(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101496377 B
(45)授权公告日 2012.07.04

(21)申请号 200780028795.5

(22)申请日 2007.07.26

(30)优先权数据
06118345.5 2006.08.02 EP

(85)PCT申请进入国家阶段日
2009.02.02

(86)PCT申请的申请数据
PCT/EP2007/057717 2007.07.26

(87)PCT申请的公布数据
WO2008/015155 FR 2008.02.07

(73)专利权人 纳格拉影像股份有限公司
地址 瑞士洛桑

(72)发明人 G·莫雷隆

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038

代理人 党建华

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
US 2005/0234735 A,2005.10.20, 说明书第6、9-10、15、29、41段.
US 2006/0112188 A1,2006.05.25, 说明书第64、125段.
WO 2005/036820 A1,2005.04.21, 全文.

审查员 陈罡

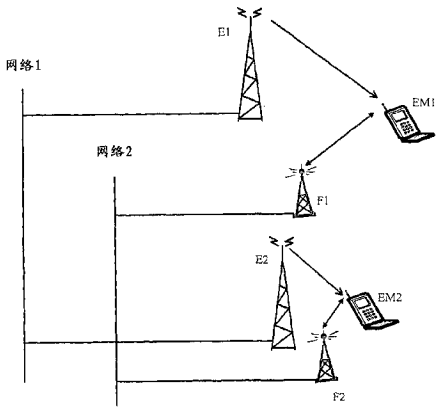
权利要求书 1 页 说明书 4 页 附图 2 页

(54)发明名称

移动设备的本地条件访问方法

(57)摘要

本发明的目的是可在移动领域利用与应用于固定接收机的限制装置相同的限制装置。此目的通过一种对数字数据流进行条件访问的方法实现的,所述数字数据流以至少一个控制字被加密并且通过广播网络中的发射机被广播到至少一个移动设备,所述发射机还发送包含控制字和访问条件的控制消息流,所述移动设备还通过移动接入点连接到移动通信网络,所述方法的特征在于:由移动设备接收控制消息流;根据所述移动接入点的标识符或者广播网络发射机的标识符确定所述移动设备的位置标识符;验证控制消息中包含的访问条件,所述访问条件包括与至少一个移动接入点标识符和/或一个广播网络发射机的标识符相关的接收条件;比较所确定的标识符与所述访问条件中包含的标识符;根据所述比较结果授权或阻止对所述数据流的访问。



CN 101496377 B

1. 一种对数字数据流进行条件访问的方法，所述数字数据流以至少一个控制字被加密并且通过广播网络中的发射机被广播到至少一个移动设备，所述发射机还发送包含控制字和访问条件的控制消息流，所述移动设备还通过移动接入点连接到移动通信网络，所述方法包括如下步骤：

- 由移动设备接收控制消息流，

- 由移动设备根据所述移动接入点的标识符或者广播网络发射机的标识符确定所述移动设备的位置标识符，

- 由移动设备验证控制消息中包含的访问条件，所述访问条件包括与至少一个移动接入点标识符和 / 或一个广播网络发射机的标识符相关的接收条件，

- 比较所确定的标识符与所述访问条件中包含的标识符，

- 根据所述比较结果授权或阻止对所述数据流的访问。

2. 根据权利要求 1 的方法，其中，仅当接收条件包括所述位置标识符时，对所述数据流的访问被授权。

3. 根据权利要求 1 的方法，其中，仅当接收条件不包括所述位置标识符时，对所述数据流的访问被授权。

4. 根据权利要求 1 的方法，其中，所述移动接入点的所述标识符是从接收自所述移动接入点的服务数据中提取的。

5. 根据权利要求 1 的方法，其中，广播网络的发射机标识符是从接收自所述广播网络发射机的服务数据中提取的。

6. 根据权利要求 1 的方法，其中，所述访问条件包括来自所述广播网络的发射机标识符列表。

7. 根据权利要求 1 的方法，其中，所述访问条件包括移动接入点标识符列表。

8. 根据权利要求 1 的方法，其中，所述访问条件包括与广播内容相关的至少一个权利描述，并且移动设备验证此权利的存在来授权或阻止对内容的访问。

9. 根据权利要求 1 的方法，其中，所述移动设备包括负责处理访问条件的安全装置。

10. 根据权利要求 1 的方法，其中，所述移动通信网络根据 GSM、GPRS、UMTS、WiMax、Wifi、Wibro 中的一种类型而被选择。

11. 根据权利要求 1 的方法，其中，所述访问条件中包含的标识符限定位置标识符的范围。

12. 根据权利要求 1 的方法，其中，所述位置标识符被签名，并且移动设备在与访问条件中包含的标识符比较之前验证标识符签名。

13. 根据权利要求 1 的方法，其中，所述移动设备包括被视为访问条件中包含的标识符的一部分的默认标识符，如果没有引入其它标识符将导致阻止对所述数据流的访问。

14. 根据权利要求 13 的方法，其中，持续期与由移动设备接收标识符相关联，此持续期期满后所述默认标识符被重建。

移动设备的本地条件访问方法

技术领域

[0001] 本发明涉及对由无线电链路广播并由多个移动设备接收的数字数据流的条件访问领域，其中移动设备的例子是，移动电话、个人数字助理 PDA(PersonalDigital Assistant)、便携式数字电视接收机、便携式计算机。

[0002] 广播数据被加密并且仅授权设备能清楚地接收，所述授权设备的用户已购买了必需的权利。这些权利保存在与所述移动设备相关联的安全模块中，由一组密钥组成，这些密钥允许对音频 / 视频数据流中广播的 ECM 控制消息（权利控制消息）中包含的控制字解密。

[0003] 安全模块是公知的防篡改设备，包括各种加密 / 解密密钥、用于识别网络上的用户的信息以及限定用户为接收广播内容所购买的权利的数据。所述安全模块可以以不同形式存在，例如插入读卡器中的可移动智能卡、焊在母板上的集成电路、嵌入了安全芯片的存储卡 (SD 或 MMC)、能够在大多数移动设备中找到的 SIM（用户识别模块）类型的卡。

[0004] 这个模块可以以软件形式实现，并且可以是移动设备软件的一部分。优选地，这个软件将在存储器中的特定区域运行、以最小化与其它软件的干扰。

背景技术

[0005] 目前，为了接收数字电视节目而配置的移动设备是基于标准技术的，例如 OMA（开放移动联盟）、DVB-H（数字视频广播，手持），或者作为 DAB（数字音频广播）的一种宽带扩展方式的 DMB（数字多媒体广播）。

[0006] 所述 OMA 技术对于例如便携电话市场的特定市场实施单一的完整解决方案，其中所有设备和内容提供商均实施 OMA 技术。

[0007] DVB 技术原本为标准化数字电视解码器（机顶盒）而设计以大幅度减少它们的成本。该技术对条件访问因特网上的移动电视的 MPEG-2 或者 MPEG-4 格式的内容广播时所包括的要素进行标准化。这些要素包括广播内容的加密算法、包括解密密钥或控制字的 ECM 控制消息、包括用户权利的 EMM 管理消息、以及解码器与管理条件访问的安全模块之间的接口。

[0008] 在 DVB-H 移动电视的特定情况中，内容保护由 DVB-CBMS 团体（数字视频广播 - 广播和移动业务融合）开发。

[0009] 所述标准化既不包括 ECM 和 EMM 消息的增值内容，也不包括保护所述消息的方法。每个条件访问的提供者使用其自身的数据结构和其自身的保护手段以用于特定广播内容。从而 DVB 技术提供多个可能性以用于开发内容安全性。

[0010] 众所周知，广播设备被允许管理依赖地理位置的事件的接收。事实上，广播设备会经常试图排除对内容的访问，例如事件发生地周围区域的体育广播。因此，通过了解各接收机的位置，所谓的“管制 (blackout)”信号被发送到具有例如不被允许接收对事件的实况报道的区域的邮政编码的接收机。所述接收机的包含位置信息（例如与服务相关的用户邮政编码或 ZIP 码）的安全模块接收这个消息，这样将在权利验证期间应用新的规则，并且即使所述接收机具备这个事件的权利，所述“管制”消息通过不发回用于加密事件的控制字而具

有禁止访问所述事件的优先权。

[0011] 不过，在移动领域，概念“邮政编码”不再有效并且不能限制在这种便携设备上的接收。

发明内容

[0012] 本发明的目的是在移动领域中能够应用与固定接收机相同的限制手段。

[0013] 这个目的是通过使用一种对数字数据流进行条件访问的方法实现的，所述数字数据流以至少一个控制字被加密并且通过广播网络中的发射机被广播到至少一个移动设备，所述发射机还发送包含控制字和访问条件的控制消息流，所述移动设备还通过移动接入点连接到移动通信网络，所述方法包括如下步骤：

[0014] - 由移动设备接收控制消息流，

[0015] - 根据所述移动接入点的标识符或者广播网络发射机的标识符确定所述移动设备的位置标识符，

[0016] - 验证控制消息中包含的访问条件，所述访问条件包括与至少一个移动接入点标识符和 / 或一个广播网络发射机的标识符相关的接收条件，

[0017] - 比较所确定的标识符与所述访问条件中包含的标识符，

[0018] - 根据所述比较结果授权或阻止对所述数据流的访问。

[0019] 这个方法可以用于阻止特定区域（管制）中便携设备的访问或者相反地，仅对这个区域（热点）中的访问授权。

[0020] 根据这个实施例，确定位置标识符的方法可以基于移动小区标识符（移动接入点）或者广播网络发射机的标识符。

[0021] 在第一实施例中，由于移动接入点有限的范围，定位精度似乎更精确。

[0022] 在第二实施例中，广播网络包括多个发射机，这些发射机除了广播数据流，也广播业务数据，在业务数据中可以标识出该移动设备所调谐到的发射机。

附图说明

[0023] 利用以下涉及作为非限制性实施例给出附图的详述，本发明可以被更好地理解。

[0024] - 图 1 显示了两个发射机位于不同位置并且在一个本地移动设备的接收距离之内的配置实施例的结构图。

[0025] - 图 2 显示了广播网发射机的覆盖区域和这些广播区域内的移动网络小区的覆盖区域的图解实例。

具体实施方式

[0026] 形成被控制字 (CW) 加密的内容 (C) 的数字数据流与 ECM 控制消息一起被广播。此数字数据可包括音频 / 视频电视节目数据，也可包括与能够运行在移动设备上的应用相应的数据。

[0027] 条件访问内容的提供者的服务器与广播网络（网络 1）连接。这个网络通过多个天线 E1、E2 广播到移动设备 EM1、EM2。取决于移动设备的位置，后者可连接到天线 E1 而非 E2。

[0028] 以相同方式，移动设备 EM1，EM2 通过适当的天线 F1、F2 连接到移动电信网络网络 2。

[0029] 所述移动设备可通过所述广播天线网络 E1、E2 或移动电信天线 F1、F2 确定其地理位置。在两个通信系统的通信协议中，天线标识符被发送到移动设备并被用作位置标识符。这个标识符用于例如测量网络的接收质量。

[0030] 像这样的标识符不一定要给出地理指示，可以是一个简单的字母数字值。

[0031] 同时，广播发射机发送具有音频 / 视频数据流的控制消息流。控制消息包括用于加密内容的控制字并且进一步包括对所述内容的访问条件。

[0032] 根据所述发明，访问条件除了包括接收内容所必需的权利（例如订阅），还包括与接收受限或被授权的区域相关的天线标识符中的一个或多个。这些标识符可以与广播网络网络 1 或者移动电信网络网络 2 相关。访问条件也可包括联合列表，该联合列表包括两种网络在访问条件中的一个或多个标识符。

[0033] 如图 2 所示，优选使用移动电信网络的标识符 C1 到 Cn。每个小区覆盖范围越小，则允许对限制区域更好的划界。然而在一些情况下，例如为了在整个城市中阻止或授权访问，使用该城市的若干广播发射机的标识符更为简便。

[0034] 当控制消息到达移动设备，所述消息被发送到设备的安全装置。这些装置可以是移动设备的 SIM 卡，或专用电路（直接焊接在印刷电路上），或者可以以软件形式实现。这些安全装置验证控制消息中指定的访问条件是否被满足。这些条件可以有多种形式，例如针对内容的权利，给定信道的一般权利或者如专利申请 WO03/085959 所述的每次付费系统。根据所述发明，除了例如前述条件，并且就根据地理位置限制内容接收而言，所述安全装置验证所获得的广播或电信天线的位置标识符是否出现在控制消息所包含的标识符列表中。如果位置标识符包括在访问条件中广播的标识符的列表中，则所述安全装置将能够发送控制字到解密装置（hot spot 热点版本）或者相反阻止控制字广播到解密装置（管制）。

[0035] 应该注意到，控制消息以第三方不能访问用于限制访问视频 / 音频数据的标识符的方式被加密。根据本发明的特定模式，位置标识符能够被签以来保证其完整性。广播中心（或根据该实施例的电信中心）使用其私钥（来自一对不对称密钥）来签名该标识符。这一签名以常规方式实现，例如通过使用标识符的哈希方法 (Hash) 和使用私钥对获得的结果加密。

[0036] 在接收端，安全模块具有相应公钥，允许其解密签名以获得假设的哈希值以及比较这个值与安全装置从位置标识符计算出的值（认证）。假设的值与算出值的比较使得，当两者相等时确信标识符未经更改。

[0037] 在一个特定实施例中，安全装置使用默认位置值预初始化。它一与安全装置通信，当前标识符就替换这个值。

[0038] 当控制消息到达所述模块，并且假设其包括管制控制，默认值被自动认为是列入黑名单的位置标识符的一部分。

[0039] 根据一实施例，可以限定标识符有效的持续期。一旦该有效性期满，并且如果没有更新的标识符发送到安全模块，则重建缺省标识符并从而认为该缺省标识符在每个管制命令下是活动的。这个持续期可以是安全模块的一个参数，或者与标识符数据相关联，例如与认证签名相关联。为避免标识符被重用，当前日期被关联到标识符，优选地以标识符自身进

行认证。这样，先前在其他网络小区中获得的标识符将不能在另一移动设备中重利用。为加强整体安全，安全模块将拒绝与比所述先前发送的标识符更早的日期相关联的所有标识符。

[0040] 除了人们熟知的电信网络例如 GSM、GPRS 或 UMTS，也可使用其它定位手段，例如，Wifi、WiMax、Wibro 或具有一组天线的任何网络。定位精度将直接依赖天线密度。应该注意到，控制消息中包含的标识符可包括标识符范围。例如，如果一城市中天线标识符都由 ABC 开始 (ABCV120，ABCJ11 等)，则可以仅发送前缀 ABC 以包括所有天线 ABCxxx。其余可能方式可包括一个范围例如 ABC100 到 ABC200。

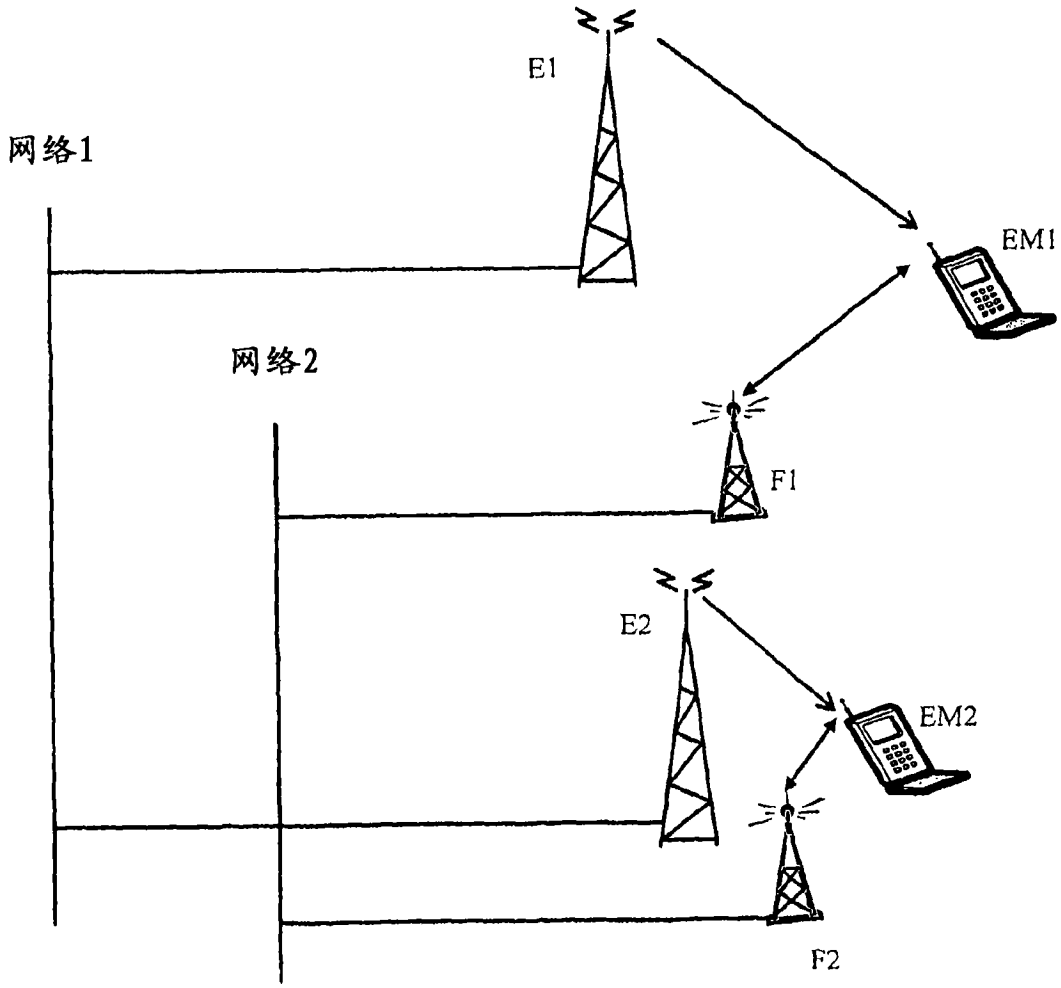


图 1

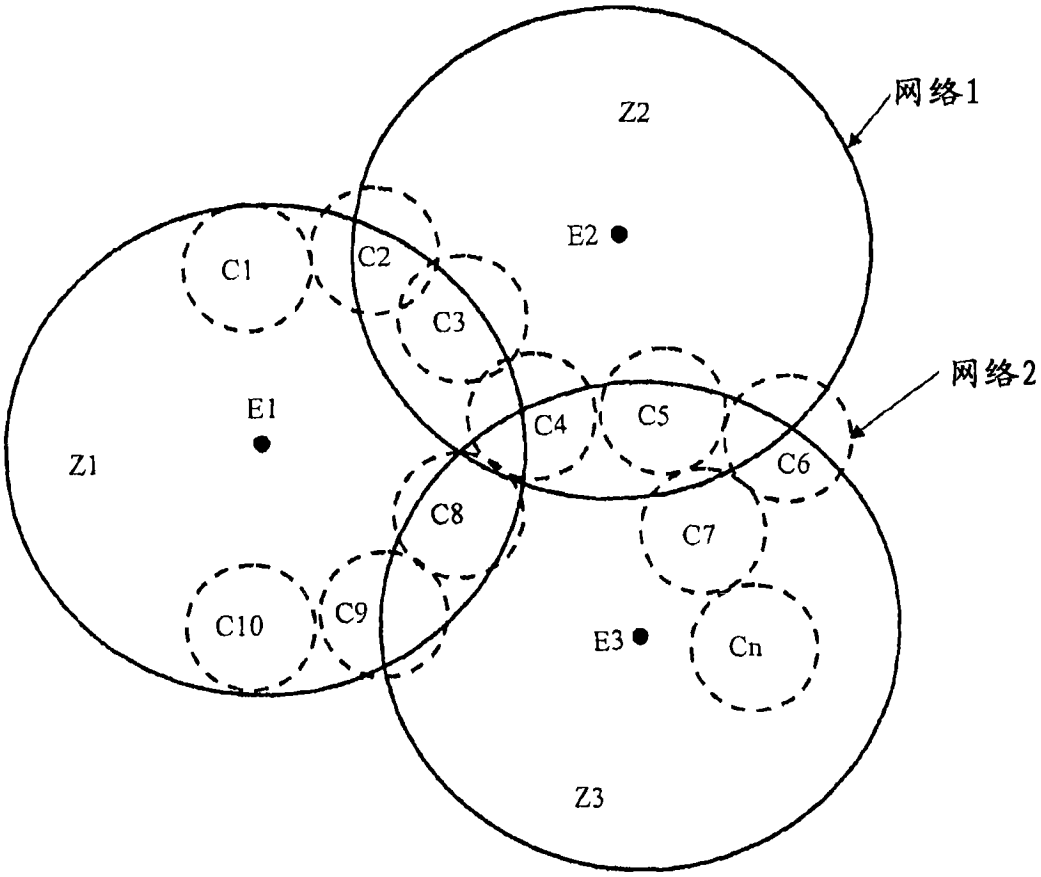


图 2