Omega\}$，那么 $u_\rho:\Omega_\rho\to R$ 是一个凹函数。

引理 2 的证明方法与引理 1 相似。

联合引理 1、引理 2 和 Ω 的双凸性，应用定义 3 可证明定理 1。

2.3 最优联合优化算法

既然已经证明服从附加约束 λ 的联合优化问题是双凹的，那么就可利用解决双凹优化问题的已有算法来获得最优解。本文基于常用于解决双凹优化问题的可替代凸搜索算法提出一种联合优化方案[11]，并将其简称为 JOACS。算法代码见算法 1，详细步骤如下。

算法的输入包括最大循环周期 $c_{\max}$、权重参数 θ，以及感知环境和能力参数 σ_n^2，γ 和 f_s。λ 和 ρ 的初始值是从它们的值域中随机选择的。尽管增大初始值可能会加快算法的收敛速度，但下一节介绍的仿真结果表明，在赋予随机初始值的几个循环周期内，算法仍然收敛。初始化之后，通过解决问题 $\arg\max_\lambda\{u_\lambda=u(\lambda,\rho_i),\lambda\in\Omega_\lambda\}$ 和 $\arg\max_\rho\{u_\rho=u(\lambda_{i+1},\rho),\rho\in\Omega_\rho\}$ 来对 λ 和 ρ 进行相互更新，这样可有效辨别算法的凹特性[12]。如果达到最大周期或连续 3 组解保持不变，则算法终止。JOACS 的最优解很容易通过文献[10]中的定理 4.9 得到证明。

算法 1 JOACS

输入：$\sigma_n^2,\gamma,f_s,\theta$，最大循环周期 $c_{\max}$

输出：λ^*,ρ^*

初始化：从 $(\sigma_n^2,\sigma_n^2(1+\gamma))$ 和 $\rho\in(0,\rho_{\max})$ 中随机选择 λ_0 和 ρ_0。

```
While 1
  λ_{i+1}=arg max_λ{u_λ=u(λ,ρ_i),λ∈Ω_λ};
  ρ_{i+1}=arg max_ρ{u_ρ=u(λ_{i+1},ρ),ρ∈Ω_ρ};
  λ_{i+2}=arg max_λ{u_λ=u(λ,ρ_{i+1}),λ∈Ω_λ};
  ρ_{i+2}=arg max_ρ{u_ρ=u(λ_{i+2},ρ),ρ∈Ω_ρ};
  if ((λ_i==λ_{i+1}==λ_{i+2})&(ρ_i==ρ_{i+1}==ρ_{i+2})|(i+2≥c_max))
    λ*=λ_{i+2},ρ*=ρ_{i+2};
    break;
  else
    i=i+1;
  end
end
```

该算法在 20 个周期以内就能收敛，对不同的输入参数获得的最优感知门限和时间如图 2 和图 3 所示。

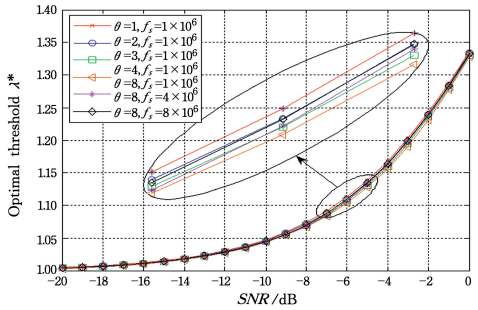

图 2 λ^* 与 SNR 的关系

Fig. 2 Relationship between λ^* and SNR

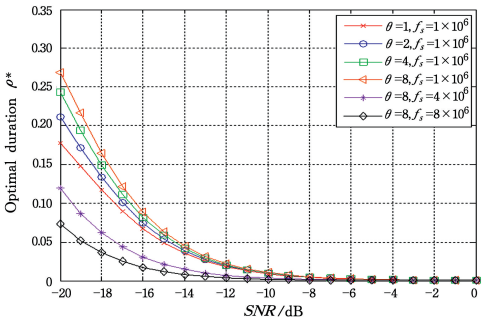

图 3 ρ^* 与 SNR 的关系

Fig. 3 Relationship between ρ^* and SNR

从图 2 中可观察出，最优感知门限 λ^* 随信噪比 SNR 的增加而递增。另外，$\gamma=-6$dB 附近的放大部分表明增大 θ 导致 λ^* 减小；同时，θ 相同时，增大 f_s 也会使 λ^* 增大。另一方面，图 3 表明，最优感知时间 ρ^* 随信噪比的增加而递减，θ 和 γ 对 ρ^* 的影响与对 λ^* 的影响相反。

本文在问题建模和算法方面均没有涉及指标门限。然而，从式(5)－式(7)和引理 1 的证明中可得增加给定门限 $P_d^*\geqslant 0.5$ 和/或 $P_f^*\leqslant 0.5$ 并不能改变问题的双凹性，且 JOACS 的复杂度保持不变。

3　仿真结果与分析

3.1　仿真步骤与指标

将提出的联合优化算法 JOACS 与两种单参数优化感知算法（分别记为 Opt ρ 和 Opt λ）作比较。Opt ρ 表示感知门限 λ 为随机，最优化感知时间 ρ 的感知算法；Opt λ 表示感知时间 ρ 为随机，最优化感知门限 λ 的感知算法。对于这 3 种算法，均将噪声功率和最大感知门限设置为 $\sigma_n^2=1$ 和 $\rho_{\max}=0.95$。主用户为相位调制（2PSK）信号，带宽分别为 5kHz，2MHz 和 4MHz，感知算法的样本速率设置为主用户信号带宽的两倍。对每一种情形，通过最优化感知参数进行蒙特卡洛仿真，来观察效用函数 $u(\lambda,\rho)$、实际频谱机会利用 A_u 和干扰概率 P_{IR} 的性能。

3.2　仿真结果

首先，比较 3 种算法的效用函数 $u(\lambda,\rho)$，仿真结果如图 4 所示。

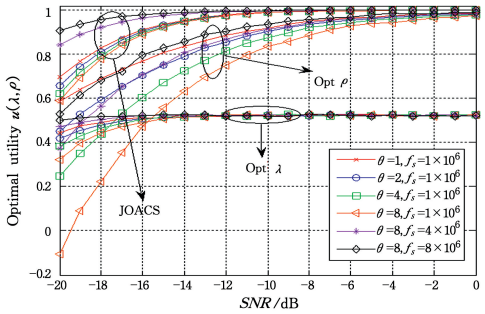

图 4　效用函数 $u(\lambda,\rho)$ 的比较

Fig. 4　Comparison of utility function $u(\lambda,\rho)$

从图 4 中可看出，3 种算法的效用函数 $u(\lambda,\rho)$ 均随信噪比 γ 的增大而增大，并且即使是在较低的信噪比环境下，JOACS 算法的性能也明显比 Opt ρ 和 Opt λ 好。另外，JOACS 和 Opt ρ 算法的 $u(\lambda,\rho)$ 增加明显，而 Opt λ 算法的 $u(\lambda,\rho)$ 一直位于 0.5 左右，这表明通过改变感知时间来提高能量检测器的性能更为有效。数值上，JOACS 的 $u(\lambda,\rho)$ 分别比 Opt ρ 和 Opt λ 的 $u(\lambda,\rho)$ 平均高出 32.0% 和 85.9%，说明联合优化算法的性能有了显著提高。JOACS 具体提高的比率与参数 θ 和 f_s 有关。

然后，令 $\theta=1$，$f_s=1\times10^6$ 作为一个样本来评估算法中 A_u 和 P_{IR} 的仿真和理论结果。图 5 和图 6 表明，理论结果与相应的仿真结果非常接近。

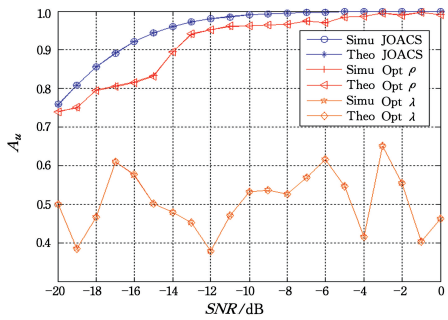

图 5　频谱机会利用 A_u 的比较

Fig. 5　Comparison of spectrum opportunity's exploitation A_u

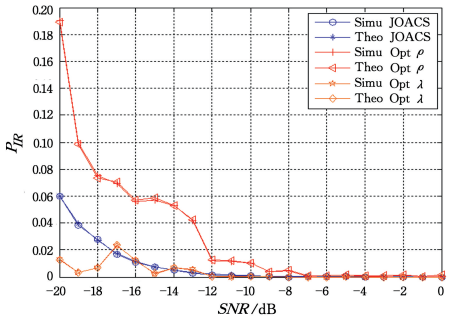

图 6　干扰概率 P_{IR} 的比较

Fig. 6　Comparison of interference probability P_{IR}

从图 5 中可看出，JOACS 的频谱机会利用 A_u 总是大于其他两种算法，且 JOACS 可成功获取 95% 的频谱信息，而 Opt ρ 和 Opt λ 分别可获取 91% 和 51% 的频谱信息。图 5 中 Opt λ 算法的结果因为参数 ρ 的随机性而发生波动。同时，JOACS 与 Opt ρ 相比，A_u 仅有很小的提高；但从图 6 中可以看出，Opt ρ 算法的高 A_u 是建立在高 P_{IR} 的基础上的。另外，JOACS 的 P_{IR} 一直小于 0.06，已相当小且符合 IEEE802.22 标准的一般引用要求。

结束语　本文讨论了能量检测器中频谱机会获取和主用户保护两个问题的折中优化，提出加权和效用函数，建立联合感知时间和门限的最优化模型并证明其是一个双凹优化问题，进而提出一种联合优化算法 JOACS。仿真结果证明，所提算法的性能比单参数优化算法的性能优越；另外，两个指标之间的设计偏好可通过权重的选择很好地实现。下一步，将研究其他典型频谱感知算法中两个指标的折中优化问题。

参 考 文 献

[1] MOHSEN G, BASSEM K, MAHDI B G, et al. Large-Scale Cognitive Cellular Systems: Resource Management Overview[J]. IEEE Communication Magazine, 2015, 53(5): 44-51.

[2] YUCEK T, ARSLAN H. A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications[J]. IEEE Communications Surveys & Turtorials, 2009, 11(1): 116-130.

[3] UMAR R, SHEIKH A U H, DERICHE M. Unveiling the Hidden Assumption of Energy Detector Based Spectrum Sensing for Cognitive Radio[J]. IEEE Communications Surveys & Tutorials, 2014, 16(2): 713-728.

[4] WANG N, GAO Y, ZHANG X. Adaptive Spectrum Sensing Algorithm under Different PU Utilization[J]. IEEE Communication Letters, 2013, 17(9): 1938-1841.

[5] CHATZIANTONIOU E, ALLEN B, VELISAVLJEVIC V. Threshold Optimization for Energy Detection-based Spectrum Sensing over Hyper-Rayleigh Fading Channels[J]. IEEE Communication Letters, 2015, 19(6): 1077-1080.

[6] LIANG Y C, ZENG Y H, PCH E C Y, et al. Sensing-Throughput Tradeoff for Cognitive Radio Networks[J]. IEEE Transaction on Wireless Communications, 2008, 7(3): 1-12.

[7] XING X S, JING T, LI H J, et al. Optimal Spectrum Sensing Interval in Cognitive Radio Networks[J]. IEEE Transactions on Parallel and Distributed System, 2014, 25(9): 2408-2417.

（下转第 137 页）

分析图 3－图 5 可知，本方案的计算量与通信量都较小，同时本文的匹配结果是精确匹配，因此本文方案比文献[11]、文献[12]方案更适应用于资源有限的智能终端。

结束语　本文针对直接应用隐私保护集合交方案在解决参与式感知数据价值匹配问题上的不足，利用 0-1 编码方法，将数据价值大小的比较问题转换成两个集合是否存在交集的判断问题；然后进一步采用 HMAC 数值化 0-1 编码集合，并采用布隆过滤器对两个集合是否存在交集进行判断，在较好地保护用户数据价值的基础上减小了匹配过程中的计算和通信开销。理论分析和仿真实验证明了所提方案的正确性和高效性。将本文方案应用于日益蓬勃的各类移动环境下的参与式感知应用是我们后期的研究方向。

参 考 文 献

[1] BURKE J A，ESTRIN D，HANSEN M，et al. Participatory sensing[J]. Center for Embedded Network Sensing，2006，13(4)：117-134.

[2] AHMADI H，ABDELZAHER T，HAN J，et al. The sparse regression cube：A reliable modeling technique for open cyber-physical systems[C]// Proc. 2nd International Conference on Cyber-Physical Systems (ICCPS'11). 2011：87-96.

[3] LI H Y，ZHU H，XIAO H，et al. Location Based Participatory Sensing Service[J]. Acta Scientiarum Naturalium Universitatis Pekinensis，2014，43(2)：341-347. (in Chinese)
李怀瑜，朱瀚，肖汉，等. 基于位置的参与式感知服务[J]. 北京大学学报(自然科学版)，2014，50(2)：341-347.

[4] LIU S B，WANG Y，LIU M J. Privacy-preserving Data Sharing and Access Control in Participatory Sensing[J]. Computer Science，2015，42(6)：139-144. (in Chinese)
刘树波，王颖，刘梦君. 隐私保护的参与式感知数据分享与访问方案[J]. 计算机科学，2015，42(6)：139-144.

[5] LI Y K，LIU S B，YANG Z H，et al. Efficient and privacy－preserving profile matching protocols in opportunistic networks [J]. Journal on Communications，2015，36(12)：163-171. (in Chinese)
李永凯，刘树波，杨召唤，等. 机会网络中用户属性隐私安全的高效协作者资料匹配协议[J]. 通信学报，2015，36(12)：163-171.

[6] LIU S B，WANG Y，LIU M J，et al. Privacy-preserving various data sharing protocol in participatory sensing [J]. Journal of Computer Applications，2015，35(7)：1865-1869. (in Chinese)
刘树波，王颖，刘梦君，等. 参与式感知中隐私保护的差异化数据分享协议[J]. 计算机应用，2015，35(7)：1865-1869.

[7] AGRAWAL R，EVFIMIEVSKI A，SRIKANT R. Information sharing across private databases[C]// Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data. ACM，2003：86-97.

[8] DE CRISTOFARO E，GASTI P，TSUDIK G. Fast and private computation of cardinality of set intersection and union[M]// Cryptology and Network Security. Springer Berlin Heidelberg，2012：218-231.

[9] FREEDMAN M J，NISSIM K，PINKAS B. Efficient private matching and set intersection[M]// Advances in Cryptology-EUROCRYPT 2004. Springer Berlin Heidelberg，2004：1-19.

[10] YE Q，WANG H，PIEPRZYK J. Distributed private matching and set operations[M]// Information Security Practice and Experience. Springer Berlin Heidelberg，2008：347-360.

[11] ZHANG R，ZHANG R，SUN J，et al. Fine-grained private matching for proximity-based mobile social networking[C]// INFOCOM. IEEE，2012：1969-1977.

[12] LI H，CHENG X，LI K，et al. Efficient Customized Privacy Preserving Friend Discovery in Mobile Social Networks[C]// 2015 IEEE 35th International Conference on Distributed Computing Systems (ICDCS). IEEE，2015：225-234.

[13] NIU B，LI X，ZHU X，et al. Are You Really My Friend? Exactly Spatiotemporal Matching Scheme in Privacy-Aware Mobile Social Networks[C]// International Conference on Security and Privacy in Communication Networks. Springer International Publishing，2014：33-40.

[14] SUN J，ZHANG R，ZHANG Y. Privacy-preserving spatiotemporal matching[C]// INFOCOM. IEEE，2013：800-808.

[15] BELLARE M，ROGAWAY P. Collision-resistant hashing：Towards making UOWHFs practical [M]// Advances in Cryptology－CRYPTO'97. Springer Berlin Heidelberg，1997：470-484.

[16] LIN H Y，TZENG W G. An efficient solution to the millionaires' problem based on homomorphic encryption[M]// Applied Cryptography and Network Security. Springer Berlin Heidelberg，2005：456-466.

[17] BRODER A，MITZENMACHER M. Network applications of bloom filters：A survey[J]. Internet Mathematics，2005，1(4)：485-509.

[18] SHANNON C E. A mathematical theory of communication[J]. ACM SIGMOBILE Mobile Computing and Communications Review，2001，5(1)：3-55.

[19] WILLIAM S. Cryptography and Network Security：Principles and Practice(Fifth Edition)[M]. Beijing：Publishing House of Electronics Industry，2012. (in Chinese)
斯托林斯. 密码编码学与网络安全：原理与实践(第 5 版)[M]. 北京：电子工业出版社，2012.

(上接第 101 页)

[8] LUO L，ROY S. Efficient spectrum sensing for cognitive radio networks via joint optimization of sensing threshold and duration [J]. IEEE Transactions Wireless Communications，2012，60(10)：2851-2860.

[9] EI-SHERIF A A，MOHAMED A. Decentralized Throughput Maximization in Cognitive Radio Wireless Mesh Networks[J]. IEEE Transactions on Mobile Computing，2014，13(9)：1967-1980.

[10] GORSKI J，PFEUFFER F，KLAMROTH K. Biconvex sets and optimization with biconvex functions：asurvey and extensions [J]. Mathematical Methods of Operations Research，2007，66(3)：373-407.

[11] WENDELL R E，HUNTER A J. Minimization of non-separable objective function subject to disjoint constraints[J]. Operations Research，1976，24(3)：643-657.

[12] BOYD S，VANDENBERGHE L，FAYBUSOVICH. Convex OPTIMIZATION[J]. IEEE Transactions on Automatic Control，2016，51(11)：1859.