[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
E05B 49/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 00814391.9

[45] 授权公告日 2006 年 11 月 22 日

[11] 授权公告号 CN 1285815C

[22] 申请日 2000.9.22 [21] 申请号 00814391.9
[30] 优先权
[32] 1999.10.16 [33] DE [31] 19949970.5
[86] 国际申请 PCT/EP2000/009276 2000.9.22
[87] 国际公布 WO2001/029352 德 2001.4.26
[85] 进入国家阶段日期 2002.4.16
[71] 专利权人 大众汽车有限公司
地址 德国沃尔夫斯堡
共同专利权人 罗伯特－博希股份公司
[72] 发明人 M·梅尔 S·施米茨 A·蒂彻
D·尼梅特舍克
审查员 高东辉

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 程天正 李亚非

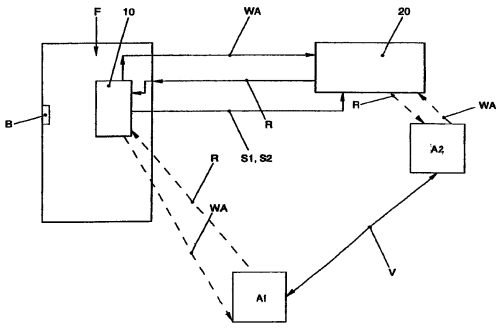
权利要求书 2 页 说明书 5 页 附图 1 页

[54] 发明名称

控制进入受保护的地点的方法和装置

[57] 摘要

用于尤其控制进入车辆(F)的方法，在该方法中，在主动或被动的通信模式下在电子钥匙(20)和基站(10)之间由这些设备(10，20)无线地交换鉴别数据，其中，在该鉴别过程开始时由所述的基站(10)向所述的电子钥匙(20)发射一个呼叫信号(WA)，该电子钥匙根据此呼叫信号(WA)以一个应答信号(R)作出回答，而且其中，所述的基站(10)随后便检查其从所述电子钥匙(20)接收的应答信号(R)是在哪个通信模式下接收的；如果所述电子钥匙(20)的应答信号(R)是以主动通信模式接收到的，那么所述基站(10)将向该电子钥匙(20)发送一个第一选择指令(S1)，由该选择指令促使所述的电子钥匙(20)在所述的主动通信模式下执行随后的通信；如果所述电子钥匙(20)的应答信号(R)是以被动通信模式被接收到的，那么，所述基站(10)将向该电子钥匙(20)发送一个第二选择指令(S2)，由该选择指令促使所述的电子钥匙(20)在该被动通信模式下执行接下来的通信。



1. 用于控制进入受保护的地点(F)的方法，在该方法中，在主动或被动的通信模式下在电子钥匙(20)和基站(10)之间由这些设备(10,20)无线地交换鉴别数据，其中，在该鉴别过程开始时由所述的基站(10)向所述的电子钥匙(20)发射一个呼叫信号(WA)，该电子钥匙根据此呼叫信号(WA)以一个应答信号(R)作出回答，而且其中，在主动通信模式下对无线链路的延长(V)执行一种保险处理，其特征在于:

所述的基站（10）随后便检查其从所述电子钥匙（20）接收的应答信号（R）是在哪个通信模式下接收的；如果所述电子钥匙（20）的应答信号（R）是以主动通信模式接收到的，那么所述基站（10）将向该电子钥匙（20）发送一个第一选择指令（S1），由该选择指令促使所述的电子钥匙（20）在所述的主动通信模式下执行随后的通信；如果所述电子钥匙（20）的应答信号（R）是以被动通信模式被接收到的，那么，所述基站(10)将向该电子钥匙(20)发送一个第二选择指令(S2)，由该选择指令促使所述的电子钥匙（20）在该被动通信模式下执行接下来的通信。

2. 如权利要求 1 所述的方法，其特征在于:

通过如下方式来执行所述主动模式的保险处理，即由电子钥匙（20）在其作为对基站（10）的呼叫信号（WA）的反应而产生的应答信号（R）中向基站(10)传输一个识别码，由基站（10）将该识别码转换成谱数据，并且只有当基站接收的谱数据与存放在基站（10）内的电子钥匙（20）的谱标志相一致时，才继续与电子钥匙（20）进行通信。

3. 如上述权利要求之一所述的方法，其特征在于:

在所述电子钥匙(20)接收到选择指令(S1,S2)之后，该电子钥匙在与所接收的选择指令（S1,S2）相对应的通信模式下至少执行所述鉴别过程的安全性较重要的通信。

4. 如权利要求 3 所述的方法，其特征在于:

在所述电子钥匙(20)接收到选择指令(S1,S2)之后，该电子钥匙在与所接收的选择指令（S1,S2）相对应的通信模式下至少执行所有接下来的鉴别过程。

5. 如上述权利要求 1-2 之一所述的方法，其特征在于:

在所述电子钥匙(20)接收到选择指令(S1,S2)之后，该电子钥

匙在与所接收的选择指令（S1,S2）相对应的通信模式下至少执行所有接下来的鉴别过程。

6. 用于控制进入受保护的地点（F）的装置，它具有一个基站（10）和一个电子钥匙（20），其中，所述的基站(10)和电子钥匙(20)具有用于在主动或被动通信模式下交换鉴别数据的工具，且所述的基站（10）具有一种用于在主动通信模式下对无线链路的延长（V）进行保险处理的工具，其特征在于:

所述的基站（10）具有分析工具，用于在通信模式方面分析从所述电子钥匙（20）接收的应答信号（R）；所述的基站（10）包括用于产生第一选择指令（S1）和把该第一选择指令（S1）发送到所述电子钥匙（20）的工具，以便当在所述基站（10）内以主动通信模式接收所述电子钥匙（20）的应答信号（R）时，由所述的电子钥匙（20）根据所述第一选择指令（S1）的接收而在所述的主动通信模式下同基站（10）执行随后的通信；而且所述的基站（10）包括用于产生第二选择指令（S2）和把该第二选择指令（S2）发送到所述电子钥匙（20）的工具，以便当在所述基站（10）内以被动通信模式接收所述电子钥匙（20）的应答信号（R）时，由所述的电子钥匙（20）在所述的被动通信模式下同基站（10）执行随后的通信。

控制进入受保护的地点的方法和装置

技术领域

本发明涉及一种用于控制进入受保护的地点、尤其是控制进入车辆的方法和装置，在该方法中，在主动或被动的通信模式下在电子钥匙和基站之间由这些设备无线地交换鉴别数据，其中，在该鉴别过程开始时由所述的基站向所述的电子钥匙发射一个呼叫信号，该电子钥匙根据此呼叫信号以一个应答信号作出回答，而且其中，在主动通信模式下对无线链路的延长执行一种保险处理，本发明还涉及一种用于执行该方法的装置。

背景技术

上述类型的方法和装置曾在较早的国际专利申请 PCT/DE99/02178 中讲述过。其中规定，在电子钥匙和基站之间运行的保险处理是如此地进行的，使得在主动工作模式下在电子钥匙和基站之间通过 UHF 频率进行通信，其中电子钥匙和基站之间的传输作用距离是有限的，以确保当拥有该钥匙的人离开受保护的地点（譬如车辆）附近时便中断该通信连接。

在此，为了避免这类被动的进入控制系统可能因如下缘故而失效，即：非法入侵者窃听从基站发送给电子钥匙的呼叫信号，被窃听的信号通过无线链路延长被传送给另一个处于该电子钥匙附近的入侵者，然后由该另一入侵者经过所述的无线链路延长把所述电子钥匙对基站呼叫信号的应答信号再送回到所述的第一入侵者，并通过该第一入侵者送回到基站，因此在该已知的方法中规定，由所述的电子钥匙给基站传输一个信号，并由该基站将其转换成谱数据。因此，只有在传输鉴别数据的过程中当该谱数据与基站内所存储的电子钥匙的谱标志相一致时，所述的基站才允许进入所述受保护的地点。在此规定，电子钥匙所发送的信号至少包括具有不同频率 f_1 或 f_2 的两个音，而且所述的谱数据描述了传输信号的三阶音，它由基站在频率 $2f_1-f_2$ 和 $2f_2-f_1$ 上进行测量。如果所接收的、从电子钥匙发送的信号的二次线的信号强度超过预定的值，则基站将其解释成

已实现无线链路的延长，并拒绝进入所述受保护的地点。

当主动通信模式失效时，为了在所谓的备用模式、也即被动通信模式下还能给电子进入控制的用户提供进入所述受保护的地点的可能性，规定在该被动通信模式下通过被动地调制基站发送的励磁场来在电子钥匙和基站之间实行数据传输：所述的电子钥匙根据需发送的数据而使其谐振回路失调，这可由基站以其振荡回路的附加负载形式来进行测量。在LF频率上产生的被动通信只限于几厘米，这意味着，如果潜在的入侵者试图在备用模式下把钥匙在LF频率上发出的数据信号发送给基站，则他必须将其相应的天线非常靠近于基站的发射天线，以便在该备用模式下工作。该已知的方法和按该方法工作的已知装置具有如下缺点，即它们没有对按上述方式和方法产生的入侵提供有效的保护。

发明内容

因此本发明的任务在于改进文章开头所述的那种方法和装置，使得在被动通信模式下能有效地防止无线链路的延长。

根据本发明的方法，该任务通过如下方式来解决，即：所述的基站随后便检查其从所述电子钥匙接收的应答信号是在哪个通信模式下接收的；如果所述电子钥匙的应答信号是以主动通信模式接收到的，那么所述基站将向该电子钥匙发送一个第一选择指令，由该选择指令促使所述的电子钥匙在所述的主动通信模式下执行随后的通信；如果所述电子钥匙的应答信号是以被动通信模式被接收到的，那么，所述基站将向该电子钥匙发送一个第二选择指令，由该选择指令促使所述的电子钥匙在该被动通信模式下执行接下来的通信。

利用本发明的方法可以有利地实现：通过由基站对其从电子钥匙接收应答信号的通信方式作出有效的反应，即便在电子钥匙和基站之间为被动通信模式的情况下也能防止非法人员的相应入侵。如果应答信号是在主动通信模式下产生的，则在该主动通信模式下执行进一步的鉴别方法，并可以通过已知的保险处理来排除无线链路的延长。但是，如果基站是以被动通信模式接收电子钥匙的应答信号，那么该基站可以有利地阻止经所述的第一主动通信模式在基站和钥匙之间进行通信，直到该进入处理过程结束。因此入侵者不可能利用主动通信模式的频率实现无线链路的延长。

根据本发明的用于控制进入受保护的地点的装置，它具有一个基站和一个电子钥匙，其中，所述的基站和电子钥匙具有用于在主动或被动通信模式下交换鉴别数据的工具，且所述的基站具有一种用于在主动通信模式下对无线链路的延长进行保险处理的工具，其中，所述的基站具有分析工具，用于在通信模式方面分析从所述电子钥匙接收的应答信号；所述的基站包括用于产生第一选择指令和把该第一选择指令发送到所述电子钥匙的工具，以便当在所述基站内以主动通信模式接收所述电子钥匙的应答信号时，由所述的电子钥匙根据所述第一选择指令的接收而在所述的主动通信模式下同基站执行随后的通信；而且所述的基站包括用于产生第二选择指令和把该第二选择指令发送到所述电子钥匙的工具，以便当在所述基站内以被动通信模式接收所述电子钥匙的应答信号时，由所述的电子钥匙在所述的被动通信模式下同基站执行随后的通信。

附图说明

本发明的其它细节和优点可以从下面借助唯一的附图示出的实施例中得出。其中：

图 1 示出了所述方法的实施例的原理简图。

具体实施方式

在图 1 中示出了一种典型的星座，它是下面所讲述的用于控制进入受保护的地点－此处是控制进入车辆 F－的方法的出发点。在所述的车辆 F 内布置了基站 10，该基站 10 无线地与电子钥匙 20 交换鉴别数据，以确保只有该电子钥匙 20 的拥有者才能进入所述受保护的地点。为此规定，当车辆 F 上的操作机构 B－譬如门把手－被操作时，所述基站 10 在主动的第一通信模式下给电子钥匙 20 发送一个呼叫信号 WA。随后，该电子钥匙 20 在主动通信模式下利用相应的应答信号 R 作出回答，由此在电子钥匙 20 和基站 10 之间建立一个在主动通信模式下运行的通信连接。在电子钥匙 20 和基站 10 之间传输的数据通过一种已知的、在此不再详细讲述的通信协议来确定，其中所述的电子钥匙 20 和基站 10 遵守该通信协议，而且该通信协议还包括把鉴别数据从电子钥匙 20 传输到基站 10。只有当电子钥匙 20 所传输的鉴别数据与基站 10 所存储的鉴别数据相一致时，所述的基站 10 才允许进入受保护的车辆 F。此处规定，由电子钥匙 20 和/或

基站 10 发送的信号只具有有限的作用距离，以防止当所述电子钥匙 20 不在所述车辆 F 的预定范围－典型地为几米－之内时也能由基站 10 允许进入所述受保护的车辆 F。

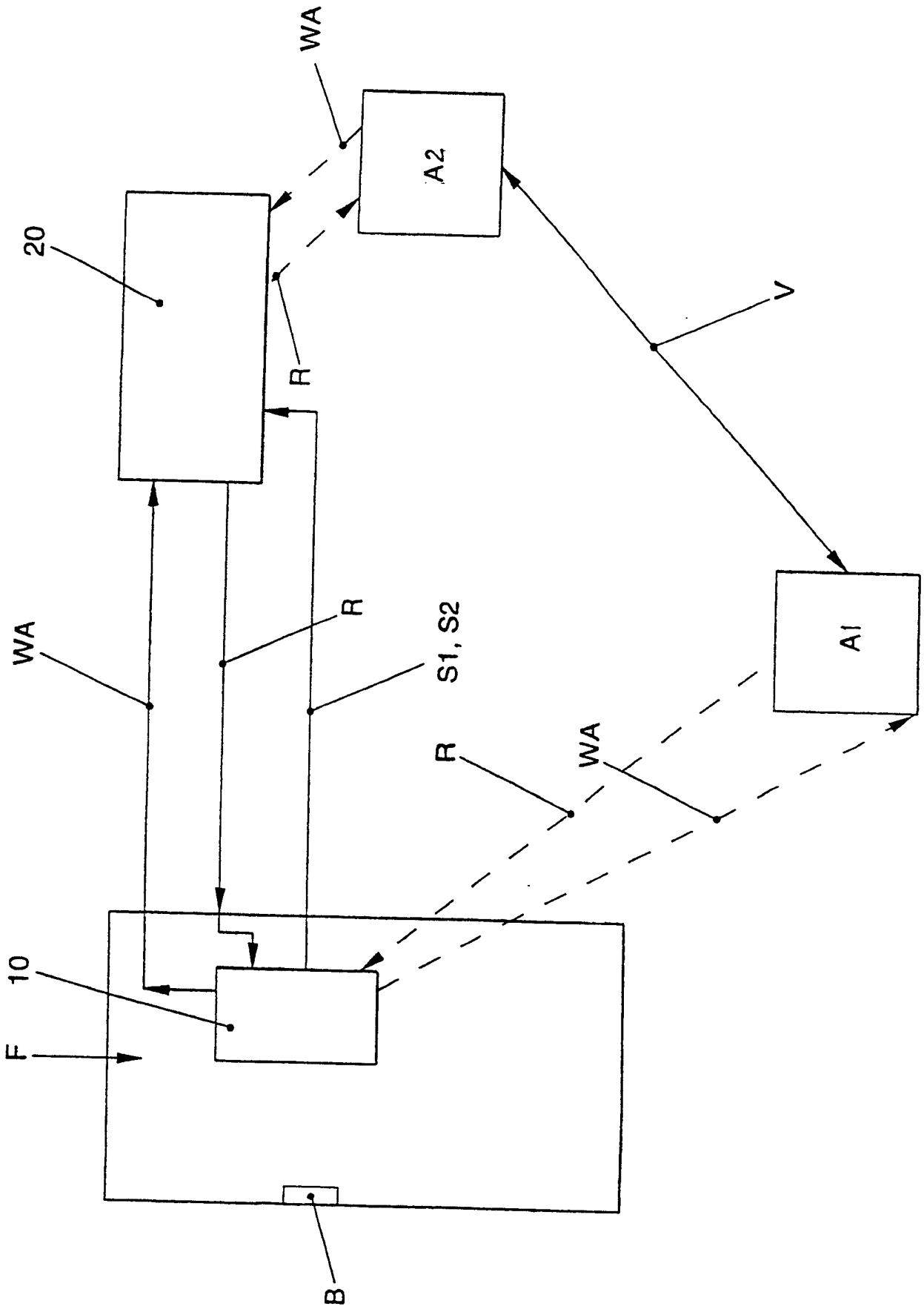
在此，为了防止入侵者通过如下方式设法进入所述受保护的车辆 F，即：第一入侵者 A1 借助无线链路延长 V 把基站 10 在第一主动通信模式下发出的呼叫信号 WA 传送给第二入侵者 A2，然后该第二入侵者 A2 把该基站 10 的呼叫信号 WA 传送给位于基站 10 的作用距离之外的电子钥匙 20，并接收电子钥匙 20 的应答信号 R，继而通过无线链路延长 V 把该信号传送给所述的第一入侵者 A1，该第一入侵者再将该电子钥匙 20 的应答信号 R 传送给基站 10，因此规定，在所述电子钥匙 20 和基站 10 之间以第一主动通信模式执行的通信还具有一种保险处理，它可以识别相应信号 WA、R 的这种无线链路延长 V，并在必要时据此中断通信。这种保险处理譬如在较早的国际专利申请 PCT/DE99/02178 中讲述过，为了避免重复可以参考该文献，而且通过参考其公开内容可以使本技术理论的内容更加明确。在那儿它可以按如下方式来实现，即由电子钥匙 20 在其作为对基站 10 的呼叫信号 WA 的反应而产生的应答信号 R 中传输一个识别信号，由基站 10 将该识别信号转换成谱数据，并且只有当基站接收的谱数据与存放在基站 10 内的电子钥匙 20 的谱标

志相一致时，才继续与电子钥匙 20 进行通信。在此尤其规定，由电子钥匙 20 发送具有频率 f_1 和 f_2 的两个音，它们随后由基站 10 进行测量。然而，不仅可以接收所述的两个音 f_1 和 f_2，而且还可以接收两个高阶基音的混合，这些音是在一些按频率与基音分开的频道内接收的。如果此时所接收的、尤其是三阶二次线的信号强度超过预定的值，则可靠地指示出所接收的电子钥匙 20 的信号是经无线链路延长 V 传送的。于是在该情形下，基站 10 将中断与电子钥匙 20 的通信，并阻止进入受保护的车辆 F。

由于通常都规定所述的电子钥匙 20 和基站 10 不仅能以上述主动通信模式相互进行通信，而且还能以所谓的备用模式在第二被动模式下彼此通信，所以还需要在该被动通信模式下为该被动通信模式设立另一个保险处理过程，其中所述主动通信模式的保险处理在该被动通信模式下是不起作用的。

这可以按如下方式有利地实现，即基站 10 不仅分析输入给它的信号的信息内容、尤其是钥匙 20 的应答信号 R，而且还检查所述电子钥匙 20 输入给它的信号是以第一主动通信模式还是以第二被动通信模式接收的。如果基站 10 以第一主动通信模式接收到所述电子钥匙 20 作为对基站发送的呼叫指令 WA 的反应而产生的应答信号 R，那么，作为对所述以主动通信模式从电子钥匙 20 接收到的应答信号 R 的反应，所述基站 10 将向该电子钥匙 20 发送一个第一选择信号 S1，除了普通的选择信号功能之外，该选择信号还促使专门在所述的第一主动通信模式下在电子钥匙 20 和基站 10 之间至少执行安全性较重要的通信，优选还执行所有的进一步通信，并且中断在被动通信模式下执行剩余的鉴别过程。这有个优点，就是可以通过该主动通信模式的保险处理来检测出无线链路的延长 V，并在必要时针对非法人员的入侵采取相应的措施。

但是，如果车辆 F 的基站 10 以第二被动通信模式接收到所述电子钥匙 20 的应答信号 R，那么，作为对该应答信号的反应，所述基站将向该电子钥匙 20 发送一个第二选择信号 S2，该选择信号以相应的方式和方法促使在所述的第二被动通信模式下执行进一步的鉴别过程的通信，并中断在第一通信模式下执行剩余的鉴别过程。于是，在主动通信模式下工作的无线链路延长 V 再也不能成功地被入侵者使用。


WA
A2
20
R
V
R
S1, S2
WA
A1
R
WA
10
F
B