发明名称  一种条件接收系统中对用户跨区进行管理的方法

摘要
本发明公开了一种条件接收系统中对用户跨区进行管理的方法，包括：把用户按照所在地区分址，条件接收系统向每个用户发送用户授权信息 EMM，授权设置用户地区分址 GCA 的值；子前端系统生成 PSI 表中的 ca 私有数据列表的数据，并添加包含 ca 版权信息；收看节目时，机顶盒的条件接收系统模块先接收来自子网络的 PSI 表的 ca 私有数据列表数据，过滤并解析出 EMM 的 pid 值；与用户智能卡中的用户地区分址 GCA 的值比较，两者一致时，如果有授权，则进行解密；否则，不能解密并收看节目。本发明使用条件接收系统设置用户的用户地区分址，可以在一个较大范围内（省级网络中）控制用户的收看，防止用户在节目相同收费不同的地市之间移动。
1. 一种条件接收系统中对用户跨区进行管理的方法，其特征在于：包括如下步骤：

基于条件接收系统，把用户按照所在地市不同而划分成不同的地区分址，条件接收系统向每个用户发送用户授权信息 EMM，授权设置用户的用户地区分址 GCA 的值；

在小的地区子网范围内，前端系统生成 PSI 表中的 ca 私有数据列表的数据，并添加包含 ca 私有信息；

在收看节目时，机顶盒上的条件接收系统模块首先接收来自子网络的 PSI 表的 ca 私有数据列表的数据，过滤并解析出 EMM 的 pid 值；

机顶盒上的条件接收系统模块将 ca 私有信息中包含的 GCA 的值与用户智能卡中的用户地区分址 GCA 的值进行比较，两者一致时，则说明该用户是本地用户，如果有授权，则进行解密并收看节目；否则，说明该用户不是本地用户，不论该用户是否有授权都不能解密并收看节目。

2. 根据权利要求 1 所述的一种条件接收系统中对用户跨区进行管理的方法，其特征在于：所述把用户按照所在地市不同而划分成不同的地区分址，具体包括：定义一个客户地理分区地址的数据结构，每个客户地理分区地址中有 4 个字节，供运营商自己按用户的不同的地理位置进行设置。

3. 根据权利要求 2 所述的一种条件接收系统中对用户跨区进行管理的方法，其特征在于：所述客户地理分区地址中的 4 个字节中，前 3 个字节为地理位置编码，用于精确地表明用户的位置，后一个字节为属性编码，用于把用户区分成不同的类别。

4. 根据权利要求 1 所述的一种条件接收系统中对用户跨区进行管理的
方法，其特征在于：所述子网络前端生成包含有节目服务信息表 PSI 及将 PMT 表中的 ECM 的 PID 值改成一个其他的无效值；同时，ECM_PID 的描述子中添入自定义的一个私有数据。

5. 根据权利要求 4 所述的一种条件接收系统中对用户跨区进行管理的方法，其特征在于：所述子网内的 PSI 信息和该子网络内用户使用的智能卡 GCA 编码完全匹配。

6. 根据权利要求 1 所述的一种条件接收系统中对用户跨区进行管理的方法，其特征在于：所述智能卡中的用户地区分址 GCA 的值由运营商通过条件接收系统设置。
一种条件接收系统中对用户跨区进行管理的方法

技术领域

本发明涉及利用一种有条件接收系统通过智能卡中的可由运营商编程的 GCA (Geographic Card Address 地域智能卡寻址) 地址并结合修改下级网络中的 PSI (Program Service Information) 表实现用户跨区管理的方法。

背景技术

在数字电视网络大发展的情况下，如何在一个较大范围内 (省级网络中) 控制用户的定点收看，防止用户在节目相同收费不同的地市之间随意移动，成为一个困扰有线电视网络公司的难题。

出现这种难题是由我国的特殊国情决定的。在上一级网络公司下传加密的节目到各个地市有线电视网络公司，各个地市有线电视网络公司将转发这些节目而不是解开节目或者重新进入复用器。由于各个地市个人收入水平的不同会产生同一套节目在各地的收费不同的状况。一些用户会利用这种状况从收费较低的地方购买节目，而到收费较高的地方收看甚至贩卖。这样将严重影响我国现行有线电视网络公司体制下的利益分配的均衡，打乱现有的有线电视网络的格局。因此如何防止用户异地移动收看电视成为网络公司需要解决的一个重要问题。

传统的加密传输模式如图 1 所示：首先数字节目以及增值业务的数据通过复用器复用成传输流 TS 流，条件接收系统 EMMG 通过 HUB 连接到复用器的 EMMI 接口上，条件接收系统 EMCG 通过 HUB 连接到复用器的 ECMI 接口上。复用器中的 DVB 标准的加扰器产生控制字 CW，复用器使用控制字 CW 对选中的节目 (或服务) 进行加扰。复用器通过 DVB 同密标准接口协议与条件接收系统 EMCG 通讯，把控制字 CW 传送给 EMCG。通过条件接收系统 EMCG 产生相
应的 ECM 流，并经过复用器的 ECMI 接口把生成的 ECM 流注入到传输流 TS 流中。用户管理系统 SMS 通过条件接收系统的用户管理系统接口（SMS-I）向条件接收系统的用户授权系统 SAS 发送授权请求，用户授权系统 SAS 响应请求产生一个用户授权信息 EMM。用户授权系统 SAS 生成的 EMM 通过 EMM-INJECTOR 注入器按照 DVB 同密标准接口协议把 EMM 注入到复用器中。复用器把接收到的用户授权信息 EMM 复用到传输流 TS 流中。

用户端机顶盒 STB 中的智能卡在接收到用户授权管理信息 EMM 后，产生授权。在收看加密节目时，机顶盒需要从 PMT 表中找到与加密节目对应的 ECM_PID。将 ECM_PID 设入滤波通道，过滤出加密节目所使用的 ECM 数据。接收 EMM 数据后，智能卡中必须有该节目的授权，才能正确地解开用户控制信息 ECM 中加密了的控制字 CW。由于智能卡和用户端机顶盒 STB 之间的通信是加密的。所以 STB 在接收信道的数据，要再次解密才能得到智能卡加密的控制字。STB 把控制字写入 DVB 标准的解密芯片中，就可以还原被加扰的视音频或者数据了。

由于传统方案中 EMM 和 ECM 没有特殊的用户的地址的标识，因此在整个运营商的网络中用户的移动时，用户的机顶盒和智能卡接收时在各个地方的接收流程都是一致的，并没有可以控制的有效手段。就会造成一些人会利用这种状况从收视费低的地方购买节目贩卖到收视费高的地方。从而严重影响我国现行有线电视网络公司体制下的利益分配的均衡，打乱现有的有线电视网络的利益格局。

发明内容

本发明要解决的技术问题是提出一种条件接收系统中对用户跨区进行管理的方法，即通过条件接收系统定义并生成 PSI 表中的 ca (conditional access) 私有数据列表，限制用户随意异地移动。

本发明所述条件接收系统中对用户跨区进行管理的方法，包括如下步
骤：

基于条件接收系统，把用户按照所在地市不同而划分成不同的地区分
址，条件接收系统向每个用户发送 EMM 授权设置用户的用户地区分址 GCA 的
值；

在小的地区子网范围，前端系统生成 PSI 表中的 ca 私有数据列表的数
据，并添加包含 ca 私有信息；

在收看节目时候，机顶盒上的条件接收系统模块首先接收来自子网络的
PSI 表的 ca 私有数据列表的数据，过滤并解析出 EMM 的 pid 值；

机顶盒上的条件接收系统模块将 ca 私有信息中包含的 GCA 的值与用户
智能卡中的用户地区分址 GCA 的值进行比较，两者一致时，则说明该用户是
本地用户，如果有授权，则进行解密并收看节目；否则，说明该用户不是本
地用户，不论该用户是否有授权都不能解密并收看节目。

当用户因为搬家或者其他合理的原因，从一个地市移动到另一个地市时
可以向运营商请求更换自己的用户地区分址 GCA。运营商经验证后，可以重
新为该用户发送新的用户地区分址 GCA，保证合理移动的用户可以继续在新
的城市收看到加密的数字电视节目。

本发明使用条件接收系统设置用户的用户地区分址，并结合在子网络前
端生成 ca 私有数据的 PSI (Program Service Information) 表。本发明所述
方法可以在一个较大范围内（省级网络中）控制用户的收看，防止用户在节目
相同收费不同的地市之间移动。

附图说明

图 1 是传统的数字电视解密流程示意图；

图 2 是本发明所述方法的流程示意图；

图 3 是 GCA 的客户地理分区地址数据结构的示意图。
具体实施方式

本发明所述方法主要是使用条件接收系统设置用户的用户地区分址，并结合在子网络前端生成ca私有数据的PSI(Program Service Information)表。本发明所述方法的具体原理说明如下：

定义基于条件接收系统的按用户实际地址进行分区编目的格式。即用户地区分址GCA；在一个大的范围例如一个省，制定一个用户地区分址的列表。即把用户按照所在地市不同而划分成不同的地区分址。在相同的地区用户有相同的地区分址编码。

通过条件接收系统按照上述实际地址分区编码的规则，向每个用户发送EMM授权设置用户的用户地区分址GCA的值。

在小的地区子网范围，如地市的网络，前端生成PSI表中的ca私有数据列表的数据，并添加包含ca私有信息。

在收看节目时候，机顶盒上的条件接收系统模块首先接收来自子网络的PSI表，过滤并解析出EMM的pid值；同时处理ca私有信息。

子网络生成并发送的ca私有信息中，所包含的GCA的数值与用户智能卡中的用户地区分址GCA的值一致时，则说明该用户是本地用户如果有授权就可以正常收看节目；否则，说明该用户不是本地用户，不论该用户是否有授权都不能解密并收看节目。

由于用户智能卡中的用户地区分址GCA值是由运营商通过条件接收系统设置的，用户无法通过其他任何方式自行修改。而用户一旦离开自己缴费的地市网络，移动到其他地市，就无法收看节目了。从而实现了控制用户的跨区移动。

本发明所述方法中所述按用户实际地址进行分区编码的格式，实际上是定义一个客户地理分区地址的数据结构，它是基于智能卡所有者所在的地理位置来划分的（如城市，区县，小区，街道等等）。智能卡中的每个密钥
集都有自己的 GCA 来指明地理位置。每个客户地理分区地址中有 4 个字节，供运营商自己按用户的不同的地理位置进行设置。参见图 3，包括 3 byte 的地理位置编码和 1 byte 的属性编码，地理位置编码用于精确地表明用户的位置，而属性编码可以把用户区分成不同的类，最大可以达到 256 个不同的类。

下面表 1 所示是一个 GCA 设置的例子：

<table>
<thead>
<tr>
<th>位</th>
<th>描述</th>
<th>例子</th>
</tr>
</thead>
</table>
| 1  | 15 个城市 | 0x0 ➔ 北京  
0x1 ➔ 上海  
0x2 ➔ 天津  
0xE ➔ ....  
0xF ➔ 所有城市 |
| 2  | 15 个区县 | In case digit 1 is set to 0x1 (USA):  
0x0 ➔ 海淀区  
0x1 ➔ 东城区  
0x2 ➔ 西城区  
0x3 ➔ 丰台  
0x4 ➔ Central states  
0xE ➔ ....  
0xF ➔ 指定市中所有的区县 |
| 3  | 15 个小区 | 0x0 ➔  
0x1 ➔  
0xE ➔ .... ....  
0xF ➔ 指定区县中的所有小区 |
| 4  | 15 个街道 | 0x0 ➔  
0x1 ➔ ....  
0xE ➔  
0xF ➔ 指定小区中所有街道 |
<table>
<thead>
<tr>
<th>位</th>
<th>描述</th>
<th>例子</th>
</tr>
</thead>
</table>
| 5  | 15 个路 | 0x0 ➜  
|    |      | 0x1 ➜  
|    |      | 0x2 ➜  
|    |      | 0xE ➜  ⋯⋯.  
|    |      | 0xF ➜ 街道中的所有路 |
| 6  | 15 个楼 | 0x0 ➜  
|    |      | 0x1 ➜  
|    |      | 0x2 ➜  
|    |      | 0xE ➜  ⋯⋯.  
|    |      | 0xF ➜ 路中的所有楼 |

节目供应商可以根据实际情况组合各个数据位，并指定它们所代表的实际地址。比如街道，可以把第 3, 4 位合并使用，这样最大可以表示 255 个街道。

参见表 2，属性编码可以把用户区分成不同的类，最大可以达到 255 个不同的类。

表 2

<table>
<thead>
<tr>
<th>属性代码</th>
<th>描述</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>医生</td>
</tr>
<tr>
<td>0x01</td>
<td>老师</td>
</tr>
<tr>
<td>0x02</td>
<td>律师</td>
</tr>
<tr>
<td>0x03</td>
<td>学生</td>
</tr>
<tr>
<td>0x04</td>
<td>⋯⋯.</td>
</tr>
<tr>
<td>0xFE</td>
<td>⋯⋯.</td>
</tr>
<tr>
<td>0xFF</td>
<td>所有职业</td>
</tr>
</tbody>
</table>

本发明所述方法中定义的客户地理分区地址是由运营商通过用条件接收系统自行定义和修改的。在定义和修改用户智能卡中的客户地理分区地址时，是需要经过安全引擎加密和签名的。用户是无法自己调整设置的客户地
理分区地址的。

下面具体说明子网内的 PSI 信息的生成机制。

在子网络生成 ca 私有数据的 PSI 的目的，是将物理上实际是同一个网络的网络环境，根据收费标准的不同，以 PSI 信息重新划分出若干个子网络，以区分各个网络的收费差别；利用条件接收系统可以鉴别修改后的不同 PSI 信息的 GCA 功能，作为校验不同网络区域的依据。

每一个子网内的 PSI 信息和其指定的 GCA 编码是完全匹配的，所以即使用户带着智能卡和机顶盒一起移动，由于他所在其它子网内收到的 PSI 信息和智能卡的 GCA 不匹配，这样，将使该机顶盒无法正常还原出加密的数字电视节目。

但是，当合法用户因为各种原因由一个子网络搬到另一个子网络内，就需要运营商使用条件接收系统发送 EMM 更改该用户的 GCA 编码，就可以顺利完成合法用户网络迁移的工作，而不必要求用户到营业大厅退回机顶盒和智能卡，即不需要重新购买另外的机顶盒和智能卡，从而减少麻烦。

省级网络公司前端系统和标准的数字电视前端没有任何的区别。在各个地市向下传输到用户家之前，各个地市的前端系统对从省级网络公司发送来的数字电视的传输流进行修改。主要修改的是 PMT（program map table）中的 ECM 的 PID，把这个值改成一个其他的无效值，即切断了加密的数字电视节目与相关的 ECM 间的联系。用户的机顶盒将无法找到与该加密的数字电视节目对应的 ECM_PID。

由于该 ECM_PID 的正确与否将决定用户的机顶盒能否找到正确的 ECM 数据，从而可以还原在 ECM 中包含的加密的控制字。这样也就直接控制用户能否正常收看与该 ECM_PID 对应的加密数字电视节目了。

为了让本地区的合法用户能正常收看加密的数字电视节目，同时还在修改了 ECM_PID 的描述子中添入自定义的一个私有数据，将正确的 ECM_PID 按照 RSA 算法生成一段数据放入私有数据段中。此算法将和用户的客户地理
分区地址相关。

例如：使用条件接收系统 ID，为 0X4901 的条件接收系统使用密钥 0X06 对节目 A 加密，其原有传输流中的 PMT 中，修改节目对应的 BCM_PID 为 0X101 条件接收 CA 描述子，其格式参见表 3。

表 3

<table>
<thead>
<tr>
<th>数据名称或作用</th>
<th>数据长度 (BIT)</th>
<th>具体数值</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES_TAG</td>
<td>8</td>
<td>09</td>
</tr>
<tr>
<td>DES_LENGTH</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>CAS_ID</td>
<td>16</td>
<td>4901</td>
</tr>
<tr>
<td>保留字段 reserved</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>ECM_PID</td>
<td>13</td>
<td>101</td>
</tr>
</tbody>
</table>

在地市 1 的前端，定义该地市的 GCA 是 0X01 ** ** **，调整后条件接收 CA 描述子的格式参见表 4。

表 4

<table>
<thead>
<tr>
<th>数据名称或作用</th>
<th>数据长度 (BIT)</th>
<th>具体数值</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES_TAG</td>
<td>8</td>
<td>09</td>
</tr>
<tr>
<td>DES_LENGTH</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>CAS_ID</td>
<td>16</td>
<td>4901</td>
</tr>
<tr>
<td>保留字段 reserved</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>ECM_PID</td>
<td>13</td>
<td>101</td>
</tr>
<tr>
<td>使用 GCA 标志</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>GCA 的密钥</td>
<td>8</td>
<td>06</td>
</tr>
</tbody>
</table>
有效 GCA 长度
（使用的 GCA 长度）
GCA.ECM_PID

2
32

1（使用 GCA 的第一个字节 01 作参数）

在地市 2 的前端，定义该地市的 GCA 是 0X02 ** ** **，调整后条件接收 CA 描述子的格式参见表 5。

表 5

<table>
<thead>
<tr>
<th>数据名称或作用</th>
<th>数据长度（BIT）</th>
<th>具体数值</th>
</tr>
</thead>
<tbody>
<tr>
<td>描述子标识符 DES_TAG</td>
<td>8</td>
<td>09</td>
</tr>
<tr>
<td>描述子长度 DES_LENGTH</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>条件接收系统 ID CAS_ID</td>
<td>16</td>
<td>4901</td>
</tr>
<tr>
<td>保留字段 reserved</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>ECM_PID</td>
<td>13</td>
<td>999</td>
</tr>
<tr>
<td>使用 GCA 标志</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>GCA 的密钥</td>
<td>8</td>
<td>06</td>
</tr>
<tr>
<td>有效 GCA 长度</td>
<td>2</td>
<td>1（使用 GCA 的第一个字节 02 作参数）</td>
</tr>
<tr>
<td>（使用的 GCA 长度）</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GCA.ECM_PID</td>
<td>32</td>
<td>*02</td>
</tr>
</tbody>
</table>

地区 1 的用户在收到授权接收加密节目 A 时，需要先从 PMT（program map table）中寻找对应 ECM_PID。该用户的机顶盒在收到地区 1 前端修改后的描述子后，先从智能卡中读出对应密钥集 06 的 GCA 的值，并根据描述子私有数据中的 GCA.ECM_PID 值就可以正确还原出真实的 ECM_PID 的值。将 ECM_PID 设入滤波通道，过滤出与加密节目对应的 ECM 数据。

如果智能卡中已经有该节目的授权，就能正确地解出用户控制信息 ECM 中加密了的控制字 CW。由于智能卡和用户端机顶盒 STB 之间的通信是加密的。所以 STB 在接收到通信的数据后，要再次解密才能得到智能卡解出控制
字。STB 把控制字写入 DVB 标准的解扰芯片中，就可以还原被加扰的视音频或者数据了。

如果地区 2 的用户跑到地区 1，来接收加密节目 A 时，需要先从 PMT 中寻找对应 ECM_PID。该用户的机顶盒在收到地区 1 前端修改后的描述子后，先从条件接收系统的模块中读出对应密钥集 06 的 GCA 的值，根据描述子私有数据中的 GCA ECM_PID 值，并不能正确还原出真实的 ECM_PID 的值。这样，将错误的 ECM_PID 设入滤波通道后，无法过滤出与加密节目对应的 ECM 数据。也就不能还原被加扰的视音频或者数据了。从而达到了控制用户异地移动的要求。

最后应说明的是：以上实施例仅用以说明而非限制本发明的技术方案，尽管参照上述实施例对本发明进行了详细说明，本领域的普通技术人员应当理解：依然可以对本发明进行修改或者等同替换，而不脱离本发明的精神和范围的任何修改或局部替换，其均应涵盖在本发明的权利要求范围当中。
图 1
图 2

划分用户地区，产生地域智能卡寻址信息GCA

条件接收系统发送EEM，设置用户智能卡的GCA

设置智能卡GCA

大型网络公司已加扰的数据流

下属子网络公司

添加本地ca私有数据

智能卡

用户机顶盒

机顶盒比较私有数据和智能卡中的GCA是否一致？

一致

正常收看节目

不一致

无法收看节目
图 3