(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
20 March 2014 (20.03.2014)

WIPO | PCT

(10) **International Publication Number**
WO 2014/043147 A9

(51) **International Patent Classification**:
H04L 29/08 (2006.01)

(21) **International Application Number**:
PCT/US2013/059102

(22) **International Filing Date**:
10 September 2013 (10.09.2013)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:

61/699,800	11 September 2012 (11.09.2012)	US
14/010,437	26 August 2013 (26.08.2013)	US
14/023,427	10 September 2013 (10.09.2013)	US

(71) **Applicant**: **NEXTNAV LLC** [US/US]; 484 Oakmead Parkway, Sunnyvale, California 94085 (US).

(72) **Inventors**: **VAJJHALA, Varaprasad**; 235 Atheana Ct, San Ramon, California 94582 (US). **JOSEPH, Deepak**; 3856 Inverness Rd, Fairfax, Virginia 22033 (US). **MEIYAPPAN, Subramanian**; 1720 Fumia Drive, San Jose, California 95131 (US). **RAGHUPATHY, Arun**; No. 14E, Asset Gardenia Enclave, Ramagondanahalli, Whitefield, Bangalore 560066 (IN).

(74) **Agent**: **PENDERGRASS, Kyle**; 1645 Emerald Street, 2M, San Diego, California 92109 (US).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

[Continued on next page]

(54) **Title**: SYSTEM AND METHOD FOR PROVIDING CONDITIONAL ACCESS TO TRANSMITTED INFORMATION

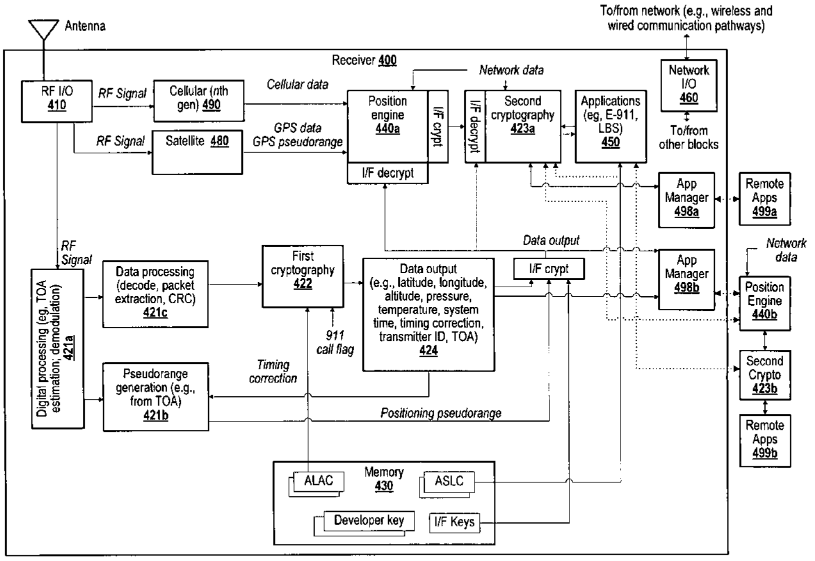


FIG. 4B

(57) **Abstract**: This disclosure relates to systems, methods, computer program products, and means that control access to position information at a receiver, or at another device external to the receiver, based on various considerations, including a requested service type, a user type, a device type, a software application type, a payment, and/or other characteristics associated with a particular software application or distributor of that software application. The disclosure further relates to systems, methods, computer program products and means for carrying out secure data transmissions intended for a particular application among other applications.

— *with information concerning authorization of rectification of an obvious mistake under Rule 91.3 (b) (Rule 48.2(i))*

(48) Date of publication of this corrected version:
9 October 2014

(15) Information about Correction:
see Notice of 9 October 2014

SYSTEMS AND METHODS FOR PROVIDING CONDITIONAL ACCESS TO TRANSMITTED INFORMATION

FIELD

[0001] This disclosure relates generally to positioning systems and methods. More specifically, but not exclusively, the disclosure relates to systems and methods for controlling access to position information.

BACKGROUND

[0002] Systems for providing position information are known in the art. For example, radio-based systems such as LORAN, GPS, GLONASS, and the like have been used to provide position information for persons, vehicles, equipment, and the like. These systems do, however, have limitations associated with factors such as location accuracy, transmitted and received signal levels, radio channel interference and/or channel problems such as multipath, device power consumption, and the like.

[0003] Determination of a mobile subscriber's exact location can be quite challenging. If the subscriber is indoors or in an urban area with obstructions, the subscriber's mobile device may not be able to receive signals from GPS satellites and the network may be forced to rely on network-based triangulation/multilateration methods that are less precise. Additionally, if the subscriber is in a multi-story building, knowing only that the subscriber is in the building and not what floor they are on, will result in delays in providing emergency assistance (which could be potentially life-threatening). Clearly, a system that can assist the subscriber's computing device (e.g., a mobile computing device) in speeding up the location determination process, provide more accuracy (including vertical information), and solve some of the challenges of location determination in urban areas and inside buildings is needed.

[0004] Moreover, position information transmitted in systems like GPS is readily available to various devices without any option to regulate which device may have access to the position information, or more particularly, which software application on the device may use the position information. Such lack of regulation may place bandwidth burdens on network operators where many applications across many devices are transmitting position information through the network to third party services that are associated with those applications.

Having an ability to regulate use of position information would further allow network operators to maintain better levels of service for its customers while reducing unnecessary bandwidth use. Moreover, providing greater control to network operators would permit per monetization at the application level or service level for each user device or each user of a user device. Accordingly, there is a need for improved positioning systems to address these and/or other problems with existing positioning systems and devices.

SUMMARY

[0005] Systems, methods and computer program products comprising a computer usable medium having a computer readable program code embodied therein that is adapted to be executed to implement a method for providing conditional access to position information for a computing device are described. For example, certain aspects of this disclosure relate to a system, method, computer program product and means for controlling access to position information by one or more applications. The system, method, computer program product and means may decrypt, using a first key, a first set of encrypted position signals received from a network of terrestrial transmitters. The system, method, computer program product and means may further determine position information from the first set of decrypted position signals, and identify a first set of the position information, where the first set of the position information is identified based on a first level of service associated with a first application. The system, method, computer program product and means may further encrypt the first set of the position information using a second key, and provide the encrypted first set of the position information to the first application. Various additional aspects, features, and functions are described below in conjunction with the appended Drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Attention is turned to the drawings and detailed description.

[0007] FIG. 1 depicts a diagram illustrating details of a terrestrial location/positioning system on which embodiments may be implemented;

[0008] FIG. 2 illustrates a diagram illustrating certain details of one embodiment of a terrestrial location/positioning system on which embodiments may be implemented;

[0009] FIG. 3 depicts a diagram of a transmitter/beacon;

[0010] FIG. 4A depicts a diagram illustrating details of one embodiment of a receiver;

[0011] FIG. 4B depicts a diagram illustrating details of one embodiment of a receiver/user device and other components external to the receiver/user device;

[0012] FIG. 4C depicts a diagram illustrating details of another embodiment of a receiver and other components external to the receiver/user device;

[0013] FIG. 5A illustrates a process for determining position information relating to a receiver and controlling access to that position information at the receiver;

[0014] FIG. 5B illustrates a process for distributing position information for E-911 calls;

[0015] FIG. 5C illustrates a process for un-provisioned keys;

[0016] FIG. 5D illustrates a process for pre-provisioned keys;

[0017] FIG. 6 illustrates a process for providing conditional access to position information;

[0018] FIG. 7 illustrates a process for provisioning conditional access certificates;

[0019] FIG. 8 illustrates a process for processing position information;

[0020] FIG. 9 illustrates types of data for use during a conditional access process;

[0021] FIG. 10A illustrates a packet structure;

[0022] FIG. 10B illustrates a series of bits for use in accordance with certain aspects; and

[0023] FIG. 11 illustrates a process for providing conditional access to position information at a receiver/user device.

DETAILED DESCRIPTION

[0024] Various aspects of the disclosure are described below. It should be apparent that the teachings herein may be embodied in a wide variety of forms and that any specific structure, function, or both, being disclosed herein is merely representative. Based on the teachings herein one skilled in the art should appreciate that any aspect disclosed may be implemented independently of any other aspects and that two or more of these aspects may be combined in various ways. For example, a system may be implemented or a method may be practiced using any number of the aspects set forth herein.

[0025] As used herein, the term "exemplary" means serving as an example, instance or illustration. Any aspect and/or embodiment described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other aspects and/or embodiments.

Overview

[0026] This disclosure relates generally to positioning systems and methods for providing signaling for position determination and determining high accuracy position/location information using a wide area transmitter array in communication with receivers (also interchangeably referred to herein as user devices, user terminals/UEs, or similar terms) such as in cellular phones or other portable devices. Positioning signaling services associated with certain aspects may utilize broadcast-only beacons/transmitters that are configured to transmit encrypted positioning signals. Receivers having an appropriate chipset may be able to receive and use the positioning signals based on air-link access authentication techniques, including authentication by way of decrypting the position signals using a stored copy of an air-link access certificate (ALAC) during an initial decryption stage. Once decrypted with the ALAC during the initial decryption stage, the receiver may provide, to a software application operating on the receiver, conditional access to the position information based on an additional decryption stage using an authorized service level certificate (ASLC) associated with that particular software application.

[0027] Various components within a receiver may be used to carry out the decryption stages. For example, decryption of the broadcast signal may occur at a GPS chip in conjunction with ALACs that are provisioned into firmware of a secure hardware area (e.g., in the GPS chip). By comparison, decryption of the position information using the ASLC may occur at another chip (e.g., a receiver's processor) in conjunction with an ASLC that is not provisioned in firmware (e.g., accessible via a different level of software). Of course, one of skill in the art will appreciate alternative configurations.

[0028] Once decrypted, the position information may be processed by a processor (e.g., a positioning engine) in order to compute various positioning signal data units such as Latitude, Longitude and Altitude to varying degrees of accuracy. Examples of altitude computations are provided in United States Utility Patent Application Serial No. 13/296,067, entitled WIDE AREA POSITIONING SYSTEMS, filed November 14, 2011, which is incorporated herein by reference.

[0029] The two-stage decryption of position information at the receiver offers several advantages over prior art. For instance, aspects of the two-stage decryption enable the transmitter and/or the receiver to provide positioning signals to authorized receivers and/or authorized software applications (hereafter referred to as "applications") while denying access to unauthorized receivers and unauthorized applications. Similarly, access to the position information may be controlled based on the user requesting access, or other types of considerations.

[0030] Controlling access to position information based on authorization permits a carrier and application developers to offer tiered levels of service that may be purchased based on different business agreements. Tier levels may relate to levels of accuracy, coverage areas, duration of validity, amounts of use, periods of use, or other considerations.

[0031] The two-stage decryption of position information at the receiver also decreases the likelihood that an unauthorized user (e.g., a hacker) can gain access to and use the positioning information, thereby causing loss of revenue.

[0032] Achievement of the above advantages must be balanced against performance requirements of the positioning system. According to certain aspects, the encryption and decryption stages performed in the system may not compromise system performance metrics such as Time to First Fix (TTFF) of a receiver's position and accuracy of any position fix. Additionally, processing associated with the various conditional access methodologies described herein may be limited based on processing power of particular receivers, which may preclude process-intensive cryptographic procedures.

[0033] According to other aspects, the conditional access feature may be available on various device platforms and may support the delivery models identified in the use cases described herein. Other aspects may involve factory-based or consumer-based provisioning of a receiver (in addition to any re-provisioning) to support the conditional access methodologies described herein. By way of example, various provisioning embodiments are described herein. Importantly, any of the conditional access processes described herein must comply with any E-911 functional requirements.

[0034] Various additional aspects, features, and functions are described below in conjunction with the appended Drawings. While the details of the embodiments of the disclosure may vary and still be within the scope of the claimed disclosure, one of skill in the art will appreciate that the Drawings described herein are not intended to suggest any limitation as to the scope of use or functionality of the inventive aspects. Neither should the Drawings and their description be interpreted as having any dependency or requirement relating to any one or combination of components illustrated in those Drawings.

[0035] In the following description, numerous specific details are introduced to provide a thorough understanding of, and enabling description for, the systems and methods described. One skilled in the relevant art, however, will recognize that these embodiments can be practiced without one or more of the specific details, or with other components, systems, and the like. In other instances, well-known structures or operations are not shown, or are not described in detail, to avoid obscuring aspects of the disclosed embodiments.

System Aspects

[0036] **FIG. 1** offers a diagram illustrating details of an example location/positioning system 100 on which various embodiments may be implemented. Positioning system 100, also referred to herein as a Wide Area Positioning System (WAPS), or "system" for brevity, includes a network of synchronized beacons (also denoted herein as "transmitters"), which are typically terrestrial, as well as user devices (also denoted herein as "receiver units" or "receivers" for brevity) configured to acquire and track signals provided from the beacons and/or other position signaling, such as may be provided by a satellite system such as the Global Positioning System (GPS) and/or other satellite or terrestrially based position systems. The receivers may optionally include a location computation engine to determine position/location information from signals received from the beacons and/or satellite systems, and the system 100 may further include a server system in communication with various other systems, such as the beacons, a network infrastructure, such as the Internet, cellular networks, wide or local area networks, and/or other networks. The server system may include various system-related information, such as an index of towers, a billing interface, one or more encryption algorithm processing component, which may be based on one or more proprietary encryption algorithms, a location computation engine, and/or other processing components to facilitate position, motion, and/or location determination for users of the system.

[0037] As shown in exemplary system 100, the beacons may be in the form of a plurality of transmitters 110, and the receiver units may be in the form of one or more user devices 120, which may be any of a variety of electronic communication devices configured to receive signaling from the transmitters 110, as well as optionally configured to receive GPS or other satellite system signaling, cellular signaling, Wi-Fi signaling, Wi-Max signaling, Bluetooth, Ethernet, and/or other data or information signaling as is known or developed in the art. The receiver units 120 may be in the form of a cellular or smart phone, a tablet device, a PDA, a notebook or other computer system, a digital camera, an asset tracking tag, and ankle bracelet, and/or similar or equivalent devices. In some embodiments, the receiver unit 120 may be a standalone location/positioning device configured solely or primarily to receive signals from the transmitters 110 and determine location/position based at least in part on the received signals. As described herein, receiver units 120 may also be denoted herein as “User Equipment” (UE), handsets, smart phones, tablets, and/or as a “receiver.”

[0038] The transmitters 110 (which may also be denoted herein as “towers”) are configured to send transmitter output signals to multiple receiver units 120 (a single receiver unit 120 is shown in **FIG. 1** for simplicity, however, a typical system will be configured to support many receiver units within a defined coverage area) via communication links 113 as shown. The transmitters 110 may also be connected to a server system 130 via communication links 133, and/or may have other communication connections (not shown) to a network infrastructure 170, such as via wired connections, cellular data connections, Wi-Fi, Wi-Max, or other wireless connections, and the like.

[0039] One or more receivers 120 may receive signaling from multiple transmitters 110 via corresponding communication links 113 from each of the transmitters 110. In addition, as shown in **FIG. 1**, a receiver 120 may also be configured to receive and/or send other signals, such as, for example, cellular network signals via communication link 163 from a cellular base station (also known as a NodeB, eNB, or base station), Wi-Fi network signals, Pager network signals, or other wired or wireless connection signaling, as well as satellite signaling via satellite communication links 153, such as from a GPS or other satellite positioning system. While the satellite positioning signaling shown in the exemplary embodiment of **FIG. 1** is shown as being provided from GPS system satellites 150, in other embodiments the signaling may be provided from other satellite systems and/or, in some embodiments, terrestrial-based wired or wireless positioning systems or other data communication systems.

[0040] In an exemplary embodiment, the transmitters 110 of system 100 are configured to operate in an exclusively licensed or shared licensed/unlicensed radio spectrum; however, some embodiments may be implemented to provide signaling in unlicensed shared spectrum. The transmitters 110 may transmit signaling in these various radio bands using novel signaling as is described subsequently herein. This signaling may be in the form of a proprietary signal configured to provide specific data in a defined format advantageous for location and navigation purposes. For example, as described subsequently herein, the signaling may be structured to be particularly advantageous for operation in obstructed environments, such as where traditional satellite position signaling is attenuated and/or impacted by reflections, multipath, and the like. In addition, the signaling may be configured to provide fast acquisition and position determination times to allow for quick location determination upon device power-on or location activation, reduced power consumption, and/or to provide other advantages.

[0041] Various embodiments of WAPS may be combined with other positioning systems to provide enhanced location and position determination. Alternately, or in addition, a WAPS system may be used to aid other positioning systems. In addition, information determined by receiver units 120 of WAPS systems may be provided via other communication network links 163, such as cellular, Wi-Fi, Pager, and the like, to report position and location information to a server system or systems 130, as well as to other networked systems existing on or coupled to network infrastructure 170. For example, in a cellular network, a cellular backhaul link 165 may be used to provide information from receiver units 120 to associated cellular carriers and/or others (not shown) via network infrastructure 170. This may be used to quickly and accurately locate the position of receiver 120 during an emergency, or may be used to provide location-based services or other functions from cellular carriers or other network users or systems.

[0042] It is noted that, in the context of this disclosure, a positioning system is one that localizes one or more of latitude, longitude, and altitude coordinates, which may also be described or illustrated in terms of one, two, or three dimensional coordinate systems (e.g., x, y, z coordinates, angular coordinates, etc.). In addition, it is noted that whenever the term 'GPS' is referred to, it is done so in the broader sense of Global Navigation Satellite Systems (GNSS) which may include other existing satellite positioning systems such as GLONASS as well as future positioning systems such as Galileo and Compass/Beidou. In addition, as noted previously, in some embodiments other positioning systems, such as terrestrially-based systems, may be used in addition to or in place of satellite-based positioning systems.

[0043] Embodiments of WAPS include multiple towers or transmitters, such as multiple transmitters 110 as shown in **FIG. 1**, which broadcast WAPS data positioning information, and/or other data or information, in transmitter output signals to the receivers 120. The positioning signals may be coordinated so as to be synchronized across all transmitters of a particular system or regional coverage area, and may use a disciplined GPS clock source for timing synchronization. WAPS data positioning transmissions may include dedicated communication channel resources (e.g., time, code and/or frequency) to facilitate transmission of data required for trilateration, notification to subscriber/group of subscribers, broadcast of messages, and/or general operation of the WAPS network. Disclosure regarding WAPS data positioning transmissions may be found in the incorporated applications.

[0044] In a positioning system that uses time difference of arrival or trilateration, the positioning information typically transmitted includes one or more of precision timing sequences and positioning signal data, where the positioning signal data includes the location of transmitters and various timing corrections and other related data or information. In one WAPS embodiment, the data may include additional messages or information such as notification/access control messages for a group of subscribers, general broadcast messages, and/or other data or information related to system operation, users, interfaces with other networks, and other system functions. The positioning signal data may be provided in a number of ways. For example, the positioning signal data may be modulated onto a coded timing sequence, added or overlaid over the timing sequence, and/or concatenated with the timing sequence.

[0045] Data transmission methods and apparatus described herein may be used to provide improved location information throughput for the WAPS. In particular, higher order modulation data may be transmitted as a separate portion of information from pseudo-noise (PN) ranging data. This may be used to allow improved acquisition speed in systems employing CDMA multiplexing, TDMA multiplexing, or a combination of CDMA/TDMA multiplexing. The disclosure herein is illustrated in terms of wide area positioning systems in which multiple towers broadcast synchronized positioning signals to UEs and, more particularly, using towers that are terrestrial; however, the embodiments are not so limited and other systems within the spirit and scope of the disclosure may also be implemented.

[0046] In an exemplary embodiment, a WAPS uses coded modulation sent from a tower or transmitter, such as transmitter 110, called spread spectrum modulation or pseudo-noise (PN) modulation, to achieve wide bandwidth. The corresponding receiver unit, such as receiver or user device 120, includes one or more components to process such signals using a despreading circuit, such as a matched filter or a series of correlators, for example. Such a receiver produces a waveform which, ideally, has a strong peak surrounded by lower level energy. The time of arrival of the peak represents the time of arrival of the transmitted signal at the UE. Performing this operation on a multiplicity of signals from a multiplicity of towers, whose locations are accurately known, allows determination of the receivers location via trilateration. Various additional details related to WAPS signal generation in a transmitter, such as transmitter 110, along with received signal processing in a receiver, such as receiver 120, are described subsequently herein.

[0047] In one embodiment, a WAPS may use binary coded modulation as the spreading method. The WAPS signals of an exemplary embodiment may include two specific types of information: (1) a high precision ranging signal (which may be delivered quickly relative to other signals), and (2) location data such as transmitter ID and position, time of day, health, environmental conditions such as atmospheric information (e.g., pressure, temperature, humidity, direction and force of wind, and other conditions). WAPS may, similarly to GPS, transmit location information by modulating a high speed binary pseudorandom ranging signal with a lower rate information source. In addition to this application, the incorporated applications disclose embodiments of methods that use a pseudorandom ranging signal and a modulating information signal, both of which may utilize higher order modulations, such as quaternary or octonary modulation. In one embodiment, the ranging signal is binary phase modulated, and location information is provided in a separate signal using higher order modulation.

[0048] Conventional systems use a format of a position location signal (e.g., used in a Time Division Multiplexing arrangement) in which each slot transmission comprises a pseudorandom ranging signal followed by various types of location data. These conventional systems also include a synchronization, or sync, signal, which may be deleted if the pseudorandom ranging signal is used also as the sync signal. However, as with other earlier systems, the location data of these conventional systems is binary, which limits throughput. These systems also transmit a large number of binary bits during the interval in which the location data is transmitted.

[0049] To address these limitations, in exemplary embodiments, a binary, or quaternary, pseudorandom signal may be transmitted in a particular slot followed by a very higher order modulated data signal. For example, in a given slot one or more location information symbols may be transmitted using differential 16-phase modulation, in order to transmit four bits of information per slot. This represents a four-fold throughput improvement versus the one bit typically transmitted when binary phase modulation is imposed upon the pseudorandom carrier. Other types of modulation of location information may also be utilized, such as 16 QAM, etc. In addition certain error control modulation methods may be used for the higher level modulation, such as the use of Trellis codes. These modulation methods generally reduce error rates.

[0050] **FIG. 2** depicts certain aspects of a positioning system 240 configured to implement conditional access processes described herein. As shown in **FIG. 2**, the positioning system 240 may perform various functions. For example, the positioning system 240 may generate and make available ALACs which may be individually generated and provided to the manufacturer 210 and/or the service provider 230 in blocks of ALACs for addition to the user device 220 (e.g., the GPS FW Image). The ALACs may be implemented in a device-specific manner, including use of a device identifier, and device-specific algorithms to provide an additional layer of protection for the ALACs. The positioning system 240 may further operate a billing and audit system to track and charge for the use of positioning functionality provided by the positioning system 240.

[0051] The positioning system 240 may generate and make available ASLCs to the manufacturer 210, the user device 220, the service provider 230, and/or the external entities 250 (e.g., an application developer or provider). The ASLCs maybe serialized to include a unique device identifier like IMEI, MAC-Address, etc.

[0052] The positioning system 240 may generate and administer developer keys, SDKs and APIs for external entities 250 that are looking to incorporate position information into downloadable applications. Each developer key may have several associated ASLCs based on the service levels of an associated application. Each application ASLC may contain the developer key as unique identifier, and may also contain other unique IDs. The positioning system 240 may also maintain a server to process requests from deployed applications in the field (i.e., on user device 220) for dynamic transmissions of ASLCs to the user device 220.

[0053] The manufacturer 210 may image one or more ALACs and ASLCs (e.g., obtained from the positioning system 240, or independently created and maintained) onto the receiver along with requisite firmware ("FW") and software ("SW"). The manufacturer 210 may also load the libraries as an image. Manufacturer 210s may include chipset suppliers, device OEMs, OS vendors. By comparison, the same ALAC may be used for all transmissions from all transmitters, while a different ASLC may be used for each application on each receiver, and based on particular user accounts. Both the ASLC and the ALAC may be encrypted or otherwise protected from unauthorized access at the UE.

[0054] The service provider 230 may provide various services to the user device 220, including cellular services and web-based services. Additional services may include any wireless or wired delivery of content (e.g., video content, audio content, image content, text content, other content). The service provider 230 may store ASLCs associated with applications it provides to the user device 220. The service provider 230 also enables Control-Plane (c-Plane) messaging flow for E-911 and network management when applicable. The service provider 230 may further enable User-Plane (u-Plane), via SUPL messaging flows for in-house LBS.

[0055] The external entities 250 may include vendors that provide various location services to users via the user's receiver. For example, external entities 250 may include PSAPs, location-based ad networks, and LBS application developers/publishers, among others. The positioning system 240 and service provider 230 may serve an external entity 250 with a range of services, including location assistance; ASLC verification and provisioning, value-added-services, billing services and audit services.

[0056] A user device 220 may include a smartphone, tablet, and a connected computing device. The user device 220 may be configured to control access to position information by individual applications (e.g., e-911, network management (NW), or LBS). Control of the access may be accomplished using ASLCs that are imaged on firmware or downloaded after the user device 220 is manufactured and enters the stream of commerce. As shown, a driver and a library layer may assist in the managing of ASLCs for multiple applications and users on device, in the decryption of position information, and in limiting the use of the decrypted position information by an application based on permissions indicated by the ASLC. For example, the library may be capable of associating an ASLC to its relevant application (e.g., E911, Network Management, LBS, etc.), and to provide or arbitrate delivery of appropriate position information to the application.

[0057] Various system features have been described above, including transmitters and receivers. **FIG. 3** and **FIGs. 4A, 4B** and **4C**, described below, provide further details regarding certain implementations of transmitter and receivers.

[0058] FIG. 3 presents diagram illustrating certain details of one embodiment 300 of a beacon/transmitter system from which location/positioning signals as described subsequently herein may be sent. Transmitter embodiment 300 may correspond with transmitters 110 as shown in **FIG. 1.** It is noted that transmitter embodiment 300 includes various components for performing associated signal reception and/or processing; however, in other embodiments these components may be combined and/or organized differently to provide similar or equivalent signal processing, signal generation, and signal transmission.

[0059] Although not shown in **FIG. 3**, transmitter/beacon embodiment 300 may include one or more GPS components for receiving GPS signals and providing location information and/or other data, such as timing data, dilution of precision (DOP) data, or other data or information as may be provided from a GPS or other positioning system, to a processing component (not shown). It is noted that while transmitter 300 is shown in **FIG. 3** with a GPS component, other components for receiving satellite or terrestrial signals and providing similar or equivalent output signals, data, or other information may alternately be used in various embodiments. GPS or other timing signals may be used for precision timing operations within transmitters and/or for timing correction across the WAPS network.

[0060] Transmitter 300 may also include one or more transmitter components (e.g., RF transmission component 370) for generating and sending transmitter output signals as described subsequently herein. A transmitter component may also include various elements as are known or developed in the art for providing output signals to a transmit antenna, such as analog or digital logic and power circuitry, signal processing circuitry, tuning circuitry, buffer and power amplifiers, and the like. Signal processing for generating the output signals may be done in the a processing component (not shown) which, in some embodiments, may be integrated with another component described in relation to **FIG. 3** or, in other embodiments, may be a standalone processing component for performing multiple signal processing and/or other operational functions.

[0061] One or more memories (not shown) may be coupled with a processing component (not shown) to provide storage and retrieval of data and/or to provide storage and retrieval of instructions for execution in the processing component. For example, the instructions may be instructions for performing the various processing methods and functions described subsequently herein, such as for determining location information or other information associated with the transmitter, such as local environmental conditions, as well as to generate transmitter output signals to be sent to the user devices 120 as shown in **FIG. 1**.

[0062] Transmitter 300 may further include one or more environmental sensing components (not shown) for sensing or determining conditions associated with the transmitter, such as, for example, local pressure, temperature, humidity, wind, or other (collectively or individually, “atmospheric”) conditions. In an exemplary embodiment, atmospheric (e.g., pressure) information may be generated in the environmental sensing component and provided to a processing component for integration with other data in transmitter output signals as described subsequently herein. One or more server interface components (not shown) may also be included in transmitter 300 to provide an interface between the transmitter and server systems, such as server system 130 as shown in **FIG. 1**, and/or to a network infrastructure, such as network infrastructure 170 as shown in **FIG. 1**.

For example, system 130 may send data or information associated with the location system and/or user devices to transmitters 300 via an interface component of the transmitter.

[0063] Each transmitter 300 may send data at the physical layer at an adjustable number of bits per second per slot (e.g., 96 bits per second per slot or greater), and each transmitter may be independent of the others, including its position information. Transmitter 300 may include various components to generate, encrypt, protect, modulate and transmit data. For example, transmitter 300 may include a data generation component 310 to generate position information, an encryption component 320 to encrypt the position information based on a particular air-link access certificate (ALAC), an access certificate storage component 330 to store the ALAC, and other components – e.g., a packet ID/CRC component 340, an encoding, puncturing and interleaving component 350, a modulation component 360, and an RF transmission component 370, among others not shown. Components 340 and 350 may provide forward error correction (FEC) and CRC schemes, along with other data formatting schemes to reduce the effects of fading, path loss, and other environmental conditions. Component 360 provides modulation on data.

[0064] Although modulation and signal structure may vary, where varying numbers of bits per frame can be used, it is contemplated that 190 bits per frame are available for transmissions from the transmitter 300. By way of example, 102 data bits are available after encoding overhead, of which 7 bits are reserved for unencrypted framing information, which leaves 95 bits for encrypted position information. It is preferred that encryption be minimally used to maintain low overhead. By way of example, one encryption rate may be about 95 bits every 3 seconds. Transmissions may repeat themselves for a few cycles (e.g., 10 cycles or 30 seconds) before data changes. Various payloads are contemplated, including: latitude, longitude, altitude, pressure, temperature, transmission correction, and transmission quality. Additional payloads may include security information, service ID, conditional access data (e.g., ASLC information). These various payloads can be segmented over multiple slots. One of skill will appreciate other payloads, other numbers of bits, and different ways to package payloads.

[0065] In some cases, there is a need for an *n*-bit indicator to denote the type of packet that is being transmitted, which type of information will be transmitted over several packets, or how multiple packets of the same information relate to each other. Packet structures may include this *n*-bit indicator at any point in the packet. **FIG. 10A** illustrates one example of a packet structure showing four packet type indicator bits, and other bits, and **FIG. 10B** illustrates one example of a series of packets that use the four-bit packet type indicator.

[0066] As shown in FIGs. 10A and 10B, four bits may indicate a packet type, and the main packet payload may include 98 bits. The four bits may be unencrypted, and the packet types that are '0' may be unencrypted, while the packet types that are '1' may be encrypted. For packet types that are not '0' or '1', for example, but not by way of limitation, the fifth bit may be the encryption bit, and may denote whether this packet is encrypted or not. This bit may be unencrypted. The sixth bit may be the start bit, and may denote whether this begins a new packet (1) or the continuation of a previous packet (0). This bit may be unencrypted. The seventh bit may be the stop bit, and may denote whether this is the last packet (1) or not (0). This bit may be unencrypted. The next 95 bits may contain the main packet payload, which may be encrypted if the encryption bit is 1, and may be otherwise unencrypted if the encryption bit is 0. The payload may optionally contain the index of the current packet and/or the total number of packets to be expected with the current information being sent.

[0067] Attention is now turned to **FIG. 4A**, which depicts features of a receiver 400 at which transmitter signals may be received and processed to determine location/position information (e.g., on behalf of an E-911 or LBS application).

[0068] Receiver embodiment 400 may correspond with user device 120 as shown in **FIG. 1**, and may include one or more GPS components 480 for receiving GPS signals and providing location information and/or other data, such as timing data, dilution of precision (DOP) data, or other data or information as may be provided from a GPS or other positioning system, to a processing component (not shown). Of course, other Global Navigation Satellite Systems (GNSS) are contemplated, and it is to be understood that disclosure relating to GPS may apply to these other systems. It is noted that while receiver 400 is shown in **FIG. 4A** with a GPS component, other components for receiving satellite or terrestrial signals and providing similar or equivalent output signals, data, or other information may alternately be used in various embodiments. Of course, any location processor may be adapted to receive and process position information described herein or in the incorporated applications.

[0069] Receiver 400 may also include one or more cellular components 490 for sending and receiving data or information via a cellular or other data communications system. Alternately, or in addition, receiver 400 may include communications components (not shown) for sending and/or receiving data via other wired or wireless communications networks, such as Wi-Fi, Wi-Max, Bluetooth, USB, or other networks.

[0070] Receiver 400 may include one or more components outlined by the dotted border 420 (referred to as "components 420") that are configured to receive signals from terrestrial transmitters, such as transmitters 110 as shown in **FIG. 1**, and processing the signals to determine position/location information as described subsequently herein. Components 420 may be integrated with and/or may share resources such as antennas, RF circuitry, and the like with other components shown in **FIG. 4A**. For example, components 420 and GPS component 480 may share some or all radio front end (RFE) components and/or processing elements. A processing component (not shown, but mentioned generally here to indicate processing functionality in the receiver 400) may integrate some or all of the components 420, or may share resources with some or all of the components 420 and/or GPS component 480 to determine position/location information and/or perform other processing functions as described herein. Similarly, cellular component 490 may share RF and/or processing functionality with RF component 410 and/or components 420. A network component 460 is also shown, which may refer to local area, wide area, or other networks that employ any type of wired and wireless communication pathways. Components 410, 420, 460, 480 and 490 may each deliver data to a position engine 440, which uses the data to determine an estimated location of the receiver 400. The position engine 400 may be implemented as known in the art or later developed in the art, including such implementations that include a processor configured to compute the estimated location.

[0071] For example, in one implementation, component 490 may deliver positioning data securely through the control plane or user plane or the data may be directly obtained through an internet link. The data on the interface between 490 and the cellular modem may also be protected through interface encryption/decryption specific to the receiver 400.

[0072] One or more memories 430 may be coupled with processing component (not shown) and other components to provide storage and retrieval of data and/or to provide storage and retrieval of instructions for execution in the processing component. For example, the instructions may perform the various processing methods and functions described herein, such as decrypting position information and determining location information. Accordingly, certain components (e.g., components 421-424) included among components 420 may perform processing of position information, decryption keys, and/or other information described herein. Some or all of that processing may alternatively be performed at a stand-alone processor (not shown).

[0073] Position data comprising the position estimate or information used for remote position computation may be transmitted to these remote components using industry standard protocols such as Control-Plane signaling, or User Plane (SUPL) signaling or internet/data protocols or some combination thereof.

[0074] Receiver 400 may further include one or more environmental sensing components (not shown) for sensing or determining conditions associated with the receiver, such as, for example, local pressure, temperature, humidity or other conditions, that may be used to determine the location of the receiver 400. In an exemplary embodiment, pressure information may be generated in such an environmental sensing component for use in determining location/position information in conjunction with received transmitter, GPS, cellular, or other signals.

[0075] Receiver 400 may further include various additional user interface components, such as a user input component (not shown), which may be in the form of a keypad, touchscreen display, mouse, or other user interface element. Audio and/or video data or information may be provided on an output component (not shown), such as in the form or one or more speakers or other audio transducers, one or more visual displays, such as touchscreens, and/or other user I/O elements as are known or developed in the art. In an exemplary embodiment, such an output component may be used to visually display determined location/position information based on received transmitter signals, and the determined location/position information may also be sent to cellular component 490 to an associated carrier or other.

[0076] The receiver 400 may include various other components configured to carry out various features of the disclosure, including processes illustrated in **FIG. 5A, FIG. 6, FIG. 7 and FIG. 8**. For example, the components 420 may include a signal processing component 421 that comprises a digital processing component 421a configured to demodulate the received RF signal from the RF component 410, and also to estimate time of arrival (TOA) for later use in determining location. The signal processing component 421 may further include a pseudorange generation component 421b and a data processing component 421c. The pseudorange generation component 421b may be configured to generate "raw" positioning pseudorange data from the estimated TOA, refine the pseudorange data, and to provide that pseudorange data to the position engine 440, which uses the pseudorange data to determine the location of the receiver 400. The data processing component 421c may be configured to decode the encoded position information, extract encrypted packet data from the encoded position information and perform error correction (e.g., CRC) on the data. The data processing component 421c outputs encrypted packet data to a first cryptography component 422.

[0077] The first cryptography component 422 may be configured to at least decrypt the position information from the encrypted packet data based on an ALAC stored in the memory 430. Since multiple ALACs may be stored on the receiver 400 and only one of them is applicable at a given time, the first cryptography block 422 can employ various techniques to determine the correct ALAC key to use. The data packet itself can have a CRC/digest field that passes check only when the correct ALAC key is applied. In the absence of a CRC/digest field due to packet content constraints, the individual fields of the decrypted packet can be checked for the expected value ranges of that field. In addition, since the receiver can obtain packet data from multiple transmitters near the receivers, the position information from the multiple transmitters will pass certain coherency checks such as the distances between the transmitters, geographic identifiers, and others, only when the correct ALAC key is selected. The first cryptography component 422 may also, upon receiving an indication that an emergency 911 call has been initiated, output the decrypted position information to an appropriate processing component associated with an E-911 procedure.

[0078] The components 420 in FIG. 4A may further comprise a second cryptography component 423 that is configured to decrypt some or all of the position information based on an appropriate ASLC stored in the memory 430. The ASLC may be determined by which application has requested the position information or a location fix. For example, ASLC's may be associated with LBS applications or E-911 applications on the receiver 400.

[0079] Once the position information is decrypted by the second cryptography component 423, the decrypted position information is output to a data unit output component 424 that determines discrete data units of the position information (e.g., latitude, longitude, altitude, pressure, temperature, humidity, system time, timing correction, and/or transmitter ID). Specific data units of the position information may then be transmitted to the position engine 440 based on service levels indicated by the ASLC for the application that requested access to the position information.

[0080] The position engine 440 may be configured to process the position information (and, in some cases, GPS data, cell data, and/or other network data) in order to determine the location of the receiver 400 within certain bounds (e.g., accuracy levels, etc.). Once determined, location information may be provided to the applications 450. One of skill in the art will appreciate that the position engine 440 may signify any processor capable of determining location information, including a GPS position engine or other position engine. Locations of the various components shown in **FIG. 4A** are contemplated at different chip space within the receiver.

[0081] As disclosed elsewhere herein, and repeated here for clarity, each application on the receiver 400 may need its own ASLC to access position information in order to determine the location of the receiver 400. With respect to some aspects, one ASLC may be used by multiple applications, and multiple ASLCs may be used by one application but for different users or under different circumstances. The ASLCs may be used to limit use of particular position information during particular time periods and in particular service areas.

[0082] E-911, Network Support and LBS applications/services may be handled separately from each other, where their respective ASLCs may be loaded into firmware of the receiver 400 or uploaded to memory after manufacture of the receiver 400. Each ASLC may be used to provide each application/service its own feed of the position information. Separate processing pathways may be used to further separate these applications/services.

[0083] The receiver 400 may have limited hardware/software capabilities dedicated for location determinations. The total footprint available for the conditional access features described herein may be on the order of 32 kilobytes. Other footprints are contemplated.

[0084] Position information may be processed at a GPS processor, an application processor or at an external server. In accordance with one aspect, features described herein may be carried out on or in association with a GPS integrated circuit (IC) on the receiver. For example, a host processor at the receiver may be used to communicate with a GPS IC via a bi-directional serial link. Latitude and longitude, along with other information may be transmitted using this serial link. The serial link may be used for certificate exchanges (e.g., ASLCs) to the GPS IC. It is contemplated that the GPS IC comprises a signal processing section that searches for transmitters (e.g., through correlation with PN sequences) and demodulates signals received from transmitters to retrieve physical layer payload, which may be (and is, according to certain embodiments described herein) in encrypted form. A decryption engine can the decrypt the data before providing the data to the next processing layer, which may be the position engine. The position engine may use the decrypted data to compute receiver location. The various engines may be provisioned in the GPS IC, or in other receiver circuitry.

[0085] Attention is now drawn to **FIG. 4B**, which depicts a receiver 400 at a first location, and further depicts components that reside at other locations that are remote from the location of the receiver 400. The receiver 400 and the other components may collectively or individually determine location information based on processing of transmitter signals. Certain aspects of FIG. 4A are depicted in FIG. 4B. Accordingly, description of those aspects in relation to FIG. 4A may be extended to those aspects in FIG. 4B for certain, but not necessarily all, embodiments.

[0086] As shown in **FIG. 4B**, the receiver 400 may include interface (I/F) encryption/decryption (also referred to as "scrambling/descrambling") components that protect data when the data crosses an unprotected interface boundary or is communicated through an unprotected communication channel. In some cases, these I/F components may operate on I/F keys that are generated by each receiver 400 independently.

[0087] FIG. 4B provides for position computation at the receiver 400 before the second cryptography component 423a, which may provide the results of the position computation to an application 450 that is resident on the receiver 400, or an application 499a that does not reside on the receiver 400. Alternatively, the position computation may be performed by remote components (e.g., a remote position engine 440b of a server) that use position data received from the receiver 400, whereby the results of that remote position computation may be returned to the receiver 400, or used by remote applications 499b.

[0088] Data transfer between components depicted by dotted lines in **FIG. 4B** may be carried out directly between those components, or through intermediate components (e.g., the RF component 410 or the network component 460). The dotted lines may represent alternative embodiments. For example, application manager 498a may receive position data from the second cryptography component 423a, after which the application manager 498a may cause that position data to be transferred to a remote application service 499a (e.g., through network component 460, or RF component 410, or other components in the receiver 400). The remote application service 499a may then use the position data (e.g., a position estimate) to provide e911 or LBS services in relation to the receiver 400.

[0089] By way of another example, application manager 498a may receive data directly from the data unit output component 424, or through an intermediate component (e.g., an I/F encryption component), after which the application manager 498b may cause that position data to be transferred to a remote position engine 440b that computes an estimated position of the receiver 400 (e.g., the latitude, longitude, altitude of the receiver 400). The remote position engine 440b may transmit that position estimate to either the second cryptography component 423a (e.g., through network component 460, or RF component 410, or other components in the receiver 400) or the second cryptography component 423b for further processing at those components. The second cryptography component 423b, for example, may operate to control access to the position estimate by one or more remote application services 499b or an application 450 running on the receiver 400 (e.g., through transfer of the position estimate via network component 460 or RF component 410 or other components in the receiver 400). The remote application service 499b or the application 450 may then use the position estimate to provide e911 or LBS services in relation to the receiver 400. Any of the remote components may be co-located or reside at different geographic locations.

[0090] In **FIG. 4B**, the first cryptography component 422 outputs decrypted position information to a data unit output component 424 that determines discrete data units of the position information (e.g., latitude, longitude, altitude, pressure, temperature, other atmospheric information or measurements, system time, timing correction, and/or transmitter ID). These data units are then transmitted to the position engine 440a or 440b. The position engine 440a or 440b may be configured to process the position information (and, in some cases, GPS data, cell data, and/or other network data) in order to determine the location of the receiver 400 within certain bounds (e.g., accuracy levels, and other bounds). Once determined, location information may be provided to an application 450, 499a, or 499b through the second level cryptography 423a or 423b (and possibly through other intermediary components). One of skill in the art will appreciate that the position engine 440a or 440b may signify any processor capable of determining location information, including a GPS position engine or other position engine.

[0091] The second cryptography component 423a may be configured to encrypt certain data using session keys meant for a specific application or a group of applications with a particular service level. Service levels may authorize access to a certain subset of data units (e.g., latitude, longitude, altitude, accuracy, and others) for certain applications.

[0092] After encrypting data (e.g., using a session key), the second cryptography component 423a may then make that encrypted data available to an application 450. Session keys may be dynamically generated at the receiver 400, and may be changed periodically for improved security. When a single session key is used for a group of applications, the session key can be changed when the ASLC validity period has expired for any of the applications, thus forcing that group of applications to request a new session key.

[0093] In one embodiment, the second cryptography component 423 validates an ASLC for a particular application before exchanging the session key with the application to enable the application to decrypt the data meant for that application. The second cryptography component 423 may initially receive the ASLC from the application, or may be instructed to look up the ASLC from the memory 430 or elsewhere. Specific encrypted data units of the position information may then be accessible to that application.

[0094] The ASLC may indicate service-level authorizations for the application. In order to manage access to only the data authorized for a particular application, the second cryptography component 423a may exchange session keys with the application for sending encrypted data according to the authorization indicated in the ASLC for that application.

[0095] For a remote application 499a, the remote application manager 498a may provide a communication interface to transport the ASLC and session keys between the remote application and the second cryptography component 423a.

[0096] Attention is turned to FIG. 4C, which depicts several aspects of the disclosure as they relate to a receiver and other components that send data to the receiver or receive data from the receiver. As shown in FIG. 4C, position signals are acquired from transmitters (e.g., using signal processing that searches for the transmitters through correlation with PN sequences). The signal processing may also demodulate the signal to retrieve the physical layer payload and raw time of arrival (TOA) for each transmitter. These signals may be acquired and tracked by various hardware (HW), firmware (FW), and/or software (SW) components. By way of example, FW and/or HW on a GPS chip may operate to decode a packet from any one of various sub-frames of the signal transmission and verify the CRC. Alternatively, a host processor could decode and verify the CRC.

[0097] Tracking HW/FW/SW may operate to generate raw TOA data and transmit raw encrypted data (e.g., packets) to a decryption component. In some implementations, a packet ID is not encrypted for all packet types. The raw encrypted data may be decrypted using ALAC keys within specific HW/FW (e.g., HW/FW specific to WAPS). The ALACs may be encrypted or otherwise wrapped based on a device ID specific to each device or class of devices. The device specific IDs may be utilized for entitlement of the WAPS location service on the device.

[0098] The ALAC decryption process, and/or FW/HW/SW responsible for decryption may vary across vendors at chip-level, receiver/handset-level, or carrier-level. The raw decrypted data along with the raw TOA measurements may then be scrambled (e.g., using a scrambling algorithm and a device generated key), and the scrambled data may be sent over a protected or unprotected data stream to a location library running on the GPS chip itself or on a host processor, or both. Scrambling may not be necessary where the decryption and the location library operate on the same HW/FW (e.g., the GPS chip).

[0099] The location library may then descramble the raw data and TOA measurements for further use within the library. For example, the descrambled data may be assembled into data units (DU) 1 through 5 as follows: DU1 (latitude, longitude, altitude (LLA) of transmitter); DU2 (pressure/temperature at transmitter); DU3 (timing correction for transmitter); DU4 (time for network of transmitters (WAPS time)); and DU5 (identifier for transmitter).

[00100] Fine TOAs may be generated using the raw and timing corrections from DU3. A positioning engine may use various data units (e.g., DU1, DU2, DU5), along with the fine TOAs and a pressure sensor reading to compute the LLA of the receiver. It is noted that DU4 may be used by a positioning engine configured to generate timing signals (e.g., used where the receiver operates to synchronize other receivers).

[00101] The receiver's LLA or any of DU1 through DU5 may be encrypted based on parameters specified by the ASLC for a requesting application or a group of applications to which the requesting application belongs. Encryption may be carried out using various techniques, including a random or pre-defined session key, another key defined by the ASLC, or other encryption methods as known in the art. Various implementations are contemplated, including implementations where the service-level encryption and decryption may involve a single instance of an application or multiple instances of different applications.

[00102] In one implementation, the encrypted data may only include data available to the requesting application as specified by the service level of that application. For example, an estimate of the receiver's LLA within a certain accuracy level may be made available (e.g., LLA accurate within 100 meters, LLA accurate within 10 meters). In such an implementation, a processor resident at the receiver may analyze known LLA with accuracy at *x* meters, and then generate a different LLA with accuracy at *y* meters depending on the service level authorization. Such an implementation may be beneficial where different paid-for service levels are associated with varying levels of position accuracy.

[00103] Either positioning engine may generate a best estimate of reference pressure using pressure and temperature readings received in DU2 for each of multiple transmitters. The reference pressure may be sent in encrypted form to either positioning engine, which may use the reference pressure and the receiver's pressure sensor reading to compute altitude as described in the incorporated references.

[00104] In certain SW architectures the positioning engine may incorporate additional measurements from other sources in a hybrid implementation that uses signals from any of Wi-Fi, GPS, WAPS, and other transmitters. Such a hybrid positioning engine may operate in conjunction with a host processor after service-level decryption of the encrypted receiver LLA or other encrypted data (e.g., any of DU1 through DU5). Alternatively, the hybrid positioning engine may operate prior to the service-level encryption so access to resultant data from the hybrid positioning engine is limited to authorized applications.

[00105] The above discussion relating to FIG. 4C may apply to MS-assist (MS-A), MS-based (MS-B), or standalone user plane call flows. In the case of a control plane call flow (e.g., E-911), the data in the form of raw or fine TOAs/pseudoranges and an altitude estimate (for MS-A mode), or data in the form of the receiver's LLA (for MS-based mode), is sent to the Positional Determining Entity (PDE), Serving Mobile Location Center (SMLC), or other device for position computation and forwarding to the PSAP. Such transmission may occur over one or more control plane channels of a cellular system.

[00106] It is noted that, although not preferred, position assistance data can be supplied to the positioning engine using alternative communication means like web-based pathways, local area network pathways, wide area network pathways, and other network pathways beyond RF pathways. Such transmission may be necessary when low signal conditions are present between the receiver and the transmitter network. When transmitted using the alternative communication means, the assistance data may be encrypted using keys associated with the ALAC, or using alternative keys specific to the communication means. Alternatively, no ALAC or similar keys may be used, but the service-level encryption and decryption may be used.

[00107] Although FIG. 4C depicts different components within different HW/FW/SW, certain embodiments may incorporate the various components of FIG. 4C into one or more hardware components like the host processor, GPS chip, or both.

Aspects Relating to Methodologies

[00108] **FIG. 5A** illustrates a diagram detailing a network process for determining position information relating to a receiver and controlling access to that position information at the receiver in accordance with certain aspects. Reference may be made to **FIG. 2** while describing the process illustrated in **FIG. 5A**. One of skill in the art will appreciate that the process flow shown in **FIG. 5A** is illustrative, and that there is no intention to limit this disclosure to the order of stages shown in **FIG. 5A**. Accordingly, stages may be removed and rearranged, and additional stages that are not illustrated may be carried out within the scope and spirit of the disclosure.

[00109] At stage 501, the positioning system 240 may create and maintain information used to control access by receivers to position information. By way of example, the positioning system 240 may create air-link access certificates (ALACs) (also referred to as "system-level keys/certificates") and authorized service-level certificates (ASLCs) that are later used by the UE 220 to decrypt position information received from the network (e.g., from the service provider 230 and/or the positioning system 240) before using that position information based on restrictions specified by the ASLC for a particular application on the receiver that has requested the position information. At stage 502, the created ALACs and ASLCs are provided to the manufacturer 210, and the manufacturer 210 provisions the UE 220 with the ALACs/ASLCs (e.g., by imaging them in firmware) at stage 503.

[00110] At stage 504 (e.g., after a user purchases the UE 220), the UE 220 launches an application or initiates an emergency 911 call. Prior to step 504, although not explicitly shown, the application may be downloaded to the UE 220. Stage 505 is unnecessary in cases where an ASLC associated with the application has been provisioned by the manufacturer. Otherwise, the UE 220 sends a developer key associated with the application to the network. The routing of the developer key may pass through the service provider 230, the positioning system 240 and/or the developer of the application as an external entity 250 (routing not shown). After receiving and verifying the developer key, the network may then transmit an ASLC for that application to the UE 220, which may then store the ASLC.

[00111] At stage 506, the UE 220 retrieves position information from the network. The position information may be obtained from a broadcast signal originating at the positioning system 240, and/or may be obtained through the service provider 230. Similarly, the UE 220 may request position information, or monitor broadcasts for position information.

[00112] At stages 507-508, the UE 220 may decrypt the position information using an ALAC (e.g., an ALAC associated with the transmitter that broadcasted the position information) and an ASLC that is associated with the application on the receiver that is requesting the position information.

[00113] At stages 509-510, the decrypted position information is processed and location information relating to the location of the UE 220 is determined (e.g., at a position engine).

[00114] In the case of a 911 call, at stages 511-512, the position information, the location information, and/or information used to determine position (e.g., such as pseudoranges and information about transmitters for which the pseudoranges were computed) are transmitted to the service provider 230 and/or the PSAP operating as an external entity 250. Otherwise, at stage 512, for LBS-based applications, the location information may remain at the UE 220 to carry out location based services and/or may be transmitted to an LBS entity operating as an external entity for aiding the provision of location based services from that LBS entity. Another alternative for an E-911 call is for the receiver to send an encrypted packet to a server along with raw TOA information. The encrypted packet may be decrypted to extract the information required to compute a position solution at the server.

[00115] FIG. 5B illustrates a process for distributing position information in relation to a network application or E-911 transaction. Note that the ASLC may or may not be used in an E911 transaction. For example, if the ASLC is used in an E-911 call, a special ASLC may be setup for use in an emergency call which has the highest service level and no expiry date.

[00116] **FIG. 6** illustrates a diagram detailing a process for providing conditional access to position information at a receiver in accordance with certain aspects. Reference may be made to **FIG. 2** and **FIGs. 4A-C** while describing the process illustrated in **FIG. 6**.

[00117] As previously described, encrypted positioning signal data may be transmitted to a receiver (e.g., receiver 400 of **FIGs. 4A-C**). Encrypting the positioning signal data helps safeguard its delivery to and use at authorized receivers. However, robust encryption techniques may not be viable given bandwidth constraints and limitations on processing power at the receiver. Accordingly, encryption must protect the transmitted data while minimally using data/packet space, and without requiring significant decryption at the receiver, which typically does not have the processing capability to perform robust decryption over a short period of time.

[00118] Additional encryption may be applied to safeguard use of position information by authorized applications and users based on various parameters (e.g., validity of payment associated with application, current location of user, whether a fixed amount of position requests by the user or application has been exceeded, time period during which position information may be accessed, and others). This second layer of encryption and decryption that controls distribution of position information to certain applications while restricting access to that position information by other applications is a key feature of various embodiments described herein, because it allows a network operator, carrier, application vendor/developer, or other entity shown in **FIG. 2** to monetize the distribution of the position information. Furthermore, the second layer of encryption and decryption frustrates various potential attempts by unauthorized users (e.g., hackers) to gain access to the position information for use with unauthorized applications.

[00119] **FIG. 6** illustrates the two stages of decryption in association with one aspect. One of skill in the art will appreciate variations in **FIG. 6** that stay within the scope and spirit of the disclosure. At stage 610, the receiver launches a first application (e.g., automatically in response to some predefined condition, in response to user input). The receiver then determines if a copy of an ASLC that is associated with the first application is stored in the receiver's memory (e.g., memory 430 of **FIGs. 4A-C**). If the copy exists, the receiver is "provisioned" with the ASLC, and stage 630 is executed. Otherwise, the receiver is 'un-provisioned", and stage 620 is executed.

[00120] At stage 620, the receiver obtains a copy of the ASLC from the network. **FIG. 7** details sub-stages of stage 620. One of skill in the art will appreciate that stage 620 may be performed after other stages shown in **FIG. 6** (e.g., after any stage before stage 660).

[00121] At stage 630, an encrypted positioning signal arrives at the receiver from a network. The positioning signal may be broadcasted by a transmitter, or may arrive over other communication pathways (e.g., cellular pathways, web-based pathways, local area network pathways). At stage 640, the receiver initially processes the positioning signal. Sub-stages associated with stage 640 are illustrated in **FIG. 8**.

[00122] At stage 650, the positioning signal arrives at the first cryptography component 422, where it is decrypted using a copy of the ALAC that is stored in memory 430. Then, at stage 660, some or all of the position data from the decrypted positioning signal is decrypted by the second cryptography component 423 using an ASLC associated with the first application. The ASLC may be retrieved from memory 430, or from the network (as described in relation to stage 620 and **FIG. 7**).

[00123] Finally, at stage 670, position engine 440 may receive the decrypted position data along with position TOA or pseudorange information to calculate the receiver's position on behalf of the first application. Calculation of the position may be determined based on a service level indicated by the ASLC for the first application.

[00124] **FIG.** 7 illustrates a diagram detailing a process for provisioning conditional access certificates at a receiver in accordance with certain aspects and stage 620 of **FIG. 6**. Reference may be made to **FIG. 2** while describing the process illustrated in **FIG.** 7.

[00125] At stage 710, the UE 220 retrieves a developer key associated with an application. The developer key may be stored on the UE 220 after the application is downloaded to the UE 220. An association of the developer key and an ASLC may be stored at the network (e.g., the service provider 230, the positioning system 240 or an external entity 250). The ASLC may be specific to not only the application, but also an access level of the UE 220. At stage 720, the developer key is transmitted to the network for processing (e.g., to the service provider 230, the positioning system 240, and/or the developer or application provider 250).

[00126] At stage 730, in response to transmitting the developer key, the UE 220/receiver 400 receives an ASLC related to the developer key/application over the network. At stage 740, the ASLC may be stored for future use. Alternatively, the ASLC may not be stored so that stages 710 through 730 are repeated the next time the application requests location information (which requires an ASLC associated with the application, under the two-stage decryption model illustrated in **FIG. 6** and described elsewhere herein).

[00127] **FIG. 8** illustrates a diagram detailing a process for processing positioning signal data in accordance with certain aspects and stage 640 of **FIG. 6**. Reference may be made to **FIGs. 4A-C** while describing the process illustrated in **FIG. 8**. By way of example, stage 640 may be performed by signal processing component 421 in **FIGs. 4A-C**.

[00128] At stage 810, a positioning signal received from a transmitter through RF component 410 may be used to estimate raw TOA (e.g., at digital processing component 421a). The raw TOA estimate may then be converted to raw positioning pseudorange information at pseudorange generation component 421b.

[00129] At stage 820, the positioning signal may be decoded at data processing component 421c. At stage 830, data processing component 421c may perform error detection on the positioning signal before sending it to the first cryptography component 422 for decryption.

[00130] **FIG. 11** illustrates a first stage of decryption, a second stage of encryption, and a third stage of decryption. One of skill in the art will appreciate variations in **FIG. 11** that stay within the scope and spirit of the disclosure. Certain stages depicted in **FIG. 11** may be rearranged or omitted in other implements. Discussion below relates generally to a receiver. However, the discussion can extend to one or more processors for carrying out some or all of the functionality specified below.

[00131] At stage 1110, a first application is launched (e.g., automatically in response to some predefined condition, in response to user input, or in response to another event or circumstance). The application may be launched at a receiver or at a server that is remote from the receiver, among other devices. The receiver may take various forms, including those shown in **FIGs. 4B-C**.

[00132] At stage 1120, the receiver obtains a copy of an ASLC associated with the first application. The receiver may obtain the ASLC from memory at the receiver, from the first application, or from an external source. The ASLC may specify parameters that determine what information can be provided to/accessed by the first application, in addition to when and how it can be provided/accessed by the first application, among other conditions. Alternatives to the using the ASLC are contemplated, including using just the data in the ASLC without using a certificate.

[00133] At stage 1130, encrypted positioning signals arrive at the receiver from transmitters. Each of the positioning signals may broadcast from respective transmitters, and may arrive over other communication pathways (e.g., cellular pathways, web-based pathways, local area network pathways), or both.

[00134] At stage 1140, the receiver initially processes the positioning signals.

[00135] At stage 1150, the positioning signal is decrypted using a key (e.g., one specified by an ALAC) stored on the receiver or otherwise accessible by the receiver from an external source.

[00136] At stage 1160, the receiver may identify or determine position information from the positioning signals. Such position information may include raw and fine TOA measurements, data units (DUs) described elsewhere herein, estimated position coordinates of a receiver that are computed based on data of the positioning signals, modified position coordinates that are determined based on the estimated position coordinates, or other data. The modified position coordinates may be determined based on the parameters from stage 1120. Such parameters may indicate that an application is permitted to receive position coordinates within a predefined level of accuracy (e.g., a distance) of the estimated position coordinates. In this case, a processor may create new position coordinates based on the level of accuracy (e.g., change the latitude so it falls within a range of *x* units of measurement from the estimated latitude, change the altitude to 0 so only two dimensions are provided). Providing less accurate position information may enable subscription services on a per-application or per-use basis.

[00137] Some or all of the position information may be encrypted at stage 1170 using a key specified by or otherwise generated based on the ASLC or its data from stage 1120. Selection of the position information to encrypt may be controlled by service level conditions specified by the ASLC. Such service level conditions may designate which data can be accessed by the first application, and may be determined from data described elsewhere herein, including some or all of the data described with respect to FIG. 9.

[00138] At stage 1180, the encrypted position information is decrypted for use by the first application. A processor running the first application may have knowledge of the key used to encrypt the position information. This knowledge may be gained by having access to the ASLC (e.g., where the ASLC specifies the key or an algorithm for determining the key), or by otherwise receiving the key (e.g., where a session identifier is used).

Aspects Related to Data

[00139] **FIG. 9** illustrates data for use during a conditional access process in accordance with certain aspects. As shown, data may identify or represent an application type (e.g., E-911, LBS, network management, law enforcement, a UE ID or UE type, a service type (e.g., accuracy of use, use coverage, time of use, data units available), a service provider type, a manufacturer type, a developer type, a user ID or user type, a type of request, or other type of information that may be used as parameters to determine a service level for an application that determines which position information can be provided to the application, when that position information can be provided, how that position information can be provided and where that position can be provided. GPS or other time may also be transmitted to monitor usage based on time limits. Some or all of this data may be incorporated into an ASLC for a particular application and/or UE, and may be later accessed by a processing component to identify position information that can be encrypted before being sent to an application that is local to a receiver or external to (i.e., remote from) the receiver. Each of the data may be used by a processor on the receiver to filter certain decrypted position information before providing that certain position information to the application, a device or a user in encrypted form. In other words, the data determine what position information is available, when it is available, for how long it is available. The ASLC may also include an encryption key or an algorithm for creating an encryption key (e.g., an algorithm for creating an encryption key using real-time data or other data that may be distributed in a protected environment or otherwise made available during encryption and decryption stages).

[00140] Service type may relate to accuracy levels in up to three dimensions, including high-range accuracy (e.g., 3 meters), mid-range accuracy (25-50 meters), and low-range accuracy (400 meters). Service type may also relate to coverage levels, including localized, regional, nationwide, and global, among others. Service type may further relate to time of validity levels involving expirations of access privileges in terms of one-time, monthly, yearly, or life-time, among other periods of validity. Service type may also relate to usage levels, including metered and unlimited. Various combinations of levels may be utilized.

[00141] Similar decryption on a location application for non-cellular devices is also contemplated. For example, E-911 calls through VoIP applications (e.g., Skype™), cameras/camcorders, and the like could have ASLCs imaged into their firmware or otherwise downloaded into memory.

Aspects Related to Use Cases

[00142] Various types of computing devices and their connectivity states are contemplated, including devices that are nearly always connected, mostly connected, or rarely (if ever connected) to a cellular network, positioning network, local area network, or other network. Additional consideration is given to processing capabilities of each of these computing devices.

[00143] Types of connectivity includes cellular (e.g., 3G/4G, pre-paid), Wi-Fi, wired (e.g., USB, Ethernet), and other connectivity.

[00144] Types of computing devices include smartphones, other cellular phones, tablets, laptops, connected TVs, VoIP phones, STBs, DMAs, appliances, security systems, PGD, PNDs, DSC, M2M applications, geo-fencing of assets, and others. Connected receivers are devices such as cell phones, tablets and laptops that have an active data pipe available (e.g., Cellular and Wi-Fi/wired Ethernet). Mostly connected receivers are devices such as tablets and laptops that have access to non-cellular means like Wi-Fi/wired Ethernet. Unconnected receivers or receivers with limited connectivity include receivers that are rarely (if ever) connected to the Internet, and have no cellular connectivity

[00145] It is contemplated that the unconnected receivers may be manufactured with a pre-authorized set of ALACs and ASLCs programmed for the lifetime of the receiver. Key updates beyond this initial period could be delivered either via a firmware update to the device (e.g., using a USB connection) or by connecting the device temporarily to a data

network. Such unconnected receivers could determine their location with an appropriate RF receiver that receives the encrypted position information (e.g., a GPS chip).

Additional Aspects

[00146] One or more aspects may relate to systems, methods, means and computer program products for controlling access to position information by one or more applications. Systems may include a processing component operable to implement a method. Computer program products may include a non-transitory computer usable medium having a computer readable program code embodied therein that is adapted to be executed to implement a method.

[00147] Method steps may: decrypt, using a first key, a first set of encrypted position signals received from a network of terrestrial transmitters; determine position information from the first set of decrypted position signals; identify a first set of the position information, wherein the first set of the position information is identified based on a first level of service associated with a first application; encrypt the first set of the position information using a second key; and provide the encrypted first set of the position information to the first application..

[00148] In accordance with some aspects, the first set of the position information includes at least one of position coordinates, timing corrections and atmospheric measurements of one or more transmitters from the network of terrestrial transmitters.

[00149] In accordance with some aspects, the method steps may further: compute estimated coordinates of a location of a receiver using the decrypted position signals, wherein the first set of the position information includes the estimated coordinates of the receiver.

[00150] In accordance with some aspects, the decrypted position signals include data that specifies atmospheric measurements at each of the terrestrial transmitters, wherein the estimated coordinates include an altitude coordinate that is computed using the decrypted position signals and at least one atmospheric measurement at the receiver.

[00151] In accordance with some aspects, the method steps may further: compute estimated coordinates of a location of a receiver using the decrypted position signals; and compute, based on a level of accuracy permitted for the first application, revised coordinates that are based on the estimated coordinates, wherein the revised coordinates are less accurate than the estimated coordinates in specifying the location of the receiver, and wherein the first set of the position information includes the revised coordinates.

[00152] In accordance with some aspects, the method steps may further: identify a second set of the position information, wherein the second set of the position information is identified based on a second level of service associated with a second application, wherein certain position information included in the first set is not included in the second set; encrypt the second set of the position information using a third key; and provide the second set of the position information to the second application.

[00153] In accordance with some aspects, the method steps may further: decrypt, using the first key or a third key, a second set of encrypted position signals received from the network of terrestrial transmitters, wherein the first set of encrypted position signals are received at a first location of the receiver, and the second set of encrypted position signals are receiver at a second location of the receiver; determine additional position information from the second set of decrypted position signals; identify a second set of the additional position information, wherein the second set of the additional position information is identified based on a second level of service associated with a second application; encrypt the second set of the position information using a fourth key ; and provide the second set of the position information to the second application.

[00154] In accordance with some aspects, the method steps may further: determine, prior identifying the first set of the position information, whether information specifying the first level of service is stored on the receiver; upon determining that the information specifying the first level of service is not stored on the receiver, access a first developer key that is associated with the first application; send the first developer key to a server; and receive the information specifying the first level of service in response to sending the first developer key to the server.

[00155] In accordance with some aspects, the information specifying the first level of service is included in a first authorized service-level certificate associated with the first application, and wherein the certificate is associated with the developer key.

[00156] In accordance with some aspects, the first level of service specifies a time period during which the second key can be used to encrypt the first set of the position information and any subsequent sets of any subsequent position information.

[00157] In accordance with some aspects, the second key is a session key that is generated after the position signals are decrypted.

[00158] In accordance with some aspects, first application runs on a remote server, and the first set of the position information is provided to the remote server.

[00159] In accordance with some aspects, the method steps may further: determine the first level of service based on parameters that are specified in a first certificate associated with the first application.

[00160] In accordance with some aspects, the method steps may further: scramble the position information before the position information is sent through an unprotected communication pathway; and unscramble the scrambled position information before identifying the first set.

[00161] In accordance with some aspects, the method steps may further: scramble the estimated coordinates before the estimated coordinates are sent through an unprotected communication pathway; and unscramble the scrambled estimated coordinates before encrypting the first set.

[00162] In accordance with some aspects, the method steps may further: select the first key from among a plurality of keys, wherein a CRC field of the encrypted position signals passes check only when the first key is used to decrypt the first set of encrypted position signals.

[00163] In accordance with some aspects, the method steps may further: select the first key from among a plurality of keys, wherein data of the decrypted position signals matches an expected value only when the first key is used to decrypt the first set of encrypted position signals.

[00164] In accordance with some aspects, the method steps may further: select the first key from among a plurality of keys, wherein the packet data from the multiple transmitters pass one or more coherency checks only when the first key is used to decrypt the first set of encrypted position signals, where the first set of encrypted position signals includes packet data from multiple transmitters.

Other Aspects

[00165] Additional disclosure regarding various features of disclosure are described in the following co-assigned patent applications which are incorporated by reference in their entirety for any and all purposes: United States Utility Patent Application Serial No. 13/412,487, entitled WIDE AREA POSITIONING SYSTEMS, filed on March 5, 2012; United States Utility Patent Serial No. 12/557,479 (now United States Patent No. 8,130,141), entitled WIDE AREA POSITIONING SYSTEM, filed September 10, 2009; United States Utility Patent Application Serial No. 13/412,508, entitled WIDE AREA POSITIONING

SYSTEM, filed March 5, 2012; United States Utility Patent Application Serial No. 13/296,067, entitled WIDE AREA POSITIONING SYSTEMS, filed November 14, 2011; Application Serial No. PCT/US12/44452, entitled WIDE AREA POSITIONING SYSTEMS, filed June 28, 2011); United States Patent Application Serial No. 13/535,626, entitled CODING IN WIDE AREA POSITIONING SYSTEMS, filed June 28, 2012; United States Patent Application Serial No. 13/536,051, entitled CODING IN WIDE AREA POSITIONING SYSTEM (WAPS), filed June 28, 2012; United States Patent Application Serial No. 13/565,614, entitled CELL ORGANIZATION AND TRANSMISSION SCHEMES IN A WIDE AREA POSITIONING SYSTEM (WAPS), filed August 2, 2012; United States Patent Application Serial No. 13/565,732, entitled CELL ORGANIZATION AND TRANSMISSION SCHEMES IN A WIDE AREA POSITIONING SYSTEM, filed August 2, 2012; United States Patent Application Serial No. 13/565,723, entitled CELL ORGANIZATION AND TRANSMISSION SCHEMES IN A WIDE AREA POSITIONING SYSTEM, filed August 2, 2012; United States Patent Application Serial No. 13/831,740, entitled SYSTEMS AND METHODS CONFIGURED TO ESTIMATE RECEIVER POSITION USING TIMING DATA ASSOCIATED WITH REFERENCE LOCATIONS IN THREE-DIMENSIONAL SPACE, filed March 14, 2013; United States Patent Application Serial No. 13/909,977, entitled SYSTEMS AND METHODS FOR LOCATION POSITIONING of USER DEVICE, filed June 4, 2013; NEXN-009-201 (United States Patent Application Serial No. 14/010,437, entitled SYSTEMS AND METHODS FOR PROVIDING CONDITIONAL ACCESS TO TRANSMITTED INFORMATION, filed August 26, 2013; United States Patent Application Serial No. 14/011,277, entitled METHODS AND APPARATUS FOR PSEUDO-RANDOM CODING IN A WIDE AREA POSITIONING SYSTEM (WAPS), filed August 27, 2013. The above applications, publications and patents may be individually or collectively referred to herein as “incorporated reference(s)”, “incorporated application(s)”, “incorporated publication(s)”, “incorporated patent(s)” or otherwise designated. The various aspect, details, devices, systems, and methods disclosed herein may be combined with disclosures in any of the incorporated references.

[00166] Systems and methods described herein may track the position computing devices or other things to provide position information and navigation with or to such devices and things. It is noted that the term “GPS” may refer any Global Navigation Satellite Systems (GNSS), such as GLONASS, Galileo, and Compass/Beidou. Transmitters may transmit positioning data in a signal received by a user device. Positioning data may include “timing data" that can be used to determine propagation time of a signal (e.g., time-of-arrival (TOA)), which can be used to estimate a distance between a user device and transmitter (e.g., pseudorange) by multiplying the propagation time of the signal by the speed of the signal.

[00167] Various architectures of GPS receivers are contemplated. For example, a GPS receiver's logical functions can be split into two sections: (1) signal processing and (2) position computation. The signal processing functions may be implemented in hardware and the position computation may be implemented in Firmware/Software. These functions may be carried out on a GPS ASIC "chip" having DSP hardware blocks and an ARM-processor subsystem that manages the DSP hardware and computes the position. Such GPS chips typically produce the final Latitude, Longitude and Altitude in the form of NMEA messages. Alternatively, position computation may be carried out on an apps processor resident on a handset to add additional location information and build a comprehensive position solution. The disclosure herein may apply to both implementations (in addition to other configurations for processing signals and computing position).

[00168] The various illustrative systems, methods, logical features, blocks, modules, components, circuits, and algorithm steps described herein may be implemented, performed, or otherwise controlled by suitable hardware known or later developed in the art, or by software executed by a processor (also referred to as a "processing device" and also inclusive of any number of processors), or by both. A processor may perform or cause any of the processing, computational, method steps, or other system functionality relating to the processes/methodologies and systems disclosed herein, including analysis, manipulation, conversion or creation of data, or other operations on data. A processor may include a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, server, or any combination thereof. A processor may be a conventional processor, microprocessor, controller, microcontroller, or state machine. A processor can also refer to a chip, where that chip includes various components (e.g., a microprocessor and other components). The term "processor" may refer to one, two or more processors of the same or different types. It is noted that the terms "computer" or "computing device" or "user device" or the like may refer to devices that include a processor, or may refer to the processor itself. Software may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium. A “memory” may be coupled to a processor such that the processor can read information from and write information to the memory. The storage medium may be integral to the processor. Software may be stored on or encoded as one or more instructions or code on a computer-readable medium. Computer-readable media be any available storage media, including non-volatile media (e.g., optical, magnetic, semiconductor) and carrier waves that transfer data and instructions through wireless, optical, or wired signaling media over a network using network transfer protocols. Aspects of systems and methods described herein may be implemented as functionality programmed into any of a variety of circuitry, including. Aspects may be embodied in processors having software-based circuit emulation, discrete logic, custom devices, neural logic, quantum devices, PLDs, FPGA, PAL, ASIC, MOSFET, CMOS, ECL, polymer technologies, mixed analog and digital, and hybrids thereof. Data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof. Computing networks may be used to carry out aspects and may include hardware components (servers, monitors, I/O, network connection). Application programs may carry out aspects by receiving, converting, processing, storing, retrieving, transferring and/or exporting data, which may be stored in a hierarchical, network, relational, non-relational, object-oriented, or other data source. “Data” and “information” may be used interchangeably. The words “comprise,” “comprising,” “include,” “including” and the like are to be construed in an inclusive sense (i.e., not limited to) as opposed to an exclusive sense (i.e., consisting only of). Words using the singular or plural number also include the plural or singular number respectively. The words “or” or “and” cover any of the items and all of the items in a list. “Some” and “any” and “at least one” refers to one or more. The term “device” may comprise one or more components (e.g., a processor, a memory, a screen). The terms “module,” “block,” “feature,” or “component” may refer to hardware or software, or a combination of both hardware and software, that is configured to carry out or otherwise achieve the functionality associated with those modules, blocks, features or components. Similarly, features in system and apparatus figures that are illustrated as rectangles may refer to hardware or software. It is noted that lines linking two such features may be illustrative of data transfer between those features. Such transfer may occur directly between those features or through intermediate features even if not illustrated. Where no line connects two features, transfer of data between those features is contemplated unless otherwise stated. Accordingly, the lines are provide to illustrate certain aspects, but should not be interpreted as limiting.

[00169] The disclosure is not intended to be limited to the aspects shown herein but is to be accorded the widest scope understood by a skilled artisan, including equivalent systems and methods. The protection afforded the present invention should only be limited in accordance with the following claims.

CLAIMS

1. A system for controlling access to position information by one or more applications, the system comprising at least one processor operable to:

decrypt, using a first key, a first set of encrypted position signals received from a network of terrestrial transmitters;

determine position information from the first set of decrypted position signals;

identify a first set of the position information, wherein the first set of the position information is identified based on a first level of service associated with a first application;

encrypt the first set of the position information using a second key; and

provide the encrypted first set of the position information to the first application.

2. The system of Claim 1, wherein the first set of the position information includes at least one of position coordinates, timing corrections and atmospheric measurements of one or more transmitters from the network of terrestrial transmitters.

3. The system of Claim 1, wherein the processor is further operable to:

compute estimated coordinates of a location of a receiver using the decrypted position signals, wherein the first set of the position information includes the estimated coordinates of the receiver.

4. The system of Claim 3, wherein the decrypted position signals include data that specifies atmospheric measurements at each of the terrestrial transmitters, wherein the estimated coordinates include an altitude coordinate that is computed using the decrypted position signals and at least one atmospheric measurement at the receiver.

5. The system of Claim 1, wherein the processor is further operable to:

compute estimated coordinates of a location of a receiver using the decrypted position signals; and

compute, based on a level of accuracy permitted for the first application, revised coordinates that are based on the estimated coordinates, wherein the revised coordinates are less accurate than the estimated coordinates in specifying the location of the receiver, and wherein the first set of the position information includes the revised coordinates.

6. The system of Claim 1, wherein the processor is further operable to:

identify a second set of the position information, wherein the second set of the position information is identified based on a second level of service associated with a second application, wherein certain position information included in the first set is not included in the second set;

encrypt the second set of the position information using a third key; and

provide the second set of the position information to the second application.

7. The system of Claim 1, wherein the processor is further operable to:

decrypt, using the first key or a third key, a second set of encrypted position signals received from the network of terrestrial transmitters, wherein the first set of encrypted position signals are received at a first location of the receiver, and the second set of encrypted position signals are receiver at a second location of the receiver;

determine additional position information from the second set of decrypted position signals;

identify a second set of the additional position information, wherein the second set of the additional position information is identified based on a second level of service associated with a second application;

encrypt the second set of the position information using a fourth key ; and

provide the second set of the position information to the second application.

8. The system of Claim 1, wherein the processor is further operable to:

determine, prior identifying the first set of the position information, whether information specifying the first level of service is stored on the receiver;

upon determining that the information specifying the first level of service is not stored on the receiver, access a first developer key that is associated with the first application;

send the first developer key to a server; and

receive the information specifying the first level of service in response to sending the first developer key to the server.

9. The system of Claim 8, wherein the information specifying the first level of service is included in a first authorized service-level certificate associated with the first application, and wherein the certificate is associated with the developer key.

10. The system of Claim 1, wherein the first level of service specifies a time period during which the second key can be used to encrypt the first set of the position information and any subsequent sets of any subsequent position information.

11. The system of Claim 1, wherein the second key is a session key that is generated after the position signals are decrypted.

12. The system of Claim 1, wherein first application runs on a remote server, and the first set of the position information is provided to the remote server.

13. The system of Claim 1, wherein the processor is further operable to:

determine the first level of service based on parameters that are specified in a first certificate associated with the first application.

14. The system of Claim 1, wherein the processor is further operable to:

scramble the position information before the position information is sent through an unprotected communication pathway; and

unscramble the scrambled position information before identifying the first set.

15. The system of Claim 3, wherein the processor is further operable to:

scramble the estimated coordinates before the estimated coordinates are sent through an unprotected communication pathway; and

unscramble the scrambled estimated coordinates before encrypting the first set.

16. The system of Claim 1, wherein the processor is further operable to:

select the first key from among a plurality of keys, wherein a CRC field of the encrypted position signals passes check only when the first key is used to decrypt the first set of encrypted position signals.

17. The system of Claim 1, wherein the processor is further operable to:

select the first key from among a plurality of keys, wherein data of the decrypted position signals matches an expected range of values only when the first key is used to decrypt the first set of encrypted position signals.

18. The system of Claim 1, wherein the first set of encrypted position signals includes packet data from multiple transmitters, and wherein the processor is further operable to:

select the first key from among a plurality of keys, wherein the packet data from the multiple transmitters pass one or more coherency checks only when the first key is used to decrypt the first set of encrypted position signals.

19. A computer-implemented method for controlling access to position information by one or more applications, the method comprising steps to:

decrypt, using a first key, a first set of encrypted position signals received from a network of terrestrial transmitters;

determine position information from the first set of decrypted position signals;

identify a first set of the position information, wherein the first set of the position information is identified based on a first level of service associated with a first application;

encrypt the first set of the position information using a second key; and

provide the encrypted first set of the position information to the first application, wherein at least one processor implements at least one of the above steps.

20. The computer-implemented method of Claim 19, wherein the first set of the position information includes at least one of position coordinates, timing corrections and atmospheric measurements of one or more transmitters from the network of terrestrial transmitters.

21. The computer-implemented method of Claim 19, wherein the method includes steps to:

compute estimated coordinates of a location of a receiver using the decrypted position signals, wherein the first set of the position information includes the estimated coordinates of the receiver.

22. The computer-implemented method of Claim 21, wherein the decrypted position signals include data that specifies atmospheric measurements at each of the terrestrial transmitters, wherein the estimated coordinates include an altitude coordinate that is computed using the decrypted position signals and at least one atmospheric measurement at the receiver.

23. The computer-implemented method of Claim 19, wherein the method includes steps to:

compute estimated coordinates of a location of a receiver using the decrypted position signals; and

compute, based on a level of accuracy permitted for the first application, revised coordinates that are based on the estimated coordinates, wherein the revised coordinates are less accurate than the estimated coordinates in specifying the location of the receiver, and wherein the first set of the position information includes the revised coordinates.

24. The computer-implemented method of Claim 19, wherein the processor is further operable to:

identify a second set of the position information, wherein the second set of the position information is identified based on a second level of service associated with a second application, wherein certain position information included in the first set is not included in the second set;

encrypt the second set of the position information using a third key; and

provide the second set of the position information to the second application.

25. The computer-implemented method of Claim 19, wherein the processor is further operable to:

decrypt, using the first key or a third key, a second set of encrypted position signals received from the network of terrestrial transmitters, wherein the first set of encrypted position signals are received at a first location of the receiver, and the second set of encrypted position signals are receiver at a second location of the receiver;

determine additional position information from the second set of decrypted position signals;

identify a second set of the additional position information, wherein the second set of the additional position information is identified based on a second level of service associated with a second application;

encrypt the second set of the position information using a fourth key ; and

provide the second set of the position information to the second application.

26. The computer-implemented method of Claim 19, wherein the processor is further operable to:

determine, prior identifying the first set of the position information, whether information specifying the first level of service is stored on the receiver;

upon determining that the information specifying the first level of service is not stored on the receiver, access a first developer key that is associated with the first application;

send the first developer key to a server; and

receive the information specifying the first level of service in response to sending the first developer key to the server.

27. The computer-implemented method of Claim 26, wherein the information specifying the first level of service is included in a first authorized service-level certificate associated with the first application, and wherein the certificate is associated with the developer key.

28. The computer-implemented method of Claim 19, wherein the first level of service specifies a time period during which the second key can be used to encrypt the first set of the position information and any subsequent sets of any subsequent position information.

29. The computer-implemented method of Claim 19, wherein the second key is a session key that is generated after the position signals are decrypted.

30. The computer-implemented method of Claim 19, wherein first application runs on a remote server, and the first set of the position information is provided to the remote server.

31. The computer-implemented method of Claim 19, wherein the method includes steps to:

determine the first level of service based on parameters that are specified in a first certificate associated with the first application.

32. The computer-implemented method of Claim 19, wherein the method includes steps to:

scramble the position information before the position information is sent through an unprotected communication pathway; and

unscramble the scrambled position information before identifying the first set.

33. The computer-implemented method of Claim 21, wherein the method includes steps to:

scramble the estimated coordinates before the estimated coordinates are sent through an unprotected communication pathway; and

unscramble the scrambled estimated coordinates before encrypting the first set.

34. The computer-implemented method of Claim 19, wherein the method includes steps to:

select the first key from among a plurality of keys, wherein a CRC field of the encrypted position signals passes check only when the first key is used to decrypt the first set of encrypted position signals.

35. The computer-implemented method of Claim 19, wherein the method includes steps to:

select the first key from among a plurality of keys, wherein data of the decrypted position signals matches an expected range of values only when the first key is used to decrypt the first set of encrypted position signals.

36. The computer-implemented method of Claim 19, wherein the first set of encrypted position signals includes packet data from multiple transmitters, and wherein the method includes steps to:

select the first key from among a plurality of keys, wherein the packet data from the multiple transmitters pass one or more coherency checks only when the first key is used to decrypt the first set of encrypted position signals.

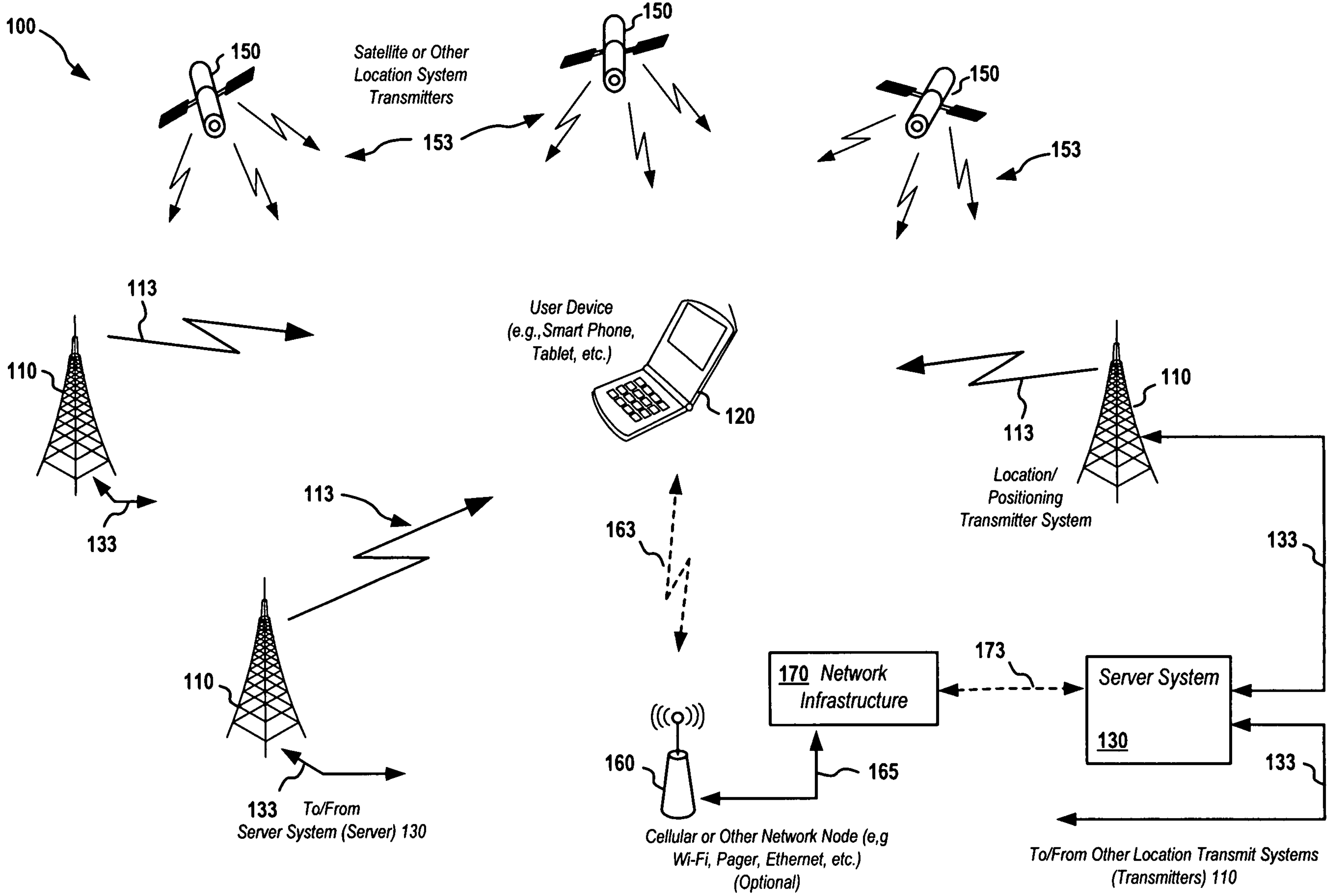

100
150
Satellite or Other
Location System
Transmitters
150
150
153
153
113
110
133
User Device
(e.g.,Smart Phone,
Tablet, etc.)
120
113
110
Location/
Positioning
Transmitter System
113
163
110
133 To/From
Server System (Server) 130
160
Cellular or Other Network Node (e,g
Wi-Fi, Pager, Ethernet, etc.)
(Optional)
170 Network
Infrastructure
165
173
Server System
130
133
133
To/From Other Location Transmit Systems
(Transmitters) 110

FIG. 1

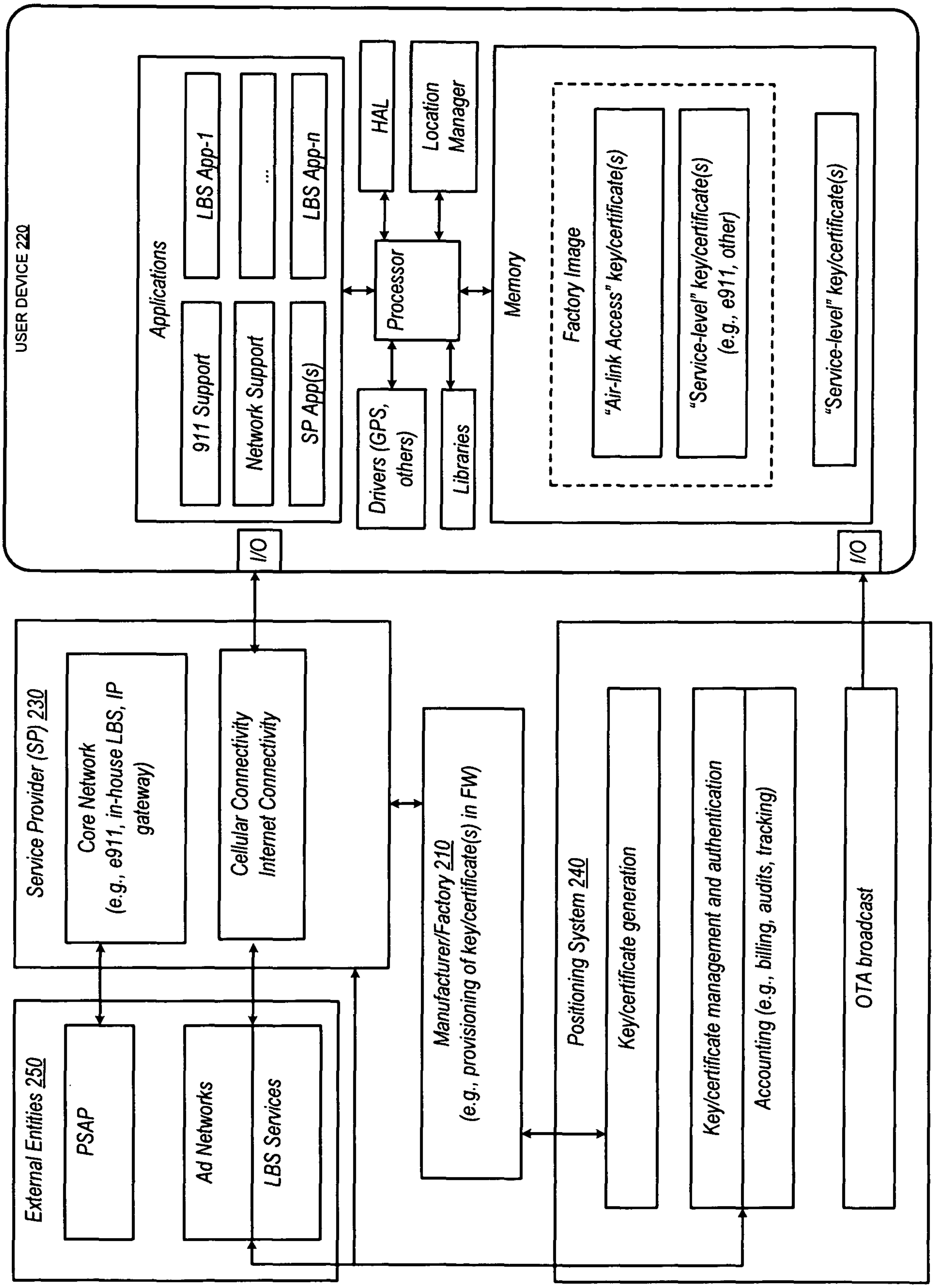

USER DEVICE 220
Applications
911 Support
Network Support
SP App(s)
LBS App-1
...
LBS App-n
HAL
Location Manager
Processor
Drivers (GPS, others)
Libraries
Memory
Factory Image
"Air-link Access" key/certificate(s)
"Service-level" key/certificate(s) (e.g., e911, other)
"Service-level" key/certificate(s)
I/O
I/O
Service Provider (SP) 230
Core Network (e.g., e911, in-house LBS, IP gateway)
Cellular Connectivity Internet Connectivity
Manufacturer/Factory 210 (e.g., provisioning of key/certificate(s) in FW)
Positioning System 240
Key/certificate generation
Key/certificate management and authentication
Accounting (e.g., billing, audits, tracking)
OTA broadcast
External Entities 250
PSAP
Ad Networks
LBS Services

FIG. 2

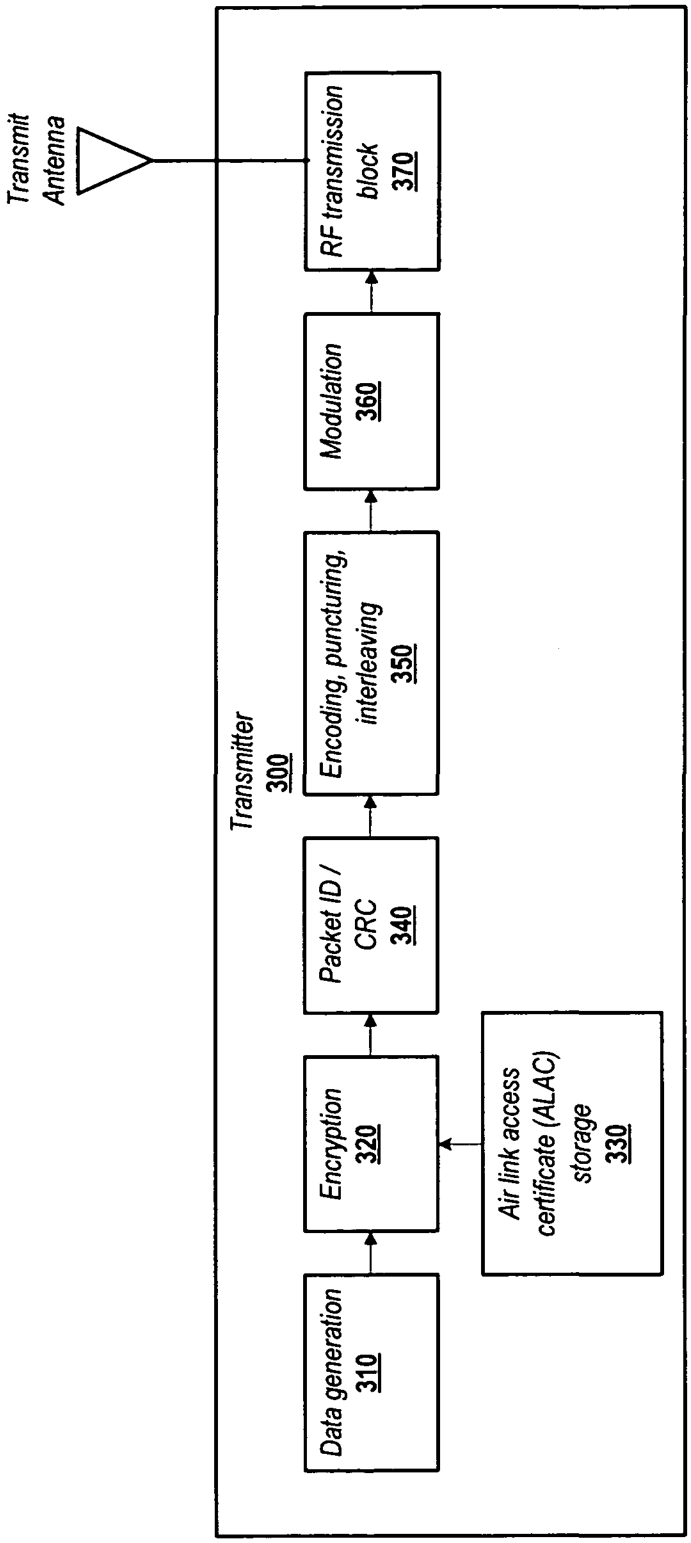

Transmitter
300
Data generation
310
Encryption
320
Air link access
certificate (ALAC)
storage
330
Packet ID /
CRC
340
Encoding, puncturing,
interleaving
350
Modulation
360
RF transmission
block
370
Transmit
Antenna

FIG. 3

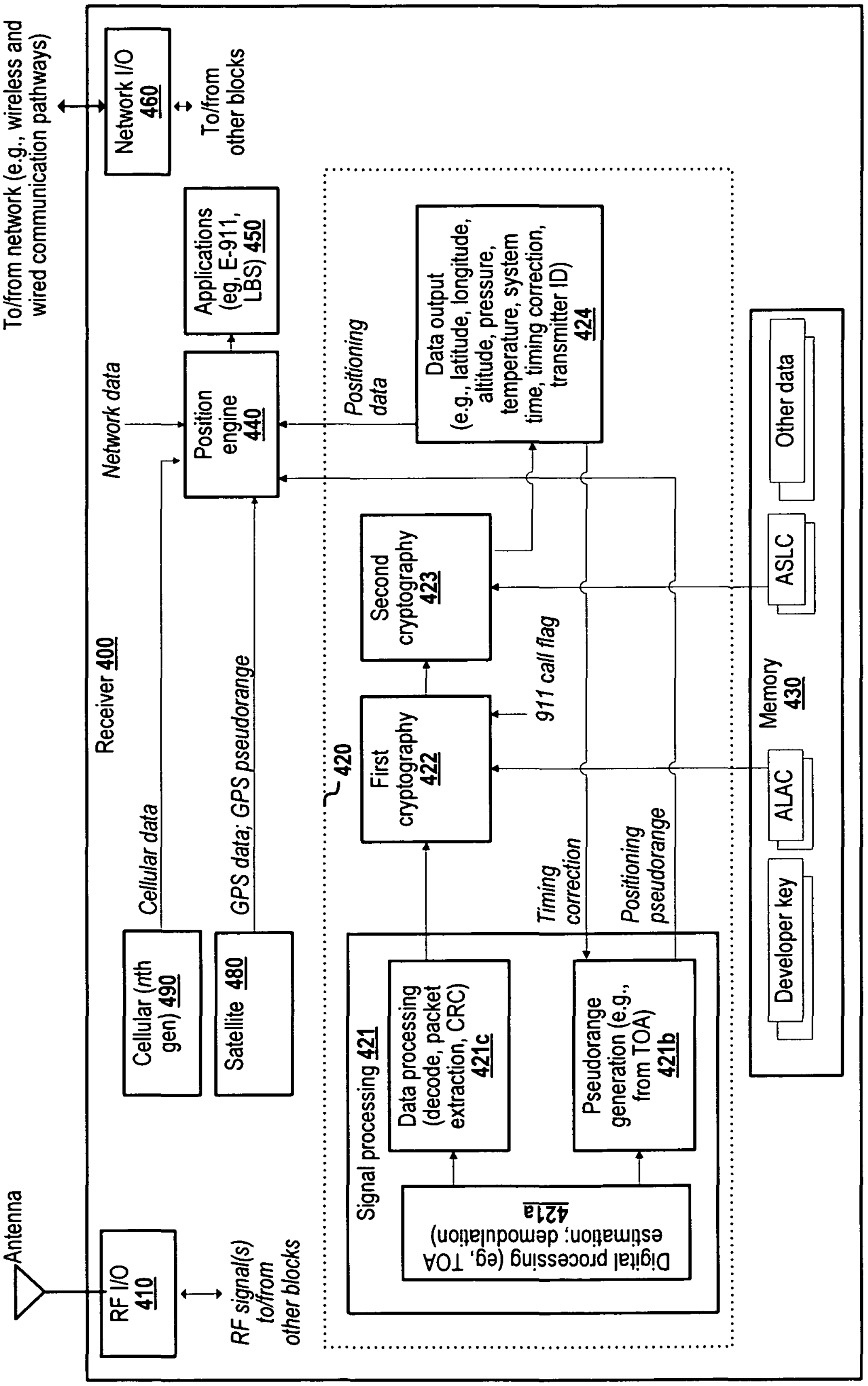

To/from network (e.g., wireless and wired communication pathways)
Network I/O 460
To/from other blocks
Applications (eg, E-911, LBS) 450
Position engine 440
Network data
Positioning data
Data output (e.g., latitude, longitude, altitude, pressure, temperature, system time, timing correction, transmitter ID) 424
Other data
Second cryptography 423
ASLC
911 call flag
Memory 430
Receiver 400
Cellular data
GPS data; GPS pseudorange
420
First cryptography 422
ALAC
Developer key
Timing correction
Positioning pseudorange
Cellular (nth gen) 490
Satellite 480
Signal processing 421
Data processing (decode, packet extraction, CRC) 421c
Pseudorange generation (e.g., from TOA) 421b
Digital processing (eg, TOA estimation; demodulation) 421a
Antenna
RF I/O 410
RF signal(s) to/from other blocks

FIG. 4A

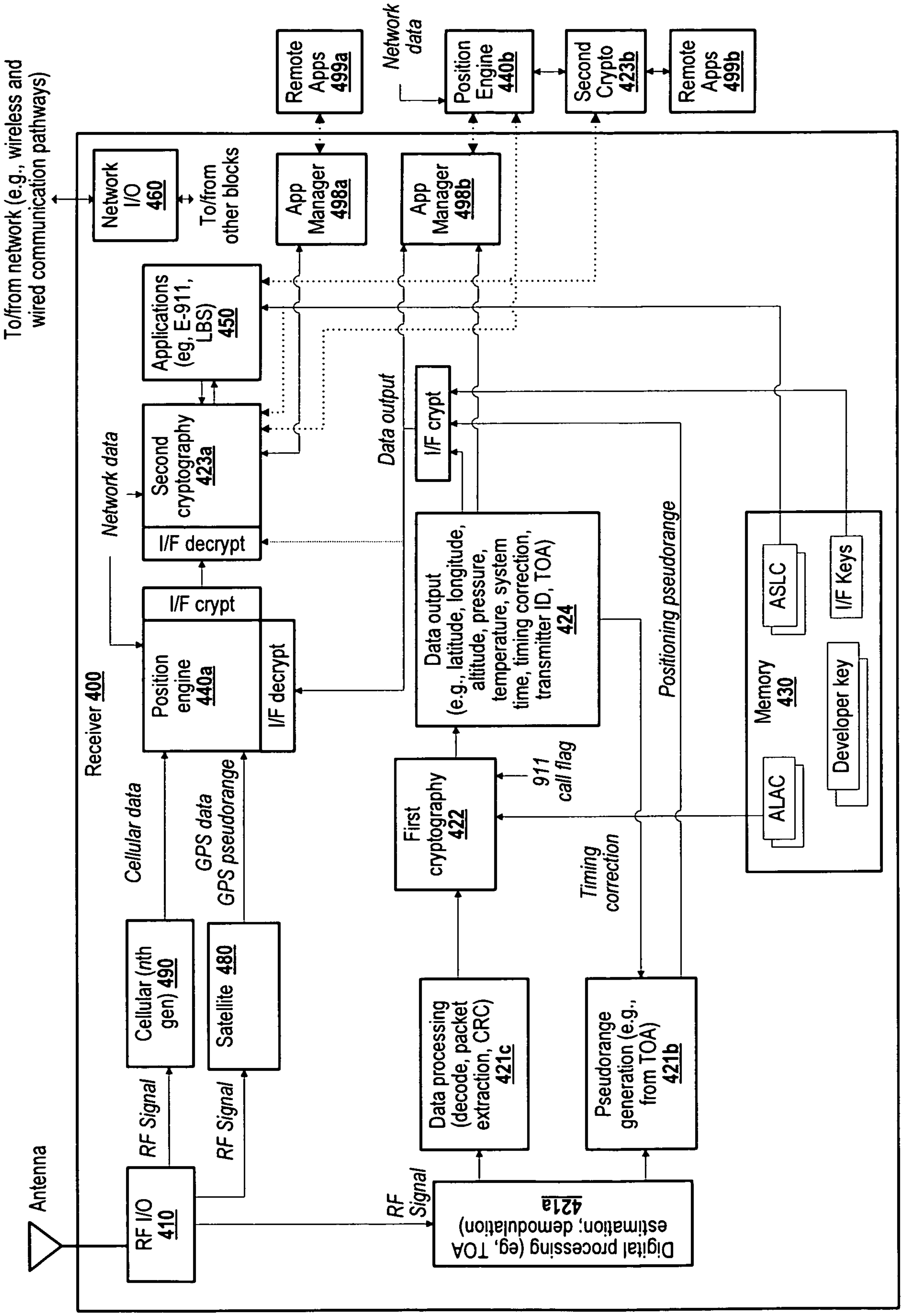

To/from network (e.g., wireless and wired communication pathways)
Antenna
Receiver 400
RF I/O 410
RF Signal
RF Signal
RF Signal
Cellular (nth gen) 490
Satellite 480
Cellular data
GPS data
GPS pseudorange
Position engine 440a
I/F decrypt
I/F crypt
Network data
I/F decrypt
Second cryptography 423a
Applications (eg, E-911, LBS) 450
Network I/O 460
To/from other blocks
App Manager 498a
App Manager 498b
Remote Apps 499a
Network data
Position Engine 440b
Second Crypto 423b
Remote Apps 499b
Data output
I/F crypt
Digital processing (eg, TOA estimation; demodulation) 421a
Data processing (decode, packet extraction, CRC) 421c
Pseudorange generation (e.g., from TOA) 421b
First cryptography 422
911 call flag
Timing correction
Data output (e.g., latitude, longiture, altitude, pressure, temperature, system time, timing correction, transmitter ID, TOA) 424
Positioning pseudorange
Memory 430
ALAC
ASLC
Developer key
I/F Keys

FIG. 4B

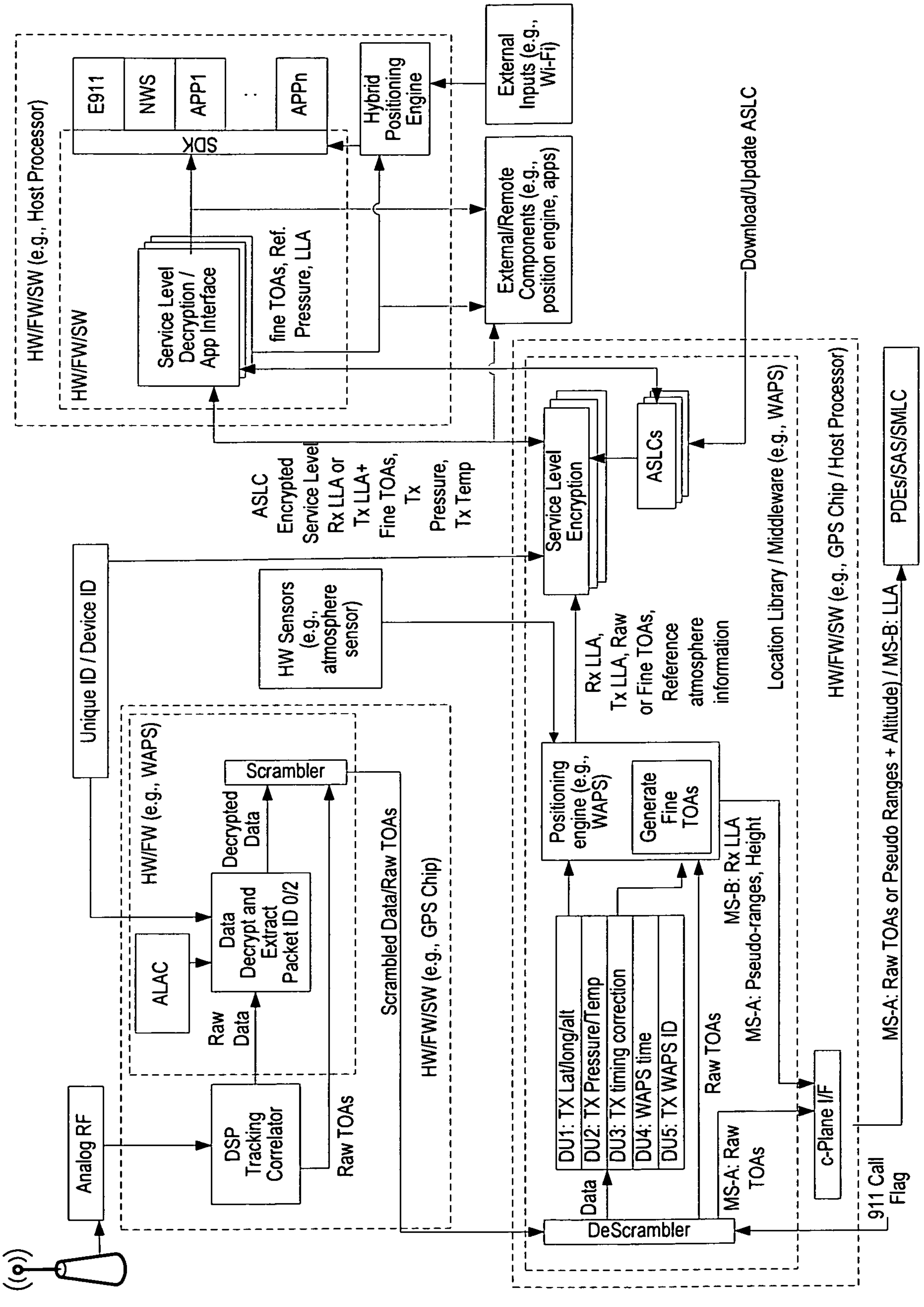

Analog RF
DSP Tracking Correlator
Raw TOAs
Raw Data
ALAC
Data Decrypt and Extract Packet ID 0/2
Decrypted Data
Scrambler
HW/FW (e.g., WAPS)
Scrambled Data/Raw TOAs
HW/FW/SW (e.g., GPS Chip)
Unique ID / Device ID
HW Sensors (e.g., atmosphere sensor)
ASLC Encrypted Service Level Rx LLA or Tx LLA+ Fine TOAs, Tx Pressure, Tx Temp
HW/FW/SW (e.g., Host Processor)
HW/FW/SW
Service Level Decryption / App Interface
fine TOAs, Ref. Pressure, LLA
SDK
E911
NWS
APP1
..
APPn
Hybrid Positioning Engine
External Inputs (e.g., Wi-Fi)
External/Remote Components (e.g., position engine, apps)
Download/Update ASLC
Service Level Encryption
ASLCs
Rx LLA, Tx LLA, Raw or Fine TOAs, Reference atmosphere information
Positioning engine (e.g., WAPS)
Generate Fine TOAs
Location Library / Middleware (e.g., WAPS)
HW/FW/SW (e.g., GPS Chip / Host Processor)
DU1: TX Lat/long/alt
DU2: TX Pressure/Temp
DU3: TX timing correction
DU4: WAPS time
DU5: TX WAPS ID
Data
Raw TOAs
MS-B: Rx LLA
MS-A: Pseudo-ranges, Height
MS-A: Raw TOAs
DeScrambler
c-Plane I/F
911 Call Flag
MS-A: Raw TOAs or Pseudo Ranges + Altitude) / MS-B: LLA
PDEs/SAS/SMLC

FIG. 4C

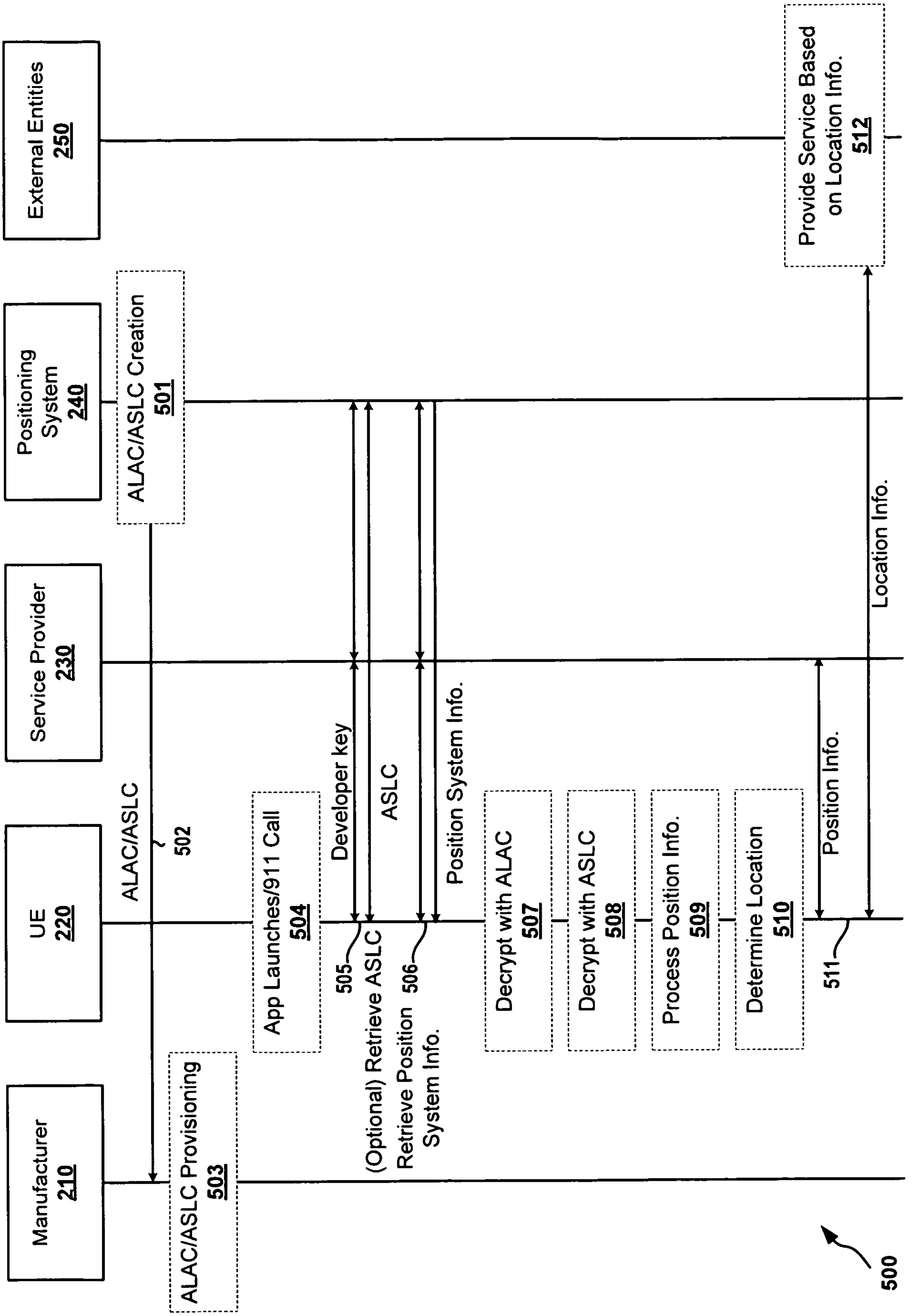

Manufacturer
210
UE
220
Service Provider
230
Positioning System
240
External Entities
250
ALAC/ASLC Creation
501
ALAC/ASLC
502
ALAC/ASLC Provisioning
503
App Launches/911 Call
504
Developer key
ASLC
Position System Info.
505
(Optional) Retrieve ASLC
506
Retrieve Position System Info.
Decrypt with ALAC
507
Decrypt with ASLC
508
Process Position Info.
509
Determine Location
510
Position Info.
511
Location Info.
Provide Service Based on Location Info.
512
500

FIG. 5A

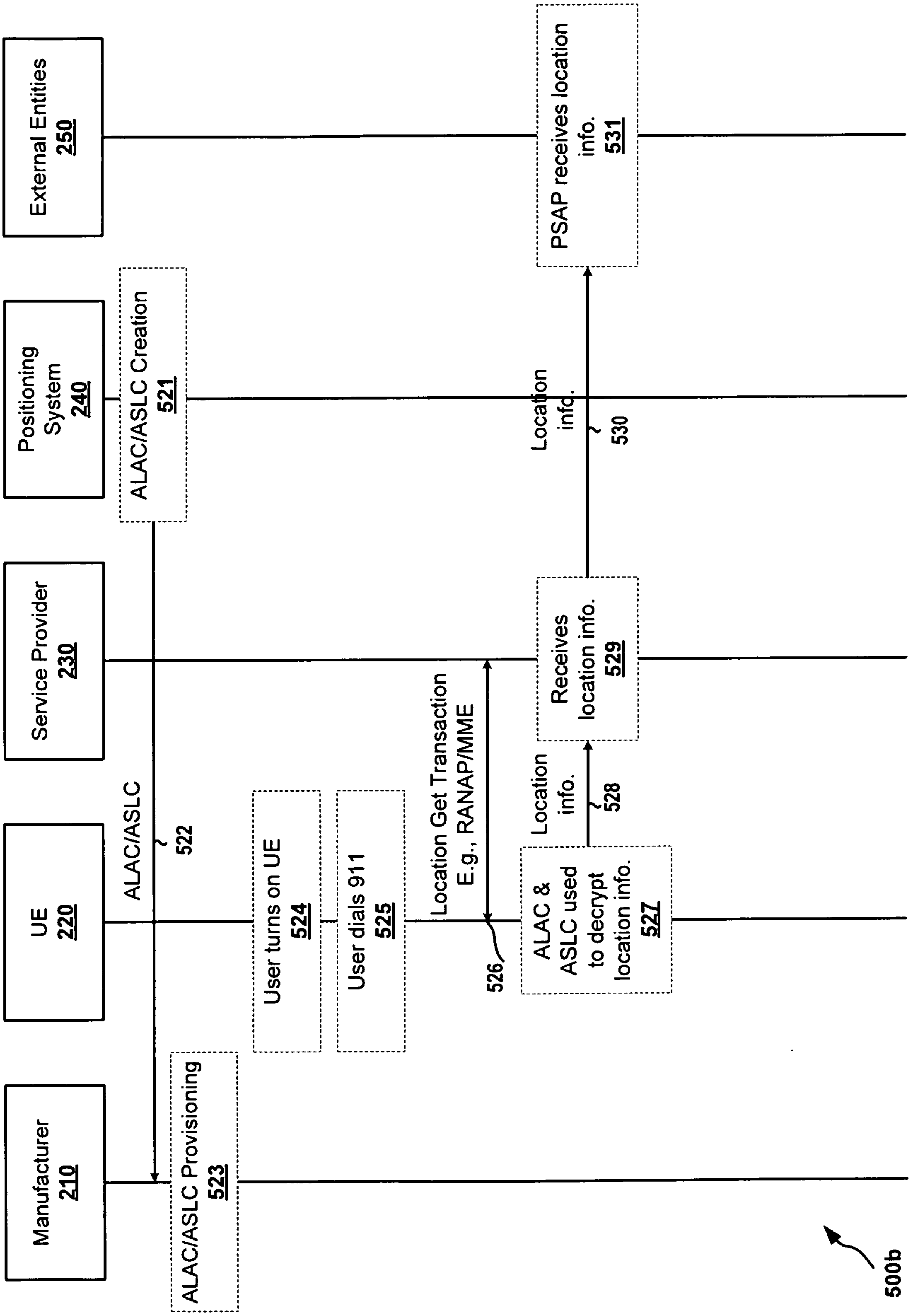

Manufacturer
210
UE
220
Service Provider
230
Positioning
System
240
External Entities
250
ALAC/ASLC Creation
521
ALAC/ASLC
522
ALAC/ASLC Provisioning
523
User turns on UE
524
User dials 911
525
Location Get Transaction
E.g., RANAP/MME
526
ALAC &
ASLC used
to decrypt
location info.
527
Location
info.
528
Receives
location info.
529
Location
info.
530
PSAP receives location
info.
531
500b

FIG. 5B

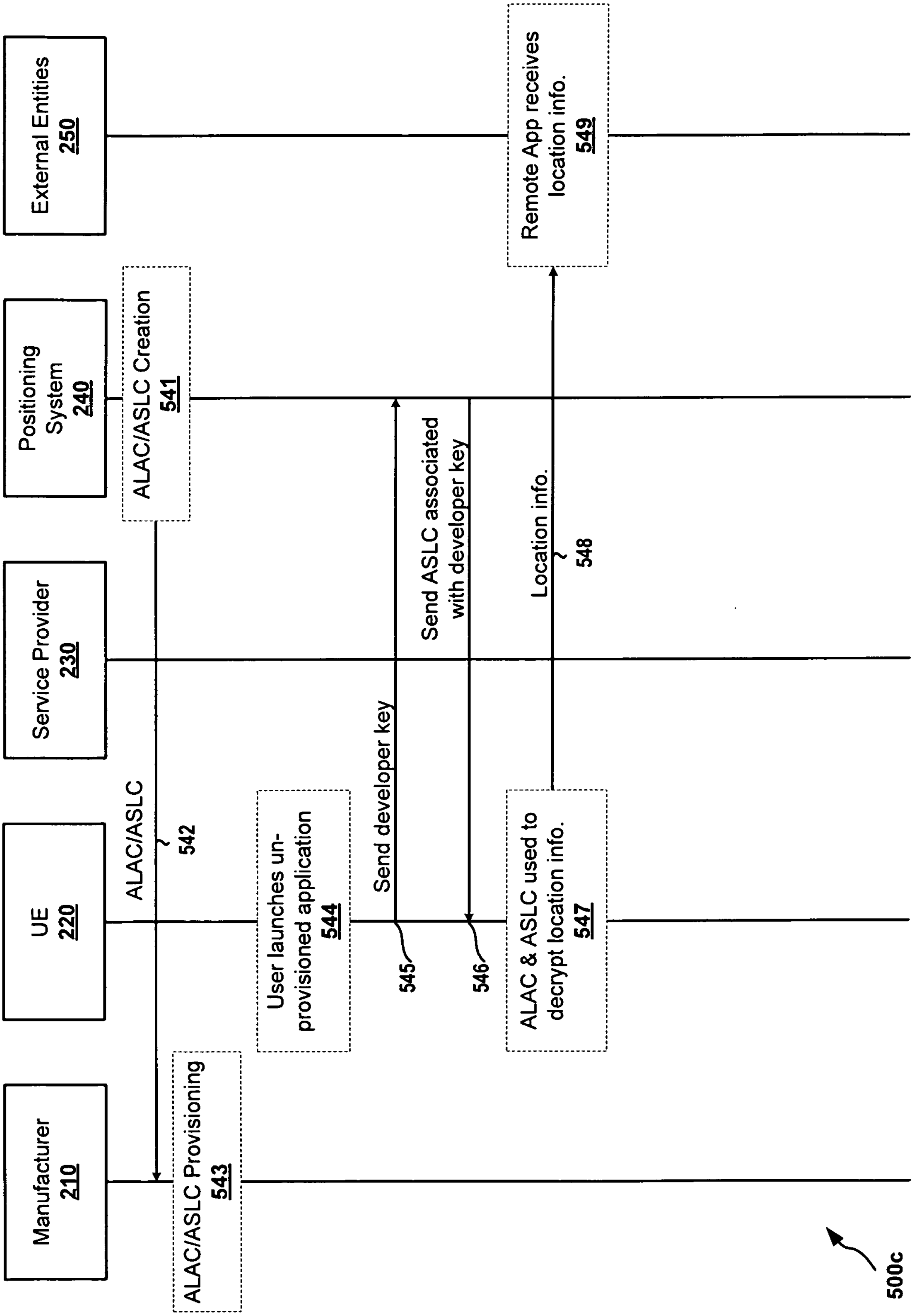

Manufacturer
210
UE
220
Service Provider
230
Positioning System
240
External Entities
250
ALAC/ASLC Creation
541
ALAC/ASLC
542
ALAC/ASLC Provisioning
543
User launches un-provisioned application
544
Send developer key
545
Send ASLC associated with developer key
546
ALAC & ASLC used to decrypt location info.
547
Location info.
548
Remote App receives location info.
549
500c

FIG. 5C

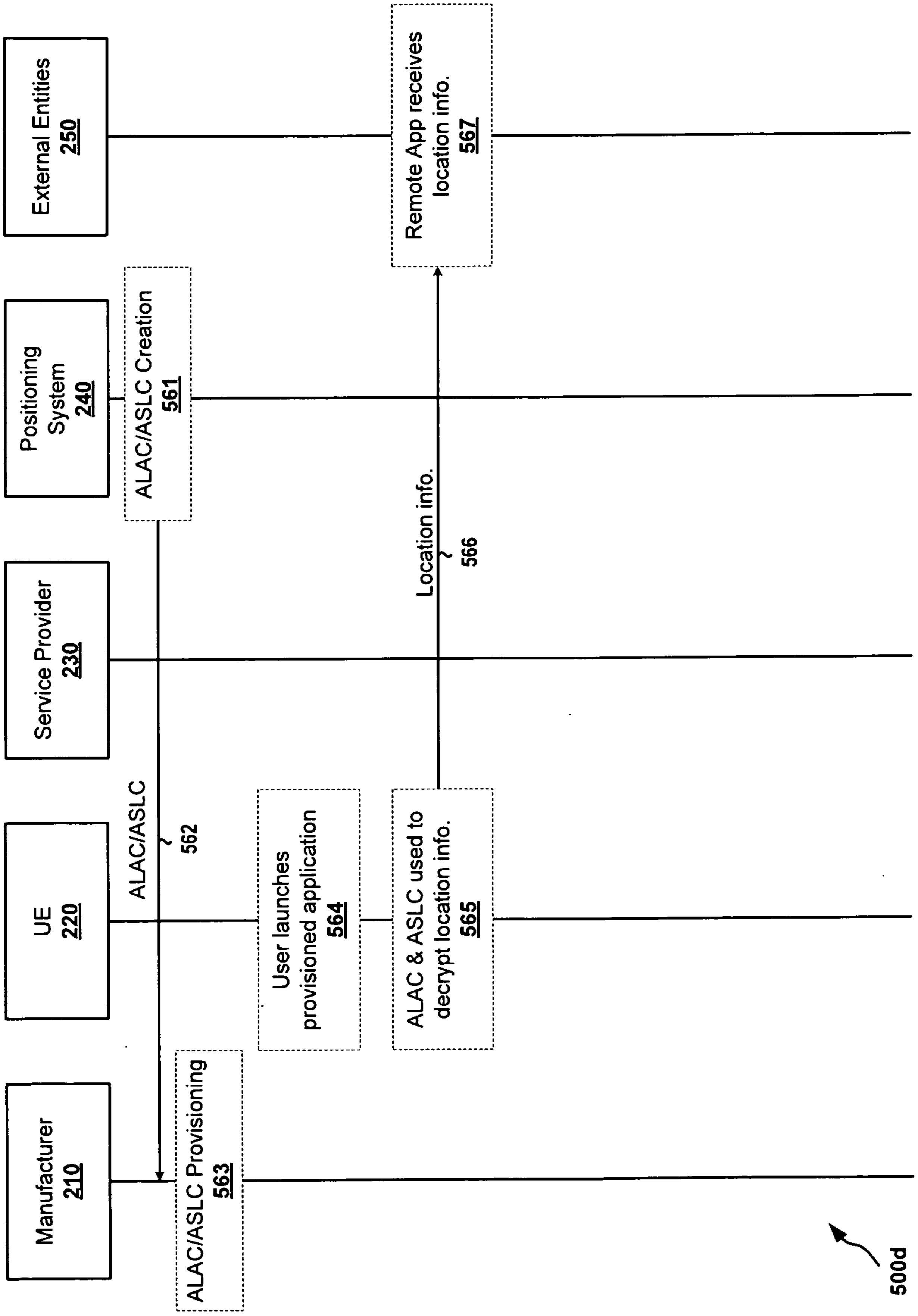

Manufacturer
210
UE
220
Service Provider
230
Positioning System
240
External Entities
250
ALAC/ASLC Creation
561
ALAC/ASLC
562
ALAC/ASLC Provisioning
563
User launches provisioned application
564
ALAC & ASLC used to decrypt location info.
565
Location info.
566
Remote App receives location info.
567
500d

FIG. 5D

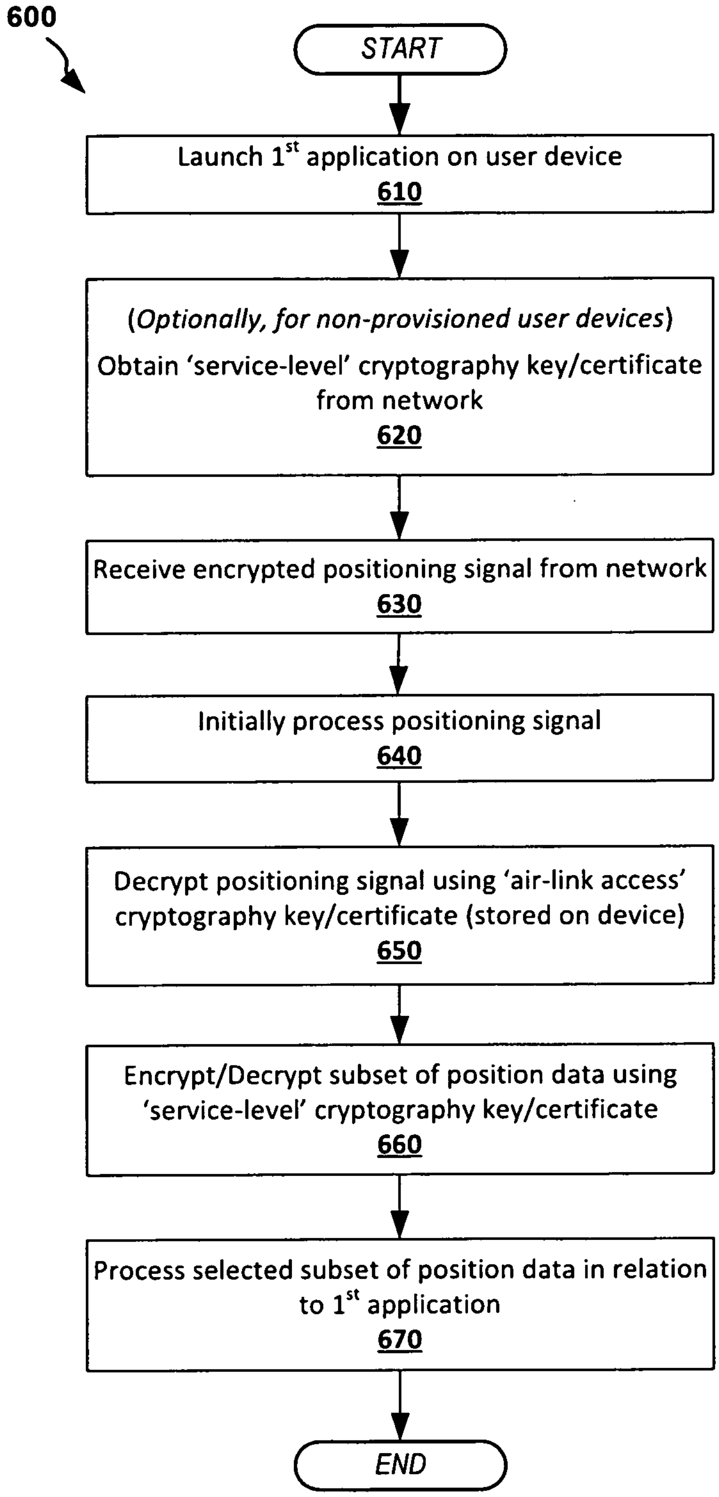

600
START
Launch 1st application on user device
610
(Optionally, for non-provisioned user devices)
Obtain 'service-level' cryptography key/certificate from network
620
Receive encrypted positioning signal from network
630
Initially process positioning signal
640
Decrypt positioning signal using 'air-link access' cryptography key/certificate (stored on device)
650
Encrypt/Decrypt subset of position data using 'service-level' cryptography key/certificate
660
Process selected subset of position data in relation to 1st application
670
END

FIG. 6

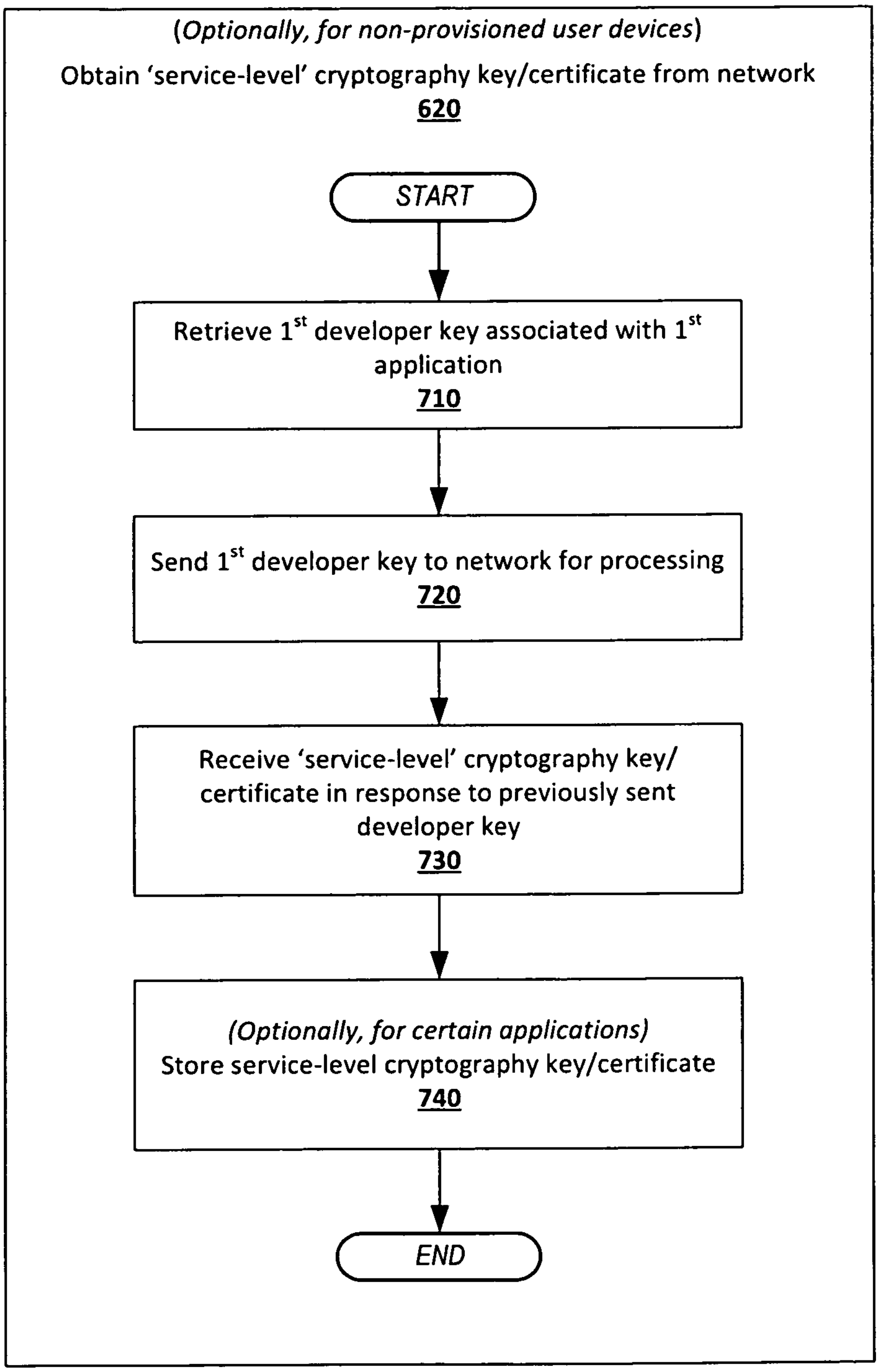

(Optionally, for non-provisioned user devices)
Obtain 'service-level' cryptography key/certificate from network
620
START
Retrieve 1st developer key associated with 1st application
710
Send 1st developer key to network for processing
720
Receive 'service-level' cryptography key/ certificate in response to previously sent developer key
730
(Optionally, for certain applications)
Store service-level cryptography key/certificate
740
END

FIG. 7

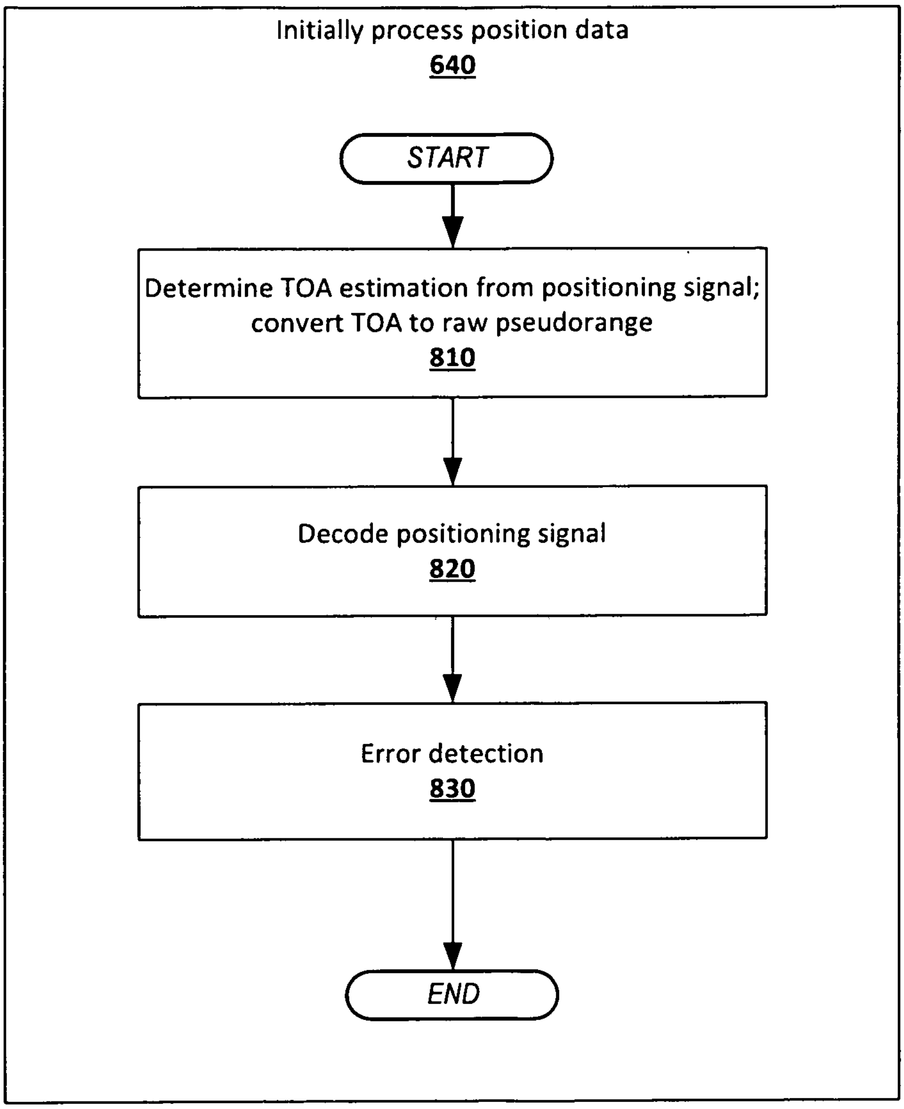

Initially process position data
640
START
Determine TOA estimation from positioning signal; convert TOA to raw pseudorange
810
Decode positioning signal
820
Error detection
830
END

FIG. 8

Application • *E-911* • *LBS* • *NW*	*UE (unique ID)*	*Service* • *Accuracy* • *Coverage* • *Time* • *DUs*	*MNO* • *ATT* • *Verizon* • *Sprint* • *Others*	*OEM* • *Apple* • *Samsung* • *MOT* • *Others*	*Developer* • *Apple* • *Google* • *Microsoft* • *Other*	*User (unique ID)*	*Type of request (ie, to determine service needs)*	*[OTHER]*

FIG. 9

X	X	X	X	Y	Z	W	Payload (95

XXXX	: Packet type
Y	: Encryption bit
Z	: Start bit
W	: Stop bit

FIG. 10A

0	1	1	0	1	1	0	Payload (95 bits)	First frame of packet type 6, encrypted
0	1	1	0	1	0	0	Payload (95 bits)	Continuation of packet
0	1	1	0	1	0	0	Payload (95 bits)	Continuation of packet
							•••	•••
0	1	1	0	1	0	1	Payload (95 bits)	Last frame of packet
1	1	0	0	0	1	0	Payload (95 bits)	First frame of packet type 12, unencrypted
1	1	1	0	0	0	1	Payload (95 bits)	Last slot of packet
1	0	0	1	1	1	1	Payload (95 bits)	First & last frame of packet type 9, encrypted

FIG. 10B

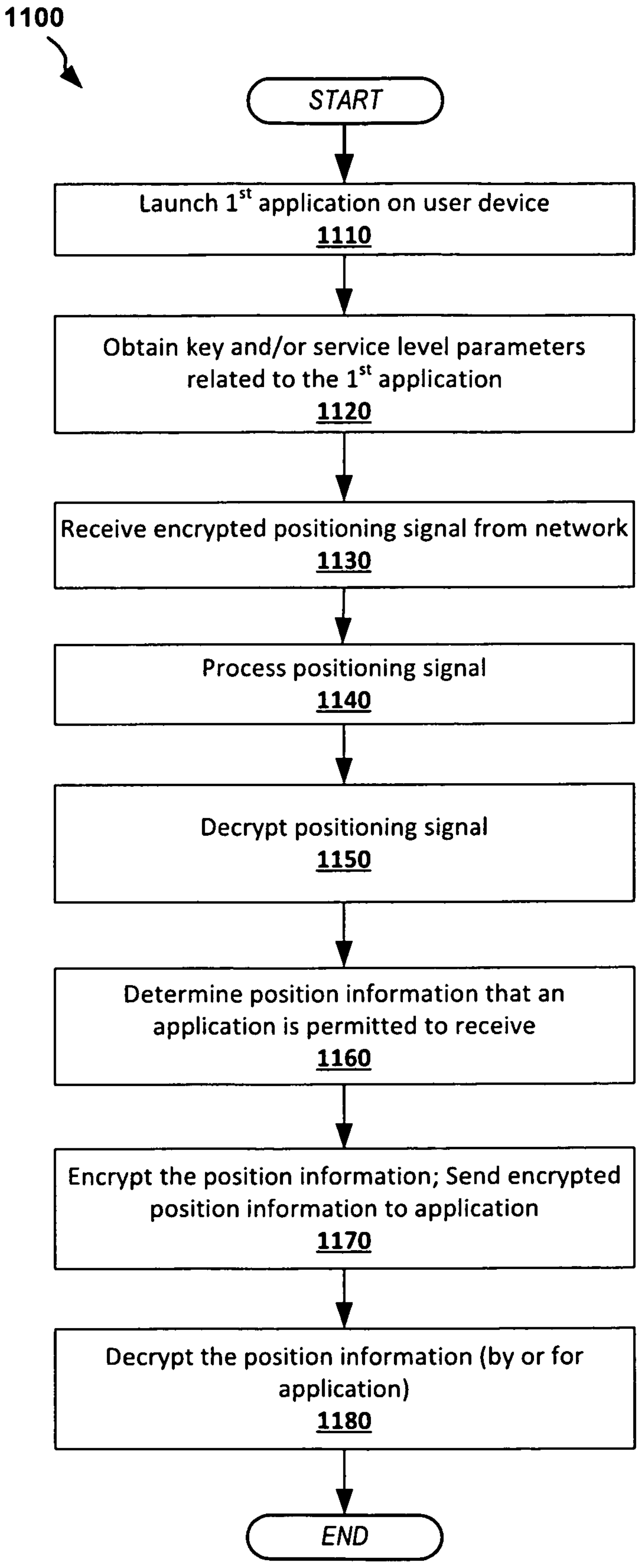

1100
START
Launch 1st application on user device
1110
Obtain key and/or service level parameters related to the 1st application
1120
Receive encrypted positioning signal from network
1130
Process positioning signal
1140
Decrypt positioning signal
1150
Determine position information that an application is permitted to receive
1160
Encrypt the position information; Send encrypted position information to application
1170
Decrypt the position information (by or for application)
1180
END

FIG. 11

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/08
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2001/055392 A1 (MCDONNELL JAMES THOMAS EDWARD [GB] ET AL) 27 December 2001 (2001-12-27) abstract paragraph [0029] paragraph [0051] - paragraph [0054] figure 7 -----	1-36
A	US 2011/078376 A1 (DESHPANDE MANOJ M [US] ET AL) 31 March 2011 (2011-03-31) abstract paragraph [0023] - paragraph [0028] paragraph [0049] figure 5 claim 1 -----	1-36

□ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 29 November 2013	Date of mailing of the international search report 06/12/2013
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Canosa Aresté, C

1

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2001055392 A1	27-12-2001	DE 60131799 T2	05-06-2008
		EP 1139687 A2	04-10-2001
		JP 2001320760 A	16-11-2001
		US 2001055392 A1	27-12-2001
US 2011078376 A1	31-03-2011	CN 102550050 A	04-07-2012
		KR 20120079117 A	11-07-2012
		US 2011078376 A1	31-03-2011
		WO 2011041329 A1	07-04-2011

(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 104620560 A

(43) 申请公布日 2015.05.13

(21) 申请号 201380046918.3

(22) 申请日 2013.09.10

(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

(71) 申请人 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 上海德昭知识产权代理有限
公司 31204

代理人 郁旦蓉

(51) Int.Cl.

H04L 29/08(2006.01)

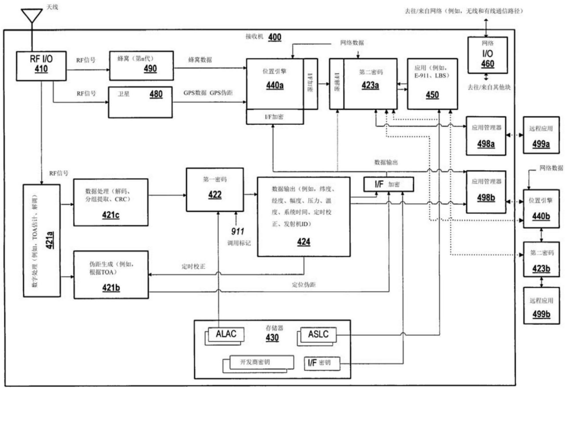
权利要求书4页 说明书22页 附图13页

(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。



1.一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，所述处理器用于：

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。

2.根据权利要求1所述的系统，其中，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。

3.根据权利要求1所述的系统，其中，所述处理器还用于：

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。

4.根据权利要求3所述的系统，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。

5.根据权利要求1所述的系统，其中，所述处理器还用于：

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。

6.根据权利要求1所述的系统，其中，所述处理器还用于：

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。

7.根据权利要求1所述的系统，其中，所述处理器还用于：

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。

8.根据权利要求1所述的系统，其中，所述处理器还用于：

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。

9. 根据权利要求 8 所述的系统，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，所述证书与所述开发商密钥相关联。

10. 根据权利要求 1 所述的系统，其中，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。

11. 根据权利要求 1 所述的系统，其中，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。

12. 根据权利要求 1 所述的系统，其中，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。

13. 根据权利要求 1 所述的系统，其中，所述处理器还用于：

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 所述的系统，其中，所述处理器还用于：

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。

15. 根据权利要求 3 所述的系统，其中，所述处理器还用于：

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。

16. 根据权利要求 1 所述的系统，其中，所述处理器还用于：

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 所述的系统，其中，所述处理器还用于：

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 所述的系统，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，所述处理器还用于：

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. 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，该方法包括以下步骤：

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，

其中，至少一个处理器实施上述步骤中的至少一者。

20.根据权利要求19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。

21.根据权利要求19所述的计算机实施的方法，其中，该方法还包括以下步骤：

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。

22.根据权利要求21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。

23.根据权利要求19所述的计算机实施的方法，其中，该方法包括以下步骤：

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。

24.根据权利要求19所述的计算机实施的方法，其中，所述处理器还用于：

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。

25.根据权利要求19所述的计算机实施的方法，其中，所述处理器还用于：

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。

26.根据权利要求19所述的计算机实施的方法，其中，所述处理器还用于：

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。

27. 根据权利要求 26 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，所述证书与所述开发商密钥相关联。

28. 根据权利要求 19 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。

29. 根据权利要求 19 所述的计算机实施的方法，其中，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。

30. 根据权利要求 19 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，并且所述位置信息的所述第一集合被提供至所述远程服务器。

31. 根据权利要求 19 所述的计算机实施的方法，其中，该方法包括以下步骤：

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。

32. 根据权利要求 19 所述的计算机实施的方法，其中，该方法包括以下步骤：

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。

33. 根据权利要求 21 所述的计算机实施的方法，其中，该方法包括以下步骤：

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。

34. 根据权利要求 19 所述的计算机实施的方法，其中，该方法包括以下步骤：

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。

35. 根据权利要求 19 所述的计算机实施的方法，其中，该方法包括以下步骤：

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。

36. 根据权利要求 19 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，所述方法包括以下步骤：

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。

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。

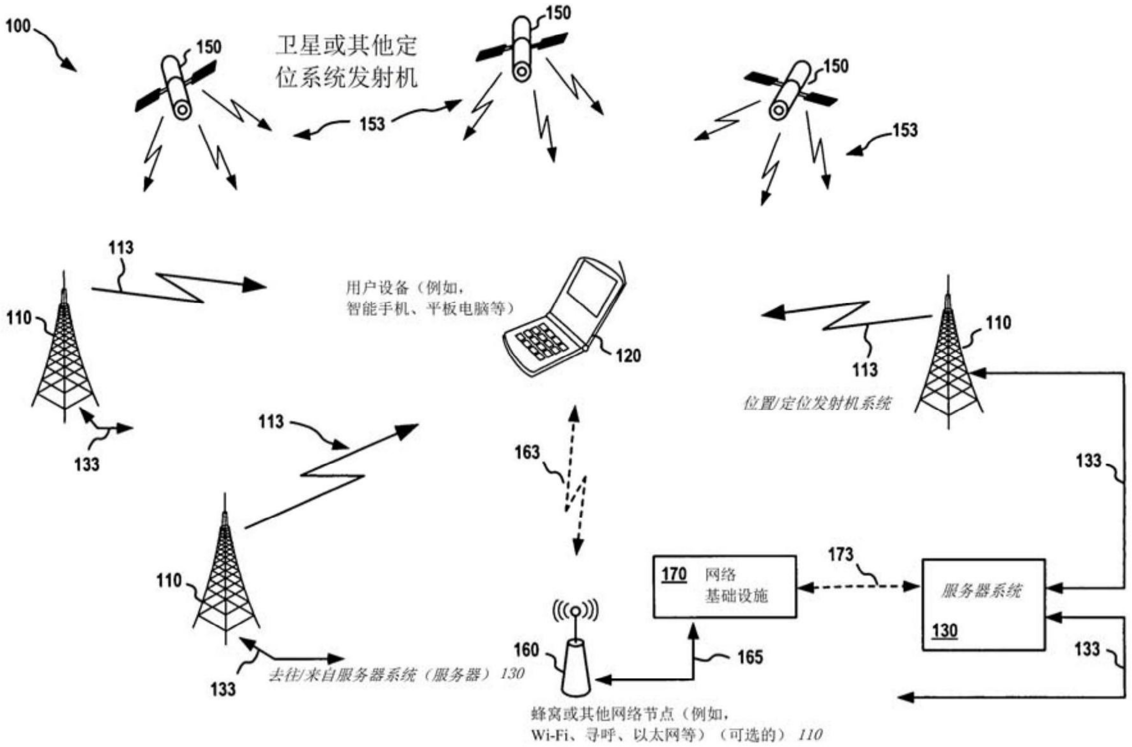

100
150
卫星或其他定
位系统发射机
150
150
153
153
113
110
用户设备（例如，
智能手机、平板电脑等）
120
110
113
位置/定位发射机系统
133
113
163
133
133
110
170
网络
基础设施
173
服务器系统
130
133
160
165
133
去往/来自服务器系统（服务器） 130
蜂窝或其他网络节点（例如，
Wi-Fi、寻呼、以太网等）（可选的） 110

图 1

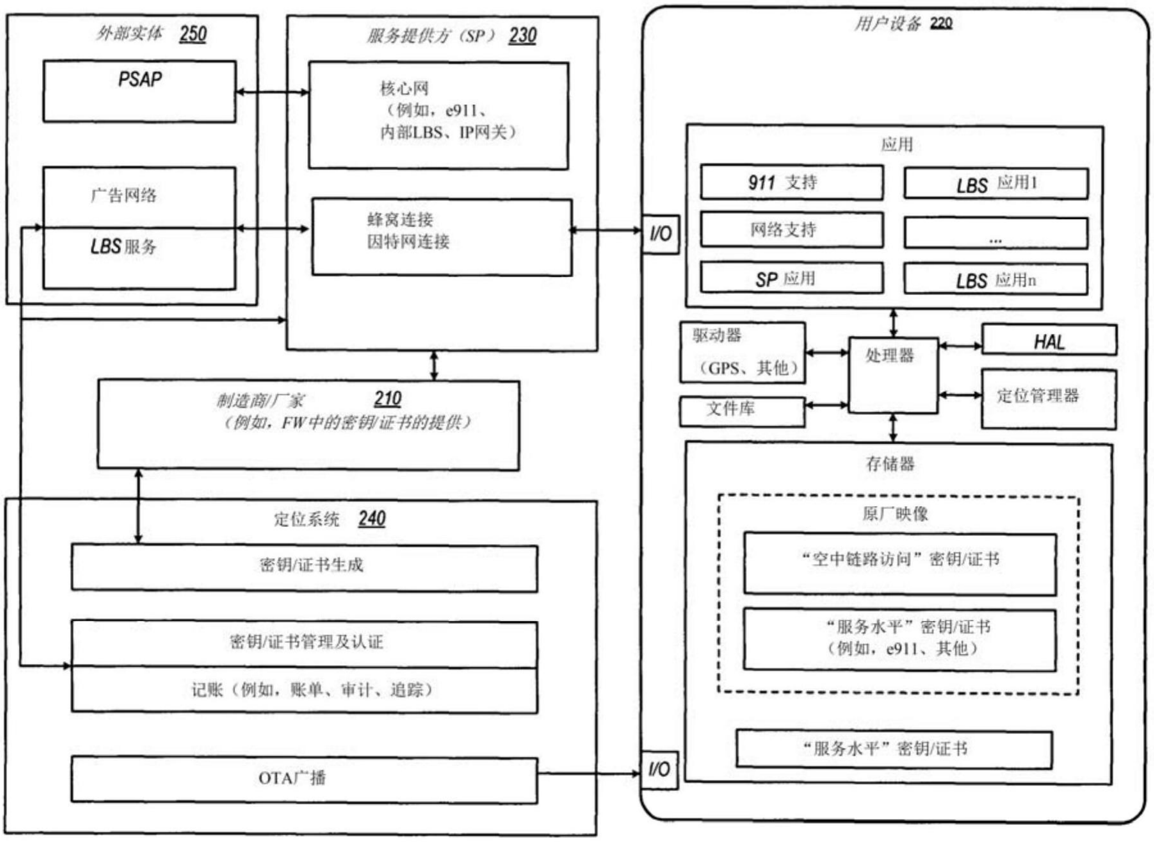

外部实体 250
PSAP
广告网络
LBS服务
服务提供方（SP） 230
核心网
（例如，e911、
内部LBS、IP网关）
蜂窝连接
因特网连接
用户设备 220
应用
911 支持
LBS 应用1
网络支持
...
SP 应用
LBS 应用n
I/O
驱动器
（GPS、其他）
处理器
HAL
文件库
定位管理器
存储器
原厂映像
“空中链路访问”密钥/证书
“服务水平”密钥/证书
（例如，e911、其他）
“服务水平”密钥/证书
制造商/厂家 210
（例如，FW中的密钥/证书的提供）
定位系统 240
密钥/证书生成
密钥/证书管理及认证
记账（例如，账单、审计、追踪）
OTA广播
I/O

图 2

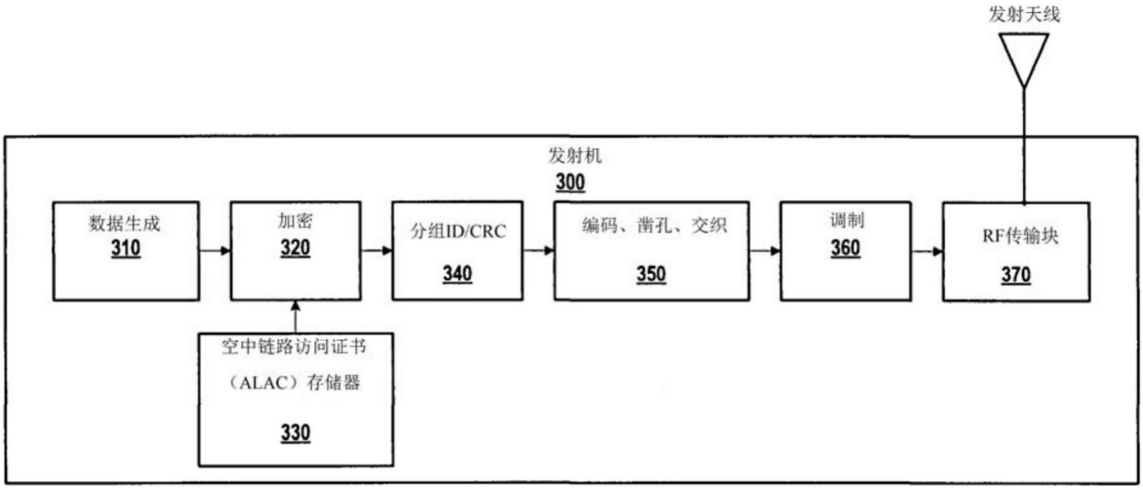

发射天线
发射机
300
数据生成
310
加密
320
分组ID/CRC
340
编码、凿孔、交织
350
调制
360
RF传输块
370
空中链路访问证书
（ALAC）存储器
330

图 3

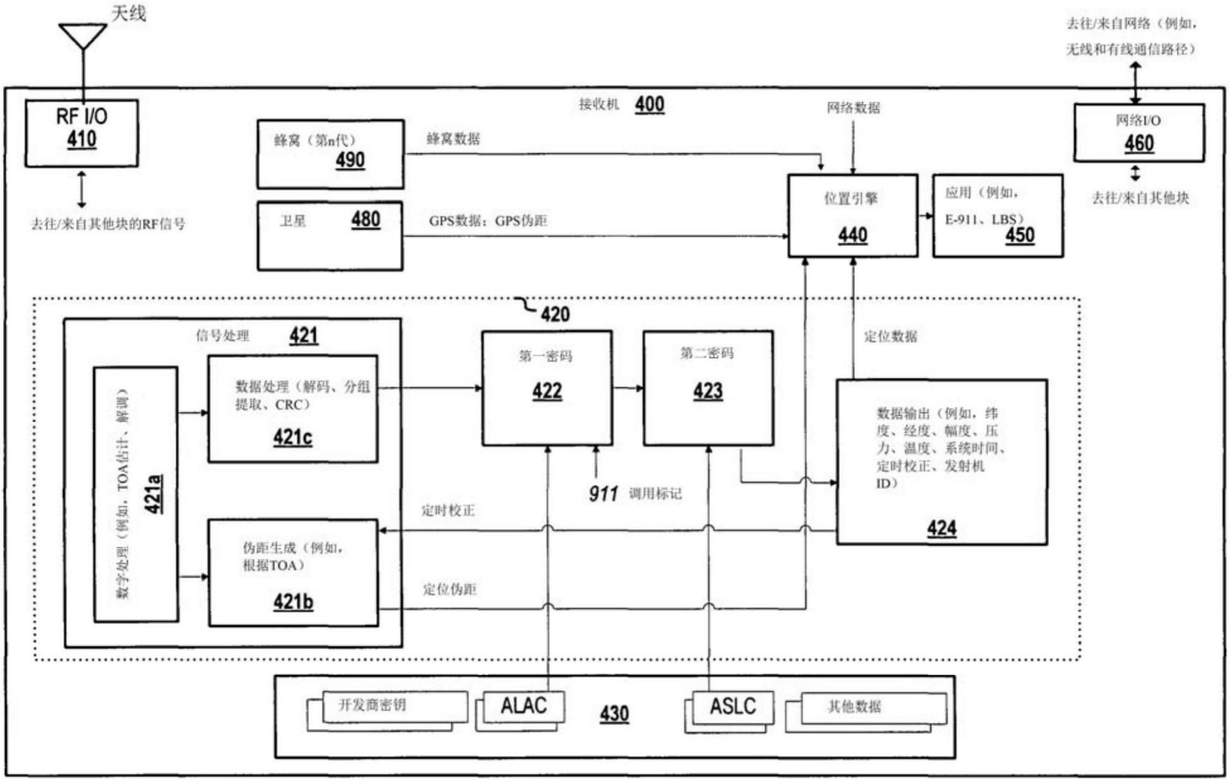

天线
RF I/O
410
去往/来自其他块的RF信号
接收机 400
蜂窝（第n代）
490
蜂窝数据
卫星 480
GPS数据：GPS伪距
网络数据
位置引擎
440
应用（例如，
E-911、LBS）
450
去往/来自网络（例如，
无线和有线通信路径）
网络I/O
460
去往/来自其他块
420
信号处理 421
数字处理（例如，TOA估计，解调）
421a
数据处理（解码、分组提取、CRC）
421c
伪距生成（例如，根据TOA）
421b
第一密码
422
第二密码
423
911 调用标记
定时校正
定位伪距
定位数据
数据输出（例如，纬度、经度、幅度、压力、温度、系统时间、定时校正、发射机ID）
424
开发商密钥
ALAC
430
ASLC
其他数据

图 4A

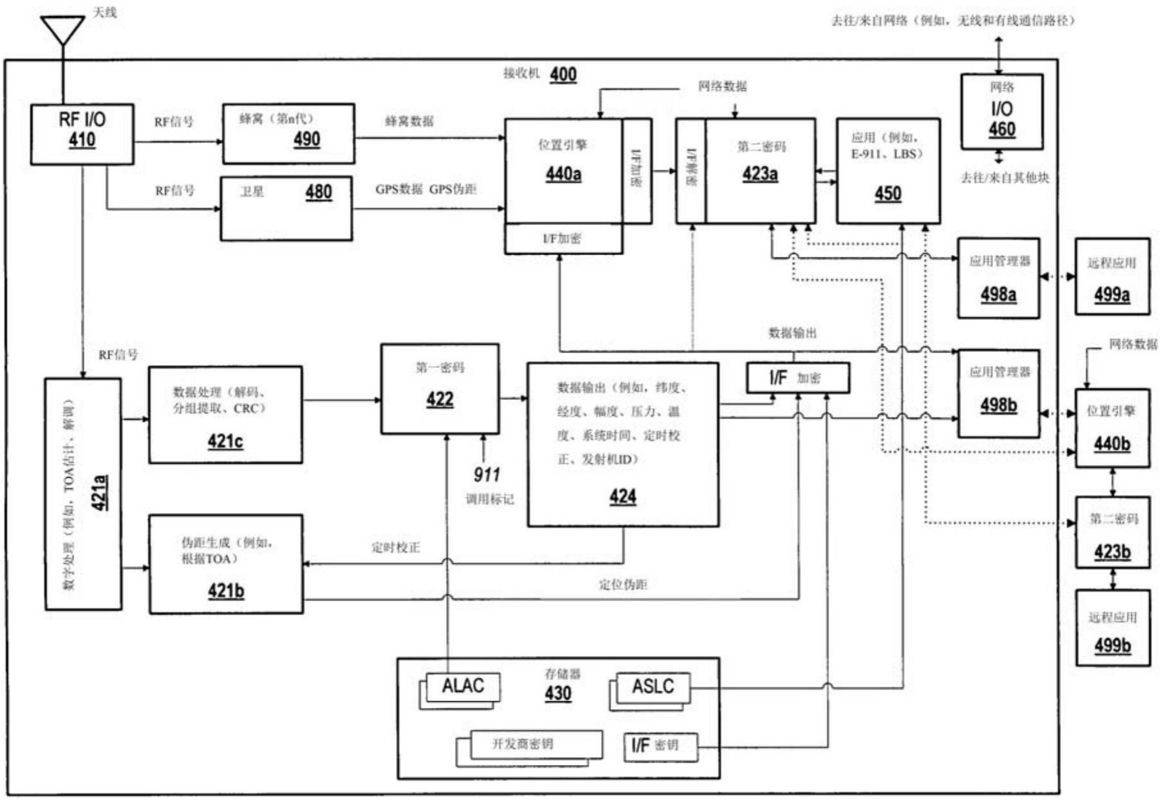

天线
去往/来自网络（例如，无线和有线通信路径）
接收机 400
网络数据
RF I/O
410
RF信号
蜂窝（第n代）
490
蜂窝数据
RF信号
卫星
480
GPS数据 GPS伪距
位置引擎
440a
I/F加密
I/F加密
I/F解密
第二密码
423a
应用（例如，
E-911、LBS）
450
网络
I/O
460
去往/来自其他块
应用管理器
498a
远程应用
499a
数据输出
RF信号
数字处理（例如，TOA估计，解调）
421a
数据处理（解码、分组提取、CRC）
421c
第一密码
422
数据输出（例如，纬度、经度、幅度、压力、温度、系统时间、定时校正、发射机ID）
424
911
调用标记
I/F 加密
应用管理器
498b
网络数据
位置引擎
440b
第二密码
423b
远程应用
499b
伪距生成（例如，根据TOA）
421b
定时校正
定位伪距
ALAC
存储器
430
ASLC
开发商密钥
I/F 密钥

图 4B

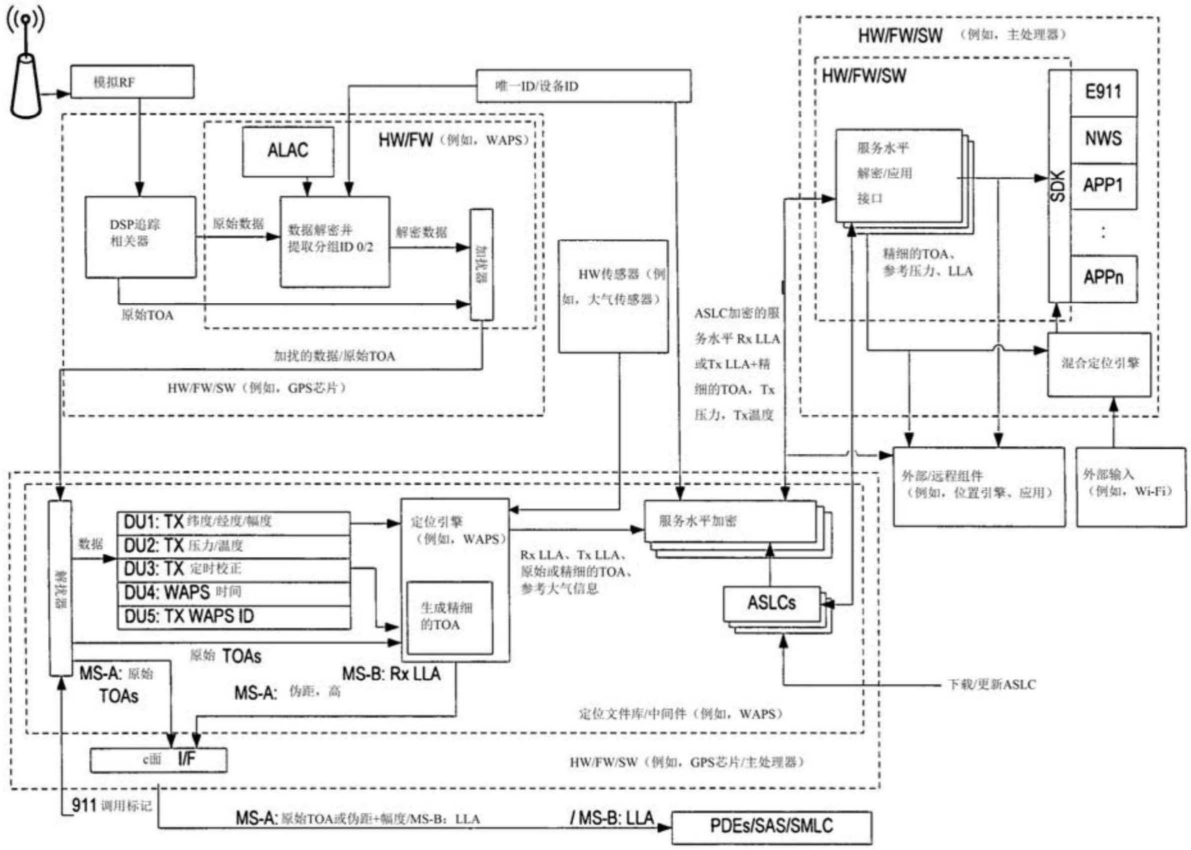

模拟RF
唯一ID/设备ID
HW/FW（例如，WAPS）
ALAC
DSP追踪
相关器
原始数据
数据解密并
提取分组ID 0/2
解密数据
加扰器
原始TOA
加扰的数据/原始TOA
HW/FW/SW（例如，GPS芯片）
HW传感器（例如，大气传感器）
ASLC加密的服务水平 Rx LLA或Tx LLA+精细的TOA，Tx压力，Tx温度
HW/FW/SW （例如，主处理器）
HW/FW/SW
服务水平
解密/应用
接口
SDK
E911
NWS
APP1
:
APPn
精细的TOA、
参考压力、LLA
混合定位引擎
外部/远程组件
（例如，位置引擎、应用）
外部输入
（例如，Wi-Fi）
解扰器
数据
DU1: TX 纬度/经度/幅度
DU2: TX 压力/温度
DU3: TX 定时校正
DU4: WAPS 时间
DU5: TX WAPS ID
定位引擎
（例如，WAPS）
生成精细
的TOA
Rx LLA、Tx LLA、
原始或精细的TOA、
参考大气信息
服务水平加密
ASLCs
下载/更新ASLC
原始 TOAs
MS-A: 原始
TOAs
MS-B: Rx LLA
MS-A: 伪距，高
定位文件库/中间件（例如，WAPS）
c面 I/F
HW/FW/SW（例如，GPS芯片/主处理器）
911 调用标记
MS-A: 原始TOA或伪距+幅度/MS-B：LLA
/ MS-B: LLA
PDEs/SAS/SMLC

图 4C

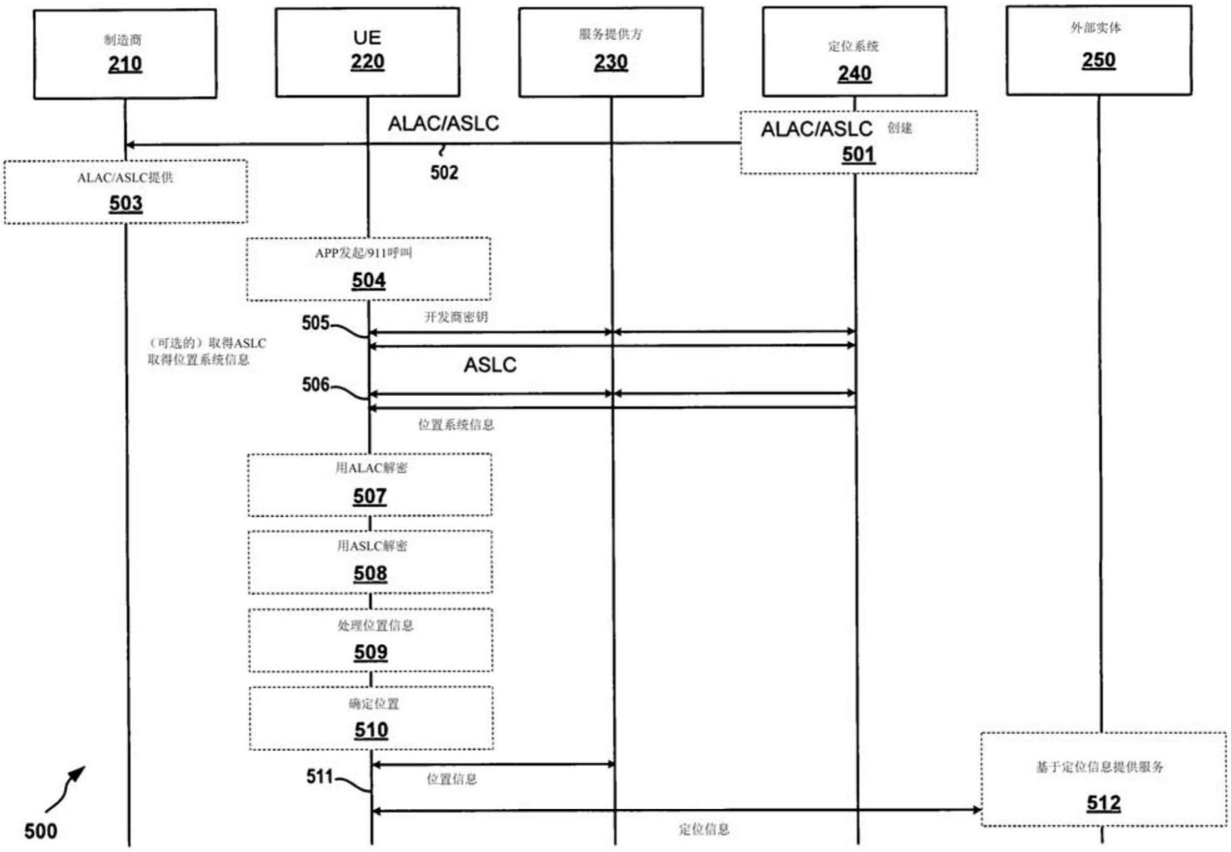

制造商
210
UE
220
服务提供方
230
定位系统
240
外部实体
250
ALAC/ASLC
502
ALAC/ASLC 创建
501
ALAC/ASLC提供
503
APP发起/911呼叫
504
505
开发商密钥
（可选的）取得ASLC
取得位置系统信息
ASLC
506
位置系统信息
用ALAC解密
507
用ASLC解密
508
处理位置信息
509
确定位置
510
511
位置信息
基于定位信息提供服务
512
定位信息
500

图 5A

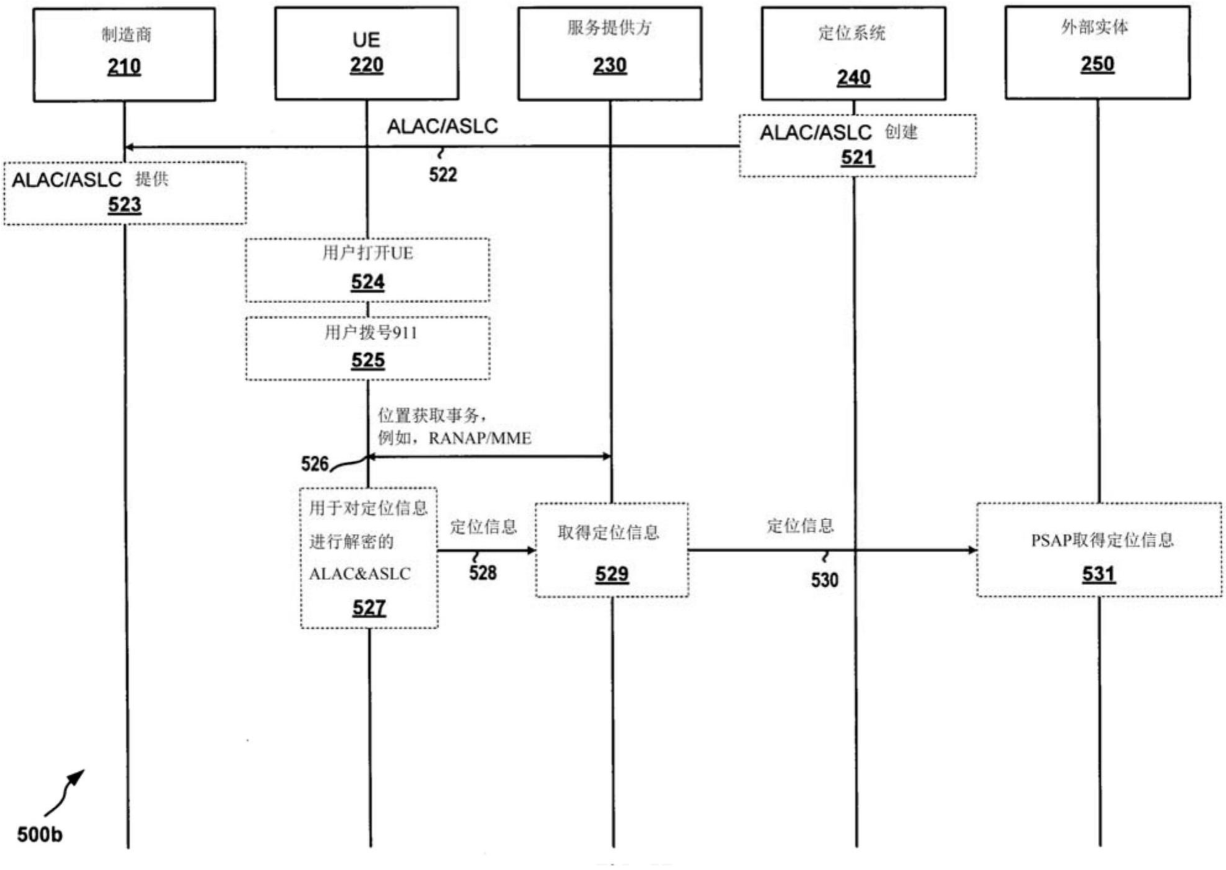

制造商
210
UE
220
服务提供方
230
定位系统
240
外部实体
250
ALAC/ASLC
522
ALAC/ASLC 创建
521
ALAC/ASLC 提供
523
用户打开UE
524
用户拨号911
525
位置获取事务，
例如，RANAP/MME
526
用于对定位信息
进行解密的
ALAC&ASLC
527
定位信息
528
取得定位信息
529
定位信息
530
PSAP取得定位信息
531
500b

图 5B

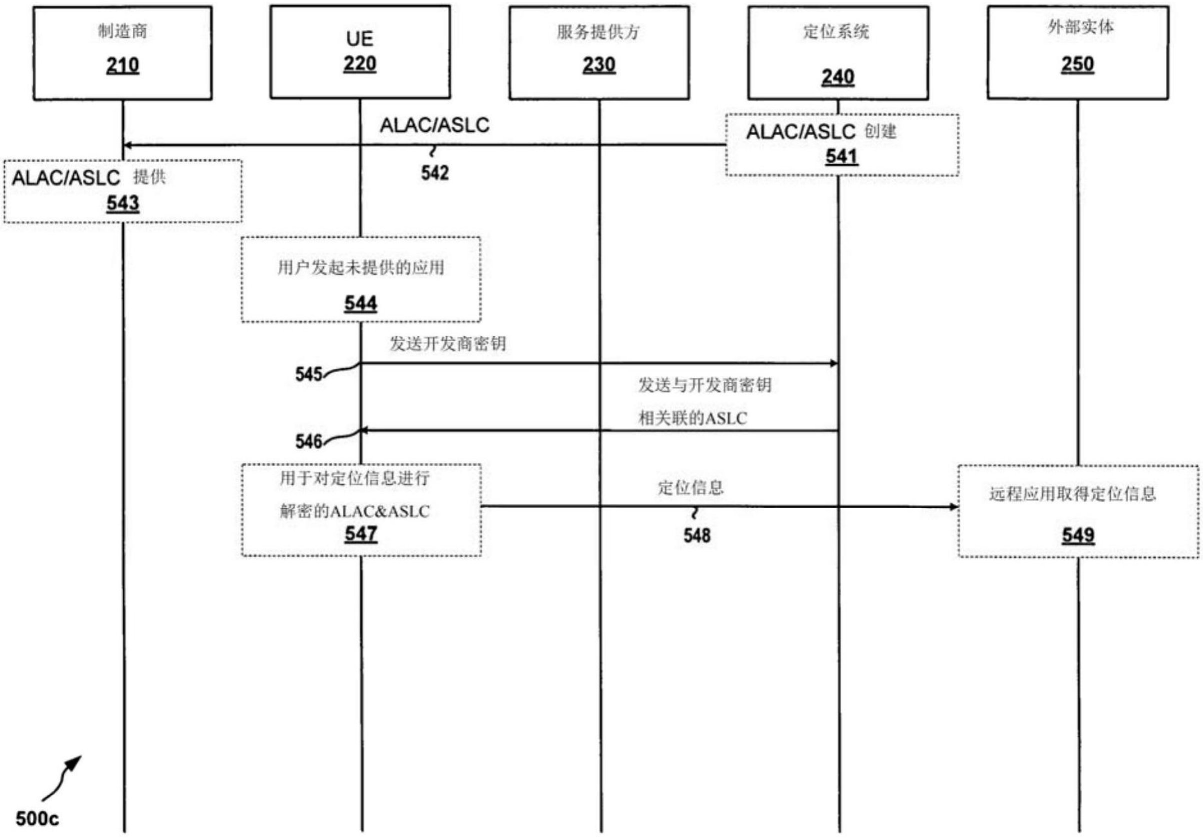

制造商
210
UE
220
服务提供方
230
定位系统
240
外部实体
250
ALAC/ASLC
542
ALAC/ASLC 创建
541
ALAC/ASLC 提供
543
用户发起未提供的应用
544
发送开发商密钥
545
发送与开发商密钥
相关联的ASLC
546
用于对定位信息进行
解密的ALAC&ASLC
547
定位信息
548
远程应用取得定位信息
549
500c

图 5C

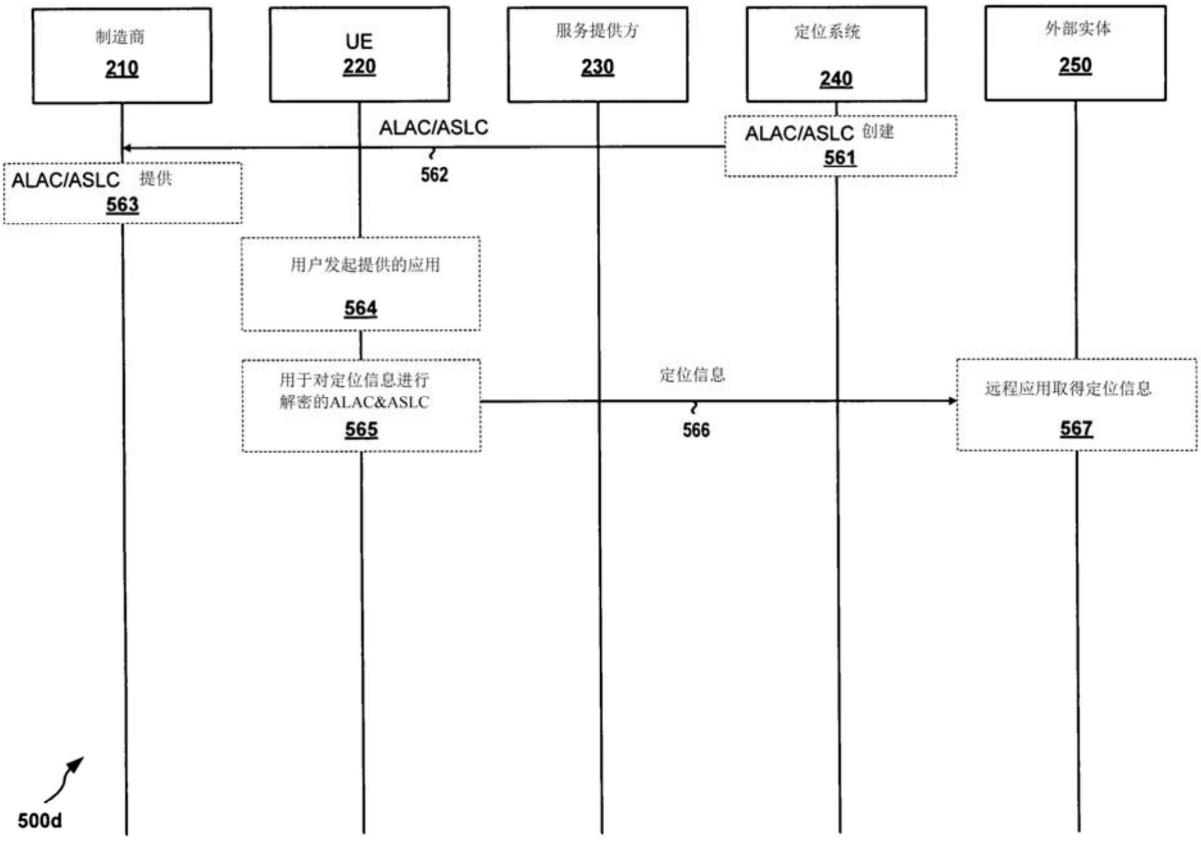

制造商
210
UE
220
服务提供方
230
定位系统
240
外部实体
250
ALAC/ASLC
562
ALAC/ASLC 创建
561
ALAC/ASLC 提供
563
用户发起提供的应用
564
用于对定位信息进行
解密的ALAC&ASLC
565
定位信息
566
远程应用取得定位信息
567
500d

图 5D

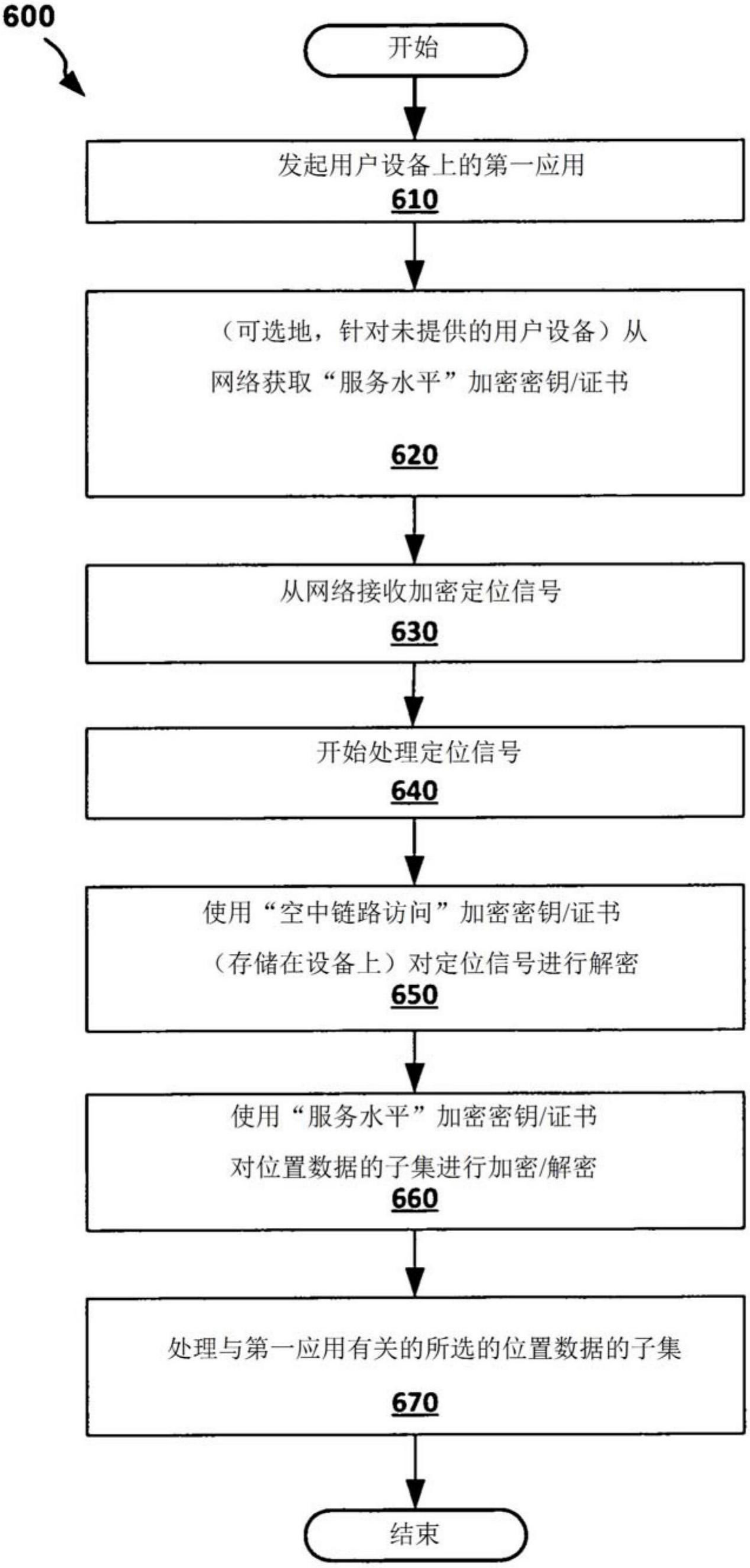

600
开始
发起用户设备上的第一应用
610
（可选地，针对未提供的用户设备）从
网络获取“服务水平”加密密钥/证书
620
从网络接收加密定位信号
630
开始处理定位信号
640
使用“空中链路访问”加密密钥/证书
（存储在设备上）对定位信号进行解密
650
使用“服务水平”加密密钥/证书
对位置数据的子集进行加密/解密
660
处理与第一应用有关的所选的位置数据的子集
670
结束

图 6

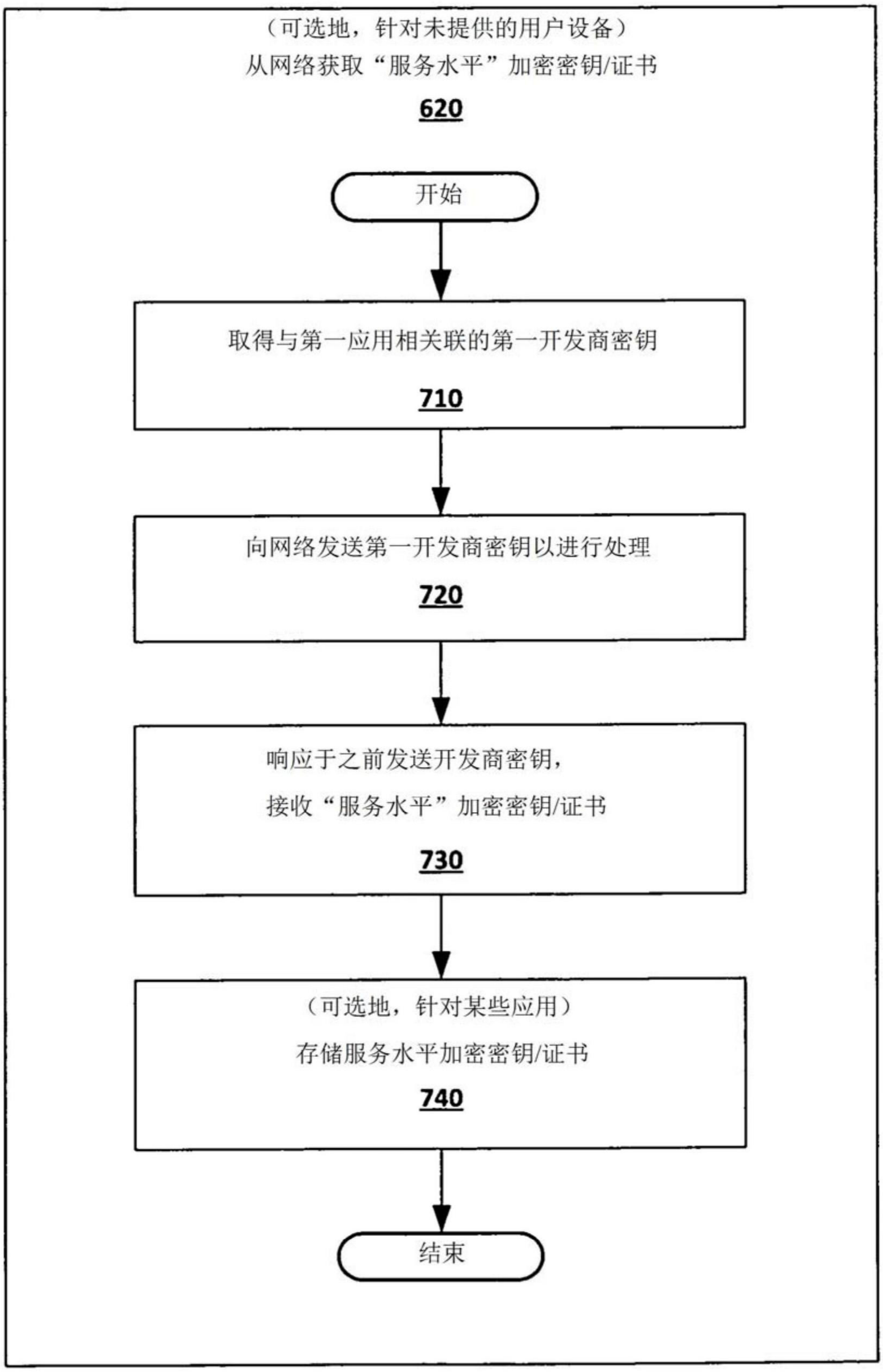

（可选地，针对未提供的用户设备）
从网络获取“服务水平”加密密钥/证书
620
开始
取得与第一应用相关联的第一开发商密钥
710
向网络发送第一开发商密钥以进行处理
720
响应于之前发送开发商密钥，
接收“服务水平”加密密钥/证书
730
（可选地，针对某些应用）
存储服务水平加密密钥/证书
740
结束

图 7

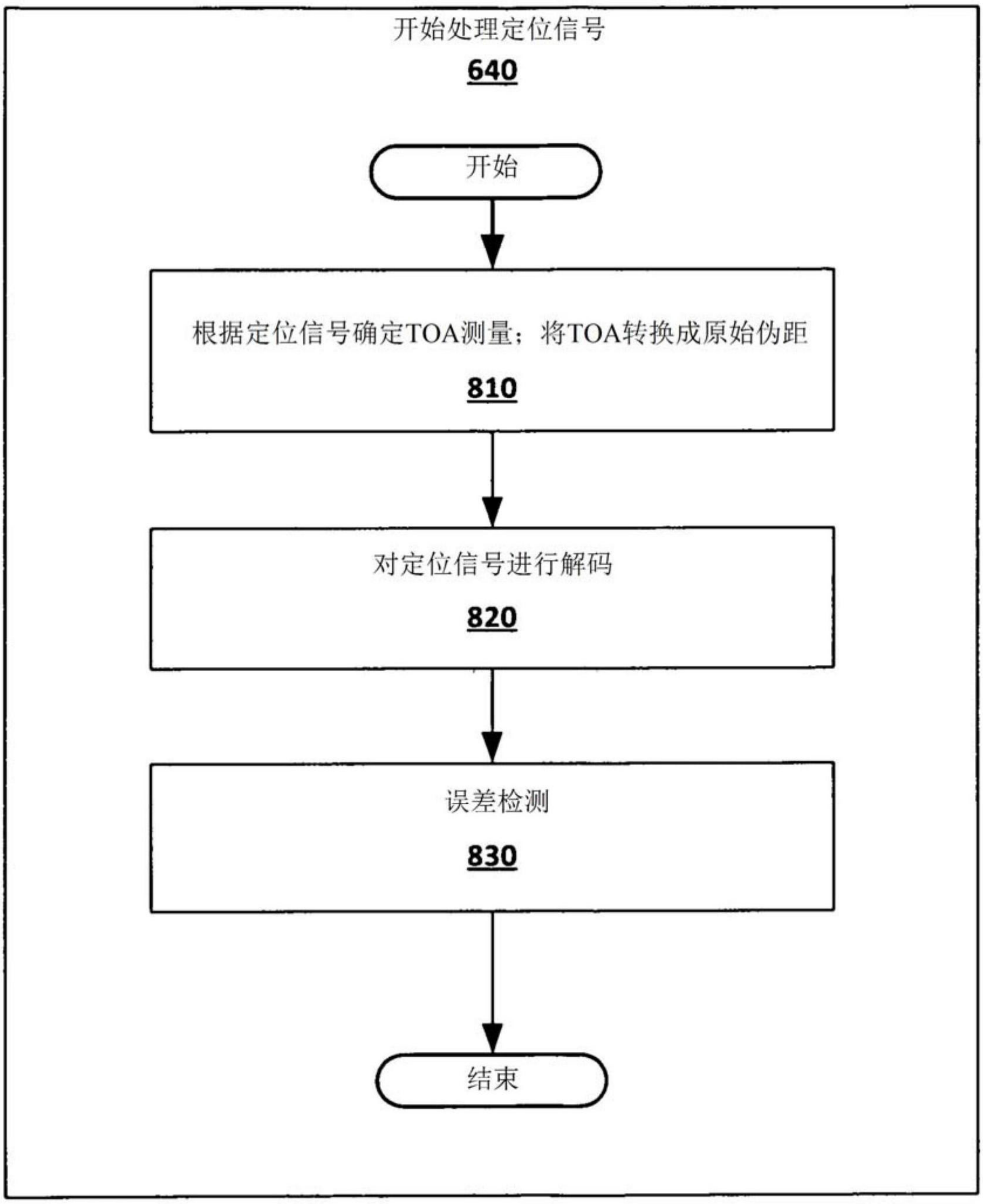
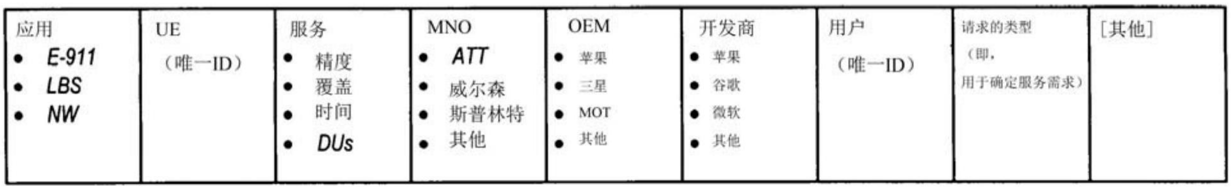


图 8



应用	UE	服务	MNO	OEM	开发商	用户	请求的类型	[其他]
• *E-911* • *LBS* • *NW*	（唯一ID）	• 精度 • 覆盖 • 时间 • *DUs*	• *ATT* • 威尔森 • 斯普林特 • 其他	• 苹果 • 三星 • MOT • 其他	• 苹果 • 谷歌 • 微软 • 其他	（唯一ID）	（即， 用于确定服务需求）	

图 9

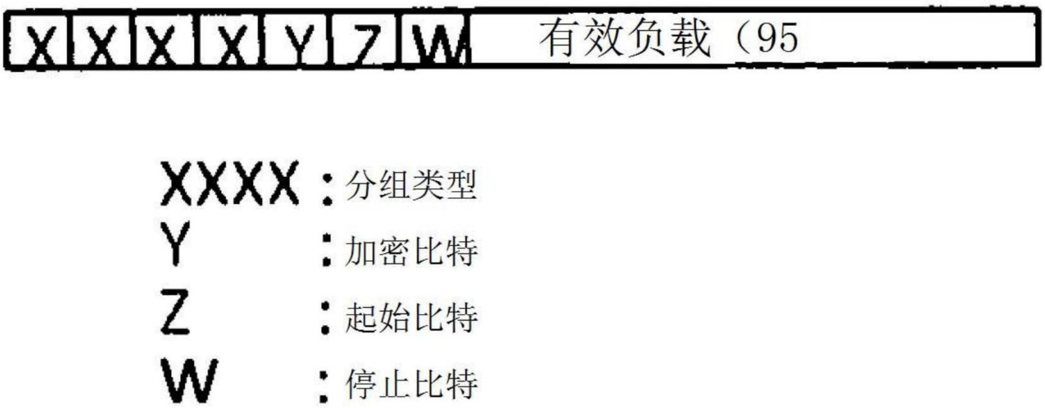

X
X
X
X
Y
Z
W
有效负载（95
XXXX：分组类型
Y：加密比特
Z：起始比特
W：停止比特

图 10A

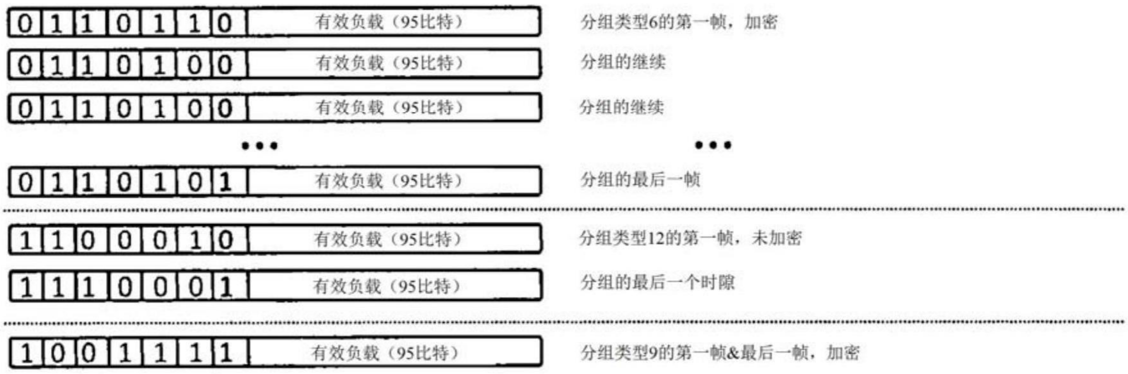

0 1 1 0 1 1 0　有效负载（95比特）　分组类型6的第一帧，加密
0 1 1 0 1 0 0　有效负载（95比特）　分组的继续
0 1 1 0 1 0 0　有效负载（95比特）　分组的继续
•••　•••
0 1 1 0 1 0 1　有效负载（95比特）　分组的最后一帧
1 1 0 0 0 1 0　有效负载（95比特）　分组类型12的第一帧，未加密
1 1 1 0 0 0 1　有效负载（95比特）　分组的最后一个时隙
1 0 0 1 1 1 1　有效负载（95比特）　分组类型9的第一帧&最后一帧，加密

图 10B

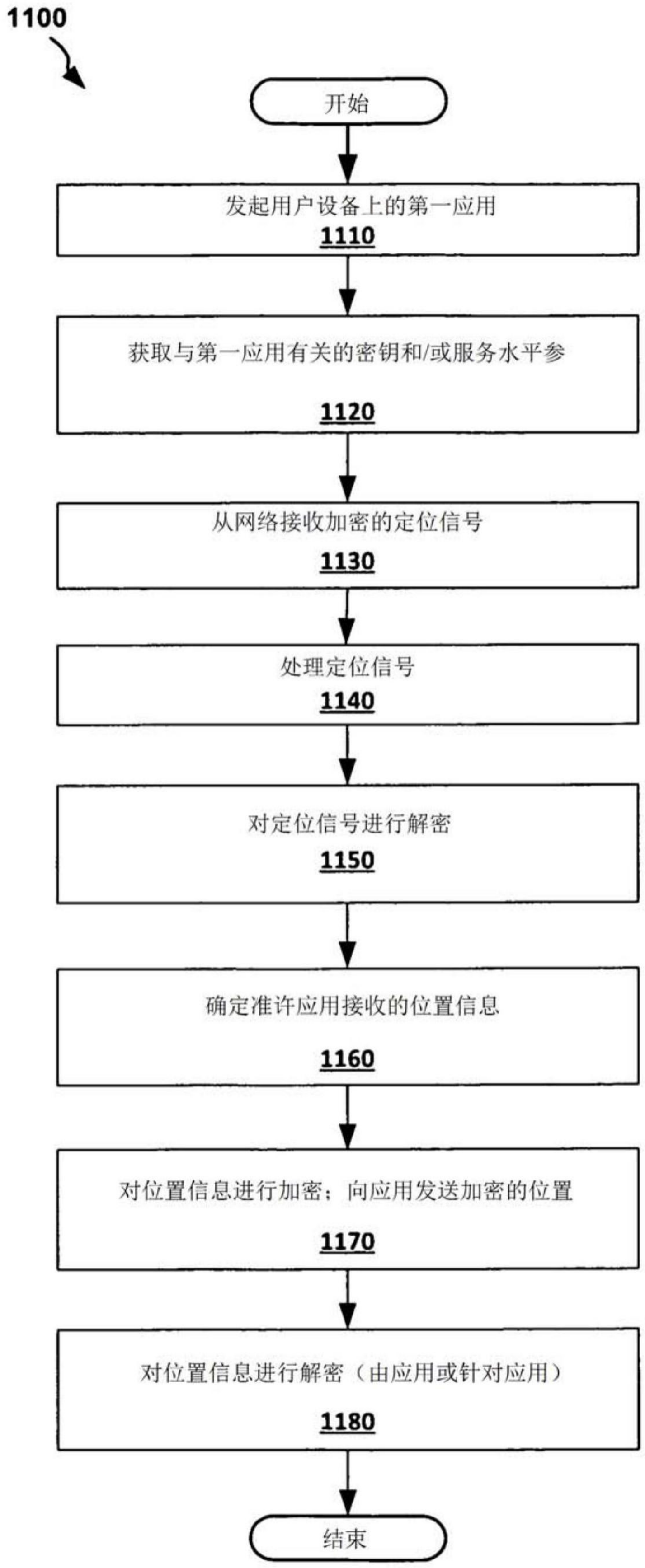

1100
开始
发起用户设备上的第一应用
1110
获取与第一应用有关的密钥和/或服务水平参
1120
从网络接收加密的定位信号
1130
处理定位信号
1140
对定位信号进行解密
1150
确定准许应用接收的位置信息
1160
对位置信息进行加密；向应用发送加密的位置
1170
对位置信息进行解密（由应用或针对应用）
1180
结束

图 11

Abstract

This disclosure relates to systems, methods, computer program products, and means that control access to position information at a receiver, or at another device external to the receiver, based on various considerations, including a requested service type, a user type, a device type, a software application type, a payment, and/or other characteristics associated with a particular software application or distributor of that software application. The disclosure further relates to systems, methods, computer program products and means for carrying out secure data transmissions intended for a particular application among other applications.