(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 102223362 B
(45)授权公告日 2015.09.09

(21)申请号 201110097813.3
(22)申请日 2011.04.19
(30)优先权数据
12/762428 2010.04.19 US
(73)专利权人 通用汽车环球科技运作有限责任公司
地址 美国密执安州
(72)发明人 B.R. 贝卢尔 D. 巴塔查亚 A.V. 艾尔
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 代易宁
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
(56)对比文件
US 2009/0260057 A1,2009.10.15, 全文.
US 2008/0027602 A1,2008.01.31, 说明书第[0049]-[0071]段,图1-5.
审查员 王戬

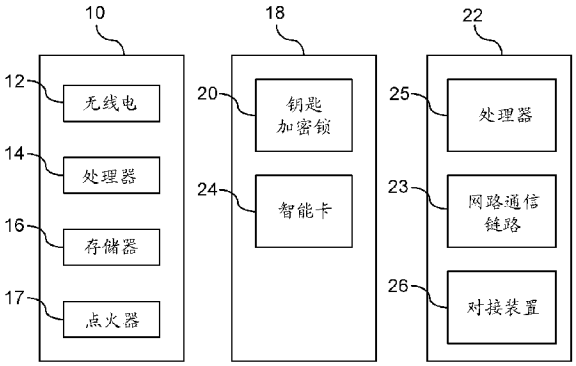
权利要求书2页 说明书5页 附图2页

(54)发明名称

车辆对车辆通信网络中的威胁缓解

(57)摘要

提供了一种为车辆对车辆通信系统中的车辆获得证书撤销清单(CRL)的方法。提供便携安全单元以访问车辆的安全操作。便携安全单元链接到能访问通信网络的装置。通信网络与用于发布更新的CRL的证书认证机构通信。已更新的CRL从证书认证机构下载到便携安全单元。稍后,当用户进入车辆,在便携安全单元和车辆处理器单元之间建立通信链路。在便携安全单元和车辆处理单元之间交换相互鉴权。响应于成功的相互鉴权,存储在便携安全单元内的已更新CRL下载到车辆通信系统的存储器。



CN 102223362 B

1. 一种为车辆对车辆通信系统中的车辆获得证书撤销清单 CRL 的方法，所述方法包括以下步骤：

提供便携安全单元来访问所述车辆的安全操作；

将所述便携安全单元链接到能够访问通信网络的网络装置，所述通信网络与用于发布更新的 CRL 的证书认证机构通信；

将所述已更新的 CRL 从所述证书认证机构下载到所述便携安全单元；

建立所述便携安全单元和车辆处理单元之间的通信链路；以及

在所述便携安全单元和所述车辆处理单元之间交换相互鉴权，其中，响应于成功的相互鉴权，存储在所述便携安全单元内的已更新的 CRL 下载到所述车辆处理单元的存储器。

2. 如权利要求 1 的方法，其特征在于，通过将点火钥匙插进车辆点火器内来开始建立所述便携安全单元和车辆处理单元之间的链路。

3. 如权利要求 1 的方法，其特征在于，所述便携安全单元通过有线连接与所述通信网络通信。

4. 如权利要求 1 的方法，其特征在于，所述便携安全单元通过无线连接与所述通信网络通信。

5. 如权利要求 1 的方法，其特征在于，所述网络装置通过因特网与证书认证机构通信。

6. 如权利要求 1 的方法，其特征在于，所述便携安全单元利用对接装置与所述网络装置通信。

7. 如权利要求 1 的方法，其特征在于，所述已更新的 CRL 存储在所述便携安全单元的存储卡内。

8. 如权利要求 1 的方法，其特征在于，所述已更新的 CRL 通过运行在后端服务器的集中恶意节点检测系统来计算。

9. 如权利要求 8 的方法，其特征在于，所述集中恶意节点检测系统检测所述车辆对车辆通信系统中的异常。

10. 如权利要求 1 的方法，其特征在于，包副本从所述便携安全单元上传到所述证书认证机构，以辅助检测所述车辆对车辆通信系统中的异常。

11. 如权利要求 1 的方法，其特征在于，加密证书从所述证书认证机构下载到车辆，用于为所述车辆对车辆通信系统中的用户提供增强的隐私。

12. 一种车辆对车辆通信系统，包括：

用于控制车辆对车辆通信系统中的无线消息广播的车辆通信处理单元，所述车辆通信处理单元具有用于存储证书撤销清单 CRL 的存储器；以及

用于链接到所述车辆通信处理单元的便携安全单元，响应于彼此的链接，所述便携安全单元与所述车辆通信处理单元通信，用于执行所述便携安全单元与所述车辆通信处理单元之间的相互鉴权，所述便携安全单元具有用于存储已更新的证书撤销清单的非易失性存储器；

其中，所述便携安全单元链接到能够访问通信网络的网络装置，所述通信网络与用于发布更新的 CRL 的证书认证机构通信，其中所述已更新的 CRL 从所述证书认证机构下载到所述便携安全单元，其中，响应于开始车辆安全操作，所述便携安全单元建立到所述车辆通信处理单元的通信链路，以及其中，响应于所述便携安全单元和所述车辆通信处理单元之

间的相互鉴权，存储在所述便携安全单元内的所述已更新的 CRL 下载到所述车辆通信处理单元的存储器。

13. 如权利要求 12 的车辆对车辆通信系统，其特征在于，所述便携安全单元包括钥匙加密锁。

14. 如权利要求 13 的车辆对车辆通信系统，其特征在于，响应于点火钥匙被插进点火器内，所述便携安全单元和所述车辆通信处理单元交换相互鉴权。

15. 如权利要求 14 的车辆对车辆通信系统，其特征在于，所述钥匙加密锁结合作为所述点火钥匙的一部分。

16. 如权利要求 15 的车辆对车辆通信系统，其特征在于，进一步包括用于与所述网络装置通信的对接装置。

17. 如权利要求 16 的车辆对车辆通信系统，其特征在于，用于从所述通信网络下载所述已更新的 CRL 的所述网络装置包括计算机。

18. 如权利要求 16 的车辆对车辆通信系统，其特征在于，用于从所述通信网络下载所述已更新的 CRL 的所述网络装置包括基于电话的装置。

19. 如权利要求 14 的车辆对车辆通信系统，其特征在于，所述钥匙加密锁包括用于存储下载的所述已更新 CRL 的存储卡。

20. 如权利要求 12 的车辆对车辆通信系统，其特征在于，使用集中恶意节点检测例程来检测所述车辆对车辆通信网络中的异常。

21. 如权利要求 12 的车辆对车辆通信系统，其特征在于，所述存储器存储车辆对车辆通信的包副本，所述包副本被上传到所述证书认证机构，用于辅助检测所述车辆对车辆通信系统中的异常。

车辆对车辆通信网络中的威胁缓解

技术领域

[0001] 实施例大体涉及车辆对车辆通信系统。

背景技术

[0002] 在因特网上使用证书撤销清单(CRL)来完成证书有效性的检查已经激发了 CRL 在其它背景下的使用,如车辆对车辆的通信。由于车辆不处于可以向证书认证机构提供可达性的路侧设备的通信范围内,由此导致与证书认证机构之间断续的连接,不能更新正在检验的已撤销状态的证书将导致对签有已撤销证书消息的接受。在车辆通信系统中,通过与路侧设备的通信来获得 CRL。然而,如果车辆不能经常地与路侧设备通信,那么车辆将不能获得 CRL 的更新清单。

发明内容

[0003] 实施例的优点是利用通信网络(而不是车辆通信系统)和路侧设备通信信道获取已更新的证书撤销清单。车辆用户可以利用如因特网的通信网络,建立与证书认证机构的通信链路,用于根据用户需求下载更新的 CRL。

[0004] 实施例设想了一种用于为在车辆对车辆系统中的车辆获得证书撤销清单(CRL)的方法。提供了便携安全单元来访问车辆的安全操作。便携安全单元链接到能够访问通信网络的装置。通信网络与证书认证机构通信,用于发布已更新的 CRL。已更新的 CRL 被从证书认证机构下载到便携安全单元。在便携安全单元和车辆处理器单元之间建立通信链路。便携安全单元与车辆处理单元之间交换相互鉴权。响应于成功的相互鉴权,存储在便携安全单元中的已更新 CRL 被下载到车辆通信系统的存储器中。

[0005] 实施例设想了车辆对车辆通信系统。车辆通信处理单元用于控制车辆对车辆通信系统内的无线消息广播。车辆通信处理单元具有用于存储证书撤销清单的存储器。便携安全单元链接到车辆处理单元。响应于彼此链接,便携安全单元与处理单元通信,用于执行便携安全单元与车通信处理单元之间的相互鉴权。便携安全单元具有用于存储包副本和已更新的证书撤销清单的非易失性存储器。便携安全单元链接到能访问通信网络的装置。通信网络与证书认证机构通信,用于将包副本从便携安全单元上传到认证机构(CA),且从 CA 下载已更新的 CRL 到便携安全单元。响应于初始化车辆安全操作,便携安全单元建立到车辆通信系统的通信链路。响应于便携安全单元与车辆处理单元之间的相互鉴权,存储在便携安全单元的已更新 CRL 下载到车辆通信系统的存储器。

[0006] 本发明还包括以下技术方案。

[0007] 1. 一种为车辆对车辆通信系统中的车辆获得证书撤销清单(CRL)的方法,所述方法包括以下步骤 :

[0008] 提供便携安全单元来访问所述车辆的安全操作 ;

[0009] 将所述便携安全单元链接到能够访问通信网路的网络装置,所述通信网络与用于发布更新的 CRL 的证书认证机构通信 ;

[0010] 将所述已更新的 CRL 从所述证书认证机构下载到所述便携安全单元；

[0011] 建立所述便携安全单元和车辆处理器单元之间的通信链路；以及

[0012] 在所述便携安全单元和所述车辆处理单元之间交换相互鉴权，其中，响应于成功的相互鉴权，存储在所述便携安全单元内的已更新的 CRL 下载到所述车辆通信系统的存储器。

[0013] 2. 如技术方案 1 的方法，其特征在于，通过将点火钥匙插进车辆点火器内来开始建立所述便携安全单元和车辆处理单元之间的链路。

[0014] 3. 如技术方案 1 的方法，其特征在于，所述便携安全单元通过有线连接与所述通信网络通信。

[0015] 4. 如技术方案 1 的方法，其特征在于，所述便携安全单元通过无线连接与所述通信网络通信。

[0016] 5. 如技术方案 1 的方法，其特征在于，所述网络装置通过因特网与证书认证机构通信。

[0017] 6. 如技术方案 1 的方法，其特征在于，所述便携安全单元利用对接装置与所述网络装置通信。

[0018] 7. 如技术方案 1 的方法，其特征在于，所述已更新的 CRL 存储在所述便携安全单元的存储卡内。

[0019] 8. 如技术方案 1 的方法，其特征在于，所述已更新的 CRL 通过运行在后端服务器的集中恶意节点检测系统计算。

[0020] 9. 如技术方案 1 的方法，其特征在于，所述集中恶意节点检测系统检测所述车辆对车辆通信系统中的异常。

[0021] 10. 如技术方案 1 的方法，其特征在于，包副本从所述便携安全单元上传到所述证书认证机构，以辅助检测所述车辆对车辆通信系统中的异常。

[0022] 11. 如技术方案 1 的方法，其特征在于，加密证书从所述证书认证机构下载到车辆，用于为所述车辆对车辆通信系统中的用户提供增强的隐私。

[0023] 12. 一种车辆对车辆通信系统，包括：

[0024] 用于控制车辆对车辆通信系统中的无线消息广播的车辆通信处理单元，所述车辆通信处理单元具有用于存储证书撤销清单（CRL）的存储器；以及

[0025] 用于链接到所述车辆处理单元的便携安全单元，响应于彼此的链接，所述便携安全单元与所述处理单元通信，用于执行所述便携安全单元与所述车辆通信处理单元之间的相互鉴权，所述便携安全单元具有用于存储已更新的证书撤销清单的非易失性存储器；

[0026] 其中，所述便携安全单元链接到能够访问通信网络的网络装置，所述通信网络与用于发布更新的 CRL 的证书认证机构通信，其中所述已更新的 CRL 从所述证书认证机构下载到所述便携安全单元，其中，响应于开始车辆安全操作，所述便携安全单元建立到所述车辆通信系统的通信链路，以及其中，响应于所述便携安全单元和所述车辆处理单元之间的相互鉴权，存储在所述便携安全单元内的所述已更新的 CRL 下载到所述车辆通信系统的存储器。

[0027] 13. 如技术方案 12 的车辆对车辆通信系统，其特征在于，所述便携安全单元包括钥匙加密锁。

[0028] 14. 如技术方案 13 的车辆对车辆通信系统，其特征在于，响应于点火钥匙被插进点火器内，所述便携安全单元和所述车辆通信处理器交换相互鉴权。

[0029] 15. 如技术方案 14 的车辆对车辆通信系统，其特征在于，所述钥匙加密锁结合作为所述点火钥匙的一部分。

[0030] 16. 如技术方案 15 的车辆对车辆通信系统，其特征在于，进一步包括用于与所述网络装置通信的对接装置。

[0031] 17. 如技术方案 16 的车辆对车辆通信系统，其特征在于，用于从所述通信网络下载所述已更新的 CRL 的所述网路装置包括计算机。

[0032] 18. 如技术方案 16 的车辆对车辆通信系统，其特征在于，用于从所述通信网络下载所述已更新的 CRL 的所述网路装置包括基于电话的装置。

[0033] 19. 如技术方案 14 的车辆对车辆通信系统，其特征在于，所述钥匙加密锁包括用于存储下载的所述已更新 CRL 的存储卡。

[0034] 20. 如技术方案 12 的车辆对车辆通信系统，其特征在于，使用集中恶意节点检测例程来检测所述车辆对车辆通信网络中的异常。

[0035] 21. 如技术方案 12 的车辆对车辆通信系统，其特征在于，所述存储器存储车辆对车辆通信的包副本，所述包副本被上传到所述证书认证机构，用于辅助检测所述车辆对车辆通信系统中的异常。

附图说明

[0036] 图 1 是根据实施例的 CRL 获取系统中使用的通信装置的示例性示意图。

[0037] 图 2 是根据实施例的 CRL 获取系统的框图。

[0038] 图 3 是根据实施例的用于更新 CRL 的方法的流程图。

具体实施方式

[0039] 图 1 显示车辆对车辆通信系统（V2V）。V2V 通信系统很容易从源（而不是路侧设备）下载已更新的证书撤销清单（CRL），路侧设备通常是用于更新 CRL 的主要通信接口装置。V2V 通信系统包括与一或多个远程实体通信的宿主车辆。远程实体可以是远程车辆或 RSE。应该理解的是相对于远离宿主车辆的车辆而言，各车辆将其自身视为宿主车辆。因此，在上下文中术语宿主车辆指的是本说明书所介绍的相应车辆。

[0040] CRL 是已撤销的或不再有效的数字证书清单。宿主车辆从远程实体接收消息，该消息的数字证书已被撤销或不再有效，宿主车辆不应该依赖该消息，该消息应该被忽略。数字证书被撤销的原因包括但不限于，证书认证机构（CA）不恰当地发布证书，证书持有者的错误行为（包括违反 CA 指定的政策），或者如果私有密钥被视为已泄漏（即，被应被发布该密钥的实体之外的任何实体了解）。

[0041] CRL 被定期再生和再发布，或者可以在数字证书被撤销后再进行再生和再发布。数字证书也可以有失效日期，用于检查来确定数字证书的有效性。每当一请求实体想要依赖数字证书时，应该检查数字证书状态；否则由持有（已撤消）数字证书的实体签名的消息可能被错误的接受为可依赖。因此，应该具有一个最近的 CRL 清单。在车辆通信中的问题是车辆不能与路侧实体或其它通信装置连续通信（由于广播范围）。因此，更新 CRL 仅可能出

现在车辆在 RSE 的通信范围内时。

[0042] 本文介绍的实施例通过拥有在 CA 和车辆之间的经常连接机制，提供了一种在车辆对车辆通信网络中用于威胁缓解的有效技术。对 CA 和车辆之间经常连接的需求提供了一些优点。首先，如果用户（如，网络中的车辆）能经常接触 CA，那么车辆对车辆通信的已更新副本能够上传以辅助 CA 检测错误行为的车辆，有助于建立撤销清单。副本是在一特定持续时间内通过 DSRC 天线收到的消息的摘要。副本可以是详尽的（即，包括接收到的所有消息）、随机的（即，包括接收到消息的随机片段）或是选择性的（即，只包括车辆感知视为可疑的或异常的消息）。通过长时间不上传可疑消息的副本，产生在识别和撤销错误行为身份方面的延迟。第二，用户能够通过经常与 CA 交互来下载更新的撤销信息。在长时间后获得撤销信息导致用户可能从撤销实体处接受包的“漏洞窗口”。另外，经常在 CA 和车辆之间交互的另一个优点是提供了更高级别的隐私。而且，通过分配特定于地理区域的证书，方便了跨地理区域的迁移。特别是，用户能够足够经常地刷新他们的身份 / 认证以增强隐私。

[0043] 参考图 1 和图 2，显示的车辆 10 具有 V2V 或车辆对实体（V2X）的通信能力。车辆 10 包括无线电 12（如，接收器的后端），无线电包括用于发射和接收无线消息的发射器和接收器（或发射接收器）。车辆 10 进一步包括用于处理在所接收到的无线消息或诸如全球定位系统（GPS）接收器的其它无线装置中所接收到的数据的处理单元 14（如，协议栈）。处理单元 14 可包括但不限于，电子控制单元（ECU），用于控制访问车辆以及车辆的发动机启动操作。V2V 通信系统还包括用于存储诸如 CRL 的数据的存储器 16，CRL 用于确定数字证书是否被撤销。

[0044] V2V 通信系统的处理单元 14 与便携安全单元 18 通信。便携安全单元 18 优选地结合作为用于访问车辆内部和促动车辆发动机启动的车辆点火钥匙的一部分。或者，便携安全单元可以是独立的装置或结合作为其它部件的一部分。便携安全单元 18 包括加密锁（dongle）20。加密锁 20 是一小块便携硬件，其与诸如计算机的网络装置 22 通信，并链接到通信网络 23，甚至到处理单元 14。加密锁 20 优选地与车辆点火钥匙在一起，用于与车辆的处理单元 14 通信。加密锁 20 包括存储器 24，如智能卡、快闪存储器等，用于存储访问车辆功能的代码和用于存储已更新的 CRL 和包副本。

[0045] 当链接到网络装置 22 时，加密锁 20 访问通信网络 23，用于上传包副本和从证书认证机构下载已更新的 CRL。加密锁 20 利用对接装置 26 来与网络装置 22（如计算机）通信。对接装置 26 可以利用有线连接或无线连接来与网络装置 22 通信。网络装置 22 进一步包括通过通信网络 23 控制与 CA 通信的处理器 25。通信网络 23 可以包括因特网或任何其它的通信介质。网络装置 22 用于与 CA 通信，用于根据用户请求上传包副本和获得已更新的 CRL。已更新的 CRL 通过装置 22 从 CA 下载到加密锁 20。加密锁 20 将下载的 CRL 存储在存储器 24 中。在从 CA 处成功地下载 CRL 后，加密锁 20 被从对接站 26 处移除。另外，伪名称形式的加密证书或其它证书可以从 CA 下载到车辆。伪名称不包含关于车辆的任何个人的或身份信息，但是使车辆能够执行发送和接收 V2V 消息所必要的安全协议。这就增强了 V2V 通信系统中的用户隐私。使用对应于各伪名称的加密材料签名的消息一般会追加相应的伪名称，用于接收方来验证消息的真实性。只要车辆使用相同的伪名称，观测器就能够链接到由相应车辆发送的消息。通过使用各伪名称一小段时间，车辆可以获得匿名性和周期性地从 CA 处请求新的伪名称集。

[0046] 一旦用户进入车辆，便携安全单元链接到车辆处理单元 14。在优选实施例中，通过将点火钥匙插进车辆点火器 17 开始将便携安全单元 18 链接到车辆处理单元 14，用于在加密锁和车辆处理单元 14 之间相互鉴权。一旦鉴权成功，已更新的 CRL 从加密锁 20 下载到车辆的处理单元 14。处理单元 14 利用已更新的 CRL 来确定已收到的消息的数字证书是否是已撤销的。

[0047] 在发送已更新的 CRL 前，在后端服务器执行的集中恶意节点检测系统分析接收到的包副本。集中恶意节点检测系统检测车辆对车辆通信系统中的异常。

[0048] 图 3 显示了用于更新 V2V 或 V2X 通信系统中的车辆 CRL 的方法的流程图。在步骤 30，提供了便携安全单元用于访问车辆的安全车辆操作。便携安全单元可以与点火钥匙结合。或者，便携安全单元可以与另一装置结合或可以是独立装置。便携安全单元包括用于存储一个或多个代码来访问安全操作的加密锁。

[0049] 在步骤 31，便携安全单元链接到具有与通信网络的通信链路的网络装置。网络装置可以包括但不限于计算机、电话、个人数字助理。便携安全单元可以利用对接站建立与网络装置的通信。对接站可以利用到网络装置（如计算机）的无线或有线的连接。

[0050] 在步骤 32，诸如计算机的网络装置进行与证书认证机构（CA）的通信。根据在接收到的包副本中检测的异常，证书认证机构相应地发布更新的 CRL。在 CRL 中列举的证书是由于期满、恶意行为或私有密钥被泄漏而撤销的数字证书。计算机根据用户请求下载局部区域的已更新证书。

[0051] 在步骤 33，初始化在加密锁和车辆处理器之间的相互鉴权，用于允许诸如发动机启动操作的安全操作。建立相互鉴权可以包括将点火钥匙插进点火器中，用于开始发动机启动操作。集成在点火钥匙内或便携安全装置内的加密锁与车辆处理器通信来相互鉴权。

[0052] 在步骤 34，响应于车辆操作或安全操作的开始（如将点火钥匙插进点火器中），建立便携通信装置和车辆处理器之间的链路。

[0053] 在步骤 35，建立了相互鉴权。成功的鉴权发生在便携安全单元验证了车辆通信处理器时，以及当车辆通信处理器验证了便携安全装置时。

[0054] 在步骤 36，在两装置相互鉴权后，已更新的 CRL 从加密锁下载到车辆处理器。另外，伪名称形式的加密证书或其它证书可从 CA 下载到车辆。而且，可以上传车辆对车辆通信的已更新副本来辅助 CA 检测错误行为的车辆，有助于建立撤销清单。

[0055] 在步骤 37，CRL 存储在车辆处理器存储器等中，用于检查与车辆接收到的消息相关的数字证书是否已撤销。如果数字证书是已撤销的，消息就被忽略。如果接收到的消息的数字证书不是已撤销的，那么消息被接受或者保留用于其它处理。

[0056] 尽管已经详细介绍了本发明的某些实施例，但是对本发明涉及到的领域熟悉的技术人员将意识到用于实践由权利要求限制的发明的各种备选设计和实施例。

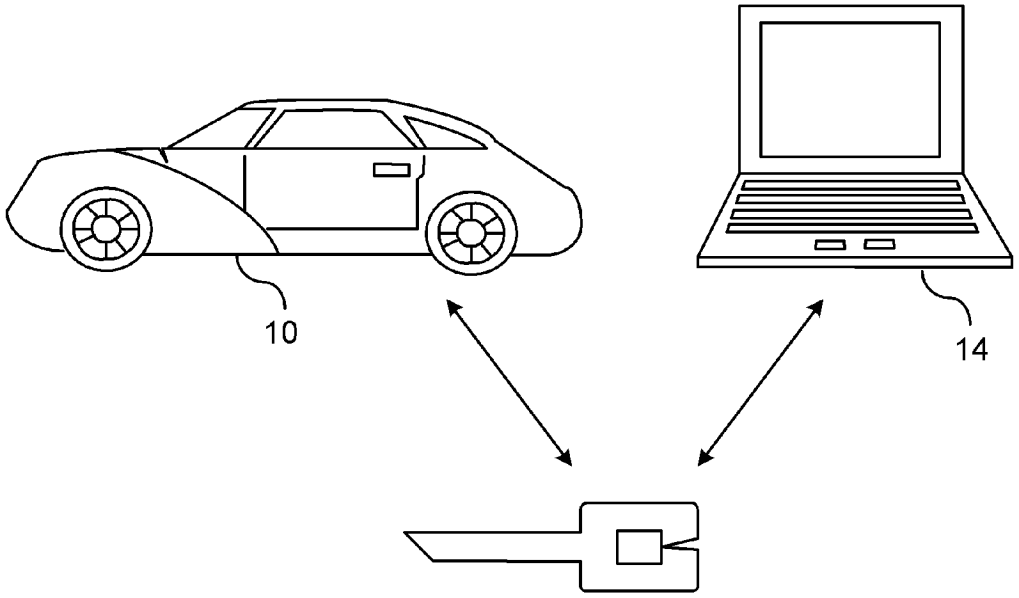

10
14

图 1

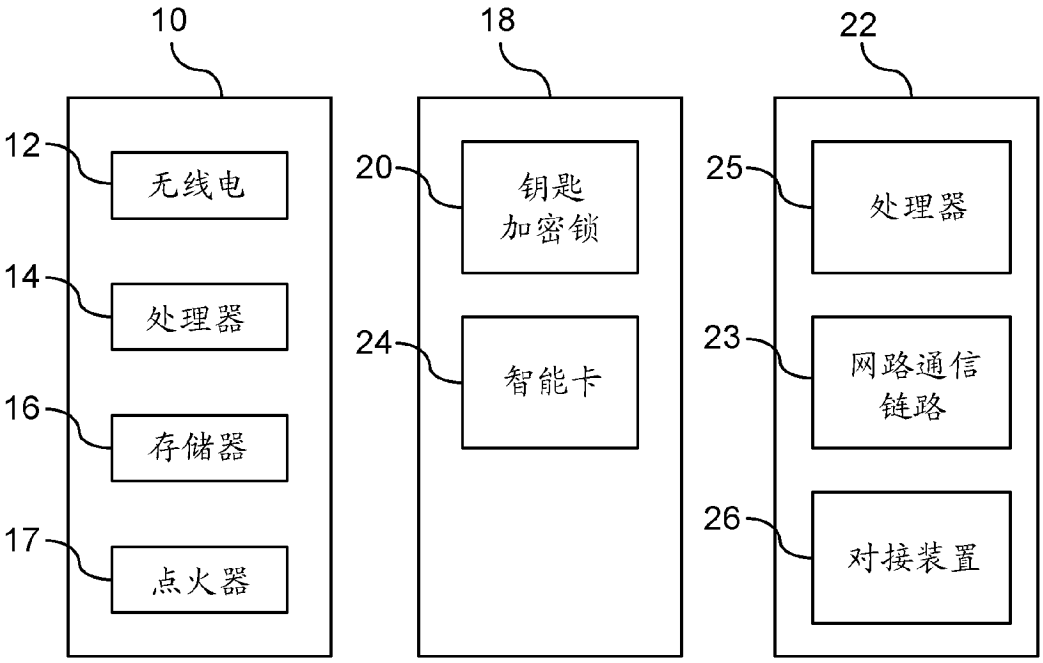

10
12
无线电
14
处理器
16
存储器
17
点火器
18
20
钥匙
加密锁
24
智能卡
22
25
处理器
23
网路通信
链路
26
对接装置

图 2

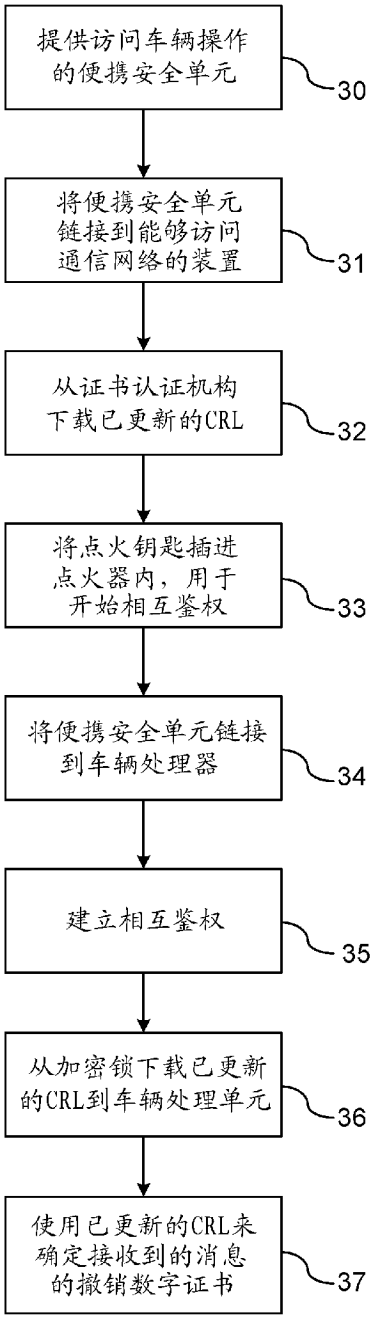

提供访问车辆操作的便携安全单元
30
将便携安全单元链接到能够访问通信网络的装置
31
从证书认证机构下载已更新的CRL
32
将点火钥匙插进点火器内，用于开始相互鉴权
33
将便携安全单元链接到车辆处理器
34
建立相互鉴权
35
从加密锁下载已更新的CRL到车辆处理单元
36
使用已更新的CRL来确定接收到的消息的撤销数字证书
37

图 3