[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G07C 9/00 (2006.01)
B60R 25/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580040739.4

[43] 公开日 2007 年 11 月 21 日

[11] 公开号 CN 101076834A

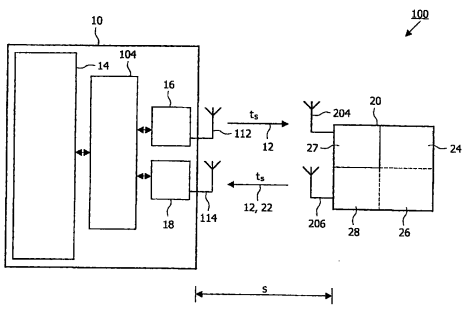
[22] 申请日 2005.9.20
[21] 申请号 200580040739.4
[30] 优先权
[32] 2004. 9.30 [33] EP [31] 04256041.7
[86] 国际申请 PCT/IB2005/053091 2005.9.20
[87] 国际公布 WO2006/035361 英 2006.4.6
[85] 进入国家阶段日期 2007.5.28
[71] 申请人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 亚当·肖·利奇
[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 陈瑞丰
权利要求书 3 页 说明书 12 页 附图 5 页

[54] 发明名称

电子通信系统、具体是用于 P［无源］K［无钥］E［进入］的访问控制系统，以及用于检测对其的中继攻击的方法

[57] 摘要

为了提供电子通信系统(100)，具体地，用于 P［无源］K［无钥］E［进入］的访问控制系统，所述系统包括：至少一个基站(10)，具体地，将所述基站设置在保护防止未授权使用和/或未授权访问的目标上或中，例如，设置在车辆上或中、和/或在访问系统上或中；至少一个远程设备(20)，具体地，至少一个应答器单元，所述远程设备(20)可以具体由授权用户携带、和/或设计用来和基站(10)交换数据信号(12，22)，在这种情况下，通过数据信号(12，22)，可以确定使用和/或访问授权、和/或对基站(10)进行相应地控制，其中，降低了远程设备(20)的成本和复杂度，本发明提出了远程设备(20)包括至少一个记录单元(24)，用于记录数据信号(12，22)的至少部分，具体地，用于记录由基站(10)发送的至少一个第一信号(12)；以及提出了基站(10)包括至少一个处理单元(14)，用于处理数据信号(12，22)。



1．一种电子通信系统（100），具体地，用于 P[无源]K[无钥]E [进入]的访问控制系统，所述系统包括

- 至少一个基站（10），具体地，设置在保护防止未授权使用和/或未授权访问的目标上或中，例如,设置在车辆上或中和/或在访问系统上或中，

- 至少一个远程设备（20），具体地，至少一个应答器单元，所述远程设备（20）

-- 具体由授权用户携带和/或

-- 设计用来和基站（10）交换数据信号（12，22），在这种情况下，通过数据信号（12，22），

--- 能够确定使用和/或访问授权，和/或

--- 能够对基站（10）进行相应地控制，

其特征在于，

- 所述远程设备（20）包括至少一个记录单元（24），用于记录数据信号（12，22）的至少部分，具体地，用于记录由基站（10）发送的至少一个第一信号（12），以及

- 所述基站（10）包括至少一个处理单元（14），用于处理数据信号（12，22）。

2．如权利要求 1 所述的电子通信系统，其特征在于

- 设计所述处理单元（14），通过确定数据信号（12，22）的至少部分的 TOF[渡越时间]（t_s）来确定基站（10）和远程设备（20）之间的距离，以及

- 至少依据已确定的基站（10）和远程设备（20）之间的距离来确定使用和/或访问授权。

3．如权利要求 1 或 2 所述的电子通信系统，其特征在于，设计所述处理单元（14），

- 用于测量由远程设备（20）（重新）发射的数据信号（12，22）的至少部分的载波频率，和/或

- 用于确定远程设备（20）的至少一个时钟速率，和/或

- 用于使以下相关：

-- 数据信号（12，22）的至少部分，和/或

-- 已确定的远程设备（20）的时钟速率。

4. 一种用于如权利要求 1 至 3 中至少一项所述的电子通信系统（100）的远程设备（20），其特征在于，

- 至少一个接收单元（27），用于接收数据信号（12，22）的至少部分，具体地，用于接收由基站（10）发送的至少一个第一信号（12），

- 至少一个记录单元（24），用于记录数据信号（12，22）的至少部分，具体地，用于记录由基站（10）发送的至少一个第一信号（12），

- 至少一个时钟单元（26），用于提供至少一个时钟速率，

- 至少一个（重新）发射单元（28），用于（重新）发射数据信号（12，22），具体地，

-- 用于重新发射由基站（10）发送的至少一个第一信号（12），以及

-- 用于向基站（10）发射至少一个第二信号（22）。

5. 一种用于如权利要求 1 至 3 中至少一项所述的电子通信系统（100）的基站（10），其特征在于，

- 至少一个发射单元（16），用于向远程设备（20）发射数据信号（12，22）的至少部分，具体地，至少一个第一信号（12），

- 至少一个接收单元（18），用于接收由远程设备（20）（重新）发射的数据信号（12，22），以及

- 至少一个处理单元（14），用于处理数据信号（12，22）。

6. 一种方法，用于在如权利要求 1 的前序所述的至少一个电子通信系统（100）上，检测和/或保护免受至少一个攻击，具体地，至少一个外部攻击，以及优选地，至少一个中继攻击，其特征在于，

- 远程设备（20）记录数据信号（12，22）的至少部分，具体地，由基站（10）发送的至少一个第一信号（12），以及

- 基站（10）对所述数据信号（12，22）进行处理。

7. 如权利要求 6 所述的方法，其特征在于

- 针对至少一个时钟单元（26），记录部分数据信号（12，22），具体

地，由基站（10）发送的第一信号（12）；和/或

- 将数据信号（12，22）（重新）发射至基站（10），所述数据信号（12，22）具体是，

-- 由基站（10）发送的第一信号（12），以及

-- 至少一个第二信号（22），优选地，包括重新发射时间。

8．如权利要求 6 或 7 所述的方法，其特征在于

- 接收（重新）发射的数据信号（12，22），和/或

- 测量由远程设备（20）（重新）发射的数据信号（12，22）的至少部分的载波频率，和/或

- 确定远程设备（20）的至少一个时钟速率，和/或

- 基站（10）使数据信号（12，22）的至少部分和/或已确定的远程设备（20）的时钟速率相关。

9．如权利要求 6 至 8 中至少一项所述的方法，其特征在于

- 通过确定数据信号（12，22）的至少部分的 TOF[渡越时间]（t_s）来确定基站（10）和远程设备（20）之间的距离，以及

- 至少依据已确定的基站（10）和远程设备（20）之间的距离来确定使用和/或访问授权。

10．一种如权利要求 1 至 3 中至少一项所述的至少一个电子通信系统（100）、和/或如权利要求 4 所述的至少一个远程设备（20）、和/或如权利要求 5 所述的至少一个基站（10）、和/或如权利要求 6 至 9 中至少一项所述的方法的使用，用于通过通信系统（100），例如运输装置和/或访问系统，来对使用、进入要保护的目标或类似操作的权限进行认证和/或识别和/或检查。

电子通信系统、具体是用于 P[无源]K[无钥]E [进入]的访问控制系统，以及用于检测对其的中继攻击的方法

技术领域

本发明通常涉及安全系统和/或访问系统的技术领域，具体地，涉及所谓 P[无源]K[无钥]E [进入]（Passive Keyless Entry）系统的技术领域，例如，在运输装置的区域中使用的系统，以及在这种情况下首先在机动车辆访问系统区域中使用的系统。

特别地，本发明涉及在权利要求 1 前序中详细描述的电子通信系统、以及涉及在权利要求 1 前序中详细描述的至少一个电子通信系统上检测和/或保护免受至少一个攻击（具体地，外部攻击，以及优选地，至少一个中继攻击）的方法。

背景技术

目前许多汽车通过钥匙、或通过应答器或钥匙卡（key fob）的发射打开，这都由用户接近车辆时启动。新一代的汽车开始使用 P[无源]K[无钥]E [进入]系统，在该系统中不需要用户启动；当用户接近汽车或当用户拉汽车门柄时，汽车就会简单打开。另一选项是所谓“无钥启动”方法，其中，用户无需使用任何钥匙或其他访问卡设备就可以启动汽车。这是可能的，因为汽车“知道”访问卡在汽车内。

为了提供上述特定种类的具有尤其是传统无源应答器系统的电子通信系统（具体地， P[无源]K[无钥]E [进入]系统），传统地，使用各种配置。一种可能的配置如图例中的图 1 所示，使用的示例是用于机动车辆的 P[无源]K[无钥]E [进入]系统：

在所谓的基站 10'（内部配备了模拟接口 104'，以及外部配备了第一电阻器 106'、电容性单元 108'，第二电阻器 110'和线圈形式的天线单元 112'）和远程设备 20'（具体地，应答站）之间，出现以数据交换形式的通信序

列。

详细地，作为基站 10'和远程设备 20'之间的信号传输，存在

- 至少一个第一信号 12'，具体地，所谓上行链路帧，例如，所述上行链路帧由至少一个电感耦合 LF（低频）信道形成，通过该信道，将信号从基站 10'传输至远程设备 20'，以及

- 至少一个第二信号 22'， 具体地，所谓下行链路帧，例如，所述下行链路帧由至少一个 UHF（超高频）信道形成，通过该信道，将信号从远程设备 20'传输至基站 10'（作为可选项，上行链路帧 12'和下行链路帧 22'每个都可以由至少一个 LF（低频）信道形成；或作为可选项，上行链路帧 12'和下行链路帧 22'每个都可以由至少一个 UHF（超高频）信道形成）。

此后，例如，所有者 300 接近或拉动机动车辆的门柄，在空间和功能上与机动车辆关联的基站 10'，开始生成称作“质询”的信号，该信号经由上行链路帧 12'传输到远程设备 20'。

然后，在远程设备 20'中的处理器 202'，具体地，电路设置（优选地配备了至少一个微处理器）使用加密算法和秘密密钥，根据“质询”来计算称作“响应”的信号序列。该响应信号然后经由下行链路帧 22'传输到基站 10'。

然后，基站 10'使用同样的加密算法和同样的秘密密钥来比较响应。如果发现相同，基站 10'就使机动车辆的门锁打开，也就是说，在作为示例给出的实施例中，通常使用加密方法，仅在认证过程将远程设备 20'识别为有效时，打开机动车辆的门锁。

然而，如果该电路设置按照图 1 所示的形式进行操作，而没有其他附加的技术防备，就存在外部攻击者（未经授权就试图打开车门的人）可以使用在技术资源方面的较少技术资源来执行所谓“中继攻击”（如下所述）的危险。

因此，P[无源]K[无钥]E[进入]的主要问题在于中继攻击的风险，其中，接近汽车的人可以使用 RF（射频）中继系统向足够靠近以至于可以发射并收听来自远程设备 20'（具体地，钥匙卡（key fob））发射的信号的另一个人转发信号。

图 2A 和 2B 图解示出了执行该类中继攻击的设置。为了该目的，将

附加发射链路 40'形式的“攻击者工具”引入图 1 所示的配置，所述攻击者工具包括

- 远程设备 20'仿真器形式的第一中继 42'，
- 基站 10'仿真器形式的第二中继 46'，以及
- 第一中继 42'和第二中继 46'之间的通信链路 44'。

为了允许与基站 10'的天线单元 112'的电感耦合，将应答站仿真器形式的第一中继 42'与线圈形式的关联天线单元 420'安装在一起；类似地，将基站仿真器形式的第二中继 46'与线圈形式的关联天线单元 460'安装在一起，以用于与应答站 20'的线圈形式的天线单元 204'电感耦合。

然后，一个攻击者开始将第一中继 42' 安置在紧靠机动车辆的位置。第二攻击者将第二中继 46'安置在足够靠近应答站 20'的位置。例如，通过接近机动车辆或拉动机动车辆的门柄进行触发，机动车辆中的基站 10'通过原始（也就是说，未仿真的）上行链路帧 12'，向第一中继 42'发射它的质询。

从该第一中继 42'中，将质询经由上述通信链路 44'传递到第二中继 46'。第二中继 46'对上行链路帧 12'进行仿真，以及以这样的方式，通过线圈形式的天线单元 460'，将该质询传递到有效应答站 20'。

一旦在有效应答站 20'中计算出响应，该应答站 20'就通过经原始（也就是说，未仿真的）下行链路帧 22'向第二中继 46'发射该响应，以对第二中继 46’进行响应。从该第二中继 46'中，将响应经由上述通信链路 44'传递到第一中继 42'。第一中继 42'对下行链路帧 22'进行仿真，以及以这样的方式，通过据线圈形式的天线单元 112'，将该响应传递到机动车辆中的有效基站 10'。

即使授权和合法的用户并不想这样，但由于可信的应答站 20'基于来自基站 10'的可信质询，利用正确的加密算法和正确的密钥来产生响应，所以认为该响应是有效的，并打开车门。

总而言之，通过两个收发机来形成中继攻击，其中，所述收发机能够在比图 2A 所示距离长得多的距离上传输来自基站 10'（具体地，来自汽车）、以及来自远程设备 20'（具体地，来自钥匙卡）的信号。这就允许甚至在所有者 300 还离汽车好几百米、甚至更远时，将汽车打开。

考虑到目前对于特定组件的操作和安全（精确地，例如在汽车区域和访问区域中）产生了更加苛刻的需求的事实，图 1 所示的配置可被图 2A 和 2B 所示的方法破坏，从而看起来不够安全。

因此，过去已经制定了用于检测和保护免受这类中继攻击的特定建议。例如，在现有技术文献 EP 1 136 955 A2 中，公开了一种用于访问防护系统（P[无源]K[无钥]E [进入]）的设置，通过该设置，可以计算基站 10'和应答站 20'与彼此的相对方位。但是，该设置基于使用汽车上的多根天线，这导致了附加成本。

此外，为防止中继攻击，已知一些基于脉冲成型的技术。从而，现有技术文献 US 2003/0043023 A1 公开了一种无源响应通信系统，根据该系统，两个应答器交换包括多个抗中继攻击脉冲的信号。

在另一个提议中，由于中继的电子器件产生的延迟以及用这种方式检测中继站之间信号的附加传输时间，为了允许检测和保护免受这样的中继攻击，确定质询和响应之间的时间，以支持附加延迟；这被称为传输时间测量方法。

使用这种传输时间测量方法（具体地，确定信号的 TOF（渡越时间）），由于中继攻击导致的风险允许确定钥匙卡 20'和汽车 10'之间的精确距离。其优点在于，由于信号的“往返行程”时间将会比汽车 10'和携带远程设备 20'的拥有者或用户 300 彼此靠近的情况更长，所以可以验证是否正在发生中继攻击。

因此，通过测量信号的 TOF（渡越时间），对检测中继攻击做了若干工作。例如，现有技术文献 WO 02/01247 A2 公开了一种方法，该方法基于使用不同频率来测量两个目标之间的距离，以用于对机动车辆的访问控制。

此外，根据现有技术文献 US 6 396 412，公开了一种基于信号强度的无源 RF-RF（射频-射频）进入系统。

现有技术文献 US 6 236 333 中公开了一种基于多个传感器的无源远程无钥进入系统。

考虑现有技术文献 WO 01/25060 A2 中的渡越时间方法，公开了一种中继攻击检测方法，该方法几乎完全基于通过改变载波频率来测量相位变

化中的延迟。

为了克服中继攻击的弱点，如在现有技术文献 US 2002/0024460 A1 中所做的测量渡越时间给出了基站 10'和远程设备 20'之间（具体地，汽车和钥匙卡之间）的距离指示。这需要在基站或主机（master）10'（具体地，汽车）和远程设备或从动单元 20'（具体地，钥匙卡）之间传递若干消息。

在现有技术文献 WO 2004/051581 A1 中，公开了正如开头所描述的电子通信系统和方法。根据该现有技术文献，由于 RF（射频）信号的速度（大约每 3 纳秒 1 米），所以使用相关性来检验到达子采样精度的 TOA（到达时间）非常重要；这引起了系统任一端（基站 10'和远程设备 20'）处的计算需求的增加。

该计算需求增加了远程设备 20'（具体地，钥匙卡）的成本和复杂度，而远程设备 20'理想地应该尽可能小，尤其没有大电池；例如，在用户钱包和手提袋中可以存放远程设备 20'。

发明内容

从上述缺点和短处开始，考虑到所讨论的现有技术，本发明的目的是：以降低远程设备的成本和复杂度的方式来进一步发展正如开始所描述的该类电子通信系统、以及正如开始所描述的方法。

本发明的目标的通过以下实现：包括权利要求 1 所述特征的电子通信系统、包括权利要求 4 所述特征的远程设备、包括权利要求 5 所述特征的基站和包括权利要求 6 所述特征的方法。在相应的从属权利要求中，公开了本发明的有利实施例和有益改进。

一般地，本发明涉及在渡越时间测量系统中消除来自远程设备（具体地，来自从动单元（slave））的处理需求。

根据本发明的示教，

- 远程设备包括至少一个记录单元，用于记录数据信号的至少部分，具体地，用于记录由基站发送的至少一个第一信号，以及

- 基站包括至少一个处理单元，用于处理数据信号。

在本发明的有利实施例中，对以上参照图 1、2A 和 2B 描述的传统 TOF（渡越时间）系统进行修改。特别地，远程设备记录至少一个数据分组，

而不是在该远程设备中通过例如相关性来处理该数据，仅针对至少一个时钟单元（具体地，至少一个从动时钟）进行记录。然后，数据分组返回基站（具体地，返回汽车），以执行至少一次相关。

因此，该有利实施例基于“移动”处理需求的思想（以附加的数据传输为代价）。特别地，这允许从远程设备（具体地，从动单元）中移除处理单元（具体地，相关器）。

根据本发明的特别发明改进，基站和远程设备之间的距离可以通过确定数据信号的至少部分的 TOF（渡越时间）来测量。基站利用对从基站（具体地，从汽车）到远程设备（具体地，到钥匙卡）距离的实际测量，来确定例如是否打开门和/或启动其他特征，如座位的位置或高度偏好等。

因而，只在基站端利用所测量的距离，在多数情况下，远程设备不需要知道它到基站的相对距离。这可以通过以下来实现：

- 消除远程设备端的所有信号处理，以及
- 重新发射（具体地，通过转发），使数据返回基站用于处理。

这导致了以下优点：

- 在远程设备端的较低功耗，以及
- 大相关阶段的消除，大相关阶段是“非整数码片速率不同时钟频率”设置中的很耗费功率的（power hungry），需要它来获得子采样精度。

在本发明的一个要点实施例中，可以对远程设备（重新）发射的数据信号的至少部分的载波频率进行测量。

此外，根据优选实施例，可以确定至少一个时钟速率（具体地，远程设备的至少一个时钟速率）。

独立地或有关地，可以使以下相关：

- 数据信号的至少部分，和/或
- 已确定的时钟速率。

有利地，可以将远程站设置在至少一个数据载体中，具体地，在至少一个钥匙卡或至少一个卡片中，以及特别地，在至少一个芯片卡中。

根据本发明方法的有利实施例，

- 针对至少一个时钟单元，记录由基站发送的部分数据信号，具体地，第一信号，和/或

- 将数据信号（重新）发射至基站，所述数据信号具体地是，

-- 由基站发送的第一信号，以及

-- 至少一个第二信号，优选地，包括重新发射时间。

此外，优选地，

- 接收（重新）发射的数据信号，和/或

- 测量由远程设备（重新）发射的数据信号的至少部分的载波频率，和/或

- 确定远程设备的至少一个时钟速率，和/或

- 由基站使数据信号的至少部分和/或已确定的远程设备的时钟速率相关。

本发明最终涉及如上所述的至少一个电子通信系统、和/或如上所述的至少一个远程设备、和/或如上所述至少一个基站、和/或如上所述的方法的使用，用于通过如上所述的通信系统，例如运输装置和/或访问系统，来对使用、进入要保护的目标或类似操作的权限进行认证和/或识别和/或检查。

附图说明

如上所述，存在以有利的方式来具体化和提高本发明的示教的多个选项。为此目的，分别参照依据权利要求 1 和权利要求 6 的权利要求；以下参照作为示例的优选实施例和附图，对本发明的进一步改进、特征和优点进行解释，其中：

图 1 基于现有技术实施例中的基站和远程设备之间的电感耦合，示意性地示出了通信原理的电路图；

图 2A 示意性地示出了针对图 1 所示的现有技术实施例的所谓“中继攻击”；

图 2B 示意性地示出了图 2A 所示的中继攻击的等效电路图；

图 3 示意性地示出了根据本发明的测量原理，用于检测如图 2A 和 2B 所示的中继攻击，其中从远程设备中消除处理需求；以及

图 4 示意性地示出了根据本发明的电路图实施例，该电路图等效于图 3 所示的测量原理。

在图 1 至 4 中，对相应部分采用了相同的参考数字。

具体实施方式

如图 3 所示，通过本发明实现的实施例为电子通信系统 100，尤其具有数据载体形式的远程设备 20，即 P[无源]K[无钥]E [进入]卡，该 P[无源]K[无钥]E [进入]卡是用于打开和关闭机动车辆门锁的系统的一部分。

具体地，该电子通信系统 100 是用于 P[无源]K[无钥]E [进入]的访问控制系统，其中，通过确定设置在汽车上的基站或主单元 10 和作为钥匙卡一部分的从动单元或远程设备 20 之间的距离来控制该访问。从而，该电子通信系统 100 基于在汽车的 P[无源]K[无钥]E [进入]系统中获取所谓渡越时间 t_s 的测量的方法。

在基站 10 和远程设备 20 之间，产生数据交换形式的通信序列。详细地，作为在基站 10 和远程设备 20 之间的信号发射链路，存在：

- 第一信号 12，所述第一信号 12 从基站 10 发射至远程设备 20，并从远程设备 20 重新发射至基站 10，以及

- 第二信号 22，所述第二信号 22 包括信号发射时间和/或重新发射时间（在图 3 和 4 中的<-->参考数字 t_s），并从远程设备 20 发射至基站 10。

如图 4 所示，对于第一信号 12 的处理和第二信号 22 的处理，基站 10 包括处理单元 14。经由模拟接口 104，处理单元 14 与以下连接：

- 发射单元 16，所述发射单元 16 与用于发射第一信号 12 的外置的天线 112 连接，以及

- 接收单元 18，所述接收单元 18 与用于接收由遥控设备 20 重新发射的第一信号 12、以及用于接收由遥控设备 20 发射的第二信号 22 的外置天线 114 连接。

另一方面，远程设备 20 包括：

- 接收单元 27，所述接收单元 27 与外置天线 204 连接，并设计用于接收第一信号 12，

- 记录单元 24，用于记录接收到的第一信号 12，

- 从动时钟单元 26，用于提供时钟速率，以及

- （重新）发射单元 28，用于重新发射第一信号 12 和发射第二信号

22，所述（重新）发射单元 28 与外置天线 206 连接。

例如，如果携带具有远程设备 20 的钥匙卡的所有者接近汽车，具体地，如果所有者经过车的预定距离，或者如果所有者拉动汽车门柄，则远程设备 20 唤醒并检查来自基站 10 的信号 12，基站 10 在空间和功能上与汽车关联。然后，基站 10 生成对于远程设备 20 称为“质询”的信号，以及该信号经由上行链路帧 12 发射到远程设备 20。

远程设备 20 仅由记录单元 24 记录数据 12，但不对该数据 12 进行处理；在记录数据 12 后，远程设备 20 通过（重新）发射单元 28，将数据 12 发射回汽车中的基站 10。此外，远程设备 20 将包括重新发射时间和/或信号传输时间的附加第二信号 22 发送到基站 10。然后，该响应信号经由下行链路帧 22，从远程设备 20 传输到主单元或基站 10。

然后，主单元 10 测量“重新发射”时间，并确定用户是否在汽车的定义区域内。此外，基站 10 使用相同的加密算法和相同的秘密密钥比较响应。如果发现相同，并且在定义区域内（与相对低的重新发射时间相对应）发送了信号 12、22，则基站 10 使汽车门锁打开。

换句话说：仅

- 如果一般地，使用加密算法，认证过程将远程设备 20 识别为有效，以及

- 如果认证过程确定远程设备 20 在定义区域内，

则汽车门锁打开。

下面，给出根据本发明的操作方法和电子通信系统的使用的示例：

用户接近他或她的汽车。间歇地，钥匙卡唤醒并检查信号；在离汽车 10m 处，钥匙卡在它的记录单元 24 中启动数据记录，这样几个周期，出现来自汽车的消息 12。钥匙卡记录数据 12，然后发起返回汽车的发射 12、22。该发射 12、22 包括“重新发射”时间和数据。

汽车接收该数据，并已经具有从动设备时钟 26 的先验知识。通过测量载波频率，确定接收机 24 中与时钟 26 有关的该信息中的一些，以及由于这是采样速率的直接倍数，因此可以识别接收机 24 的时钟速率。与时钟速率有关、与接收数据文件 12、22 耦合的该信息允许发生相关。

这发生两次：

- 首先，针对来自从动设备 20 的数据分组，以及

- 其次，针对来自从动设备 20 的重新发射。

这意味着，主单元 10 具有用于对渡越时间 t_s 进行测量的所有信息，从而，主单元 10 确定用户在汽车的定义区域内，因此，打开汽车门。

作为钥匙卡中电子器件的有限数量的结果，通常保存在用户皮夹中的该钥匙卡很纤细。

结果，提出了一种用于在 P[无源]K[无钥]E[进入]环境中以增加汽车装载和功耗的代价来简化钥匙卡设计和复杂性的技术。假定主接收机已经具有执行 TOA（到达时间）测量的相关器，除了对允许在两个设备 10 和 20 之间发送数据分组的协议的少许改变之外，对额外数据分组进行处理几乎不会增加复杂性。

参考数字列表

100 电子通信系统

100' 根据现有技术（参见图 1、2A 和 2B）的电子通信系统

10 基站，具体地，主单元，例如汽车

10' 根据现有技术（参见图 1、2A 和 2B）的基站

12 数据信号，具体地，由基站 10 发送、和/或由远程设备 20 重新发射的第一信号，例如，上行链路帧

12' 根据现有技术（参考图 1、2A、2B）的第一信号，具体地，上行链路帧

14 基站 10 的处理单元，具体地，控制单元，例如微控制器单元

14' 根据现有技术（参考图 1、2A、2B）的基站 10'的处理单元

16 基站 10 的发射单元

18 基站 10 的接收单元

20 远程设备，具体地，应答器，例如数据载体，更具体地，钥匙卡的 P[无源]K[无钥]E [进入]卡

20' 远程设备，具体地，应答器，例如数据载体，更具体地，根据现有技术（参考图 1、2A、2B）的钥匙卡的 P[无源]K[无钥]E [进入]卡

22 数据信号，具体地，由远程设备 20 发送的第二信号，例如下行链路帧，

22' 第二信号，具体地，根据现有技术（参考图 1、2A、2B）的下行链路帧

24 远程设备 20 的记录单元

26 时钟单元，具体地，远程设备 20 的从动时钟

27 远程设备 20 的接收单元

28 远程设备 20 的（重新）发射单元

40' 根据现有技术（参考图 1、2A、2B）的附加发射链路

42' 第一中继，具体地，用于第一位攻击者和/或用于第一个贼，形成远程设备 20'的仿真器

44' 在第一中继 42'和第二中继 46'之间的通信链路

46' 第二中继，具体地，用于第二位攻击者和/或用于第二个贼，形成基站 10'的仿真器

104 基站 10 的模拟接口

104' 基站 10'的模拟接口

106' 基站 10'的第一电阻器

108' 基站 10'的电容性单元

110' 基站 10'的第二电阻器

112 基站 10 的天线单元，与发射单元 16 关联

112' 基站 10'的天线单元

114 基站 10 的天线单元，与接收单元 18 关联

202' 远程设备 20'的处理器，具体地，电路设置或控制单元，例如微控制器单元

204 远程设备 20 的天线单元，与接收单元 27 关联

204' 远程设备 20'的天线单元

206 远程设备 20 的天线单元，与（重新）发射单元 28 关联

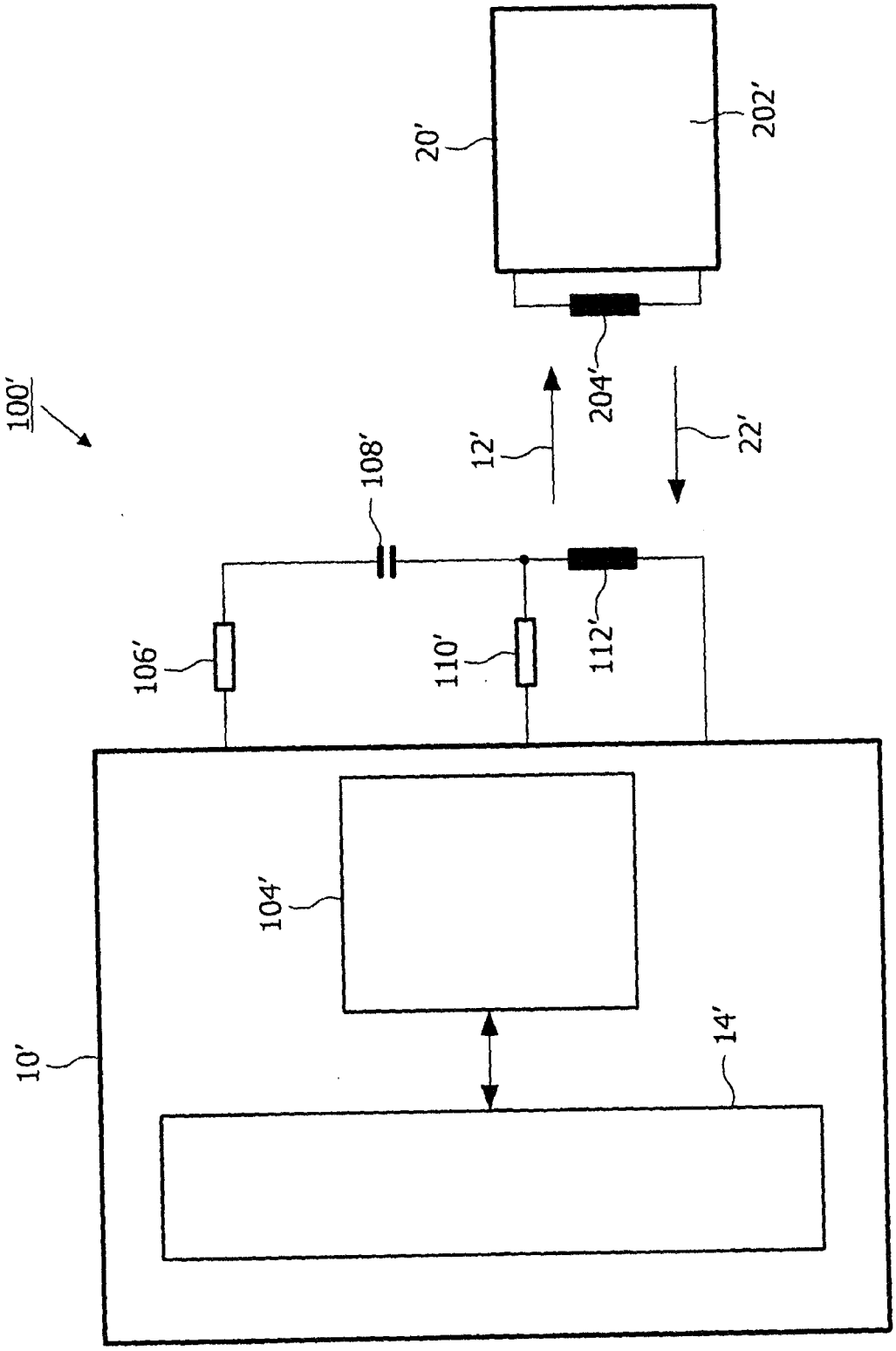
300 授权人，具体地，电子通信系统 100 和 100'的所有者和/或用户

420' 第一中继 42'的天线单元

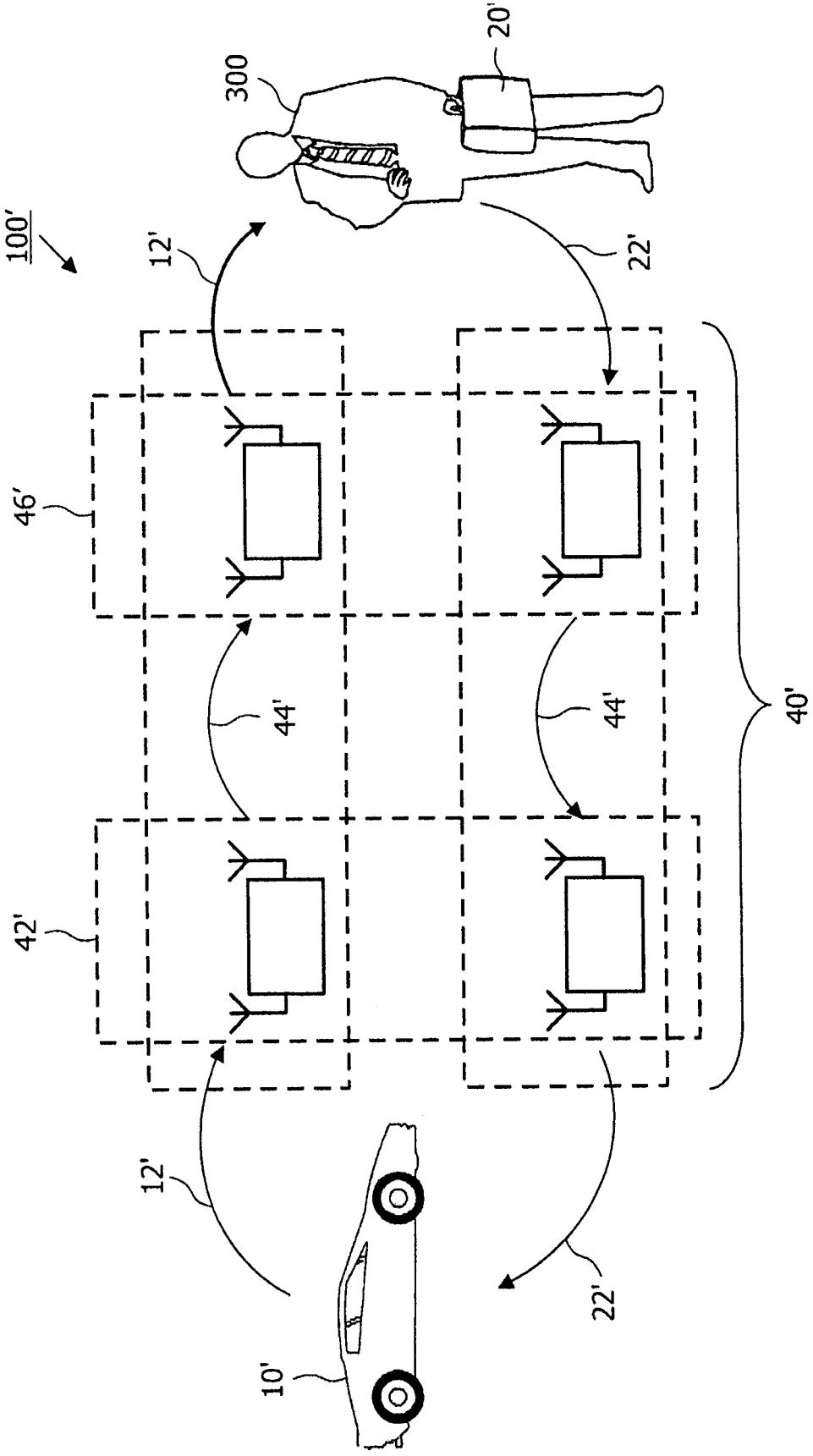
460' 第二中继 46'的天线单元

s 基站 10 和远程设备 20 之间的距离

t_s 数据信号 12、22 的 TOF（渡越时间）和/或基站 10 和远程设备 20 之间的信号传输时间

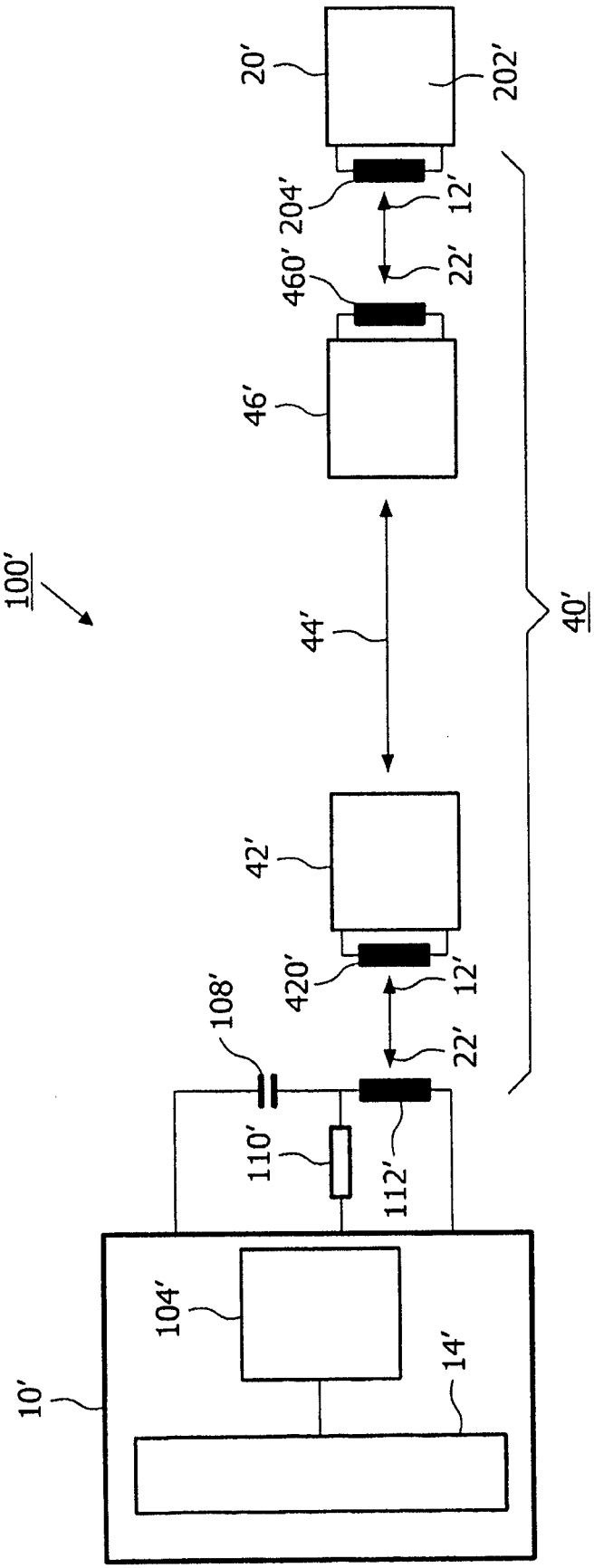


现有技术
图 1



现有技术

图 2A



现有技术
图 2 B

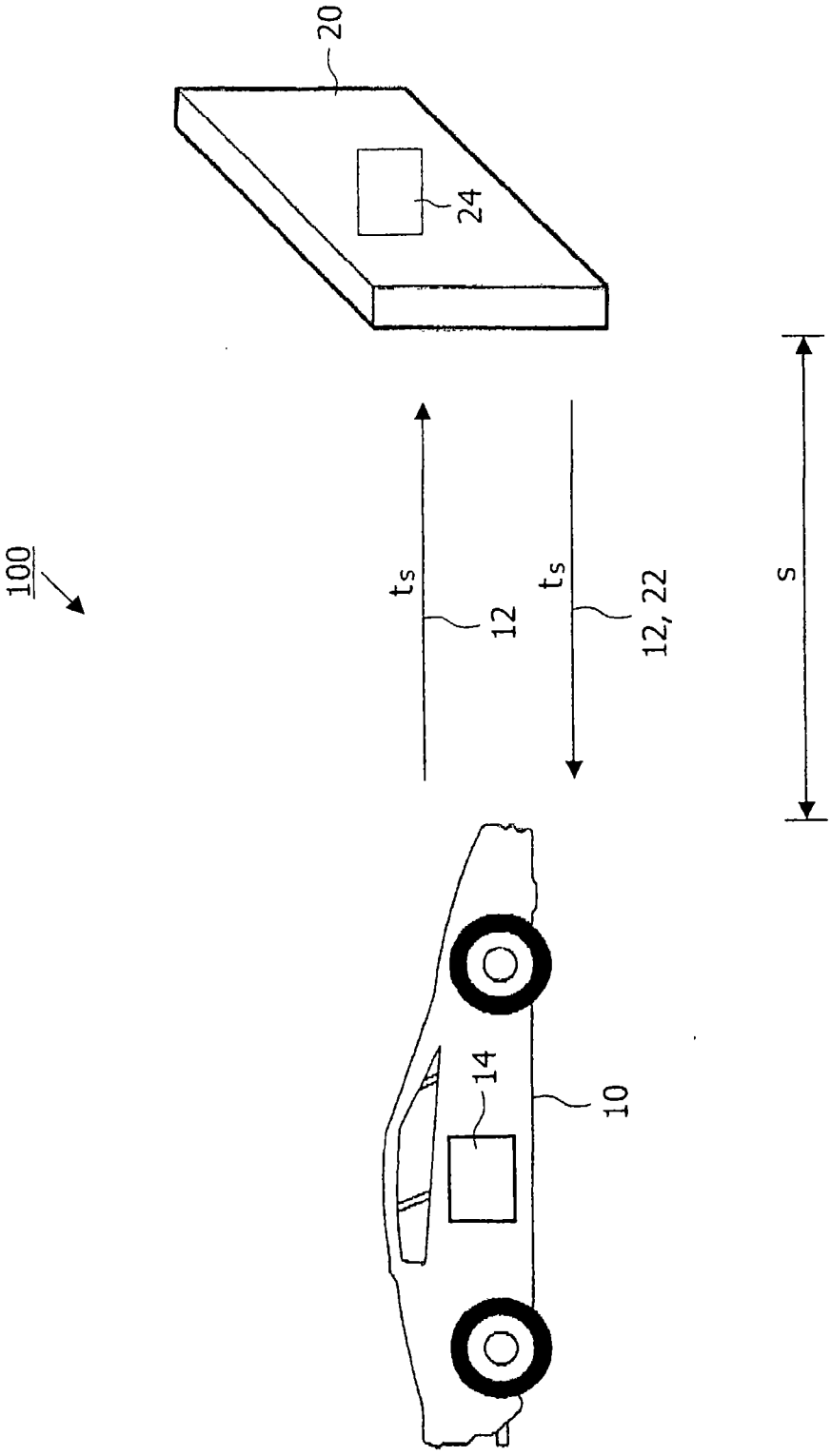


图 3

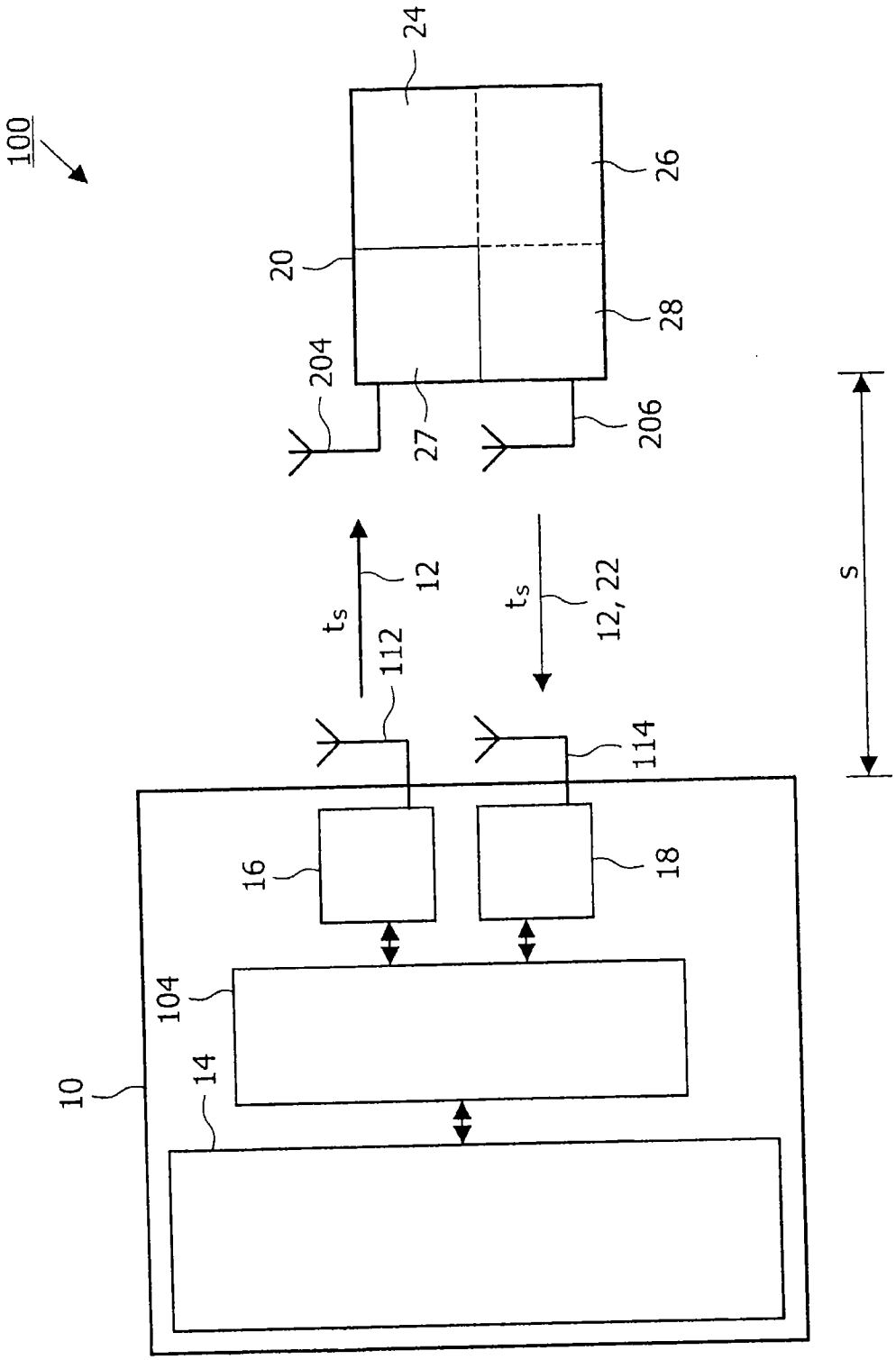


图 4