[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04N 7/167 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200380104885.X

[43] 公开日 2006 年 1 月 11 日

[11] 公开号 CN 1720736A

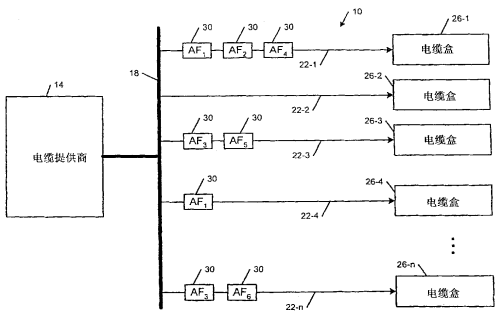
[22] 申请日 2003.11.10
[21] 申请号 200380104885.X
[30] 优先权
[32] 2002.12.3 [33] US [31] 10/308,909
[86] 国际申请 PCT/US2003/035704 2003.11.10
[87] 国际公布 WO2004/052007 英 2004.6.17
[85] 进入国家阶段日期 2005.6.2
[71] 申请人 松下电器产业株式会社
地址 日本大阪府门真市
[72] 发明人 拉杰什·B·汉杜瓦尔 李路阳 张介中
[74] 专利代理机构 中原信达知识产权代理有限责任公司
代理人 陆锦华 樊卫民
权利要求书 3 页 说明书 15 页 附图 15 页

[54] 发明名称

用于减少数字电缆网络中的欺诈的系统和方法

[57] 摘要

一种数字电缆网络体系结构包括主机，主机包括具有哈稀函数发生器的接收器，哈稀函数发生器根据哈稀函数和来自接收器中的存储模块的数据来计算哈稀值。 策略文件存储器包含策略文件，策略文件具有服务提供商分段、消费者分段和/或制造商分段，其能够由服务提供商、消费者和/或接收器制造商更新。 服务提供商通过电缆媒体下载监视器应用(MA)和策略文件到主机上。 MA 访问策略文件的服务提供商分段、消费者分段和/或制造商分段，以改变资源争夺、服务供应和/或改变欺诈性接收器识别计算。 接收器的哈稀函数输出哈稀值给 MA，其将哈稀值与预期哈稀值进行比较，以识别欺诈性访问。



1. 一种数字电缆网络体系结构，包括：

电缆媒体；

多个主机，包括具有哈稀函数发生器的接收器，哈稀函数发生器根据哈稀函数和来自所述接收器中的存储模块的数据来计算哈稀值；

含有策略文件的策略文件存储器，策略文件具有服务提供商分段、消费者分段和制造商分段的至少一个，其能够分别由所述服务提供商、消费者和/或接收器制造商中的至少一个进行更新；

与所述策略文件存储器相关的服务提供商，所述服务提供商通过所述电缆媒体提供数字电缆服务给所述主机和通过所述电缆媒体下载监视器应用（MA）和策略文件到所述主机上，

其中所述 MA 访问所述策略文件的所述服务提供商分段、所述消费者分段和/或所述制造商分段中的所述至少一个，以进行以下至少一项改变：改变资源争夺、改变低于频道水平的水平上的服务供应和改变欺诈性接收器识别计算，并且其中所述接收器的所述哈稀函数输出所述哈稀值给所述 MA，其将所述哈稀值与预期哈稀值进行比较，以识别欺诈性访问。

2. 如权利要求 1 所述的数字电缆网络体系结构，其中所述哈稀函数发生器通过使用多个可选哈稀函数之一来选择性地进行操作。

3. 如权利要求 2 所述的数字电缆网络体系结构，其中所述 MA 发送哈稀函数选择符给所述接收器，以选择将使用的所述多个可选哈稀函数中的一个。

4. 如权利要求 2 所述的数字电缆网络体系结构，其中所述 MA 发送数据选择符给所述接收器，以从所述存储器中选择将使用的数据块，以产生当前哈稀值。

5. 如权利要求 4 所述的数字电缆网络体系结构，其中，所述当前哈稀值由所述 MA 与所述预期哈稀值进行比较，所述预期哈稀值存储在所述策略文件的所述制造商分段中。

6. 如权利要求 5 所述的数字电缆网络体系结构，其中所述预期哈稀值以表格式存储在所述策略文件的所述制造商分段中且与发送给所述接收器的所述数据选择符和所述哈稀函数选择符相关。

7. 如权利要求 1 所述的数字电缆网络体系结构，其中所述预期哈稀值存储在所述 MA 和所述策略文件的所述制造商分段之一之中。

8. 如权利要求 7 所述的数字电缆网络体系结构，其中所述预期哈稀值被加密。

9. 一种用于操作数字电缆网络体系结构的方法，包括：

将包括接收器的多个主机与服务提供商连接；

将具有服务提供商分段、消费者分段和制造商分段的至少一个的策略文件存储在策略文件数据存储器中，所述策略文件数据存储器与所述服务提供商相关；

允许所述服务提供商、消费者和/或接收器制造商中的至少一个分别更新所述策略文件中的所述服务提供商分段、所述消费者分段和所述制造商分段的至少一个；

下载监视器应用和所述策略文件到所述主机上；

使用所述策略文件的所述服务提供商分段、所述消费者分段和所述制造商分段中的所述至少一个，以进行以下至少一项改变：改变资源争夺、改变低于频道水平的水平上的服务供应和改变欺诈性接收器识别计算；

使用所述接收器的哈稀函数发生器来计算哈稀函数；和

根据所述策略文件中的数据，改变所述接收器中的所述哈稀函数发生器所作出的哈稀函数计算。

10. 如权利要求 9 所述的方法，进一步包括将所述哈稀函数所产生的哈稀值与预期哈稀值进行比较。

11. 如权利要求 10 所述的方法，其中所述预期哈稀值存储在所述 MA 和所述策略文件的所述制造商分段中的至少一个之中。

12. 如权利要求 9 所述的方法，进一步包括：根据所述策略文件的所述制造商分段，发送哈稀函数选择符至所述接收器的所述哈稀函数发生器。

13. 如权利要求 12 所述的方法，进一步包括：根据所述策略文件的所述制造商分段，发送数据选择符至所述接收器的所述哈稀函数发生器。

14. 如权利要求 13 所述的方法，进一步包括：使用所述哈稀函数选择符来选择所述主机的接收器将执行的哈稀函数。

15. 如权利要求 14 所述的方法，进一步包括：使用所述数据选择符来选择接收器存储器中的用于所述所选择的哈稀函数的存储模块。

16. 如权利要求 10 所述的方法，进一步包括：将所述预期哈稀值以表格式以及对应的数据选择符和哈稀函数选择符存储在所述策略文件的所述制造商分段中。

用于减少数字电缆网络中的欺诈的系统和方法

技术领域

本发明涉及电缆网络，更具体地说，涉及数字电缆网络中的提供了改善的平台验证或防欺诈性访问的体系结构。

背景技术

电缆系统运营商按月收取各种服务的费用。电缆系统能够使用模拟和/或数字网络来实现。模拟电缆网络典型地提供有限的服务，例如基本频道和额外收费频道（premium channel）。除了基本服务之外，数字电缆网络还提供了扩展的服务，包括下述的一种或多种：电子节目向导（EPG）、额外收费频道、即时按次收费（IPPV）、视频点播（VOD）、互动式体育节目、游戏节目、诸如电子邮件、聊天和即时消息发送的网络访问和特别报导、互动游戏和/或诸如购物（电视商务或“T-Commerce）”、家庭银行和个人视频记录器（PVR）等服务。

一些消费者可能试图欺诈性地获得一种或多种电缆服务。为了维持收入，服务提供商必须能够减少这种欺诈性访问。切断和/或识别已欺诈性地获取电缆服务的顾客位置将可以帮助减少欺诈性访问。

服务提供商还必须能够以节约成本的方式提供服务供应。在模拟电缆网络中，服务供应是一个昂贵的过程。现在参考图 1，模拟电缆网络 10 包括电缆服务提供商 14，其产生通过电缆 18 的电缆信号。传输线 22-1,22-2...和 22-n 提供电缆信号给位于顾客位置上的电缆盒 26-1,26-2...和 26-n。在顾客位置上，如果该顾客不是订户，则向每个传输线 22 添加一个或多个模拟滤波器 30 用以禁用或者过滤一个或多个额外收费频道。当有订购改变请求时，电缆服务提供商 14 必须分派一组工作人员到顾客所在地。这组工作人员添加或者拆除滤波器 30，

其分别拆除或添加一个额外收费频道。分派工作人员的成本必须包括在额外收费频道的价格中，其增加了对于消费者的成本。

OpenCable™是一种已由电缆运营商定义的标准，使用公共平台提供现成的数字电缆设备。现在参考图 2，OpenCable™标准定义了主机 50，其典型的是机顶盒 50-1 或者集成电视机 50-2。机顶盒 50-1 典型地连接至电视机或者监视器 54。可从主机 50 上拆除的 POD 模块 58 提供了安全性和用户鉴权。POD 模块 58 包括与本地电缆提供商或多个系统运营商（MSO，multiple system operator）60 的专有条件性访问系统有关的功能。POD 模块 58 由 MSO 60 提供且典型地使用 PCMCIA 或 PC 卡来实现。POD 模块 58 可以使用带内频道 64-1 和/或带外（OOB）频道 64-2 通过电缆 64 与 MSO 60 进行通信。

OpenCable™的一个目的是提供便携性。购买主机 50 用于一个电缆系统的消费者能够重新定位另一电缆系统和使用相同的主机 50。OpenCable™还致力于降低服务供应的成本和减少欺诈性访问。OpenCable™应用平台（OCAP™）规范（OC-SP-OCAP1.0-104-021028 和 OC-SP-OCAP2.0-101-020419）（这已完全合并在此作为参考）在制造商的操作系统（OS，operating system）和运行在主机 50 内的各种应用之间提供了开放式接口。目前，交互式电视机（iTV）应用的开发商必须重新为每个专用平台撰写程序。OCAP™提供了标准应用编程接口（API），允许应用部署在所有主机 50 上。

为了允许实现便携性，加密和安全性与主机 50 分开且位于 POD 模块 58 中。当插入主机 50 中时，POD 模块 58 解码来自电缆提供商 60 的加密内容。

OpenCable™提供了基于频道的服务供应。当消费者请求额外收费频道或其它资源时，POD 模块 58 发送消息给电缆提供商 60。如果消费者订购额外收费频道或其它资源，则电缆提供商 60 发送权限消

息（EMM，entitlement message）至 POD 模块 58。如果 EMM 被接收到，则主机 50 被授权可以访问。对于额外收费频道，OpenCable™所提供的控制细度在物理频道的水平上。换言之，额外收费频道被允许或者被禁用。

OCAP™还规定了用于平台验证的机制，其检测主机中的欺诈性和/或有嫌疑的接收器。如在此所使用，平台验证和防欺诈性访问可以互换地使用。证书、签名文件和哈稀文件被嵌入在主机的接收器中。哈稀文件为接收器中的存储模块列举了一组哈稀值。监视器应用（MA，monitor application）通过数据总线读取数据块和计算哈稀值。MA 将所计算的哈稀值与加密文件中规定的哈稀值进行比较。当出现不匹配时，MA 采取适当的动作，例如终止服务和发送通知给 MSO。

用于防止欺诈性接收器的上述机制具有若干缺点。首先，哈稀文件嵌入在接收器中，当未重新编程接收器时，哈稀文件的内容不容易改变。其次，MA 每次都计算同一哈稀值。黑客能够监视用于哈稀计算的主机数据总线。随着时间的流逝，由于这种计算很容易预测，因此，黑客将会得出哈稀函数。。此外，用于 OCAP™规范的 API 已被公布，其包括用于读取闪存的内容的 API。总之，整个固件通过使用这种方法被暴露且欺诈性访问的可能性大大增大了。

此外，OpenCable™标准定义了资源管理器（RM，resource manager），其管理诸如调谐、音频/视频解码、图形平面和后台设备的系统资源。一旦被编程，RM 根据预先设定的默认规则来管理资源争夺，预先设定的默认规则在没有重新编程主机时不能改变。

发明内容

根据本发明的数字电缆网络体系结构包括电缆媒体和多个主机，多个主机包括具有哈稀函数发生器的接收器，哈稀函数发生器根据哈稀函数和来自接收器中的存储模块中的数据来计算哈稀值。策略文件

存储器包含策略文件（PF，policy file），策略文件具有服务提供商分段，消费者分段和制造商分段的至少一个，其能够由服务提供商、消费者和/或接收器制造商更新。与策略文件存储器相关的服务提供商通过电缆媒体提供数字电缆服务给主机和通过电缆媒体下载监视器应用（MA）和策略文件到主机上。MA 访问策略文件的服务提供商分段、消费者分段和/或制造商分段，以改变资源争夺、改变低于频道水平的服务供应和/或改变欺诈性接收器识别计算。接收器的哈稀函数输出哈稀值给 MA，其将哈稀值与预期的哈稀值进行比较，以识别欺诈性访问。

在其它特征中，哈稀函数发生器通过使用多个可选哈稀函数之一来选择性地进行操作。MA 发送哈稀函数选择符（hash function selector）给接收器，以选择将使用的多个可选哈稀函数中的一个。MA 发送数据选择符（data selector）给接收器，以从存储器中选择将使用的数据块，以产生当前哈稀值。当前哈稀值由 MA 与预期哈稀值进行比较，预期哈稀值存储在策略文件的制造商分段中。

在其它特征中，预期哈稀值以表格式存储在策略文件的制造商分段中且与发送给接收器的数据选择符和哈稀函数选择符相关。预期哈稀值存储在 MA 和策略文件的制造商分段之一之中。预期哈稀值被加密。

本发明的其它应用领域将从下面的详细描述变得显而易见。应当理解，示出本发明的优选实施例的详细描述和具体示例只是示出性的且不是对本发明的范围的限制。

附图说明

根据下面详细的描述和附图，本发明将变得更加容易理解。在附图中：

图 1 是示出了根据现有技术的模拟电缆网络中的服务供应的功能

框图；

图 2 是示出了根据现有技术的数字电缆网络中的服务供应的功能框图；

图 3 是示出了根据本发明的数字电缆网络中的服务供应的功能框图；

图 4 是更加详细地示出图 3 中的主机的功能框图；

图 5 是示出了根据现有技术的服务供应的一个示例的功能框图；

图 6 是示出了根据本发明的使用策略文件（PF）和监视器应用（MA）的服务供应的功能框图；

图 7 是示出了根据本发明的使用 PF 和 MA 的资源争夺解决方案的功能框图；

图 8 是示出了根据本发明的用于更新 MA 和 PF 的步骤的流程图；

图 9A 和 9B 是示出了根据本发明的用于资源争夺解决方案的步骤的流程图；

图 10 示出了服务供应示例；

图 11A 是示出了根据现有技术的欺诈性访问识别系统的功能框图；

图 11B 示出了根据现有技术的欺诈性访问识别方法；

图 12A 是示出了根据本发明的第一欺诈性访问识别系统的功能框图；

图 12B 示出了根据本发明的第一欺诈性访问识别方法；

图 13A 是示出了根据本发明的第二欺诈性访问识别系统的功能框图；和

图 13B 示出了根据本发明的第二欺诈性访问识别方法。

具体实施方式

下面对优选实施例的描述只是示例性的且不是对本发明、其应用或使用的限制。为了清楚的目的，在附图中使用相同的参考数字来表示类似的元件。

本发明公开了一种用于数字电缆服务的开发式体系结构。监视器应用（MA）由 MSO 周期性地更新。MA 访问策略文件（PF），其包括消费者、MSO 和/或制造商分段。这些分段能够分别由消费者、MSO 和制造商改变。策略文件允许消费者、MSO 和制造商定制其各自的接口，而无需重新编程主机、接收器等。

例如，消费者能够使用 PF 的消费者分段，以在低于当前提供的频道水平的水平上提供附加的内容、时间和/或金钱控制，例如操作时间、节目内容、游戏内容、频道、花费的美元和其它细节。例如，MSO 能够使用 PF 的 MSO 分段来更新资源争夺默认设置，例如状况、业务关系或其它条件命令。例如，制造商能够使用 PF 的制造商分段来随时间改变平台验证计算，以避免黑客的欺诈性使用。

现在参考图 3，数字电缆网络 100 提供数字电缆服务给多个主机 102-1,102-2,....和 102-n。主机 102 能够是机顶盒、集成 TV 或任何其它类型的主机。主机 102 包括可拆除的 POD 模块 104-1,104-2,....和 104-n，其处理安全性和加密。分别使用带内和带外频道 108-1 和 108-2，POD 模块 104 通过电缆媒体 108 将主机 102 与 MSO 连接。主机 102 可以可选地包括网络浏览器 112。

MSO 120 包括策略文件（PF）管理器 122，其管理 PF 数据存储器 124，其含有用于数字电缆网络 100 中的主机的 PF。每个 PF 优选地包括一个或多个分段。PF 的第一或消费者分段用于消费者。例如，消费者可以使用消费者分段来提供具有额外细度的服务供应。PF 的可选第二分段用于 MSO。例如，MSO 可以使用 MSO 分段来限定用于主机应用的资源许可设置和解决主机应用之间的资源争夺。PF 的第三可选分段用于制造商。制造商分段可以用于周期性地修改欺诈性识别技术。PF 的分段可以由各分段“所有者”针对每个主机 102 进行修改。换言之，制造商能够修改制造商分段，消费者能够修改消费者分段，且 MSO 能够修改 MSO 分段。

MSO、消费者和/或制造商可以以若干不同的方式访问 PF。包括网络浏览器 128 的计算机 126 能够通过诸如互联网的分布式通信系统 130 访问 PF。与 MSO 相关的网络服务器 132 与 PF 管理器 122 接口，以改变 PF。具有网络浏览器 112 的主机 102 可以通过电缆 108 使用电缆调制解调器和/或使用其它互联网访问方法来访问 PF。当对存储在 PF 管理器 122 中的 PF 进行改变时，MSO 120 将 PF 推至对应的主机 102。或者，MSO 120 通知主机 102 新 PF 版本可用。MSO 优选地使用加密设备 134 对 PF 加密且使用数据转发器（head end gear）136 发送 PF。上述的其它服务 140 也通过数据转发器 136 在电缆 108 上提供。

现在参考图 4A，更加详细地示出了主机 102。当初始与数字电缆网络 100 连接时且在接收（或拥有）常驻 MA（MA）150 之前，主机 102 由存储在存储器 153 中的执行应用程序（EA，executive application）152 控制，存储器 153 可以包括只读存储器、FLASH 存储器或任何其它合适的电子数据存储器。

接收器 154 监视存储器 153 中的扩展应用信息表（XAIT）156。MSO 120 使用 XAIT 156 通知接收器 154 MA 150 的当前版本。接收器 154 检测当前 MA 版本（或没有 MA）和 XAIT 156 中的当前 MA 版本之间是否不匹配。如果出现版本不匹配，则接收器 154 读取虚拟频道表（VCT）160，其识别用于接收 MA 150 的物理频道。接收器 154 调谐到规定的物理频道且接收 MA 150。MSO 120 以连续循环的方式、以预定时间的方式、或者以任何其它合适的方式在规定频道上广播 MA 150。在接收到 MA 150 和将其存储在 FLASH 中之后，主机 102 开始使用 MA 150 进行操作。

在下载 MA 时，MSO 120 可以将 PF 推到主机 102 上。或者，MA 120 可以包括一个例行程序，以在新 MA 或新 MA 版本被下载和存储在 FLASH 中时自动下载当前 PF。MSO 120 还在 PF 发生变化的任何

时候自动下载 PF 至主机 102。MSO 120 优选地在发送之前使用加密设备 134 加密 PF。MA 150 解密 PF 且将 PF（示出为 164）存储在存储器 153 中。

MSO 120 可以可选地使用 XAIT 156 通知接收器 154 PF 的当前版本。当接收器 154 检测到 PF 164（或没有 PF）的当前版本与 XAIT 156 中的当前 PF 版本之间的不匹配时，接收器 154 与 MSO 120 联系且请求较新的 PF 版本。MSO 120 发送较新的 PF 版本给 MA 150，MA 150 解密 PF 且使用较新 PF 版本开始进行操作。或者，当制造商、MSO 和/或消费者改变 PF 时，MSO 120 能够自动地下载新 PF 至 MA 150。

消费者可以使用遥控（RC）168（其产生 RC 接收器 169 接收的信号）选择电缆频道、游戏或其它内容。消费者还可以使用集成 TV 102-2、机顶盒 102-1 或显示器 172 上的面板控制器 170 选择电缆频道、游戏或其它内容。消费者还可以使用相同或其它控制器调节音频输出 176 和与其它输入/输出设备 178 接口。

资源管理器 180 管理诸如调谐器 184、图形面板 186、音频/视频解码器 188、后台设备 190 的主机资源 182 和任何其它资源。资源管理器 180 管理应用 192 对资源 182 的争夺，例如电子节目向导（EPG）、额外收费频道、即时按次收费（IPPV）、视频点播（VOD）、互动体育节目、游戏节目、诸如电子邮件、聊天和即时消息发送的网络访问和特别报导、互动游戏和/或诸如购物（电视商务或“T-Commerce）”、家庭银行和个人视频记录器（PVR）。事件管理器（EM）194 使用一个或多个表来处理事件，如下面的描述。在图 4B 中，PF 164 可以包括 MSO 分段 196、制造商分段 198、消费者分段 199 和/或其它分段。

现在参考图 5，示出了根据现有技术的服务供应的一个示例。RC 168 发送频道改变请求，其由 RC 接收器 169 接收。频道改变请求通过数据总线发送给事件管理器 194。事件管理器 194 包括应用表，例

如 EPG 192-1、APP1 和 APP2，其已登记用于频道改变事件。事件管理器 194 发送频道改变事件给 EPG 192-1、APP1 和 APP2。

如果需要，EPG 192-1 从 RM 180 请求调谐器 184。如果 EPG 192-1 已具有调谐器 184 资源，则 EPG 192-1 调用调谐 API。在 POD 104 解码该频道之前，POD 104（其收听调谐 API）发送用于合适频道的 request_channel_access 消息给 MSO 120。如果被允许，则 MSO 120 发送 EMM 至 POD 104，其解码该频道。如果 EMM 未被接收到，则该频道被调谐而不是被解码。如上所述，这种服务供应方法只提供频道水平上的访问。

现在参考图 6，示出了根据本发明的服务供应的一个示例。MA 150 在授权对频道 182 的访问之前查询 PF 164。MA 150 可以访问特权 API，例如应用过虑和升级、系统重启、资源冲突、事件处理、错误处理和系统功能。在优选实施例中，PF 是基于 XML 的程序，其通过 POD OOB 连接下载至 FLASH 存储器中，并且 MA 是基于 Java 的。尽管公开了 XML 和 Java，但是也可以使用任何其它合适的语言。

MA 150 是具有特权的无界应用。MA 150 管理所有 OCAP™应用（包括其自身）的寿命周期。MA 150 提供资源争夺，在应用数据库中登记无界应用、验证所有启动的应用、识别系统错误和重启系统。MA 150 能够使用 OCAP™接口改变版权保护位和输出分辨率。MA 150 还可以过滤用户输入事件和在将它们发送至其各自的目的地之前改变它们的值。因此，MA 150 能够启动或禁用 RC 168 或其它控制器 170 上的键，其对应启动和禁用功能。

在图 6 中，RC 168 发送频道改变请求，其被 RC 接收器 169 接收。频道改变请求通过总线发送给事件管理器 194。事件管理器 194 包括已登记用于频道改变事件的应用表。MA 150 能够覆写事件管理器 194 中的 APP/Event 表。虽然图 6 所示的表示出了包括用于频道改变事件

的 MA 150 而不是 EPG、APP1 和 APP2 的表，该表无需被覆写，如图所示。MA 150 可以简单地覆写表中的当前值或者禁用用于这些事件和应用的 EM。

事件管理器 194 发送频道改变请求给 MA 150。MA 150 查询 PF 164。如果 PF 164 允许消费者选择频道（和/或其它内容和/或其它资源），则 MA 转发频道改变请求至 EPG 192-1。或者，MA 能够指示 EM 将该频道改变请求直接转发给 EPG 192-1。操作继续进行，如上面参考图 5 所述。

现在参考图 7，本发明还允许资源访问由 MA 150 和 PF 164 控制。在授权访问给一个资源之前，MA 150 检查 PF 164。如果 PF 164 允许应用 192 访问该资源，则 MA 176 发送 access_approved 信号至 RM 174。否则，MA 176 发送 access_denial 信号至 RM 174。

MA 150 还根据 PF 164 解决资源争夺。应用 192-3 当前可以具有诸如调谐器 184、图形面板 186、音频/视频解码器 188、后台设备 190 的资源和/或任何其它资源。应用 192-2 可以请求应用 192-3 当前所使用的资源。应用 192-4 当前可以具有诸如调谐器 184、图形面板 186、音频/视频解码器 188、后台设备 190 的资源和/或任何其它资源。应用 192-5 可以请求应用 192-4 当前所使用的资源。MA 150 和 PF 164 解决冲突。

MA 150 和 PF 164 可以根据业务关系解决资源争夺。换言之，MSO 120 可以以满足业务合作伙伴的方式来限定 PF 164 的 MSO 分段 196，以解决资源争夺。例如，当第一应用请求资源调谐到诸如 Speed™的特定频道和诸如浏览器的另一应用请求调谐器用于其它原因（和/或已具有该资源），则第一应用将接收该资源。

现在参考图 8，在 200 一般地示出用于下载 MA 和 PF 的示例性

方法。控制器从步骤 202 开始。在步骤 204 中，控制器确定主机是否包括常驻 MA。如果没有，则在步骤 206 中，控制器运行执行应用程序（EA）。在步骤 208 中，控制器检查 XAIT 和 VCT 且在指定频道上从 MSO 下载 MA。步骤 208 可以通过使主机给 MSO 发送一个 need_MA 消息来执行。MSO 通过发送该 MA 来对 need_MA 消息进行响应。主机将 MA 存储在存储器中，然后将 MA 加载到 FLASH 存储器中。如果 MA 是常驻的，则在步骤 214 中，控制器运行该 MA。

在步骤 218 中，主机可以确定 PF 是否是最新版本。如果没有出现版本匹配，则在步骤 220 中，主机下载 PF。步骤 220 可以通过使主机给 MSO 发送 need_latest_PF 消息来执行。MSO 通过发送最新 PF 版本来对 need_latest_PF 消息进行响应。主机将 PF 存储在存储器中和将 PF 加载到 FLASH 存储器中。或者，当出现对 PF 的改变时，MSO 可以自动地发送 PF。

控制器继续进行到步骤 224，其中主机确定 MA 是否是最新版本（典型地使用 XAIT）。如果 MA 不是最新版本，则在步骤 228 中，主机调谐到 VCT 所识别的频道且下载最新 MA 版本。步骤 224 和 228 可以以类似于上述步骤 218 和 220 的方式来执行。在步骤 230 中，主机使用 MA 和 PF 来管理资源。

现在参考图 9A，在 280 一般示出了使用 PF 164 用于管理资源争夺的方法的步骤。控制器从步骤 282 开始。在步骤 284 中，控制器确定应用（APP）是否已请求一个资源。如果没有，控制器返回步骤 284。如果 APP 请求一个资源，则控制器继续到步骤 286，其中 RM 确定是否有对资源的争夺。如果没有，则在步骤 288 中，RM 授权该应用可以使用该资源且继续进行到步骤 284。否则，RM 发送消息给 MA。在步骤 292 中，MA 依次读取 PF，以通过 PF 确定资源争夺是否得到解决。例如，PF 的 MSO 分段可以根据业务关系标准来解决争夺。

在步骤 294 中，MA 发送资源争夺解决方案给 RM。或者，PF 可以直接发送资源争夺解决方案给 RM。如果 PF 没有解决该争夺，则 MA 可以解决该争夺和/或发送 not_covered 消息。在 not_covered 情况中，RM 可以使用默认规则来解决资源争夺。在步骤 296 中，RM 解决该争夺。

现在参考图 9B，即使没有争夺，RM 也可在授权对资源的访问之前与 PF 协商。在步骤 302 中，RM 与 MA 协商（其与 PF 协商），以确定 PF 是否允许该应用使用该资源。如果不允许，则在步骤 304 中，RM 拒绝该应用使用该资源。

根据本发明的 PF 和 MA 实现在数字电缆网络 100 中实现对服务供应和改善资源争夺的精确控制。PF 和 MA 使服务供应比 OCAP™规范所提供的频道水平具有更精确的细度。

现在参考图 10，示出了一个示例性实现方式。单个消费者住宅包括 STB_1、STB_2 和 STB_3。STB_1 位于诸如父母卧室的受控环境中。STB_2 位于一个孩子的卧室中。STB_3 位于另一个孩子的卧室中。

根据本发明的服务供应允许高于频道水平的控制。具体地说，STB_1 被 MSO 和消费者 PF 授权在任何时候完全访问基本频道、三个额外收费频道和游戏。STB_2 和 STB_3 也被 MSO 授权在任何时候完全访问基本频道、三个额外收费频道和游戏。但是，消费者 PF 在某些时候限制 STB_2 访问基本频道，在某些时候访问一些额外收费频道，在某些时候访问其它额外收费频道和访问没有暴力内容的游戏。消费者 PF 在某些时候限制 STB_3 访问基本频道，在某些时候在某个等级水平上访问一些额外收费频道，在某些时候访问所有游戏。消费者还可以对所有服务和/或单个服务的花费设限。

从上面所述可以理解，根据本发明的数字电缆系统提供了具有更

小细度的控制。数字电缆系统允许创建等级式的服务。可以使用 MA 来搜集使用统计数字，其能够由消费者使用，用于服务供应。例如，消费者能够设置按次收费或游戏服务的花费上限和/或在互联网上浏览的总时间。节目等级水平也可以由消费者控制。

此外，MSO 可以远程地禁用或重启主机。例如，在消费者未付款时，在策略文件已受损害时、在主机处于某种被入侵的状态下时或者在 MSO 还未收到 MA 的信跳（heartbeat）时，MSO 可以禁用或重启主机。此外，当消费者具有多个主机时，可以为每个主机定义计费细节。

现在参考图 11A，根据现有技术的 MA 340 包括欺诈控制模块 342，其包括哈稀函数发生器且存储哈稀值。MA 340 通过数据总线 346 读取嵌入在接收器 345 中的哈稀文件 344、证书、和签名。哈稀文件 344 列举接收器 345 内的用于信息块的哈稀值列表。MA 340 的哈稀函数发生器 347 通过数据总线 346 读取数据块且计算哈稀值。欺诈控制模块 342 将所计算的哈稀值与加密文件中的哈稀值 348 进行比较。在出现不匹配时，MA 340 采取合适的动作，例如终止服务和发送通知给 MSO。

现在参考图 11B，控制器从步骤 352 开始。在步骤 356 中，控制器等待 MA、MSO 或制造商所作出的 fraud_check 请求，和/或 fraud_check 请求可以是基于时间的或基于事件的。如果 fraud_check 请求被接收到，则在步骤 358 中，MA 通过数据总线读取数据块且计算哈稀值。在步骤 360 中，MA 将所计算的哈稀值与加密文件中所存储的哈稀值进行比较。在步骤 364 中，控制器确定是否有匹配。如果没有，则 MA 采取合适的动作，例如（但不限于）终止服务、与 MSO 联系或任何其它合适的动作。

应当理解，通过经由所暴露的数据总线 346 发送数据和在 MA 340

中重复计算同一哈稀函数，传统的系统增大了被黑客欺诈性地访问的可能性。

现在参考图 12A，MA 150 包括欺诈控制模块 374，其产生欺诈请求。接收器 154 包括哈稀函数发生器 375，其使用一个或多个哈稀函数产生哈稀值。哈稀函数发生器 375 所使用的存储模块也可以改变。哈稀函数发生器 375 通过数据总线 376 接收哈稀函数请求。哈稀函数发生器 375 使用存储器 377 中的存储模块产生哈稀函数。哈稀函数发生器 375 产生发送给欺诈控制模块 374 的哈稀值。MA 150 中的欺诈控制模块 374 将所产生的哈稀值与存储在 MA 150 或 PF 164 中的加密形式的哈稀值进行比较。该哈稀值可以存储在 PA 的制造商分段中。

现在参考图 12B，在 380 示出了根据本发明的欺诈性访问识别方法。控制器从步骤 352 开始。在步骤 356 中，控制器等待 MA、MSO 或制造商所作出的 fraud_check 请求，和/或 fraud_check 请求可以是基于时间的或基于事件的。如果 fraud_check 请求被接收到，则在步骤 382 中，MA 发送消息给接收器，以计算哈稀值和发送所得的哈稀值给 MA。在步骤 384 中，MA 将所计算的哈稀值与加密文件中和/或 PF 中所存储的哈稀值进行比较。在步骤 364 中，控制器确定是否有匹配。如果没有，则 MA 采取合适的动作，例如（但不限于）终止服务、与 MSO 联系或任何其它合适的动作。

应当理解，通过减少经由暴露的数据总线 346 的数据发送和屏蔽接收器中的哈稀函数计算，根据本发明的欺诈性访问识别系统降低了被黑客欺诈性访问的可能性。

现在参考图 13A，MA 150 包括欺诈控制模块 374，其产生欺诈请求。接收器 154 包括产生多个不同哈稀函数的哈稀函数发生器 375。哈稀函数发生器 375 通过数据总线 376 接收哈稀函数请求。

MA 发送在接收器中实现的识别多个哈稀函数之一的哈稀函数选择符和/或用于选择要使用的存储模块的数据选择符。哈稀函数选择符和数据选择符能够从可行哈稀函数和数据块中随机地选择。哈稀函数发生器 375 使用所选择的哈稀函数和存储器 377 中的所选择的存储模块来产生哈稀函数。哈稀函数发生器 375 产生发送给欺诈控制模块 374 的哈稀值。MA 150 中的欺诈控制模块 374 将所产生的哈稀值与存储且对应于所使用的哈稀值选择符和数据选择符的哈稀值进行比较。哈稀值、哈稀函数识别和/或存储模块可以存储在 MA 150、PF 164 和/或 PF 164 的制造商分段中。

现在参考图 13B，在 400 中示出了根据本发明的欺诈性访问识别方法。控制器从步骤 352 开始。在步骤 356 中，控制器等待 MA、MSO 或制造商所作出的 fraud_check 请求，和/或 fraud_check 请求可以是基于时间的或基于事件的。在步骤 404 中，MA 识别在哈稀函数选择符中所使用的哈稀函数和/或数据选择符 154 中的存储模块。

如 fraud_check 请求被接收到，则在步骤 382 中，MA 发送消息给接收器，以计算哈稀值和发送所得的哈稀值给 MA。在步骤 384 中，MA 将所计算的哈稀值与加密文件中或 PF 中所存储的哈稀值进行比较。在步骤 364 中，控制器确定是否有匹配。如果没有，则 MA 采取合适的动作，例如（但不限于）终止服务、与 MSO 联系或任何其它合适的动作。

应当理解，提高哈稀函数的数目和改变存储模块数目可以增大哈稀值计算的复杂度和减少欺诈性访问的可能性。

本领域技术人员现在从上面的描述中应当理解，本发明的广泛教导可以以各种形式实现。因此，虽然结合具体示例描述了本发明，但是本发明的范围不应当受此限制，因为在研究了附图、说明书和权利要求书之后，本领域技术人员可以进行其它修改。

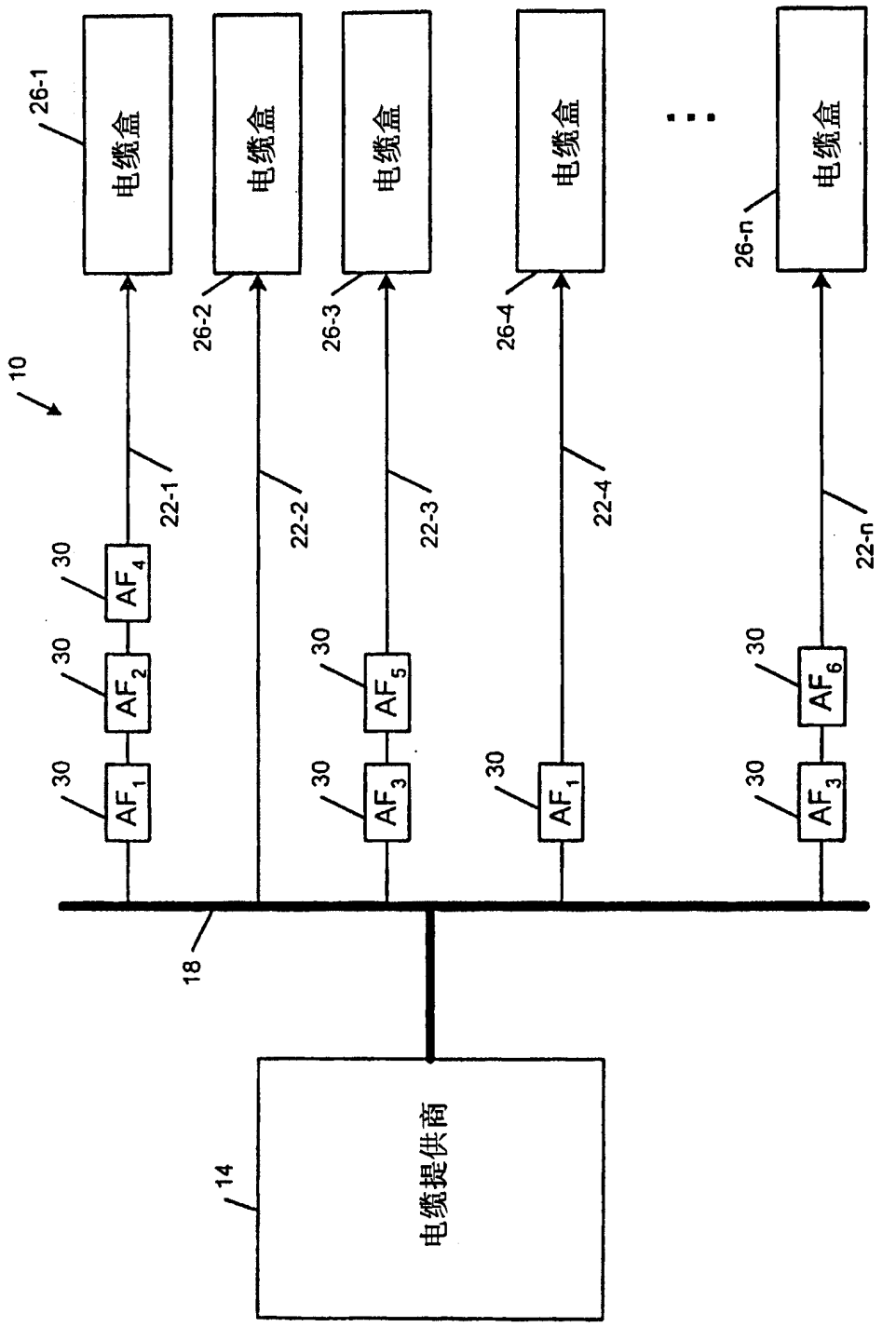

10
26-1
电缆盒
26-2
电缆盒
26-3
电缆盒
26-4
电缆盒
26-n
电缆盒
22-1
22-2
22-3
22-4
22-n
30
AF4
AF2
AF1
AF5
AF3
AF1
AF6
AF3
18
14
电缆提供商

图1
现有技术

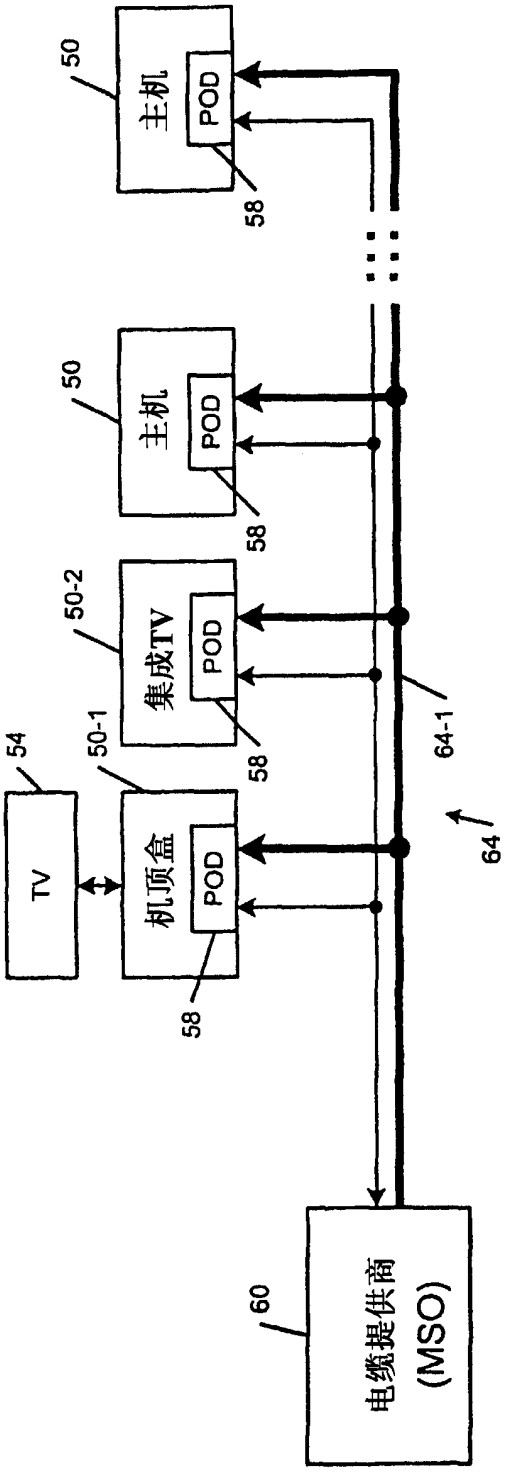

50
主机
POD
58
50
主机
POD
58
50-2
集成TV
POD
58
50-1
机顶盒
POD
58
54
TV
64-1
64
60
电缆提供商
(MSO)

图2
现有技术

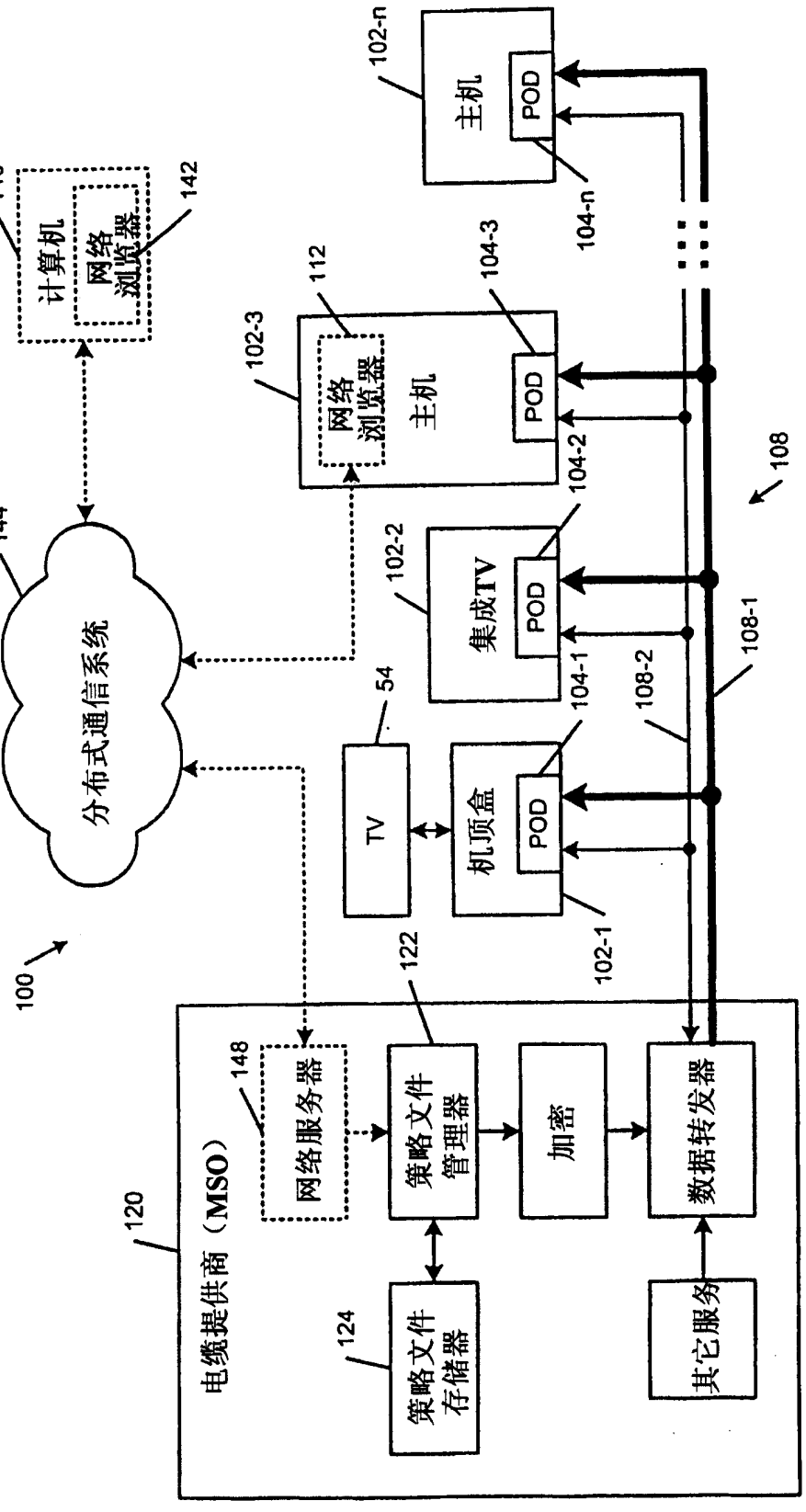

100
分布式通信系统
144
计算机
网络浏览器
140
142
电缆提供商（MSO）
120
网络服务器
148
策略文件管理器
122
加密
数据转发器
策略文件存储器
124
其它服务
TV
54
机顶盒
POD
102-1
104-1
集成TV
102-2
104-2
网络浏览器
112
主机
102-3
104-3
主机
102-n
104-n
108
108-1
108-2

图3

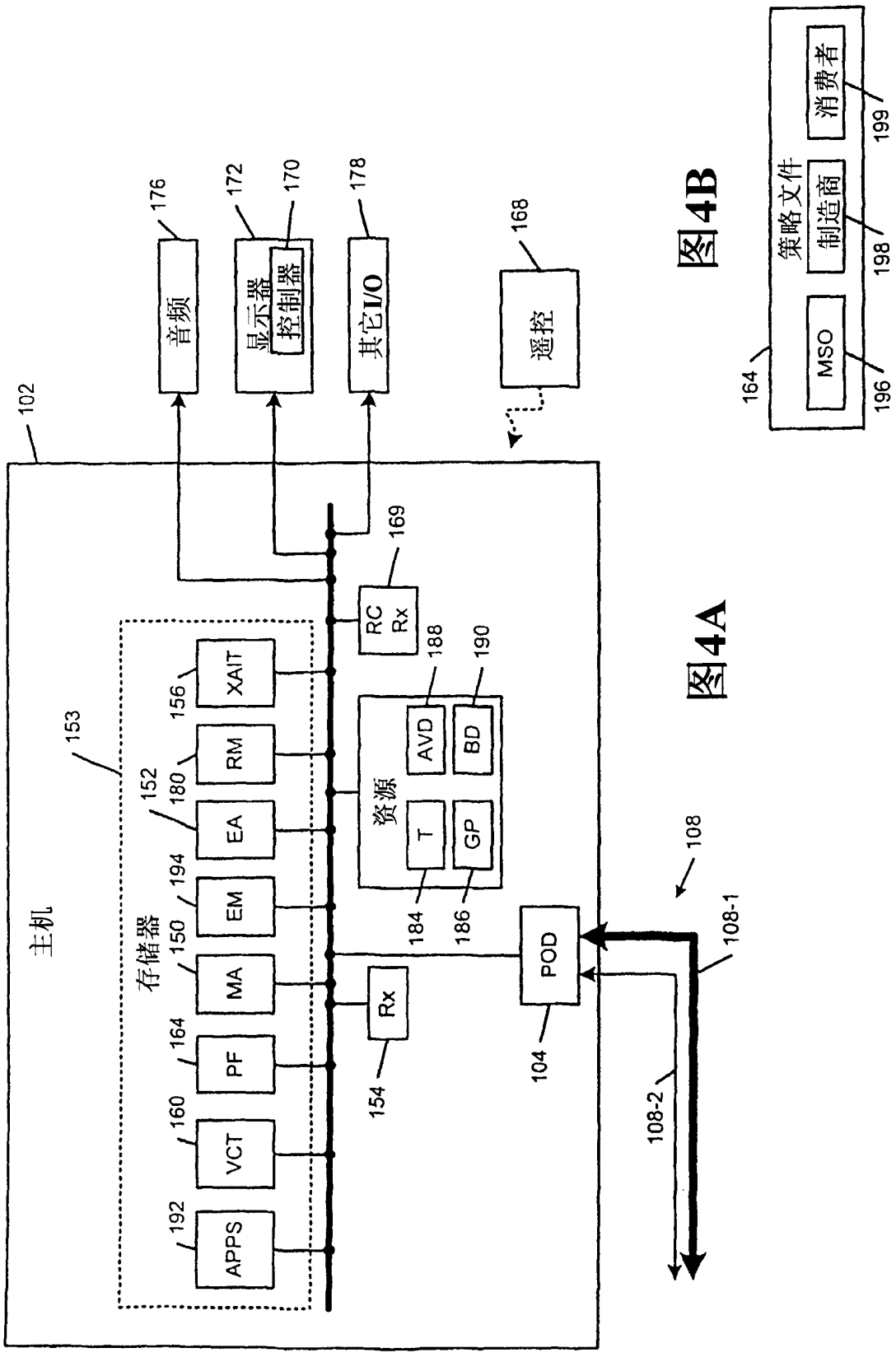

102
主机
153
存储器
152
APPS
192
VCT
160
PF
164
MA
150
EM
194
EA
180
RM
156
XAIT
音频
176
显示器
172
控制器
170
其它I/O
178
遥控
168
RC
Rx
169
Rx
154
资源
AVD
188
BD
190
T
184
GP
186
POD
104
108
108-1
108-2
164
策略文件
MSO
196
制造商
198
消费者
199

图4A

图4B

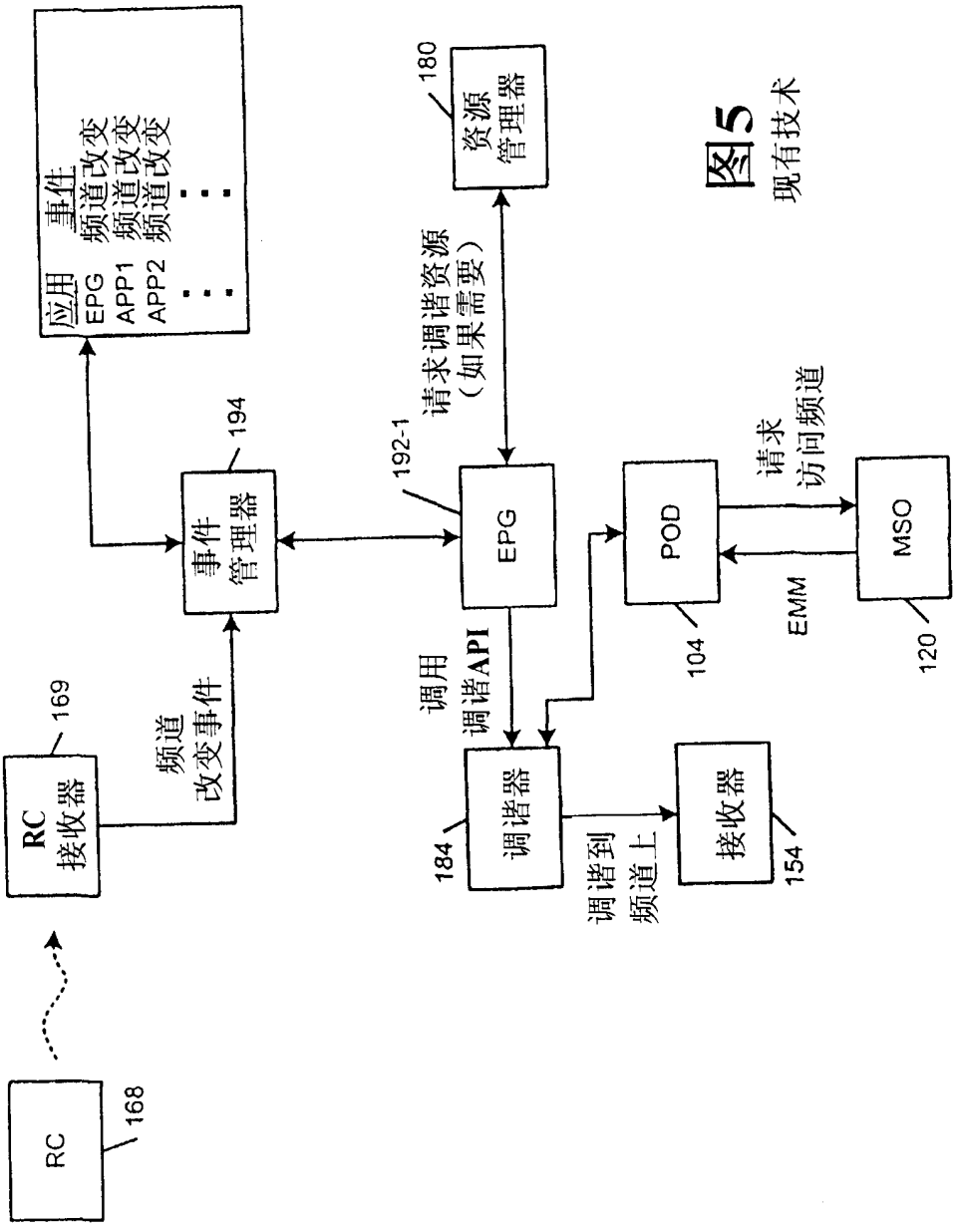

RC
168
RC
接收器
169
频道
改变事件
事件
管理器
194
应用 事件
EPG 频道改变
APP1 频道改变
APP2 频道改变
192-1
请求调谐资源
（如果需要）
资源
管理器
180
EPG
调用
调谐API
调谐器
184
调谐到
频道上
接收器
154
POD
104
请求
访问频道
EMM
MSO
120

图5
现有技术

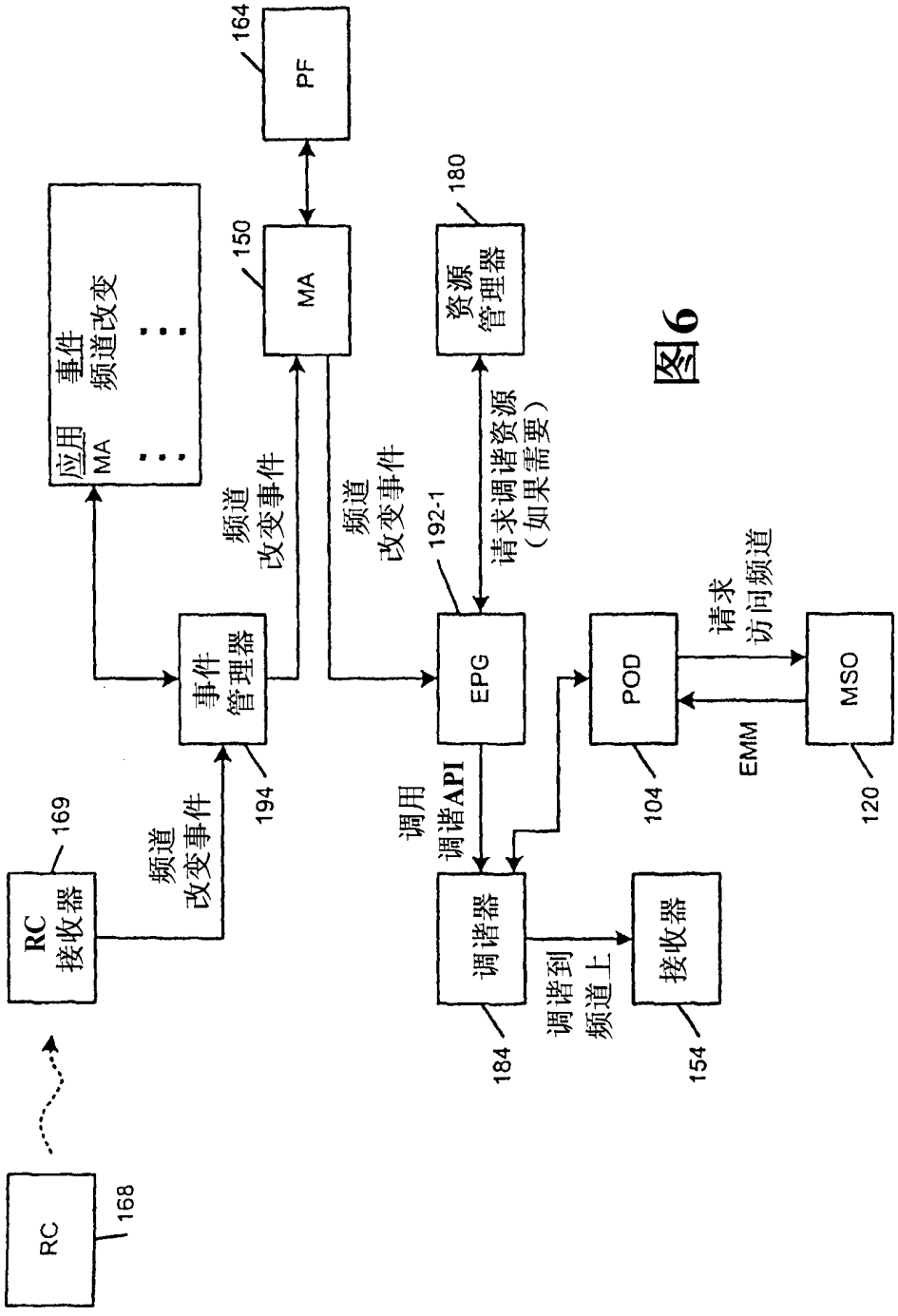

RC
168
RC
接收器
169
频道
改变事件
事件
管理器
194
应用
MA
事件
频道改变
频道
改变事件
MA
150
PF
164
频道
改变事件
192-1
请求调谐资源
（如果需要）
资源
管理器
180
调用
调谐API
EPG
调谐器
184
调谐到
频道上
接收器
154
POD
104
请求
访问频道
EMM
MSO
120

图6

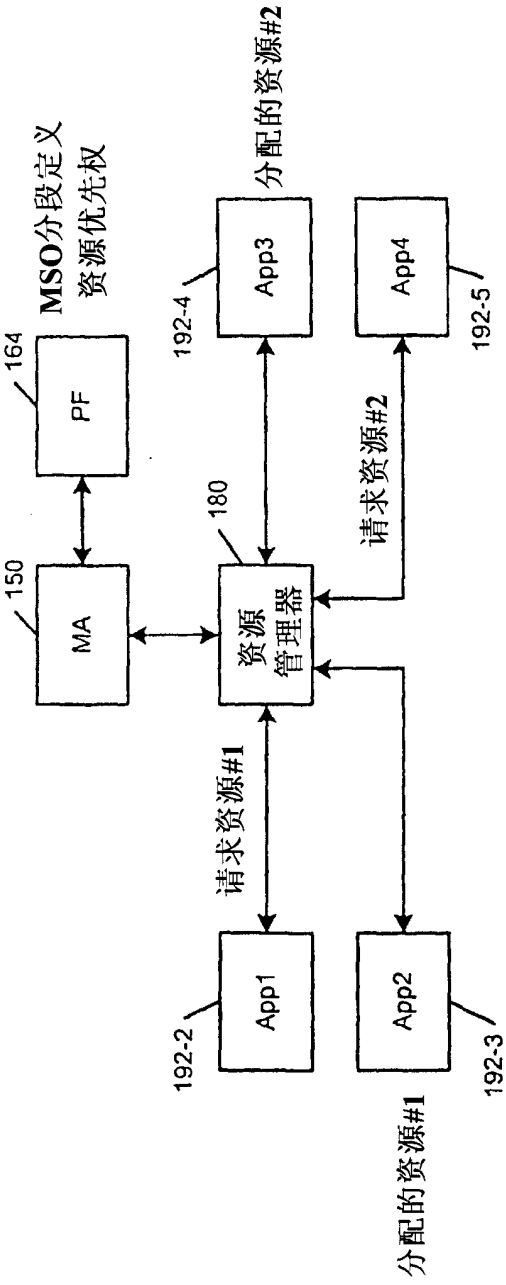

MSO分段定义
资源优先权
164
PF
150
MA
180
资源
管理器
请求资源#1
请求资源#2
192-2
App1
192-3
App2
192-4
App3
192-5
App4
分配的资源#1
分配的资源#2

图7

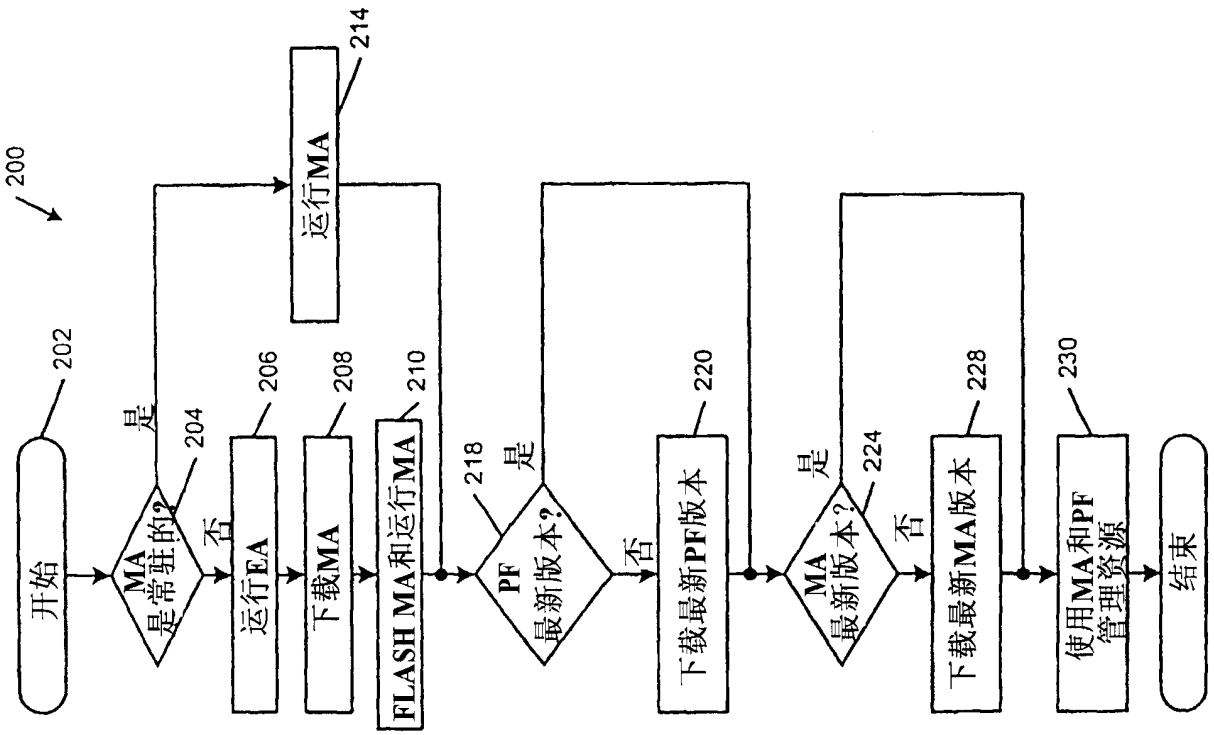

200
开始
202
MA是常驻的?
204
是
否
运行MA
214
运行EA
206
下载MA
208
FLASH MA和运行MA
210
PF最新版本?
218
是
否
下载最新PF版本
220
MA最新版本?
224
是
否
下载最新MA版本
228
使用MA和PF管理资源
230
结束

图8

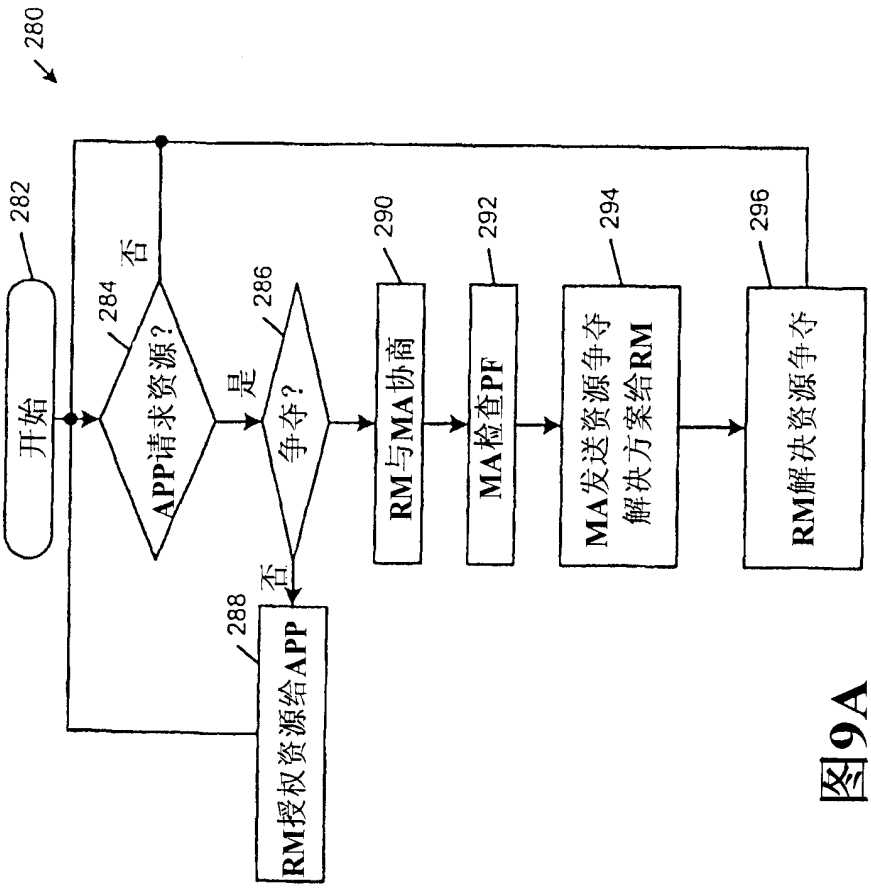

280
开始
282
APP请求资源?
284
否
是
争夺?
286
否
RM授权资源给APP
288
RM与MA协商
290
MA检查PF
292
MA发送资源争夺解决方案给RM
294
RM解决资源争夺
296

图9A

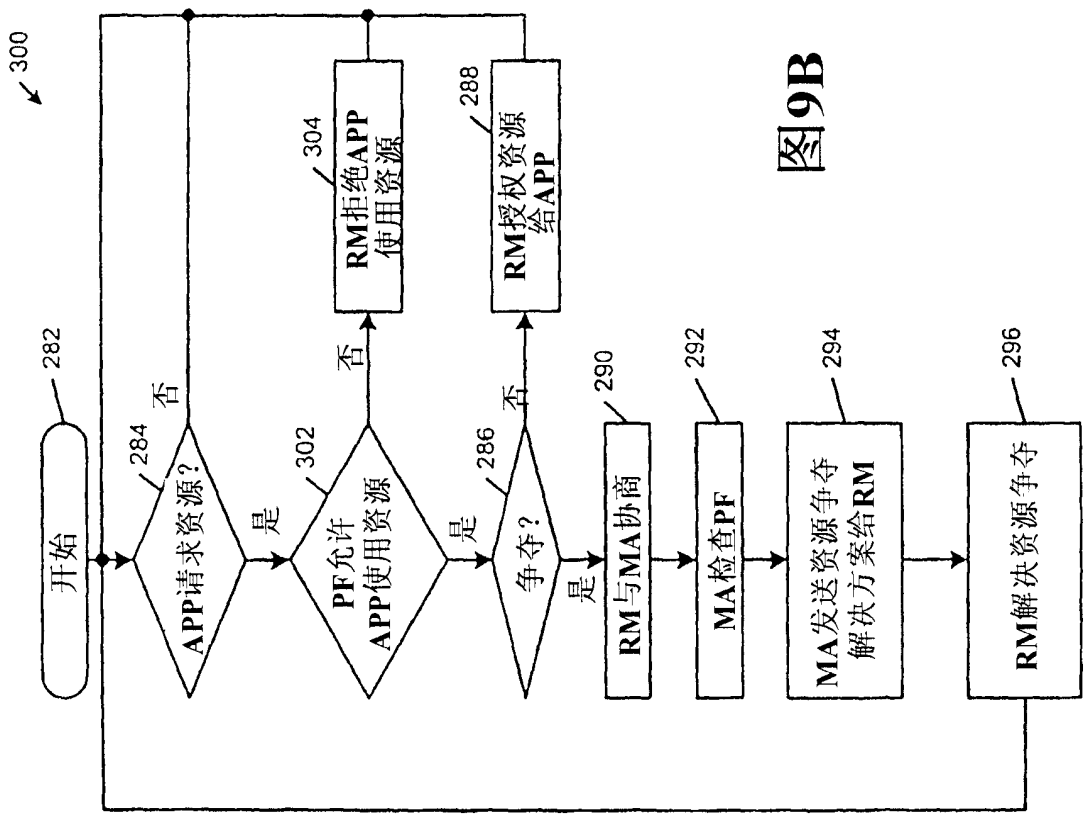

300
开始
282
APP请求资源?
284
否
是
PF允许APP使用资源
302
否
RM拒绝APP使用资源
304
是
争夺?
286
否
RM授权资源给APP
288
是
RM与MA协商
290
MA检查PF
292
MA发送资源争夺解决方案给RM
294
RM解决资源争夺
296

图9B

	STB_1		STB_2		STB_2	
	MSO	消费者	MSO	消费者	MSO	消费者
基本频道	总是	总是	总是	6A-8P	总是	6A-8P
收费频道1	总是	总是	总是	从不	总是	只有6A-8P和G, PG
收费频道2	总是	总是	总是	从不	总是	从不
收费频道3	总是	总是	总是	6A-8P	总是	只有6A-8P和G, PG
游戏	总是	总是	总是	5P-6P; No V	总是	5P-8P

图10

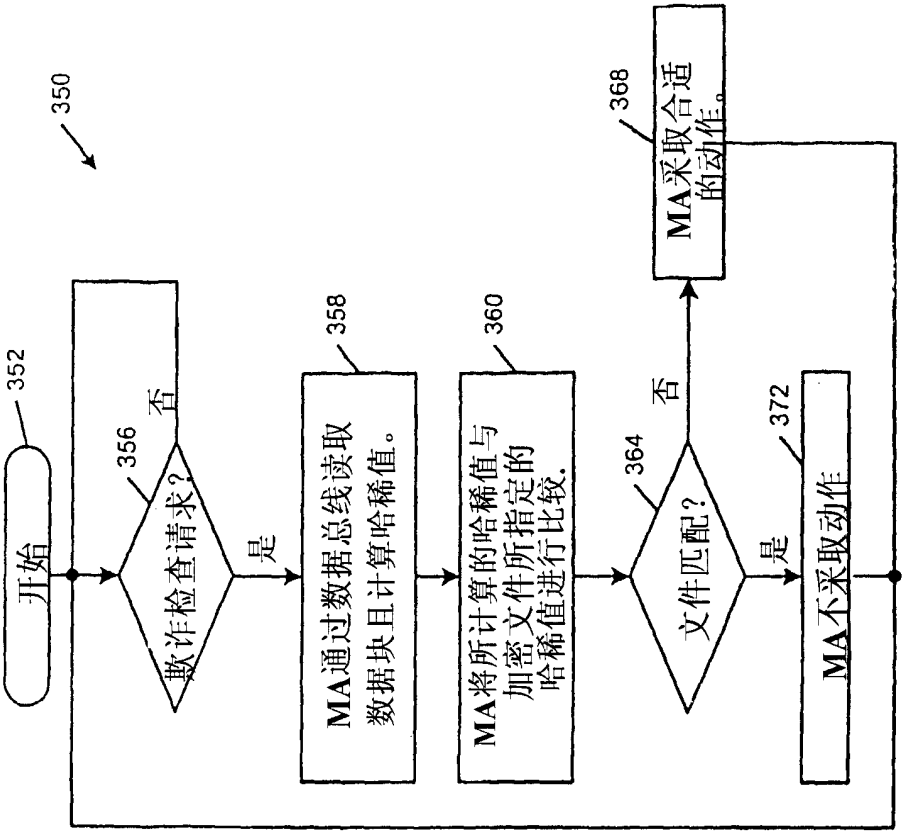


图11B
现有技术

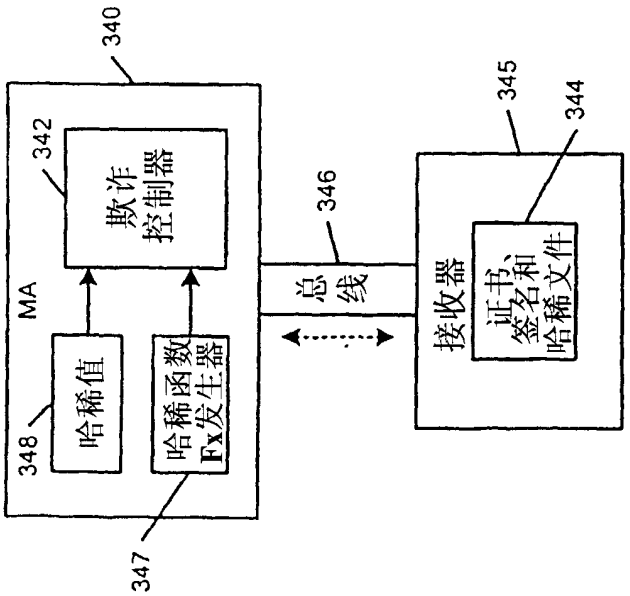


图11A
现有技术

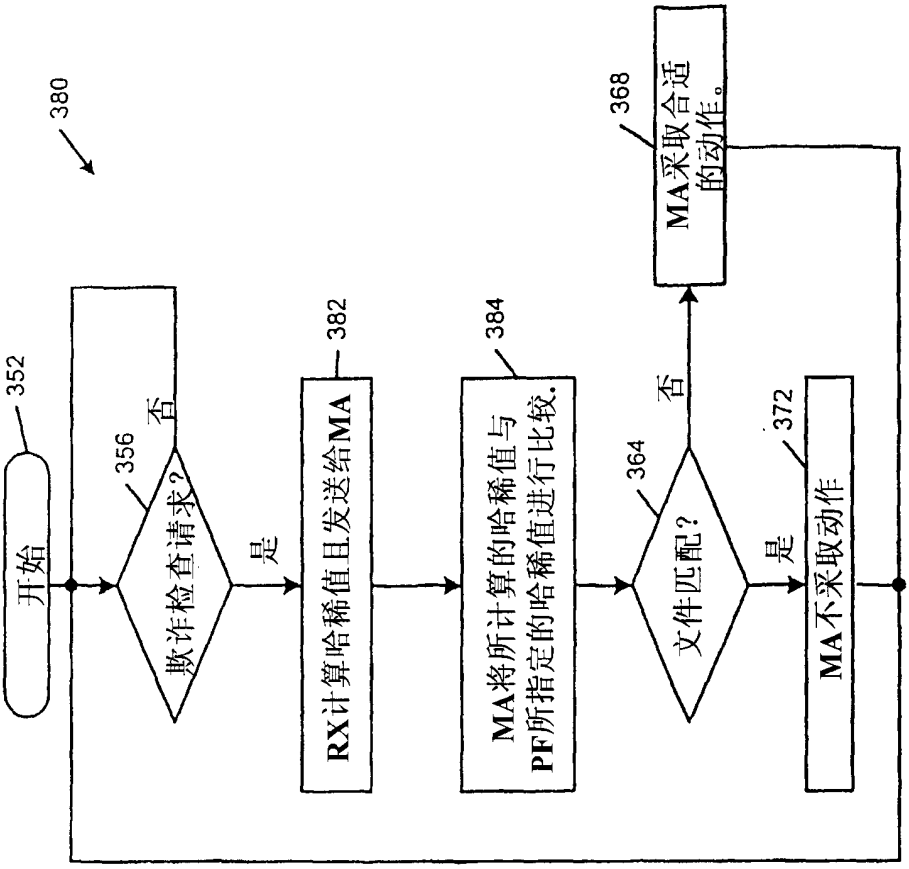

380
开始
352
欺诈检查请求?
356
否
是
RX计算哈稀值且发送给MA
382
MA将所计算的哈稀值与PF所指定的哈稀值进行比较.
384
文件匹配?
364
否
是
MA采取合适的动作。
368
MA不采取动作
372

图12B

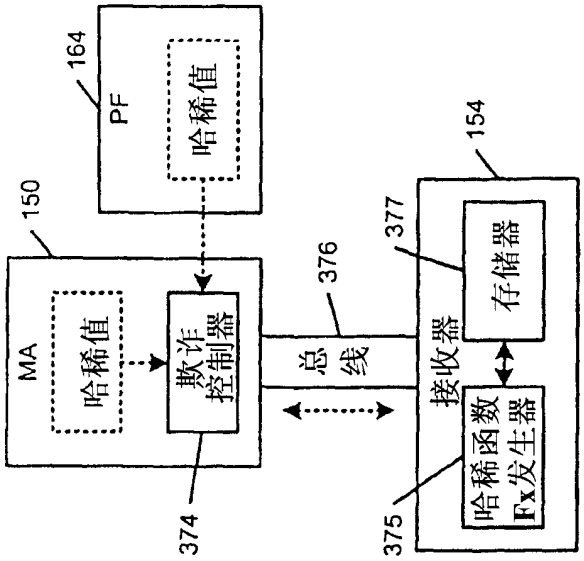

MA
哈稀值
欺诈控制器
150
374
PF
哈稀值
164
总线
376
接收器
377
存储器
154
哈稀函数Fx发生器
375

图12A

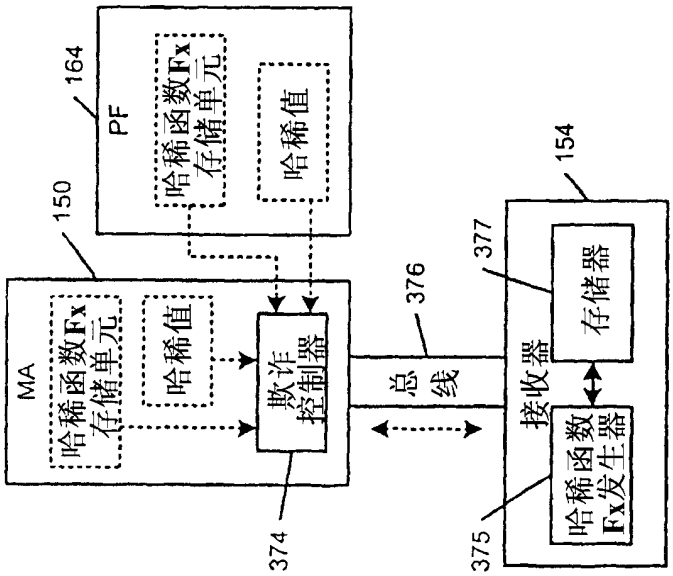

MA
哈稀函数Fx存储单元
哈稀值
欺诈控制器
150
374
PF
哈稀函数Fx存储单元
哈稀值
164
376
总线
377
接收器
存储器
哈稀函数Fx发生器
154
375

图13A

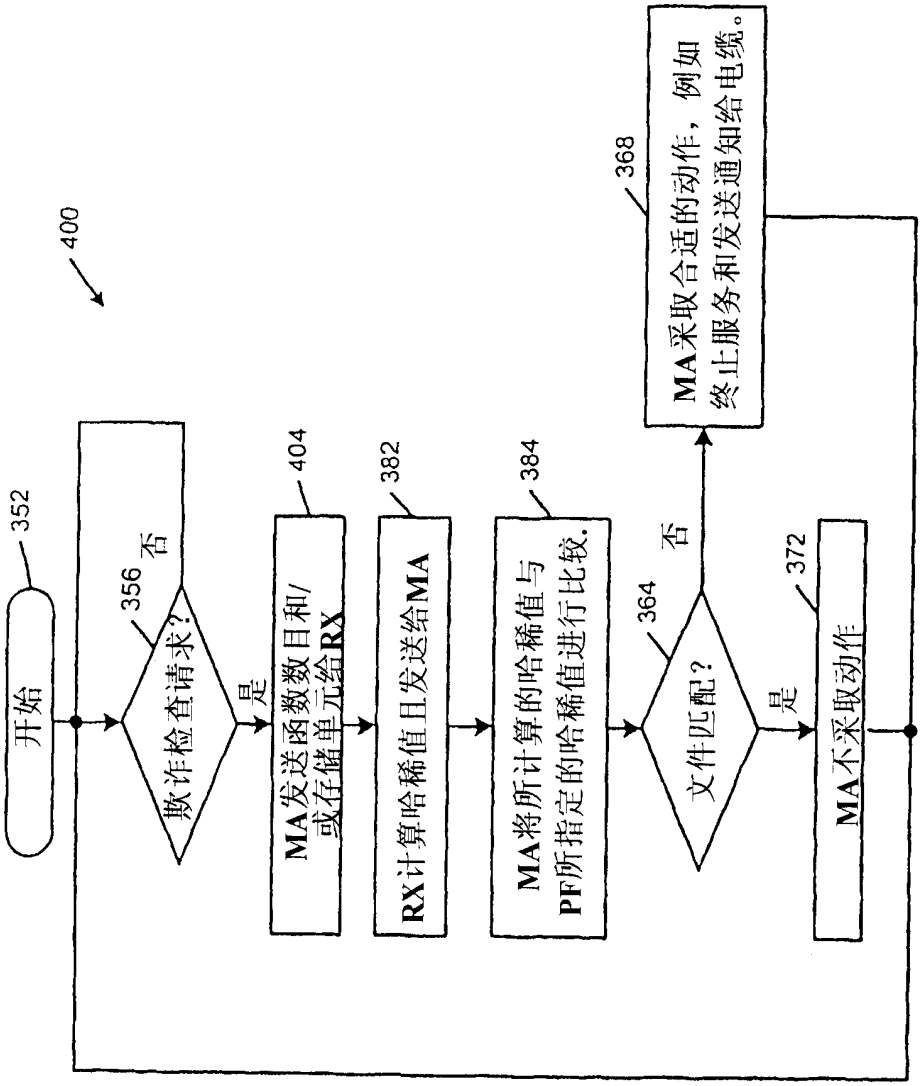

400
开始
352
欺诈检查请求?
356
否
是
MA发送函数数目和/或存储单元给RX
404
RX计算哈稀值且发送给MA
382
MA将所计算的哈稀值与PF所指定的哈稀值进行比较.
384
文件匹配?
364
否
是
MA采取合适的动作，例如终止服务和发送通知给电缆。
368
MA不采取动作
372

图13B