[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] 发明专利说明书

专利号 ZL 200380104323.5

[45] 授权公告日 2009 年 7 月 29 日

[11] 授权公告号 CN 100520834C

[22] 申请日 2003.11.24
[21] 申请号 200380104323.5
[30] 优先权
[32] 2002.11.29 [33] DE [31] 10255880.9
[86] 国际申请 PCT/IB2003/005378 2003.11.24
[87] 国际公布 WO2004/051581 英 2004.6.17
[85] 进入国家阶段日期 2005.5.27
[73] 专利权人 NXP 股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 J·诺沃特尼克
[56] 参考文献
US2002/0163419A1 2002.11.7
EP0983916A1 2000.3.8
US6353776B1 2002.3.5
US5760700A 1998.6.2
EP1004726A2 2000.5.31
审查员 何 理
[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 王波波

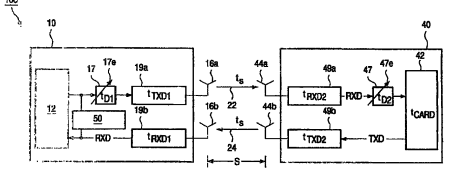
权利要求书 5 页 说明书 13 页 附图 7 页

[54] 发明名称

电子通信系统和检测针对该系统的中继攻击的方法

[57] 摘要

对于电子通信系统(100)和对于检测和/或防范针对这种电子通信系统(100)的至少一个攻击的方法而言，为了进一步开发电子通信系统(100)和方法，以使攻击至少变得困难，并且可能的话被全面防范和阻止攻击，提出了：g)在基站(10)中设置至少一个用于在基站(10)的内部设定一个限定的并且特别是基本上恒定的信号传递时间(t_1)的第一延迟元件(17)，和/或 h)在应答站(40)中设置至少一个用于在应答站(40)内部设定一个限定的并且特别是基本上恒定的信号传递时间(t_2)的第二延迟元件(47)。其中所述系统具有：a)至少一个基站(10)，它具有尤其采用了线圈形式的至少一个天线单元(16：16a，16b)，特别地，该基站(10)被设置在一个受到保护以便防范未经授的权使用和/或未经授权的访问的物体上或设置在其中，例如设置在交通工具上或其中或是设置在访问系统上或其中，以及 b)尤其采用了数据载体形式的至少一个应答站(40)，其具有尤其采用了线圈形式的至少一个天线单元(44：44a，44b)，特别地，该应答站(40)c)可以由授权用户携带和/或 d)被设计成与基站(10)交换数据信号(22，24)，在这种情况下，借助于数据信号(22，24)，e)可以确定使用和/或访问权限，和/或 f)由此可以对基站(10)进行控制，其中所述攻击尤其是外部攻击并且最好是至少一个中继攻击。



1．一种电子通信系统（100），具有：

- 至少一个基站（10），该基站具有至少一个天线单元（16：16a，16b），该基站（10）被设置在一个被保护不被未经授权使用和／或未经授权访问的物体上或其中，以及

- 至少一个应答站（40），其中包括至少一个天线单元（44：44a，44b），该应答站（40）

-- 由授权用户携带和／或

-- 被设计成与基站（10）交换数据信号（22，24），在这种情况下，通过数据信号（22，24）

--- 确定使用和／或访问权限和／或

--- 对基站（10 ）进行控制，

其特征在于：

- 在基站（10）中设置至少一个第一延迟元件（17），用于在基站（10）的内部设定一个限定的并且恒定的第一信号传递时间（t_1），和／或

- 在应答站（40）中设置至少一个第二延迟元件（47），用于在应答站（40）内部设定一个限定的并且恒定的第二信号传递时间（t_2）。

2．如权利要求 1 所述的通信系统，其特征在于：

所述天线单元采用线圈形式，

所述物体是交通工具或访问系统，以及

所述应答站（40）采用数据载体的形式。

3．如权利要求 1 所述的通信系统，其特征在于：第一延迟元件（17）和／或第二延迟元件（47）被设置成是可设定的、多级的并且是可切换的，并且具有：

- 至少一个受已知信号传递时间控制的数字门，和／或

- 至少一个滤波器，和／或

- 至少一个受时钟控制的移位寄存器。

4．如权利要求 1 或 3 所述的通信系统，其特征在于：

- 在第一延迟元件（17）的最后一级（17z）的下游连接了至少一个第一判决单元（18），其中所述第一判决单元与基站（10）的至少一个控制单元（12）和／或基站（10）的至少一个接收机单元（19b）相连，和／或

- 在第二延迟元件（47）的最后一级（47z）的下游连接了至少一个第二判决单元（48），其中所述第二判决单元与应答站（40）的至少一个控制单元(42)和／或应答站(40)的至少一个接收机单元(49b)相连。

5. 一种用于如权利要求 1-4 中任何一个权利要求所述的电子通信系统（100）的基站（10），其特征在于：

- 至少一个用于从应答站（40）接收数据信号（24）的接收机单元（19b），该接收机单元（19b）与关联于基站（10）的第一天线单元（16b）相连接，

- 至少一个控制单元（12），用于对基站(10)进行控制，该控制单元（12）与接收机单元（19b）相连接，并且连接在第一延迟元件（17）的上游，

- 至少一个用于在基站（10）的内部设定所限定的并且恒定的第一信号传递时间（t_1）的第一延迟元件（17），以及

- 至少一个用于向应答站（40）发射数据信号（22）的发射机单元（19a），该发射机单元（19a）与关联于基站（10）的第二天线单元（16a） 相连，并且连接在第一延迟元件（17）的下游。

6. 如权利要求 5 所述的基站，其特征在于：

所述控制单元（12）是微控制器单元。

7. 一种用于如权利要求 1-4 中任何一个权利要求所述的电子通信系统（100）的应答站（40），其特征在于：

- 至少一个用于接收来自基站（10）的数据信号（22）的接收机单元（49a），该接收机单元（49a）与关联于应答站（10）的第一天线单元（44a）相连，并且连接在第二延迟元件（47）的上游，

- 至少一个用于在应答站（40）内部设定所限定的并且恒定的第二信号传递时间（t_2）的第二延迟元件（47），

- 至少一个控制单元（42），用于对应答站（40 ）进行控制，该控制单元（42）连接在第二延迟元件（47） 的下游，以及

- 至少一个用于向基站（10）发射数据信号（24）的发射机单元(49b)，该发射机单元（49b）与关联于应答站（40）的第二天线单元（44b) 相连，并且连接在控制单元（42）的下游。

8．如权利要求 7 所述的应答站，其特征在于：

所述控制单元（42）是微控制器单元。

9．如权利要求 7 所述的应答站，其特征在于：应答站（40）设置在至少一个数据载体中。

10．如权利要求 9 所述的应答站，其特征在于：所述至少一个数据载体是至少一个卡。

11．如权利要求 10 所述的应答站，其特征在于：所述至少一个卡是至少一个芯片卡。

12．一种检测和／或防范针对至少一个电子通信系统（100）所进行的至少一个攻击的方法，所述电子通信系统（100）具有：至少一个基站（10），该基站具有至少一个天线单元（16：16a，16b），该基站（10）被设置在一个被保护不被未经授权使用和／或未经授权访问的物体上或其中，以及至少一个应答站（40），其中包括至少一个天线单元（44：44a，44b），该应答站（40）由授权用户携带和／或被设计成与基站（10）交换数据信号（22，24），在这种情况下，该应答站（40）通过数据信号（22，24）确定使用和／或访问权限，和／或对基站（10 ）进行控制，

所述方法的特征在于：

- 在基站（10）的内部设定一个限定的并且恒定的第一信号传递时间（t_1），和／或

- 在应答站（40）的内部设定一个限定的并且恒定的第二信号传递时间（t_2），

这样，如果基站（10）内部的第一信号传递时间（t_1）、应答站（40）内部的第二信号传递时间（t_2 ）以及在基站（10）与应答站（40）

之间的数据信号（22，24）的第三信号传递时间（t_s）的二倍的总和超出了限定的阈值，则检测到攻击。

13．如权利要求 12 所述的方法，其特征在于：

所述攻击是外部攻击或中继攻击。

14．如权利要求 12 所述的方法，其特征在于：

[a.1] 在基站（10）的内部，将构成至少一部分发射到应答站（40）的数据信号（22）的脉冲传递到至少一个第一延迟元件（17），

[a.2]然后，将由第一延迟元件（17）延迟的第一延迟脉冲馈送到至少一个与基站（10）相关联的发射机单元（16a），并且直接由至少一个与基站（10）相关联的接收机单元（16b）接收，即在没有相关附加延迟的情况下由至少一个与基站（10）相关联的接收机单元（16b）接收，

[b]与此同时，经由整个第一延迟元件（17a，17b，…，17y，17z）馈送构成发射到应答站（40）的至少一部分数据信号（22）的脉冲，

[c]在第一延迟元件（17）的最后一级（17z）的下游连接的至少一个第一判决单元（18）用信号向基站（10）的至少一个控制单元（12）告知最先到达第一判决单元（18）的是第一延迟脉冲还是经由整个第一延迟元件（17a，17b，…，17y，17z）馈送的脉冲，以及

[d]对第一延迟元件（17）进行设定或切换或校正，以使第一延迟脉冲和经由整个第一延迟元件（17a，17b，…，17y，17z）馈送的脉冲同时到达。

15．如权利要求 12 或 14 所述的方法，其特征在于：

[e] 在应答站（40）内部，将构成接收自基站（10）的数据信号（22）的至少一部分的脉冲传递到至少一个第二延迟元件（47），

[f]与此同时，经由整个第二延迟元件（47a，47b，…，47y，47z）来馈送构成从基站（10）接收的数据信号（22）的至少一部分的脉冲，

[c] 连接在第二延迟元件（47）的最后一级（47z）的下游的至少一个第二判决单元（48）用信号向应答站（40）的至少一个控制单元（42）告知最先到达第二判决单元（48）的是由第二延迟元件（47）

延迟的第二延迟脉冲还是经由整个第二延迟元件（47a，47b ，… ，47y，47z ）馈送的脉冲，以及

[d] 对第二延迟元件进行设定或切换或校正，以使第二延迟脉冲和经由整个第二延迟元件（47a，47b ，… ，47y，47z）馈送的脉冲同时到达。

16．如权利要求1-4 中任何一个权利要求所述的至少一个电子通信系统（100）的应用，其中借助了通信系统（100）来验证和／或识别和／或检查针对受安全保护的物体的使用、进入的授权，该物体是交通工具或访问系统。

17．如权利要求7或9中所述的至少一个应答站（40）的应用，其中借助了通信系统（100）来验证和／或识别和／或检查针对受安全保护的物体的使用、进入的授权，该物体是交通工具或访问系统。

电子通信系统和检测针对该系统的中继攻击的方法

本发明总体涉及安全和／或访问系统的技术领域，尤其涉及例如在交通工具的领域中使用的所谓的无源遥控开锁PKE系统的技术领域，特别地，在这种情况下，无源遥控开锁系统是在用于机动车辆的访问系统的领域中使用的。

具体而言，本发明涉及一种电子通信系统，以及一种检测和／或防范针对至少一个电子通信系统的至少一个攻击的方法，特别地，该攻击是一个外部攻击，并且最好是至少一个中继攻击。

为了制造电子通信系统，尤其是上述所指定类型并特别具有一个常规无源应答器系统的无源遥控开锁PKE系统，通常会使用到多种结构。附图中的图1A 和1B 显示了一种可能的结构，所使用的实例是用于机动车辆的无源遥控开锁系统PKE。

在所谓的基站10与应答站40 之间进行的是数据交换形式的通信序列，其中基站10 配备了线圈形式的天线单元16。

详细地说，作为基站10与应答站40之间的信号传输链路，形成了所谓的上行链路帧22，举例来说，上行链路帧22 是由至少一个电感辐合的低频LF信道构成并且信号经由所述帧从基站10传送到应答站40，此外还形成了所谓的下行链路帧24，举例来说，下行链路帧由至少一个特高频UHF信道构成并且信号经由所述帧从应答站40传送到基站10。作为替换，上行链路帧22和下行链路帧24中的每个可以由至少一个低频信道构成，或再作为替换，上行链路帧22和下行链路帧24 中的每个可以由至少一个特高频UHF信道构成。

例如，在操作了机动车辆的门把手或车门按扭之后，在空间和功能上与机动车辆相关的基站10开始产生一个称为“询问”的信号，该信号经由上行链路帧22传送到应答站40。然后，对于优选配备至少一个微处理器的应答站40中的电路装置42而言，该装置使用加密算法和密钥而从询问中计算出一个称为“响应”的信号序列。随后，借助下行链路帧24 而将这个响应信号从应答站40传送到基站10 。然后，基站10 使用相同的加密算法和相同的密钥来对该响应进行

比较。在作为实例给出的实施例中，如果发现等同，也就是说，只有在验证过程认定应答站 40 有效的时候，基站 10 才会打开机动车辆的门锁，其中所述认定通常是使用加密方法实行的。

然而，如果在没有提供任何其它附加技术的情况下以图 1A 和 1B 所显示的形式来操作这个电路装置，那么，试图在未经许可的情况下打开车门的攻击者可以使用相对较少的技术资源来进行如下文所述的所谓的“中继攻击”，这将是危险的。

在图 2A 和 2B 示意性地示出了用于执行这种中继攻击的方案。为此目的，在图 1A 和 1B 的结构中引入了一个以附加传输链路 30 的形式的“攻击者工具箱”，其包括以用于应答站的仿真器形式的第一中继器 32、以用于基站的仿真器形式的第二中继器 36 以及第一中继器 32 与第二中继器 36 之间的通信链路 35。

关于这一点，第一中继器 32 与第二中继器 36 之间的通信链路 35 可以采用允许第一中继器 32 与第二中继器 36 之间存在任意距离的任何希望类型的至少一种双向传输信道的形式。

为了能够电感耦合到基站 10 的天线单元 16，以应答站仿真器形式的第一中继器 32 配备了线圈形式的相关天线单元 34；同样，以基站仿真器形式的第二中继器 36 配备了线圈形式的相关天线单元 38，用于与应答站 40 中的线圈形式的天线单元 44 进行电感耦合。

然后，一个攻击者携带第一中继器 32 并占据紧邻机动车辆的位置。第二攻击者则携带第二中继器 36 并使自身位置足够接近有效应答站 40。举例来说，受到机动车辆门把手或是机动车辆车门按钮操作的触发，机动车辆中的基站 10 借助原始的即非仿真上行链路帧 22 而向第一中继器 32 发射其询问。

该询问从这个第一中继器 32 经由上述通信链路 35 传递到第二中继器 36。第二中继器 36 则对上行链路 22 进行仿真，并以这种方式借助线圈形式的天线单元 38 将询问传递到有效应答站 40。一旦在有效应答站 40 中计算出响应，那么这个应答站 40 借助原始的即非仿真下行链路帧 24 来发射这个响应，从而对第二中继器 36 作出响应。

该响应从这个第二中继器 36 经由上述通信链路 35 传递到第一中继器 32。第一中继器 32 对下行链路帧 24 进行仿真，并以这种方式借助线圈形式的天线单元 34 而将该响应传递到机动车辆中的有效基站

10。

由于该响应是由真实应答站 40 依照来自基站 10 的真实询问使用正确的加密算法和正确密钥产生的，因此该响应被视为是有效的，并且机动车辆的门被打开，即使授权和合法用户不想这样。

鉴于现今对某些组件的操作和安全性提出了更严格的要求，例如确切地说在汽车领域以及访问领域，因此，对于图 1A 和 1B 中显示的可能受到图 2A 和 2B 中的措施破坏的结构而言，看来它们似乎并不是足够安全的。

因此，过去已经提出了某些用于检测和防范这种中继攻击的建议。例如，在印刷出版物 EP1136955A2 中公开了一种用于对访问加以防护的系统（无源遥控开锁 PKE 系统）的装置，借助于所述装置，可以对基站 10 与应答站 40 彼此之间的相对方位进行计算。

依照另一个建议，为了能够检测和防范这种中继攻击，确定询问与响应之间的时间以允许一个附加延迟，该延迟是由中继器的电子仪器以及以这种方式检测的中继站之间信号的附加传递时间导致的（传递时间测量法）。

然而，在载波频率为 125 千赫的当前的应答器系统中，实际上不可能通过信号传递时间测量法来检测中继攻击，因为在实践中很难满足时间测量精度的严格要求，主要原因是所用滤波器的容差以及温度问题。

因此，为了能够通过传递时间测量来对中继攻击进行安全而可靠的检测，在时间测量精度方面必须提出非常严格的要求。在图 3 中以示意图的形式显示了这种信号传递时间测量的原理，其例如将在图 1A 和 1B 所示的现有技术实施例的情况下使用，用于对如图 2A 和 2B 所示的中继攻击进行检测。在这种情况下，总的信号传递时间是如下计算的：

$$t_{total}=t_{TXD1}+t_{a}+t_{RXD2}+t_{CARD}+t_{TXD2}+t_{a}+t_{RXD1}$$

因此，由于存在附加的中继链路，用于中继攻击出现的标准是基站 10 与应答站 40 之间的距离 s 超过给定的最大容许距离 s_{max}。为了能够检测到中继攻击，必须尽可能精确地确定这个距离 s，该距离可以使用公式 $s=v_s \cdot t_s$ 根据信号 22、24 的传递时间 t_s 和信号 22、24 的已知传播速度进行计算。

然而必须记住的是，在如图 3 的信号传递时间测量的情况下，对想要的信号传递时间 t_s 添加附加延迟 t_{TXD1}、t_{RXD2}、t_{CARD}、t_{TXD2} 以及 t_{RXD1}。对基站 10 与应答站 40 之间精确确定的距离 S 而言，并且由此还对于所选择的足够短的最大容许距离 s_{max}（没有多的安全保留）而言，信号传递时间的这些附加成分必须是已知的，或者必须以足够的精度被确定。

在这种情况下需要记住的另一件事是，在以低成本大量制造的实际系统中，可能由于基站 10 和 / 或应答站 40 的电子仪器而在信号传递时间方面预期相当大的容差 $\triangle t_{TXD1}$、$\triangle t_{TXD2}$、$\triangle t_{RXD1}$ 以及 $\triangle t_{RXD2}$。这些容差是由老化效应、所用组件的分散以及温度效应导致的。除非采取额外步骤，否则在确定阈值 s_{max} 的时候还必须顾及这些容差。

基于上述的缺陷和不足，并且结合所概述的现有技术应有的肯定方面，本发明的目的是进一步开发在开始部分中所述的该种电子通信系统，以及一种检测和 / 或防范针对开始部分所述的至少一个电子通信系统的至少一个外部攻击的方法，其中所述至少一个外部攻击最好是至少一个中继攻击，这样一来，攻击至少变得相当更加困难，如果可能的话，还可以被彻底防范并阻止。

这个目的是通过具有本发明所限定的特征的电子通信系统以及通过具有本发明限定的特征的方法来实现的。在稍后部分的具体描述中表征了本发明的有利实施例以及有益改进。依照本发明的教导，

- 在基站中设置至少一个第一可调延迟元件，用于在基站内部设定一个限定的并且特别是基本上恒定的信号传递时间 t_1，和 / 或
- 在应答站中设置至少一个第二可调节延迟元件，用于在应答站内部设定一个限定的并且特别是基本上恒定的信号传递时间 t_2。

由此依照本发明而将一个附加的可调信号传播延迟引入传输链中。

借助于第一可调延迟元件和借助于第二可调延迟元件，可以分别设定基站内部的信号传递时间 t_1，以及应答站内部的信号传递时间 t_2，这意味着：如果基站内部的信号传递时间 t_1、应答站内部的信号传递时间 t_2 以及在基站与应答站之间数据信号的信号传递时间 t_s 的二倍的总和超过限定的阈值 $t_{s,\,max}$，则检测到攻击。

因此，本发明的基本思想是对无源遥控开锁 PKE 系统中的发射和接收机单元的信号传递时间进行补偿，采取适当的技术步骤（＝设置至少一个用于在基站内部设定限定的并且特别是基本上恒定的信号传递时间 t_1 的第一可调延迟元件，和/或设置至少一个用于在应答站内部设定限定的并且特别是基本上恒定的信号传递时间 t_2 的第二可调延迟元件）以确保基站端与应答器端的发射和接收子部件的信号传播延迟尽可能恒定，举例来说，基站端位于要确保安全的车辆上或其中，而应答器端则位于 PKE 数据载体（PKE 卡）上或其中。

通过分别借助于相应的附加延迟元件来对基站和应答站内部的特定延迟 t_{D1} 以及 t_{D2} 进行适当调整和设定，为中继攻击的检测和/或防范获得了改进的条件，如下列等式所示：

$t_1=t_{RXD1}+t_{D1}+t_{TXD1}$=基本上恒定，

$t_2=t_{RXD2}+t_{D2}+t_{CARD}+t_{TXD2}$=基本上恒定。

因此，如果满足以下阈值条件，则发生了中继攻击：

$t_{s,max}<t_1+t_2+2t_s=t_{RXD1}+t_{D1}+t_{TXD1}+t_{RXD2}+t_{D2}+t_{CARD}+t_{TXD2}+2t_s$。

因此，有利的是在实际实施中一旦定义了固定阈值 $t_{s,max}$ 则使用该阈值来进行比较，在这种情况下，有利的是对信号传递时间对于系统容差 Dt_{TXD1}、Dt_{TXD2}、Dt_{RXD1} 以及 Dt_{RXD2} 的依赖性产生容差。

特别地，在当前电子通信系统和检测针对该系统的中继攻击的方法的发明改进中还可以提供可选的温度测量，由此可以通过使用附加延迟元件来确保对温度相关性的补偿，目的在于获取基站内部总延迟 t_1 以及应答站内部延迟 t_2，其中所述延迟都是恒定的，尤其是与温度无关的。

优选地，即使在基站与应答站之间进行通信的过程中，也可以执行用于实施根据本发明的方法的（调节）算法，以通过检测攻击性中继来阻止针对调节算法的外部攻击。在这种情况下，如果不破坏协议，那么中继器必须传递数据。

在本发明的一个有利实施例中，用于产生信号传递时间 t1 和 t2 的调节算法可以由任何期望的方法来执行，举例来说，例如计数法或逐次逼近法。

延迟元件优选是多级的以及优选是可切换的，有益的是其可以包含任何期望类型的适当组件，例如：

- 至少一个受已知信号传递时间控制的数字门，和/或
- 至少一个滤波器，和/或
- 至少一个时钟控制的移位寄存器。

特别地，对举例来说诸如熟知安全系统领域的电子工程师之类的通信电子学领域的技术人员而言，他们将会了解这样一个事实，那就是本发明有助于制造一个高度抵抗外部攻击的无源遥控开锁 PKE 系统，也就是说，通过精确测量时间，本发明使得所谓的“中继攻击”变得极其困难。由此可以用一种适合实际应用的方式来对时间进行附加的精确测量，从而更可靠地检测中继攻击。

为了实际执行时间测量，有利的是可以高精度地将测量得到的总的信号传递时间与一个受严格容差影响的固定阈值 $t_{s,max}$ 相比较，在这种情况下，可能的廉价的实施模式使得电子通信系统以及相关方法对用于大规模生产具有高度吸引力。

本发明扩展到至少一个上述类型的基站以及至少一个上述类型的应答站，有利的是可以在用于交通工具并且尤其是机动车辆的所谓的“引擎停机防盗装置（immobilizer）”系统的领域中广泛使用的系统中利用本发明。

对于本发明而言，另一个应用领域是建筑安全领域，因为具有其基站和具有其应答站的电子通信系统还非常适合制造基于应答器的安全访问系统，尤其是基于比如说芯片卡或无源遥控开锁 PKE 卡之类的数据载体的安全访问系统。

因此，基站可以设置在防范未经授权的使用和/或未经授权访问的物体或建筑上或其中，例如交通工具或访问系统上或其中。

如上所述，目前存在多种可以有利实施和改进本发明的教导的方式。参考下文所述的实施例，本发明的这些及其他方面是显而易见的并将被阐明。

在附图中：

图 1A 是示出如在现有技术实施例中基站与相关应答站之间的基于电感耦合的通信原理的示意图。

图 1B 是图 1A 所示的通信原理的等效电路图。

图 2A 是对图 1A 和 1B 中显示的现有技术实施例进行的所谓的“中继攻击”的图示。

图 2B 是图 2A 所示的中继攻击的等效电路图。

图 3 是在图 1A 和 1B 所示出的现有技术实施例的情况下允许通过测量信号传递时间来检测图 2A 和图 2B 所示的中继攻击的原理的图示。

图 4 是依照本发明检测图 2A 和 2B 所示的中继攻击的测量原理的图示，在依照本发明的一个实施例中，该原理是以产生恒定信号传递时间为基础的；以及

图 5 是依照本发明用于将基站和/或应答站内部的信号传播延迟调节成如图 4 中的恒定信号传递时间值的措施的图示。

在图 1A－5 中相同或相似的装置、元件或特征被给予相同的附图标记。

如图 4 中的实施例所示，借助本发明所实现的是电子通信系统 100，特别地，该系统具有一个应答器系统（＝以数据载体形式的应答站 40，即无源遥控开锁 PKE 卡），该应答器系统是用于打开和关闭机动车辆门锁的系统的一部分。

PKE 卡 40 具有一个信号传递时间为 t_{RXD2} 的接收机单元 49a，该接收机单元 49a 与天线单元 44a 相连，并且用于接收来自基站 10 的数据信号 22。PKE 卡 40 还具有一个信号传递时间为 t_{TXD2} 的发射机单元 49b，该发射机单元 49b 与天线单元 44b 相连，并且用于将数据信号 24 发射到基站 10。以微控制器单元形式的控制单元 42（--->信号传递时间 t_{CARD}）与接收机单元 49a 的下游以及发射机单元 49b 的上游相连，它被提供来控制 PKE 卡 40。

在图 4 中还显示了一个基站 10，它具有一个信号传递时间为 t_{RXD1} 的接收机单元 19b，该接收机单元 19b 与天线单元 16b 相连，并且用于接收来自 PKE 卡 40 的数据信号 24。基站 10 还具有一个信号传递时间为 t_{TXD1} 的发射机单元 19a，该发射机单元 19a 与天线单元 16a 相连，并且用于向 PKE 卡 40 发射上述数据信号。以微控制器单元形式的控制单元 12 与接收机单元 19b 的下游以及发射机单元 19a 的上游相连，它被提供来控制基站 10。

当 PKE 卡 40 处于激活状态时（参见图 4），用于验证目的的通信序列以基站 10 与 PKE 卡 40 之间的数据交换的形式出现，为此目的，在基站 10 与应答站 40 之间交换数据信号 22、24；借助于这些数据信

号 22、24，不但可以确定使用和/或访问机动车辆的授权，而且可以使用恰当的方式来控制基站 10。对这里描述的无源遥控开锁 PKE 而言，电源最好由至少一个电池单元提供。

详细地说，作为基站 10 与 PKE 卡 40 之间的信号传输链路存在的是所谓的“上行链路帧”22 以及所谓的“下行链路帧”24，举例来说，“上行链路帧”22 由至少一个电感耦合的低频 LF 信道构成，并且信号是借助上行链路帧而从基站 10 被传送到 PKE 卡 40 的，“下行链路帧”24 由至少一个特高频 UHF 信道构成，并且信号是借助下行链路帧而从 PKE 卡 40 被发射到基站 10 的。

然而，在图 4 和 5 所示的实施例中，上行链路帧 22 和下行链路帧 24 中的每个都由至少一个低频 LF 信道构成，这同样处于本发明的范围内。作为替换，上行链路帧 22 和下行链路帧 24 又可以由至少一个特高频 UHF 信道构成。

例如，一旦操作了机动车辆门锁，那么在功能和空间上与机动车辆相关的基站 10 开始产生一个称为“询问”的信号，该信号经由上行链路帧 22 传送到 PKE 卡 40。优选地，PKE 卡 40 中的电子电路装置被设置成具有至少一个微处理器，然后该电子电路装置使用加密算法以及密钥而从询问中计算出一个称为“响应”的信号序列。随后，这个响应信号从 PKE 卡 40 经由下行链路帧 24 传送到基站 10。

然后，基站使用相同的加密算法以及相同的密钥来比较响应；如果发现等同，则基站使得机动车辆的门锁被打开，或者换句话说，在引用的实施例中，只有验证认定 PKE 卡 40 有效，才会打开机动车辆的车锁，其中所述认定通常是用加密方法实行的。

现在，为了抵抗参考图 2A 和 2B 所述的该种中继攻击，在基站 10 中设置了第一延迟元件 17，该元件与控制单元 12 的下游以及发射机单元 19a 的上游相连，并且用于在基站 10 的内部设定一个基本上恒定的限定信号传递时间 t_1。同样，在 PKE 卡 40 中设置了一个第二延迟元件 47，该元件与接收机单元 49a 的下游以及控制单元 42 的上游相连，并且用于在 PKE 卡 40 内部设定一个基本上恒定的限定信号传递时间 t_2。

现在，如果基站 10 内部的信号传递时间 t_1、PKE 卡 40 内部的信号传递时间 t_2 以及基站 10 与 PKE 卡 40 之间的信号传递时间 t_3 的两倍（<—>“输出”信号 22 以及“返回”信号 24）的总和超出了限定的

阈值 $t_{s,max}$，也就是说，如果满足阈值条件

$t_{s,max}<t_1+t_2+2t_s$，或者

$t_{s,max}<t_{RXD1}+t_{D1}+t_{TXD1}+t_{RXD2}+t_{D2}+t_{CARD}+2t_s$，则检测到外部中继攻击，其中：

基站10内部的信号传递时间 t_1 实质上由接收机单元19b内部的信号传递时间 t_{RXD1}、第一延迟元件17所导致的信号传递时间延迟 t_{D1} 以及发射机单元19a内部的信号传递时间 t_{TXD1} 构成，以及PKE卡40内部的信号传递时间 t_2 实质上由接收机单元49a内部的信号传递时间 t_{RXD2}、第二延迟元件47所导致的信号传递时间延迟 t_{D1}、控制单元42的信号传递时间 t_{CARD} 以及发射机单元49a内部的信号传递时间 t_{TXD2} 构成，而 t_s 则是信号在基站10与PKE卡40之间传递一次的时间，因此，$2t_s$ 是这个信号传递时间的二倍。

于是，为了能够实现本发明的基本思想，也就是使用一个用于发射和接收在机动车辆（-->基站10）与无源遥控开锁PKE卡40之间所交换的数据的电子子部件的一次定义的恒定信号传播延迟 t_1（→基站10）或 t_2（→PKE卡40），基站10内部的第一延迟元件17和PKE卡40内部的第二延迟元件47（分别参见附图标记17e和47e）都被设置为可以采用下列形式来执行四级调节（分别参见附图标记17a、17b、17y、17z 以及 47a、47b、47y、47z）和可以进行切换（分别参见附图标记17s 以及47s），例如：

- 至少一个受已知信号传递时间控制的数字门，和/或
- 至少一个滤波器，和/或
- 至少一个时钟控制的移位寄存器。

为了将适于信号传播的延迟时间 t_1 和 t_2 调整成恒定值，在这里提供了具有明显可能性的各种技术实施方式。在下文中将会参考图5中的详细表示来对使用传递时间调节的简单廉价的实施方式进行描述。首先以基站10为例：

从基站10发射到PKE卡40的脉冲被传送到多级的（参见附图标记17a、17b、17y）可切换的（参见附图标记17s）的第一延迟元件17。然后，经过延迟的脉冲将会馈送到发射机（=基站10的发射机单元19a）并直接（即，在信号传播中没有相关的附加延迟）地由接收机（=基站10的接收机单元19b）接收。同时，该脉冲还经由整条延迟

线进行馈送，也就是说，脉冲经过了第一延迟元件 17 的所有四级 17a、17b、17y、17z（-->延迟时间 t_1）。

判决器（＝基站 10 的第一判决单元 18）与延迟元件 17 的第四级同时也是最后一级 17z 的下游相连，并且还与接收机单元 19b 相连，该判决器用信号向控制单元 12 告知这两个脉冲（“延迟脉冲”或“经由整条延迟线馈送的脉冲”）中的哪一个最先到达第一判决单元 18。

可切换延迟元件 17 是结合在控制单元 12 中实施的调节算法、以这样一种方式来进行设定或校正的，其中这两个脉冲是尽可能几乎同时到达的；在延迟脉冲和经由整条延迟线馈送的脉冲基本上同时到达的情况下，在信号传播中产生望期的恒定总延迟 t_1。

在下文中还将参考图 5 中的详细表示并以 PKE 卡 40 为例来描述一种使用了传递时间调节的实施方式，其中将会显示：通过使用一种相同或相似的方式，可以将上述以简单廉价的方式调节信号传递时间的方法用于补偿 PKE 卡 40 中的信号传递时间。

从基站 10 发射到 PKE 卡 40 的脉冲将会传递到多级的(参见附图标记 47a、47b、47y)可切换的(参见附图标记 47s)的第二延迟元件 47。同时，该脉冲还会经由整条延迟线来进行馈送，也就是经由第二延迟元件 47 的所有四级 47a、47b、47y、47z（→延迟时间 t_2）。

判决器（＝PKE 卡 40 的第二判决单元 48）与延迟元件 47 的第四级同时也是最后一级 47z 的下游相连，并且还连接到发射机单元 49b，该判决器用信号向控制单元 42 告知这两个脉冲（“延迟脉冲”或“经由整条延迟线馈送的脉冲”）中的哪一个最先到达第二判决单元 48。

可切换延迟元件 47 是结合在控制单元 42 中实施的调节算法而以这样一种方式来进行设定或校正的，其中这两个脉冲是尽可能几乎同时到达的；在延迟脉冲和经由整条延迟线馈送的脉冲基本上同时到达的情况下，在信号传播中产生期望的恒定总延迟 t_2。

因此，其结果是借助图 4 和 5 所示的电子通信系统 100 以及与这个通信系统 100 相关联的方法而获得了对发射机和接收机单元的信号传递时间容差的补偿，其中有利的是，该补偿可以在无源遥控开锁 PKE 系统或是相似的结构中使用。在这样的系统中，本发明实现了一种形式的传递时间测量，由此可以检测和/或防范以所谓的中继攻击形式的潜在外部攻击。

在这种情况下，所述的电子通信系统 100 以及所述的方法构成对现有技术中可行的信号传递时间测量的灵活、成本有效、新颖并具有创造性的扩展，以允许在实际状况下使用这些测量。在这种情况下，时间测量原理的精度和可靠性（参见图 4 中的时间测量单元 50）都得到了提升。

就此而论，依照本发明，可以克服过去导致很难使用信号传递时间测量的典型特定条件，其中举例来说，这些特定条件是：

- 由于组件容差所导致的发射机和接收机内部的信号传递时间的分散
- 由于温度效应和老化所导致的发射机和接收机内部的信号传递时间变化，和/或
- 用于大规模生产时的成本压力。

有利的是，本发明可以在机动车辆访问系统领域中的应用程度日益提高的无源遥控开锁 PKE 系统中使用。此外，在建筑安全领域，所述的电子通信系统 100 和所述的方法还适合产生基于芯片卡 40 的安全访问系统，在这种情况下，也可以使用图 4 和 5 中显示的所述装置并以相似方式来防范针对访问/入口系统的中继攻击。

附图标记列表

100 电子通信系统

10 基站

11 基站 10 的第一电阻器

12 基站 10 的控制单元，尤其是微控制器单元

13 基站 10 的电容单元

14 基站 10 的模拟接口

15 基站 10 的第二电阻器

16 基站 10 的天线单元

16a 与发射机单元 19a 相关联的基站 10 的天线单元

16b 与接收机单元 19b 相关联的基站 10 的天线单元

17 基站 10 的第一延迟元件

17a 第一延迟元件 17 的第一级

17b 第一延迟元件 17 的第二级

17e 第一延迟元件 17 的设定装置

17s 第一延迟元件 17 的切换装置

17y 第一延迟元件 17 的倒数第二级

17z 第一延迟元件 17 的最后一级

18 基站 10 的第一判决单元

19a 基站 10 的发射机单元

19b 基站 10 的接收机单元

22 上行链路帧

23 上行链路帧仿真

23 下行链路帧

25 下行链路帧仿真

30 附加的传输链路

32 构成应答站 40 的仿真器的第一中继器

34 第一中继器 32 的天线单元

35 第一中继器 32 与第二中继器 36 之间的通信链路

36 构成基站 10 的仿真器的第二中继器

38 第二中继器 36 的天线单元

40 应答站，尤其是数据载体和具体的是无源遥控开锁 PKE 卡

42 应答站 40 的电路装置或控制单元，尤其是微控制器单元

44 应答站 40 的天线单元

44a 与接收机单元 49a 相关联的应答站 40 的天线单元

44b 与发射机单元 49b 相关联的应答站 40 的天线单元

47 应答站 40 的第二延迟元件

47a 第二延迟元件 47 的第一级

47b 第二延迟元件 47 的第二级

47e 第二延迟元件 47 的设定装置

47s 第二延迟元件 47 的切换装置

47y 第二延迟元件 47 的倒数第二级

47z 第二延迟元件 47 的最后一级

48 应答站 40 的第二判决单元

49a 基站 40 的接收机单元

49b 基站 40 的发射机单元

50 时间测量设备

S 基站 10 与应答站 40 之间的距离

t_1 基站 10 内部的信号传递时间

t_2 应答站 40 的信号传递时间

t_{CARD} 应答站 40 的控制单元 42 中的信号传递时间

t_{D1} 基站 10 的第一延迟元件 17 内部的传递时间延迟

t_{D2} 应答站 40 的第二延迟元件 47 内部的传递时间延迟

t_{RXD1} 基站 10 的接收机单元 19b 中的信号传递时间

Δt_{RXD1} 基站 10 的接收机单元 19b 中的信号传递时间容差

t_{RXD2} 应答站 40 的接收机单元 49a 中的信号传递时间

Δt_{RXD2} 应答站 40 的接收机单元 49a 中的信号传递时间容差

t_s 基站 10 与应答站 40 之间的信号传递时间

t_{total} 电子通信系统 100 中的总的信号传递时间

t_{TXD1} 基站 10 的发射机单元 19a 中的信号传递时间

Δt_{TXD1} 基站 10 的发射机单元 19a 中的信号传递时间容差

t_{TXD2} 应答站 40 的发射机单元 49b 中的信号传递时间

Δt_{TXD2} 应答站 40 的发射机单元 49b 中的信号传递时间容差

V_s 基站 10 与应答站 40 之间的信号传播速度

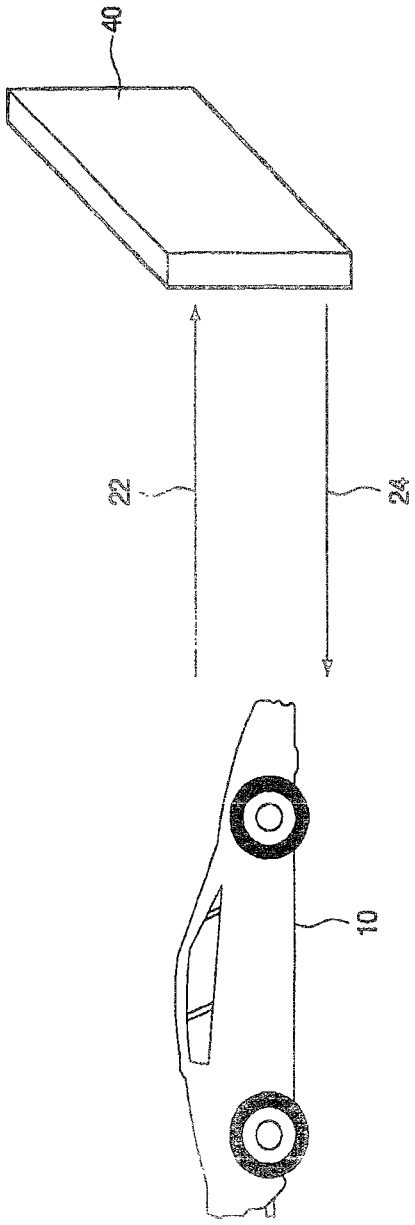
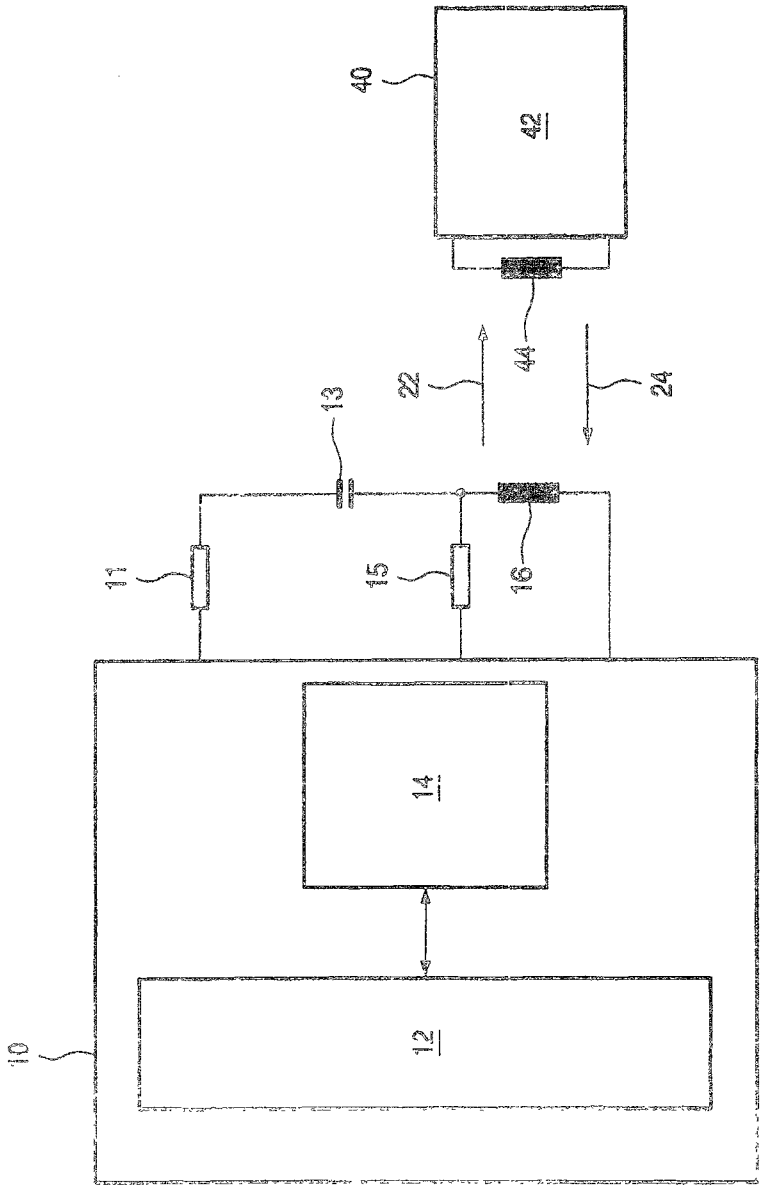


图 1A



1B

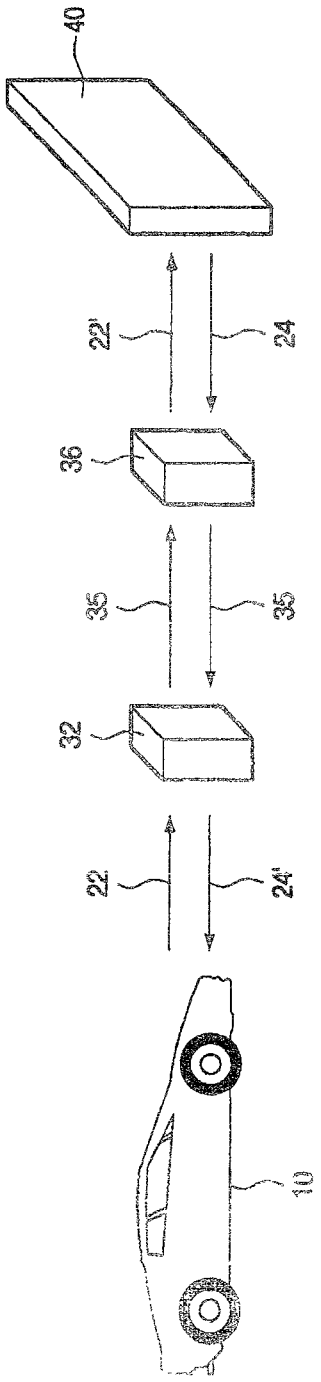


图 2A

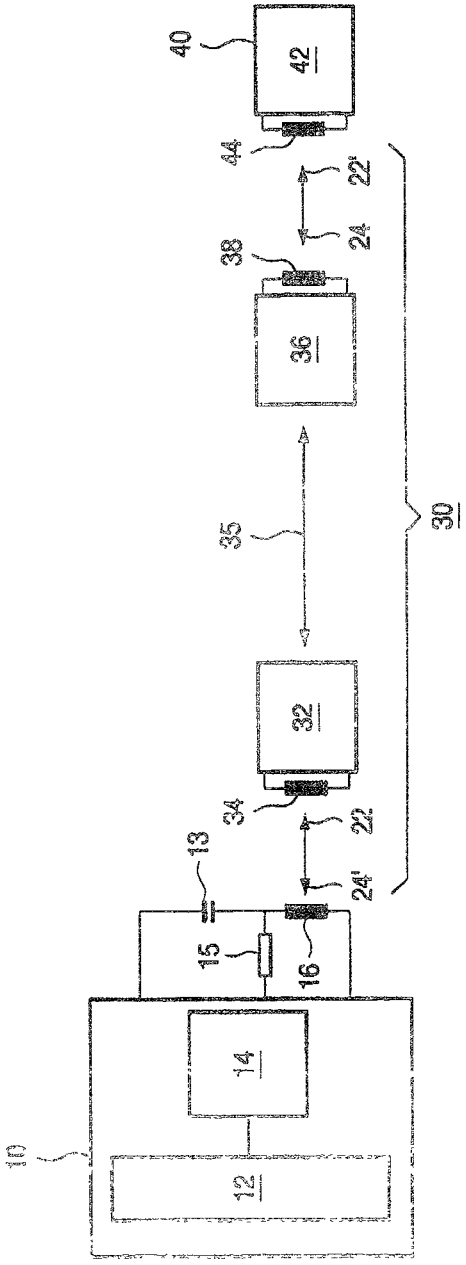


图 2B

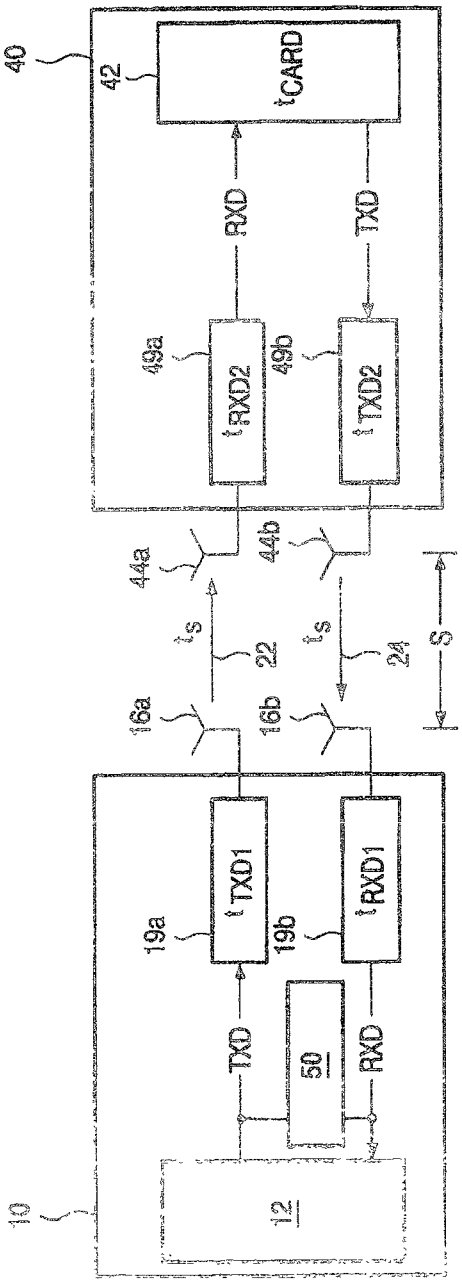

40
42
tCARD
RXD
TXD
49a
tRXD2
49b
tTXD2
44a
44b
ts
22
ts
24
S
16a
16b
19a
tTXD1
19b
tRXD1
TXD
50
RXD
12
10

图 3

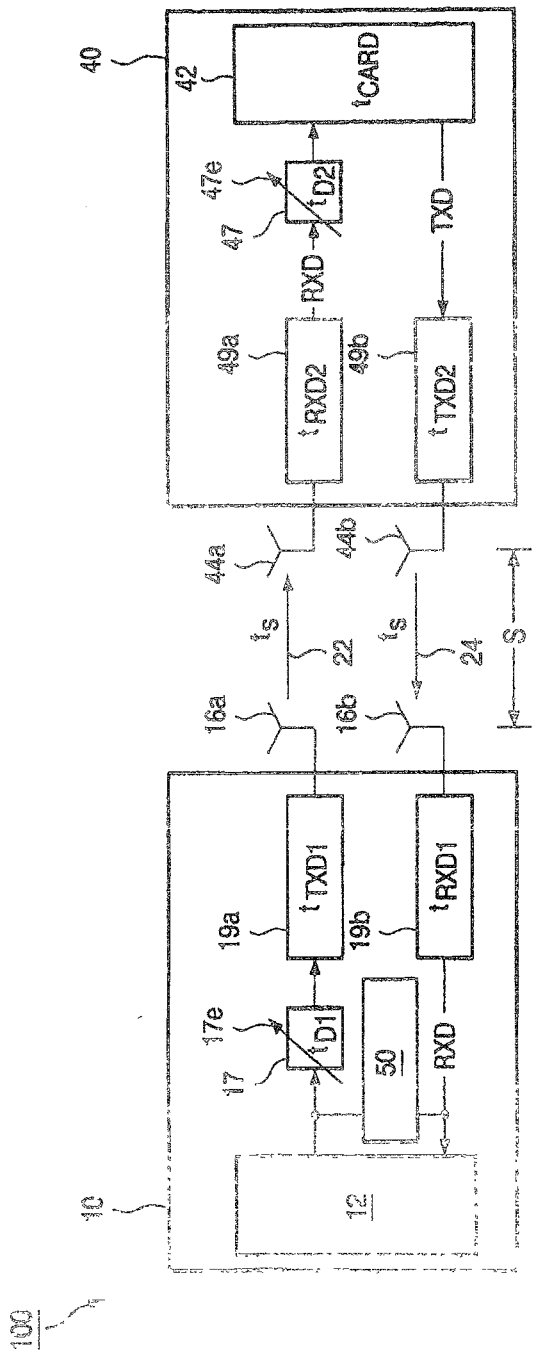

100
10
12
50
17
17e
tD1
19a
tTXD1
19b
tRXD1
RXD
16a
16b
tS
22
24
S
44a
44b
40
42
tCARD
47
47e
tD2
RXD
TXD
49a
tRXD2
49b
tTXD2

图 4

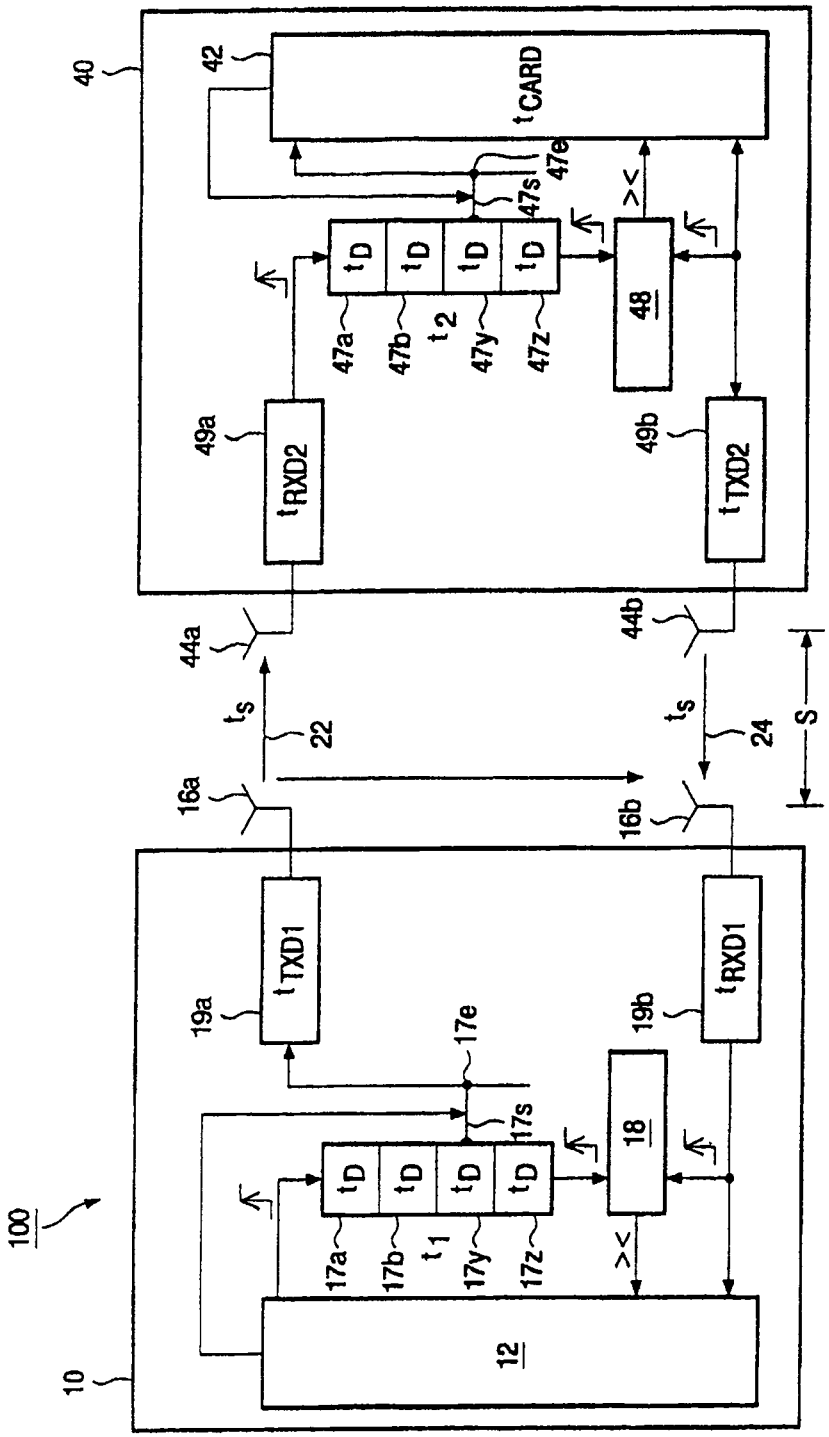

100
10
40
42
tCARD
47e
47s
tD
47a
47b
t2
47y
47z
48
49a
tRXD2
49b
tTXD2
44a
44b
tS
22
24
S
16a
16b
19a
tTXD1
19b
tRXD1
17e
17s
17a
17b
t1
17y
17z
18
12

图 5