[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04N 7/16 (2006.01)
H04N 7/167 (2006.01)
H04N 5/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580005714.0

[43] 公开日 2007 年 2 月 28 日

[11] 公开号 CN 1922876A

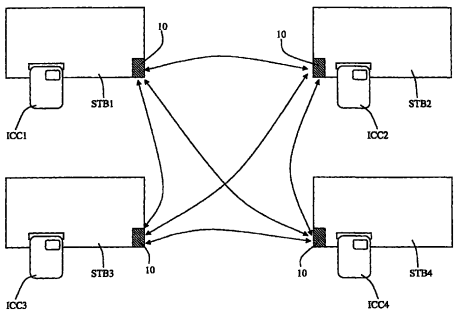
[22] 申请日 2005.2.22
[21] 申请号 200580005714.0
[30] 优先权
[32] 2004. 2.23 [33] EP [31] 04100702.2
[86] 国际申请 PCT/EP2005/050750 2005.2.22
[87] 国际公布 WO2005/091634 法 2005.9.29
[85] 进入国家阶段日期 2006.8.23
[71] 申请人 纳格拉影像股份有限公司
地址 瑞士洛桑
[72] 发明人 亨利·库杰利斯基
克里尼·李－布汉 盖伊·莫瑞尔龙
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 康建忠
权利要求书 3 页 说明书 10 页 附图 2 页

[54] 发明名称

通过至少两个解码器进行条件访问数据处理的管理方法

[57] 摘要

本发明涉及用于提供给用户的至少两个解码器的条件访问数据处理的管理方法。 所述解码器包括条件访问数据处理的启用/停用装置和允许用户的所述解码器之间的通信的本地通信装置。 该方法包括：第一解码器(STB)的本地通信装置(10)从提供给所述用户的至少一个第二解码器(STB)接收至少一个消息的接收步骤；所述第一解码器应该从其接收消息的所述用户的不同解码器的最小数目的确定步骤；以及所述第一解码器已经从其接收到消息的不同解码器的数目和所述第一解码器应该从其接收消息的解码器的最小数目之间的比较步骤。 如果所述解码器没有从要求数目的解码器接收到消息，则停用所述第一解码器(STB)的条件访问数据处理。



1. 用于与订户相关联的至少两个解码器的条件访问数据处理的管理方法，所述解码器包括条件访问数据处理的启用/停用装置和被构建用来允许订户的解码器之间的通信的本地通信装置，该方法包括以下步骤：

由第一解码器（STB）的本地通信装置（10）接收发自与所述订户相关联的至少一个第二解码器（STB）的至少一个消息；

确定所述第一解码器必须从其接收消息的所述订户的不同解码器的最小数目；

在一方面所述第一解码器已经从其接收到消息的不同解码器的数目以及另一方面所述第一解码器必须从其接收消息的解码器的最小数目之间进行比较；

如果所述第一解码器未从所要求数目的不同解码器接收到消息，则停用所述第一解码器（STB）的条件访问数据处理，

其特征在于，所述第一解码器必须从其接收消息的所述订户的解码器的最小数目至少等于与所述订户相关联的解码器总数的绝对多数减一。

2. 根据权利要求 1 的方法，其中，确定一个周期，在该周期期间，第一解码器必须已经从最小数目的不同解码器接收到消息，并且其中，如果第一解码器在所述周期内没有从所要求数目的不同解码器接收到消息，则停用所述第一解码器的数据处理。

3. 根据权利要求 1 的方法，其特征在于，所述消息从所述第二解码器直接发送给所述第一解码器。

4. 根据权利要求 1 的方法，其中，一个订户与至少三个解码器相关联，其特征在于，由所述解码器之一发送给所述第一解码器的所

述消息被存储在至少一个其它解码器中，该其它解码器不同于所述第一解码器和已经发送所述消息的解码器，并且其特征在于，所述第一解码器从所述其它解码器接收消息，或者直接，即在已经发送所述消息的所述解码器和所述第一解码器之间没有中介，或者间接，即通过向所述第一解码器重发存储在所述至少一个其它解码器中的所述消息。

5. 根据前述权利要求中的任何一个的方法，其特征在于，至少所述第二解码器向具有本地通信和存储装置的中央服务器（11）发送消息，并且其特征在于，所述第一解码器通过所述中央服务器从所述第二解码器接收至少一个消息。

6. 根据前述权利要求中的任何一个的方法，其特征在于，所述消息包括已经发布所述消息的所述解码器的标识符。

7. 根据权利要求 1 的方法，其特征在于，所述消息包括可变部分，并且其特征在于，如果该可变部分与之前发送的一个或多个可变部分不同，则所述第一解码器认为消息有效。

8. 根据权利要求 8 的方法，其特征在于，所述可变部分是计数值。

9. 根据权利要求 8 的方法，其特征在于，所述可变部分允许确定所述消息的日期和发布时间。

10. 根据前述权利要求中的任何一个的方法，其特征在于，所述消息通过加密密钥被加密。

11. 根据权利要求 11 的方法，其特征在于，所述加密密钥对于确定的解码器/安全模块单元对是唯一的。

12. 根据权利要求 11 的方法，其特征在于，所述加密密钥对于一个订户的解码器/安全模块单元是公用的。

13. 提供用于条件访问数据处理的解码器，该解码器与订户相关联，并且包括用于处理该条件访问数据的启用/停用装置，和被构建用来允许所述解码器和与所述订户相关联的至少一个其它解码器之间的本地通信的本地通信装置，其特征在于，它包括:

用于处理本地通信装置（10）接收到的消息的装置，这些处理装置被构建用来确定所述订户的哪个解码器（STB）发布了所述消息;

所述解码器必须从其接收消息的所述订户的不同解码器的最小数目的确定和存储装置;

在一方面所述解码器已经从其接收到消息的不同解码器的数目和另一方面所述解码器必须从其接收消息的与订户相关联的解码器的最小数目之间进行比较的装置。

14. 根据权利要求 13 的解码器，其特征在于，它包括存储发自另一个解码器的消息的装置，并且其特征在于，所述本地通信装置（10）被构建用来向至少一个其它解码器发送存储的消息。

15. 根据权利要求 13 或 14 的解码器，其特征在于，它包含用于确定被称为隔离持续时间的持续时间的装置，所述持续时间被定义为接收的消息数和要接收的消息数之间的比较结果给出负值的解码器的最大操作持续时间。

16. 根据权利要求 13 至 15 的任何一个的解码器，其特征在于，它包括本地连接至所述解码器的可去除安全模块，并且其特征在于，所述本地通信装置（10）、用于处理所述消息的装置、所述确定和存储装置以及所述比较装置位于所述安全模块中。

通过至少两个解码器进行条件访问数据处理的管理方法

技术领域

本发明涉及通过至少两个解码器进行条件访问数据处理的管理方法，特别是访问付费电视（TV）事件的领域。它还涉及执行该方法的解码器。

背景技术

通常，为了能够访问对应于由付费电视操作员广播的事件的加密内容，诸如电影、体育赛事等，需要购买预订、解码器和安全模块。有些订户希望有几个解码器和几个安全模块，使得几个用户可以从位于其家中不同位置的几台电视来访问广播的事件。

在这种情况下，请求增补预订、解码器和/或安全模块的价格通常低于请求第一次预订、解码器和/或安全模块的价格。然而，目标是避免订户通过利用增补单元的减价来购买几个解码器/安全模块单元，以及避免订户使非订户的第三方能够利用该减价，或订户将这些单元以比正常购买价格更低的价格转售。

避免该情形的一种解决方案包括：强制操作条件，使得从其环境移开的解码器不再允许对加密内容进行解密，而同样的解码器只要保留在其环境中就可以按正常方式操作。这样，被转卖或提供给第三方的解码器不能运行。

欧洲专利第 EP0826288 号公布的系统可部分达到该目标。该专利描述了一种付费电视系统，其中，订户具有至少两个解码器，每个解码器与一个智能卡相关联，以允许对发送到连接至电视系统的解码器的内容进行解密。每个智能卡包含一定量的数据以允许其识别。被称为“链接数据”的该信息例如是签名、密钥或其它确定元素。所有连接

至同一个订户的卡具有至少一个公用链接数据。不同订户的卡不具有任何公用数据。

订户的智能卡或至少其中之一在使用一段时间之后被停用。发送至涉及的解码器的内容不能再被解密。如果订户还有另一个仍然有效的卡并且有一个解码器连接至该相同订户，则被停用的卡可以被重新启用。为实现这一点，根据该发明的系统按如下方式进行操作。连接至有效卡的数据首先被存储在插入该卡的解码器中。当一个卡被停用时，它必须被插入与该订户的有效卡相关联的解码器中。存储在解码器中的诸如签名、密钥等的链接数据由被停用卡的链接数据进行验证。如果该数据匹配，则该卡被重新启用一段时间。如果该链接数据不匹配，则该卡不被重新启用。

在该系统中，任何连接至该订户的有效卡的解码器可以允许重新启用同一订户的被停用卡。这样，如果订户的卡被卖给地理上接近原订户的人，则具有被停用卡的人可以将该卡插入连接至该订户的有效卡的任何解码器中以便重新起作用。这样，该发明所致力的阻止效果只实现了一部分。另外，停用须定期执行并且需要用户来操作。这些限制通常不受“诚实”用户的欢迎。而且，还存在误操作或丢失卡的严重风险。

此外，存在另一种简单方法来避免与该专利方法相关的限制。事实上，购买未授权的解码器/智能卡单元的人只要购买两个单元即足够。这样，一个卡被停用时总可以被重新启用。

申请 WO 03/105437 与美国专利申请 2003/0097563 一样描述了由属于同一个用户的两个终端来接收条件访问内容的系统。在该系统中，其中一个终端作为主终端。另一个终端是与主终端成对的辅助终端。当辅助终端要对条件访问内容进行解密时，首先确认它能够与主终端通信。进一步确认辅助终端是否与主终端配对。如果事实成立，则辅助终端可以解密该内容。

该系统有一个严重的缺陷。它依赖于存在管理通过辅助终端对内容的访问授权的主终端。万一主终端没有适当地起作用，或者它被切

断，或者被损坏，则整个系统将瘫痪。另外，如果可以欺骗性地把主终端的功能分配给两个不同的终端，则有可能建立两个都能很好地起作用的独立网络。

发明内容

本发明提出一种更可靠和自主的解决方案，可以保证只有合法订户实际使用的解码器才能正确地起作用，并允许对加密事件进行解密。另外，该解决方案不需要诚实用户做任何操作。

根据本发明，解码器及其相关安全模块对授权用户透明地运行，只要它们保持在其“正常”环境中。这意味着用户将不需要执行任何类型的操作，特别是，只要解码器和安全模块保持在其环境中，就不需要定期重新启用安全模块。

相反，在“非正常”使用的情况下，特别是当解码器/安全模块被转卖时，则数据解密不被授权并自动停止。

本发明的目标的实现是通过至少两个与订户相关联的解码器进行条件访问数据处理的管理方法，并包括条件访问数据处理的启用/停用装置和允许订户的解码器之间的通信的本地通信装置，该方法包括以下步骤：

由第一解码器（STB）的本地通信装置（10）接收至少一个消息，该消息发自与所述订户相关联的至少一个第二解码器（STB）；

确定所述第一解码器必须从其接收消息的所述订户的不同解码器的最小数目；

在一方面所述第一解码器已经从其接收到消息的不同解码器的数目以及另一方面所述第一解码器必须从其接收消息的解码器的最小数目之间进行比较；

如果未从所要求数目的不同解码器接收到消息，则停用所述第一解码器（STB）的条件访问数据处理，

其特征在于，所述第一解码器必须从其接收消息的所述订户的解码器的最小数目至少等于与所述订户相关联的解码器的总数的绝对多

数（absolute majority）减一。

其目标也通过提供用于条件访问数据处理的解码器来达到，该解码器与订户相关联，并且包括用于处理该条件访问数据的启用/停用装置，以及被构建用来允许所述解码器和至少一个与所述订户相关联的其它解码器之间的本地通信的本地通信装置，其特征在于它包括：

用于处理由本地通信装置（10）接收的消息的装置，这些处理装置被构建用来确定所述订户的哪个解码器（STB）发布了所述消息；

所述解码器必须从其接收消息的所述订户的不同解码器的最小数目的确定和存储装置；

在一方面所述解码器已经从其接收消息的不同解码器的数目和另一方面所述解码器必须从其接收消息的与订户相关联的解码器的最小数目之间进行比较的比较装置。

简单来说，根据本发明的处理允许确定解码器是否在同一个近程内。如果这是事实，则解码器以常规方式运行。另一方面，如果一个解码器被移动，例如被另一个用户移动，则该解码器将被停用并且将不再能够对加密数据进行解密。属于该订户的其它解码器将正常运行，使得可以移动一个解码器以便进行修复，而不会因此阻止订户的所有解码器。

附图说明

本发明将参考作为非限定性示例给出的附图，通过以下详细描述被更好地理解，其中：

图 1 显示了允许实施本发明的方法的两个实施例的元件；以及

图 2 表示了用于实施本发明的方法的另一个实施例的元件。

具体实施方式

以下将参考几个实施例来说明本发明，其中，假定一个确定的订户配置了几个解码器 STB1, STB2, STB3,...，每个解码器包括一个安全模块 ICC1, ICC2, ICC3,...，它们可以被制成例如微处理器卡或智能

卡的形式，或者集成电路盒的形式。在图示的实施例中，订户有四个解码器/安全模块单元。从订户配置了至少两个解码器/安全模块单元时即可开始使用本发明的方法。从技术角度来看并不存在该上限，而是通常由操作员决定。原则上每个订户包括 5 至 10 个解码器。需要注意的是，在下文中，术语解码器需在更广泛的意义下被理解，即作为允许对条件访问数据进行解密的元件。该数据可涉及付费电视事件，还可以是需要解密数据以便访问服务的任何其它应用。所述实施例示例基本上涉及付费电视。在该领域，术语解码器可用来指定解码器或仅仅安全解码器/模块单元，除了上下文指示这些术语必须被区分。

所使用的解码器都包括本地通信装置 10，其被构建用来发送和接收源自附近的其它解码器的信号或数据。可在大约几百米的范围内进行本地通信，使得位于同一楼层的解码器可以相互通信，而不同楼层的解码器原则上不能通信。

通信装置 10 是公知的类型，并以形成无线网络的方式来使用无线电频率。每个解码器/安全模块单元，或简称为每个解码器也起着发射器和接收器的作用，使得本发明的处理都是一样的，而不管它所分析的解码器。

根据第一实施例的本发明的处理按以下方式操作：首先，解码器之一，例如解码器 STB1 作为发射器并通过本地通信装置发送消息。该消息可以包含可变部分以及相应于使用的解码器或安全模块的单个标识符。该可变部分随消息而变化。因此，不可能借助于作为真解码器被贩卖的非法解码器来存储消息并重发该消息多次。该可变部分可以是诸如计数值的数值或者例如是该消息的时间和发布日期。该消息可以包括一个对应于预订号的标识符。该标识符允许识别消息是否来自与收到消息的解码器所属的同一订户相连的解码器，或它是否属于另一订户。例如当不同订户的解码器较接近，特别是在相互接近的两个楼层中时，这种情况是可能的。该消息以如下方式被加密使得它可以被属于同一订户的其它解码器解密。为此，订户的解码器/安全模块可以配置密钥表，类型为公共密钥、私钥或对一个订户的所有解码器

或安全模块相同并对每个订户不同的网络密钥。

当解码器之一用作发射器时，另一个用作接收器。因此，这些解码器通过本地通信装置来接收发射器解码器 STB1 的消息并按如下说明来处理。首先，确认该消息是否被适当地送至应接收所述消息的解码器。这可以用公知的方式来进行，即，通过在该消息中使用明文报头。然后，确定所需的解密密钥。该密钥可以是网络密钥，它对于一个订户的所有解码器是相同的，或者可以是取决于解码器发射器/接收器对的特定密钥。然后该消息被解密并且它所包含的相干数据被存储在解码器或安全模块中。在相干数据中，显然存在对应于发布日期和时间的可变部分以及发布该消息的解码器标识符。

从作为接收器的解码器的角度来看，所有涉及该解码器的消息都这样被存储，用于进一步的确认阶段。

解码器包含一个参数表，该参数表包括用于该确认阶段的值。特别地，这些参数是解码器/安全模块单元未从其它网络解码器接收通信的最大工作持续时间，以下被称为“隔离持续时间”，以及必须发送消息的不同解码器的最小数目，以下被称为“发送解码器数目”。该参数表中可包含其它参数，特别是属于订户或属于同一网络的解码器数目。

在本发明的处理中，只要从同一订户的其它解码器收到消息，每个解码器根据以下详细说明的条件进行操作。当解码器不再从其它解码器接收消息时，它被停用使得不再授权对加密内容进行解密。

隔离持续时间参数允许选择不再从其它解码器接收消息的解码器在被阻止对加密内容进行解密之前可以运行的持续时间。该持续时间可以被固定为例如 48 个小时，这允许订户在这 48 小时内，在他的其它解码器的本地通信装置的范围之外使用他的解码器之一。如果在超过了这 48 小时的持续时间之后，解码器还没有接收到所需的发自同一个订户的其它解码器的本地通信装置的消息，则阻止对加密内容进行解密。

描述必须发送消息的解码器的最小数目的参数或“发射器解码器数目”可以由操作员来决定，并且通常取决于属于订户的解码器的数

目。根据一个有利的实施例，该发射器解码器的数目对应于解码器的“绝对多数”减一，这意味着，如果解码器的数目为偶数，则它等于解码器数目的一半，并且如果解码器的数目为奇数，则它等于解码器数目的一半舍入到较低值。在具体条件下，对于具有 3 个解码器的订户，发射器解码器的最小数目等于 1，而对于具有 4 或 5 个解码器的订户，发射器解码器的最小数目等于 2，以及对于具有 6 或 7 个解码器的订户，发射器解码器的最小数目等于 3，等等。将在后面描述用户配置了两个解码器的特殊情形。

关于发射器解码器的数目有一点必须指出。实际上，其目的是在订户的不同解码器之间形成网络，该网络包括对应于该订户的绝对多数解码器的“参与者数目”。发射器解码器的数目等于参与者数目减一，因为解码器不向其本身发送消息。

用于属于订户的解码器的数目的参数是可选的。一方面它可以用来确认订户未连接比操作员授权的最大数目更多的解码器，另一方面用来计算参与者的最小数目。

前面提到的确认步骤按以下方式展开：执行确认的解码器确定在对应于隔离持续时间的持续时间内，解码器是否已接收到发自对应于至少若干发射器解码器的不同数目解码器的消息。

例如，如果隔离持续时间为 48 小时并且发射器解码器的最小数目为 3，则每个解码器必须在最近的 48 小时内从至少 3 个不同解码器接收到消息。如果其中一个解码器不满足这些标准，则该解码器中的数据解密被停用。

建立对应于解码器数目的至少绝对多数的参与者的最小数目的目的是，防止从仅一个订户的网络产生两个自主操作的网络。没有上述条件，将可能从一个订户的网络取出一定数目的解码器并重建一个新的网络，然后两个网络都可独立运行，例如对于两个不同用户。

每个解码器的消息发送频率可以被自由选择，当然须假定它低于隔离持续时间。根据一个具体实施例，该频率可以是例如每分钟一条消息。这样，只有发自每个不同解码器的最后一条消息被存储在“接收

器解码器”中。该消息中包含的可变部分与发自其它消息的可变部分进行比较。如果该消息中的可变部分不同于其它消息中的可变部分，则它被认为是有效的。这意味着，如果一条消息被保存并且然后以相同的可变部分被返回，则它将不能被认为是有效的，并且不能与隔离持续时间期间接收的消息一起被考虑。

当一个解码器/安全模块单元由于在隔离持续时间内未收到最小数目的消息而被停用时，需要在它被重新结合到网络中时重新启用它，会在例如以下情形发生上述停用，当解码器在比隔离持续时间更长的时间内被切断时，或者特别地当它被从网络中撤出以进行修理时。可以通过两种方式来实现重新启用，即自动地或请求方式。

在自动重新启用的情况下，只要提供解码器并等待直到它收到发自对应于发射器解码器的至少最小数目的不同解码器的消息。由于它在重新启用时不要求任何操作，该实施例令人感兴趣。另一方面，需要以相对高的频率发送消息，例如每分钟和每解码器一条消息，即使隔离持续时间要长得多，或者等待相对较长的时间直到重新启用生效。

在手动实施例中，当解码器/安全模块单元被重新结合到现有网络中时，需要与网络的其它解码器强制通信。这可以通过由本地通信装置从将要被重新结合的解码器发送消息来实现，该消息要求来自所有接收到所述消息的解码器的响应。在该实施例中，可以提供比一般操作条件下，例如每小时一条消息明显更高的消息发送频率，因为可以在解码器重新启用时强制发送消息。

也可以在断电之后提供解码器以做防备，该解码器向其它解码器发送请求，请求它们发送消息。该实施例对应于按请求重新启用。但对于用户是不可见的因为它不要求用户有任何操作。

在上述实施例中，解码器发出的消息被直接发送给接收器解码器，这意味着，在发射器解码器和接收器解码器之间没有中介。如果其中解码器之一被切断而另一个解码器正在被重新启用，则后者没有接收到被切断的解码器的消息。在某些配置下，这可以防止该解码器的重新启用。

使用图 1 中的元件的本发明的第二个实施例允许解决该问题。在该实施例中，每个解码器接收到的消息被存储在该解码器中或相关联的安全模块中。这些消息可以再被重发给另一解码器，使得每个解码器都可以用作中继。

例如，一个人希望重新启用解码器 STB3 而解码器 STB2 被切断。解码器 STB1 存储了 STB2 解码器在被切断前发送的消息。当解码器 STB3 被重新结合到该网络中时，它接收到来自解码器 STB1 的直接消息和来自解码器 STB2 的由 STB1 发送的间接消息。通过在消息中加入日期和时间，可以确定后者是否足够新近以授权重新启用该解码器。

在本发明第三个实施例中，如图 2 所示，本地通信装置 10 不是用来建立解码器之间的直接通信，而是建立解码器和中央服务器 11 之间的双向通信。该中央服务器从每个解码器接收通信并进行存储。同样进行准备以向采用上述方法来处理所述消息的解码器发送消息。

使用该中央服务器 11 允许消息管理的更大灵活性。例如，可以请求解码器在收到来自确定的解码器的消息时发送收条消息。这样，作为示例，如果第二解码器 STB2 接收到来自第一解码器 STB1 的消息，在所述第一解码器 STB1 将消息发送回第二解码器 STB2 之前，可以等待相对较长的时间。另一方面，如果第三解码器 STB3 未从第一解码器 STB1 接收到消息并且隔离持续时间很快将结束，则中央服务器可以以更高频率向第三解码器 STB3 发送消息，直到后者发送收条。

此外，由于该中央服务器 11，即使当消息应该被接收时解码器被切断，服务器将能够在解码器再次接通时将它发送给后者。事实上可以预期，例如当解码器在中断一段时间后被接通时，它向服务器发送一个请求以向后者指示它重新出现在系统中。因此，服务器能够向所述解码器发送相关消息，使得如果该消息与固定参数相符，则该解码器将马上可以操作。

当订户有两个解码器时，情形与另一个相似，除了以下事实，如果解码器因某种原因必须从系统中被移开，则第二解码器也将在隔离

期结束时被停用。这样，将不能再解密任何加密内容。在订户具有至少三个解码器的情况下，可以从系统中移开一个解码器，而对其它解码器的操作不产生任何后果。一种潜在的解决方案在于，通知管理中心一个解码器必须从系统中移开，其它解码器因此将不会被停用。

另一个解决方案在于，向其中一个解码器，例如向包含最高功能数目的解码器分配特权角色。该解码器被授权独立于其它解码器运行。另一方面，第二解码器总是需要第一解码器操作。在第二解码器故障或延期启用的情况下，第一个将继续操作。尤其在第二解码器只零星使用的情况下采用该解决方案，例如客厅中长时间保持切断的解码器。主解码器继续操作，第二解码器只能在被连接到主解码器之后操作。

在以上描述中，可以看出在解码器之间或解码器/安全模块单元之间建立通信。根据变型，也进行准备使得安全模块本身包含本地通信装置，其形式为置于诸如智能卡的模块中的天线。因此，消息的发送、接收和处理可以直接通过安全模块来执行，而不需要经过解码器。

本发明尤其具有优势之处在于，当订户具有几个解码器时，其中一个可以被移置，例如修理或周末，而不妨碍其它解码器的运行。另外，每个解码器是相同的并且同时具有发射器和接收器的功能。这允许从系统中移除任何解码器，但在一个解码器起主要作用而其它起从属作用的配置中不是这样。

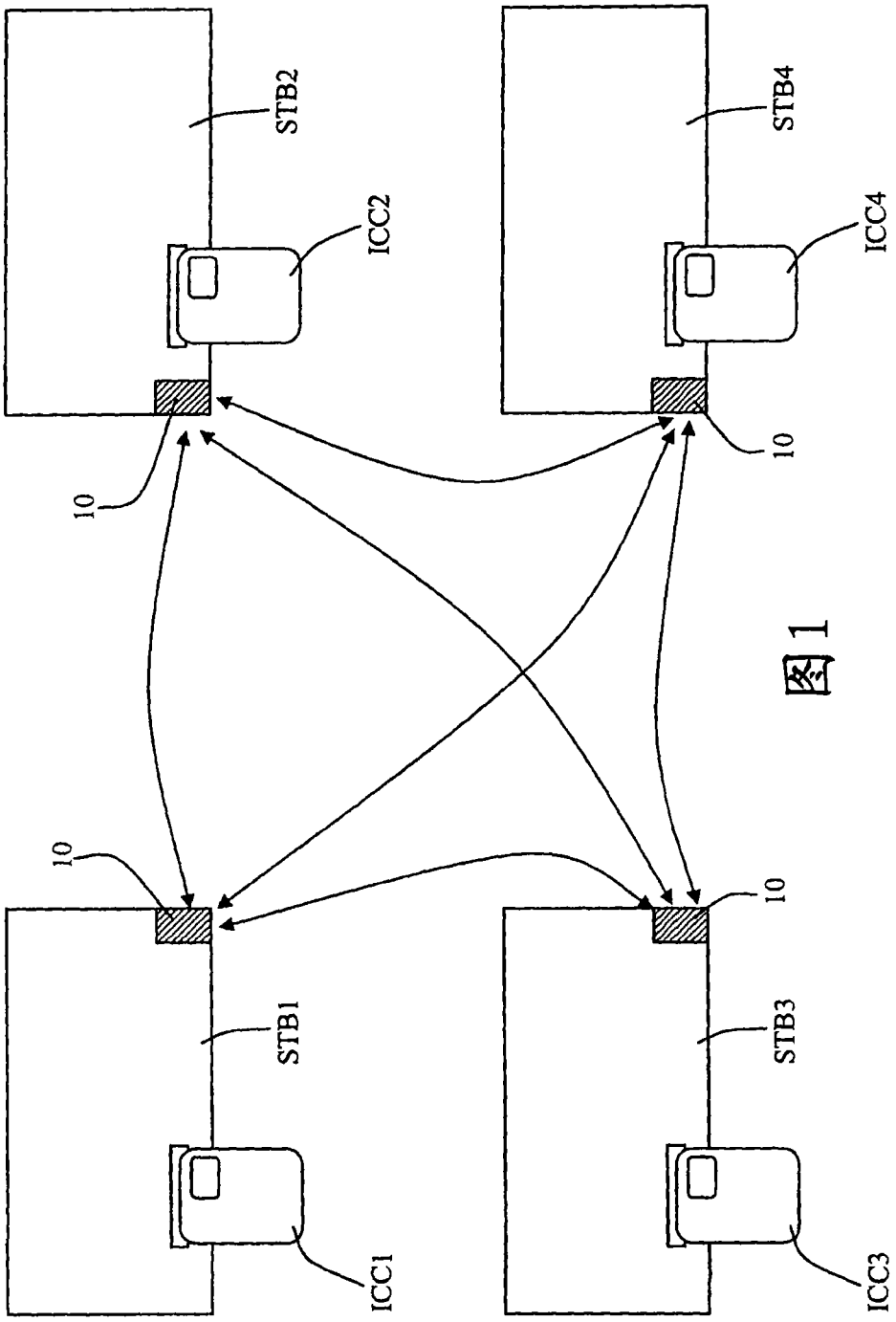


图 1

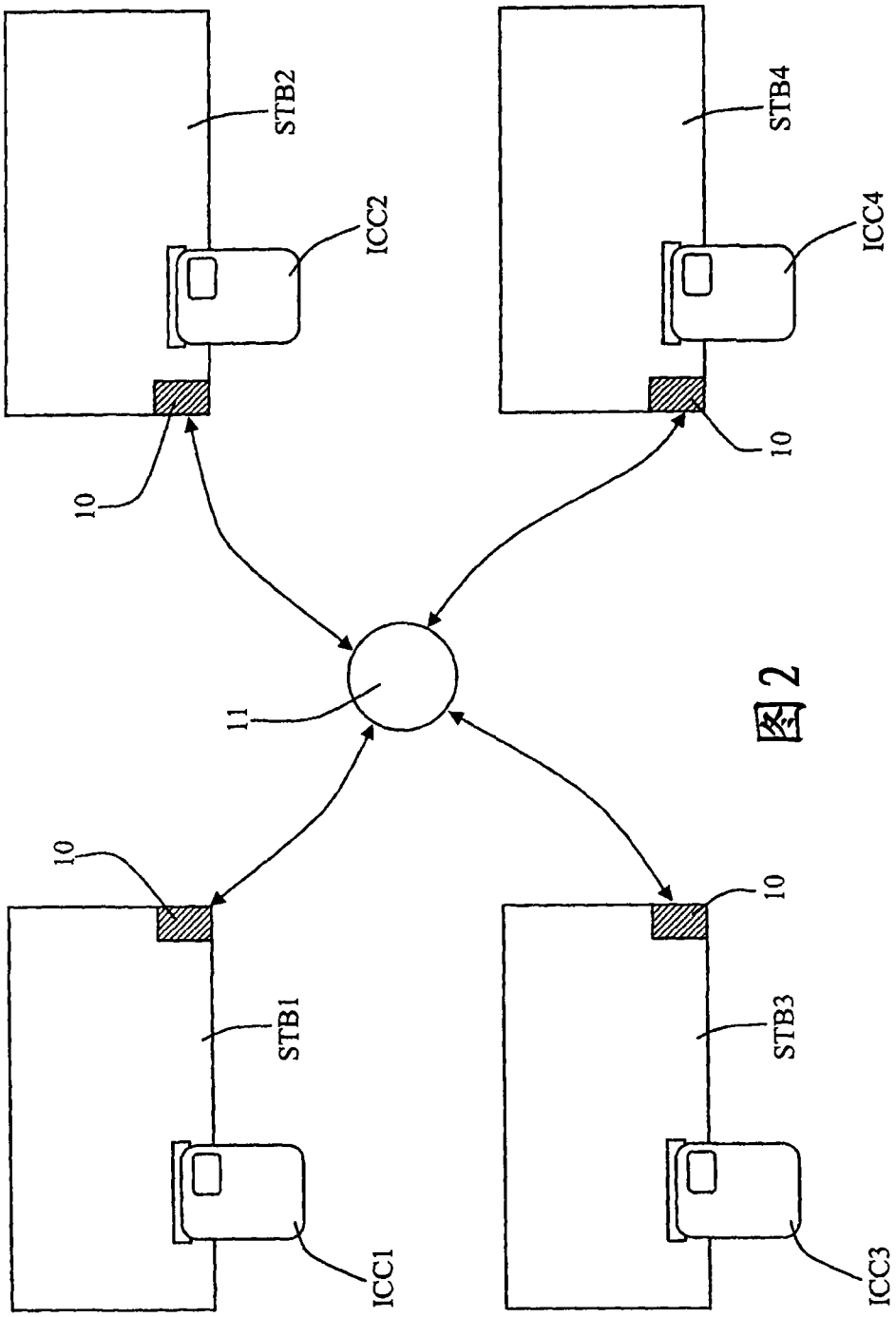


图 2