(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103874061 A
(43)申请公布日 2014.06.18

(21)申请号 201310757140.9
(22)申请日 2013.12.13
(30)优先权数据
61/737,615 2012.12.14 US
14/084,495 2013.11.19 US
(71)申请人 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 N·R·高塔马 A·J·卡尔霍斯 S·S·马沙尔 K·L·佩尔斯
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 李涛 何逵游
(51)Int.Cl.
H04W 12/02(2009.01)
H04W 76/02(2009.01)
B60R 25/24(2013.01)

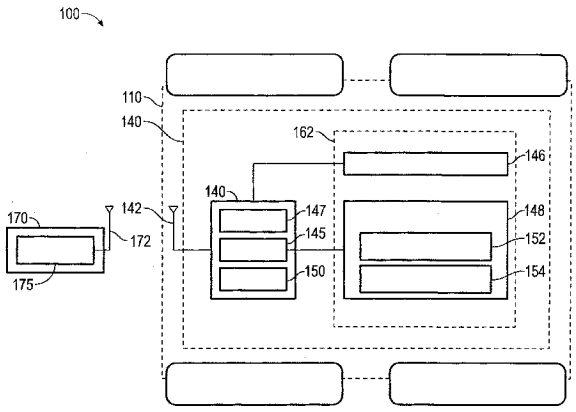
权利要求书1页 说明书13页 附图12页

(54)发明名称

用于车辆与无线通信装置或密钥卡之间的安全和授权通信的方法和系统

(57)摘要

本发明提供了一种系统，其包括无线通信装置（或终端装置）、具有中央模块的车辆、以及密钥配置服务器。所述密钥配置服务器经由无线连接通信地联接至无线通信装置和中央模块。中央模块可与无线通信装置建立无线连接以发起当前通信对话。当与中央模块建立了无线连接时，无线通信装置发出请求消息以请求临时安全信息（例如公共密钥和/或数字证书）。然后密钥配置服务器可响应于所述请求消息提供临时安全信息到无线通信装置和/或中央模块。然后，所述临时安全信息可被用于加密无线通信装置与中央模块之间的通信。



CN 103874061 A

1. 一种系统，包括：

无线通信装置；

车辆，其包括：被构造成用以与所述无线通信装置建立无线连接以发起当前通信对话的中央模块，其中当与所述中央模块建立了无线连接时，所述无线通信装置发出请求消息，其中所述请求消息请求临时安全信息；和

密钥配置服务器，其通信地联接至所述无线通信装置和所述中央模块，其中所述密钥配置服务器被构造成用以响应于所述请求消息来提供所述临时安全信息到所述无线通信装置和所述中央模块，

其中所述临时安全信息被用于对所述无线通信装置与所述中央模块之间的通信进行加密。

2. 根据权利要求 1 所述的系统，其中，所述无线通信装置被构造成用以临时地存储所述临时安全信息，直到确认当前通信对话已结束。

3. 根据权利要求 1 所述的系统，其中，当无线连接已终止达特定时长时，所述无线通信装置和 / 或所述中央模块确认当前通信对话已结束。

4. 根据权利要求 1 所述的系统，其中，当在一定时长内无线连接已终止特定次数时，所述无线通信装置和 / 或所述中央模块确认当前通信对话已结束。

5. 根据权利要求 1 所述的系统，其中，每当所述无线通信装置确定当前通信对话已结束、并且可在所述无线通信装置与所述密钥配置服务器之间获得通信连接时，所述无线通信装置发出请求新的临时安全信息的新的请求消息。

6. 根据权利要求 2 所述的系统，其中，所述密钥配置服务器从所述无线通信装置接收注册消息，其包括用于所述无线通信装置的识别码和用于所述无线通信装置的个人识别号，其中所述密钥配置服务器将所述识别码和所述个人识别号通信到所述中央模块，并且

当已确认当前通信对话已结束、并且所述无线通信装置确定在所述无线通信装置与所述密钥配置服务器之间无法建立通信连接时，其中所述无线通信装置被构造成用以显示用户提示以输入个人识别号，所述个人识别号允许临时存储的所述临时安全信息继续被用于加密所述无线通信装置与所述中央模块之间的通信，即使已经确认当前通信对话已结束。

7. 根据权利要求 1 所述的系统，其中，所述安全信息包括：

加密密钥。

8. 根据权利要求 7 所述的系统，其中，所述安全信息进一步包括：

签署有私有密钥的数字证书。

9. 根据权利要求 1 所述的系统，其中，所述无线通信装置是支持蓝牙的消费类电子装置。

10. 一种方法，包括：

在车辆的中央模块与无线通信装置之间建立无线连接用以发起当前通信对话；

当与所述中央模块建立了无线连接时，从所述无线通信装置发出请求消息，其中所述请求消息请求临时安全信息；以及

响应于所述请求消息从密钥配置服务器提供所述临时安全信息到所述无线通信装置和所述中央模块，其中所述临时安全信息被用于加密所述无线通信装置与所述中央模块之间的通信。

用于车辆与无线通信装置或密钥卡之间的安全和授权通信的方法和系统

技术领域

[0001] 本技术领域主要涉及车辆，尤其涉及无钥匙进入无钥匙启动 (PEPS) 系统以及无线通信装置或密钥卡与车辆之间的安全和授权通信。

背景技术

[0002] 无钥匙进入无钥匙启动系统允许驾驶员或持有授权密钥卡的任何人在接近车辆时无需触碰密钥卡即开启车门。一旦密钥卡处于车辆的范围内，例如 1 米距离内，通过拉动门把即可打开锁住的门。此外，某些 PEPS 系统可被构造成用以当授权密钥卡接近车辆时自动启动车辆的发动机。其他的 PEPS 系统要求驾驶员按动点火按钮来启动和 / 或停止车辆发动机。

[0003] PEPS 系统通常需要位于车辆内部和外部的多个低频 (LF)（例如，125kHz）发射天线。外部天线可位于门把中。在一个 PEPS 系统中，密钥卡检测到从车辆发出的低功率信号，并通过发射密钥码或其他识别码来自动做出响应。车辆中的接收器接收密钥码（或其他识别码）并将其发送给电子控制单元 (ECU)。如果密钥码（或其他识别码）被确认，则密钥卡被“授权”，并且当驾驶员触碰或拉动门把时，ECU 解锁车门。为了启动车辆发动机，驾驶员仅需按动点火按钮。只有当检测到密钥卡位于驾驶室内并且密钥码被再次确认时，ECU 才允许发动机启动。

[0004] 实施 PEPS 系统所需的这些天线和其他硬件及配线的整合是非常昂贵的，而且人们总希望能降低包含这类 PEPS 系统的车辆的成本。

[0005] 一种典型的 PEPS 系统采用与车辆内的中央模块通信的密钥卡。然而，在某些情况下，密钥卡是不可获得的或者无法工作的。例如，驾驶员可能丢失密钥卡，或者无意地将其锁在他们的车辆中。此外，密钥卡授权过程需要密钥卡是可操作的并且可与车辆通信。在这类情况下，希望提供解锁和启动车辆的备用方法。换句话说，希望提供在 PEPS 系统中总是必须使用密钥卡的替代方案。

[0006] 密钥卡与车辆之间的通信的安全性相对较强。密钥卡在制造时被编程有独特的密钥，然后在制造期间或者在经销商处与车辆配对。该编程是使用外人无法访问的专用编程装置在带外完成的。此外，密钥卡具有其自身的不会改变的蓝牙地址。此外，密钥卡不会运行允许它与其他装置（除所述编程装置和车辆外）通信的软件。

[0007] 然而，当无线通信装置例如智能电话被使用来代替密钥卡作为 PEPS 系统的一部分时，发生在使用密钥卡时不会担心的额外的安全风险。可以使用多种不同的黑客技术来访问存储于无线通信装置处的独特密钥。一旦某人获得了该独特的密钥，他们可以利用其与车辆通信，就好像他们是被授权如此做的。这可能允许某人能够进入车辆。

[0008] 此外，某些替代的 PEPS 系统是不安全的，且容易受中继站攻击。在某些情况下，车辆可能违背驾驶员的意愿未被解锁和 / 或启动。正因如此，希望提供采用更复杂的安全机制的更安全的 PEPS 系统。

[0009] 相应地，希望的是提供可帮助解决以上提及的缺点中的一个或多个的改善的 PEPS 系统。例如，希望提供这样的 PEPS 系统，其相对于车辆与比如智能电话等无线通信装置之间的通信提供改善的安全。更进一步，从后续详细描述和所附权利要求书，结合附图和前述技术领域和背景技术来理解，本发明的其它所需特征和特性将变得清楚明了。

发明内容

[0010] 希望提供这样的系统，其相对于车辆与比如智能电话等无线通信装置之间的通信提供改善的安全。

[0011] 提供了一种系统，其包括无线通信装置（在本文中也被称为终端装置）、具有中央模块的车辆、以及密钥配置服务器。所述密钥配置服务器经由无线连接通信地联接至无线通信装置和中央模块。中央模块可与无线通信装置建立无线连接以发起当前通信对话。当与中央模块建立了无线连接时，无线通信装置发出请求消息以请求临时安全信息（例如公共密钥和 / 或数字证书）。然后密钥配置服务器可响应于所述请求消息提供临时安全信息到无线通信装置和 / 或中央模块。然后，所述临时安全信息可被用于加密无线通信装置与中央模块之间的通信。

[0012] 本发明进一步提供以下技术方案：

[0013] 1. 一种系统，包括：

[0014] 无线通信装置；

[0015] 车辆，其包括：被构造成用以与所述无线通信装置建立无线连接以发起当前通信对话的中央模块，其中当与所述中央模块建立了无线连接时，所述无线通信装置发出请求消息，其中所述请求消息请求临时安全信息；和

[0016] 密钥配置服务器，其通信地联接至所述无线通信装置和所述中央模块，其中所述密钥配置服务器被构造成用以响应于所述请求消息来提供所述临时安全信息到所述无线通信装置和所述中央模块，

[0017] 其中所述临时安全信息被用于对所述无线通信装置与所述中央模块之间的通信进行加密。

[0018] 2. 根据技术方案 1 所述的系统，其中，所述无线通信装置被构造成用以临时地存储所述临时安全信息，直到确认当前通信对话已结束。

[0019] 3. 根据技术方案 1 所述的系统，其中，当无线连接已终止达特定时长时，所述无线通信装置和 / 或所述中央模块确认当前通信对话已结束。

[0020] 4. 根据技术方案 1 所述的系统，其中，当在一定时长内无线连接已终止特定次数时，所述无线通信装置和 / 或所述中央模块确认当前通信对话已结束。

[0021] 5. 根据技术方案 1 所述的系统，其中，每当所述无线通信装置确定当前通信对话已结束、并且可在所述无线通信装置与所述密钥配置服务器之间获得通信连接时，所述无线通信装置发出请求新的临时安全信息的新的请求消息。

[0022] 6. 根据技术方案 2 所述的系统，其中，所述密钥配置服务器从所述无线通信装置接收注册消息，其包括用于所述无线通信装置的识别码和用于所述无线通信装置的个人识别号，其中所述密钥配置服务器将所述识别码和所述个人识别号通信到所述中央模块，并且

[0023] 当已确认当前通信对话已结束、并且所述无线通信装置确定在所述无线通信装置与所述密钥配置服务器之间无法建立通信连接时，其中所述无线通信装置被构造成用以显示用户提示以输入个人识别号，所述个人识别号允许临时存储的所述临时安全信息继续被用于加密所述无线通信装置与所述中央模块之间的通信，即使已经确认当前通信对话已结束。

[0024] 7. 根据技术方案 1 所述的系统，其中，所述安全信息包括：

[0025] 加密密钥。

[0026] 8. 根据技术方案 7 所述的系统，其中，所述安全信息进一步包括：

[0027] 签署有私有密钥的数字证书。

[0028] 9. 根据技术方案 1 所述的系统，其中，所述无线通信装置是支持蓝牙的消费类电子装置。

[0029] 10. 根据技术方案 1 所述的系统，其中，所述无线通信装置是能够通过蜂窝网络进行通信的个人无线通信装置。

[0030] 11. 一种方法，包括：

[0031] 在车辆的中央模块与无线通信装置之间建立无线连接用以发起当前通信对话；

[0032] 当与所述中央模块建立了无线连接时，从所述无线通信装置发出请求消息，其中所述请求消息请求临时安全信息；以及

[0033] 响应于所述请求消息从密钥配置服务器提供所述临时安全信息到所述无线通信装置和所述中央模块，其中所述临时安全信息被用于加密所述无线通信装置与所述中央模块之间的通信。

[0034] 12. 根据技术方案 11 所述的方法，进一步包括：

[0035] 在所述无线通信装置处临时地存储所述临时安全信息，直到确认当前通信对话已结束。

[0036] 13. 根据技术方案 11 所述的方法，进一步包括：

[0037] 确定无线连接是否已终止达特定时长；以及

[0038] 当无线连接已终止达特定时长时，在所述无线通信装置和 / 或所述中央模块处确认当前通信对话已结束。

[0039] 14. 根据技术方案 11 所述的方法，进一步包括：

[0040] 确定无线连接是否已终止达特定时长；以及

[0041] 当在一定时长内无线连接已终止特定次数时，在所述无线通信装置和 / 或所述中央模块处确认当前通信对话已结束。

[0042] 15. 根据技术方案 11 所述的方法，进一步包括：

[0043] 每当所述无线通信装置确定当前通信对话已结束、并且在所述无线通信装置与所述密钥配置服务器之间可获得通信连接时，从所述无线通信装置发出请求新的临时安全信息的新的请求消息。

[0044] 16. 根据技术方案 12 所述的方法，其中，所述密钥配置服务器接收来自所述无线通信装置的注册消息，其包括用于所述无线通信装置的识别码和用于所述无线通信装置的个人识别号，其中所述密钥配置服务器将所述识别码和所述个人识别号通信至所述中央模块，并且当已确认当前通信对话已结束、并且所述无线通信装置确定在所述无线通信装置

与所述密钥配置服务器之间无法获得通信连接时，

[0045] 在所述无线通信装置处显示用户提示，用于输入个人识别号，其允许临时地存储的临时安全信息继续被使用来加密所述无线通信装置与所述中央模块之间的通信，即使已经确认当前通信对话已结束。

[0046] 17. 根据技术方案 11 所述的方法，其中所述安全信息包括：

[0047] 加密密钥。

[0048] 18. 根据技术方案 17 所述的方法，其中，所述安全信息进一步包括：

[0049] 签署有私有密钥的数字证书。

[0050] 19. 根据技术方案 11 所述的方法，其中，所述无线通信装置是支持蓝牙的消费类电子装置。

[0051] 20. 根据技术方案 11 所述的方法，其中，所述无线通信装置是能够通过蜂窝网络进行通信的个人无线通信装置。

附图说明

[0052] 下面将结合以下附图来描述示例性实施例，附图中相似附图标记表示相似要素，并且附图中：

[0053] 图 1 是框图，其示出了根据所公开的实施例的包括车辆和终端装置的系统。

[0054] 图 2 是简易框图，其示出了根据某些公开的实施例的可被实施在组合功能传感器装置、中央模块和 / 或终端装置处的蓝牙芯片组和蓝牙天线的示例。

[0055] 图 3 是示意图，其示出了根据所公开的实施例的用于将私有 / 公共密钥对和 / 或数字证书分配给密钥卡和车辆的系统。

[0056] 图 4 是示意图，其示出了根据所公开实施例的在将无线通信装置注册到密钥配置服务器 (KPS) 和车辆的中央模块时的图 3 的系统。

[0057] 图 5 是示意图，其示出了根据所公开的实施例的在无线通信装置接近车辆、进入蓝牙通告范围内并请求新的公共密钥时的图 3 的系统。

[0058] 图 6 示出了根据所公开的实施例的、在无线通信装置进入车辆的建立授权所需的授权范围内时、在无线通信装置与车辆的中央模块之间的安全通信信道的建立。

[0059] 图 7 示出了根据所公开的实施例的、当无线通信装置无法与 KPS 建立连接以读取新的公共密钥时的情形。

[0060] 图 8 示出了根据所公开实施例的、当无线通信装置无法与 KPS 建立连接以读取新的公共密钥时、在无线通信装置与车辆的中央模块之间建立安全通信信道的方法。

[0061] 图 9 示出了根据所公开的实施例的、在无线通信装置进入车辆的授权范围内时、在无线通信装置与车辆的中央模块之间的安全通信信道的建立。

[0062] 图 10 示出了根据所公开的实施例的、当无线通信装置移动返回蓝牙通告范围内使得无线通信装置可发起与车辆的中央模块的新的安全通信对话时的、由无线通信装置从密钥配置服务器读取新的公共密钥情形。

[0063] 图 11 是系统的示意图，其示出了根据所公开的实施例的当密钥卡进入蓝牙通告范围内时用于将公共密钥分配给密钥卡的方法。

[0064] 图 12 是图 11 的系统的示意图，其示出了根据所公开的实施例的当密钥卡进入车

辆的授权范围内时用于在密钥卡之间安全通信的方法。

具体实施方式

[0065] 以下详细描述本质上仅仅是示例性的，并不旨在限制应用和用途。更进一步，没有意图被在前面的技术领域、背景技术、发明内容或以下详细描述中给出的任何明示或暗示的理论限制。

[0066] 图 1 示出了系统 100，其包括根据所公开的实施例的车辆 110 和终端装置 170。

[0067] 终端装置 170 为支持蓝牙的装置。终端装置 170 包括蓝牙天线 172 和蓝牙芯片组 175，且且能够执行所有已知的蓝牙标准和协议，包括蓝牙低功耗 (BLE) 协议。蓝牙技术规范由蓝牙技术联盟 (SIG) 开发和公布。2010 年 6 月 30 日采用的蓝牙核心规范 4.0 版、2011 年 12 月 27 日采用的核心规范补充 (CSS) 第 1 版、2011 年 12 月 27 日采用的核心规范附录 (GSA)2、2012 年 7 月 24 日采用的核心规范补充 (CSS) 第 2 版和 2012 年 7 月 24 日采用的核心规范附录 (CSA)3 描述了 BLE 标准的各种特征，并通过引用整体并入本文。包括蓝牙规范 4.0 版在内的任何合并入本文的核心规范的副本都可以从蓝牙技术联盟 (SIG) 获得，方法是通过写信到Bluetooth Special Interest Group，5209Lake Washington Blvd NE，Suite 350，Kirkland，WA98033，USA，或者存取他们的网站并下载副本。蓝牙核心规范 4.0 版包括经典蓝牙、蓝牙高速 (HS) 协议和蓝牙低功耗 (BLE)。

[0068] 没有限制地，终端装置 170 可以是任何支持蓝牙的通信装置，例如智能电话或其他蜂窝电话、膝上型或掌上型电脑、平板电脑、个人数字助理、支持蓝牙的遥控器、令牌 (token)、密钥卡 (key fob)、表、游戏手柄、娱乐装置或任何其他的支持蓝牙的装置。此外，需要注意的是，终端装置 170 实际上在某些实施方式中可以是多种不同的装置（例如，密钥卡和比如智能电话等支持蓝牙的通信装置）。正因如此，如果驾驶员携带有支持蓝牙的智能电话和支持蓝牙的密钥卡，则系统可以独立地处理来自这些装置中的每个的信号强度信息，以确定驾驶员与车辆的接近程度。这同样有利于这些装置之一不可用（例如，丢失、没电、无法工作）的情形，因为其提供了备用。例如，在一种情形中，支持蓝牙的智能电话可能死机了，但是驾驶员可能携带有密钥卡，或反之亦然。在另一种情形中，驾驶员可能意外地将他们的密钥卡锁在车内，并且只带有智能电话。

[0069] 车辆 110 包括多个执行各项管理和控制功能的车载模块 140。

[0070] 车载模块

[0071] 再次参考图 1 所示的具体实施例，车载模块 140 包括 ：中央模块 144 和电子控制单元 (ECU)162。

[0072] 中央模块 144 包括蓝牙芯片组 145、终端装置验证和授权模块 147、和终端装置接近检测模块 150。根据某些公开的实施例，中央模块 144 可被实施在资讯娱乐模块或远程信息处理模块内。将中央模块 144 实施在资讯娱乐模块或远程信息处理模块内的一个优势为 ：这些模块中的任一个通常已具有蓝牙芯片组，因此无需提供额外的专用蓝牙芯片组来供中央模块 144 使用。在一个实施例中，中央模块 144 在每个驾驶循环结束时动态地并随机地生成用于终端装置 170 的新蓝牙地址。中央模块 144 可利用用于终端装置 170 的新蓝牙地址来验证和验证终端装置 170。

[0073] ECU162 可包括其他车载模块，包括但不限制于胎压管理模块 146、和无钥匙进入

无钥匙启动 (PEPS) 系统控制模块 148。PEPS 系统控制模块 148 包括远程致动模块 152 和主体控制模块 154。车载模块 140 被示出为组合在界定出车载模块 140 的单个框中；然而，需要指出的是，车载模块 140 也可以分散在车辆 110 内，并且可彼此通过一个或多个总线进行通信。

[0074] 终端装置 170、中央模块 144 和 ECU162 被用于提供无钥匙进入无钥匙启动 (PEPS) 系统，以便在终端装置 170（例如，智能电话或密钥卡等）接近车辆并符合授权标准时，相对于车辆实施至少一个无钥匙进入无钥匙启动（PEPS) 功能。

[0075] 为此，中央模块 144 可经由蓝牙无线连接（例如，蓝牙低功耗（BLE) 无线连接）通信地联接至终端装置 170。终端装置 170 根据蓝牙通信协议与中央模块 144 通信。此外，终端装置 170 在其上装有各种应用，例如无钥匙进入无钥匙启动（PEPS) 应用程序（如在图 2 中由附图标记 201 所示），其允许终端装置 170 作为 PEPS 系统的一部分与位于车辆内的无钥匙进入无钥匙启动系统控制模块 148 结合来提供信息和生成指令。

[0076] 在某些实施例中，中央模块 144 可对终端装置 170 通过通告信道传输来的通告消息进行过滤扫描。

[0077] 中央模块 144 可以基于来自接收于终端装置 170 的报告消息的信号强度信息来确定终端装置 170 与车辆的距离。

[0078] 基于终端装置 170 与车辆的距离，中央模块 144 于是可确定终端装置是否位于授权范围内。因此，信号强度信息可用于确定与车辆的接近程度。在某些实施例中，当终端装置被确定为位于授权范围内时，中央模块 144 可通过与终端装置在数据信道上交换消息来对终端装置 170 发起授权程序，然后控制在车辆 100 处的至少一个无钥匙进入无钥匙启动 (PEPS) 功能的性能。例如，在一个实施例中，中央模块 144 可进行质询 / 应答，并发送结果给 BCM。这里，将确定终端装置 170 是否被授权进入车辆。

[0079] 例如，在某些实施例中，当确定终端装置 170 足够靠近车辆 110 时，执行 PEPS 功能（例如，解锁车门、启动发动机等）。当确定终端装置 170 距离车辆 110 太远时，PEPS 系统保持未启动状态且车门保持锁定。

[0080] 此外，根据某些公开的实施例，中央模块 144 还包括验证和授权模块 147，其可执行在本文中提及的任一蓝牙通信标准所描述的验证和 / 或授权机制，以及未在蓝牙标准中描述的其他验证和 / 或授权机制。正因如此，验证和授权模块 147 可接收从终端装置 170 传输的信号，并执行终端装置 170 的授权和 / 或验证。当终端装置 170 已被授权和 / 或验证时，这允许终端装置 170 作为用于某些车载模块 140 的控制器。取决于实施方式，这种控制可以被自动执行，也可以是在持有终端装置 170 的用户的命令下执行。

[0081] 如以上指出的，在一个实施方式中，中央模块 144 和终端装置 170 可各自包括蓝牙芯片组 145/175。下面将参考图 2 描述蓝牙芯片组的一个实施方式的某些特征。

[0082] 图 2 是框图，其示出了根据所公开实施例的一部分非限制性示例的终端装置 170 和 / 或可被实施在中央模块 144 处的蓝牙芯片组 145/175 和蓝牙天线 142/172 的示例。

[0083] 蓝牙芯片组 145/175 包括：应用程序 200；蓝牙低功耗 (BLE) 协议栈 203；可选的蓝牙基本速率（BR)/ 增强数据速率 (EDR) 协议栈 204；蓝牙无线电收发器 208；处理器 220，处理器 220 包括例如中央处理单元 (CPU)，比如双核核心处理单元 (CPU)260 和 261（或其他任何具有任意数量的处理器内核的多核 CPU)；随机存取存储器（RAM) 262；只读存储器

(ROM)264；和与蓝牙无线电收发器208交接的接口电路266。RAM262和ROM264可使用任何已知类型的半导体存储器来实施。

[0084] 在本文中描述的任一蓝牙芯片组145/175基于实施方式可以是单模装置或双模装置。

[0085] 单模蓝牙芯片组是唯BLE芯片组，其被最优化来用于超低功率操作，并且其可以与其他单模蓝牙芯片组和双模蓝牙芯片组通信，对于后者是在其使用他们的构造中的BLE技术部分来传输和接收时。单模芯片可使用纽扣电池（例如，3V，220mAh CR2032）来长时间（数月甚至数年）操作。

[0086] 相比之下，双模蓝牙芯片组还能够与使用常规蓝牙结构的经典蓝牙技术或其他多模芯片组通信。双模蓝牙芯片组能够与所有的传统经典蓝牙装置以及BLE装置通信。然而，由于它们被要求执行经典蓝牙和BLE任务，双模芯片对于用以达到与单模装置相同程度的ULP操作来说并不是最佳的。相反，经典蓝牙技术和BLE双模装置通常要求至少两个AAA电池的电量（其具有10-12倍纽扣电池的电量以及高得多的峰值电流公差），并且常常用以给它们供电达数天或数周（取决于应用）。

[0087] 正因如此，蓝牙芯片组145/175至少包括蓝牙低功耗(BLE)协议栈203，并且在某些实施方式中，还可包括蓝牙BR/EDR协议栈204。

[0088] BLE协议栈203在蓝牙核心规范4.0版协议规范中有描述，其通过引用整体并入本文。BLE协议栈203被最佳化来用于偶尔连接，其允许连接之间的更长休眠时间、少量数据传递、极低占空比和拓扑比经典蓝牙更简单的装置。作为基础帮助实现超低功率(ULP)性能的BLE技术的一些特性是最大化的待机时间、快速连接、和低峰值传输/接收功率。经典蓝牙采用带有固定的连接间隔时间的“以连接为导向的”无线电。相反地，BLE技术采用可变连接间隔时间，其可被设定为从数毫秒到数秒，取决于应用。此外，由于其特征在于非常快速的连接，BLE技术可通常处于无连接的状态，其中链路的两端知道彼此，但是只在绝对必要时才链接上并且时间尽可能短。BLE技术的这种无连接的操作模式理想地适合于这样的数据传输，其中可使用完全异步的通信来非频繁地通信发送少量数据。

[0089] 在某些实施方式中，任意或所有的蓝牙芯片组145/175还可包括蓝牙BR/EDR协议栈204，其在蓝牙规范3.0+HS版中有描述，该规范通过引用整体并入本文。

[0090] 蓝牙协议栈203和204和/或应用程序200可体现为以程序指令序列的形式存储在RAM262和/或ROM264内的程序逻辑，其在CPU260和/或261中被执行时，实现所公开实施例中的至少一部分功能。程序逻辑可以从计算机程序产品输送至RAM262或ROM264，所述计算机程序产品呈计算机可使用介质的形式，例如常驻存储装置、智能卡或其他可移除的存储装置。替代地，他们可以体现为呈编程逻辑阵列或定制设计的专用集成电路(ASIC)形式的集成电路逻辑。在一些实施方式中，程序逻辑可以从这种计算机可读介质中被下载，用以存储在例如RAM262或可编程ROM264中，用于由CPU260和/或261执行。

[0091] 蓝牙无线电208可包括单独的收发器电路，或替代地，无线电208可以是能够以高度速度、时间和频率多路复用的方式处理一个或多个信道的单个无线电模块。

[0092] 其他无线电270可以是本领域中公知的各种无线个人区域、无线本地区域，或无线广域无线电装置中的任一种。其他无线电270可以是能够在蜂窝式无线电网络内通信的无线电。其他无线电270可包括蜂窝接口，其可使用多种不同的多路存取技术中的任一

种，例如频分多路复用 (FDM)、时分多路复用 (TDM)、码分多路复用 (CDM) 等。可使用的多路存取方案的示例可包括以下中的任一个或多个 ：时分多路存取 (TDMA) ；直接序列或频率跳变码分多路存取 (CDMA) ；全球移动通信系统 (GSM) ；宽带 CDMA(WCDMA) ；通用移动电信系统 (UMTS) ；频分多路存取 (FDMA) ；正交频分多路复用 (OFDM) ；机会分割多路存取 (ODMA) ；前述多路存取技术中任意种的组合 ；这样的多路存取技术，其中待使用的频谱的一些部分由本地信号质量测量来确定，并且其中频谱中的多个部分可被同时使用 ；或者任何其他的多路存取或多路复用操作方法或其组合。此外，另一无线电 270 可支持遵从至少下列通信标准的通信 ：(1) 由名为“第三代合作伙伴项目”(3GPP) 的协会监管的标准 ；(2) 由名为“第三代合作伙伴项目 3”(3GPP2) 的协会监管的标准 ；(3) 遵守 TIA/EIA/IS-856 标准 (IS-856 标准) 的高数据速率 (HDR) 系统 ；和 (4) 其他标准。

[0093] 此外，另一无线电 270 还可包括 WLAN 接口，其可为例如自设组网空中接口，所述自设组网空中接口遵守 ：IEEE802.11 标准和规范 (例如，IEEE802.11(a)，(b)，(g)，或 (n) 中的任一个)；IEEE802.16 标准 (例如，IEEE802.16eWiMax 规范) 中的任一个 ；或另外的无线标准 (例如，用于基于 IP 的服务的 IEEE802.20 移动宽带无线接入 (MWA) 规范)。

[0094] 最后，除了别的外，应用程序 200 还可包括 ：PEPS 系统控制模块 201 ；和可用于执行任一下述的安全性相关任务的安全模块 202。

[0095] 公共密钥加密术和数字证书的概述

[0096] 在以下描述中，将对公共密钥加密术和数字证书进行各种参考。在参考图 3-12 描述各实施例前，将描述关于公共密钥加密术和数字证书的一些基本信息。

[0097] 公共密钥加密术

[0098] 公共密钥加密术是指需要两个单独密钥的加密系统 ：机密的私有密钥以及非机密的公共密钥。公共密钥可以公开而不会危及安全性，而私有密钥则不能泄露给未经授权来读取消息的任何人。公共密钥加密术使用不对称密钥算法 (例如 RSA)，并且还可由更通用的术语“不对称密钥加密术”来称呼。公共密钥加密术是基础的、重要的、并且被广泛使用的技术。它是被许多加密算法和加密系统使用的途径。有三种主要类型的公共密钥系统 ：公共密钥分配系统、数字签名系统，以及可执行公共密钥分配和数字签名服务两者的公共密钥加密系统。迪菲 - 赫尔曼密钥交换是最广泛使用的公共密钥分配系统，而数字签名算法是最广泛使用的数字签名系统。

[0099] 公共密钥加密术中使用的区别技术是不对称密钥算法的使用，其中用于对消息进行加密的密钥与用于对它进行解密的密钥是不同的。尽管不同，该配对密钥的两部分在数学上是有联系的。一个密钥对明文进行锁定或加密，而另外一个对密文进行解锁或解密。任一密钥都不能独自执行两项功能。每个用户拥有一对加密密钥——公共加密密钥和私有解密密钥。可公共获得的加密密钥被广泛分配，而私有解密密钥仅有接受者知晓。消息由接受者的公共密钥加密，并且仅能以相应的私有密钥解密。密钥在数学上相关联，但是参数被选择成使得从公共密钥来确定私有密钥要么不可能的要么是极其昂贵的。

[0100] 公共密钥加密术的两个主要用途为 ：

[0101] 公共密钥加密 ：在公共密钥加密中，由接受者的公共密钥加密的消息不能被除了匹配私有密钥的持有者之外的任何人解密。换句话说，发送者使用接受者的公共密钥加密的消息只能由接受者的配对的私有密钥解密。假定的是这将是密钥的所有者以及与所使用

的公共密钥相关的人。这被使用来试图确保保密性。

[0102] 数字签名：公共密钥加密术还可用于数字签名方案（例如用于发送者验证和抗抵赖）。在数字签名方案中，希望发送消息的用户计算用于该消息的数字签名，然后发送该数字签名（与信息一起）到目标接收者。数字签名方案具有这样的性能，即仅能在知晓正确私有密钥的情况下计算出签名。为了检验消息已经由用户签名并且未被修改，接收者仅需要知晓相应的公共密钥。在数字签名方案中，可通过使用私有密钥生成消息的数字签名来检查消息的真实性，其然后可通过使用公共密钥来得到检验。((在很多情况下，只有消息的散列(hash)通常被加密来用于签名验证目的。))正因如此，签署有发送者的私有密钥的消息可被拥有该发送者的公共密钥的任何人验证，由．比证明发送者可以利用私有密钥，因此可能是与所使用的公共密钥相关的人。这还确保消息未被篡改。

[0103] 为了实现验证和保密性两者，发送者可首先使用他的私有密钥来对消息签名，然后使用接受者的公共密钥对消息和签名两者加密。这些特征可被用于构建多种其他的（有时是意外的）加密协议和应用，例如数字货币、密码验证密钥协商、多方密钥协商、时间戳服务、抗抵赖协议等。在某些情况下（例如，RSA），存在与加密方案具有许多相似性的数字签名方案。在另一些情况下（例如，DSA），该算法与任何加密方案都不相似。

[0104] 公其密钥基础结构(PKI)

[0105] 在公共密钥机构(PKI)中，被称作认证机构的一个或多个第三方证明密钥对的所有权。

[0106] 数字证书

[0107] 数字证书（也称为公共密钥证书或身份证书）是使用数字签名来将公共密钥与身份（例如，人名或机构名、他们的地址等信息）绑定的电子文件。证书可用于检验公共密钥属于某个个体。

[0108] 在典型的公共密钥基础结构(PKI)方案中，签名将属于认证机构(CA)。在信任方案的网络中，签名要么属于用户（自签名证书），要么属于其他用户（“背书(endorsement)”）。无论哪种情况下，证书上的签名都是证书签名者对身份信息和公共密钥属于彼此的证明。

[0109] 为了可证明的安全性，这种对系统外的事物的依赖具有的后果是：任何公共密钥认证方案都不得不依赖某些特别的设置假定，例如认证机构的存在。

[0110] 更多关于加密术、公共密钥加密术、PKI、数字证书等的信息可以例如从以下文献中找到：N.Ferguson、B.Schneier(2003).Practical Cryptography.Wiley.ISBN0-471-22357-3；J.Katz、Y. Lindell(2007).Introduction to Modern Cryptography.CRC Press.ISBN1-58488-551-3；和 A.J.Menezes、P. C.van Oorschot、S.A.Vanstone(1997).Handbook of Applied Cryptography.ISBN0-8493-8523-7，它们都通过引用整体并入本文。

[0111] 经由密钥配置服务器的密钥卡编程

[0112] 图3是示出了根据所公开的实施例的用于将私有/公共密钥对和/或数字证书分配给密钥卡175和车辆110的中央模块140的系统300示意图。系统300包括密钥配置服务器(KPS)310、制造工厂320、车辆经销商330、密钥卡编程装置340、车辆110和密钥卡175。

[0113] 如以上所说明的，车辆 110 包括中央模块 140 和 ECU 模块 162。

[0114] 在 314，密钥卡编程装置 340 将请求消息传输到 KPS410 来请求公共密钥基础结构 (PKI) 私有 / 公共密钥对和 / 或数字证书。请求消息包括车辆的车辆识别号 (VIN)。KPS410 生成新的 PKI 私有 / 公共密钥对（和 / 或数字证书）并存储它与 VIN。新的 PKI 私有 / 公共密钥对将用于在未来的终端装置注册过程中将终端装置（智能电话、密钥卡等）与中央模块 140 配对。

[0115] 在 316，KPS410 传输响应消息到装置 340。响应消息包括私有 / 公共密钥对和 / 或数字证书。在 318，密钥卡编程装置 340 将私有密钥传输到车辆 110 的中央模块 140。中央模块 140 可最终使用私有密钥来加密发送给密钥卡 175 的通信或解密从密钥卡 175 接收到的通信。

[0116] 在 320，密钥卡编程装置 340 将 (PKI 私有 / 公共密钥对的）公共密钥和 / 或数字证书传输到密钥卡 175。

[0117] 在 322，密钥卡 175 可在制造工厂 320 或车辆经销商 330 处被预编程，以将密钥卡 175 与车辆的中央模块 140 配对。

[0118] 以密钥配置服务器注册无线通信装置

[0119] 图 4 是示出了根据所公开实施例的以图 3 的 KPS410 和中央模块 140 注册无线通信装置 170 示意图。在图 4 中，框 420 代表经由无线通信装置 170 上的应用访问的注册网站。

[0120] 当无线通信装置 170 的用户打开应用时，开始对话 (session)。无线通信装置 170 在 412 处将消息通信至 KPS410 来以 KPS410 注册无线通信装置 170；该注册信息可包括用于无线通信装置 170 的 IMEI（或其他独特的识别码）。在一替代实施例中，注册信息可包括附加的信息（例如，是装置 170 独有的，但不是 IMEI）。这可以帮助防止电子欺骗和恶意软件的使用。

[0121] 在 414，无线通信装置 170 的用户输入个人识别号 (PIN)。

[0122] 在 422，注册信息和 PIN 被通信至 KPS410，并且 KPS410 存储注册信息以及 PIN。这时，PIN 码和 IEMI 都已注册到 KPS410。

[0123] 在 432，KPS410 将无线通信装置 170 的 PIN 和国际移动设备识别码 (IMEI) 通信到车辆 110 的中央模块（图 4 中未示出，但是在图 1 中显示为 140）。PIN 码以及识别码已被提供给车辆的中央模块用于授权。

[0124] 使用从密钥配置服务器提供的安全信息在无线通信装置与中央模块之间建立安全通信连接

[0125] 根据所公开的实施例，提供了系统和方法来用于无线通信装置（例如，智能电话）与车辆的中央模块之间的安全通信。

[0126] 将参考图 5-10 来描述用于在无线通信装置（例如，智能电话）与车辆的中央模块之间分配安全信息的系统和方法的描述。在该描述中，将描述一个示例性实施方式，其中被分配的安全信息将被描述为公共密钥。

[0127] 然而，在另一些实施方式中，安全信息可包括任何其它公知类型的安全信息，例如在加密系统中经常使用的密钥或证书。

[0128] 例如，在另一实施方式中，安全信息可以是签署有私有密钥的数字证书。

[0129] 在另一些实施方式中，一旦无线通信装置被确认为位于授权范围内时，这些不同类型的安全信息的组合可以被分配并用于保证无线通信装置（例如，智能电话）与车辆的中央模块之间的通信。例如，在一个实施方式中，安全信息可包括公共密钥和签署有私有密钥的数字证书两者。

[0130] 图 5 是示出了在无线通信装置 170 接近车辆 110 时的图 3 所示系统 400 示意图。

[0131] 当无线通信装置 170 进入车辆的蓝牙通告范围时，无线通信装置将请求消息通信至 KPS410，来请求新的公共密钥，其可在与车辆 110 的中央模块的新对话过程中使用。为了进一步说明，当无线通信装置 170 接近车辆 110 并进入蓝牙通告范围 520 内（例如，在一个实施方式中为大约 100 米）时，无线通信装置 170 处的安全模块通过向密钥配置服务器 (KPS)410 传输（在 512）请求消息来请求新的公共密钥，从而尝试开始新的安全通信对话。该请求消息包括对于新公共密钥的请求，用以在与车辆 110 的中央模块 140 进行该新的安全通信对话过程中使用。每次对话都可请求不同的新的公共密钥（或其他安全信息）。此外，在一些实施方式中，一旦与 KPS410 已经建立安全连接，KPS410 可发送其他的安全信息例如加密密钥给无线通信装置 170，该安全信息也可用于为无线通信装置 170 与中央模块 140 之间的通信加密。

[0132] KPS410 通过生成新的公共密钥并将响应消息 514 通信返回无线通信装置 170 来做出响应。该响应消息包括新的公共密钥。KPS410 还将消息通信至车辆 110 的中央模块 140（在 516），以提供公共密钥给中央模块 140，并让中央模块 140 知道已经建立了新的对话，并且已经将公共密钥提供给无线通信装置 170。然后，中央模块 140 在 518 通信响应消息给 KPS410，以确认对话已经建立。

[0133] 特别地，该新的（临时的）公共密钥仅用于无线通信装置 170 与中央模块 140 之间的该特定通信对话。每当在无线通信装置 170 与车辆 110 的中央模块 140 之间开始新的安全通信对话时，在无线通信装置 170 与 KPS410 之间执行请求 / 响应交换 512、514。

[0134] 图 6 示出了根据所公开的实施例的在无线通信装置 170 与图 3 的中央模块 140 之间建立安全的和授权的通信信道的示意图。

[0135] 在获取新的公共密钥后，当无线通信装置 170 进入车辆 110 的授权范围内时，在 612，无线通信装置 170 可传输连接请求消息到中央模块 140 以尝试建立授权连接。如本文中所使用的，术语“授权范围”是指无线通信装置 170 必须相对于中央模块 140 处于其内以便与车辆的中央模块 140 建立授权连接的距离。在一个实施方式中，授权范围大约为 5 米。中央模块 140 可以使用上述的任何邻近检测技术来确定无线通信装置 170 是否处于授权范围内。

[0136] 在 612 通信的连接请求消息是使用在图 5 的 514 处提供给无线通信装置的公共密钥而得到加密。

[0137] 响应于连接请求消息，在 614，中央模块 140 通信连接响应消息到无线通信装置 170。连接响应消息由私有密钥（其从 KPS410 下载到中央模块 140，并且在图 3 的 318 处被编程到中央模块 140 中）加密，并且被用于与无线通信装置 170 建立授权连接。

[0138] 对于任何后续通信，在该特定的通信对话过程中，新的公共密钥可被无线通信装置 170 和中央模块 140 使用来加密和 / 或解密这两个实体 170、140 之间通信的信息。特别地，该新的公共密钥仅用于该对话，并且不被存储在无线通信装置的存储器中。当该特定

的通信对话结束（例如，被关闭）时，最新获取的公共密钥不再有效，并且不能用于保护两个实体 140、170 之间的通信，除非使用无线通信装置 170 的 PIN 执行附加的验证。这样，当通信对话结束时（例如，如果无线通信装置在对话有效期间移动出车辆的蓝牙通告范围 520），在某些实施例中，公共密钥可被临时地存储于无线通信装置 170 的存储器中，以便在不能与 KPS410 建立连接时使用，如现在将在下面描述的。

[0139] 当与密钥配置服务器没有连接时在无线通信装置与中央模块之间安全建立授权连接

[0140] 根据一些其他公开的实施例，当无线通信装置（和 / 或车辆）无法连接到 KPS（例如，数据或者网络连接不可用）时，提供了其他机制来确保无线通信装置 170 与中央模块 140 仍可以安全的方式通信。这样，当无法连接到 KPS 时，可提供备用方法。例如，在一个实施例中，当无线通信装置检测到不再能够连接到 KPS410 时，公共密钥（用于最近一次对话）可被临时地存储于存储器中。无线通信装置的安全模块应用将提示用户手动地输入预注册的个人识别号 (PIN) 到无线通信装置 170 中。然后，无线通信装置 170 和中央模块 140 可使用该 PIN 以及之前的或“最近获取的”公共密钥（其被存储于存储器中），来在该对话过程中对无线通信装置与中央模块之间通信的信息进行加密或解密。更多细节将在下面参考图 7-10 进行描述。

[0141] 图 7 示出了无线通信装置 170 位于蓝牙通告范围 520 内但是无法与 KPS410（在 712）建立连接来读取新的公共密钥时的情形。此处，无线通信装置 170 试图建立新的对话，但是无法连接到 KPS410。希望的是即使无线通信装置 170 无法读取通常情况下启动新的安全通信对话所需的新的公共密钥，无线通信装置 170 也能够继续与中央模块 140 通信。

[0142] 图 8 示出了当无线通信装置 170 无法与 KPS410 建立连接以读取新的公共密钥时在无线通信装置 170 与车辆 110 的中央模块 140 之间建立安全通信信道的方法。当无线通信装置 170 进入车辆 110 的蓝牙通告范围 520（例如，在一个实施方式中为大约 100 米）内并且无法连接到 KPS410 时，无线通信装置 170 的用户将被提示输入预注册的 PIN。在某些实施例中，在无线通信装置上运行的安全模块应用随机地改变用户界面上的数字按钮的位置，使得预注册的 PIN 无法被确定。

[0143] 图 9 示出了当无线通信装置 170 进入车辆 110 的授权范围 530 内但是尚未与 KPS410 建立数据连接时在无线通信装置 170 与车辆 110 的中央模块 140 之间建立安全通信信道。当无线通信装置 170 进入授权范围 530 内时，预注册的 PIN（其由无线通信装置 170 的用户输入）于是可与最近获取的公共密钥一起被用于对通信至中央模块 140 的信息进行加密。另一方面，中央模块 140 使用 PIN 以及签署有私有密钥的数字证书，来对将被发送至无线通信装置 170 的信息进行加密。

[0144] 图 10 示出了当无线通信装置 170 已与密钥配置服务器 410 重新建立连接时由无线通信装置 170 从密钥配置服务器 410 读取新的公共密钥。特别地，当无线通信装置 170 移动返回车辆的蓝牙通告范围 520 内（例如，在一个实施方式中为大约 100 米）时，无线通信装置 170 可以读取新的公共密钥（使用以上参考图 5 所描述的请求 / 响应交换）。为进一步说明，装置 170 将必须获取新的密钥以与车辆 110 的中央模块 140 通信。这样，无线通信装置 170 可以与车辆的中央模块 140 进行新的安全通信对话，其中所述新的公共密钥于是被用于在所述新的通信对话过程中对无线通信装置与中央模块之间通信的信息进行加

密或解密。旧的公共密钥（其被临时地存储于无线通信装置的存储器中）于是可被删除。如果在蓝牙范围内并且已经开启了新的对话，一旦已与 KPS410 重新建立连接，则新的密钥将被发出并且立即被用于当前的对话。

[0145] 使用公共 / 私有密钥对在密钥卡与中央模块之间安全建立授权连接

[0146] 图 11 是系统 1100 的示意图，其示出了根据所公开的实施例的当密钥卡 175 进入蓝牙通告范围 520 内时用于将公共密钥分配给密钥卡 175 的方法。当密钥卡 175 进入车辆的蓝牙通告范围 520 内时，如果 RKE 功能被执行，则密钥卡 175 将建立安全通信。

[0147] 图 12 是图 11 的系统 1100 的示意图，其示出了根据所公开的实施例的当密钥卡 175 进入车辆 110 的授权范围 530 内时用于在密钥卡 175 之间安全通信的方法。当密钥卡 175 进入用于与车辆授权连接的范围内时，来自车辆的公共密钥以及签署有私有密钥的数字证书将被用于加密正在中央模块 140 与无线通信装置 170 之间通过安全蓝牙信道发送的数据，并且用于任何将在该特定的通信对话过程中通信的消息。再次，用于公共密钥的滚动码基础结构被用于防止来自未授权装置的中继 / 回放攻击。

[0148] 虽然在前述详细描述中给出了至少一个示例性实施例，但是应该理解的是存在大量的变型。还应该理解的是：一个示例性实施例或多个示例性实施例只是示例，并不旨在以任何方式限制本公开的范围、适用性或构造。相反，前述详细描述将为本领域技术人员提供便利的线路图来实施一个示例性实施例或多个示例性实施例。应该明白的是：可在要素的功能和配置中做出各种变化，而不背离如在所附权利要求及其法律等同方案中阐述的本公开的范围。

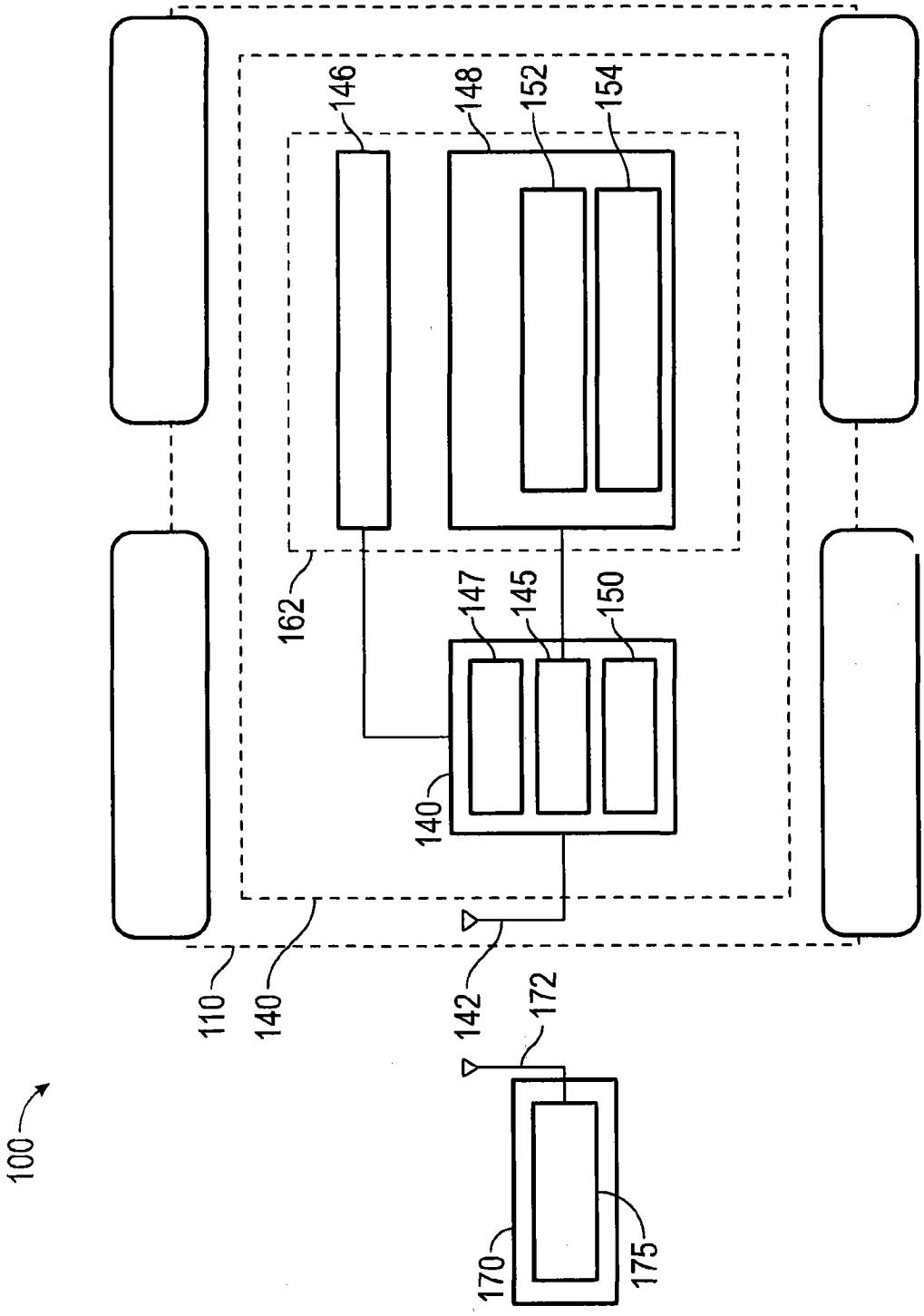


图 1

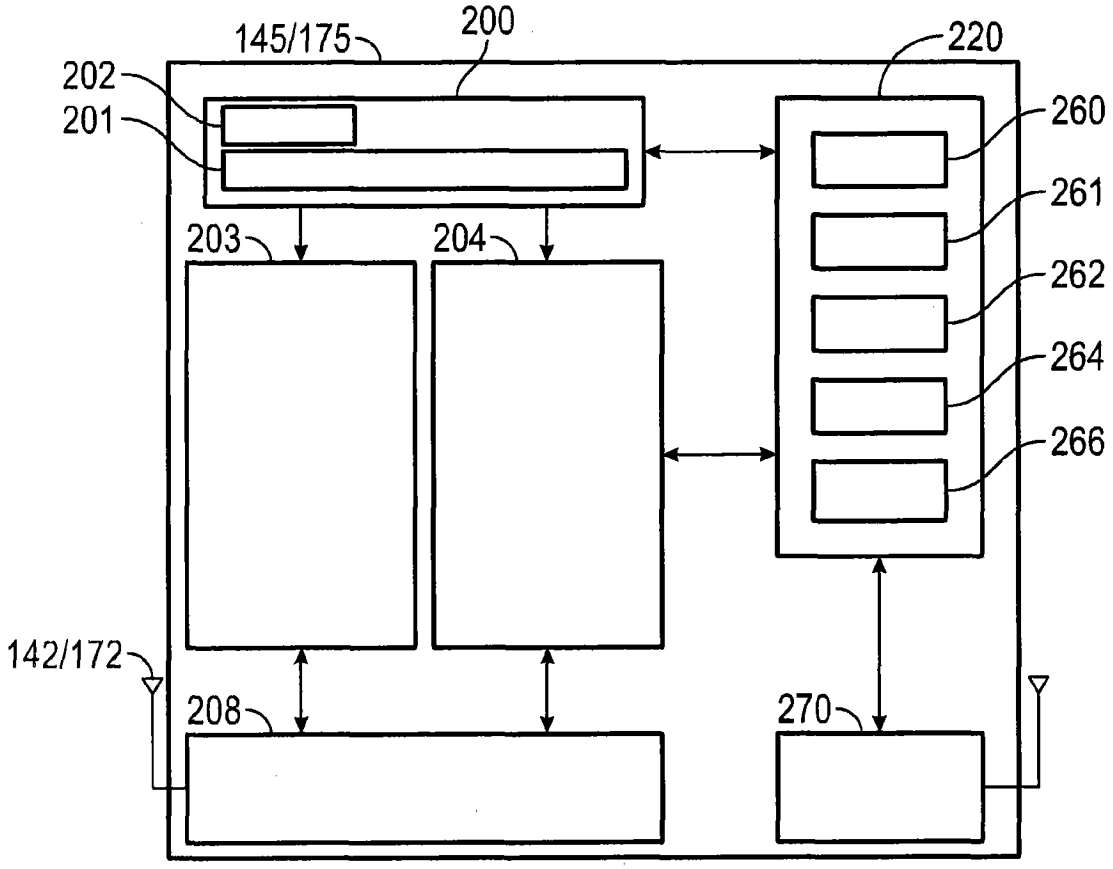

145/175
200
220
202
201
260
261
262
264
266
203
204
142/172
208
270

图 2

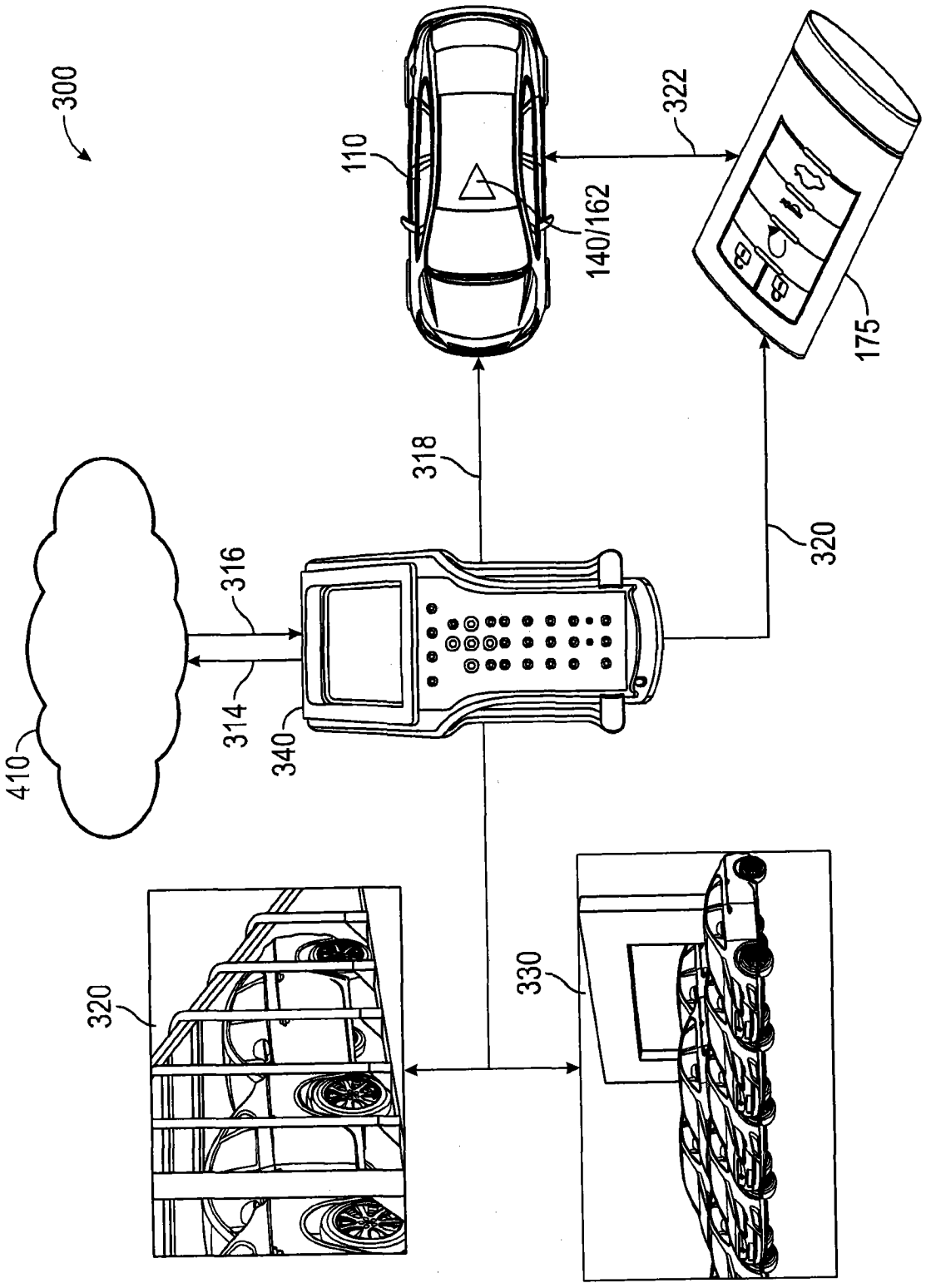


图 3

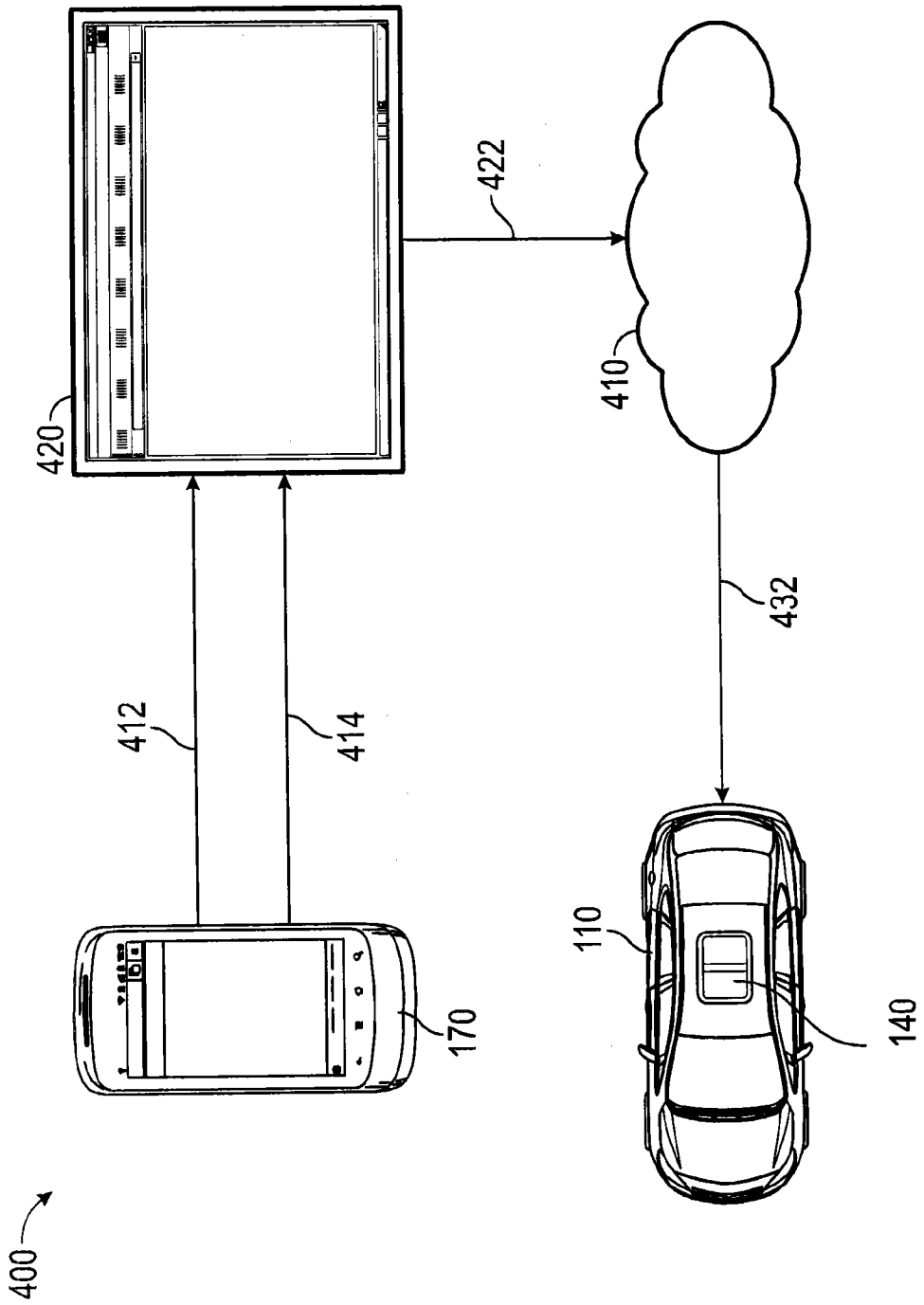


图 4

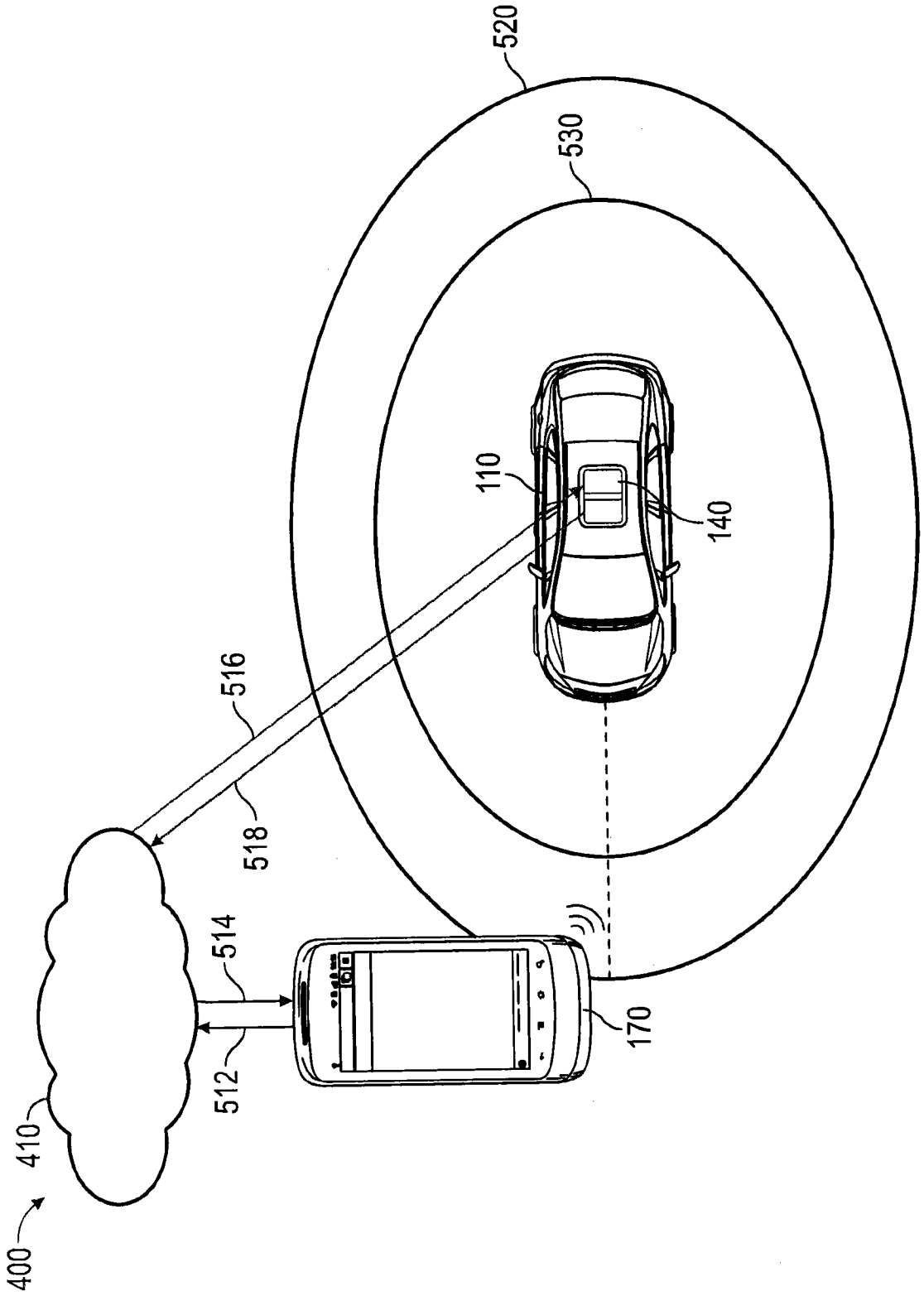


图 5

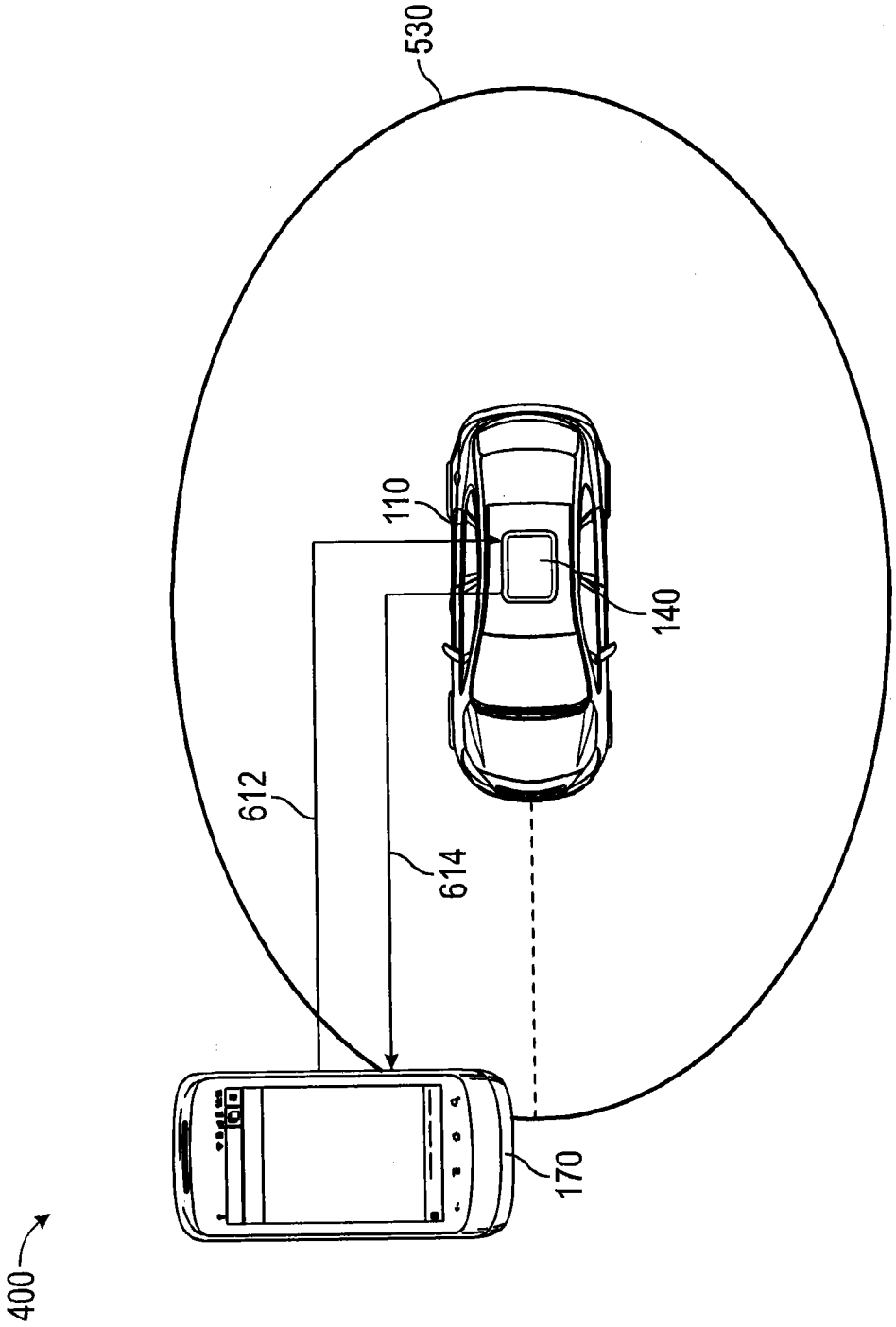


图 6

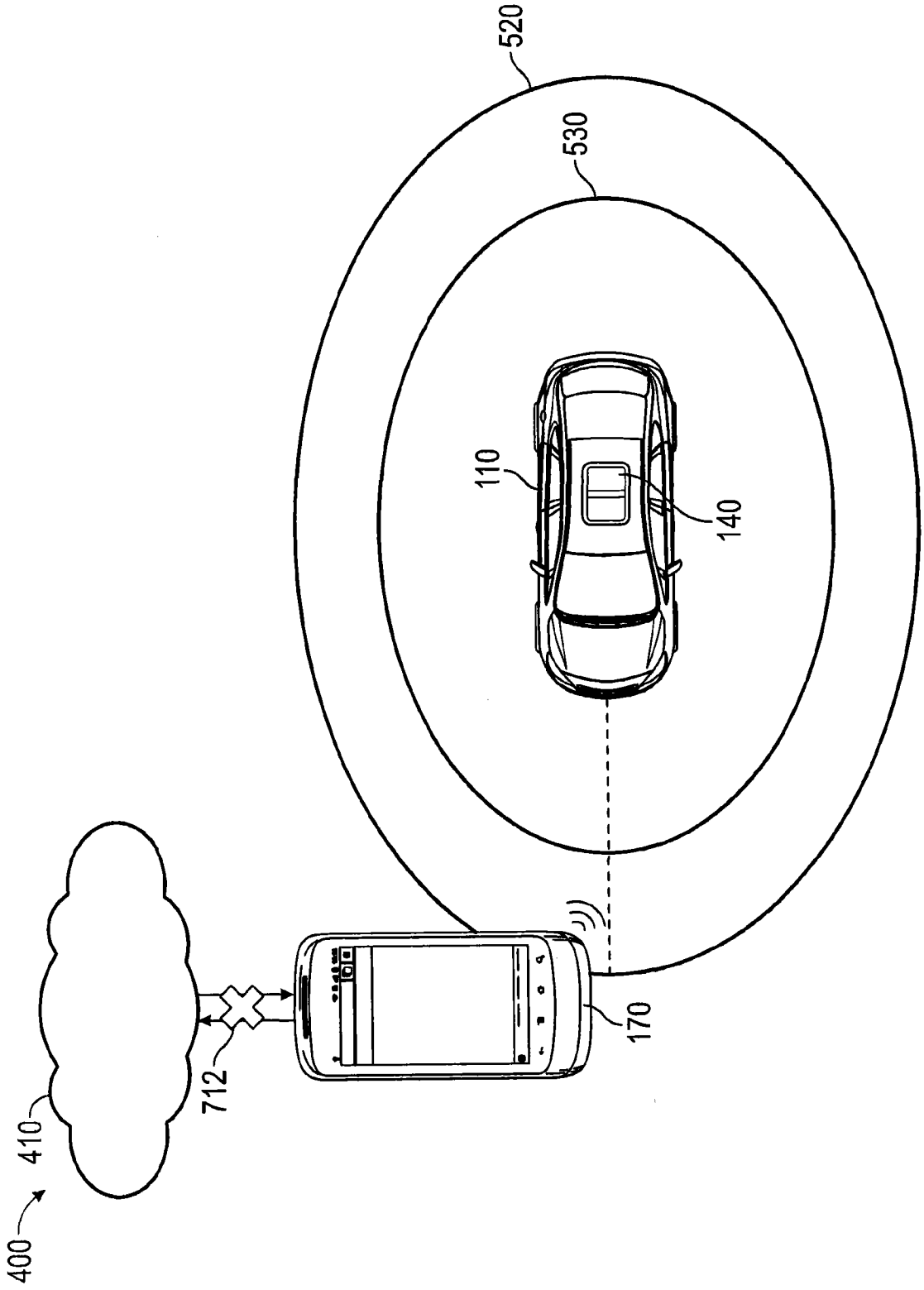


图 7

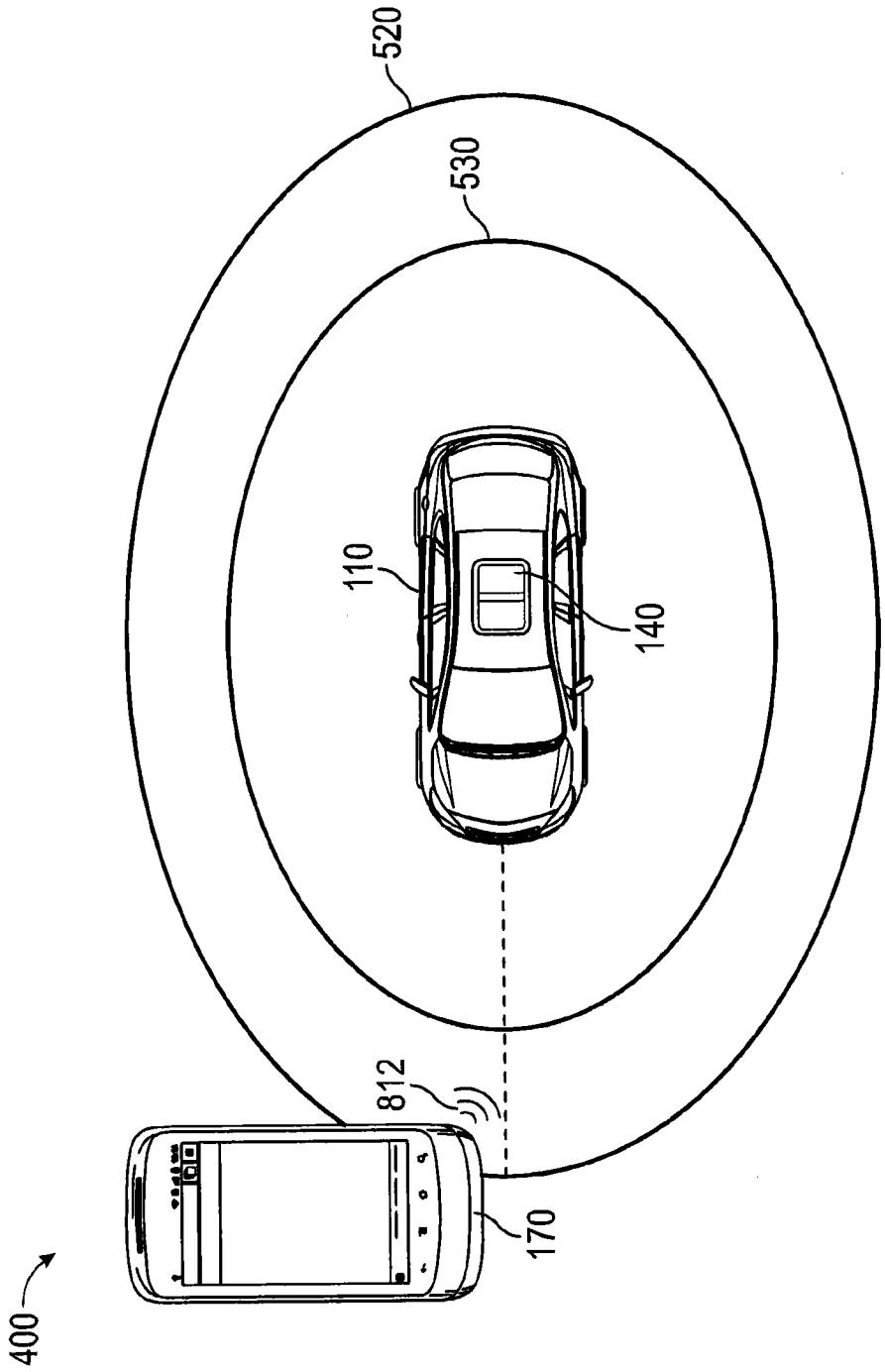


图 8

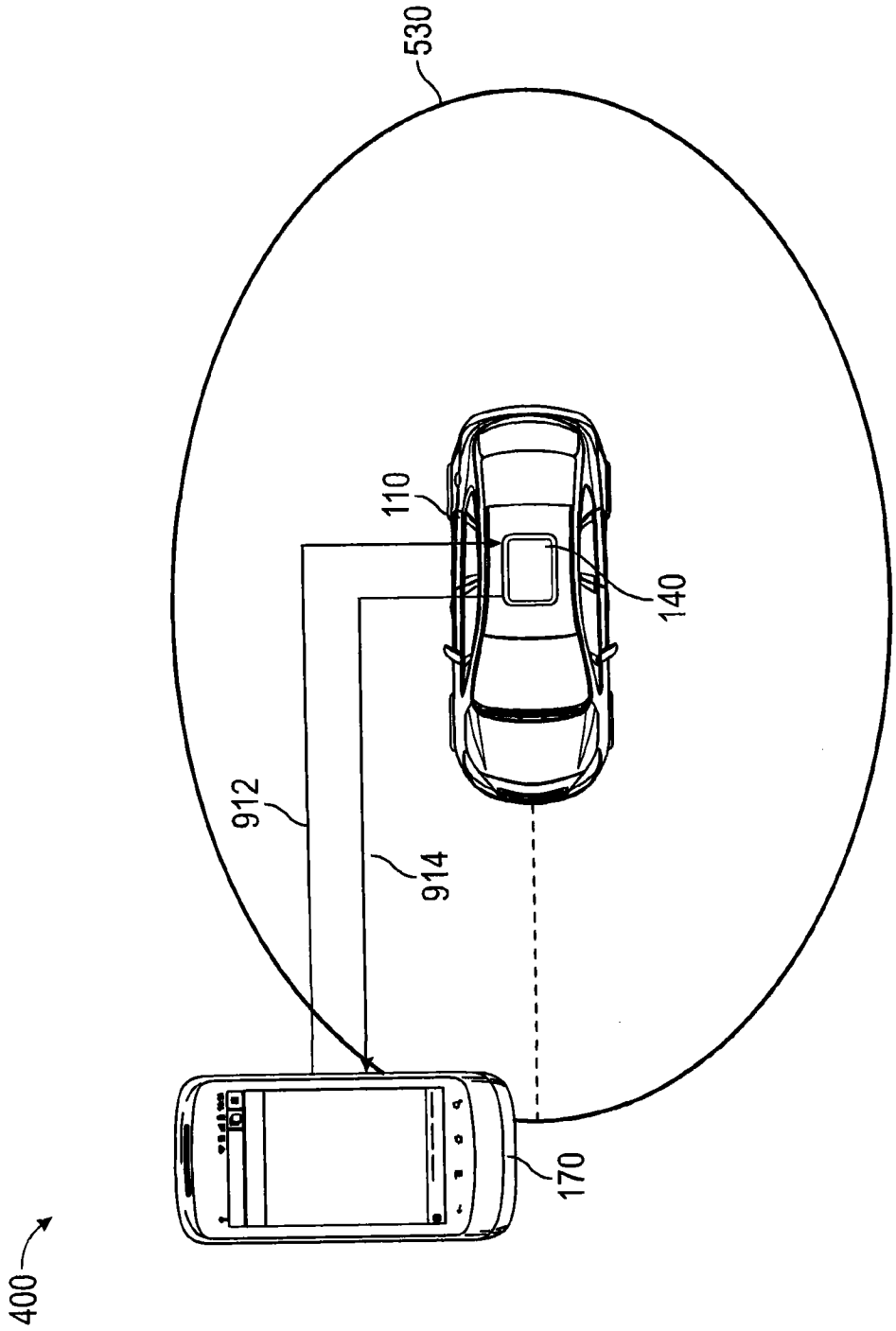


图 9

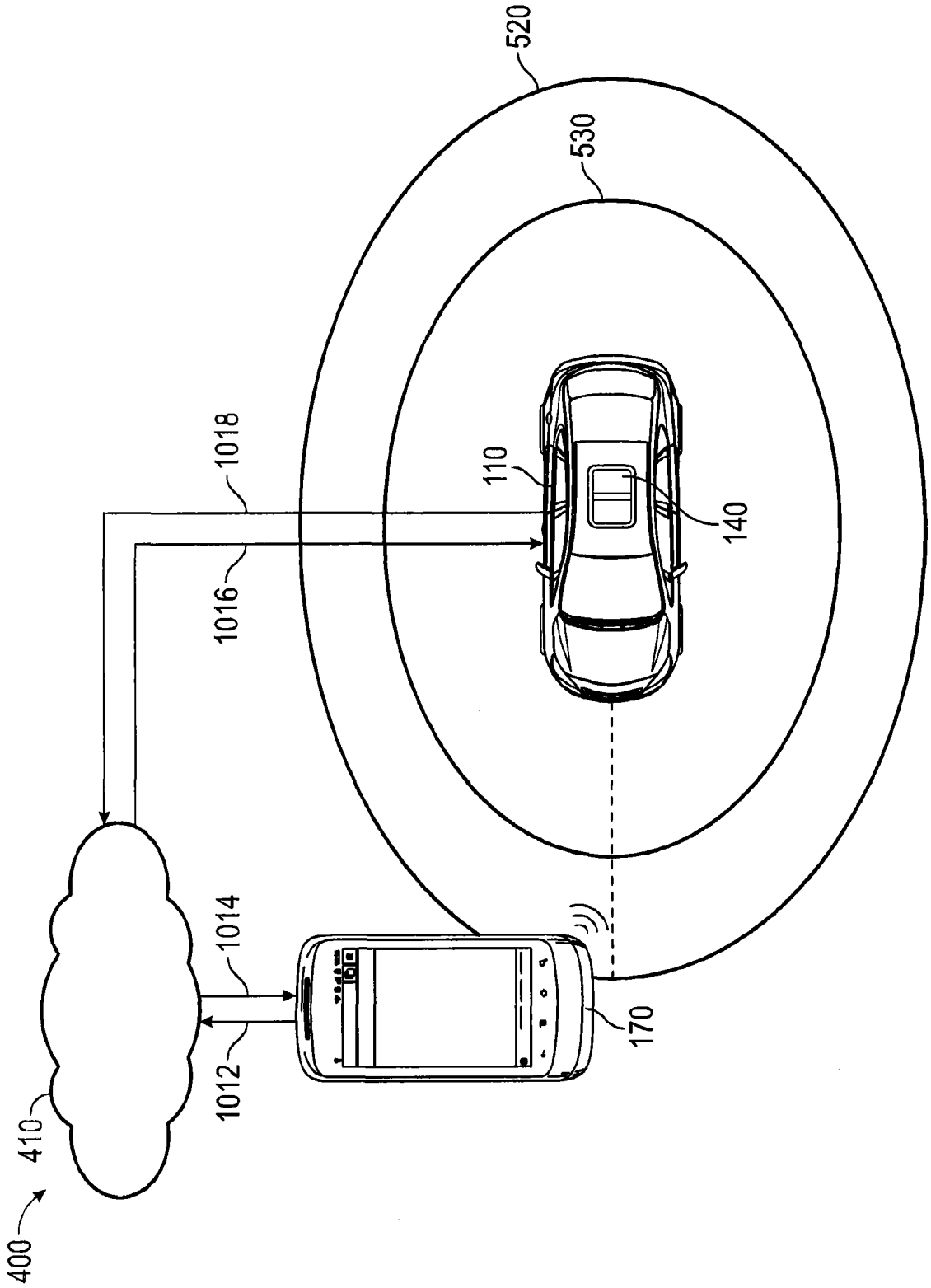


图 10

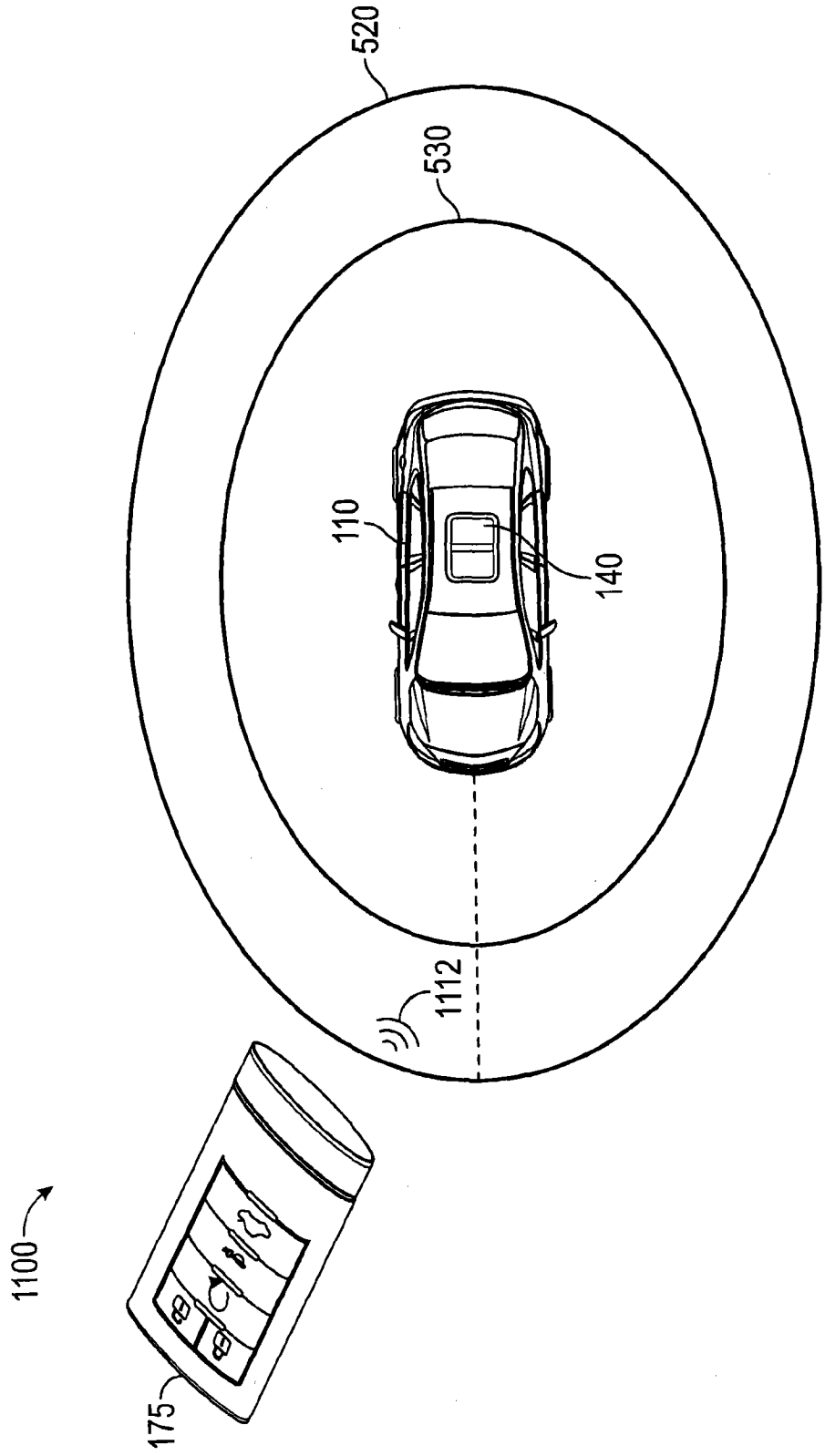


图 11

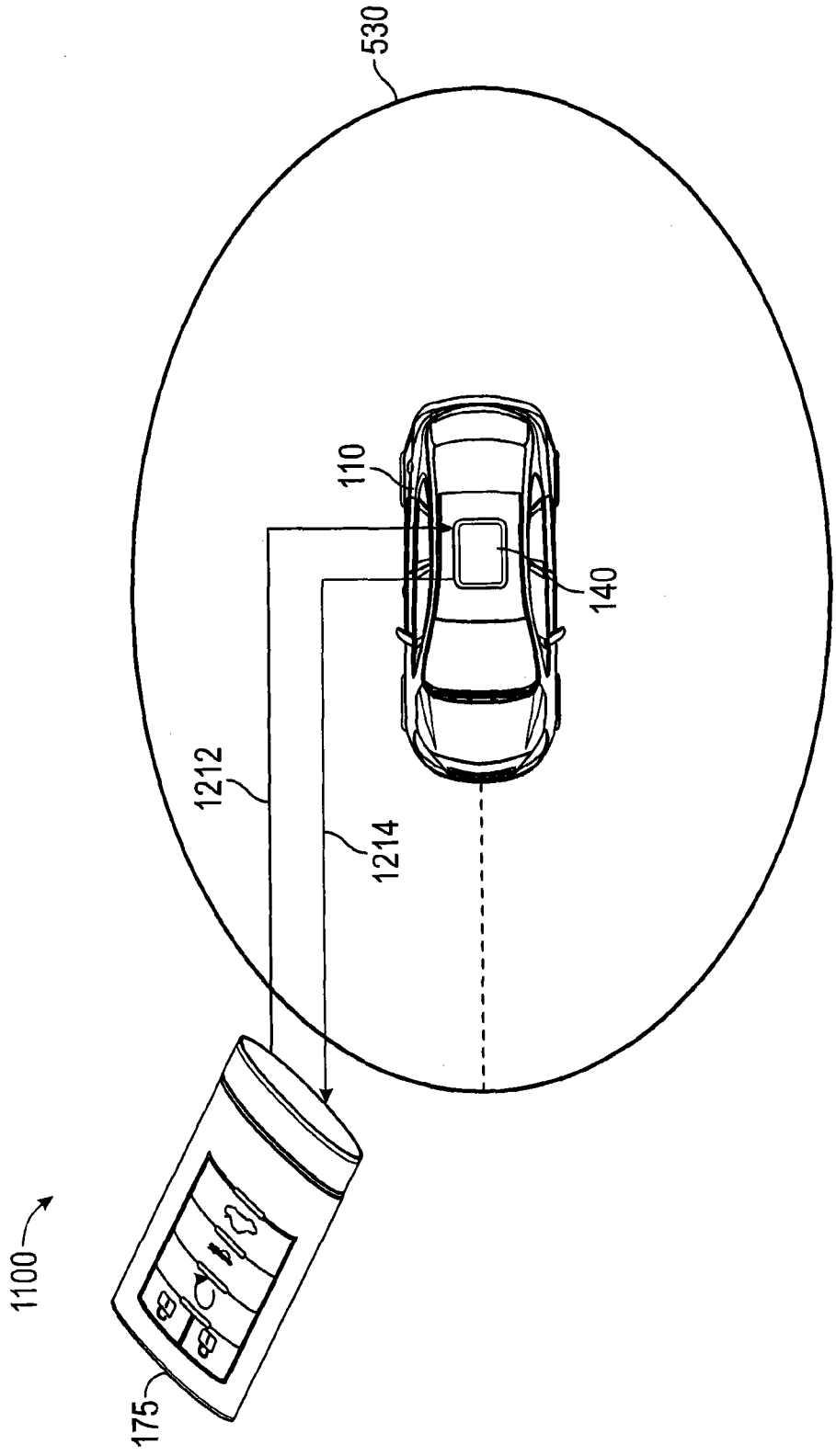


图 12