(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 104620560 B
(45)授权公告日 2018.04.27

(21)申请号 201380046918.3

(22)申请日 2013.09.10

(65)同一申请的已公布的文献号
申请公布号 CN 104620560 A

(43)申请公布日 2015.05.13

(30)优先权数据
61/699,800 2012.09.11 US
14/010,437 2013.08.26 US
14/023,427 2013.09.10 US

(85)PCT国际申请进入国家阶段日
2015.03.09

(86)PCT国际申请的申请数据
PCT/US2013/059102 2013.09.10

(87)PCT国际申请的公布数据
WO2014/043147 EN 2014.03.20

(73)专利权人 耐克斯特纳威公司
地址 美国加利福尼亚州桑尼维尔市奥克米德大道484号

(72)发明人 华拉保绍·瓦杰哈拉
迪帕克·约瑟
萨勃拉曼尼·梅雅潘
阿鲁姆·拉格胡帕西

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 陈炜

(51)Int.Cl.
H04L 29/08(2006.01)

(56)对比文件
US 2001055392 A1,2001.12.27,
CN 102263637 A,2011.11.30,
CN 102026090 A,2011.04.20,
CN 101388907 A,2009.03.18,
WO 2009093951 A1,2009.07.30,
US 2012106738 A1,2012.05.03,

审查员 黄淑美

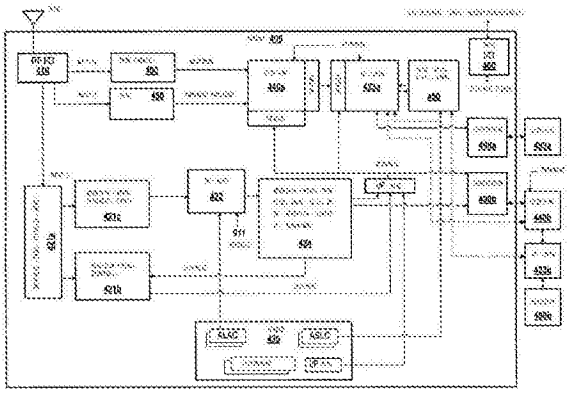
权利要求书3页 说明书22页 附图13页

(54)发明名称

用于提供对传送的信息的条件访问的系统及方法

(57)摘要

本公开涉及基于各种考虑(包括请求的服务类型、用户类似、设备类型、软件应用类型、支付、和/或与特定软件应用相关联的其他特性、或该软件应用的经销商)控制在接收机处、或在接收机外部的另一设备处对位置信息的访问的系统、方法、计算机程序产品及装置。本公开还涉及用于针对除其他应用之外的特定应用执行安全数据传输的系统、方法、计算机程序产品及装置。



CN 104620560 B

1.一种用于控制由一个或多个应用对位置信息的访问的计算机实施的方法，该方法包括：

使用第一密钥对由接收机从陆地发射机的网络中的发射机上接收的加密位置信号的第一集合进行解密；

根据解密位置信号的第一集合确定位置信息；

识别来自所述确定的位置信息的位置信息的第一集合，其中，位置信息的所述第一集合基于与第一应用相关联的第一服务水平来被识别；

使用第二密钥对所述位置信息的所述第一集合进行加密；以及

向所述第一应用提供加密的所述位置信息的第一集合。

2.根据权利要求1所述的计算机实施的方法，其中，所述位置信息的所述第一集合包括指定所述陆地发射机的网络中的发射机的位置的位置坐标。

3.根据权利要求1所述的计算机实施的方法，其中，该方法还包括：

使用所述解密位置信号来计算所述接收机的位置的估计坐标，其中，位置信息的所述第一集合包括所述接收机的所述估计坐标。

4.根据权利要求3所述的计算机实施的方法，其中，所述解密位置信号包括规定在所述陆地发射机中的每个陆地发射机处确定的大气信息的数据，并且其中，所述方法包括：

使用所述解密位置信号和在所述接收机测量到的大气测量计算所述接收机的估计幅度坐标，其中，所述估计坐标包括所述估计幅度坐标。

5.根据权利要求1所述的计算机实施的方法，其中，该方法包括：

使用所述解密位置信号计算所述接收机的位置的估计坐标；以及

基于针对所述第一应用准许的精度水平，计算修正坐标，该修正坐标基于所述估计坐标，其中，所述修正坐标在指定所述接收机的所述位置方面比所述估计坐标精度低，并且其中，位置信息的所述第一集合包括所述修正坐标。

6.根据权利要求1所述的计算机实施的方法，其中，所述方法包括：

从所述确定的位置信息中识别位置信息的第二集合，其中，位置信息的所述第二集合基于与第二应用相关联的第二服务水平来被识别，其中，包括在位置信息的所述第一集合中的位置信息不包括在位置信息的所述第二集合中；

使用第三密钥对位置信息的所述第二集合进行加密；以及

向所述第二应用提供位置信息的所述第二集合。

7.根据权利要求1所述的计算机实施的方法，其中，所述方法包括：

使用所述第一密钥或第三密钥对由所述接收机从所述陆地发射机的网络中的所述发射机上接收的加密位置信号的第二集合进行解密，其中，当所述接收机在第一位置处时，加密位置信号的所述第一集合被所述接收机接收，以及当所述接收机在第二位置处时，加密位置信号的所述第二集合被所述接收机接收；

根据所述解密位置信号的第二集合确定附加的位置信息；

从所述附加的位置信息识别位置信息的第二集合，其中，所述位置信息的所述第二集合基于与第二应用相关联的第二服务水平来被识别；

使用第四密钥对位置信息的所述第二集合进行加密；以及

向所述第二应用提供位置信息的所述第二集合。

8.根据权利要求1所述的计算机实施的方法，其中，所述方法包括：

在识别位置信息的所述第一集合之前，确定规定所述第一服务水平的信息是否存储在所述接收机上；

一旦确定规定所述第一服务水平的所述信息未被存储在所述接收机上，访问与所述第一应用相关联的第一开发商密钥；

向服务器发送所述第一开发商密钥；以及

响应于向所述服务器发送所述第一开发商密钥，接收规定所述第一服务水平的所述信息。

9.根据权利要求8所述的计算机实施的方法，其中，规定所述第一服务水平的所述信息包括在与所述第一应用相关联的第一授权的服务水平证书中，并且其中，所述第一授权的服务水平证书与所述第一开发商密钥相关联。

10.根据权利要求1所述的计算机实施的方法，其中，所述第一服务水平规定所述第二密钥能够用于对位置信息的所述第一集合进行加密的时段。

11.根据权利要求1所述的计算机实施的方法，其中，所述第二密钥是在加密位置信号的所述第一集合被解密之后生成的会话密钥。

12.根据权利要求1所述的计算机实施的方法，其中，第一应用在远程服务器上运行，并且位置信息的所述第一集合被从所述接收机提供至所述远程服务器。

13.根据权利要求1所述的计算机实施的方法，其中，该方法包括：

基于在与所述第一应用相关联的第一证书中规定的参数来确定所述第一服务水平。

14.根据权利要求1所述的计算机实施的方法，其中，该方法包括：

在通过未保护的通信路径发送所述位置信息之前，对所述位置信息进行加扰；以及

在识别位置信息的所述第一集合之前，对加扰的位置信息进行解扰。

15.根据权利要求3所述的计算机实施的方法，其中，该方法包括：

在通过未保护的通信路径发送所述估计坐标之前，对所述估计坐标进行加扰；以及

在对位置信息的所述第一集合进行加密之前，对加扰的估计坐标进行解扰。

16.根据权利要求1所述的计算机实施的方法，其中，该方法包括：

从多个密钥中选择所述第一密钥，其中，所述加密位置信号的CRC字段仅在所述第一密钥用于对所述加密位置信号的第一集合进行解密时通过校验。

17.根据权利要求1所述的计算机实施的方法，其中，该方法包括：

从多个密钥中选择所述第一密钥，其中，所述解密位置信号的数据仅在所述第一密钥用于对所述加密位置信号的第一集合进行解密时匹配期望的值范围。

18.根据权利要求1所述的计算机实施的方法，其中，所述加密位置信号的第一集合包括来自多个发射机的分组数据，并且其中，所述方法包括：

从多个密钥中选择所述第一密钥，其中，来自所述多个发射机的所述分组数据仅在所述第一密钥用于对所述加密位置信号的第一集合进行解密时通过一个或多个相关性校验。

19.根据权利要求1所述的计算机实施的方法，其中，位置信息的所述第一集合包括来自所述陆地发射机的网络的定时校正。

20.根据权利要求1所述的计算机实施的方法，其中，位置信息的所述第一集合包括来自所述陆地发射机的网络中的所述发射机的大气信息。

21.根据权利要求1所述的计算机实施的方法，其中，所述确定的位置信息包括加密的定位信号的所述第一集合的每个位置信号的估计到达时间。

22.一种用于控制由一个或多个应用对位置信息的访问的系统，该系统包括至少一个处理器以及与所述处理器耦合的存储器，所述处理器从所述存储器中读取指令来可操作地执行权利要求1-21中任一项所述的方法。

23.一种其上存储有程序指令的非暂态性计算机可读介质，当由一个或多个计算机执行时，所述程序指令使一个或多个计算机执行权利要求1-21中任一项所述的方法。

用于提供对传送的信息的条件访问的系统及方法

技术领域

[0001] 本公开通常涉及定位系统及方法。更具体地，但不专门地，本公开涉及用于控制对位置信息的访问的系统及方法。

背景技术

[0002] 用于提供位置信息的系统是本领域公知的。例如，基于无线电的系统(LORAN、GPS、GLONASS等)已经为人、车辆、装备等提供位置信息。然而，这些系统具有与诸如定位精度、传输和接收信号水平、无线电信道干扰、和/或诸如多路、设备功耗等之类的信道问题之类的因素相关联的限制。

[0003] 移动订户的准确位置的确定能够是非常有挑战性的。如果订户处于室内或位于具有障碍物的城市区域内，订户的移动设备可能不能从GPS卫星接收信号，并且网络可能被迫使依赖于精度较低的基于网络的三边测量/多边测量定位方法。此外，如果订户处于多层建筑物中，只知道该订户处于该建筑物内，而不知道他们位于哪层，这将导致提供紧急救援的延迟(其能够潜在地威胁生命)。清楚的是，需要能够辅助订户的计算设备(例如，移动计算设备)加速位置确定过程、提供更高的精度(包括垂直信息)、并且解决一些在城市区域中以及建筑物内部的位置确定的挑战性的系统。

[0004] 此外，在类似GPS的系统中传送的位置信息容易地可用于各种设备，而无需任何对管理哪个设备具有对位置信息的访问的选项，或者更具体地，设备上的哪个软件应用可以使用位置信息。该管理的缺乏可以向网络运营商造成带宽负担，其中，多个设备之间的多个应用通过该网络向与那些应用相关联的第三方服务传送位置信息。具有管理位置信息的使用的能力还将允许网络运营商为其客户维持更好的服务水平，同时降低不需要的带宽使用。此外，提供对网络运营商的更好的控制将允许针对每个用户设备或每个用户设备的用户以应用水平或服务水平的每货币化。因此，需要改善的定位系统来解决现有的定位系统和设备的这些和/或其他问题。

发明内容

[0005] 描述了用于为计算设备提供对位置信息的条件访问的系统、方法和计算机程序产品，所述计算机程序产品包括计算机可用介质，该计算机可用介质具有在其中编码的计算机可读程序代码，所述代码被适配成被运行以实施用于为计算设备提供对位置信息的条件访问的方法。例如，本公开的某些方法涉及用于控制由一个或多个应用对位置信息的访问的系统、方法、计算机程序产品及装置。所述系统、方法、计算机程序产品和装置可以使用第一密钥对从陆地发射机的网络接收的加密位置信号的第一集合进行解密。所述系统、方法、计算机程序产品和装置还可以根据解密位置信号的第一集合来确定位置信息，并识别所述位置信息的第一集合，其中，所述位置信息的所述第一集合基于与第一应用相关联的第一服务水平来被识别。所述系统、方法、计算机程序产品和装置还可以使用第二密钥对所述位置信息的所述第一集合进行加密，并向所述第一应用提供加密的所述位置信息的第一集

合。下面结合附图来描述各种附加的方面、特征及功能。

附图说明

[0006] 注意力转到附图和具体实施方式。

[0007] 图1描绘了示出可以在其上实施实施方式的陆地位置/定位系统的细节的图示；

[0008] 图2示出了示出可以在其上实施实施方式的陆地位置/定位系统的一个实施方式的特定细节的图示；

[0009] 图3描绘了发射机/信标的图示；

[0010] 图4A描绘了示出接收机的一个实施方式的细节的图示；

[0011] 图4B描绘了示出接收机/用户设备以及所述接收机/用户设备外部的其他组件的一个实施方式的细节的图示；

[0012] 图4C描绘了示出接收机以及所述接收机/用户设备外部的其他组件的另一实施方式的细节的图示；

[0013] 图5A示出了用于确定与接收机有关的位置信息以及在接收机处控制对所述位置信息的访问的过程；

[0014] 图5B示出了用于为E-911呼叫分配位置信息的过程；

[0015] 图5C示出了用于未提供的密钥的过程；

[0016] 图5D示出了用于预提供的密钥的过程；

[0017] 图6示出了用于提供对位置信息的条件访问的过程；

[0018] 图7示出了用于提供条件访问证书的过程；

[0019] 图8示出了用于处理位置信息的过程；

[0020] 图9示出了用于在条件访问过程期间使用的数据的类型；

[0021] 图10A示出了分组结构；

[0022] 图10B示出了用于根据某些方面的使用的比特序列；以及

[0023] 图11示出了用于在接收机/用户设备处提供对位置信息的条件访问的过程。

具体实施方式

[0024] 下面描述本公开的各种方面。显而易见的是，这里的教导可以以各种形式来被具体化，并且这里公开的任何具体结构、功能或两者仅仅是示意性的。基于这里的教导，本领域的技术人员应当理解的是，公开的任何方面可以独立于任何其他方面来实施，并且这些方面中的两个或更多个可以以各种方式来进行组合。例如，可以使用这里阐述的任意数量的方面来实施系统或实践方法。

[0025] 如这里使用的，术语“示意性”意味着用作示例、实例或示意。这里描述为“示意性”的任何方面和/或实施方式不必须被理解为超过其他方面和/或实施方式的优选的或有利的。

[0026] 概述

[0027] 本公开通常涉及用于提供用于位置确定的信令、并使用与例如在蜂窝电话或其他便携式设备中的接收机(在这里还可替换地称为用户设备、用户终端/UE或类似的术语)通信的广域发射机来确定高精度的位置/定位信息的定位系统和方法。与某些方面相关联的

定位信令服务可以使用仅广播信标/发射机，其被配置成传送加密的定位信号。具有合适的芯片集的接收机能够基于空中链路访问认证技术来接收并使用定位信号，所述空中链路访问认证技术包括通过在初始解密阶段期间使用存储的空中链路访问证书(ALAC)的副本对位置信号进行解密的方式来进行认证。一旦在初始解密阶段期间使用ALAC解密，接收机可以基于附加的解密阶段、使用与在该接收机上运行的特定软件应用相关联的授权服务水平证书(ASLC)，向该软件应用提供对位置信息的条件访问。

[0028] 接收机内的各种组件可以用于执行解密阶段。例如，广播信号的解密可以连同ALAC一起发生在GPS芯片处，所述ALAC被提供到安全硬件区域(例如，在GPS芯片中)的固件中。通过比较，使用ASLC对位置信息进行解密可以连同ASLC一起发生在另一芯片处(例如，接收机的处理器)，所述ASLC未被提供在固件(例如，可经由不同水平的软件访问)中。当然，本领域的技术人员将理解替换的配置。

[0029] 一旦解密，位置信息可以由处理器(例如，定位引擎)来处理，以计算各种定位信号数据(例如，纬度、经度和幅度)，从而改变精确度。幅度计算的示例在于2011年11月14日提交的序列号为13/296,067、名称为WIDE AREA POSITIONING SYSTEMS的美国实用新型专利申请中被提供，该申请通过引用合并于此。

[0030] 在接收机处的位置信息的两阶段解密提供一些优于现有技术的优势。例如，两阶段解密的方面使得发射机和/或接收机能够向授权的接收机和/或授权的软件应用(下文称为“应用”)提供定位信号，同时拒绝对未授权的接收机和未授权的应用的访问。类似地，可以基于用户请求访问或其他类型的考虑来控制对位置信息的访问。

[0031] 基于授权来控制对位置信息的访问准许载体和应用开发商提供层级式服务水平，其可以基于不同的商业协定来购买。层级水平可以与精度水平、覆盖区域、有效时段、使用量、使用周期或其他考虑有关。

[0032] 在接收机处的位置信息的两阶段解密还降低未授权的用户(例如，黑客)能够获得对定位信息的访问并使用该定位信息、从而导致收入损失的可能性。

[0033] 上述优势的实现必须针对定位系统的性能需求来进行平衡。根据某些方面，在该系统中执行的加密和解密阶段可以不包括系统性能度量，例如，接收机的位置的首次定位时间(TTFF)和任何位置定位的精度。此外，与这里描述的各种条件访问方法相关联的处理可以基于特定接收机的处理功率来限定，其可以防止过程密集化的加密程序。

[0034] 根据其他方面，条件访问特征可以在各种设备平台上应用，并且可以支持在这里描述的使用情况中识别的分发模型。其他方面可以涉及接收机的基于厂家或基于客户的提供(除了任何重复提供之外)，以支持这里描述的条件访问方法。例如，这里描述了各种提供实施方式。重要的是，这里描述的条件访问过程中的任意过程必须符合任何E-911功能需求。

[0035] 下面结合附图来描述各种其他方面、特征和功能。虽然本公开的实施方式的细节可以变化，并且仍然落入所要求保护的公开的范围内，但本领域的技术人员将理解的是，这里描述的附图不意图启示关于使用范围或创造性方面的功能性的任何限制。附图及其描述都不应当被解释为具有与在那些附图中示出的组件中的任意一个或组合有关的任何依赖性或者需求。

[0036] 在以下描述中，引入多种具体细节来提供对描述的系统和方法的全面理解，并使

能对描述的系统和方法的描述。然而，相关领域的技术人员将认识到，这些实施方式能够不使用具体细节中的一者或多者来实践，或者使用其他组件、系统等来实践。在其他实例中，公知的结构或操作未示出，或者未被具体描述，以避免模糊所公开的实施方式的方面。

[0037] 系统方面

[0038] 图1提供了示出可以在其上实施各种实施方式的示例位置/定位系统100的细节的图示。定位系统100(在这里也称为广域定位系统(WAPS)或简称为“系统”)包括同步的信标(在这里也表示为“发射机”)和用户设备(在这里也表示为“接收机单元”或简称为“接收机”)的网络，所述信标典型地为陆地的，所述用户设备被配置成获取和追踪从所述信标提供的信号和/或其他位置信令，例如，所述其他位置信令可以由卫星系统提供，例如，全球定位系统(GPS)和/或其他基于卫星或陆地的位置系统。可选地，接收机可以包括位置计算引擎，其用于根据从信标和/或卫星系统接收的信号来确定位置/定位信息，并且所述系统100还可以包括与各种其他系统通信的服务器系统，例如，信标、网络基础设施(例如，因特网、蜂窝网络、广域网或局域网和/或其他网络)。服务器系统可以包括各种与系统有关的信息，例如，塔索引、计费接口、一个或多个加密算法处理组件(其可以基于一个或多个专用的加密算法)、位置计算引擎和/或用于便于系统的用户的位置、运动和/或定位确定的其他处理组件。

[0039] 如在示例性系统100中示出的，信标可以为多个发射机110的形式，并且接收机单元可以为一个或多个用户设备120的形式，所述用户设备可以是被配置成从发射机110接收信令、以及可选地被配置成接收GPS或其他卫星系统信令、蜂窝信令、Wi-Fi信令、Wi-Max信令、蓝牙信令、以太网、和/或本领域公知或将来开发的其他数据或信息信令的多种电子通信设备中的任意电子通信设备。接收机单元120可以为蜂窝或智能电话、平板电脑设备、PDA、笔记本或其他计算系统、数码相机、资产追踪标签、以及脚链(ankle bracelet)和/或类似的或等价的设备的形式。在一些实施方式中，接收机单元120可以是独立式位置/定位设备，其被配置成仅或主要接收来自发射机110的信号，并至少部分地基于接收到的信号确定定位/位置。如这里描述的，接收机单元120在这里还可以被表示为“用户装置”(UE)、手持设备、智能手机、平板电脑、和/或“接收机”。

[0040] 发射机110(其在这里也被表示为“塔”)被配置成经由示出的通信链路113向多个接收机单元120(为了简便，在图1中示出了单个接收机单元120，然而，典型的系统将被配置成在定义的覆盖区域内支持多个接收机单元)发送发射机输出信号。发射机110还可以经由通信链路133与服务器系统130连接，和/或可以具有到网络基础设施170的其他通信连接(未示出)，例如，经由有线连接、蜂窝数据连接、Wi-Fi、Wi-Max或其他无线连接等等。

[0041] 一个或多个接收机120可以经由来自每个接收机110的对应的通信链路113从多个接收机110接收信令。此外，如图1所示，接收机120还可以被配置成接收和/或发送其他信号，例如，经由来自蜂窝基站(也称为节点B、eNB或基站)的通信链路163接收和/或发送蜂窝网络信号，Wi-Fi网络信号、寻呼网络信号、或其他有线或无线连接信令，以及经由例如来自GPS或其他卫星定位系统的卫星通信链路153来接收和/或发送卫星信令。虽然在图1的示例性实施方式中示出的卫星定位信令被示为从GPS系统卫星150提供，但是在其他实施方式中，该信令可以被从其他卫星系统，和/或，在一些实施方式中，基于陆地的有线或无线定位系统或其他数据通信系统提供。

[0042] 在示例性实施方式中，系统100的发射机110被配置成在专门许可的或共享许可/未许可的无线电频谱中运行；然而，一些实施方式可以被实施为在未许可的共享频谱中提供信令。发射机110可以使用新型信令(如这里随后描述的)在这些各种无线电频段中传送信令。该信令可以为专用信号的形式，所述专用信号被配置成以定义的格式提供特定的数据，以有利的用于定位和导航的目的。例如，如这里随后描述的，信令可以被构建为特别有利于在有障碍的环境中操作，例如，其中传统的卫星位置信令通过反射、多路等被减弱和/或影响。此外，该信令可以被配置成提供快速获取和位置确定时间，以在设备上电或定位激活时允许快速位置确定、降低功耗和/或提供其他优势。

[0043] WAPS的各种实施方式可以与其他定位系统合并，来提供增强的定位和位置确定。可替换地或附加地，WAPS系统可以用于辅助其他定位系统。此外，由WAPS系统的接收机单元120确定的信息可以经由其他通信网络链路163(例如，蜂窝、Wi-Fi、寻呼等)来被提供，以向一个或多个服务器系统130以及存在于网络基础设施170上的或与网络基础设施170耦合的其他网络系统报告位置和定位信息。例如，在蜂窝网络中，蜂窝回程链路165可以用于经由网络基础设施170向相关联的蜂窝载体和/或其他(未示出)提供来自接收机单元120的信息。这可以用于在紧急期间快速且精确地定位接收机120的位置，或者可以用于提供来自蜂窝载体或其他网络用户或系统的基于位置的服务或其他功能。

[0044] 注意的是，在本公开的上下文中，定位系统是定位纬度、经度和幅度坐标中的一者或多者的系统，其还可以按照一维坐标系、二维坐标系或三维坐标系(例如，x、y、z坐标、角度坐标等等)来描述或示出。此外，注意的是，无论何时提及术语“GPS”，其应当在全球导航卫星系统(GNSS)的更宽泛的意义上被理解，所述GNSS可以包括其他现有的卫星定位系统(例如，GLONASS)和未来的定位系统(例如，伽利略(Galileo)和罗盘/北斗(Compass/Beidou))。此外，如之前示出的，在一些实施方式中，其他定位系统(例如，基于陆地的系统)可以在基于卫星的定位系统之外被使用，或者代替基于卫星的定位系统来被使用。

[0045] WAPS的实施方式包括多个塔或发射机，例如，图1中示出的多个发射机110，其在发射机输出信号中、向接收机120广播WAPS数据定位信息和/或其他数据或信息。定位信号可以被坐标化，以在特定系统或局部覆盖区域的所有发射机之间被同步，并且可以具有规律的GPS时钟源，以用于定时同步。WAPS数据定位传输可以包括专用通信信道资源(例如，时间、编码和/或频率)，以便于三边测量法所需的数据的传输、到订户/订户群组的通知、消息的广播、和/或WAPS网络的通用操作。关于WAPS数据定位传输的公开可以在合并的申请中找到。

[0046] 在使用不同的到达时间差或三边测量法的定位系统中，传送的定位信息典型地包括精度时间序列和定位信号数据中的一者或多者，其中，所述定位信号数据包括发射机的位置和各种定时校正和其他相关的数据或信息。在一个WAPS实施方式中，数据可以包括附加的消息或信息，例如，对订户群组的通知/访问控制消息、通用广播消息、和/或与系统操作、用户、与其他网络的交互、以及其他系统功能有关的其他数据或信息。所述定位信号数据可以以多种方式来提供。例如，定位信号数据可以被调制到编码的时间序列、增加或覆盖到所述时间序列上、和/或与所述时间序列串联。

[0047] 这里描述的数据传输方法和装置可以用于提供WAPS的改善的定位信息吞吐量。特别地，高阶调制数据可以作为来自伪噪声(PN)测距数据的信息的分离部分被传送。这可以

用于允许在使用CDMA多路复用、TDMA多路复用、或CDMA/TDMA多路复用的组合的系统中改善的获取速度。本公开按照广域定位系统来被示出，在该广域定位系统中，多个塔向UE广播同步的定位信号，并且更特别地，使用陆地的塔；然而，实施方式不限于此，并且落入本公开的精神和范围内的其他系统也可以被实施。

[0048] 在示例性实施方式中，WAPS使用从塔或发射机(例如，发射机110)发送的编码调制(称为扩频调制或伪噪声(PN)调制)来实现宽的带宽。相应的接收机单元(例如，接收机或用户设备120)包括用于使用解扩电路来处理所述信号的一个或多个组件，例如，匹配滤波器或一串相关器。这种接收机产生理想地具有被低水平能力围绕的强峰值的波形。峰值的到达时间表示在UE处传送的信号的到达时间。对来自多个塔(其位置是准确已知的)的多个信号执行该操作，允许借由三边测量法来确定接收机的位置。这里随后描述与发射机(例如，发射机110)中的WAPS信号生成以及接收机(例如，接收机120)中的接收信号处理有关的各种附加细节。

[0049] 在一个实施方式中，WAPS可以使用二进制编码调制作为扩频方法。示例性实施方式的WAPS信号可以包括两种特定类型的信息：(1)高精度测距信号(其可以相对于其他信号被快速传输)，以及(2)定位数据，例如，发射机ID和位置，一天中的时间，健康、环境条件，例如，大气信息(例如，压力、温度、湿度、风向及风力、以及其他条件)。与GPS相似，WAPS可以通过将高速二进制伪随机测距信号与低速率信息源进行调制来传送定位信息。除了该申请，合并的申请公开了使用伪随机测距信号和调制信息信号的方法的实施方式，二者都可以使用高阶调制，例如，四进制或八进制调制。在一个实施方式中，测距信号被二进制相位调制，以及使用更高阶调制来在分开的信号中提供定位信息。

[0050] 常规的系统使用位置定位信号的格式(例如，在时分多路复用配置中使用的)，其中，每个时隙传输包括伪随机测距信号，其后跟随各种类型的定位数据。这些常规的系统还包括同步或同时信号，该信号在伪随机测距信号也被用作同时信号的情况下被删除。然而，正如其他较早的系统一样，这些常规系统的定位数据是二进制的，其限制吞吐量。这些系统还在其中传送定位数据的间隔期间传送大量的二进制比特。

[0051] 为了解决这些限制，在示例性实施方式中，二进制或四进制的伪随机信号可以在特定的时隙中传送，所述特定的时隙后面跟随非常高阶的调制数据信号。例如，在给定的时隙中，一个或多个定位信息码元(symbol)可以使用差分16相位调制来传送，以在每个时隙传送4比特的信息。这表示针对典型地在向伪随机载体应用二进制相位调制时传送的1比特而言，具有4倍的吞吐量改进。定位信息的其他类型的调制也可以被使用，例如，16QAM等等。此外，某些误差控制调制方法可以用于更高水平的调制，例如，格码的使用。这些调制方法通常降低误差率。

[0052] 图2描绘了被配置成实施在这里描述的条件访问过程的定位系统240的某些方面。如图2所示，定位系统240可以执行各种功能。例如，定位系统240可以生成并构造可用的ALAC，该ALAC可以被独个生成，并以ALAC块的形式提供给制造商210和/或服务提供方230，以添加到用户设备220(例如，GPS FW图像)。ALAC可以以设备特定的方式来实施，包括设备标识符的使用，以及设备特定的算法，以提供对ALAC的附加的保护层。定位系统240还可以运行账单和审计系统，以对由定位系统240提供的定位功能的使用进行追踪和计费。

[0053] 定位系统240可以向制造商210、用户设备220、服务提供方230、和/或外部实体250

(例如,应用开发商或提供方)生成并构造可用的ASLC。ASLC可以被序列化以包括唯一的设备标识符,例如,IMEI、MAC地址等等。

[0054] 定位系统240可以为期望将位置信息合并到可下载的应用中的外部实体250生成并管理开发商密钥、SDK及API。每个开发商密钥可以基于相关联的应用的服务水平,具有一些相关联的ASLC。每个应用ASLC可以包含开发商密钥,作为唯一的标识符,并且也可以包含其他唯一的ID。定位系统240还可以维持服务器处理来自领域中(即,在用户设备220上)部署的应用、针对到用户设备220的ASLC的动态传输的请求。

[0055] 制造商210可以将一个或多个ALAC和ASLC(例如,从定位系统240获取,或者被单独创建和维护)连同必备的固件("FW")和软件("SW")一起映像到接收机上。制造商210还可以将文件库(library)加载为图像。制造商210可以包括芯片集供应商、设备OEM、OS供应商等等。通过比较,相同的ALAC可以用于来自所有发射机的所有传输,而不同的ASLC可以用于在每个接收机上的每个应用,并且基于特定的用户账户。ASLC和ALAC两者可以在UE处被加密,或者免受未授权的访问。

[0056] 服务提供方230可以向用户设备220提供各种服务,包括蜂窝服务和基于网络的服务。其他服务可以包括内容(例如,视频内容、音频内容、图像内容、文本内容、其他内容)的任意无线或有线传输。服务提供方230可以存储其向用户设备220提供的与应用相关联的ASLC。服务提供方230还可以使能针对E-911的控制面(c面)消息流,以及网络管理(在可应用时)。服务提供方230还可以经由SUPL使能针对内部LBS的用户面(u面)消息流。

[0057] 外部实体250可以包括经由用户的接收机向用户提供各种定位服务的供应商。例如,外部实体250可以包括PSAP、基于位置的广告网络、以及LBS应用开发商/发布商、等等。定位系统240和服务提供方230可以向外部实体250提供一系列服务,包括定位辅助、ASLC验证和提供、增值服务、账单服务和审计服务。

[0058] 用户设备220可以包括智能电话、平板电脑以及连接的计算机设备。用户设备220可以被配置成控制由各个应用(例如,e-911、网络管理(NW)、或LBS)对位置信息的访问。访问的控制可以使用ASLC来完成,所述ASLC被映像到固件上,或者在用户设备220被制造并进入商业流之后被下载。如所示出的,驱动器和文件库层可以为设备上的多个应用和用户辅助ASLC的管理、辅助位置信息的解密、以及辅助限制由应用对解密的位置信息的使用,这基于由ASLC指示的准许。例如,文件库能够将ASLC与其相关的应用(例如,E911、网络管理、LBS等等)相关联,并且能够为应用提供或仲裁合适的位置信息的传输。

[0059] 上面已经描述了各种系统特征,包括发射机和接收机。下面描述的图3和图4A、图4B和图4C提供了关于发射机和接收机的某些实施的其他细节。

[0060] 图3表示示出了信标/发射机系统的一个实施方式300的某些细节的图示,这里随后描述的位置/定位信号可以从所述信标/发射机系统发送。发射机实施方式300可以与图1中示出的发射机110相对应。注意的是,发射机实施方式300包括各种用于执行相关联的信号接收和/或处理的组件;然而,在其他实施方式中,这些组件可以以不同的方式被组合和/或组织,以提供类似的或等价的信号处理、信号生成和信号传输。

[0061] 尽管未在图3中示出,发射机/信标实施方式300可以包括用于接收GPS信号并向处理组件(未示出)提供定位信息和/或其他数据(例如,定时数据、精度因子(DOP)数据或可以从GPS或其他定位系统提供的其他数据或信息)的一个或多个GPS组件。注意的是,虽然在图

3中示出了发射机300具有GPS组件，但是其他用于接收卫星或陆地信号并提供相似的或等价的输出信号、数据或其他信息的组件可以用于发射机内的精确定时操作，和/或用于WAPS网络上的定时校正。

[0062] 发射机300还可以包括用于生成和发送发射机输出信号的一个或多个发射机组件(例如，RF传输组件370)，如这里随后描述的。发射机组件还可以包括本领域公知的或发展的用于向发射天线提供输出信号的各种元件，例如，模拟或数字逻辑和功率电路、信号处理电路、调谐电路、缓存和功率放大器等等。可以在处理组件(未示出)中进行信号处理，以生成所述输出信号，在一些实施方式中，所述处理组件可以与结合图3描述的其他组件集成，或者在其他实施方式中，所述处理组件可以是用于执行多信号处理和/或其他操作功能的独立式处理组件。

[0063] 一个或多个存储器(未示出)可以与处理组件(未示出)耦合，以提供数据存储和取得，和/或提供用于在处理组件中运行的指令的存储和取得。例如，指令可以是用于执行这里随后描述的各种处理方法和功能的指令，例如，用于确定定位信息或与发射机相关联的其他信息(例如，局部环境条件)，以及生成发射机输出信号，该信号被发送至如图1中示出的用户设备120。

[0064] 发射机300还可以包括用于感测或确定与发射机相关联的条件(例如，局部压力、温度、湿度、风或其他(统称为或单独称为“大气”))的一个或多个环境感测组件(未示出)。在示例性实施方式中，大气(例如，压力)信息可以在环境感测组件中被生成，并且被提供给处理组件，以与这里随后描述的在发射机输出信号中的其他数据集成。一个或多个服务器接口组件(未示出)也可以被包括在发射机300中，以提供发射机与服务器系统(例如，图1中示出的服务器系统130)之间的对接，和/或与网络基础设施(例如，图1中示出的网络基础设施170)的对接。例如，系统130可以经由发射机的接口组件向发射机300发送与定位系统和/或用户设备相关联的数据或信息。

[0065] 每个发射机300可以以每时隙每秒可调数量的比特(例如，每时隙每秒96比特)在物理层发送数据，并且每个发射机可以独立于其他，包括其位置信息。发射机300可以包括用于生成、加密、保护、调制和传送数据的各种组件。例如，发射机300可以包括用于生成位置信息的数据生成组件310，用于基于特定的空中链路访问证书(ALAC)对位置信息进行加密的加密组件320，用于存储ALAC的访问证书存储组件330，以及其他组件——例如，分组ID/CRC组件340、编码、凿孔(puncture)和交织组件350、调制组件360、和RF传输组件370，等等未示出的组件。组件340和350可以提供前向误差校正(FEC)和CRC方案，以及其他数据格式化方案，以降低衰弱的影响、路径损耗以及其他环境条件。组件360提供对数据的调制。

[0066] 尽管调制和信号结构可以变化，其中，能够使用每帧变化数量的比特，预期的是，每帧190比特可用于来自发射机300的传输。例如，在编码开销之后，102个数据比特可用，其中7个比特被预留用于未加密的帧信息，留下95个比特用于加密的位置信息。优选的是，最小化地应用加密以维持低开销。例如，一个加密速率可以大约是每3秒95比特。在数据交换之前，传输可以自身重复几循环(例如，10循环或30秒)。各种有效负载被考虑，包括：纬度、经度、幅度、压力、温度、传输校正以及传输质量。其他有效负载可以包括安全信息、服务ID、条件访问数据(例如，ASLC信息)。这些各种有效负载能够被分段到多个时隙上。本领域的技术人员将理解其他有效负载、其他数量的比特、以及对有效负载进行分组的不同方式。

[0067] 在一些情况下，需要n比特指示符来表示被传送的分组的类型(该类型的信息将通过一些分组传送)，或者多个相同信息的分组如何彼此相关。分组结构可以在分组中的任意点处包括该n比特指示符。图10A示出了分组结构的一个示例，该分组结构示出了4个分组类型指示符比特、以及其他比特，以及图10B示出了分组序列的一个示例，该分组序列使用4比特分组类型指示符。

[0068] 如图10A和图10B所示，4个比特可以指示分组类型，以及主分组有效负载可以包括98个比特。4个比特可以不被加密，并且为“0”的分组类型可以是未加密，而为“1”的分组类型可以是加密。对于不为“0”或“1”的分组类型，例如但不限于，第5比特可以是加密比特，并且可以表示该分组是否被加密。该比特可以是未加密。第6比特可以是启示比特，并且可以表示其开始新的分组(1)或者继续之前的分组(0)。该比特可以是未加密。第7比特可以是停止比特，并且可以表示其是最后的分组(1)或者不是(0)。该比特可以是未加密。接下来的95个比特可以包括主分组有效负载，其可以在加密比特为1的情况下被加密，并且在加密比特为0的情况下不被加密。可选地，有效负载可以包括当前分组的索引和/或期望与当前信息一起发送的分组的总数。

[0069] 注意力现在转到图4A，该图4A描绘了接收机400的特征，在该接收机400处，发射机信号可以被接收和处理，以确定定位/位置信息(例如，代替E-911或LBS应用)。

[0070] 接收机实施方式400可以与图1中示出的用户设备120相对应，并且可以包括用于接收GPS信号并向处理组件(未示出)提供定位信息和/或其他数据(例如，定时数据、精度因子(DOP)数据或可以从GPS或其他定位系统提供的其他数据或信息)的一个或多个GPS组件480。当然，其他全球导航卫星系统(GNSS)被考虑，并且应当理解的是，与GPS有关的公开可以应用于这些其他系统。注意的是，虽然在图4A中示出了接收机400具有GPS组件，但是在各种实施方式中，其他用于接收卫星或陆地信号并提供相似的或等价的输出信号、数据或其他信息的组件可以被替换使用。当然，任何定位处理器可以被适配成接收和处理这里描述的或在合并的申请中的位置信息。

[0071] 接收机400还可以包括用于经由蜂窝或其他数据通信系统发送和接收数据或信息的一个或多个蜂窝组件490。可替换地或附加地，接收机400可以包括用于经由其他有线或无线通信网络(例如，Wi-Fi、Wi-Max、蓝牙、USB或其他网络)发送和/或接收数据的通信组件(未示出)。

[0072] 接收机400可以包括由点边线勾勒的一个或多个组件420(称为“组件420”)，其被配置成从陆地发射机(例如，图1中示出的发射机110)接收信号，并处理信号以确定位置/定位信息，如这里随后描述的。组件420可以与图4A中示出的其他组件集成，和/或与所述其他组件共享资源，例如，天线、RF电路等等。例如，组件420和GPS组件480可以共享一些或所有无线电前端(RFE)组件和/或处理元件。处理组件(未示出，但这里通常提到以指示接收机400中的处理功能)可以集成组件420中的一些或所有，或者可以与组件420和/或GPS组件480中的一些或所有共享资源，以确定位置/定位信息，和/或执行其他处理功能，如这里描述的。类似地，蜂窝组件490可以与RF组件410和/或组件420共享RF和/或处理功能。网络组件460也被示出，其可以指代使用任意类型的有线和无线通信路径的局域网、广域网或其他网络。组件410、420、460、480和490中的每个可以向位置引擎440传输数据，该位置引擎440使用数据来确定接收机400的估计位置。位置引擎400可以被实施为本领域公知的或本领域

中未来发展的，包括这样的实施，该实施包括被配置成计算估计位置的处理器。

[0073] 例如，在一个实施方式中，组价490可以通过控制面或用户面安全地传输定位数据，或者数据可以直接通过因特网链路来获取。490与蜂窝调制解调器之间的接口上的数据还可以通过特定于接收机400的接口加密/解密来被保护。

[0074] 一个或多个存储器430可以与处理组件(未示出)和其他组件耦合，以提供数据存储和取得，和/或提供用于在处理组件中运行的指令的存储和取得。例如，指令可以执行这里描述的各种处理方法和功能，例如，解密位置信息和确定定位信息。因此，在组件420之间包括的某些组件(例如，组件421-424)可以执行位置信息、解密密钥、和/或这里描述的其他信息的处理。可替换地，该处理中的一些或所有可以在独立式处理器(未示出)被执行。

[0075] 包括位置估计或用于远程位置计算的信息的位置数据可以使用行业标准协议(例如，控制面信令、用户面(SUPL)信令或因特网/数据协议或上述的一些组合)被传送至这些远程组件。

[0076] 接收机400还可以包括用于感测或确定与接收机相关联的条件(例如，局部压力、温度、湿度或可以用于确定接收机400的位置的其他条件)的一个或多个环境感测组件(未示出)。在示例性实施方式中，压力信息可以在这种环境感测组件中被生成，以用于结合接收到的发射机、GPS、蜂窝或其他信号来确定定位/位置信息。

[0077] 接收机400还可以包括各种附加的用户交互组件，例如，用户输入组件(未示出)，其可以为键盘、触摸屏、鼠标或其他用户交互元件的形式。音频和/或视频数据或信息可以在输出组件(未示出)中被提供，例如，以一个或多个扬声器或其他音频转换器(未示出)、一个或多个视觉显示器(例如，触摸屏)、和/或本领域中公知或发展的其他用户I/O元件的形式。在示例性实施方式中，这种输出组件可以用于基于接收到的发射机信号来可视地显示确定的定位/位置信息，并且所确定的定位/位置信息还可以被发送到蜂窝组件490，进而到达相关联的载体或其他。

[0078] 接收机400可以包括被配置成执行本公开的各种特征的各种其他组件，包括在图5A、图6、图7和图8中示出的过程。例如，组件420可以包括信号处理组件421，该信号处理组件421包括数字处理组件421a，该数字处理组件421a被配置成对从RF组件410接收到的RF信号进行解调，以及还被配置成估计到达时间(TOA)，以未来用于确定位置。信号处理组件421还可以包括伪距生成组件421b和数据处理组件421c。伪距生成组件421b可以被配置成根据估计的TOA生成“原始”定位伪距数据，精炼所述伪距数据，并向位置引擎440提供所述伪距数据，该位置引擎440使用所述伪距数据来确定接收机400的位置。数据处理组件421c可以被配置成对编码的位置信息进行解调，从编码的位置信息中提取加密的分组数据，并对该数据执行误差校验(CRC)。数据处理组件421c向第一密码组件422输出加密的分组数据。

[0079] 第一密码组件422可以被配置成至少基于存储在存储器430中的ALAC对来自加密的分组数据的位置信息进行解密。由于在接收机400上可以存储多个ALAC，并且只有它们中的一者能够在给定的时间应用，第一密码块422能够使用各种技术来确定要使用的正确的ALAC密钥。数据分组本身能够具有CRC/摘要字段，该字段仅在应用正确的ALAC密钥时通过校验。在由于分组内容限制而缺乏CRC/摘要字段的情况下，解密的分组的各个字段能够针对该字段的期望的值范围来被校验。此外，由于接收机能够从位于该接收机附近的多个发射机获取分组数据，来自多个发射机的位置信息将仅在选择了正确的ALAC密钥时通过某些

相关性校验，例如，发射机之间的距离、地理标识符等等。第一密码组件422还可以在接收到表明已经发起紧急911呼叫的指示时向与E-911程序相关联的合适的处理组件传送解密的位置信息。

[0080] 图4A中的组件420还可以包括第二密码组件423，该第二密码组件423被配置成基于存储在存储器430中的合适的ASLC来对位置信息中的一些或所有进行解密。ASLC可以由具有请求的位置信息或位置固定的应用来确定。例如，ASLC可以与接收机400上的LBS应用或E-911应用相关联。

[0081] 一旦由第二密码组件423解密了位置信息，解密的位置信息被输出至数据单元输出组件424，该数据单元输出组件424确定位置信息的离散数据单元(例如，纬度、经度、幅度、压力、温度、湿度、系统时间、定时校正、和/或发射机ID)。位置信息的特定的数据单元之后可以基于由ASLC指示的针对请求访问位置信息的应用的服务水平来被传送至位置引擎440。

[0082] 位置引擎440可以被配置成处理位置信息(以及在一些情况中，GPS数据、小区数据和/或其他网络数据)以确定特定边界内的接收机400的位置(例如，精度水平等等)。一旦确定了，定位信息可以被提供至应用450。本领域的技术人员将理解的是，位置引擎440可以表示能够确定定位信息的任何处理器，包括GPS位置引擎或其他位置引擎。图4A中示出的各种组件的定位在接收机内、在不同的芯片空间被考虑。

[0083] 如在这里任意地方公开的，并且为了清楚在这里重复的，接收机400上的每个应用可能需要其自身的ASLC来访问位置信息，以确定接收机400的位置。关于一些方面，一个ASLC可以由多个应用使用，以及多个ASLC可以由一个应用来使用，但是针对不同用户或在不同的环境下。ASLC可以用于在特定的时段期间以及在特定的服务区域中限制对特定的位置信息的使用。

[0084] E-911、网络支持和LCS应用/服务可以彼此相互独立地来处理，其中，它们各自的ASLC可以被加载到接收机400的固件上，或者在接收机400的制造之后被上传到存储器。每个ASLC可以用于向每个应用/服务提供其自身对位置信息的馈入。分开的处理路径可以用于进一步分离这些应用/服务。

[0085] 接收机400可以具有专用于位置确定的有限的硬件/软件能力。可用于这里描述的条件访问特征的总脚本可以大约为32千字节。其他脚本被考虑。

[0086] 位置信息可以在GPS处理器、应用处理器或在外部服务器被处理。根据一个方面，这里描述的特征可以在接收机上的GPS集成电路(IC)上被执行，或者与所述GPS IC相关联。例如，在接收机处的主处理器可以用于经由双向串形链路与GPS IC通信。纬度、经度连同其他信息可以使用该串行链路来传送。串行链路可以用于验证到GPS IC的交换(例如，ASLC)。考虑的是，GPS IC包括信号处理部分，该信号处理部分搜索发射机(例如，通过与PN序列的相关性)，并对从发射机接收的信号进行解调，以取得物理层有效负载，该有效负载可以为(并且根据这里描述的某些实施方式，是)加密形式。解密引擎能够在将数据提供至下一处理层之前对数据进行解密，所述下一处理层可以为位置引擎。位置引擎可以使用解密的数据来计算接收机位置。各种引擎可以在GPS IC中或在其他接收机电路中被提供。

[0087] 注意力现在落到图4B，该图4B描绘了在第一位置处的接收机400，并且还描绘了位于其他位置的组件，所述其他位置位于接收机400的位置的远程。接收机400和其他组件可

以集体地或单独地基于发射机信号的处理来确定位置信息。图4A的某些方面在图4B中描绘。因此，针对某些实施方式(但不必须是所有)，与图4A有关的那些方面的描述可以被扩展到图4B中的那些方面。

[0088] 如图4B所示，接收机400可以包括接口(I/F)加密/解密(也称为“加扰/解扰”)组件，该组件在数据穿过未保护的接口边界或通过未保护的通信信号来传输时对数据进行保护。在一些情况下，这些I/F组件可以作用于由每个接收机400独立地生成的I/F密钥。

[0089] 图4B提供在第二密码组件423a之前在接收机400处的位置计算，所述第二密码组件423a可以向位于接收机400上的应用450、或不位于接收机400上的应用499a提供位置计算的结果。可替换地，位置计算可以由远程组件(例如，服务器的远程位置引擎440b)来执行，该远程组件使用从接收机400接收的位置数据，从而该远程位置计算的结果可以被返回到接收机400，或者由远程应用499b使用。

[0090] 由图4B中的虚线描绘的组件之间的数据传递可以直接在那些组件之间执行，或者通过中间组件(例如，RF组件410或网络组件460)来执行。虚线可以表示替换的实施方式。例如，应用管理器498a可以从第二密码组件423a接收位置数据，在这之后，应用管理器498a可以促使位置数据被传递至远程应用服务499a(例如，通过网络组件460、或RF组件410、或接收机400中的其他组件)。之后，远程应用服务499a可以使用位置数据(例如，位置估计)来提供与接收机400有关的e911或LBS服务。

[0091] 如另一示例，应用管理器498a可以直接从数据单元输出组件424接收数据，或者通过中间组件(例如，I/F加密组件)接收数据，在这之后，应用管理器498a可以促使位置数据被传递至远程位置引擎440b，该远程位置引擎440b计算接收机400的估计的位置(例如，接收机400的纬度、经度、幅度)。远程位置引擎440b可以向第二密码组件423a(例如，通过网络组件460、或者RF组件410、或接收机400中的其他组件)或第二密码组件423b传送该位置估计，以在那些组件处进行进一步处理。第二密码组件423b例如用于控制由一个或多个远程应用服务499b或在接收机400上运行的应用450对位置估计的访问(例如，通过经由网络组件460或RF组件410或接收机400中的其他组件的位置估计的传递)。远程应用服务499b或应用450之后可以使用位置估计来提供与接收机400有关的e911或LBS服务。任意远程组件可以共位，或者位于不同的地理位置。

[0092] 在图4B中，第一密码组件422向数据单元输出组件424输出解密的位置信息，该数据单元输出组件424确定位置信息的离散数据单元(例如，纬度、经度、幅度、压力、温度、其他大气信息或测量、系统时间、定时校正、和/或发射机ID)。这些数据单元之后被传送至位置引擎440a或440b。位置引擎440a或440b可以被配置成处理位置信息(以及，在一些情况中，GPS数据、小区数据和/或其他网络数据)，以确定特定边界内的接收机400的位置(例如，精度水平、以及其他边界)。一旦确定了，定位信息可以通过第二水平密码423a或423b(并且可能地，通过其他中间组件)被提供至应用450、499a或499b。本领域的技术人员将理解的是，位置引擎440a或440b可以表示能够确定定位信息的任何处理器，包括GPS位置引擎或其他位置引擎。

[0093] 第二密码组件423a可以被配置成使用用于特定应用或具有特定服务水平的应用群组的会话密钥对特定数据进行加密。服务水平可以向某些应用授权对数据单元(例如，纬度、经度、幅度、精度等等)的某些子集的访问。

[0094] 在加密数据(例如,使用会话密钥)之后,第二密码组件423a之后可以使得该加密的数据可用于应用450。会话密钥可以在接收机400处被动态生成,并且可以被周期性地改变,以改善安全性。当单个会话密钥用于应用群组时,该会话密钥能够在针对任何应用,ASLC有效期已逝去时被改变,因此迫使该应用群组请求新的会话密钥。

[0095] 在一个实施方式中,第二密码组件423在与特定应用交换会话密钥之前,针对该应用验证ASLC,以使得应用能够对用于该应用的数据进行解密。初始,第二密码组件423可以从应用接收ASLC,或者可以被指示从存储器430或其他位置查询ASLC。位置信息的特定的加密数据单元之后对该应用是可访问的。

[0096] ASLC可以指示对应用的服务水平授权。为了管理仅对授权用于特定应用的数据的访问,第二密码组件423a可以根据ASLC中指示的对用于发送加密数据的应用的授权,来与该应用交换会话密钥。

[0097] 针对远程应用499a,远程应用管理器498a可以提供通信接口,以在远程应用与第二密码组件423a之间传输ASLC和会话密钥。

[0098] 注意力转到图4C,该图4C描绘了它们涉及接收机和向接收机发送数据或从接收机接收数据的其他组件的本公开的一些方面。如图4C所示,从发射机获取位置信号(例如,使用通过与PN序列的相关性收缩发射机的信号处理)。该信号处理还可以对该信号进行解调,以取得针对每个发射机的物理层有效负载和原始到达时间(TOA)。这些信号可以由各种硬件(HW)、固件(FW)和/或软件(SW)组件来获取和追踪。例如,GPS芯片上的FW和/或HW可以用于从信号传输的各种子帧中的任意一个子帧中解码分组,并验证CRC。可替换地,主处理器能够解码并验证CRC。

[0099] 追踪HW/FW/SW可以用于生成原始TOA数据,并向解密组件传送原始的加密数据(例如,分组)。在一些实施方式中,分组ID针对所有分组类型不加密。原始加密数据可以使用特定HW/FW(例如,特定于WAPS的HW/FW)内的ALAC密钥来解密。ALAC可以基于特定于每个设备的设备ID或设备类别来被加密或封装。设备特定的ID可以用于设备上的WAPS定位服务的权利。

[0100] ALAC解密过程和/或负责解密的FW/HW/SW可以以芯片级、接收机/手持设备级、或载体级针对供应商变化。原始的解密数据连同原始的TOA测量之后可以被加扰(例如,使用加扰算法和设备生成的密钥),并且加扰的数据可以通过保护的或未保护的数据流被发送至在GPS芯片自身上或在主处理器上或者在两者上运行的定位文件库。在解密和定位文件库在相同的HW/FW(例如,GPS芯片)上运行的情况下,加扰可以不是必须的。

[0101] 定位文件库之后可以对原始数据和TOA测量进行解扰,以供未来在文件库中使用。例如,解扰的数据可以被组合成数据单元(DU)1到5,如下所示:DU1(发射机的纬度、经度、幅度(LLA));DU2(在发射机处的压力/温度);DU3(针对发射机的定时校正);DU4(发射机的网络的时间(WAPS时间));以及DU5(发射机的标识符)。

[0102] 可以使用来自DU3的原始的和定时校正来生成精细的TOA。定位引擎可以使用各种数据单元(例如,DU1、DU2、DU5)、连同精细的TOA和压力传感器读数来计算接收机的LLA。注意的是,DU4可以由被配置成生成定时信号(例如,在接收机用于同步其他接收机的情况下使用的)的定位引擎来使用。

[0103] 接收机的LLA或DU1到DU5中的任意一者可以基于由ASLC特定用于请求应用或请求

应用所属于的应用群组的参数来被加密。可以使用各种技术来执行加密，包括随机或预定义的会话密钥、由ASLC定义的其他密钥、或本领域公知的其他加密方法。各种实施被考虑，包括其中服务水平加密和解密可以涉及单个应用实例或多个不同的应用实例的实施。

[0104] 在一个实施中，加密数据可以仅包括用于请求应用的数据，该数据由该应用的服务水平规定。例如，特定精度水平内的接收机的LLA的估计可以变得可用(例如，100米内的LLA精度、10米内的LLA精度)。在这个实施中，位于接收机处的处理器可以对具有x米的精度的已知LLA进行分析，并且之后，依赖于服务水平授权生成具有y米的精度的不同的LLA。这种实施会是有益的，其中，不同的有偿服务水平于变化水平的定位精度相关联。

[0105] 定位引擎可以使用在DU2中接收到的针对多个发射机中的每个发射机的压力和温度读数来生成参考压力的最佳估计。该参考压力可以以加密形式被发送至各个定位引擎，该定位引擎可以使用参考压力和接收机的压力传感器读数来计算幅度，如在合并的参考文献中描述的。

[0106] 在某些SW架构中，定位引擎可以合并在混合实施中的其他源的其他测量，所述混合实施使用来自Wi-Fi、GPS、WAPS及其他发射机中的任意一者的信号。在加密的接收机LLA或其他加密数据(例如，DU1到DU5中的任意一者)的服务水平解密之后，这种混合定位引擎可以结合主处理器运行。可替换地，混合定位引擎可以在服务水平加密之前运行，因此，对从混合定位引擎得到的数据的访问被限于授权的应用。

[0107] 上面关于图4C的讨论可以应用于MS辅助(MS-A)、基于MS(MS-B)或独立式用户面呼叫流。在控制面呼叫流(例如，E-911)的情况下，为原始或精细的TOA/伪距形式的数据和幅度估计(针对MS-A模式)、或为接收机的LLA形式的数据(针对基于MS模式)被发送至位置确定实体(PDE)、服务移动定位中心(SMLC)或其他用于位置计算并向PSAP转发的其他设备。这种传输可以通过蜂窝系统的一个或多个控制面信号进行。

[0108] 注意的是，尽管不是优选的，位置辅助数据能够使用替换的通信方式(例如，基于网络的路径、局域网路径、广域网路径、以及超越RF路径的其他网络路径)被提供至定位引擎。当接收机与发射机网络之间存在低信号条件时，这种传输可以是必须的。当使用替换的通信方式传送时，辅助数据可以使用与ALAC相关联的密钥、或者使用特定于该通信方式的替换的密钥来加密。可替换地，可以不使用ALAC或相似的密钥，而是可以使用服务水平加密和解密。

[0109] 尽管图4C描绘了不同HW/FW/SW内的不同组件，某些实施方式可以将图4C的各种组件合并到一个或多个硬件组件，如主处理器、GPS芯片或两者。

[0110] 与方法有关的方面

[0111] 图5A示出了详细描述根据某些方面的用于确定与接收机有关的位置信息、并在接收机处控制对该位置信息的访问的网络过程的图示。在描述图5A中示出的过程的同时参考图2。本领域的技术人员将理解的是，图5A中示出的过程流是示意性的，并且不意图将本公开限制到图5A中示出的阶段顺序。因此，阶段可以被移除和重排，并且未示出的其他阶段可以被执行，这落入本公开的范围和精神内。

[0112] 在阶段501，定位系统240可以创建并维护用于由接收机对位置信息的控制访问的信息。例如，定位系统240可以创建空中链路证书(ALAC)(也称为“系统级密钥/证书”)和未授权的服务水平证书(ASLC)，其未来由UE 220使用以在使用该位置信息之前、基于由ASLC

针对接收机上已请求位置信息的特定应用规定的限制，来对从网络(例如，从服务提供方230和/或定位系统240)接收的信息进行解密。在阶段502，创建的ALAC和ASLC被提供至制造商210，并且在阶段503，该制造商210向UE 220提供ALAC/ASLC(例如，通过将它们映像在固件中)。

[0113] 在阶段504(例如，在用户购买UE 220之后)，UE 220发起应用或发起紧急911呼叫。在步骤504之前，尽管未显式示出，应用可以被下载到UE 220。在与应用相关联的ASLC已经由制造商提供的情况下，阶段505不是必须的。否则，UE 220向网络发送与应用相关联的开发商密钥。开发商密钥的路由可以通过服务提供方230、定位系统240和/或应用的开发商，如外部实体250(路由未示出)。在接收并验证开发商密钥之后，网络则可以向UE 220传送针对该应用的ASLC，该UE 220之后可以存储该ASLC。

[0114] 在阶段506，UE 220从网络取得位置信息。所述位置信息可以从在定位系统240发起的广播信号获取，和/或可以通过服务提供方230获取。类似地，UE 220可以请求位置信息，或者监控位置信息的广播。

[0115] 在阶段507-508，UE 220可以使用ALAC(例如，与广播位置信息的发射机相关联的ALAC)和与接收机上请求位置信息的应用相关联的ASLC来对位置信息进行解密。

[0116] 在阶段509-510，解密的位置信息被处理，以及与UE 220的位置有关的定位信息被确定(例如，在位置引擎处)。

[0117] 在911呼叫的情况下，在阶段511-512，位置信息、定位信息和/或用于确定位置的信息(例如，伪距和关于计算其伪距的发射机的信息)被传送至服务提供方230和/或作为外部实体250运行的PSAP。否则，在阶段512，针对基于LBS的应用，定位信息可以保持在UE 220处，以执行基于位置的服务，和/或可以被传送至作为外部实体运行的LBS实体，用于辅助基于来自LBS实体的服务的定位的提供。针对E-911呼叫的另一替换是接收机向服务器发送加密分组和原始TOA信息。加密分组可以在服务器处被解密，以提取计算位置解所需的信息。

[0118] 图5B使出了用于描述与网络应用或E-911事务有关的位置信息的过程。注意的是，ASLC可以用于或不用于E911事务。例如，如果ASLC用于E-911呼叫，特定的ASLC可以被建立，以用于具有最高服务水平并且没有有效期的紧急呼叫。

[0119] 图6示出了详细描述根据某些方面的用于在接收机处提供对位置信息的条件访问的过程的图示。在描述图6中示出的过程的同时参考图2和图4A-C。

[0120] 如之前描述的，加密的定位信号数据可以被传送至接收机(例如，图4A-图4C的接收机400)。对定位信号数据进行加密有助于防护其到授权的接收机的传输，以及在授权的接收机处的使用。然而，假定带宽约束并对接收机处的处理功率进行限制，鲁棒的加密技术可能不可行。因此，加密必须保护传送的数据，同时最小地使用数据/分组空间，并且不需要在接收机处的显著的解密，该接收机典型地不具有在短时段执行鲁棒解密的处理能力。

[0121] 其他加密可以用于基于各种参数(例如，与应用相关联的支付的有效性、当前用户位置、由用户或应用的位置请求的固定数量是否已经被超出、可以访问位置信息的时段、等等)来防护由授权的应用和用户对位置信息的使用。控制位置信息到某些应用的分发、同时限制由其他应用对该位置信息的访问的该第二层加密和解密是这里描述的各种实施方式的重要特征，因为其允许网络运营商、载体、应用供应商/开发商或图2中示出的其他实体将位置信息的分发货币化。此外，第二层加密和解密使由未授权的用户(例如，黑客)为了获得

对位置信息的访问以用于未授权的应用的各种潜在尝试无效。

[0122] 图6示出了与一个方面相关联的解密的两个阶段。本领域的技术人员将理解图6中落入本公开的范围和精神的变形。在阶段610，接收机发起第一应用(例如，自动地响应于一些预定义的条件、响应于用户输入)。之后，接收机确定于第一应用相关联的ASLC的副本是否存储在接收机的存储器(例如，图4A-C的存储器430)中。如果副本存在，接收机被“提供”有ASLC，并且运行阶段630。否则，接收机“不被提供”，并且运行阶段620。

[0123] 在阶段620，接收机从网络获取ASLC的副本。图7详细描述了阶段620的子阶段。本领域的技术人员将理解的是，阶段620可以在图6中示出的其他阶段之后被执行(例如，在阶段660之前的任意阶段之后)。

[0124] 在阶段630，加密的定位信号从网络到达接收机。定位信号可以由发射机广播，或者可以通过其他通信路径(例如，蜂窝路径、基于网络的路径、局域网络路径)到达。在阶段640，接收机开始处理定位信号。与阶段640相关联的子阶段在图8中示出。

[0125] 在阶段650，定位信号到达第一密码组件422，在该第一密码组件422处，使用存储在存储器430中的ALAC的副本来解密该定位信号。之后，在阶段660，来自解密的定位信号的位置数据中的一些或所有由第二密码组件423使用与第一应用相关联的ASLC来解密。ASLC可以从存储器430中取得，或者从网络中取得(如结合阶段620和图7所描述的)。

[0126] 最后，在阶段670，位置引擎440可以接收解密的位置数据和位置TOA或伪距信息，以代替第一应用计算接收机的位置。位置的计算可以基于由针对第一应用的ASLC指示的服务水平来确定。

[0127] 图7示出了详细描述根据某些方面和图6的阶段620的用于在接收机处提供条件访问证书的过程的图示。在描述图7中示出的过程的同时参考图2。

[0128] 在阶段710，UE 220取得与应用相关联的开发商密钥。该开发商密钥可以在应用下载到UE 220上之后被存储在UE 220上。开发商密钥与ASLC的关联可以存储在网络(例如，服务提供方230、定位系统240或外部实体250)处。ASLC不仅可以特定于应用，还可以特定于UE 220的访问水平。在阶段720，开发商密钥被传送至网络进行处理(例如，传送至服务提供方230、定位系统240、和/或开发商或应用提供方250)。

[0129] 在阶段730，响应于传送开发商密钥，UE 220/接收机400通过网络接收与开发商密钥/应用有关的ASLC。在阶段740，ASLC可以被存储以便未来使用。可替换地，ASLC可以不被存储，以使阶段710到730在下次应用请求定位信息时重复(在图6中示出的以及这里任何地方描述的两阶段解密模型下，其要求与应用相关联的ASLC)。

[0130] 图8示出了详细描述根据某些方面和图6的阶段640的用于处理定位信号数据的过程的图示。在描述图8中示出的过程的同时参考图4A-C。例如，阶段640可以由图4A-C中的信号处理组件421来执行。

[0131] 在阶段810，通过RF组件410从发射机接收的定位信号可以用于估计原始TOA(例如，在数字处理组件421a处)。之后，原始TOA估计可以在伪距生成组件421b处被转换成原始定位伪距信息。

[0132] 在阶段820，定位信号可以在数据处理组件421c处被解码。在阶段830，数据处理组件421c可以在将定位信息发送到第一密码组件422以进行解码之前，对该定位信号执行误差检测。

[0133] 图11示出了解密的第一阶段、加密的第二阶段、以及解码的第三阶段。本领域的技术人员将理解图11中落入本公开的范围和精神内的变形。图11中描绘的某些阶段可以在其他实施中被重排或省略。下面的讨论通常涉及接收机，然而，该讨论能够扩展到一个或多个用于执行下面指定的功能中的一些或所有的处理器。

[0134] 在阶段1110，发起第一应用(例如，自动地响应于一些预定义的条件、响应于用户输入、或者响应于另一事件或情况)。应用可以在接收机处发起，或者在位于接收机远程的服务器处发起，或者在其他设备处发起。接收机可以采用各种形式，包括在图4B-C中示出的那些。

[0135] 在阶段1120，接收机获取与第一应用相关联的ASLC的副本。接收机可以从在该接收机的存储器、从第一应用、或从外部源获取ASLC。ASLC可以规定参数，该参数确定何种信息能够被提供到第一应用/由第一应用访问，以及其何时及如何能够被提供/由第一应用访问，等等其他条件。对使用ASLC的替换选择被考虑，包括仅使用ASLC中的数据而不使用证书。

[0136] 在阶段1130，加密的定位信息从发射机到达接收机。定位信号中的每个可以被从各自的发射机广播，并且可以通过其他通信路径(例如，蜂窝路径、基于网络的路径、局域网路径、或全部)到达。

[0137] 在阶段1140，接收机开始处理定位信号。

[0138] 在阶段1150，使用存储在接收机或可由接收机从外部源中访问的密钥(例如，由ALAC规定的密钥)来对定位信号进行解密。

[0139] 在阶段1160，接收机可以根据定位信号识别或确定位置信息。所述位置信息可以包括原始且精细的TOA测量、在这里任何地方描述的数据单元(DU)、估计的接收机的位置坐标(基于定位信号的数据来计算)、修改的位置坐标(基于估计的位置坐标或其他数据来确定)。修改的位置坐标可以基于来自阶段1120的参数来确定。所述参数可以指示应用被允许接收估计的位置坐标的预定义的精度水平(例如，距离)内的位置坐标。在这种情况下，处理器可以基于精度水平来创建新的位置坐标(例如，改变纬度，使其落入距离估计的纬度的x个测量单元的范围内，将幅度改变为0，使仅提供两个维度)。提供不太精确的位置信息可以使能以每个应用或每个使用为基础的订阅服务。

[0140] 在阶段1170，可以使用由来自阶段1120的ASLC或其数据规定的、或基于所述ASLC或其数据生成的密钥来对位置信息中的一者或所有进行加密。用于加密的位置信息的选择可以受由ASLC规定的服务水平条件来控制。所述服务水平条件可以指定哪些数据能够由第一应用访问，并且可以根据这里任何地方描述的数据(包括参考图9描述的数据中的一些或所有)来确定。

[0141] 在阶段1180，加密的位置信息被解密，以供第一应用使用。运行第一应用的处理器可以具有关于用于对位置信息进行加密的密钥的先知。该先知可以通过访问ASLC来获得(例如，在ASLC规定了密钥或用于确定密钥的算法的情况下)，或者通过接收密钥来获得(例如，在使用会话标识符的情况下)。

[0142] 与数据有关的方面

[0143] 图9示出了根据某些方面用于在条件访问过程期间使用的数据。如图所示，数据可以标识或表示应用类型(例如，E-911、LBS、网络管理、执法)、UE ID或UE类型、服务类型(例

如，使用精度、使用范围、使用时间、可用的数据单元)、服务提供方类型、制造商类型、开发商类型、用户ID或用户类型、请求类型、或可以用作确定应用的服务水平的参数的其他类型的信息，所述应用的服务水平决定哪种位置信息能够被提供至该应用、该位置信息何时能够被提供、该位置信息如何能够被提供以及该位置能够在哪儿被提供。GPS或其他时间也可以被传送以基于时间限制监控使用。该数据中的一些或所有可以被合并到针对特定应用和/或UE的ASLC中，并且可以未来由处理组件访问，以识别能够在发送至位于接收机本地或接收机外部(即，远程)的应用之前被加密的位置信息。每个数据可以由接收机上的处理器使用，以在将特定解密的位置信息以加密的形式提供至应用、设备或用户之前，对该特定的位置信息进行过滤。换句话说，该数据决定何种位置信息可用、其何时可用、其持续多久可用。ASLC还可以包括加密密钥或用于创建加密密钥的算法(例如，用于使用实时数据、或可以在保护的环境中分发的或在加密和解密阶段期间变得可用的其他数据来创建加密密钥的算法)。

[0144] 服务类型可以与多达三维中的精度水平有关，包括高范围精度(例如，3米)、中范围精度(25-50米)、以及低范围精度(400米)。服务类型还可以与覆盖水平有关，包括本地化、区域化、全国及全球等等。服务类型还可以与有效时间水平有关，该有效时间水平涉及按一次、每月、每年或终身、等等其他有效周期的访问权限的期满。服务类型还可以与使用水平有关，包括计量的和未限制的。可以使用水平的各种组合。

[0145] 对非蜂窝设备的定位应用的相似的解密也被考虑。例如，通过VoIP应用(例如，Skype™)的E-911呼叫、照相机/摄像机等等，其能够具有被映像到它们的固件或被下载到存储器中的ASLC。

[0146] 与使用情况有关的方面

[0147] 各种类型的计算设备及其联接状态被考虑，包括几乎总是连接、经常连接、或很少连接(极少连接)到蜂窝网络、定位网络、局域网或其他网络的设备。对这些计算设备中的每个的处理能力给出其他考虑。

[0148] 连接的类型包括蜂窝(例如，3G/4G，预付费的)、Wi-Fi、有线(例如，USB、以太网)以及其他连接。

[0149] 计算设备的类型包括智能手机、其他蜂窝电话、平板电脑、膝上型计算机、互联TV、VoIP电话、STB、DMA、应用、安全系统、PGD、PND、DSC、M2M应用、资产的地理围栏等等。连接的接收机是诸如具有可用的活动数据通道(例如，蜂窝和Wi-Fi/有线以太网)的手机、平板电脑及膝上型计算机之类的设备。总是连接的接收机是诸如具有对非蜂窝装置的接入(例如，Wi-Fi/有线以太网)的平板电脑和膝上型计算机之类的设备。未连接的接收机或者具有有限的连接性的接收机包括很少(极少)连接至因特网、并且没有蜂窝连接的接收机。

[0150] 考虑的是，未连接的接收机可以被制造有预授权的ALAC和ASLC集，其被编程用于接收机的终身。超过其初始周期的密钥更新能够经由固件更新被传输到设备(例如，使用USB连接)，或者通过临时将设备与数据网络连接来被传输。这种未连接的接收机能够使用合适的RF接收机来确定其位置，该RF接收机接收加密的位置信息(例如，GPS芯片)。

[0151] 附加方面

[0152] 一个或多个方面可以涉及用于控制由一个或多个应用对位置信息的访问的系统、方法、装置和计算机程序产品。系统可以包括用于实施方法的处理组件。计算机程序产品可

以包括具有在其中编码的计算机可读程序代码的非暂态性计算机可用介质，所述程序代码被适配成被运行以实施方法。

[0153] 方法步骤可以包括：使用第一密钥对从陆地发射机的网络接收的加密位置信号的第一集合进行解密；根据解密位置信号的第一集合确定位置信息；识别所述位置信息的第一集合，其中，所述位置信息的所述第一集合基于与第一应用相关联的第一服务水平来被识别；使用第二密钥对所述位置信息的所述第一集合进行加密；以及向所述第一应用提供加密的所述位置信息的第一集合。

[0154] 根据一些方面，所述位置信息的所述第一集合包括以下中的至少一者：来自所述陆地发射机的网络的一个或多个发射机的位置坐标、定时校正、以及大气测量。

[0155] 根据一些方面，所述方法步骤还可以包括：使用所述解密位置信号来计算接收机的位置的估计坐标，其中，所述位置信息的所述第一集合包括所述接收机的所述估计坐标。

[0156] 根据一些方面，所述解密位置信号包括规定在所述陆地发射机中的每个陆地发射机处的大气测量的数据，其中，所述估计坐标包括在所述接收机处使用所述解密位置信号和至少一个大气测量计算的幅度坐标。

[0157] 根据一些方面，所述方法步骤还可以包括：使用所述解密位置信号计算接收机的位置的估计坐标；以及基于针对所述第一应用准许的精度水平，计算修正坐标，该修正坐标基于所述估计坐标，其中，所述修正坐标在指定所述接收机的所述位置方面比所述估计坐标精度低，并且其中，所述位置信息的所述第一集合包括所述修正坐标。

[0158] 根据一些方面，所述方法步骤还可以包括：识别所述位置信息的第二集合，其中，所述位置信息的所述第二集合基于与第二应用相关联的第二服务水平来被识别，其中，包括在所述第一集合中的特定位置信息不包括在所述第二集合中；使用第三密钥对所述位置信息的所述第二集合进行加密；以及向所述第二应用提供所述位置信息的所述第二集合。

[0159] 根据一些方面，所述方法步骤还可以包括：使用所述第一密钥或第三密钥对从所述陆地发射机的网络接收的加密位置信号的第二集合进行解密，其中，所述加密位置信号的第一集合在所述接收机的第一位置处被接收，以及所述加密位置信号的第二集合在所述接收机的第二位置处被接收；根据所述解密位置信号的第二集合确定附加的位置信息；识别所述附加的位置信息的第二集合，其中，所述附加的位置信息的所述第二集合基于与第二应用相关联的第二服务水平来被识别；使用第四密钥对所述位置信息的所述第二集合进行加密；以及向所述第二应用提供所述位置信息的所述第二集合。

[0160] 根据一些方面，所述方法步骤还可以包括：在识别所述位置信息的所述第一集合之前，确定规定所述第一服务水平的信息是否存储在所述接收机上；一旦确定规定所述第一服务水平的所述信息未被存储在所述接收机上，访问与所述第一应用相关联的第一开发商密钥；向服务器发送所述第一开发商密钥；以及响应于向所述服务器发送所述第一开发商密钥，接收规定所述第一服务水平的所述信息。

[0161] 根据一些方面，规定所述第一服务水平的所述信息包括在与所述第一应用相关联的第一授权的服务水平证书中，并且其中，所述证书与所述开发商密钥相关联。

[0162] 根据一些方面，所述第一服务水平规定所述第二密钥能够用于对所述位置信息的所述第一集合以及任意后续的位置信息的任意后续的集合进行加密的时段。

[0163] 根据一些方面，所述第二密钥是在所述位置信号被解密之后生成的会话密钥。

[0164] 根据一些方面，第一应用在远程服务器上运行，并且所述位置信息的所述第一集合被提供至所述远程服务器。

[0165] 根据一些方面，所述方法步骤还可以包括：基于在与所述第一应用相关联的第一证书中规定的参数来确定所述第一服务水平。

[0166] 根据一些方面，所述方法步骤还可以包括：在通过未保护的通信路径发送所述位置信息之前，对所述位置信息进行加扰；以及在识别所述第一集合之前，对加扰的位置信息进行解扰。

[0167] 根据一些方面，所述方法步骤还可以包括：在通过未保护的通信路径发送所述估计坐标之前，对所述估计坐标进行加扰；以及在对所述第一集合进行加密之前，对加扰的估计坐标进行解扰。

[0168] 根据一些方面，所述方法步骤还可以包括：从多个密钥中选择所述第一密钥，其中，所述加密位置信号的CRC字段仅在所述第一密钥用于对所述加密位置信号的第一集合进行解密时通过校验。

[0169] 根据一些方面，所述方法步骤还可以包括：从多个密钥中选择所述第一密钥，其中，所述解密位置信号的数据仅在所述第一密钥用于对所述加密位置信号的第一集合进行解密时匹配期望的值范围。

[0170] 根据一些方面，所述方法步骤还可以包括：从多个密钥中选择所述第一密钥，其中，来自所述多个发射机的所述分组数据仅在所述第一密钥用于对所述加密位置信号的第一集合进行解密时通过一个或多个相关性校验，其中，所述加密位置信号的第一集合包括来自多个发射机的分组数据。

[0171] 其他方面

[0172] 关于本公开的各种特征的其他公开在以下伴同转让(co-assigned)的专利申请中描述，出于任何以及所有目的，所述专利申请的全部内容通过引用合并于此：于2012年3月5日提交的、序列号为13/412,487、题为WIDE AREA POSITIONING SYSTEMS的美国实用新型专利申请；于2009年9月10日提交的、序列号为12/557,479、题为WIDE AREA POSITIONING SYSTEM的美国实用新型专利(现在是美国专利No.8,130,141)；于2012年3月5日提交的、序列号为13/412,508、题为WIDE AREA POSITIONING SYSTEM的美国实用新型专利申请；于2011年11月14日提交的、序列号为13/296,067、题为WIDE AREA POSITIONING SYSTEM的美国实用新型专利申请；于2011年6月28日提交的、序列号为PCT/US12/44452、题为WIDE AREA POSITIONING SYSTEM的申请；于2012年6月28日提交的、序列号为13/535,626、题为CODING IN WIDE AREA POSITIONING SYSTEMS的美国专利申请；于2012年6月28日提交的、序列号为13/536,051、题为CODING IN WIDE AREA POSITIONING SYSTEM(WAPS)的美国专利申请；于2012年8月2日提交的、序列号为13/565,614、题为Cell Organization and Transmission Schemes in a Wide Area Positioning System(WAPS)的美国专利申请；于2012年8月2日提交的、序列号为13/565,732、题为Cell Organization and Transmission Schemes in a Wide Area Positioning System的美国专利申请；于2012年8月2日提交的、序列号为13/565,723、题为Cell Organization and Transmission Schemes in a Wide Area Positioning System的美国专利申请；于2013年3月14日提交的、序列号为13/831,740、题为Systems and Methods Configured to Estimate Receiver Position Using Timing

Data Associated with Reference Locations in Three-Dimensional Space的美国专利申请;于2013年6月4日提交的、序列号为13/909,977、题为SYSTEMS AND METHODS FOR LOCATION POSITIONING of USER DEVICE的美国专利申请;于2013年8月26日提交的、序列号为14/010,437、题为SYSTEMS AND METHODS FOR PROVIDING CONDITIONAL ACCESS TO TRANSMITTED INFORMATION的美国专利申请;于2013年8月27日提交的、序列号为14/011,277、题为METHODS AND APPARATUS FOR PSEUDO-RANDOM CODING IN A WIDE AREA POSITIONING SYSTEM(WAPS)的美国专利申请。这里,上述申请、公布及专利可以被单独地或统称为“合并的参考文献”、“合并的申请”、“合并的公布”、“合并的专利”,或者另外指定。这里公开的各种方面、细节、设备、系统和方法可以与合并的参考文献中的任意参考文献中的公开合并。

[0173] 这里描述的系统和方法可以追踪位置计算设备或其他事物,以为或向这些设备和事物提供位置信息和导航,注意的是,术语“GPS”可以指任何全球导航卫星系统(GNSS),例如,GLONASS、伽利略、和罗盘/北斗。发射机可以在由用户设备接收的信号中传送定位数据。定位数据可以包括能够用于确定信号的传播时间的“定时数据”(例如,到达时间(TOA)),其能够用于通过将信号的传播时间乘以信号的速度,来估计用户设备与发射机之间的距离(例如,伪距)。

[0174] GPS接收机的各种架构被考虑。例如,GPS接收机的逻辑功能能够分为两个部分:(1)信号处理,以及(2)位置计算。信号处理功能可以在硬件中实施,以及位置计算可以在固件/软件中实施。这些功能可以在具有DSP硬件块和管理DSP硬件并计算位置的ARM处理器子系统的GPS ASIC“芯片”上执行。这种GPS芯片典型地生成为NMEA消息形式的最终的纬度、经度和幅度。可替换地,位置计算可以在位于手持设备上的应用处理器上执行,以增加附加的定位信息,并建立全面的位置解决方案。这里,本公开可以用于全部实施(除了用于处理信号和计算位置的其他配置之外)。

[0175] 这里描述的各种示意性系统、方法、逻辑特征、块、模块、组件、电路及算法步骤可以由本领域公知的或未来发展的合适的硬件来实施、执行或控制,或者通过由处理器(也称为“处理设备”,并且也包括任何数量的处理器)运行的软件来实施、执行或控制,或者通过两者来实施、执行或控制。处理器可以执行或导致以下中的任意一者:处理、计算、方法步骤,或者与这里公开的过程/方法及系统有关的其他系统功能,包括数据的分析、处理、转换或创建,或者其他关于数据的操作。处理器可以包括通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其他可编程逻辑设备、离散门或晶体管逻辑、离散硬件组件、服务器、或上述的任意组合。处理器可以是常规处理器、微处理器、控制器、微控制器或状态机。处理器还能够指代芯片,其中,该芯片包括各种组件(例如,微处理器和其他组件)。术语“处理器”可以指代一个、两个货更多个相同类型或不同类型的处理器。注意的是,术语“计算机”或“计算设备”或“用户设备”等可以指代包括处理器的设备,或者可以指代处理器本身。软件可以位于RAM存储器、闪存、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可移除磁盘、CD-ROM、或任何其他形式的存储介质中。“存储器”可以与处理器耦合,以使处理器能够从存储器中读取信息,以及向该存储器中写入信息。存储介质可以与处理器集成。软件可以存储在计算机可读介质上,或者编码为计算机可读介质上的一个或多个指令或代码。计算机可读媒介可以是任意可用的存储媒介,包括非易失性媒

介(例如,光学半导体、磁性半导体),以及使用网络传输协议通过无线、光学、或有线信令媒介在网络上传输数据和指令的载波。这里描述的系统和方法的方面可以被实施为可编程到多个电路中的任意电路中的功能性。方面可以在处理器中被具体化,该处理器具有基于软件的电路仿真、离散门、定制设备、神经逻辑、量子设备、PLD、FPGA、PAL、ASIC、MOSFET、CMOS、ECL、聚合物工艺、混合模拟和数据、以及上述的混合。在整个上面的描述中提及的数据、指令、命令、信息、信号、比特、码元以及芯片可以由电压、电流、电磁波、磁场或粒子、光场或粒子、或上述的任意组合来标示。计算网络可以用于执行方面,并且可以包括硬件组件(服务器、监视器、I/O、网络连接)。应用程序可以通过接收、转换、处理、存储、取得、传输和/或输出数据来执行方面,所述数据可以存储在分层数据源、网络数据源、关系型数据源、非关系型数据源、面向对象的数据源、或其他数据源中。"数据"和"信息"可以交换使用。术语"包括"、"包含"、"包括"、"包含"等应当以与排外含义(即,只由这些组成)相反的包含含义(即,不限于)来理解。使用单数或复数的词语还分别包括多数或单数。词语"或者"或"以及"涵盖列表中的任意项以及所有项。"一些"以及"任意"和"至少一者"指代一个或多个。术语"设备"可以包括一个或多个组件(例如,处理器、存储器、屏幕)。术语"模块"、"块"、"特征"或"组件"可以指代硬件或软件,或者硬件和软件这二者的组合,所述硬件和软件被配置成执行或实现与那些模块、块、特征或组件相关联的功能。类似地,示出为矩形的系统及装置附图中的特征可以指代硬件或软件。注意的是,连接两种所述特征的线可以表示那些特征之间的数据传递。这种传递可以直接在那些特征之间进行,或者通过中间特征进行(尽管未示出)。在没有线连接两个特征的情况下,考虑那些特征之间的数据传递,除非另有表述。因此,线被提供以表示某些方面,但不应当被解释为限制。

[0176] 本公开不意图被限制于这里示出的方面,而是应当被给予由本领域的技术人员的最宽范围的理解,包括等价的系统及方法。给予本发明的保护应当仅根据以下权利要求书来限制。

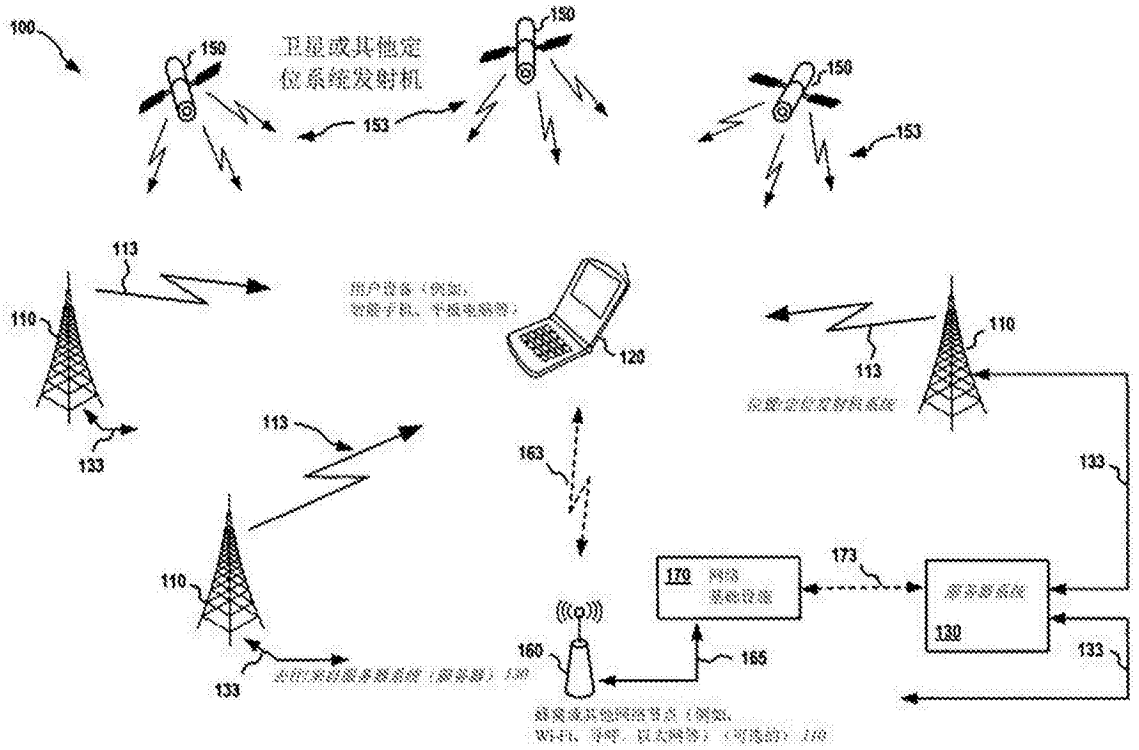

100
150
卫星或其他定位系统发射机
153
113
110
133
120
163
160
165
170
173
130

图1

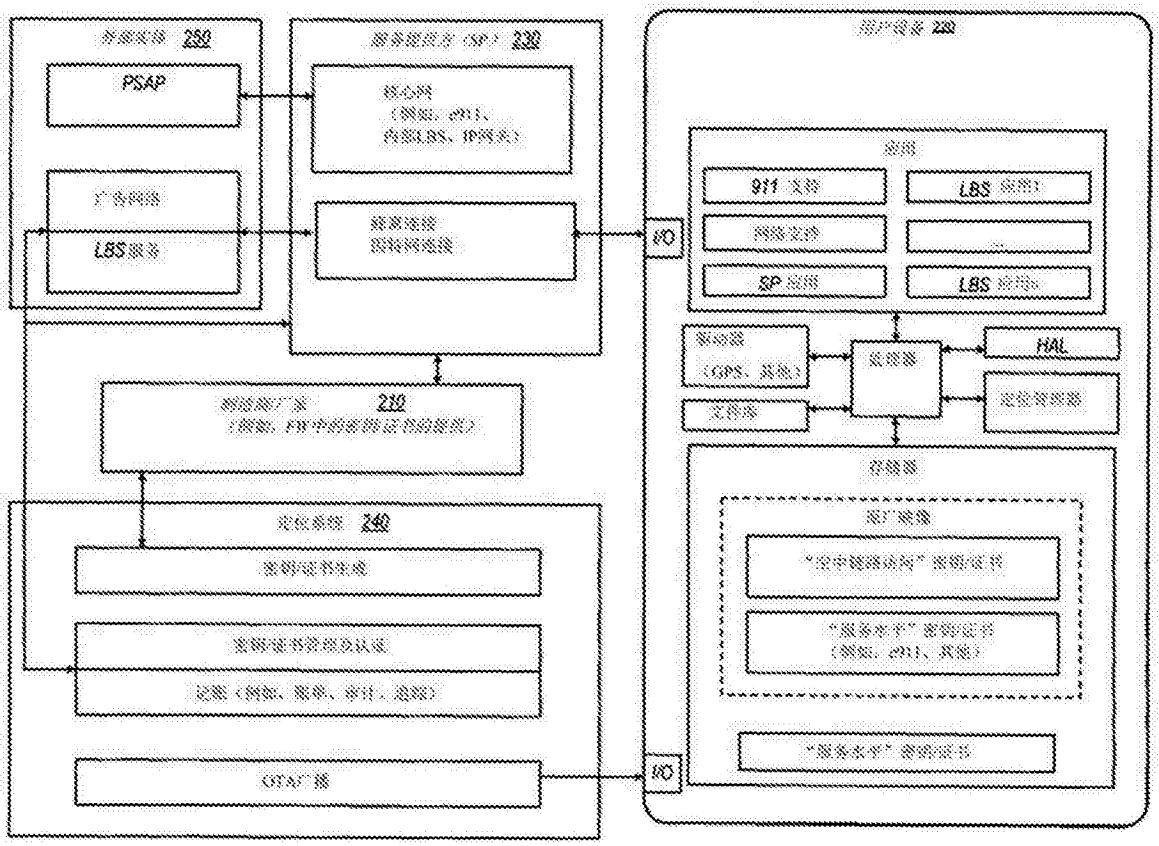

250
PSAP
LBS服务
230
210
240
OTA广播
280
911 支持
SIM
HAL

图2

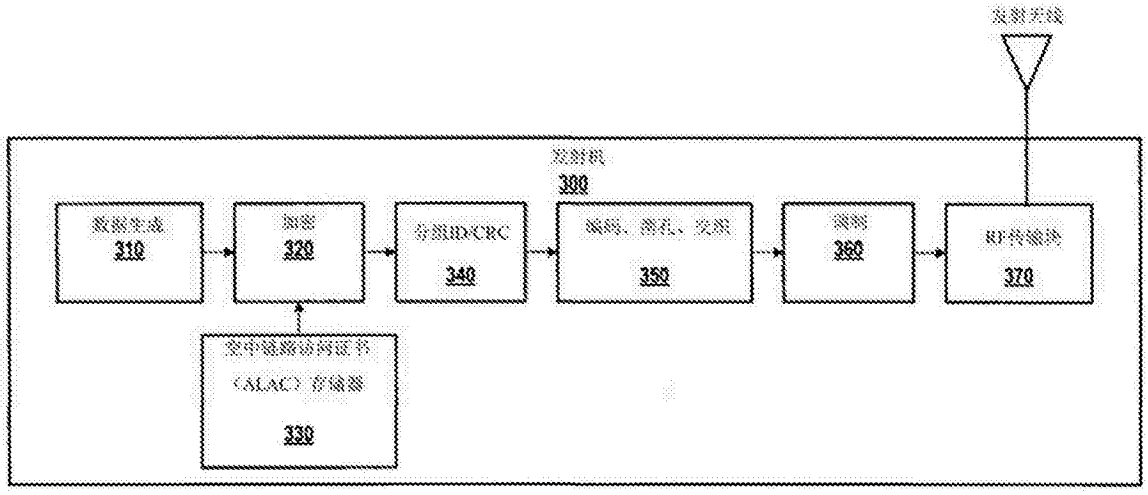

发射天线
发射机
300
310
320
340
350
360
370
330

图3

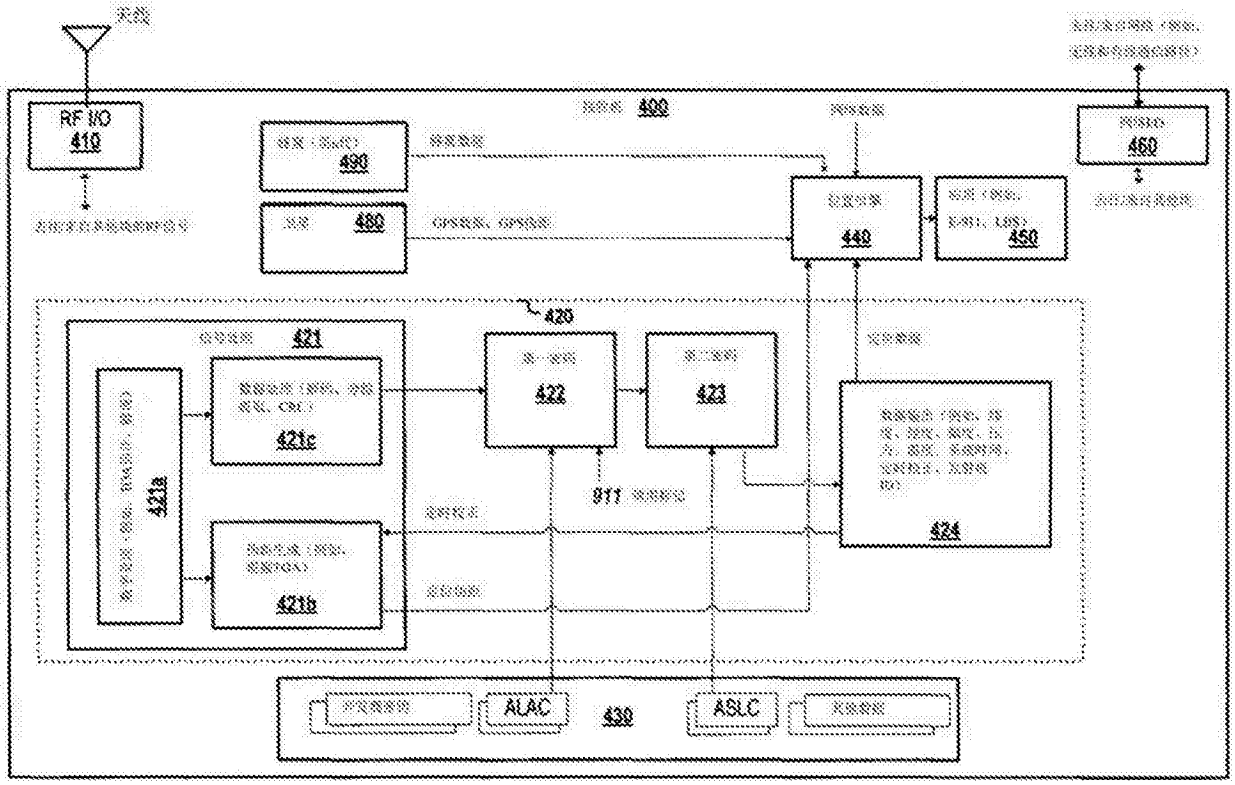

RF I/O
410
400
490
480
440
460
450
420
421
421c
421a
421b
422
423
424
AUAC
430
ASLC

图4A

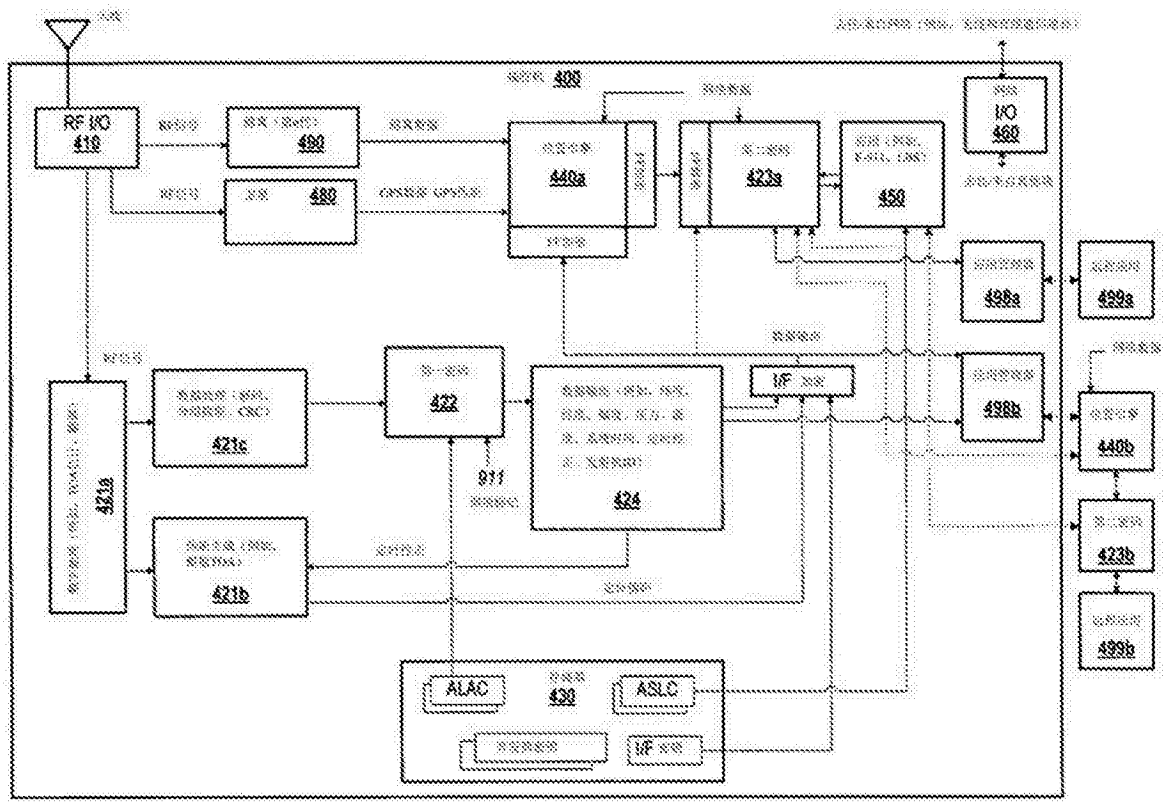

RF I/O
410
480
440a
423a
450
I/O
460
498a
499a
498b
440b
423b
499b
422
424
421c
421b
421a
911
IF
ALAC
430
ASLC

图4B

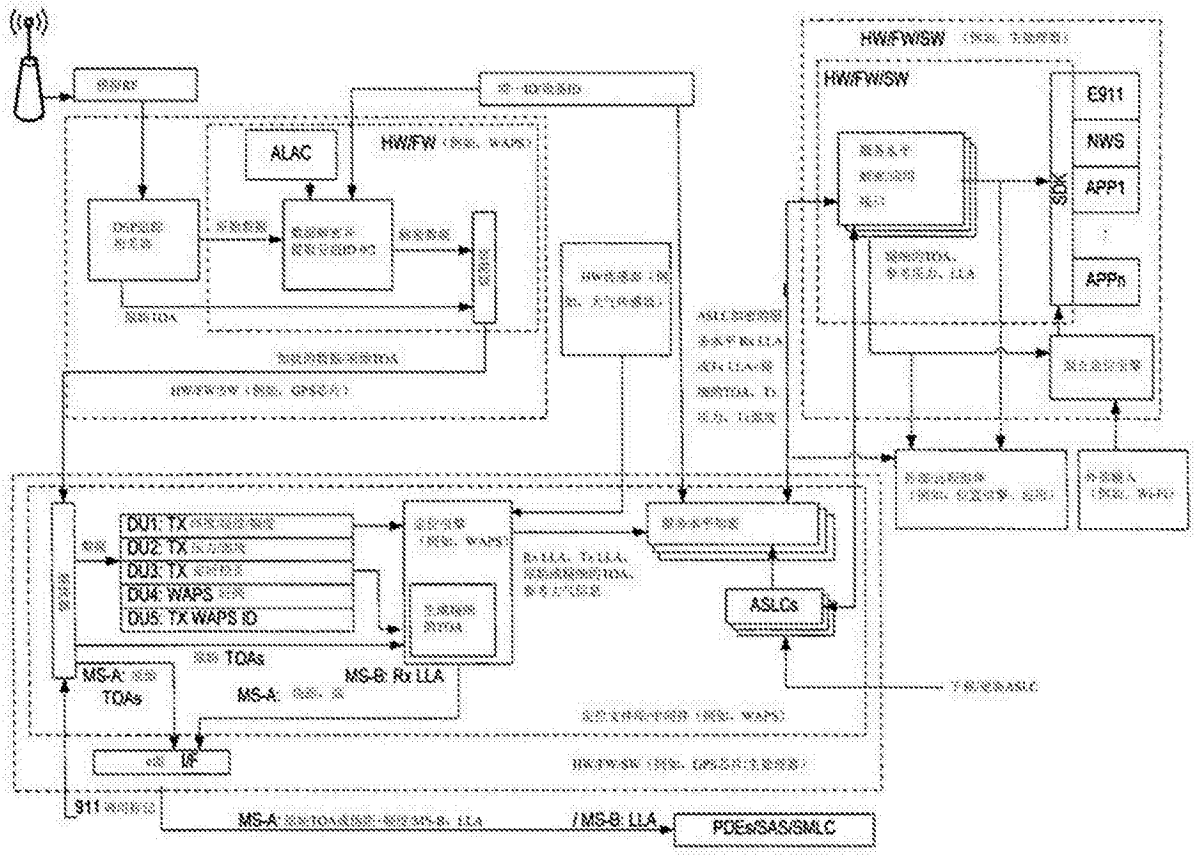

HW/FW/SW
HW/FW/SW
E911
NWS
APP1
APPn
SDK
ALAC
HW/FW
DU1: TX
DU2: TX
DU3: TX
DU4: WAPS
DU5: TX WAPS ID
TDAs
MS-A:
TDAs
MS-B: Rx LLA
MS-A:
ASLCs
IP
911
MS-A:
/MS-B: LLA
PDEs/SAS/GMLC

图4C

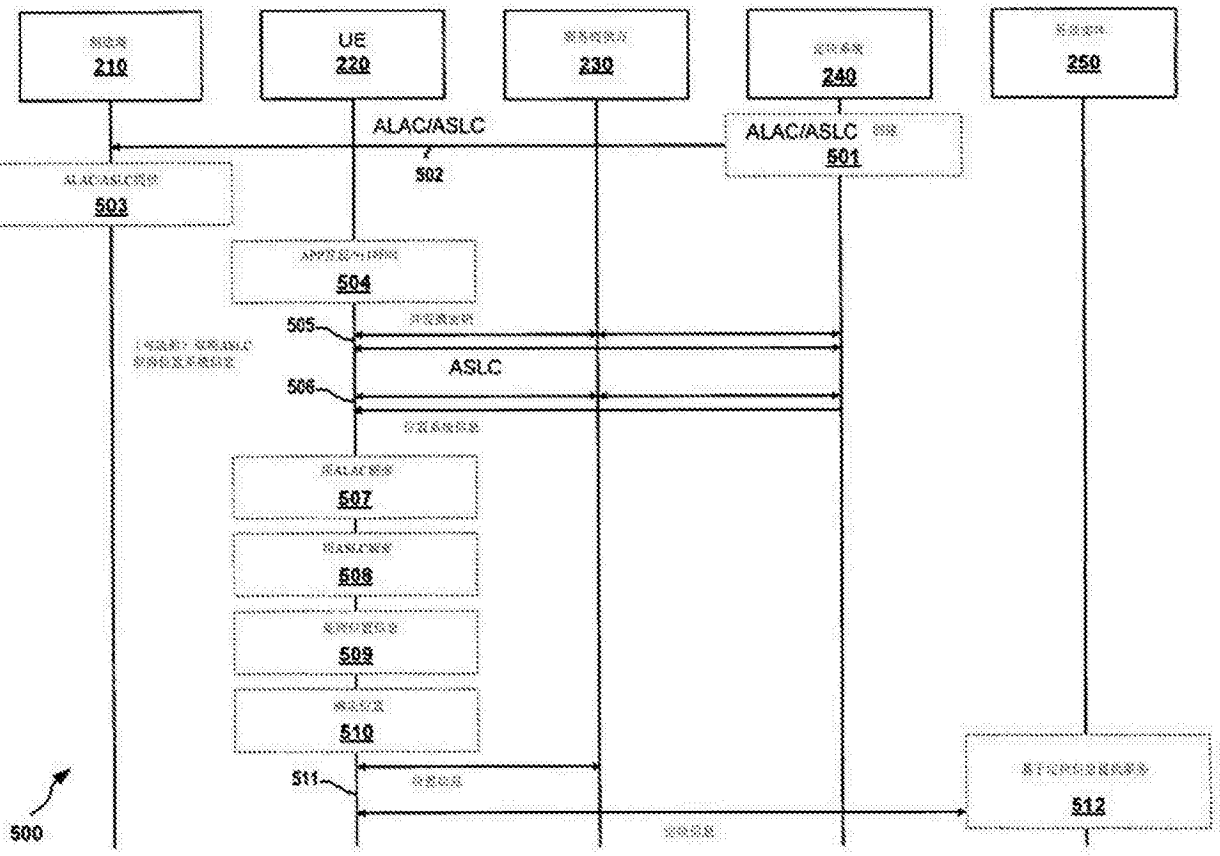

UE
220
230
240
250
ALAC/ASLC
ALAC/ASLC
501
502
503
504
505
ASLC
506
507
508
509
510
511
512
500

图5A

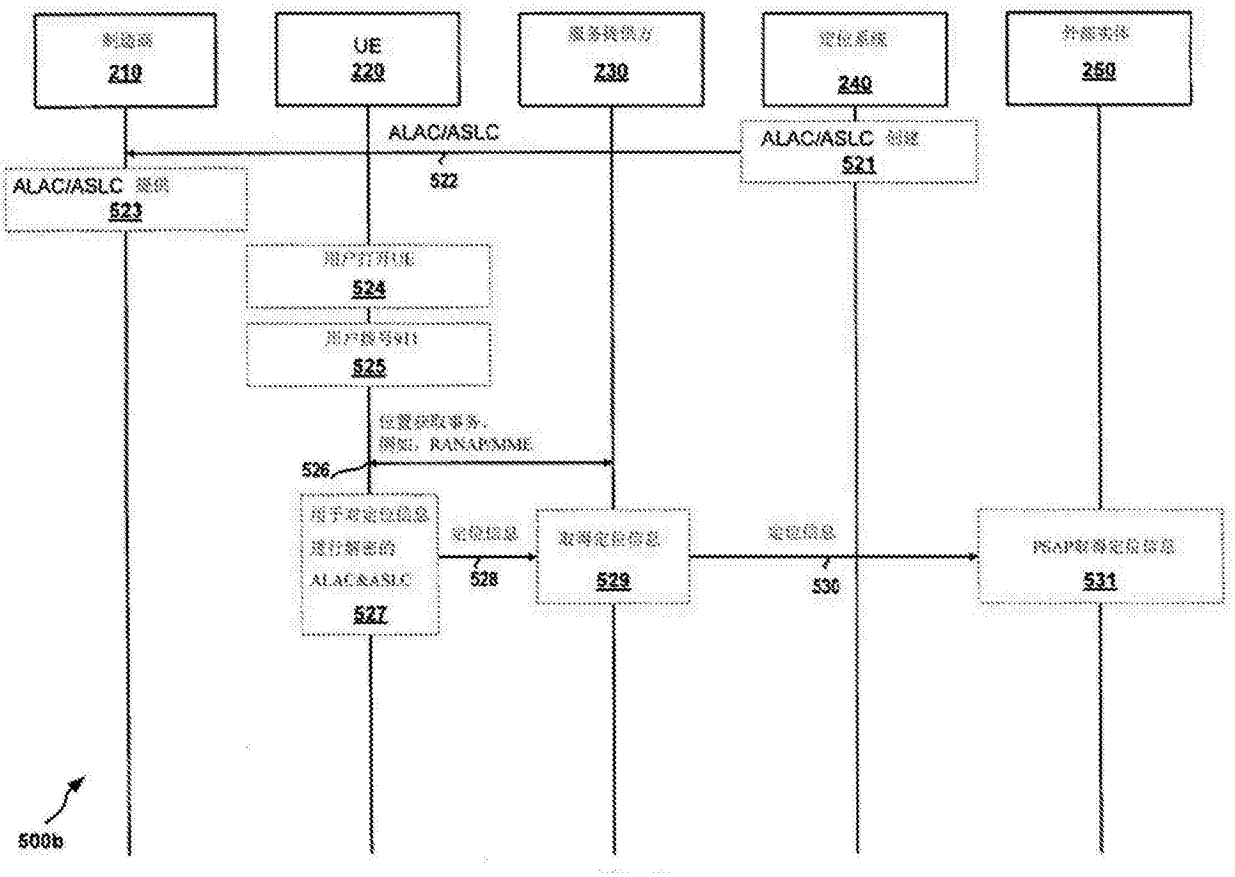

UE
220
239
240
260
ALAC/ASLC
522
ALAC/ASLC
521
ALAC/ASLC
523
524
525
526
527
528
529
530
531
500b

图5B

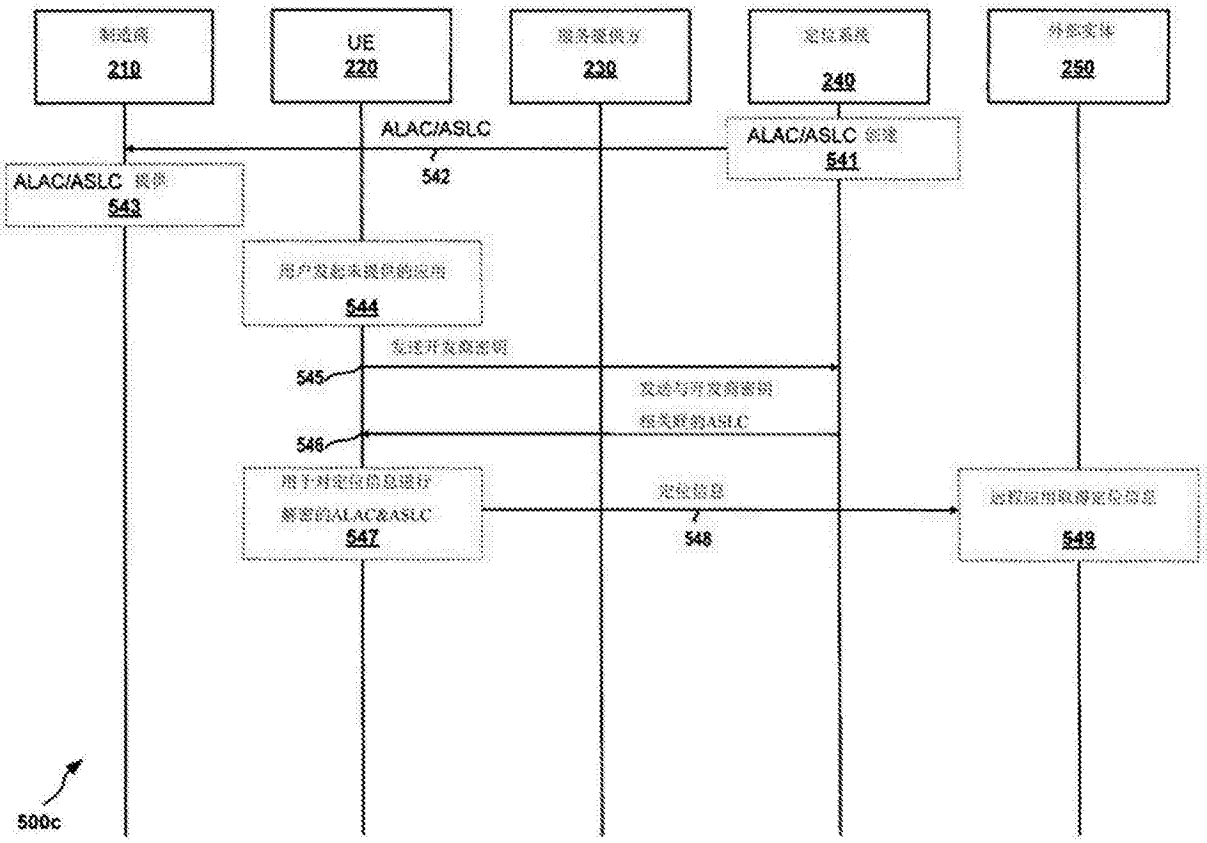


图5C

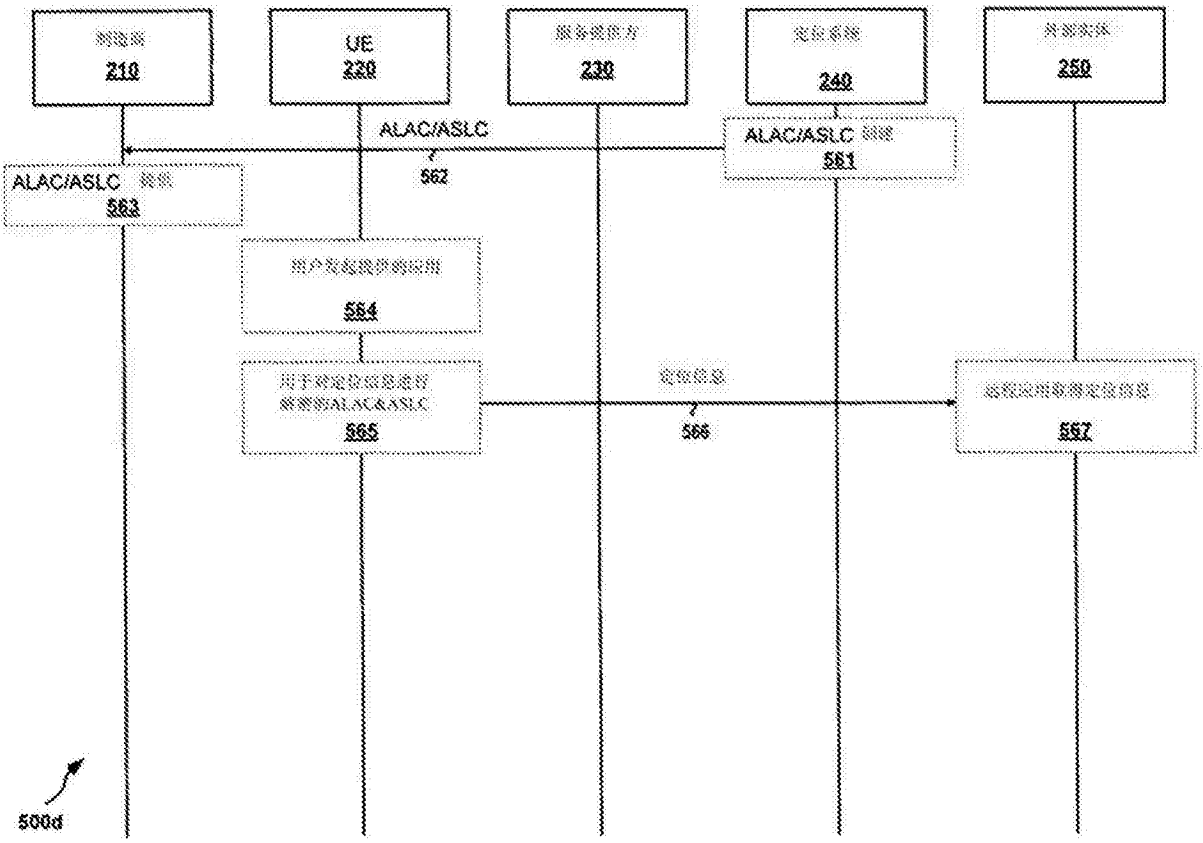

210
UE
220
230
240
250
ALAC/ASLC
562
ALAC/ASLC
563
ALAC/ASLC
561
564
565
566
567
500d

图5D

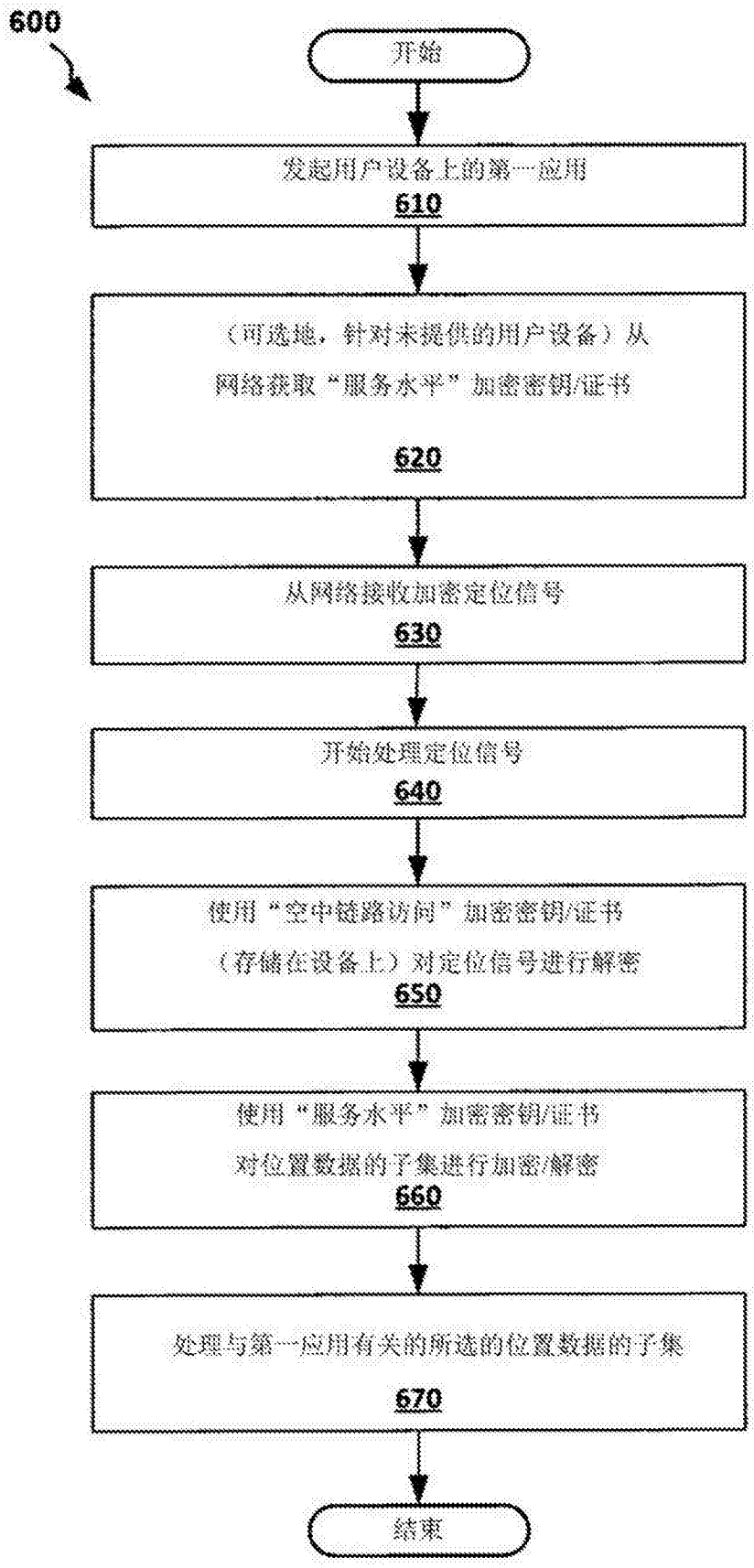

600
开始
发起用户设备上的第一应用
610
（可选地，针对未提供的用户设备）从
网络获取“服务水平”加密密钥/证书
620
从网络接收加密定位信号
630
开始处理定位信号
640
使用“空中链路访问”加密密钥/证书
（存储在设备上）对定位信号进行解密
650
使用“服务水平”加密密钥/证书
对位置数据的子集进行加密/解密
660
处理与第一应用有关的所选的位置数据的子集
670
结束

图6

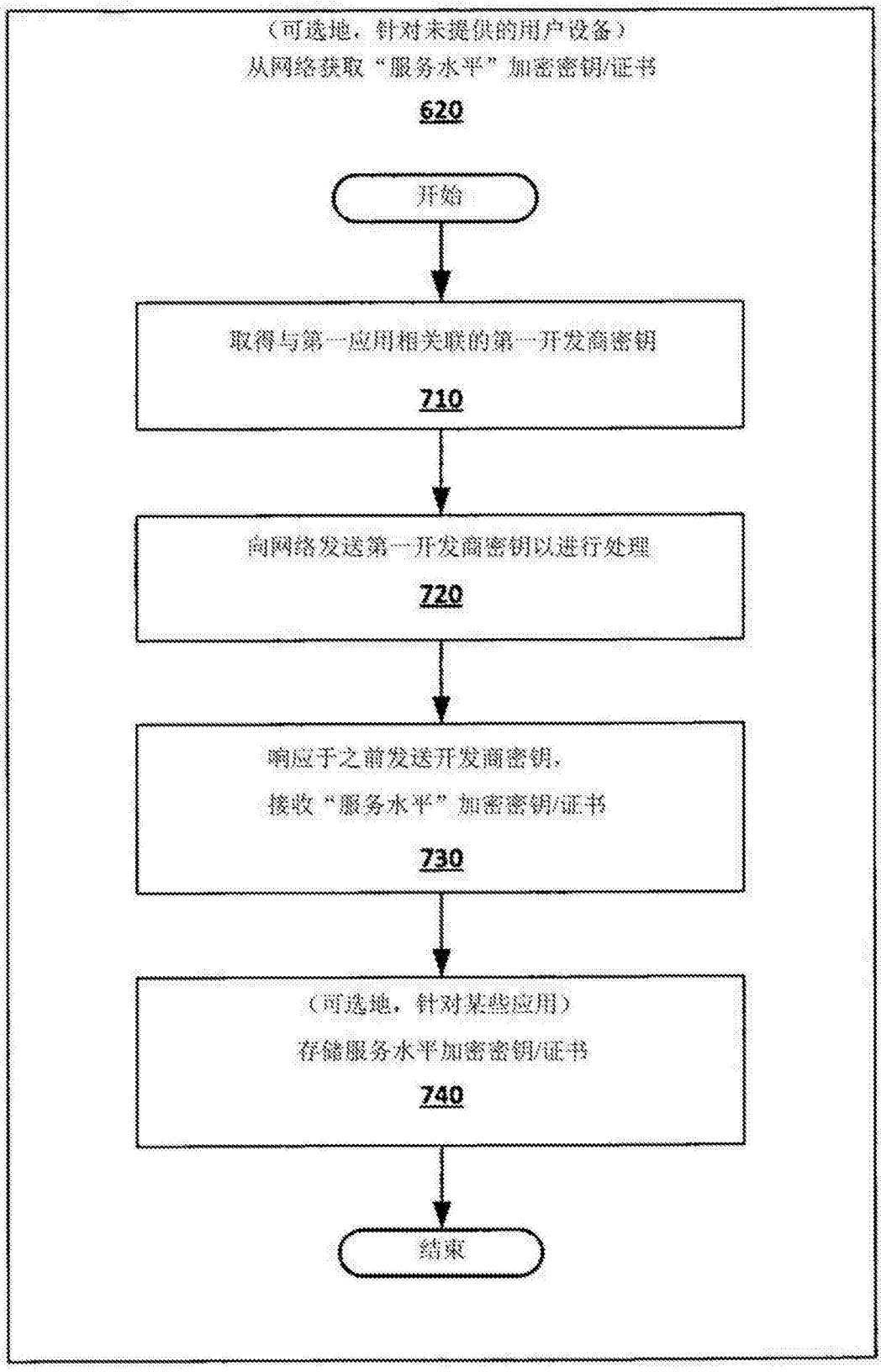

（可选地，针对未提供的用户设备）
从网络获取“服务水平”加密密钥/证书
620
开始
取得与第一应用相关联的第一开发商密钥
710
向网络发送第一开发商密钥以进行处理
720
响应于之前发送开发商密钥，
接收“服务水平”加密密钥/证书
730
（可选地，针对某些应用）
存储服务水平加密密钥/证书
740
结束

图7

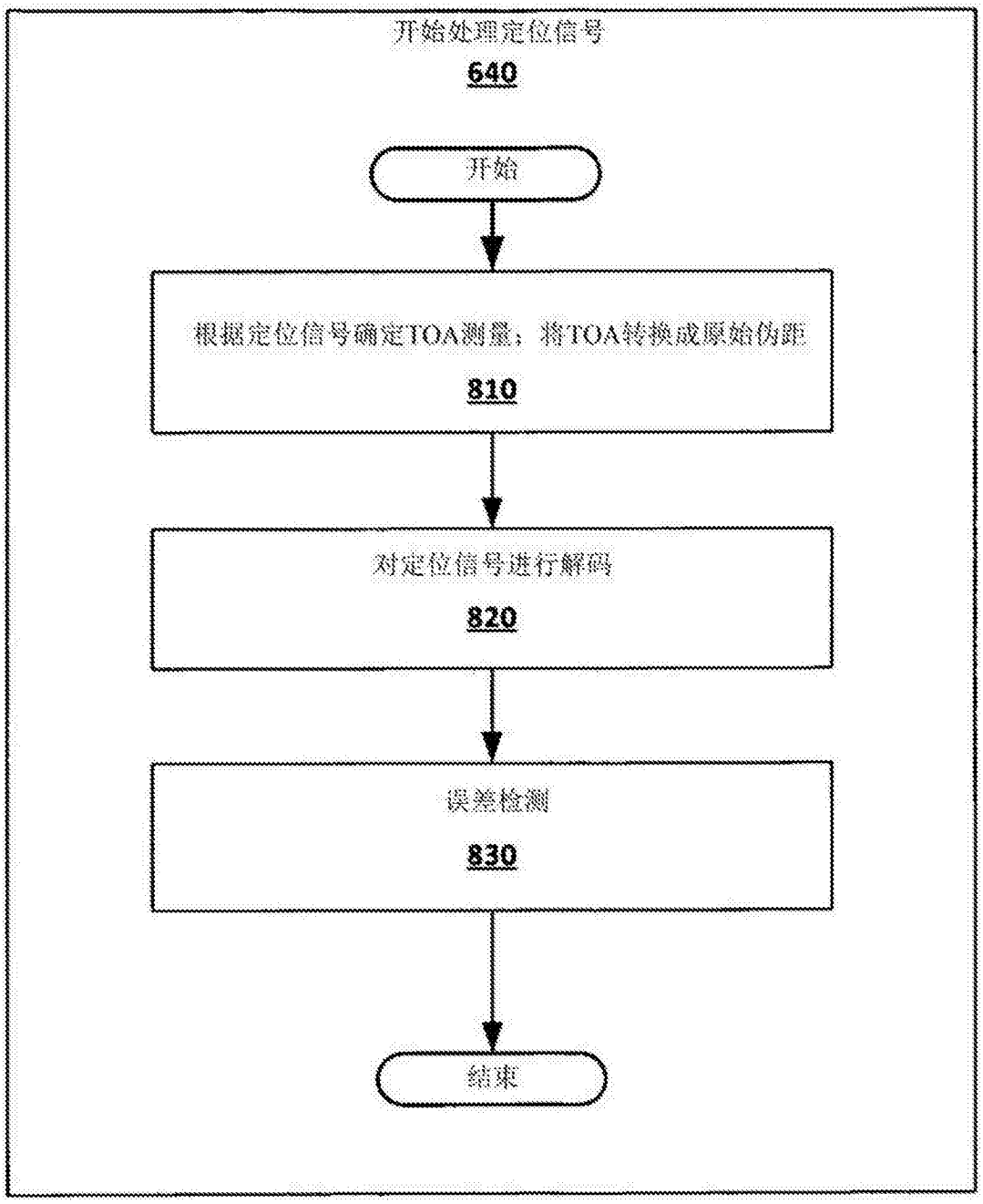

开始处理定位信号
640
开始
根据定位信号确定TOA测量，将TOA转换成原始伪距
810
对定位信号进行解码
820
误差检测
830
结束

图8

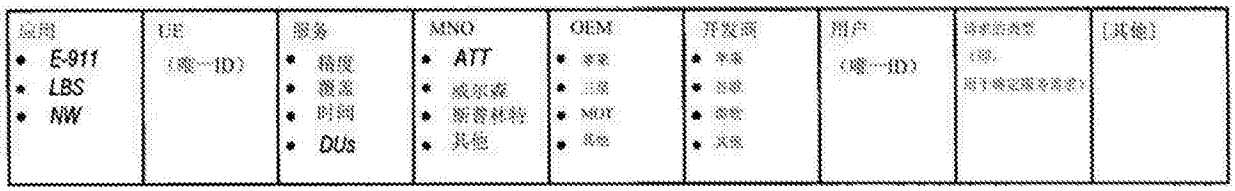

应用
E-911
LBS
NW
UE
（唯一ID）
服务
MNO
ATT
OEM
开发商
用户
（唯一ID）
[其他]

图9

图10A

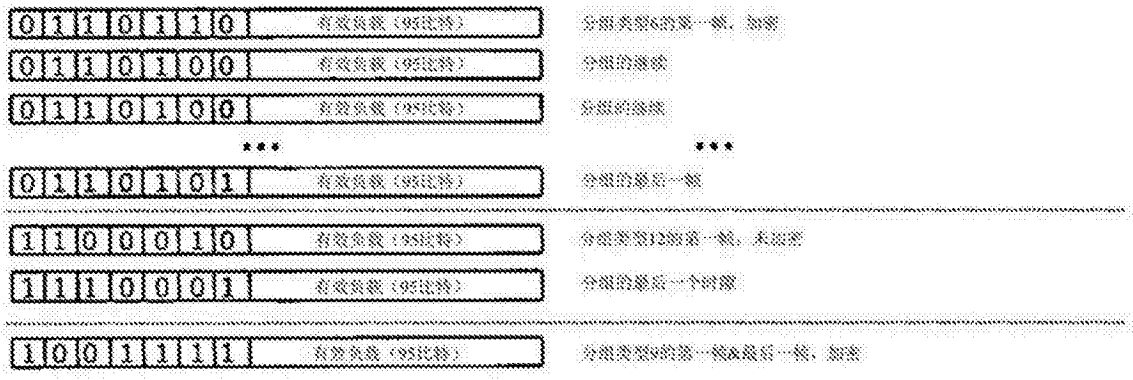


图10B

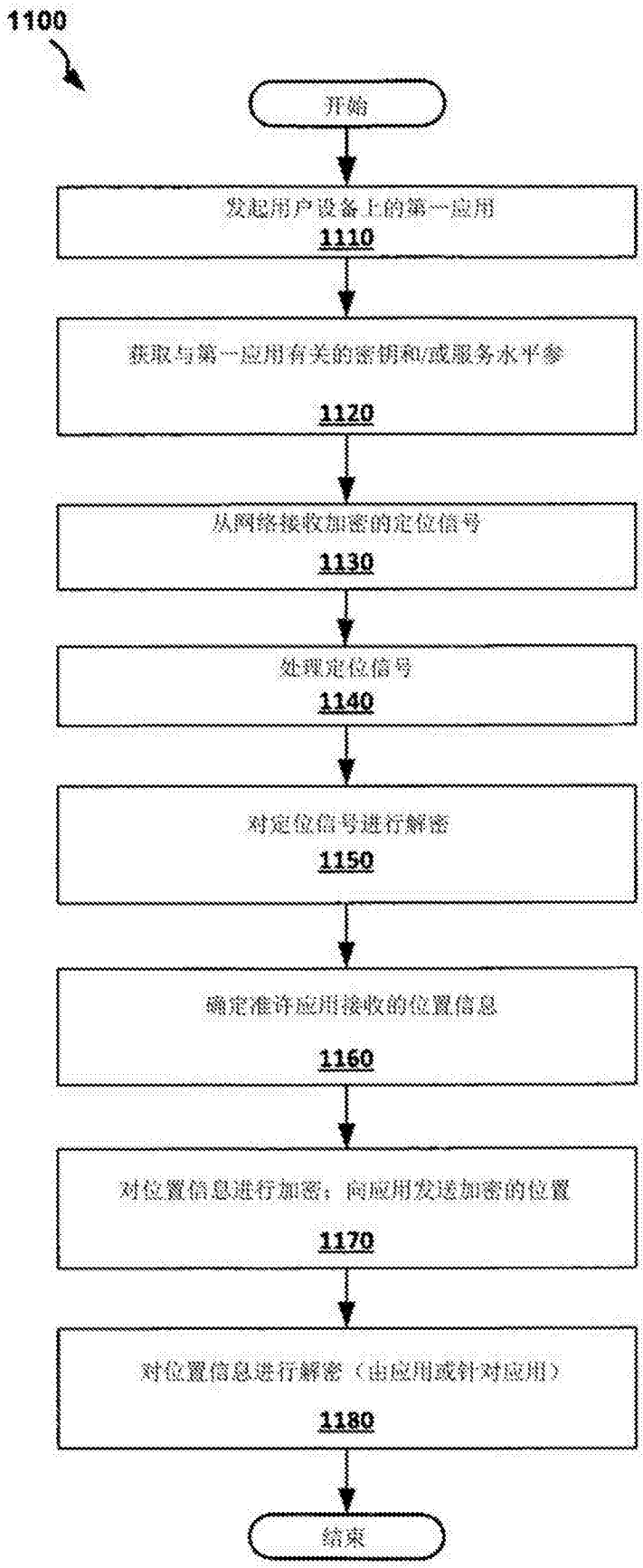

1100
开始
发起用户设备上的第一应用
1110
获取与第一应用有关的密钥和/或服务水平参
1120
从网络接收加密的定位信号
1130
处理定位信号
1140
对定位信号进行解密
1150
确定准许应用接收的位置信息
1160
对位置信息进行加密，向应用发送加密的位置
1170
对位置信息进行解密（由应用或针对应用）
1180
结束

图11