一种新型面向频谱高利用率的认知MAC协议

宋 化 林小拉
(中山大学信息科学与技术学院 广州 510006)

摘 要 认知无线电是无线访问领域出现的新技术,目的在于大幅度提高无线频谱的使用。其基本思想是:次用户(非授权用户)在不干扰主用户(授权用户)的条件下允许使用授权频谱。提出一种新的基于独占模式的认知MAC协议。在该协议中,次用户被划分为若干不重叠的组,每个组使用特定的拍卖算法来对其需要租用的信道进行投标。实验表明,这种新协议能够最大化利用频谱资源,并且保证信道在组间分配的公平性和动态性。

关键词 认知无线电,认知MAC协议,信道租用,独占模式

中图法分类号 TP393 **文献标识码** A

Novel High Spectrum Utilization-oriented Cognitive MAC Protocol

SONG Hua LIN Xiao-la
(School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China)

Abstract Cognitive radio (CR) is an emerging technology in wireless access, aiming at vastly improving the way in which radio spectrum is utilized. Its basic idea is that a secondary user (unlicensed user) can be permitted to use licensed spectrum, provided that it does not interfere with any primary users (licensed users). This paper proposed a novel cognitive MAC protocol under the property-rights model, in which, secondary users are divided into several non-overlapping groups, and each group uses the proposed auction algorithm to bid for leasing the required channels. Simulations indicate that proposed MAC protocol utilizes spectrum resources to the maximum, guarantees the fairness and dynamics of channels allocation among groups.

Keywords Cognitive radio, Cognitive MAC, Channel leasing, Property-rights model

1 引言

近年来,随着无线服务以及设备的快速部署,当前可用频谱已几乎完全分配给各种基于频谱的业务,频谱短缺问题已严重阻碍了无线通信的发展。然而,有报告[1]指出:静态频谱分配方式导致授权频谱在大部分时间内处于低利用率(6%)状态。

为了解决频谱短缺问题和提高频谱的利用率,提出一种称为认知无线电的技术来提供随机和动态频谱访问[2]。通常,认知无线电使用公共模型(commons model)[3],该模型要求次用户首先感知无线电环境并搜索未被主用户使用的空闲信道,然后随机使用这些频谱机会。另一种频谱访问模型称为独占模型(property-rights model)[3],使用该模型的主用户将未使用的信道细分成多个子信道后按时间租给次用户。

目前,很少提出针对独占模型的认知MAC协议,已知的协议[4-8]既没有考虑到最大化利用空闲频谱资源,也没有考虑次用户的带宽需求。本文提出一种新的认知MAC协议,在此协议中,次用户被划分为若干不重叠的组,主用户委托拍卖者来拍卖信道租用权,每个组使用特定的拍卖算法来对其需要租用的信道进行投标。本协议的优点主要包括以下几方面:(1)最大化利用频谱资源;(2)主用户得到最大化收益;(3)在组间公平及均匀地分配信道;(4)考虑了次用户的带宽需求,即若给一个组分配信道,该组的最小带宽需求必须满足(此特性在流媒体环境中特别重要)。

2 系统模型

2.1 场景描述与假设

我们聚焦一个包含多个不重叠组的单跳认知无线电网络,每个组由两个或多个需要相互通信的次用户组成。在任何时刻,组内仅有一个成员允许使用分配给该组的信道传输信息,而同组内的其它成员均可接收/响应此成员发出的消息。另外,交互的信息可以是连续性的流媒体资源,例如音乐和视频。因此,必须将次用户的带宽需求考虑在内。

本文做如下假设:(1)每个次用户装备两个无线收发器。其中一个称作数据收发器,用来感知空闲数据信道(DC),并且通过DC交换数据;另一个收发器称作控制收发器,用来从控制信道(CC)发送或接收控制消息。值得注意的是,CC是事先指定好的,而且按照文献[5]的建议,两个收发器都是半双工的。(2)每个次用户看见相同的空闲信道全局,具有全频

到稿日期:2009-08-04 返修日期:2009-10-23 本文受国家自然科学基金(60773199,U0735001)资助。

宋 化(1980—),男,博士生,主要研究方向为无线网络等,E-mail:songhua@mail2.sysu.edu.cn;林小拉(1956—),男,博士,教授,主要研究方向为并行与分布式、计算机网络等。

段感知能力，能够使用聚集频谱技术[9]。(3)假设用户的传输能量足够大，以致于使用相同信道的用户能监听到在该信道上传输的帧。

2.2 控制结构

在认知无线电网络的分布式环境中，次用户被划分为多个非重叠的组。每个组指定一个组长(组长可根据实际情况动态调整)，负责小组成员的管理、组信道的管理和通信管理。除此之外，主用户委托一个拍卖者通过控制信道 CC 在组长间拍卖信道租用权。

3 认知 MAC 协议设计

设计本 MAC 协议的主要目标是在实现主用户收益最大的同时最大化频谱资源利用率，并考虑到次用户的带宽要求。首先给出设计 MAC 协议的总体描述。

3.1 总体描述

图 1 显示了提出的 MAC 协议的基本原理。如图 1 所示，时间轴被分成一系列的租用周期，每个周期包含两个连续的阶段：拍卖阶段和通信阶段。

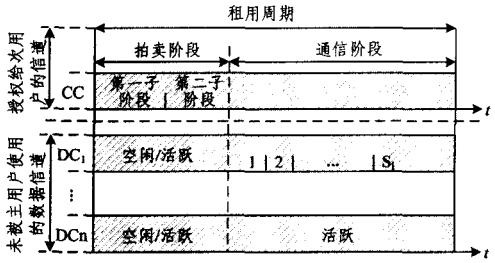

图 1 所提出的 MAC 协议的原理

在本协议中，次用户在任何时刻将处于以下的一个阶段。

1)网络初始化阶段：若一个次用户没有加入任何组，他首先会监听控制信道 CC，以接收从已有组发来的 Invite 帧。当收到来自多个组的 Invite 帧时，选择一个合适的组(在这里，假设次用户事先知道它要加入组的信息)，然后发送 JoinReq 帧给这个组的组长。一旦收到组长响应的 JoinACK 帧，次用户将其数据收发器切换到该组使用的数据信道上。若次用户没有找到一个合适的组加入，并且已有组数小于 M(系统规定的最大组数)，他会自己建立一个新的组并在控制信道上发送 Invite 帧。若次用户在 CC 上监听不到任何 Invite 帧，表明该用户是网络中的唯一用户，于是创建一个组。

2)拍卖阶段：在这个阶段，代表各组的 $m(m\leqslant M)$ 个组长使用拍卖算法(该算法将在 3.4 节中介绍)来对其需要租用的信道进行投标。获得空闲信道的组利用这些信道在通信阶段进行信息交互。

2)通信阶段：在该阶段，每个组使用联合/聚集技术通过在拍卖阶段分配的空闲信道交换信息。因为在任一时刻组内仅有一个成员能使用分配给该组的信道传递数据，因此组员采用时间片轮转法使用信道，并且其使用顺序由成员编号确定。另外，拍卖者跟踪未被主用户使用的空闲信道，为下一租用周期的拍卖作好准备。

伪码 1 描述了次用户加入或离开组的操作。总的来说，上面关于租用周期及伪码 1 的描述刻画了所提出的认知 MAC 协议的原理和工作流程。在下面的小节中，将呈现该协议的一些细节。

伪码 1 次用户加入/离开组

```
1:  switch (次用户的操作){
2:  case 加入组:
3:    监听控制信道 CC;
4:    if (从 CC 至少收到一个 Invite 帧)
5:Label 1:if (找到一个合适的组加入){
6:        向该组的组长发送一个 JoinReq 帧;
7:        if (从组长收到一个 JoinACK 响应帧)
8:          将其数据收发器转向该组使用的数据信道;
9:        else go to Label 1;
10:     }
11:     else {
12:       if (Invite 帧 GrpNum 域的值小于 M){
13:         创建一个组并且它自己作为组长;
14:         在控制信道上发送 Invite 帧;
15:       }
16:       else exit;
17:     }
18:   else{
19:       创建一个组并且它自己作为组长;
20:       在控制信道上发送 Invite 帧;
21:   }
22:   break;
23: case 离开组
24:   if(次用户是组长){
25:     if(不是组中的最后一个成员){
26:       从剩下的组员中选出新组长;
27:       在组内宣布新组长;
28:       离开组;
29:     }
30:     else 在 CC 上发送一个 Die 帧;
31:   }
32:   else{
33:       在组内发送一个 LeaveReq 帧;
34:       离开组;
35:   }
36:   break;
37: }
```

3.2 信道拍卖目标

在拍卖阶段，拍卖者在 m 个组间拍卖 n 条空闲信道。系统除了尽可能高地获得收益外，还有如下目标：(1)最大化获得空闲信道的组的数目 m'；(2)最大化空闲频谱资源的利用率；(3)考虑用户的带宽需求。以上 3 个目标可以描述为：

$$\max m'$$

$$\max \sum_{i=1}^{m'}\sum_{j=1}^{c_i} b_{ij}$$

$$s.t.\ m'\leqslant m, \sum_{i=1}^{m'} c_i \leqslant n, \tag{1}$$

$$R_{\min}^{i}\leqslant\sum_{j=1}^{c_i} b_{ij}\leqslant(1+\varepsilon)R_{\max}^{i}, \sum_{i=1}^{m'}\sum_{j=1}^{c_i} b_{ij}\leqslant\sum_{k=1}^{n} B_k$$

式中，$c_i(i=1,\cdots,m')$ 表示分配给第 i 组的空闲信道数量，b_{ij} $(j=1,\cdots,c_i)$ 为分配给第 i 组第 j 条信道的带宽(本文假设所有信道带宽不一定相同并且是均匀分布的)，$R_{\min}^{i}$ 与 $R_{\max}^{i}$ 表示第 i 组的最小与最大带宽需求，ε 用来保证信道分配的准确和均匀，$B_k(k=1,\cdots,n)$ 为第 k 条信道的带宽。第 3 个约束说明为每个组分配的带宽必须介于该组的最小与最大带宽需求之

间。最后一个约束要求分配给所有组的带宽之和不能超过系统总的空闲带宽。

3.3 投标单价函数

在一轮投标中，每个组长根据本组需要的带宽和能承受的单价（使用每 Mbps 的价格来衡量）来决定投标价格。对于第 $i(i=1,\cdots,m)$ 组，定义一个度量参数，即饥饿度（δ_i）来反映该组需要带宽的迫切程度：

$$\delta_i = 1 - \frac{\sum_{j=1}^{t_i} b_{ij}}{R_{\max}^i}$$

式中，$t_i(i=1,\cdots,m)$ 表示在前几轮投标中分配给第 i 组空闲信道的数目。

组长在决定单价时会考虑本组当前的饥饿度，这样可以保证“饥饿的”组使用较高的价格投标，从而尽快获得所需要的空闲信道。组 i 的投标单价使用一个递增函数 $U_i(\delta_i,\theta_i)$ 来决定，其中 θ_i 是依赖组的一个特定参数。在本研究中，选择对数函数 $U_i(\delta_i,\theta_i)=\theta_i \ln(\delta_i+1)$ 作为单价函数。值得注意的是，当分配给第 i 个组的带宽超过其最大带宽需求时，单价为 0。因为如果一个组的最大带宽需求已满足，它不会再投标获得其它可用空闲信道。很显然，该特性反映了信道拍卖算法设计的第一个目标，节省出来的多余空闲信道可分配给更多的组。组 i 的单价函数为：

$$U_i(\delta_i,\theta_i)=\begin{cases} 0, & -\varepsilon \leqslant \delta_i \leqslant 0 \\ \theta_i \ln(\delta_i+1), & 0<\delta_i \leqslant 1 \end{cases}$$

如图 2 所示，单价函数分成两个区域：$[-\varepsilon,0]$ 和 $(0,1]$。称区域 $(0,1]$ 为活动区域，区域内的函数值变化显著。它显示了随着饥饿度的增加，组长通过增加提供的单价来提高中标机率。在区域 $[-\varepsilon,0]$ 内，由于组需要的最大带宽已经满足，组长不必为争取空闲信道继续投标，因此，带宽单价变为 0。

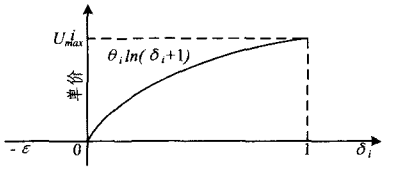

图 2 单价函数曲线

3.4 信道拍卖算法

借用组合拍卖[10]的思想，提出一个新的拍卖算法，即自助拍卖：在一轮拍卖中，有多个组长试图从拍卖者获得信道，每个组长决定并投标它需要的空闲信道。拍卖者根据每个组长的出价与所需带宽计算出单价（每 Mbps 的价格），并且最终满足一个出单价最高的组长的租用要求。

在每个租用周期，拍卖者利用空闲时间探测出 n 条空闲信道，然后将之分配给 m 个组。考虑到实际应用背景和协议设计目标，整个算法分成两个子阶段。在第一个子阶段，通过使用自助拍卖，将部分空闲信道分配给 $m'(m' \leqslant m)$ 个组，并且满足它们的最小带宽需求（在本文中称这些组为活动组）。即，在满足每个组最小带宽要求的情况下，将信道分配给尽可能多的组。显然，该阶段反映了信道拍卖算法设计的第一与第三个目标。在第二子阶段，使用标准的向前拍卖[11]将第一子阶段过后剩余的信道（未能满足更多组的最小带宽需求）在活动组间分配。这反映了信道拍卖算法设计的第二个目标：最大化空闲信道资源的利用率。详细的算法在伪码 2 中描述。

伪码 2 信道分配算法

```
0: 初始化: soldChannelSet = Ø, oneRoundBidSet = Ø, activeLeaderSet = Ø,
每条信道状态 h_l. s = AVAILABLE (l = 1,2,…,n);
1: activeLeaderSet中的组长投标，构造 oneRoundBidSet;
2: Label 1: while (oneRoundBidSet≠Ø) {
3:   在 oneRoundBidSet 中找出具有最大单价的投标(A_i)及对应的组长 i;
4:   for(k=1;k<=|A_i|;k++)
5:     if (a_i^k. s == OCCUPIED) break;
6:   if (k==|A_i|) {
7:     将 A_i 加入到 soldChannelSet 集合;
8:     从 oneRoundBidSet 集合中删除 A_i;
9:     将组长 i 加入到 activeLeaderSet 中;
10:    for(j=1;j<=k;j++) a_i^j. s == OCCUPIED;
11:  }
12:  else
13:    从 oneRoundBidSet 中删除 A_i;
14: }
15: 在控制信道上发送本轮投标结果;
16: activeLeaderSet中的组长投标，构造 oneRoundBidSet;
17: if (oneRoundBidSet≠Ø) go to Label 1;
18: 将 activeLeaderSet 中每个组长的优先级设为 1;
19: for(k=1;k<=n;k++) {
20:    if (h_k. s == AVAILABLE) {
21:      组长投标以获得信道 h_k;
22:      找出在本次投标中具有最高优先级的组长 i(若多个组长具有相同的优先级，投标最高者获胜；若仍有组长投标价格相同，组号最小者获胜);
23:      将 h_k 加入到 soldChannelSet 的 A_i 中;
24:      h_k. s == OCCUPIED;
25:      组长 i 的优先级变为原来的一半;
26:    }
27: }
28: return soldChannelSet;
```

伪码的第 1 行到 17 行描述了信道拍卖算法的第一个子阶段。在该阶段，进行拍卖循环直到没有额外的组能够获得满足其最小带宽要求的信道集。在每轮拍卖中，组长 i 选择一组信道 $A_i=\{a_i^j\}j\in\{1,2,\cdots,n_i\}$ 并为之投标。其中，a_i^j 表示系统中的一条信道，n_i 是 A_i 中信道的总数。若组长 i 投标的单价是所有投标者中最高的，则拍卖者将 A_i 分配给组 i（若多个组长提供相同的投标单价，组号小的组长获胜）。在每轮投标结束后，拍卖者将本轮的投标结果在控制信道 CC 上发送，已“租出”的信道在后续的投标中不能被任何组选择。若某个组长在某轮投标中成功地获得一组信道，他在余下的第一子阶段时间内不再参与投标。在伪码 2 中，定义了 3 个集合：soldChannelSet，oneRoundBidSet 和 activeLeaderSet。soldChannelSet 集合表示已分配给活动组的信道集的集合 $\{A_i\}i\in\{1,2,\cdots,m'\}$；oneRoundBidSet为一轮投标的投标集合；activeLeaderSet 表示活动组长（活动组组长）的集合 $\{g_i\}i\in\{1,2,\cdots,m'\}$。特别地，使用 s 来表示信道的一个属性：该信道是否已被分配。若已分配给某个组，此信道 s 属性的值设为 OCCUPIED，否则为 AVAILABLE。$\overline{\text{activeLeaderSet}}$ 是 activeLeaderSet 的补集，表示未分配信道的组长集合。

伪码的第 18 至 28 行描述了拍卖算法的第二子阶段。在该子阶段，投标的信道不能由各个组自由选择，而是由拍卖者统一决定。拍卖者将第一子阶段拍卖剩下的信道一次一个地向活动组长拍卖。即在第二子阶段，每轮拍卖中仅有一个组获得一条信道。每个活动组长被指定一个优先级（初始值为

1)，在对某条信道的投标中，具有最高优先级的活动组长中标。若多个组长具有相同的优先级，投标价格最高的组长获胜(如果多个组长提供相同的价格，组号最小的获胜)。通过使用这种机制，剩余信道可以公平和均匀地在所有活动组长间分配。

4 仿真与性能评估

本节使用网络仿真器(NS2)[12]来评估提出的协议的性能，在250m×250m区域内随机放置25个相同(具有相同的无线电能力)的静态次用户结点和1个拍卖者结点，并且根据典型的2.4GHz无线电配置把无线范围设置成372.214m。将20MHz～2.4GHz范围内可用频段的聚集带宽(35Mbps～45Mbps)划分成30条可用数据信道(DCs)，同时指定一条2Mbps的公共控制信道(CC)。在仿真实验中，为不受传输协议的影响，仅仅仿真饱和CBR交通来评估系统性能，并且使用单价函数 $U_i(\delta_i,\theta_i)=\theta_i\ln(\delta_i+1)$，对于所有组，$\theta_i(i=1,\cdots,m)$都设为10。仿真使用的参数在表1中列出。

表1 仿真参数

参数	值
次用户组数	5,8
数据信道数	30
每条数据信道带宽	1～1.5Mbps
每个组最小带宽要求	1Mbps,2Mbps
每个组最大带宽要求	6Mbps
数据包长度	1024Bytes
传输能量	0.01W
校正因子	0.1①

为了简洁起见，定义整个系统的空闲信道比例为 $p_n=n/N$。

4.1 吞吐量评估

本节将新协议的吞吐量与其它两种协议的吞吐量相比较：OS-MAC[5]与CO-MAC[7]。吞吐量通过计算给定时间内传输的有效载荷来衡量协议的性能。

图3显示了在不同网络场景次用户组数为5和8的情况下吞吐量的对比。首先注意到，随着空闲带宽比例(p_n)的增加，3种协议的系统吞吐量都有一定程度增加。其次，新MAC协议的吞吐量单调递增，而CO-MAC的吞吐量很快达到上界，OS-MAC的吞吐量则在到达一个固定值后只有少量的增加。这反映了随着 p_n 的增加，新协议可以充分地利用空闲信道资源。

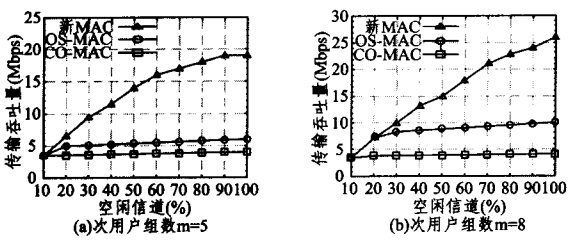

图3 不同 p_n 下系统的吞吐量

在OS-MAC协议中，由于一个组仅能使用一条信道，并且所有信道的带宽在1Mbps和1.5Mbps之间均匀分配，若每个组独占一个信道(即该组不和其它组共享此信道)，系统的总吞吐量不会随 p_n 的增加而增加许多，但是会随着次用户组数 m 的增加而增加。例如，在图3(a)中，OS-MAC协议在 $p_n=40\%$ 时的系统吞吐量高于其在 $p_n=30\%$ 时的系统吞吐量。因为随着 p_n 的增加，尽管每个组不能分配到更多的信道，但它有机会切换到一个"较好"的信道。而且，在图3(b)中，OS-MAC协议的吞吐量高于图3(a)的相应部分，因为当 m 增加时，更多的空闲信道被使用。对于CO-MAC协议，因为在任何时刻仅有一对次用户使用系统空闲信道(可使用多条)，并且在实验中，用户需要的最大带宽相同，所以只要次用户要求的最大带宽获得满足，整个系统的吞吐量就不会改变。

另外需要注意的是，在图3(a)中，当 $p_n=80\%$ 时，代表新MAC协议的系统吞吐量曲线接近一个固定值。因为在这种情况下，所有组的最大带宽都已满足，整个系统的吞吐量达到一个上界，并且不再需要更多的空闲信道(若继续将空闲信道分配给这些组，将造成信道浪费)。

4.2 带宽利用率评估

图4显示了3种MAC协议的带宽利用率(σ)随着 p_n 变化的对比。其中，图4(a)中次用户组数 m 为5，图4(b)中 m 为8。

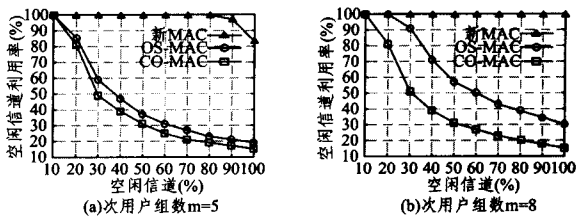

图4 不同 p_n 下空闲信道利用率

在图4中，可以观察到3点：第一，在所有组的最大带宽要求满足之前，新MAC协议的空闲信道利用率(σ)几乎为100%，而其它两种协议的 σ 随着 p_n 的增加而减少。第二，在新MAC协议中，用户能够尽量使用空闲信道并且达到高信道利用率。而OS-MAC协议由于使用了固定数量的空闲信道，其空闲信道利用率随着 p_n 的增加而迅速下降，除非增大 m 的值。第三，在图4(a)中，代表新MAC协议的 σ 曲线在 $p_n=80\%$ 后迅速下降，因为剩余空闲信道将不会被带宽需求已满足的次用户所占用，这部分信道可分配给其它急需信道的用户。

4.3 公平性评估

图5显示了本协议在不同空闲信道数目($p_n=30\%$，$p_n=60\%$及 $p_n=90\%$)情况下每个组的吞吐量。在该仿真实验中，组数 m 为5。在图5(a)中，每个组的最小带宽需求 R_{min} 为1Mbps；而在图5(b)中，R_{min} 为2Mbps。通常，对于某个 p_n，所有组吞吐量的对比反映了整个系统的公平性，而某个组在不同 p_n 吞吐量的对比反映了资源分配的动态性。

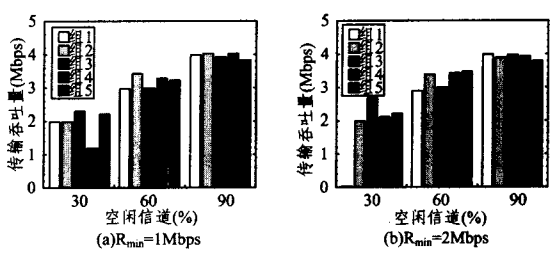

图5 不同 p_n 下组吞吐量

从图5可以看出，对于某个 p_n，每个组的吞吐量非常接近。特别是当 p_n 为90%时，各个组的吞吐量几乎相同，图5(a)尤为明显，这反映了协议的公平性。另一方面，随着 p_n 的

①通过重复仿真实验，该值在保证用户带宽要求与节省空闲信道之间获得较好的平衡。

增加，某个组的吞吐量单调增加。例如，在图5(b)中，当 p_n 从60%增加到90%时，组2的吞吐量从3.294Mbps增加到3.88Mbps。因此，增加的空闲信道可在组间动态分配。注意在图5(b)中，当 $p_n=30\%$ 时，组1的吞吐量为0Mbps。这是因为在该环境下，空闲信道非常少，不足以为每个组分配信道，仅部分投标较高的组能获得。

从以上仿真可以看出，新协议能够保证信道分配的公平性及动态性。

结束语 本文提出了一种新的认知MAC协议。协议的目标是在主用户达到收益最大化的同时最大化频谱的利用率，并且将次用户的带宽要求考虑在内。借用组合拍卖的思想，设计出一种新的拍卖算法，该算法作为协议的核心非常适合在特定场合解决信道分配问题。仿真实验表明，提出的新协议能最大化地利用频谱资源，保证信道分配的公平性及动态性。

参 考 文 献

[1] Federal Communications Commission, Spectrum Policy Task Force[R]. Rep. ET Docket no. 02-135. 2002

[2] Haykin S. Cognitive radio: Brain-empowered wireless communications[J]. IEEE Journal on Selected Areas in Communications, 2005,23(2):201-220

[3] Neel J O. Analysis and Design of Cognitive Radio Networks and Distributed Radio Resource Management Algorithms[D]. Virginia Polytechnic Institute,2006

[4] Jia J, Zhang Q, Shen X. HC-MAC: A Hardware-constrained Cognitive MAC for Efficient Spectrum Management[J]. IEEE Journal on Selected Areas in Communications,2008,26(1):106-117

[5] Shin K G, Hamdaoui B. OS-MAC: An Efficient MAC Protocol For Spectrum-Agile Wireless Networks[J]. IEEE Transactions on Mobile Computing,2008,7(8):915-930

[6] Mishra A. A Multi-channel MAC for Opportunistic Spectrum Sharing in Cognitive Networks[C]// Military Communications Conference. 2006:1-6

[7] Su H, Zhang X. Cross-Layer Based Opportunistic MAC Protocols for QoS Provisionings Over Cognitive Radio Wireless Networks[J]. IEEE Journal on Selected Areas in Communications, 2008,26(1):118-129

[8] Mansi T, Ravi P. CSMA-based MAC Protocol for Cognitive Radio Networks[C]// IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks. 2007:1-8

[9] Corderio C, Challapali K, Birru D, et al. IEEE 802.22: an introduction to the first wireless standard based on cognitive radios [J]. Journal of Communications,2006,1(1):38-47

[10] de Vries S, Vohra R V. Combinatorial auctions: A survey[J]. INFORMS Journal on Computing,2003,15(3):284-309

[11] Krishna V. Auction Theory[M]. Academic Press,2002

[12] The network simulator (ns-2)[EB/OL]. http://www.isi.edu/nsnam/ns/

(上接第92页)

人的身份。

证明：完整有效的密文中有原始签密人所建立的授权许可证 m_w，而 m_w 中有代理签密人的身份信息，任何第三方都可以从 m_w 中确定相应代理签密人的身份。

因此，本文方案满足强可识别性。

定理5 代理签密人不能将代理签密密钥用于产生有效密文以外的其它目的。

证明：由于授权许可证 m_w 出现在解签密阶段的验证等式 $RS=h(m,R)h(m_w)((y_A+(yQ_A)_xG)+(y_B+(yQ_B)_xG))$ 中，而且代理签密密钥中包含有原始签密人的授权信息，因此，代理签密人不能签署未经授权的信息，只能用于产生有效的代理签密组，当然他也不能把代理签密权利转给其他人。

因此，本文方案能够有效防止签密权力的滥用。

定理6 本文方案满足可区分性。

证明：授权许可证 m_w 描述了代理签密人的信息、原始签密人和代理签密人之间的约束信息，并会出现在有效的代理签密里。原始签密人的公钥及代理签密人的公钥都会出现在代理签名的验证等式里，而且最重要的是代理签密密钥里也包含代理签密人的私钥。因此本文方案能够很好地满足可区分性。

结束语 本文设计了一个新的基于ECC的自认证代理签密方案，此方案克服了双线性对运算量大以及计算效率低的缺陷，具有安全性强、计算量小、速度快、密钥长度短、便于计算机实现等优点，因而在移动通信、移动代理、电子商务、电子选举、电子拍卖等领域有着很好的应用前景。

参 考 文 献

[1] Gamage C, Leiwo J, Zheng Y. An efficient scheme for secure message transmission using proxy signcryption[C]// Proceedings of 22nd Australasian computer science conference. Berlin: Springer-Verlag,1999:420-431

[2] Chan W K, Wei V K. A threshold proxy signcryption[C]// Proceedings of International Conference on Security and Management. Monte Carlo Resort, Las Vegas, Nevada, USA, 2002:24-27

[3] Chan W K, Wei V K. A threshold proxy signcryption[C]// Proceedings of International Conference on Security and Management. Monte Carlo Resort, Las Vegas, Nevada, USA, 2002:24-27

[4] Wang Q, Cao Z F. Two proxy signcryption schemes from bilinear pairings[C]// Proceedings of CANS 2005, LNCS 3810. Berlin: Springer-Verlag, 2005:161-171

[5] Wang M, Li H, Liu Z J. Efficient identity based proxy-signcryption schemes with forward security and public verifiability[C]// ICCNMC 2005. LNCS3619. Berlin: Springer-verlag, 2005:982-991

[6] Li X X, Chen K F. Identity based proxy-signcryption scheme from pairings[C]// IEEE International Conference on Services Computing. Los Alamitos, California: IEEE Computer Society Press, 2004:494-497

[7] 刘俊宝，肖国镇. 带门限共享解密的多代理签密方案[J]. 计算机工程，2006,32(23):21-23

[8] 胡振鹏，钱海峰，李志斌. 基于身份的多接收者的代理签密方案[J]. 华东师范大学学报：自然科学版，2008(1):83-87

[9] 于刚，黄根勋. 一个前向安全的基于身份的代理签密方案[J]. 计算机工程与应用，2008(2):157-159

[10] 张学军，王育民. 高效的基于身份的代理签密[J]. 计算机工程与应用，2007,43(3):109-111

[11] 王书海，冯志勇，綦朝晖. 权限可控的公开验证代理签密方案[J]. 计算机应用，2008,28(12):3163-3164

[12] 禹勇，杨波，李发根，等. 基于身份的可快速撤销代理权的代理签密方案[J]. 电子与信息学报，2008,30(3):672-675

[13] 俞惠芳，王彩芬. 一个高效的自认证签密方案[J]. 计算机工程，2009,35(16):138-139,142