



(12) 发明专利申请

(10) 申请公布号 CN 105681270 A

(43) 申请公布日 2016. 06. 15

(21) 申请号 201510882536. 5

(51) Int. Cl.

(22) 申请日 2015. 12. 03

H04L 29/06(2006. 01)

H04M 1/725(2006. 01)

(30) 优先权数据

14/559, 582 2014. 12. 03 US

(71) 申请人 福特全球技术公司

地址 美国密歇根州迪尔伯恩市

(72) 发明人 斯特凡·班考夫斯基

米歇尔·瑞曼德·威斯查

大卫·蔡斯·米切尔

朱利叶斯·玛奇维奇

伊丽莎白·哈雷斯

(74) 专利代理机构 北京铭硕知识产权代理有限

公司 11286

代理人 王秀君 鲁恭诚

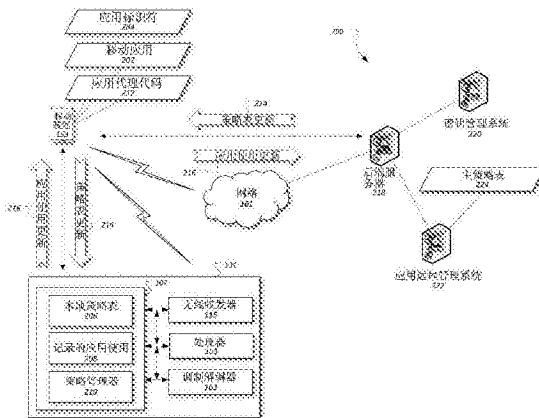
权利要求书2页 说明书11页 附图6页

(54) 发明名称

远程车辆应用许可的控制与监测

(57) 摘要

本公开涉及远程车辆应用许可的控制与监测。一种车辆可识别移动应用的应用标识符，其中，移动应用由与车辆配对的移动装置执行；在本地策略表中查询与所述应用标识符关联的应用许可，所述应用许可限定了哪些用户界面特征、车辆信息元素和车辆功能能由移动应用访问；根据所述应用许可为移动应用提供车辆准入。车辆还可附加地根据与车辆配对的移动装置的移动装置标识符，识别所述应用许可。与车辆配对的移动装置可向车辆发送从服务器接收的策略表更新，所述策略表更新包括本地策略表，本地策略表包括限定了车辆的哪些用户界面特征、信息元素和功能能由移动应用访问；根据所述应用许可执行移动应用。



1. 一种系统，包括：

车辆的处理器，被配置为：

识别移动应用的应用标识符，其中，移动应用由与车辆配对的移动装置执行；

在本地策略表中查询与所述应用标识符关联的应用许可，所述应用许可限定了车辆的哪些用户界面特征、哪些车辆信息元素和哪些车辆功能能由移动应用访问；

根据所述应用许可为移动应用提供车辆准入。

2. 如权利要求1所述的系统，其中，所述处理器还被配置为：附加地根据与车辆配对的移动装置的移动装置标识符，识别所述应用许可。

3. 如权利要求1所述的系统，其中，所述处理器还被配置为：

识别所述本地策略表缺乏与所述应用标识符关联的应用许可；

向所述移动装置发送应用使用更新消息，应用使用更新消息被配置为使所述移动装置向远程服务器请求策略表更新。

4. 如权利要求3所述的系统，其中，应用使用更新消息包含所述本地策略表。

5. 如权利要求4所述的系统，其中，所述本地策略表包括记录的应用使用，记录的应用使用指示车辆的所述用户界面特征、所述信息元素和所述功能的移动应用使用。

6. 如权利要求1所述的系统，其中，本地策略表包括表明所述应用许可有效的地理区域的指示，并且所述处理器被配置为：当车辆处在所述地理区域内时，利用所述应用许可。

7. 如权利要求1所述的系统，其中，所述处理器还被配置为：

捕获与移动应用的使用相关的应用使用；

将所述应用使用记录在所述本地策略表中。

8. 如权利要求1所述的系统，其中，所述处理器还被配置为：响应于移动应用试图利用根据本地策略表该移动应用对其缺乏许可的车辆的功能而终止该移动应用。

9. 如权利要求1所述的系统，其中，所述处理器还被配置为：响应于自本地策略表被更新以来的预定时间段、预定数量的点火周期、车辆里程表距离的预定增量中的至少一项的发生，向所述移动装置发送应用使用更新消息，应用使用更新消息被配置为使所述移动装置向远程服务器请求策略表更新。

10. 一种系统，包括：

与车辆配对的移动装置，被配置为：

向车辆发送从服务器接收的策略表更新，所述策略表更新包括本地策略表，本地策略表包括限定了车辆的哪些用户界面特征、信息元素和功能能由移动应用访问的应用许可；

根据所述应用许可执行移动应用。

11. 如权利要求10所述的系统，其中，所述移动装置还被配置为：

从车辆接收应用使用更新消息；

将应用使用更新消息转发到服务器，以使服务器向所述移动装置发送策略表更新。

12. 如权利要求11所述的系统，其中，应用使用更新消息包含所述本地策略表。

13. 如权利要求10所述的系统，其中，所述本地策略表包括记录的应用使用，记录的应用使用指示车辆的所述用户界面特征、所述信息元素和所述功能的移动应用使用。

14. 如权利要求10所述的系统，其中，从服务器接收的策略表更新包括与地理区域关联的应用许可，所述移动装置被配置为：当车辆处在所述地理区域内时，利用所述应用许可。

15. 一种系统,包括:

应用远程管理服务器,被配置为:

从车辆接收包括本地策略表的应用使用更新消息,所述本地策略表具有能由车辆使用的来自配对的移动装置的应用标识符;

向车辆发送包括应用许可的本地策略表,应用许可限定了车辆的哪些用户界面特征、信息元素和功能能由移动应用访问。

16. 如权利要求15所述的系统,其中,应用远程管理服务器还被配置为:访问主策略表以检索与所述应用标识符关联的应用许可,其中,主策略表包括根据应用标识符编索引的应用许可的当前列表。

17. 如权利要求16所述的系统,其中,应用远程管理服务器还被配置为:

从请求方接收针对包括新应用许可的新应用标识符的请求,新应用许可限定了车辆的哪些用户界面特征、信息元素和功能能由其应用标识符被请求的移动应用所访问;

根据所述新应用标识符,在主策略表中产生包括所述新应用许可的条目。

18. 如权利要求17所述的系统,其中,应用远程管理服务器还被配置为:响应于所述请求,向请求方发送所述新应用标识符。

19. 如权利要求15所述的系统,其中,所述本地策略表包括与多个地理区域关联的应用许可。

20. 如权利要求15所述的系统,其中,应用使用更新消息包含移动应用的版本指示,且本地策略表包括与移动应用的该版本关联的应用许可。

远程车辆应用许可的控制与监测

技术领域

[0001] 本公开的多个方面涉及针对车辆应用的应用许可的控制与监测。

背景技术

[0002] 用于车辆的语音控制系统可以允许第三方应用将语音命令集成到它们的系统中。通过这样做，第三方应用可经由车辆的语音界面来控制。然而，一些第三方应用可能不适于在车辆运动时被使用，或者根据政府法规可能受限制。此外，一些第三方应用可能试图检索对于应用操作不必要的信息，从而导致潜在的用户隐私的担忧。

发明内容

[0003] 在第一说明性实施例中，一种系统包括车辆的处理器，所述处理器被配置为：识别移动应用的应用标识符，其中，移动应用由与车辆配对的移动装置执行；在本地策略表中查询与所述应用标识符关联的应用许可，所述应用许可限定了哪些用户界面特征和车辆信息元素能由移动应用访问；根据检索到的应用许可为移动应用提供车辆准入(vehicle access)。

[0004] 在第二说明性实施例中，一种系统包括与车辆配对的移动装置，所述移动装置被配置为：向车辆发送从服务器接收的策略表更新，所述策略表更新包括本地策略表，本地策略表包括限定了车辆的哪些用户界面特征、信息元素和功能能由移动应用访问的应用许可；根据所述应用许可执行移动应用。

[0005] 在第三说明性实施例中，一种应用远程管理服务器被配置为：从车辆接收包括本地策略表的应用使用更新消息，所述本地策略表具有能由车辆使用的来自配对的移动装置的移动应用的应用标识符；向车辆发送包括应用许可的本地策略表，应用许可限定了车辆的哪些用户界面特征、信息元素和功能能由移动应用访问。

[0006] 根据本发明，一种系统包括：车辆的处理器，被配置为：识别移动应用的应用标识符，其中，移动应用由与车辆配对的移动装置执行；在本地策略表中查询与所述应用标识符关联的应用许可，所述应用许可限定了车辆的哪些用户界面特征、哪些车辆信息元素和哪些车辆功能能由移动应用访问；根据所述应用许可为移动应用提供车辆准入。

附图说明

- [0007] 图1示出了示例性车辆计算系统；
- [0008] 图2示出了示例性应用策略架构；
- [0009] 图3示出了可从其选择同意利用移动应用的车辆计算系统的示例性用户界面；
- [0010] 图4A示出了可从其配置移动应用设置的车辆计算系统的示例性用户界面；
- [0011] 图4B示出了可从其配置移动应用设置的车辆计算系统的示例性用户界面的可选示图；
- [0012] 图5示出了用于对移动应用授予由本地策略表指定的许可的车辆计算系统的示例

性用户界面；

- [0013] 图6示出了应用远程管理系统的示例性用户界面；
- [0014] 图7示出了用于更新主策略表的示例性处理；
- [0015] 图8示出了用于更新车辆的本地策略表的示例性处理；
- [0016] 图9示出了用于使用针对移动应用的许可控制的本地策略表的示例性处理。

具体实施方式

[0017] 根据需要，在此公开本发明的具体实施例；然而，将理解的是，所公开的实施例仅仅是本发明的示例，本发明可以以各种替代形式来实现。附图无需按比例绘制；可夸大或缩小一些特征以示出特定组件的细节。因此，此处所公开的具体结构和功能细节不应被解释为具有限制性，而仅仅作为教导本领域技术人员以多种形式利用本发明的代表性基础。

[0018] 应用远程管理和报告服务器可被配置为向安装到用户的配对移动装置的连接的车辆远程信息处理应用提供远程应用许可控制。这样可允许通过服务器对哪些应用和/或哪些配对的移动装置具有用于访问车辆系统的许可进行远程配置。对于具有许可的那些应用和装置，系统还可提供应用或装置可访问什么性能或车辆功能的配置。系统还可被配置为在允许使用连接的应用之前使车辆确保用户同意以及用户通知。

[0019] 服务器可包括管理界面(例如，安全网站界面)，所述管理界面允许管理的用户输入应用信息并限定系统的功能和其它操作。服务器还可包括允许策略表文件在服务器与车辆之间被传送的连接到车辆的接口。策略表文件可包括：详述车辆中的应用许可的信息和描述车辆应如何请求许可更新以及何时请求许可更新的信息。此外，车辆可被配置为将使用信息写入策略表文件，以返回到服务器来用于报告目的。

[0020] 策略表文件可经由用户的移动装置在服务器和车辆之间被传送，所述用户的移动装置与车辆配对并执行车辆应用。在示例中，所述文件可通过响应于对服务器的全球资源定位符(universal resource locator, URL)的超文本传输协议(HTTP)请求，经由移动装置被传输到车辆，其中，所述请求与车辆应用策略的规定相关联。在示例中，URL可被包括在策略表文件中。策略表文件可通过车辆密钥被加密和签名，以降低中间攻击者拦截数据的可能性。

[0021] 安装到用户的配对移动装置的每个连接的车辆远程信息处理应用可与应用标识符(例如，由车辆制造商或其它标识符管理授权机构(authority)提供的应用标识符)相关联。在示例中，具有对服务器的管理界面的访问权的管理用户可输入应用的信息(包括允许的API和许可)，并可产生针对请求应用的应用标识符。

[0022] 当该应用在具有车辆计算系统的车辆中进行注册时，该应用随应用标识符一起传送。然后，车辆计算系统可针对与提供的应用标识符相关联的应用策略检查本地策略表文件。在某些情况下，系统可支持特定装置的许可，并且车辆计算系统可针对与提供的应用标识符和装置标识符相关联的应用策略检查本地策略表文件。

[0023] 应用策略可指示应用是否被允许在车辆中运行，如果应用被允许在车辆中运行，则应用策略可指示许可被控制的那些车辆功能可由所述应用进行访问。如果策略表文件不包含针对应用标识符的策略许可，则车辆计算系统可向服务器请求策略表文件更新。策略表文件更新请求可包括车辆的当前策略表文件以及未知的应用标识符。策略表文件更新请

求还可包括记录的应用使用,记录的应用使用指示许可被策略表文件控制的车辆功能的移动应用使用。服务器提供的更新的策略表文件可包括更新的策略许可,更新的策略许可包括针对新注册应用的策略。下面详细讨论了连接的应用功能的远程配置和报告的其它方面。

[0024] 图1示出用于车辆131的基于车辆的计算系统(VCS)100的示例方框拓扑图。这种VCS 100的示例为由福特汽车公司制造的SYNC系统。设置有VCS 100的车辆131可包含位于车辆131中的可视前端界面104。如果界面104设置有例如触摸敏感屏幕,则用户还能够与界面104进行交互。在另一说明性实施例中,通过按钮按压、具有自动语音识别和语音合成的口语对话系统来进行交互。作为另一种可能性,与车辆131的交互可隐含于移动装置153或安装到与VCS 100连接的移动装置153的应用中。

[0025] 在图1所示的说明性VCS 100中,处理器103(例如,CPU、应用微处理器、调制解调器处理器等)控制VCS 100的至少一部分操作。设置在车辆131内的处理器103允许对命令和例程进行车载处理。另外,处理器103被连接到非持久性存储器105和持久性存储器107两者。在此说明性实施例中,非持久性存储器105是随机存取存储器(RAM),持久性存储器107是硬盘驱动器(HDD)或闪存。一般而言,持久性(非暂时性)存储器107可包括当计算机或其它装置掉电时保持数据的所有形式的存储器。这些存储器包括但不限于:HDD、致密盘(CD)、数字通用光盘(digital versatile disk,DVD)、磁带、固态驱动器(SSD)、便携式通用串行总线(USB)驱动器和任何其它适当形式的持久性存储器。

[0026] 处理器103还设置有允许用户与处理器103进行交互的若干不同的输入。在该说明性实施例中,麦克风129、辅助输入125(用于输入133)、USB输入123、GPS输入124、前端界面104(可以包括触屏显示器)和无线电收发器115(诸如,蓝牙输入)全部被提供。还设置有输入选择器151,以允许用户在各种输入之间进行切换。针对麦克风129和辅助输入125两者的输入在被传送到处理器103之前,可由转换器127进行模数转换。尽管未被示出,但是与VCS 100进行通信的众多的车辆131组件和辅助组件可使用车辆131的网络(诸如,但不限于控制器局域网(CAN)总线)向VCS 100(或其组件)传送数据并传送来自VCS 100(或其组件)的数据。

[0027] 系统的输出可包括但不限于视觉显示器104以及扬声器113或音频系统输出。扬声器113被连接到放大器111,并通过数模转换器109从处理器103接收其信号。还可分别沿着在119和121示出的双向数据流进行到远程蓝牙装置(诸如,个人导航装置(PND)154)或USB装置(诸如,车辆导航装置160)的输出。

[0028] 在一说明性实施例中,系统100使用无线收发器115与用户的移动装置(ND)153(例如,蜂窝电话、智能电话、个人数字助理(PDA)或具有无线远程网络连接能力的任何其它移动装置)进行通信(117)。移动装置153随后可用于通过例如与蜂窝塔157的通信(155)来与车辆131外部的网络161进行通信(159)。在一些实施例中,蜂窝塔157可以是WiFi接入点。移动装置153与无线收发器115之间的示例性通信由连接114表示。使用配对的移动装置153,数据可以通过利用例如与移动装置153关联的数据计划、话上数据或DTMF音的连接114在处理器103和网络161之间被传送。

[0029] 可通过按钮152或类似的输入来指示移动装置153与无线收发器115进行配对。相应地,处理器103被指示VCS 100的无线收发器115将与移动装置153中的无线收发器(例如,

集成在移动装置153中的蓝牙收发器,未示出)进行配对。

[0030] 另外地或可选地,VCS 100可以包括具有天线118的车载调制解调器163,车载调制解调器163被配置为:在处理器103与网络161之间传送数据(116)。该传送可以通过数据带和/或数据通道被执行。移动装置153随后可用于通过例如与蜂窝塔157的通信(155)来与车辆131外部的网络161进行通信(159)。在一些实施例中,调制解调器163可与蜂窝塔157建立通信(120),以与网络161进行通信。作为非限制性示例,调制解调器163可以是USB蜂窝调制解调器163,并且通信120可以通过蜂窝通信协议来进行。

[0031] 在一说明性实施例中,处理器103设置有包括与调制解调器应用软件进行通信的应用程序编程接口(API)的操作系统。调制解调器应用软件可访问无线收发器115上的嵌入式模块或固件,以完成与远程无线收发器(诸如,在移动装置153中发现的)的无线通信。蓝牙是IEEE 802PAN(个域网)协议的子集。IEEE 802LAN(局域网)协议包括WiFi,并与IEEE 802PAN具有相当多的交叉功能。两者都适合于车辆131内的无线通信。可在这一范围使用的另一通信方式是自由空间光通信(诸如,IrDA)和非标准化消费者红外(IR)协议。

[0032] 在另一实施例中,移动装置153包括用于语音频带或宽带数据通信的调制解调器。在话上数据的实施例中,当移动装置153的所有者可在数据被传送的同时通过移动装置153说话时,可实施被称为频分复用的技术。在其它时间,当所有者没有在使用装置时,数据传送可使用整个带宽(在一示例中是300赫兹(Hz)至3.4千赫(kHz))。尽管频分复用对于车辆131与互联网之间的模拟蜂窝通信而言会是常见的并仍在被使用,但其已经很大程度上被用于数字蜂窝通信的码分多址(CDMA)、时分多址(TDMA)、空分多址(SDMA)的混合体所替代。这些都是ITU IMT-2000(3G)兼容的标准,为静止或行走的用户提供高达2兆比特每秒(mbs)的数据速率,并为在移动的车辆131中的用户提供高达385千比特每秒(kbs)的数据速率。3G标准现在正被IMT-Advanced(4G)所替代,所述IMT-Advanced(4G)为在车辆131中的用户提供100mbps的数据速率并为静止的用户提供1千兆比特每秒(gbs)的数据速率。如果用户具有与移动装置153关联的数据计划,则所述数据计划可允许宽带传输且系统可使用宽得多的带宽(加速数据传送)。在另一实施例中,移动装置153被安装至车辆131的蜂窝通信装置(未示出)所替代。在又一实施例中,移动装置153可以是能够通过例如(而非限制)802.11g网络(即WiFi)或WiMax网络进行通信的无线局域网(LAN)装置。

[0033] 在一实施例中,传入数据可经由话上数据或数据计划穿过移动装置153,穿过车载蓝牙收发器,并进入车辆131的内部处理器103。例如,在某些临时数据的情况下,数据可被存储在HDD或其它持久性存储器107上,直至不再需要所述数据时为止。

[0034] 可与车辆131进行接口连接的其它的源包括:具有例如USB连接156和/或天线158的PND 154、具有USB 162或其它连接的车辆导航装置160、车载GPS装置124、或具有与网络161连接的能力的远程导航系统(未示出)。USB是一类串行联网协议中的一种。IEEE 1394(火线TM(苹果)、i.LINKTM(索尼)和LynxTM(德州仪器))、EIA(电子工业协会)串行协议、IEEE 1284(Centronics端口)、S/PDIF(索尼/飞利浦数字互连格式)和USB-IF(USB开发者论坛)形成了装置-装置串行标准的骨干。多数协议可针对电通信或光通信来实施。

[0035] 此外,处理器103可与各种其它的辅助装置165进行通信。这些辅助装置165可通过无线连接167或有线连接169来连接。辅助装置165可包括但不限于:个人媒体播放器、无线保健装置、便携式计算机等。

[0036] 此外或可选地,可使用例如WiFi(IEEE 803.11)收发器171将处理器103连接到基于车辆的无线路由器173。这可允许处理器103在局域路由器173的范围中连接到远程网络。

[0037] 除了由位于车辆131中的VCS 100执行示例性处理之外,在某些实施例中,还可由与VCS 100通信的计算系统来执行示例性处理。这样的系统可以包括但不限于:无线装置(例如,但不限于移动电话)或通过无线装置连接的远程计算系统(例如,但不限于服务器)。这样的系统可被统称为与车辆关联的计算系统(VACS)。在某些实施例中,VACS的特定组件可根据系统的特定实施而执行处理的特定部分。通过示例而并非限制的方式,如果处理具有与配对的无线装置发送或者接收信息的步骤,则很可能无线装置不执行该处理,这是因为无线装置不会与自身进行信息的“发送和接收”。本领域的普通技术人员将理解何时不适合对给定解决方案应用特定的VACS。在所有解决方案中,预期至少位于车辆内的车辆计算系统(VCS)自身能够执行示例性处理。

[0038] 在此讨论的每个说明性实施例中,示出了可由计算系统执行的处理的示例性非限制示例。针对每个处理,为了执行处理的限制性目的,执行处理的计算系统被配置为用于执行处理的专用处理器103是可行的。所有处理无需被全部执行,而应被理解为可被执行以实现本发明的要素的处理类型的示例。可如期望地添加附加步骤或将附加步骤从示例性处理中去除。

[0039] 图2示出了示例性应用策略架构200。如示出的,架构200包括具有策略管理器210的车辆131,车辆131经由网络161与后端服务器218通信。策略管理器210可被配置为维护本地策略表206和记录的应用使用208。移动装置153可执行移动应用202,移动应用202与应用标识符204相关联并包括利于通过网络161与后端服务器218进行通信的应用代理代码212。后端服务器218可被配置为提供对密钥管理系统220和应用远程管理系统222的访问,应用远程管理系统222维护主策略表224。如下面详细说明的,应用远程管理系统222可被配置为经由移动装置153的应用代理代码212向车辆131提供策略表更新214。

[0040] 移动应用202可以是安装到移动装置153的应用,以供车辆131的VCS 100使用。在示例中,移动应用202可通过将控制移动应用202的功能的语音命令与VCS 100的语音命令界面集成,来给VCS 100添加功能。移动应用202还可被配置为利用VCS 100的用户界面特征,诸如,视觉显示器104或扬声器113,以向车辆乘员提供信息。

[0041] 应用标识符204可以是分配给移动应用202的唯一号码或字母数字字符串。在某些情况下,应用标识符204可以是随机产生的值。在其它情况下,应用标识符204可通过被配置为管理应用标识符204的授权机构来分配给移动应用202。

[0042] 本地策略表206可被配置为将详述应用许可的密钥信息存储在车辆131中。因此,本地策略表206可限定VCS 100和给定的移动应用202之间允许的交互类型。在示例中,本地策略表206可包括根据被分配给移动应用202的应用标识符204而键入(key)的针对移动应用202的许可信息。许可信息可包括:例如,被认为允许由移动应用202使用的API和车辆131系统的列表。作为一些特定示例,本地策略表206可包括关于被允许由移动应用202访问的VCS 100的远程过程调用的许可信息,诸如,以用于流传输音频或检索车辆131的当前GPS位置的许可信息。作为一些其它示例,本地策略表206可包括关于移动应用202是否具有执行情境切换和从另一应用转移注意力的许可信息,例如用于中断无线电来提供消息。作为另一示例,本地策略表206可包括关于移动应用202是否可以执行VCS 100上的脚本的许可信

息。作为另一示例，本地策略表206可包括关于以下内容的许可信息：当车辆131停车或静止时车辆131的哪些功能可被利用，当车辆131运动时哪些功能可被使用。本地策略表206还可包括：用于配置车辆131如何请求以及何时请求对本地策略表206的更新的信息，以及关于如何联系更新的本地策略表206的源(例如，后端服务器218的URL或其它地址)的信息。

[0043] 在一些示例中，本地策略表206可包括针对不同的移动装置153而键入的不同的应用许可集。作为一种可能性，本地策略表206可包括针对移动装置标识符(例如，移动装置号码、配对信息等)键入的应用许可。作为另一种可能性，车辆131可保存针对与VCS 100配对的移动装置153的每个移动装置标识符的不同的本地策略表206。作为另一种可能性，针对移动装置标识符而键入的许可可包括供移动装置153使用而不考虑应用的许可。在示例中，本地策略表206可包括供电话远程处理功能使用的许可，诸如，使用显示器104或另一车辆131显示器显示来自用户的移动装置153的视频或其它内容的能力。

[0044] 记录的应用使用208可包括车辆131系统使用和API的记录使用，或者其许可针对移动应用202而被控制的车辆131的其它功能。因此，记录的应用使用208可包括收集到的关于用户如何在车辆131中使用移动应用202的使用数据。与本地策略表206类似，记录的应用使用208可根据被分配给移动应用202的应用标识符204而被键入。在一些示例中，记录的应用使用208可被包括在本地策略表206中，而在其它示例中，记录的应用使用208可与本地策略表206分开被保存。作为记录的信息的一些特定示例，记录的应用使用208可包括移动应用202的运行尝试、移动应用202经历的错误(例如，许可被拒绝错误、诸如由于编程错误而产生的错误的非预期错误等)、记录的HMI使用信息(例如，方向盘控制使用、语音命令使用等)、移动应用202通过车辆131的HMI提供音频的收听时间。

[0045] 策略管理器210可被配置为管理针对车辆131的VCS 100的移动应用202许可。在示例中，策略管理器210可维护本地策略表206。当移动应用202被启动或激活时，策略管理器210可基于本地策略表206识别与移动应用202关联的许可。此外，当移动应用202与VCS 100进行交互时，策略管理器210可将车辆131系统和车辆API的移动应用202使用记录在记录的应用使用208。

[0046] VCS 100的策略管理器210还可被配置为管理与后端服务器218的通信。就策略管理器210和后端服务器218之间的请求和响应而言，策略管理器210可被配置为启动与后端服务器218的通信。在示例中，策略管理器210可向后端服务器218提供消息以通知后端服务器218车辆131启动并且正在收听信息。在一些情况下，后端服务器218可将未经请求的消息提交给特定车辆131，并将该消息推送到云。然而，直至VCS 100连接后端服务器218并向后端服务器218请求该消息，所述消息才可被传送到车辆131。

[0047] 策略管理器210可被配置为请求后端服务器218向车辆131提供对本地策略表206的更新。例如，如果具有未存在于本地策略表206中的应用标识符204的移动应用202试图与车辆的VCS 100集成，则策略管理器210可请求对本地策略表206的更新。

[0048] 策略管理器210还可被配置为向后端服务器218提供记录的应用使用208，以用于远程查阅和处理。为此，策略管理器210可提供应用使用更新216消息，应用使用更新216消息包括由车辆131存储的记录的应用使用208信息。考虑到移动应用202的明显目的，这样可允许系统核查移动应用202正在适当地利用API和车辆131的系统。例如，导航移动应用202向车辆131周期性请求速度信息可能是合理的，但是互联网无线电移动应用202这样做可能

是不合理的。

[0049] 应用代理代码212可被配置为帮助策略管理器210与后端服务器218的通信。在示例中,应用代理代码212可包括代码库(library)或其它代码模块,代码库(library)或其它代码模块被编译或链接到移动应用202并提供允许策略管理器210通过移动应用202与后端服务器218通信的功能。策略管理器210可相应地利用应用代理代码212来经由后端服务器218请求策略表更新214,向后端服务器218提供应用使用更新216,并从后端服务器218接收策略表更新214。策略表更新214可包括:例如,新的本地策略表206,用于替换当前由策略管理器210存储的本地策略表206;或对现存的本地策略表206的更新,用于增加本地策略表206的当前条目。应用代理代码212还可包括可有利于与后端服务器218通信的其它功能,诸如,用于在VCS 100和后端服务器218之间传输加密消息的能力。

[0050] 车辆131的无线收发器115可连接到配对的移动装置153(例如,经由蓝牙连接、经由USB连接等),使得移动装置153的通信功能可被用于允许VCS 100经由网络161与后端服务器218进行通信。网络161可相应地经由移动装置153的蜂窝数据计划被移动装置153利用,例如,用于向VCS 100提供基于TCP/IP的通信功能。附加地或可选地,VCS 100可包括车载调制解调器163,车载调制解调器163被配置为在处理器103和网络161之间传送数据(116)。经由网络161指向车辆131的消息可在云中排队,直到与车辆131的连接可被建立或所述消息终止为止。在示例中,排队以及消息终止功能可经由后端服务器218来实现。网络161消息排队功能还可用作防御服务器拒绝服务攻击的第一条防线。

[0051] 后端服务器218可被配置为作为网络161和内部应用管理基础设施之间的网关进行操作。在示例中,内部应用管理基础设施可由车辆131的制造商管理,而在另一示例中,内部应用管理基础设施可由诸如应用认证实体的另一方来管理。后端服务器218可被配置为作为防火墙来执行,以在后端服务器218后方的系统(诸如,密钥管理服务器220和应用远程管理系统222)与内部应用管理基础设施外部的车辆131之间验证、转换和传输消息。

[0052] 密钥管理服务器220可被配置为对来往于后端服务器218的消息提供安全传送服务。例如,密钥管理服务器220可对传入的消息进行认证、解密和验证,将解密并验证后的消息转发到合适的内部目的地,提供出站消息安全性以对传出数据进行加密和签名,并确保当传出消息被预期的车辆131的VCS 100接收时传出消息通过了安全检查。在示例中,密钥管理服务器220可通过将消息标识符分配给传出消息并核查合适的消息标识符被包括在传入消息中,来针对重放攻击验证消息。

[0053] 当消息或请求被后端服务器218接收时,后端服务器218将消息转发到密钥管理系统220,在密钥管理系统220中,消息被认证、解密和验证。如果这些操作成功了,则后端服务器218可在消息中检索有效负荷(payload),并根据由消息标识的服务类型将消息传送到合适的应用。在示例中,策略表消息(例如,对策略表更新214的请求)可与指示消息将被传送到应用远程管理系统222的服务类型相关联。

[0054] 应用远程管理系统222可被配置为从车辆131接收应用使用更新216,并向车辆131提供策略表更新214。在示例中,应用远程管理系统222可接收在应用使用更新216消息中的车辆131的本地策略表206的快照(snapshot)。本地策略表206可包括针对已与车辆131交互的移动应用202的记录的应用使用208。应用远程管理系统222可将来自接收到的本地策略表206的记录的应用使用208进行存档,并通过向车辆131提供策略表更新214来更新由车

辆131存储的应用许可。策略表更新214可基于在最近的移动应用202许可的主策略表224中由应用远程管理系统222维护的最新信息。在示例中，移动应用202的每个版本(例如，版本2相对于版本2.1)可与其自身的在主策略表224中的许可信息相关联。应注意，在策略表更新214中的提供给车辆131的主策略表224信息可能缺乏任何的记录的应用使用208数据，但可包括针对任何移动应用202的最新许可，其中，所述移动应用202根据应用使用更新216的接收到的本地策略表206而被识别为被车辆131使用。

[0055] 应用远程管理系统222还可被配置为提供接口，主策略表224可通过所述接口被维护。在示例中，主策略表224可根据用户输入而被更新，以借由移动应用202的基础来设置移动应用202上的策略，其中，所述用户输入从考虑第三方请求、客户反馈以及其它因素的连接的应用管理器被接收。

[0056] 图3示出了可从其选择同意利用移动应用202的VCS 100的示例性用户界面300。在示例中，用户界面300可在VCS 100的显示器104中显示。用户界面300可包括消息提示302，消息提示302被配置为接收用户同意以经由VCS 100利用移动应用202的功能。作为一些示例，当用户首先将移动装置153与VCS 100进行配对时，或者，当车辆131确定用户试图使用移动应用202但尚未接收到同意时，消息提示302可被提供。

[0057] 消息提示302可包括应用同意文本304，应用同意文本304向用户指示消息提示302正在请求用户启用移动应用202的功能。消息提示302还可经由VCS 100的HMI的音频功能(例如，经由扬声器113)通过语音响应来提供关于所述请求的信息。语音信息可指示：为了利用VCS 100使用移动应用202，VCS 100将使用用户的移动装置153的数据计划来与后端服务器218进行通信(例如，至少每月一次)，并且该标准数据速率可应用于所述通信。语音信息还可指示出VCS 100可向后端服务器218发送标识车辆131的信息，诸如，VIN或VCS 100的模块号。

[0058] 消息提示302可通过用户讲出语音命令(例如，“是”)或通过用户选择消息提示302的同意控制306来接收用户同意。消息提示302还可通过用户讲出语音命令(例如，“不是”)或通过用户选择消息提示302的不同意控制308来接收不同意的指示。消息提示302还包括重复控制310，当重复控制310被选择时，重复控制310被配置为使消息提示302重复用于解释消息提示302的语音信息。

[0059] 消息提示302还包括帮助控制312，当帮助控制312被选择时，帮助控制312被配置为向用户提供关于该同意的附加信息。在示例中，所述附加信息可包括：更新是关于电子邮件的大小的，策略表更新214的产生依赖于车辆131的使用以及何时在移动装置153上发现新的移动应用202。所述附加信息还可指示：用户可在VCS 100的移动应用202的设置内开启和关闭移动应用202的支持。

[0060] 图4A示出了可从其配置移动应用202的设置的VCS 100的示例性用户界面400-A。在示例中，用户界面400-A可响应于用户选择而被显示在VCS 100的显示器104中，以配置VCS 100的移动应用202的设置。用户界面400-A可包括标题标签402，以向用户指示用户界面400-A是用于移动应用202的配置的。

[0061] 用户界面400-A还可包括列表控制404，列表控制404被配置为显示指示用户界面400-A的可用配置选项的条目406。列表控制404可操作为菜单，使得用户界面400-A的用户能够在列表控制404的整个列表条目中滚动(例如，使用向上和向下箭头按钮以及选择按钮

来调用所选择的菜单项408)。在某些情况下,列表控制404可被显示在触屏显示器104上,使得用户能够触摸列表控制404来选择和调用菜单项。

[0062] 如示出的,连接的应用的列表控制404包括:条目406-A,用于指示本地策略表206是否是最新的;条目406-B,当被选择时允许用户请求更新的本地策略表206;条目406-C,当被选择时允许用户禁用本地策略表206的更新;条目406-D,当被选择时,允许用户查看其它的移动应用202的设置。

[0063] 图4B示出了可从其配置移动应用202的设置的VCS 100的示例性用户界面400-B的可选示图。在说明性用户界面400-B中,用户先前已禁用了本地策略表206的更新(例如,由于从用户界面400-A选择了条目406-C)。由于本地策略表206的更新被禁用了,列表控制404的其它功能也相应地被禁用。如果用户希望启用本地策略表206的更新,用户可从用户界面400-B选择条目406-C,然后例如可选择条目406-B来检索更新的本地策略表206。

[0064] 图5示出了用于对移动应用202授予由本地策略表206指定的许可的VCS 100的示例性用户界面500。用户界面500可包括应用消息提示502,应用消息提示502被配置为指示用户界面500正在请求授予对调用的移动应用202的许可。在示例中,当在策略表更新214从后端服务器218被接收之后,用户第一次开启移动应用202时,用户界面500可被显示在VCS 100的显示器104中。

[0065] 应用消息提示502可包括应用同意文本304,应用同意文本304向用户指示:应用消息提示502正在请求用户启用在本地策略表206中的针对移动应用202指定的许可。应用消息提示502还可经由VCS 100的HMI的音频功能(例如,经由扬声器113)通过语音响应来提供关于所述请求的信息。所述语音信息可(例如,通过移动应用202的名称)识别请求许可的移动应用202和根据需要而由本地策略表206指示的许可(例如,基本车辆信息、车辆131的位置和速度等)。所述语音信息还可指示:通过对移动应用202授予请求的许可,用户接受承担对于由于数据变为可用而导致失去隐私的责任。

[0066] 应用消息提示502可通过用户讲出语音命令(例如,“是”)或通过用户选择应用消息提示502的同意控制506来接收用户同意。应用消息提示502还可通过用户讲出语音命令(例如,“不是”)或通过用户选择应用消息提示502的不同意控制508来接收不同意的指示。应用消息提示502还可包括帮助控制510,当帮助控制510被选择时,帮助控制510被配置为向用户提供关于授予许可的附加信息。在示例中,所述附加信息可指示:用户调整在VCS 100的移动应用202的设置中的针对移动应用202的许可。

[0067] 图6示出了应用远程管理系统222的示例性用户界面600。在示例中,用户界面600可通过与应用远程管理系统222通信的终端(例如,通过与应用远程管理系统222的网站服务器通信的网站浏览器)来进行显示。用户界面600还可包括用于查看和编辑最近的移动应用202许可的主策略表224的信息。

[0068] 用户界面600可包括标题602,标题602指示用户界面600是用于应用远程管理系统222的。用户界面600还可包括控制,所述控制被配置为允许管理用户输入应用信息并限定系统100的功能和其它操作。例如,用户界面600可包括策略表查看控制604,策略表查看控制604被配置为显示用于用户查看和编辑的主策略表224的条目。每个条目可表示针对移动应用202(或者针对移动应用202的版本)的许可。针对每个条目,策略表查看控制604可包括以下信息,诸如:策略表条目的标识符,关联的移动应用202的供应商,关联的移动应用202

的应用标识符204,所述移动应用202的名称,所述移动应用202的说明,移动应用202的信息是否用于移动应用202的生产或开发版本,可应用移动应用202的许可的一个或更多个区域,以及关于何种API、RPC(远程过程调用)和车辆131系统可由移动应用202访问的许可信息。作为一些可能性,这些许可可包括:移动应用202是否具有用于提供高于其它移动应用202的信息消息、移动应用202是否能够在处于后台时或仅作为前台应用时访问HMI功能、以及移动应用202能够访问的一个或更多个信息集的列表(例如,车辆131的位置、关于驾驶员对车辆131的踏板输入的信息等)。

[0069] 用户界面600还可包括一个或更多个查看控制606,查看控制606被配置为允许用户对在策略表查看控制604中列出的许可条目进行分类、查看和过滤。用户界面600还可包括创建新控制608,当创建新控制608被选择时,创建新控制608允许用户向主策略表224添加新条目。作为另一示例,用户界面600还可包括刷新数据控制610,当刷新数据控制610被选择时,刷新数据控制610允许用户从应用远程管理系统222接收主策略表224的更新版本(例如,如果另一用户已编辑过则接收改变)。作为另一示例,用户界面600可包括输出控制612,当输出控制612被选择时,输出控制612允许用户输出来自应用远程管理系统222的主策略表224信息(例如,经由用于下载的文本文件或电子表格文件)。

[0070] 图7示出了用于更新主策略表224的示例性处理700。处理700可由例如应用远程管理系统222的用户来执行。

[0071] 在操作702,应用远程管理系统222接收针对移动应用202的应用标识符204的请求。所述请求还可包括附加信息,诸如,被请求由移动应用202使用的许可、移动应用202应处于的类别、移动应用202的供应商。

[0072] 在操作704,应用远程管理系统222响应于所述请求在主策略表224中产生条目。产生的条目可指示请求的许可以及其它信息,并且还可指定应用标识符224与移动应用202相关联。在一些示例中,应用标识符204可以是随机或递增式产生的值(例如,下一可用的号码或序列标识符)。

[0073] 在操作706,应用远程管理系统222向请求方发送应用标识符204。例如,应用远程管理系统222可产生与在操作702接收到的信息关联的应用标识符204,并可向应用开发方提供产生的应用标识符204以用于与移动应用202相关联。在操作706之后,处理700结束。

[0074] 图8示出了用于更新车辆131的本地策略表206的示例性处理800。处理800例如可由VCS 100的策略管理器210执行。

[0075] 在操作802,VCS 100确定对本地策略表206的更新是否被指示。在示例中,由于VCS 100识别出在本地策略表206中没有列出标识移动应用202app(应用)的应用标识符204,因此,VCS 100可确定本地策略表206应被更新。在另一示例中,当用户开启需要本地策略表206更新的移动应用202并且策略管理器210尚未越过(over)初始的请求序列接收到更新的本地策略表206时,VCS 100可确定本地策略表206应被更新。在另一示例中,VCS 100可确定本地策略表206应在以下状况中的一个或更多个之后被更新:“N”个点火周期(例如,其中,“N”在本地策略表206中被限定),在车辆131的里程表上已记录了“M”千米(例如,其中,“M”在本地策略表206中被限定),经过了时间“O”(例如,其中,“O”在本地策略表206中被限定)。

[0076] 在操作804,VCS 100向应用远程管理系统222发送应用使用更新216消息。应用使用更新216可包括当前的本地策略表206,并可根据本地策略表206中包括的地址信息(例

如,更新服务器URL)被发送到某地址。应用使用更新216或当前的本地策略表206还可包括记录的应用使用208。应用使用更新216可经由后端服务器218被发送到应用远程管理系统222,并可与指示消息将被传送到应用远程管理系统222的服务类型相关联。

[0077] 在操作806,VCS 100从后端服务器218接收策略表更新214的消息。策略表更新214可包括用于扩充或替换车辆131的当前的本地策略表206的新的本地策略表206。更新的本地策略表206可包括针对移动应用202的最近的应用许可,所述许可被包括在被发送到后端服务器的本地策略表206中。然而,新的本地策略表206可不包括任何记录的应用使用208。

[0078] 在操作808,VCS 100应用更新的本地策略表206。相应地,可使得更新的应用许可能够被使用。在操作808之后,处理800返回至操作802。

[0079] 图9示出了用于使用针对移动应用202的许可控制的本地策略表206的示例性处理900。与处理800类似,处理900可由例如VCS 100的策略管理器210执行。

[0080] 在操作902,VCS 100识别调用的移动应用202。例如,VCS 100可接收在移动装置153上可用的移动应用202的应用标识符204的列表。作为另一示例,VCS 100可接收在移动装置153上的移动应用202的启动指示。

[0081] 在操作904,VCS 100在本地策略表206中检索针对移动应用202的许可。在示例中,VCS 100可在本地策略表206中查询与移动应用202的应用标识符204关联的应用许可。在另一示例中,VCS 100可在本地策略表206中查询与执行移动应用202的配对移动装置153以及移动应用202的应用标识符204关联的应用许可。在某些情况下,如果用户尚未同意移动应用202的使用,则VCS 100可显示用于授予使用移动应用202的许可的用户界面,诸如以上描述的用户界面500。

[0082] 在操作906,VCS 100根据检索到的许可执行移动应用202。根据与移动应用202关联的应用许可以及在某些示例中还根据移动装置153,VCS 100可相应地为移动应用202提供对车辆131系统(诸如,可用的功能和HMI)的访问。

[0083] 在操作908,VCS 100记录移动应用202的应用使用。例如,VCS 100可记录应用使用208,应用使用208包括移动应用202对API、RPC和车辆131系统的使用。在操作908之后,处理900结束。

[0084] 尽管上面描述了示例性实施例,但并不意在这些实施例描述了本发明的所有可能形式。更确切地,说明书中使用的词语为描述性词语而非限制,并且应理解的是,可在不脱离本发明的精神和范围的情况下做出各种改变。此外,可将各种实现的实施例的特征进行组合以形成本发明进一步的实施例。

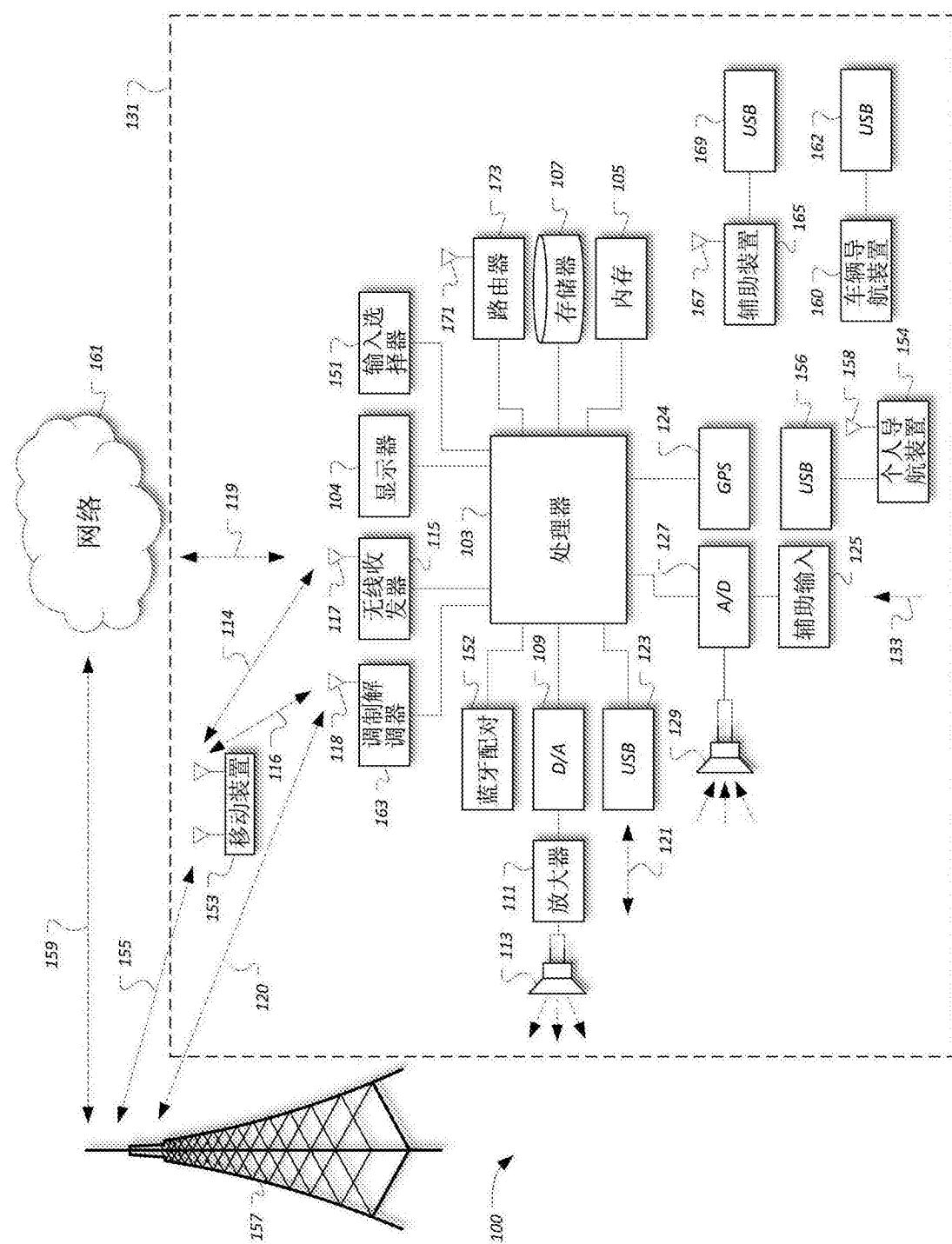


图 1

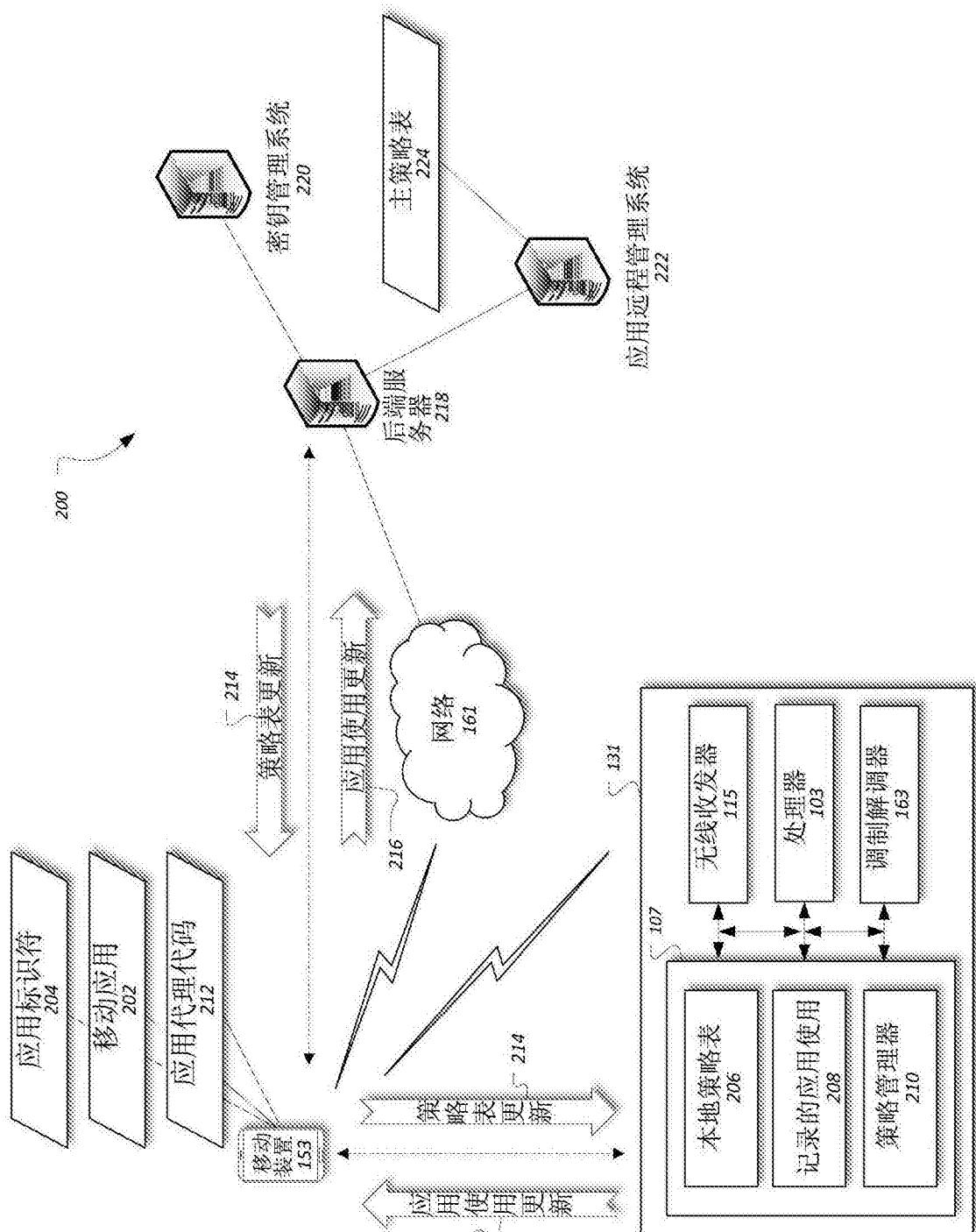


图2

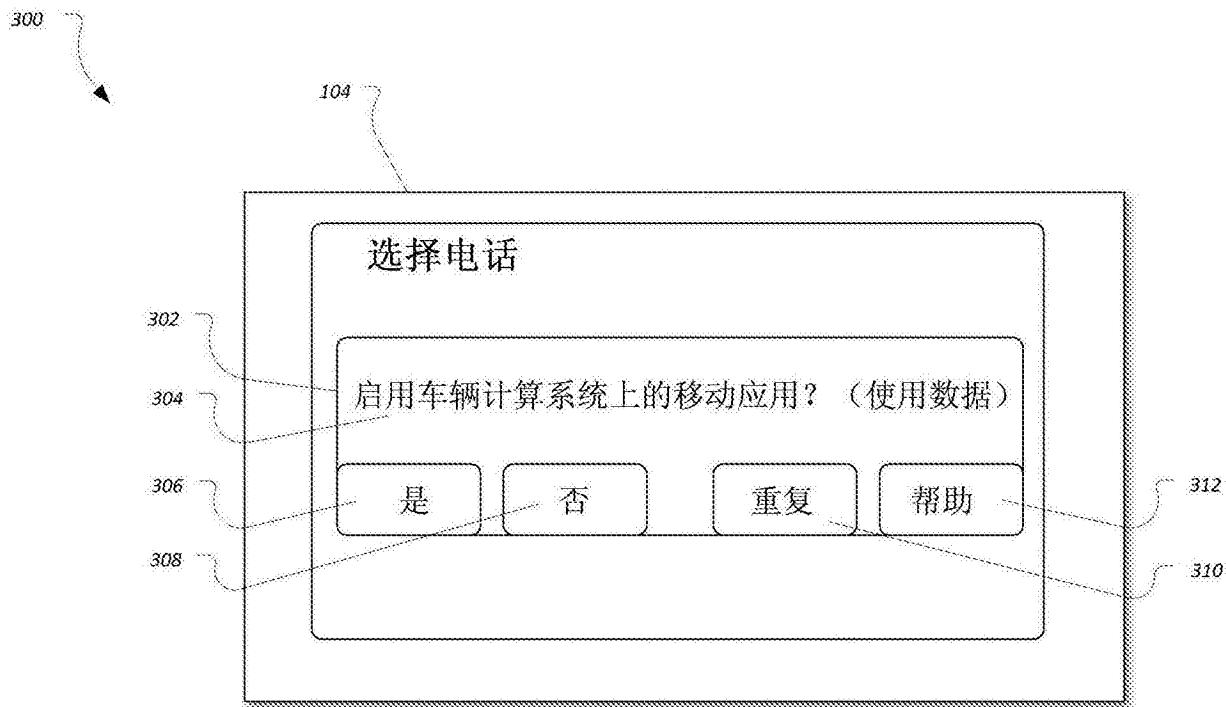


图3

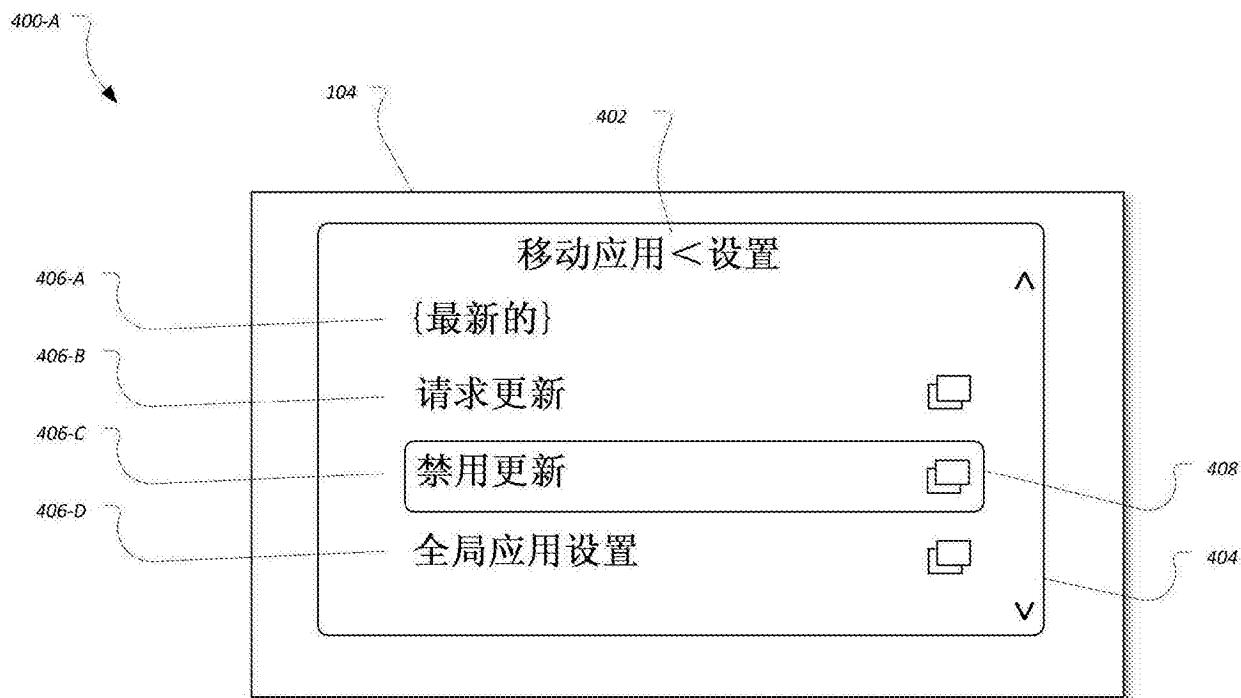


图4A

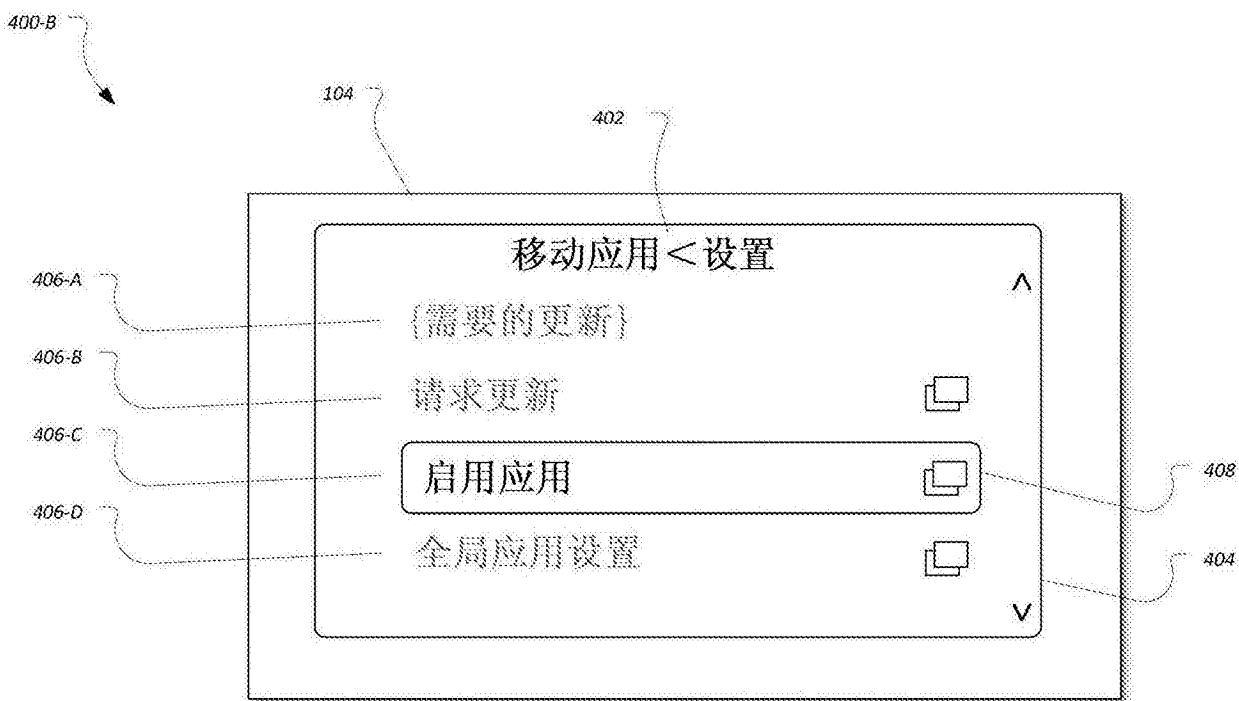


图4B

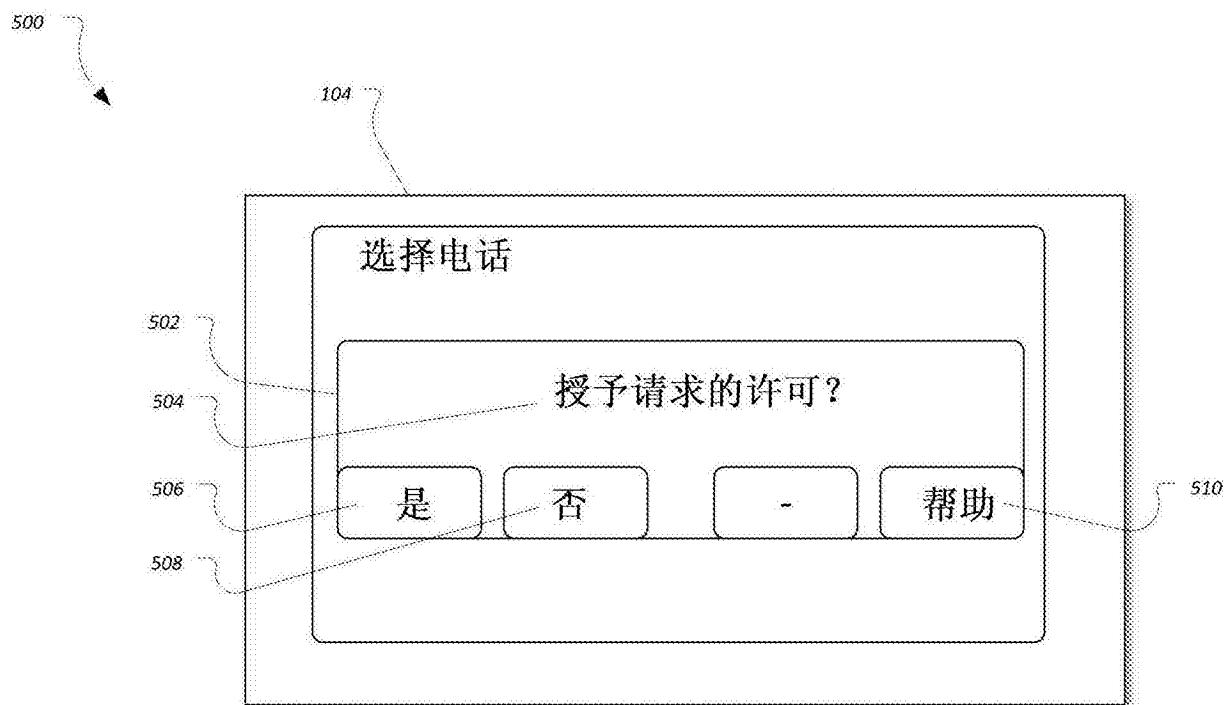
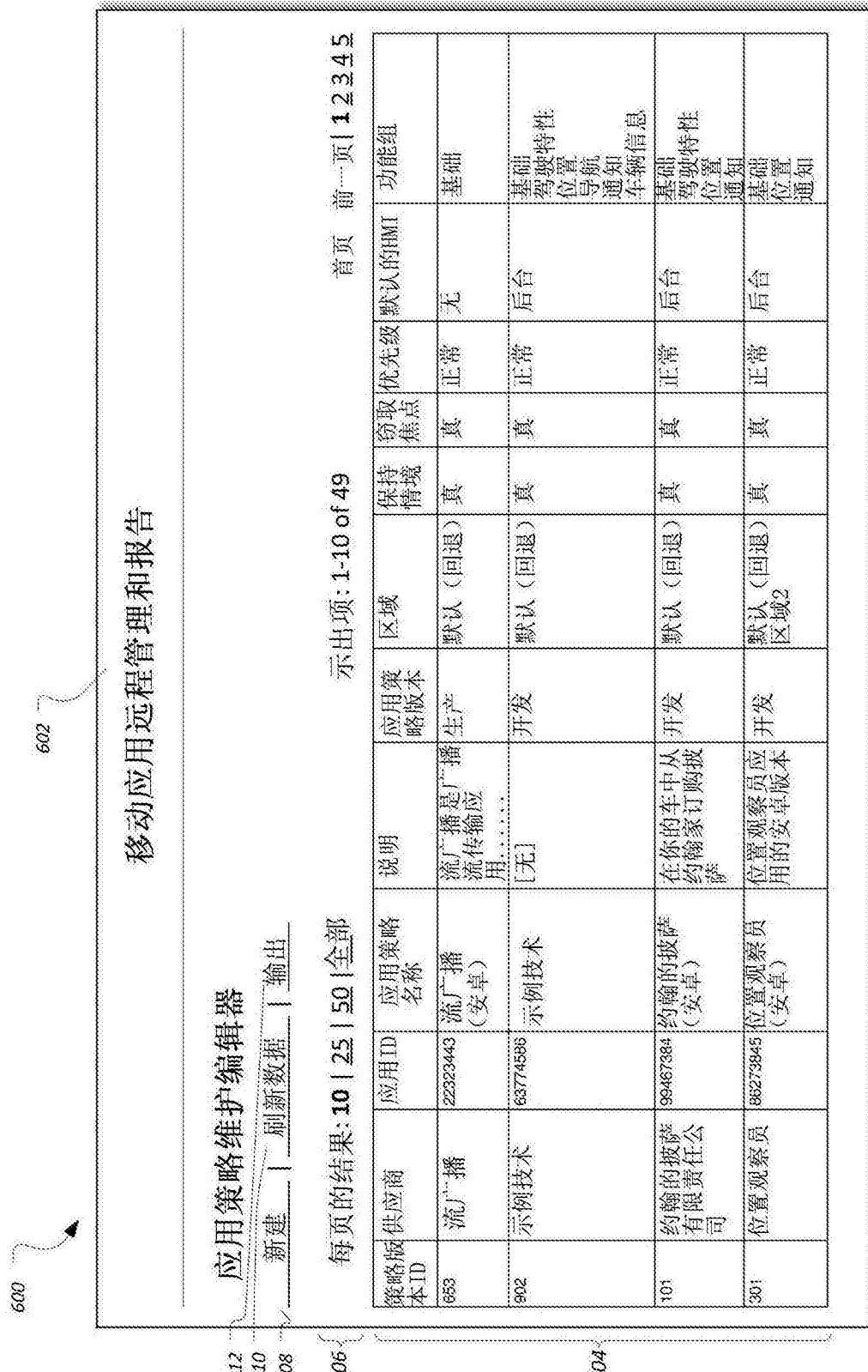


图5



The screenshot shows a mobile application management and reporting interface. At the top, there are tabs for '新建' (New), '刷新数据' (Refresh Data), and '输出' (Output). Below the tabs, the title '移动应用远程管理和报告' (Mobile Application Remote Management and Reporting) is displayed. On the left, there is a sidebar with icons for '策略' (Strategy), '应用' (Application), '设备' (Device), and '日志' (Log). The main content area shows a table titled '应用策略维护编辑器' (Application Strategy Maintenance Editor). The table has columns for '策略版本ID' (Strategy Version ID), '供应商' (Supplier), '应用ID' (App ID), '应用名称' (App Name), '说明' (Description), '应用策略版本' (Strategy Version), '区域' (Region), '保持情境' (Keep Context), '窃取焦点' (Steal Focus), '优先级' (Priority), '默认的HMI' (Default HMI), and '功能组' (Function Group). There are 10 rows of data in the table, each with a unique ID (e.g., 653, 902, 101, 301) and various configuration details. The table also includes navigation buttons like '首项' (First Item), '前一项' (Previous Item), '后一项' (Next Item), and '最后项' (Last Item). The bottom of the interface shows a footer with icons for '策略' (Strategy), '应用' (Application), '设备' (Device), and '日志' (Log).

策略版本ID	供应商	应用ID	应用名称	说明	应用策略版本	区域	保持情境	窃取焦点	优先级	默认的HMI	功能组
653	流广播	222323443	流广播(安卓)	广播是广播 流传输应用……	默认(回退)	真	正常	无	基础		
902	示例技术	63774586	示例技术	[无]	开发	默认(回退)	真	真	正常	后台	基础驾驶特性 驾驶位置 导航通知 车辆信息
101	约翰的披萨有限公司	99467384	约翰的披萨(安卓)	在你的车中从约翰的披萨订购	开发	默认(回退)	真	真	正常	后台	基础驾驶特性 驾驶位置 通知
301	位置观察员	862753845	位置观察员(安卓)	位置观察员应位置的安卓版本	开发	默认(区域2)	真	真	正常	后台	基础位置 通知

图6

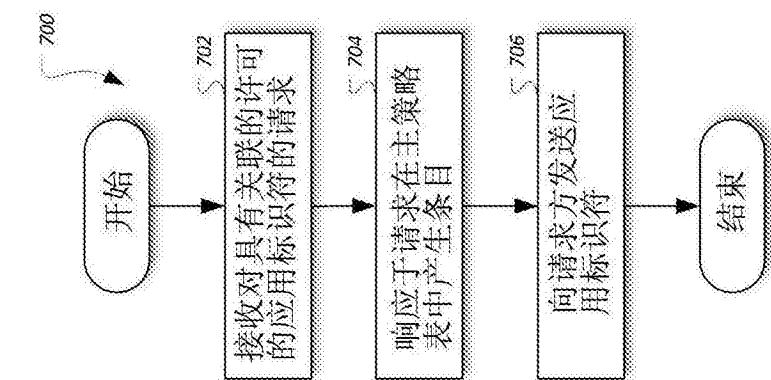


图 7

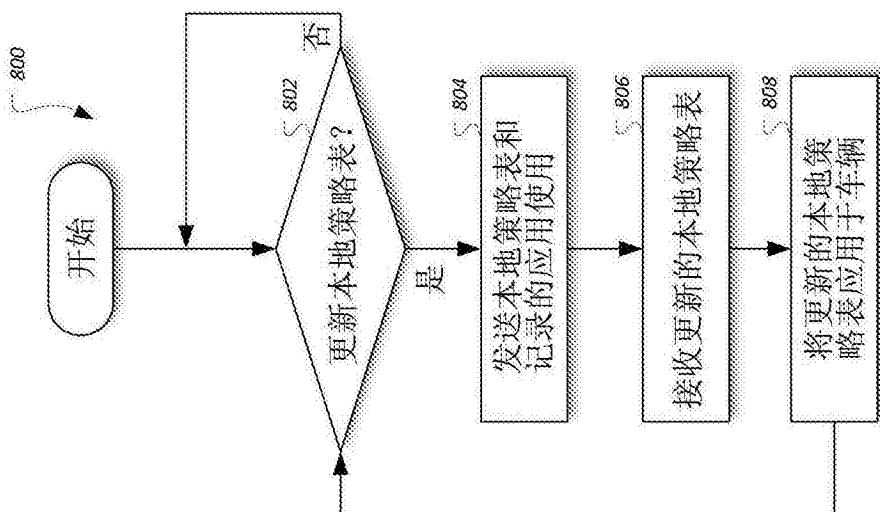


图 8

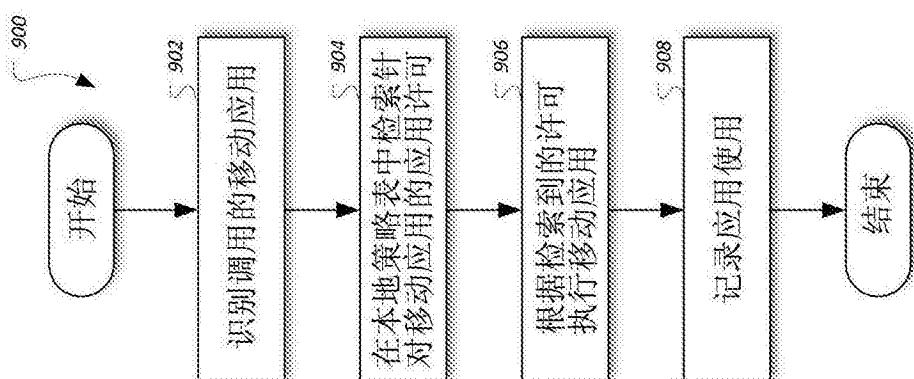


图 9