(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 107085870 B
(45)授权公告日 2020.08.18

(21)申请号 201710066236.9

(22)申请日 2017.02.06

(65)同一申请的已公布的文献号
申请公布号 CN 107085870 A

(43)申请公布日 2017.08.22

(30)优先权数据
15/044990 2016.02.16 US

(73)专利权人 通用汽车环球科技运作有限责任公司
地址 美国密歇根州

(72)发明人 K·B·勒伯夫 R·菲利普斯三世 E·A·卢西特三世

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 安文森

(51)Int.Cl.
G07C 9/00(2020.01)
H04L 29/06(2006.01)

(56)对比文件
US 2006131412 A1,2006.06.22
CN 103139769 A,2013.06.05
CN 104163158 B,2016.01.20
US 2005060555 A1,2005.03.17

审查员 蔡伊青

权利要求书3页 说明书10页 附图2页

(54)发明名称

使用加密方法调节车辆访问

(57)摘要

一种调节从使用短程无线通信进行通信的无线装置对车辆的访问的系统和方法,该方法包括:将车辆访问证书签名请求从无线装置传输至中央设备;响应于该车辆访问证书签名请求从中央设备接收经认证车辆访问证书,其中该经认证车辆访问证书是使用中央设备私钥进行签名并且包括无线装置公钥;经由短程无线通信协议将包括无线装置公钥的经认证车辆访问证书从无线装置传输至车辆;从车辆接收由无线装置公钥加密的共享密钥;使用无线装置私钥解密接收到的共享密钥;生成控制车辆功能的命令;以及将该命令从无线装置传输至车辆。

CN 107085870 B

1.一种调节从使用短程无线通信进行通信的无线装置对车辆的访问的方法,包括以下步骤:

(a)将车辆访问证书签名请求从所述无线装置传输至中央设备,其中所述车辆访问证书签名请求包括无线装置公钥和车辆标识符,并且所述中央设备被配置成使用所述车辆标识符验证所述无线装置是否被认证以控制所述车辆的一个或多个操作;

(b)响应于所述车辆访问证书签名请求并且响应于通过所述中央设备验证所述无线装置已被认证以控制所述车辆的一个或多个操作,从所述中央设备接收经认证车辆访问证书,其中所述经认证车辆访问证书是使用中央设备私钥进行签名并且包括所述无线装置公钥;

(c)经由短程无线通信协议将包括所述无线装置公钥的所述经认证车辆访问证书从所述无线装置传输至所述车辆;

(d)从所述车辆接收由所述无线装置公钥加密的共享密钥;

(e)使用无线装置私钥解密所述接收到的共享密钥;

(f)生成使用所述共享密钥认证的控制一个或多个车辆功能的命令;以及

(g)将所述命令从所述无线装置传输至所述车辆。

2.根据权利要求1所述的方法,其中通过以下项认证控制一个或多个车辆功能的所述命令:

在所述无线装置处接收包括从所述车辆生成和发送的随机数的车辆询问消息;

生成车辆响应消息,其包括所述随机数的加密散列、所述共享密钥和所述命令;以及

经由所述短程无线协议将所述车辆响应消息从所述无线装置传输至所述车辆。

3.根据权利要求1所述的方法,进一步包括将经解密共享密钥连同车辆标识符一起存储在所述无线装置处的步骤。

4.根据权利要求1所述的方法,其中所述车辆访问证书签名请求包括用于控制车辆功能的一个或多个授权。

5.根据权利要求1所述的方法,其中接收自所述中央设备的所述经认证车辆访问证书包括用于控制已经添加或由所述中央设备改变的车辆功能的授权。

6.根据权利要求1所述的方法,进一步包括在所述无线装置处生成所述无线装置私钥和所述无线装置公钥的步骤。

7.一种调节从使用短程无线通信进行通信的无线装置对车辆的访问的方法,包括以下步骤:

(a)在所述车辆处接收经由短程无线通信从所述无线装置发送的经认证车辆访问证书,其中所述车辆访问证书已由中央设备认证;

(b)在所述车辆处使用中央设备公钥确认所述经认证车辆访问证书;

(c)当所述经认证车辆访问证书有效时在所述车辆处生成共享密钥;

(d)在所述车辆处使用无线装置公钥加密所述共享密钥;

(e)经由所述短程无线通信协议将经加密共享密钥从所述车辆传输至所述无线装置;

(f)在所述车辆处接收从所述无线装置发送的控制一个或多个功能的命令;

(g)使用所述共享密钥认证所述命令;以及

(h)控制所述一个或多个车辆功能,

其中，响应于从所述无线装置传输至所述中央设备的车辆访问证书签名请求并且响应于通过所述中央设备验证所述无线装置已被认证以控制所述车辆的一个或多个操作，所述无线装置从所述中央设备接收经认证车辆访问证书，其中，所述车辆访问证书签名请求包括车辆标识符。

8.根据权利要求7所述的方法，其中通过以下项认证控制一个或多个车辆功能的所述命令：

在所述车辆处生成随机数；

将包括所述随机数的车辆询问消息传输至所述无线装置；

从所述无线装置接收车辆响应消息，其包括所述随机数的加密散列、所述共享密钥和所述命令；

基于所述随机数的所述加密散列、所述共享密钥和所述命令计算验证输出；

将所述车辆响应消息与所述验证输出进行比较；以及

当所述车辆响应消息匹配所述验证输出时控制所述一个或多个车辆功能。

9.根据权利要求8所述的方法，进一步包括将所述随机数连同车辆标识符一起存储在所述车辆处的步骤。

10.根据权利要求7所述的方法，其中由中央设备使用所述中央设备私钥对所述经认证车辆访问证书进行签名。

11.根据权利要求7所述的方法，其中所述经认证车辆访问证书包括车辆标识符。

12.根据权利要求7所述的方法，其中所述经认证车辆访问证书包括用于控制车辆功能的一个或多个授权。

13.根据权利要求7所述的方法，其中接收自所述无线装置的所述经认证车辆访问证书包括用于控制已经添加或由所述中央设备改变的车辆功能的授权。

14.一种调节从使用短程无线通信进行通信的无线装置对车辆的访问的方法，其包括以下步骤：

(a)将车辆访问证书签名请求从无线装置传输至中央设备，其中所述车辆访问证书签名请求包括访问车辆的请求、无线装置公钥和车辆标识符，并且所述中央设备被配置成使用所述车辆标识符验证所述无线装置是否被认证以控制所述车辆的一个或多个操作；

(b)添加控制对所述车辆的访问的一个或多个授权字段至所述车辆访问证书签名请求；

(c)通过使用中央设备私钥在中央设备处对所述车辆访问证书签名请求的至少一部分进行签名来创建经认证车辆访问证书，其中所述经认证车辆访问证书包括所述无线装置公钥和所述一个或多个授权字段；

(d)经由无线载波系统将所述经认证车辆访问证书从所述中央设备传输至所述无线装置；

(e)经由短程无线通信协议将所述经认证车辆访问证书和无线装置公钥从所述无线装置传输至所述车辆；

(f)在所述车辆处使用中央设备公钥确认所述经认证车辆访问证书；

(g)当所述经认证车辆访问证书有效时在所述车辆处生成共享密钥；

(h)使用所述无线装置公钥加密所述共享密钥；

(i)经由所述短程无线通信协议将经加密共享密钥从所述车辆传输至所述无线装置；

(j)在所述无线装置处使用无线装置私钥解密所述接收到的共享密钥；

(k)生成使用所述共享密钥认证的控制一个或多个车辆功能的命令；以及

(l)将所述命令从所述无线装置传输至所述车辆。

使用加密方法调节车辆访问

技术领域

[0001] 本发明涉及调节车辆访问，并且更具体地涉及经由加密保护车辆访问证书签名请求调节这样的访问。

背景技术

[0002] 车辆访问传统上是由一个或多个物理钥匙控制。当车主或用户持有物理钥匙时，用户可将钥匙插入至锁中并将车门解锁，或插入至点火装置中并启动车辆发动机。随着车辆技术的发展，车钥匙保持为物理的但是被实施为与车辆无线通信以提供访问的无源装置。无源装置包括车主/用户携带以取得对车辆和其功能性的访问的无线传输机。调节车辆访问的这些机构涉及用于操作车辆的专用钥匙或装置的物理持有。虽然物理钥匙/装置是可靠且有效的，但是将它们传递至需要访问车辆的人可能并不方便。经由可无线地接收虚拟钥匙并且使用那些虚拟钥匙来控制车辆访问的无线装置调节车辆访问提高了用户取得对车辆的访问的灵活性。

发明内容

[0003] 根据本发明的实施例，提供了一种调节从使用短程无线通信进行通信的无线装置对车辆的访问的方法。该方法包括将车辆访问证书签名请求从无线装置传输至中央设备，其中该车辆访问证书签名请求包括无线装置公钥；响应于该车辆访问证书签名请求从中央设备接收经认证车辆访问证书，其中该经认证车辆访问证书是使用中央设备私钥进行签名并且包括无线装置公钥；经由短程无线通信协议将包括无线装置公钥的经认证车辆访问证书从无线装置传输至车辆；从车辆接收由无线装置公钥加密的共享密钥；使用无线装置私钥解密接收到的共享密钥；生成使用共享密钥认证的控制一个或多个车辆功能的命令；以及将该命令从无线装置传输至车辆远程信息处理单元。

[0004] 根据本发明的另一个实施例，提供了一种调节从使用短程无线通信进行通信的无线装置对车辆的访问的方法。该方法包括在车辆处接收经由短程无线通信从无线装置发送的经认证车辆访问证书，其中该车辆访问证书已由中央设备认证；在车辆处使用中央设备公钥确认经认证车辆访问证书；当经认证车辆访问证书有效时在车辆处生成共享密钥；在车辆处使用无线装置公钥加密共享密钥；经由短程无线通信将经加密共享密钥从车辆传输至无线装置；在车辆处接收从无线装置发送的控制一个或多个功能的命令；使用共享密钥认证该命令；以及控制一个或多个车辆功能。

[0005] 根据本发明的另一个实施例，提供了一种调节从使用短程无线通信进行通信的无线装置对车辆的访问的方法。该方法包括将车辆访问证书签名请求从无线装置传输至中央设备，其中该车辆访问证书签名请求包括访问车辆的请求以及无线装置公钥；添加控制对车辆的访问的一个或多个授权字段至车辆访问证书签名请求；通过使用中央设备私钥在中央设备处对车辆访问证书签名请求的至少一部分进行签名来创建经认证车辆访问证书，其中该经认证车辆访问证书包括无线装置公钥和一个或多个授权字段；经由无线载波系统将

经认证车辆访问证书从中央设备传输至无线装置;经由短程无线通信协议将经认证车辆访问证书和无线装置公钥从无线装置传输至车辆;在车辆处使用中央设备公钥确认经认证车辆访问证书;当经认证车辆访问证书有效时在车辆处生成共享密钥;使用无线装置公钥加密共享密钥;经由短程无线通信协议将经加密共享密钥从车辆传输至无线装置;在无线装置处使用无线装置私钥解密接收到的共享密钥;生成使用共享密钥认证的控制一个或多个车辆功能的命令;以及将该命令从无线装置传输至车辆。

附图说明

[0006] 下文将结合附图描述本发明的一个或多个实施例,其中相同的标号标示相同的元件,且其中:

[0007] 图1是描绘能够利用本文所公开的方法的通信系统的实施例的框图;

[0008] 图2是描绘调节从使用短程无线通信进行通信的无线装置对车辆的访问的方法的实施例的通信流;以及

[0009] 图3是描绘实施询问/响应认证的方法的实施例的通信流。

具体实施方式

[0010] 下文描述的系统和方法使得无线装置能够从中央设备请求车辆访问,并且继而接收无线装置可以使用来访问车辆的经认证车辆访问证书以及无线装置的公钥/私钥。例如,用户可通过创建无线装置向中央设备发送的车辆访问证书签名请求来引导无线装置请求车辆访问。无线装置可以生成其自身的一组加密密钥;无线装置私钥和无线装置公钥。车辆访问证书签名请求包括无线装置公钥,其在由中央设备经由使用中央设备私钥创建的数字签名认证时可限于无线装置的标识,由此创建经认证车辆访问证书。无线装置可以向中央设备发送车辆标识符以及车辆访问证书签名请求。中央设备可从无线装置接收车辆访问证书签名请求,并且基于无线装置或用户的标识以及车辆标识符来确定无线装置是否能访问车辆。如果访问被授权,那么中央设备可将一个或多个权限编码至车辆访问证书中。在中央设备已将权限编码至车辆访问证书中之后,中央设备使用其私钥来对车辆访问证书签名请求进行签名,由此认证该车辆访问证书签名请求。中央设备接着可将经认证车辆访问证书无线地传输至无线装置,该无线装置接着将此证书传送至车辆以取得访问。

[0011] 该车辆包括在接收到经认证车辆访问证书之前便已经存储在这里的中央设备公钥的副本。在经由短程无线通信从无线装置接收到经认证车辆访问证书和无线装置公钥之后,该车辆可通过使用中央设备公钥的副本验证以中央设备私钥加密的经认证车辆访问证书来认证经认证车辆访问证书和无线装置公钥。经认证车辆访问证书的成功验证指示包括在经认证车辆访问证书中的无线装置公钥和权限是有效的。鉴于该车辆可使用先前存储的中央设备公钥来验证经认证车辆访问证书,该车辆可在无需与中央设备通信的情况下授权或拒绝车辆访问。

[0012] 该车辆接着可生成将存储在车辆处并且传输至无线装置的共享密钥。共享密钥可用作由无线装置发出以控制车辆功能的命令的对称加密的部分、用于询问/响应机制的消息认证代码的生成,或这二者。该车辆可生成诸如随机生成数的共享密钥,并且使用无线装置公钥加密共享密钥。在加密之后,共享密钥可经由短程无线通信无线地传输至无线装置。

无线装置可使用其私钥解密共享密钥并且将该密钥存储在其存储器装置中。

[0013] 当无线装置生成控制车辆功能的命令时，该车辆可使用共享密钥验证那些命令。一种用于验证这些命令的机制涉及使用共享密钥的询问/响应机制。这将在下文加以更详细讨论。使用经认证车辆访问证书促使其中在中央设备处授权对车辆的访问的系统不依赖于物理钥匙链且受类似于现有无钥匙进入无钥匙启动(PEPS)钥匙链的响应性控制。更具体地，本文所述的系统和方法提供了一种无线装置，其在接收到共享密钥之后可在起始命令的200毫秒(ms)内将车门解锁或锁定或在400ms内启动车辆的推进系统。除该系统响应性之外，该系统和方法也不依赖于由通过该无线通信路径发送通信的无线通信路径(诸如短程无线通信或无线载波系统)固有地提供的任何安全机制。

[0014] 参考图1，示出了一种操作环境，其包括移动车辆通信系统10并且可用于实施本文所公开的方法。通信系统10通常包括车辆12、一个或多个无线载波系统14、陆地通信系统16、计算机18和呼叫中心20。应当理解的是，所公开方法可结合任何数量的不同系统使用并且具体不限于此处所示的操作环境。另外，系统10的架构、构造、设置和操作以及其个别部件在本领域中通常是公知的。因此，以下段落简单地提供对一种这样的通信系统10的简要概述。然而，此处未示出的其它系统也可采用所公开方法。

[0015] 车辆12在所说明实施例中被描绘为客车，但是应当明白的是，也可使用包括摩托车、卡车、运动型多功能车(SUV)、旅游车(RV)、船舰、飞机等的任何其它装置。某些车辆电子器件28在图1中进行了总体示出，并且包括远程信息处理单元30、麦克风32、一个或多个按钮或其它控制输入34、音频系统36、可视显示器38和GPS模块40以及许多车辆系统模块(VSM)42。这些装置中的某些装置可直接连接至远程信息处理单元，诸如(例如)麦克风32和按钮34，而其它装置则使用诸如通信总线44或娱乐总线46的一个或多个网络连接间接地连接。合适的网络连接的实例包括控制器区域网络(CAN)、媒体导向系统转移(MOST)、本地互连网络(LIN)、局域网(LAN)和其它适当的连接，诸如以太网或符合已知ISO、SAE和IEEE标准和规范的其它连接等等。

[0016] 远程信息处理单元30可为安装有(嵌入有)OEM或配件市场装置，其安装在车辆中并且使得能够通过无线载波系统14且经由无线联网进行无线语音和/或数据通信。这使得车辆能够与呼叫中心20、其它启用远程信息处理的车辆或某种其它实体或装置进行通信。远程信息处理单元优选地使用无线电传输来与无线载波系统14建立通信信道(语音信道和/或数据信道)使得可通过该信道发送和接收语音和/或数据传输。通过提供语音和数据通信这二者，远程信息处理单元30使得车辆能够提供包括与导航、电话、紧急救援、诊断、信息娱乐等有关的服务的许多不同服务。数据可经由数据连接(诸如经由通过数据信道进行的分组数据传输或经由语音信道)使用本领域中已知的技术而发送。对于涉及语音通信(例如，利用呼叫中心20处的现场顾问或语音响应单元)和数据通信(例如，向呼叫中心20提供GPS位置数据或车辆诊断数据)这二者的组合服务，该系统可利用通过语音信道进行的单次呼叫并且必要时通过语音信道在语音传输与数据传输之间切换，且这可使用本领域技术人员所已知的技术来进行。

[0017] 根据一个实施例，远程信息处理单元30利用根据GSM、CDMA或LET标准的蜂窝通信并且因此包括用于语音通信(如免提呼叫)的标准蜂窝芯片集50、用于数据传输的无线调制解调器、电子处理装置52、一个或多个数字存储器装置54以及双天线56。应当明白的是，调

制解调器可通过存储在远程信息处理单元中并且由处理器52执行的软件来实施，或其可为位于远程信息处理单元30内部或外部的单独硬件部件。调制解调器可使用诸如LTE、EVDO、CDMA、GPRS和EDGE的任何数量的不同标准或协议来操作。还可使用远程信息处理单元30实行车辆与其它联网装置之间的无线联网。为此目的，远程信息处理单元30可配置成根据一个或多个无线协议(包括短程无线通信(SRWC)，诸如IEEE802.11协议、WiMAX、ZigBee™、Wi-Fi直连、蓝牙、低功耗蓝牙(BLT)或近场通信(NFC)中的任一种)进行无线通信。当用于诸如TCP/IP的分组交换数据通信时，远程信息处理单元可配置有静态IP地址或可设置成从网络上的另一个装置(诸如路由器)或从网络地址服务器接收所分配的IP地址。

[0018] 车辆12的其它实施例是可行的，其中车辆仅配备有短程无线通信能力。除具有可使用蜂窝通信协议使用蜂窝芯片集以及短程无线通信进行通信的车辆远程信息处理单元的车辆之外，所公开方法还可使用缺少蜂窝芯片集并且可仅经由短程无线通信协议进行通信的车辆远程信息处理单元来实施。或在另一个实施方案中，车辆可能未配备有车辆远程信息处理单元，但是尽管如此，该车辆还是拥有经由一种或多种短程无线通信协议或技术进行无线通信的能力。这样的设置可在经由短程无线通信使用VSM42或车辆12上的其它ECU进行通信的车辆中实施。VSM42可单独专用于短程无线通信(诸如包括其自身的短程无线天线的BLE VSM)并且经由通信总线44或娱乐总线46通信地链接至车辆电子器件28的其它部分。在其它实施方案中，音频系统34的信息娱乐主机单元(IHU)可包括专用天线并且具有经由短程无线通信协议进行无线通信并实行所公开方法的步骤的能力。下文关于该方法描述的车辆远程信息处理单元的功能性(诸如随机数发生器)可完全使用VSM42或IHU来实施。

[0019] 可与远程信息处理单元30通信的一个联网装置是无线装置，诸如智能手机57。智能手机57可包括计算机处理能力、能够使用短程无线协议进行通信的收发器，和可视智能手机显示器59。在某些实施方案中，智能手机显示器59还包括触摸屏图形用户界面和/或能够接收GPS卫星信号并且基于那些信号生成GPS座标的GPS模块。智能手机57的实例包括由苹果公司(Apple)制造的iPhone™和三星(Samsung)制造的Galaxy™以及其它手机。虽然智能手机57可以包括经由蜂窝通信使用无线载波系统14进行通信的能力，但是情况并非总是如此。例如，苹果公司(Apple)制造诸如iPad™和iPodTouch™的各种型号的装置，其包括处理能力、显示器59和通过短程无线通信链路进行通信的能力。然而，iPod Touch™和某些iPads™并不具有蜂窝通信能力。即使如此，这些和其它类似装置也可以用作或视为用于本文所述的方法的目的的一种无线装置，诸如智能手机57。

[0020] 处理器52可为能够处理电子指令的任何类型的装置，包括微处理器、微控制器、主机处理器、控制器、车辆通信处理器以及专用集成电路(ASIC)。其可为仅用于远程信息处理单元30的专用处理器或可为其它车辆系统所共享。处理器52执行各种类型的数字存储指令，诸如存储在存储器54中的软件或固件程序，其使得远程信息处理单元能够提供多种服务。例如，处理器52可执行程序或程序数据以实行本文所讨论的方法的至少一部分。

[0021] 远程信息处理单元30可用于提供涉及至车辆和/或来自车辆的无线通信的各种各样的车辆服务。这样的服务包括：分段导航和结合基于GPS的车辆导航模块40提供的其它导航相关服务；安全气囊展开通知和结合一个或多个碰撞传感器接口模块(诸如车体控制模块(未示出))提供的其它紧急或道路救援相关服务；使用一个或多个诊断模块的诊断报告；以及信息娱乐相关服务，其中音乐、网页、电影、电视节目、视频游戏和/或其它内容是由信

息娱乐模块(未示出)下载并且存储以供当前或后续回放。上文列举的服务决不是远程信息处理单元30的全部能力的详尽列表,而仅仅是远程信息处理单元能够提供的某些服务的枚举。另外,应当理解的是,至少某些前述提及的模块可以保存在远程信息处理单元30内部或外部的软件指令的形式来实施,它们可为位于远程信息处理单元30内部或外部的硬件部件,或它们可与彼此或与位于整个车辆中的其它系统集成和/或共享,这里仅列举几种可能性。如果模块被实施为位于远程信息处理单元30外部的VSM42,那么它们可利用车辆总线44来与远程信息处理单元交换数据和命令。

[0022] GPS模块40从GPS卫星群60接收无线电信号。从这些信号中,模块40可确定用于向车辆驾驶员提供导航和其它位置相关服务的车辆位置。导航信息可展现在显示器38(或车辆内的其它显示器)上或可以口头形式展现,诸如当供应分段导航时进行该口头展现。可使用专用车辆中导航模块(可为GPS模块40的部分)提供导航服务,或可经由远程信息处理单元30进行某些或全部导航服务,其中将位置信息发送至远程位置用于给车辆提供导航地图、地图注记(兴趣点、餐馆等)、路线计算等目的。可将位置信息供应至呼叫中心20或其它远程计算系统(诸如计算机18)用于其它目的(诸如车队管理)。另外,可经由远程信息处理单元30将新的或更新的地图数据从呼叫中心20下载至GPS模块40。

[0023] 除音频系统36和GPS模块40之外,车辆12可包括呈电子硬件部件的形式的其它车辆系统模块(VSM)42,该电子硬件部件位于整个车辆中并且通常从一个或多个传感器接收输入并使用所感测的输入来执行诊断、监测、控制、报告和/或其它功能。每个VSM42均优选地由通信总线44连接至其它VSM以及远程信息处理单元30,并且可编程为运行车辆系统和子系统诊断测试。作为实例,一个VSM42可为控制诸如燃料点火和点火正时的发动机操作的各个方面的发动机控制模块(ECM),另一个VSM42可为调节车辆动力系的一个或多个部件的操作的动力系控制模块,且另一个VSM42可为支配位于整个车辆中的各种电气部件(如车辆的电动门锁和前灯)的车体控制模块。根据一个实施例,发动机控制模块配备有车载诊断(OBD)特征,其提供诸如接收自包括车辆排放传感器的各种传感器的多种实时数据并且提供允许技术人员快速地识别并修复车辆内的故障的标准化一系列的诊断故障代码(DTC)。如本领域技术人员所明白的是,上述提及的VSM仅仅是可以在车辆12中使用的某些模块的实例,因为许多其它模块也是可能的。

[0024] 车辆电子器件28还包括给车辆乘客提供一种提供和/或接收信息的装置(包括麦克风32、按钮34、音频系统36和可视显示器38)的许多车辆用户接口。如本文所使用,术语‘车辆用户接口’大体上包括位于车辆上并且使得车辆用户能够与车辆的部件通信或通过车辆的部件进行通信的任何合适形式的电子装置,包括硬件和软件部件这二者。麦克风32向远程信息处理单元提供音频输入以使得驾驶员或其它乘客能够经由无线载波系统14提供语音命令并且实行免提呼叫。为此目的,其可利用本领域中已知的人机接口(HMI)技术连接至车载自动语音处理单元。按钮34允许手动用户输入至远程信息处理单元30中以起始无线电话呼叫并且提供其它数据、响应或控制输入。单独按钮可用于向呼叫中心20起始紧急呼叫或常规服务救援呼叫。音频系统36向车辆乘客提供音频输出并且可为专用、独立系统或主要车辆音频系统的部分。根据此处所示的特定实施例,音频系统36操作地耦合至车辆总线44和娱乐总线46这二者并且可提供AM、FM和卫星无线电广播、CD、DVD以及其它多媒体功能性。此功能性可结合或独立于上述信息娱乐模块提供。可视显示器38优选地是图形显

示器，诸如仪表板上的触摸屏或从挡风玻璃反射的平视显示器，并且可用于提供大量输入和输出功能。还可利用各种其它车辆用户接口，因为图1的接口仅仅是一个特定实施方案的实例。

[0025] 无线载波系统14优选地包括蜂窝电话系统，其包括多个小区发射塔70(仅示出一个)、一个或多个移动交换中心(MSC)72以及连接无线载波系统14与陆地网络16所需要的任何其它联网部件。每个小区发射塔70均包括发送和接收天线以及基站，其中来自不同小区发射塔的基站直接或经由诸如基站控制器的中间设备连接至MSC72。无线载波系统14可实施任何合适的通信技术，包括(例如)诸如AMPS的模拟技术或诸如CDMA(例如，CDMA2000)或GSM/GPRS的较新数字技术。如本领域技术人员将明白的是，各种小区发射塔/基站/MSC设置是可能的并且可结合无线载波系统14使用。例如，基站和小区发射塔可共同位于相同站点处或它们可远离彼此，每个基站可负责单个小区发射塔或单个基站可服务于各个小区发射塔，且各个基站可耦合至单个MSC，这里仅列举几种可能设置。

[0026] 除使用无线载波系统14外，可使用呈卫星通信的形式的不同无线载波系统来提供与车辆的单向或双向通信。这可使用一个或多个通信卫星62和上行链路传输站64来进行。单向通信可为(例如)卫星无线电广播服务，其中节目内容(新闻、音乐等)是由传输站64提供、封装上传并且然后发送至卫星62，从而向用户广播该节目。双向通信可为(例如)使用卫星62以在车辆12与站64之间中继电话通信的卫星电话服务。如果使用了，那么除了或代替无线载波系统14，可利用此卫星电话。

[0027] 陆地网络16可以是连接至一个或多个路线电话并且将无线载波系统14连接至呼叫中心20的常规路基电信网络。例如，陆地网络16可以包括诸如用于提供硬接线电话、分组交换数据通信和互联网基础设施的公共交换电话网(PSTN)。一段或多段陆地网络16可通过使用标准有线网络、光纤或其它光学网络、电缆网络、电力线、其它无线网络(诸如无线局域网(WLAN))或提供宽带无线访问(BWA)的网络或其任何组合来实施。另外，呼叫中心20不需要经由陆地网络16连接，反而可包括无线电话设备使得其可直接与无线网络(诸如无线载波系统14)通信。

[0028] 计算机18可为可经由诸如互联网的专用或公共网络访问的许多计算机。每个这样的计算机18均可用于一个或多个目的，诸如可由车辆经由远程信息处理单元30以及无线载波系统14访问网络服务器。其它这样的可访问计算机18可为例如：服务中心计算机，其中可经由远程信息处理单元30从车辆上传诊断信息和其它车辆数据；客户端计算机，其由车辆所有者或其它用户使用以用于访问或接收车辆数据或设定或配置用户偏好或控制车辆功能的这样的目的；或第三方数据仓库，将车辆数据或其它信息提供至该第三方数据仓库或从该第三方数据仓库提供车辆数据或其它信息，而无关于是否通过与车辆12或呼叫中心20或这二者通信。计算机18还可用于提供诸如DNS服务器或网络地址服务器的互联网连接性，该网络地址服务器使用DHCP或其它合适协议来将IP地址分配至车辆12。

[0029] 呼叫中心20设计成给车辆电子器件28提供许多不同的系统后端功能，并且根据此处所示的示例性实施例，呼叫中心通常包括全部在本领域中已知的一个或多个交换机80、服务器82、数据库84、现场顾问86以及自动语音响应系统(VRS)88。这样的各种呼叫中心部件优选地经由有线或无线局域网90耦合至彼此。交换机80(可为专用分支交换(PBX)交换机)路由传入信号使得语音传输通常由常规电话发送至现场顾问86或使用VoIP发送至自动

语音响应系统88。现场顾问电话还可如图1中的虚线所指示般使用VoIP。经由连接在交换机80与网络90之间的调制解调器(未示出)实施通过交换机80进行的VoIP和其它数据通信。经由调制解调器将数据传输传递至服务器82和/或数据库84。数据库84可存储账号信息(诸如用户认证信息、车辆标识符、设定档记录、行为方式以及其它相关用户信息)。还可以由诸如802.11x、GPRS等无线系统进行数据传输。虽然所说明的实施例已经被描述为其结合人工操纵呼叫中心20使用现场顾问86而使用,但是将明白的是,呼叫中心反而可利用VRS作88为自动顾问或可使用VRS88与现场顾问86的组合。

[0030] 现在转向图2,示出了调节从使用短程无线通信进行通信的智能手机57访问处理12的方法200的实施例。方法200开始于步骤205,将车辆访问证书签名请求从智能手机57传输至中央设备,诸如由计算机18或呼叫中心20实施的后台。为了说明目的,中央设备在此实施例中将就计算机18进行描述。然而,应当明白的是,呼叫中心20或其它中央设备也可取得相同效果。另外,可使用车辆远程信息处理单元30的处理器52、一个或多个VSM42的计算机处理能力(诸如车体控制模块)或这二者来实施此方法200的部分。

[0031] 当智能手机57起始取得对车辆12的访问或控制车辆12的功能性的程序时,手机57生成由智能手机57使用的一对加密密钥;无线装置私钥和无线装置公钥。智能手机57可在本地创建加密密钥或远程请求计算机18生成密钥对。在其中计算机18接收到对加密密钥的请求的实施方案中,计算机18可经由无线载波系统14使用本领域技术人员所理解的非对称加密技术向智能手机57提供无线装置私钥和无线装置公钥。可使用椭圆曲线密码学(ECC)算法(诸如ECCP-256算法)生成无线装置私钥和无线装置公钥。

[0032] 在生成或者获得无线装置私钥和无线装置公钥之后,智能手机57可创建包括对访问车辆12的请求的车辆访问证书签名请求。可以证书签名请求(CSR)从计算机18请求车辆访问证书,该证书签名请求包括使车辆12被访问的无线装置公钥和车辆标识符、识别将授权访问57的级别的授权或权限字段,或这二者。智能手机57可接着使用签名算法或方案以及无线装置私钥来对车辆访问证书进行签名以在从智能手机57发送时向计算机18认证该证书。签名算法和签名验证算法可采用散列函数作为签名/验证程序的部分。该方法可使用各种不同的签名算法和签名验证算法,包括数字签名算法(DSA)、椭圆曲线数字签名算法(ECDSA)、RSASSA-PSS(附带概率签名方案的RSA签名方案)和RSASSA-PKCS1-v1_5(附带公钥密码学标准1,版本1.5的RSA签名方案)。

[0033] 授权字段可由智能手机57或由计算机18在其从手机57接收到证书之后插入至车辆访问证书。授权字段可识别允许智能手机57控制的车辆功能,和期间智能手机57可访问车辆12的时间和日期范围,或这二者。车辆功能可以包括解锁/锁定车辆12中的某些车门或车厢、启动/停止车辆推进系统、控制音频系统34或从通信总线44访问GPS位置数据的能力,这里仅列出几个实例。

[0034] 在某些实施方案中,智能手机57可从用户访问指示用户将希望访问的车辆功能的输入。智能手机57可接着包括具有车辆访问证书签名请求连通车辆标识符和无线装置公钥的那些车辆功能。智能手机57可接着对包括车辆标识符、无线公钥和具有无线装置私钥的请求车辆功能的证书进行签名。当计算机18接收车辆访问证书签名请求时,计算机18可识别智能手机57希望使用车辆标识符在数据库中要访问的车辆12。计算机18可维护其中车辆由车辆标识符(诸如VIN)识别且一个或多个权限与车辆标识符相关联的数据库。这些权限

包括允许控制车辆12的智能手机的标识符、可对允许访问车辆的每个智能手机控制的车辆功能的标识符，和期间智能手机57访问每个车辆功能的时间/日期。

[0035] 当计算机18接收车辆访问证书时，计算机18可使用车辆标识符识别数据库中的车辆12、基于与车辆标识符和智能手机57相关联的权限确定智能手机57是否允许访问车辆12，且识别智能手机57可访问包括在证书中的哪些车辆功能。如果智能手机57可访问车辆访问证书中识别的所有车辆功能，那么计算机18可以原来的方式认证该证书。然而，如果不允许智能手机57访问车辆访问证书中请求的一个或多个车辆功能，那么计算机18可修改证书以删除智能手机57不允许访问的车辆功能。除车辆功能之外，计算机18可确定期间智能手机57可访问车辆12的时间和日期。如果车辆访问证书包括时间/日期，那么计算机18可将其与数据库中的车辆标识符中所包括的允许时间进行比较。如果允许请求时间，那么计算机18可使车辆访问证书保持不被修改。且如果期间智能手机57可访问车辆12的时间窗是无效的，那么计算机18可改变车辆访问证书中的时间值。

[0036] 然而，在其它实施方案中，计算机18可在无任何识别的车辆功能的情况下从智能手机57接收车辆访问证书。在那种情况下，计算机18可从车辆访问证书中提取车辆标识符，确定智能手机57访问的车辆功能，且接着将那些车辆功能插入至车辆访问证书中。车辆访问证书还可以包括智能手机57创建证书的时间和日期以及由智能手机57使用的任何扩展，诸如蓝牙媒体访问控制(MAC)地址或国际移动设备标识符(IMEI)。方法200前进至步骤210。

[0037] 在步骤210处，在计算机18处使用中央设备私钥对车辆访问证书进行签名。计算机18包括表示属于中央设备的加密密钥对的根证书；中央设备公钥和中央设备私钥。在确定智能手机57被授权的权限之后，计算机18可编码期间证书有效的时间窗且接着使用签名验证算法和中央设备私钥来认证车辆访问证书签名请求。当接收到经认证车辆访问证书时，可使用中央设备公钥验证其内容。方法200前进至步骤215。

[0038] 在步骤215处，经由无线载波系统14将经认证车辆访问证书从计算机18传输至智能手机57。计算机18可经由小区发射塔70使用许多可能蜂窝协议中的一种将经认证访问证书无线地发送至智能手机57。当智能手机57与Wi-Fi热点或连接至因特网的其它类似WLAN通信地链接时，还可经由因特网将经认证车辆访问证书从计算机18无线地传输至手机57。方法200前进至步骤220。

[0039] 在步骤220处，经由短程无线通信协议将经认证车辆访问证书和无线装置公钥从智能手机57传输至车辆12。智能手机57可通过向车辆12呈现经认证车辆访问证书而与车辆12配对。智能手机57可使用许多短程无线通信协议与车辆12的车辆远程信息处理单元30建立短程无线通信链路。例如，使用低功耗蓝牙(BLE)，智能手机57可将经认证车辆访问证书无线地传输至车辆12。方法200前进至步骤225。

[0040] 在步骤225处，在车辆12处使用中央设备公钥认证车辆访问证书。在接收到经认证车辆访问证书之前，可将中央设备私钥存储在车辆12处。中央设备公钥可在制造车辆12时存储在车辆处，或这些密钥可经由无线载波系统14从计算机18或呼叫中心20定期地提供至车辆12。当车辆12接收到经认证车辆访问证书时，车辆12可访问存储在车辆12处的中央设备公钥，且使用散列函数和签名验证功能，确定车辆18是否已对证书进行了签名。如果不可信，那么车辆12可以拒绝该证书。然而，当车辆12确定证书可信时，车辆12可生成将加密地学发送至智能手机57的共享密钥。在一个实施方案中，使用创建具有限定深度的随机数的

随机数发生器创建共享密钥。方法200前进至步骤230。

[0041] 在步骤230处，由车辆12使用无线装置公钥加密共享密钥且经由短程无线通信协议将该共享密钥传输至智能手机57。一旦车辆12确定经认证车辆访问证书是有效的，车辆12可使用无线装置公钥和公钥加密算法来加密共享密钥。车辆12可接着将共享密钥传输至智能手机57，而不考虑由用于发送共享密钥的短程无线通信协议使用的安全或加密技术。方法200前进至步骤235。

[0042] 在步骤235处，在智能手机57处使用无线装置私钥解密接收到的共享密钥。在从车辆12接收到共享密钥之后，智能手机57可在发送命令来控制车辆12时将共享密钥存储在其存储器装置中以供后续检索之用。

[0043] 在步骤240处，在智能手机57处生成命令，该命令控制一个或多个车辆功能并且使用短程无线通信技术传输至车辆12。每当智能手机57尝试控制车辆12时，车辆12可使用共享密钥确定命令是否有效。例如，如果智能手机57经由智能手机显示器59从用户接收到启动推进系统的命令，那么智能手机57可将此命令编码为消息中的数据并且将其经由BLE发送至车辆12。该命令是由车辆12的车辆远程信息处理单元30接收，并且由车辆12使用共享密钥基于各种加密技术(诸如其实施例在图3中示出的询问/响应机制)来认证。该认证是由车辆远程信息处理单元30或由一个或多个VSM42实行。当车辆12确定该命令有效时，其可接着控制所识别的车辆功能。

[0044] 转向图3，示出了实时询问/响应认证的方法300的实施例，该方法可用于认证从智能手机57发送至车辆12的命令。在共享密钥存储在车辆12和智能手机57这二者处之后，智能手机57可通过生成由车辆12认证的命令来控制车辆功能。方法300开始于步骤305，在车辆12处生成随机数。车辆12可使用由车辆远程信息处理单元30使用的随机数发生器以生成具有预定大小或长度的随机数。接着可将车辆询问消息从车辆远程信息处理单元30发送至智能手机57。方法300前进至步骤310。

[0045] 在步骤310处，智能手机57从车辆远程信息处理单元30接收到包括在车辆12处生成的随机数的车辆询问消息。方法300前进至步骤315。

[0046] 在步骤315处，在智能手机57处创建车辆响应消息，其包括控制车辆功能的命令的加密散列、在车辆12处生成的随机数，和共享密钥。车辆询问(例如，随机数)、该命令和共享密钥可被并置在一起并且使用许多可能的加密散列函数中的一种进行处理。该命令的明文版本连同车辆响应消息一起包括在内，或其可在车辆响应消息之前且与车辆响应消息分开发送。在某些实施方案中，方法300的加密散列函数可为基于散列的消息认证代码，诸如HMAC-SHA256，而其它实施方案使用基于密码的消息认证码(CMAC)。然而，将理解的是，使用其它类型的加密散列函数也可取得相同效果。接着可以经由短程无线协议将车辆响应消息从智能手机57传输至车辆12。方法300前进至步骤320。

[0047] 在步骤320处，从智能手机57接收车辆响应消息。车辆12可接着验证车辆响应消息的真实性。鉴于车辆12已知共享密钥、其发送的车辆询问以及命令，车辆12可使用加密散列函数来计算验证输出。车辆12可将其车辆输出与车辆响应消息进行比较。当车辆12确定验证输出匹配接收自智能手机57的车辆响应消息时，可授权车辆功能的访问或控制。在此实例中，车辆响应消息还可向车辆指示其中随机数、共享密钥和命令并置的顺序使得车辆可成功地重现散列输出。

[0048] 在某些实施方案中除了执行在车辆12处起始的询问/响应程序之外，还可在智能手机57处起始并且完成询问/响应程序，而非在车辆12处起始询问/响应程序。通过使用两个单独的询问/响应程序，车辆12和智能手机57这二者可认证接收实体。另外，应当理解的是，中央设备可远程撤销经认证车辆访问证书。当中央设备接收到终止经认证车辆访问证书的请求时，中央设备可经由无线载波系统14将指令从中央设备传输至车辆远程信息处理单元30，该指令包括特定无线装置的标识和引导该单元30擦除无线装置公钥和属于所识别的无线装置的包括在经认证车辆访问证书中的任何其它数据的可执行命令。或在另一个实例中，车辆12可添加特定经认证车辆访问证书至车辆12处的存储器装置中维护的黑名单。

[0049] 应当理解的是，前文是本发明的一个或多个实施例的描述。本发明不限于本文所公开的特定实施例，而是由下面的权利要求书来唯一限定。另外，包括在前述描述中的声明涉及特定实施例，并且不能解释为限定本发明的范围或限定权利要求书中所使用的术语，除非术语或措词在上面进行了明确限定。各个其它实施例和对所公开实施例的各种改变以及修改对本领域技术人员而言显而易见。所有这样的其它实施例、改变和修改均旨在属于所附权利要求书的范围。

[0050] 如本说明书和权利要求书中所使用，术语“例如(e.g.)”、“例如(forexample)”、“例如(forinstance)”、“诸如”和“等”以及动词“包括(comprising)”、“具有”、“包括(including)”和它们的其它动词形式在结合一个或多个部件或其它项目的列表使用时，各自被解释为开放式，意指所述列表不应被视为排除其它、另外的部件或项目。其它术语是使用它们的最广泛的合理含义来解释，除非它们用于要求有不同解释的上下文中。

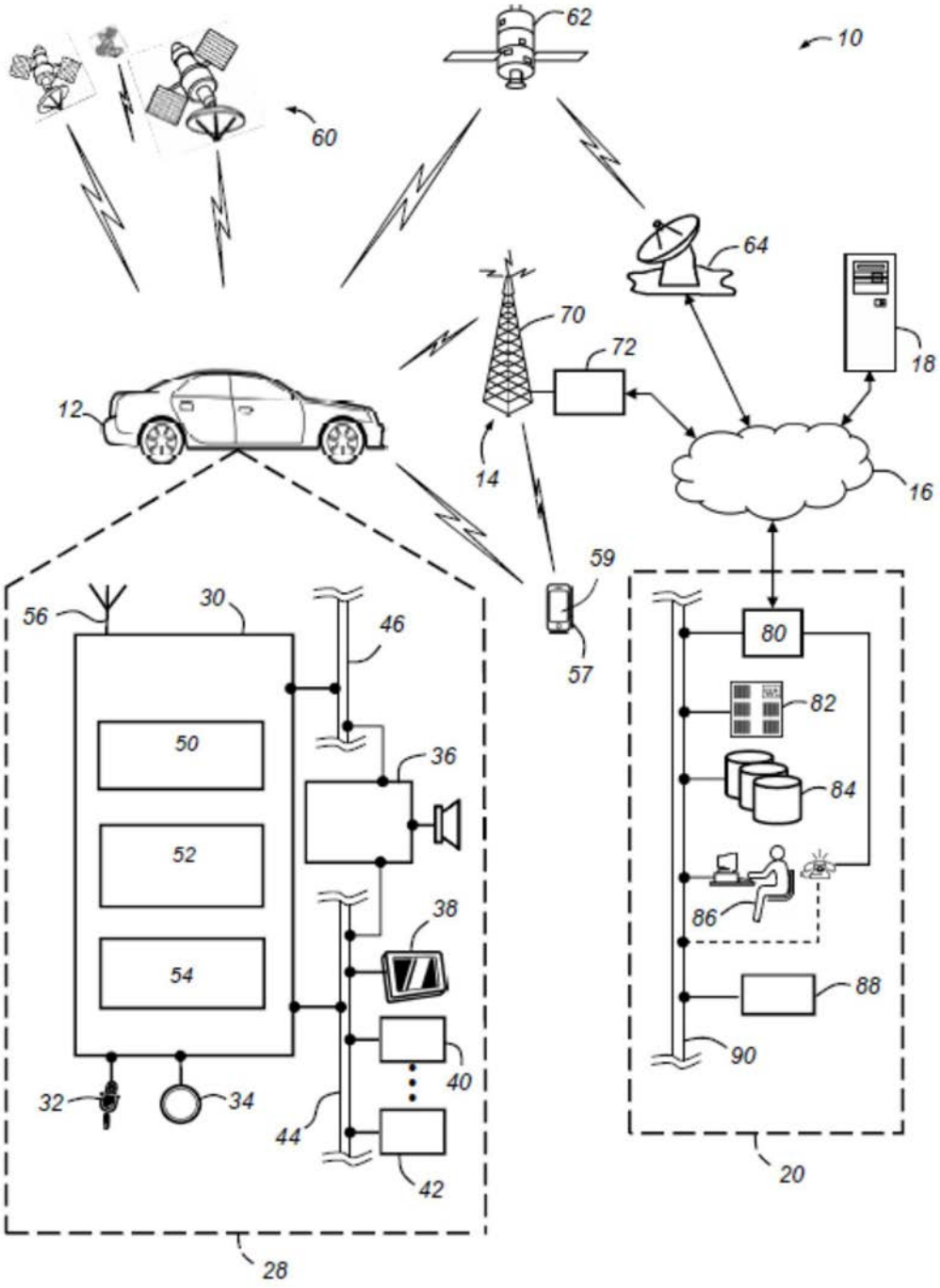
62
10
60
64
70
72
18
12
14
16
59
57
56
30
46
50
36
52
38
54
32
34
44
40
42
28
80
82
84
86
88
90
20

图1

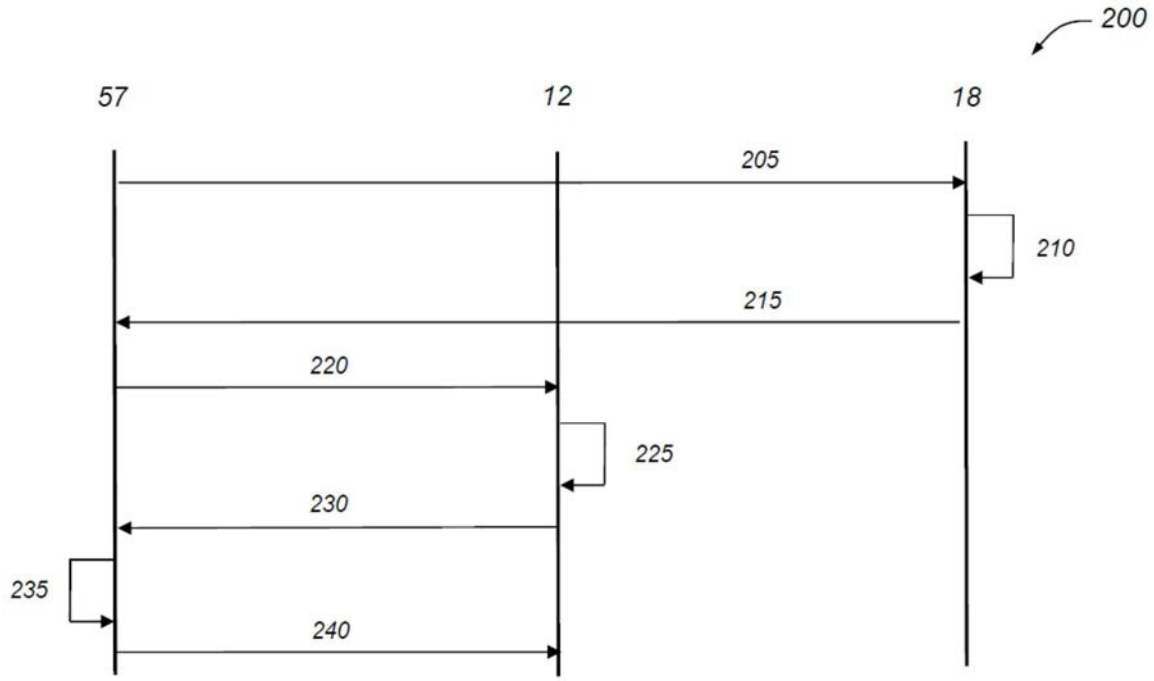
200
57
12
18
205
210
215
220
225
230
235
240

图2

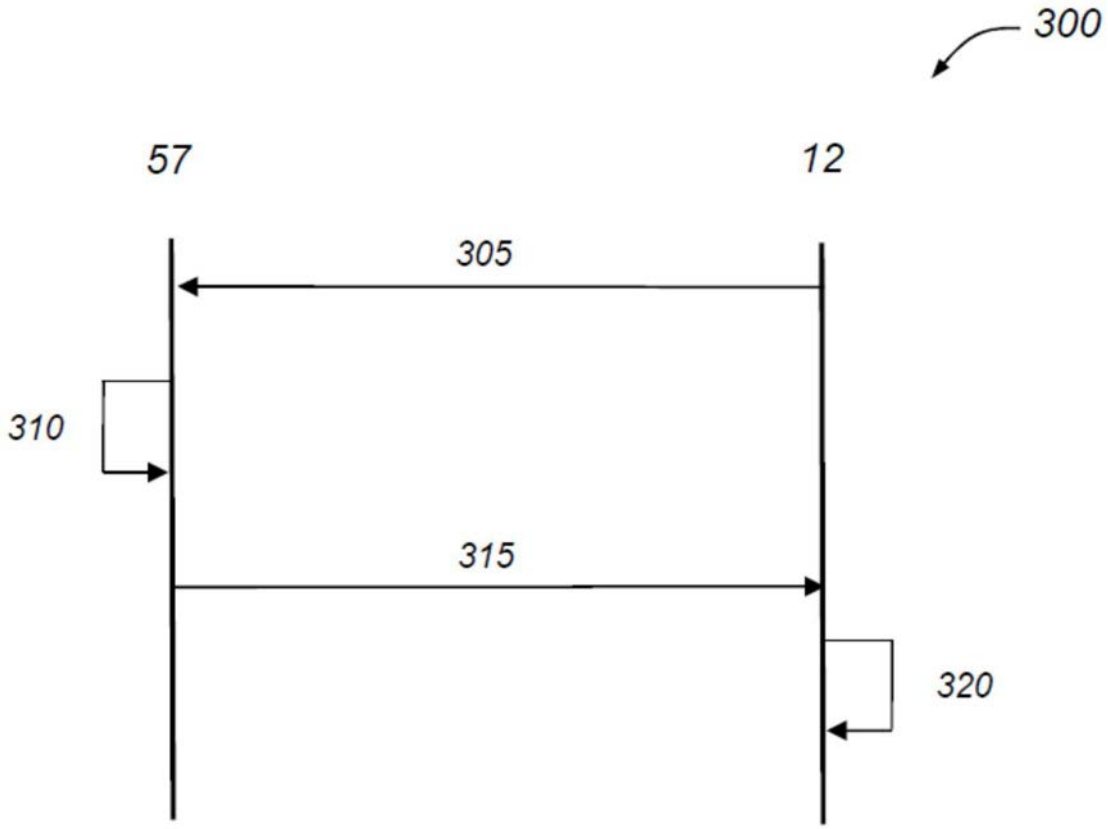
300
57
12
305
310
315
320

图3