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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 October 2023 (26.10.2023)

WIPO | PCT

(10) International Publication Number
WO 2023/201428 A1

(51) International Patent Classification:
H04W 8/00 (2009.01) *H04W 64/00* (2009.01)
G01S 1/20 (2006.01)

(21) International Application Number:
PCT/CA2023/050528

(22) International Filing Date:
19 April 2023 (19.04.2023)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/332,517 19 April 2022 (19.04.2022) US

(71) Applicant: **FARM HEALTH GUARDIAN LTD.** [CA/CA]; 100 Stone Rd W, Suite 109, Guelph, Ontario N1G 5L3 (CA).

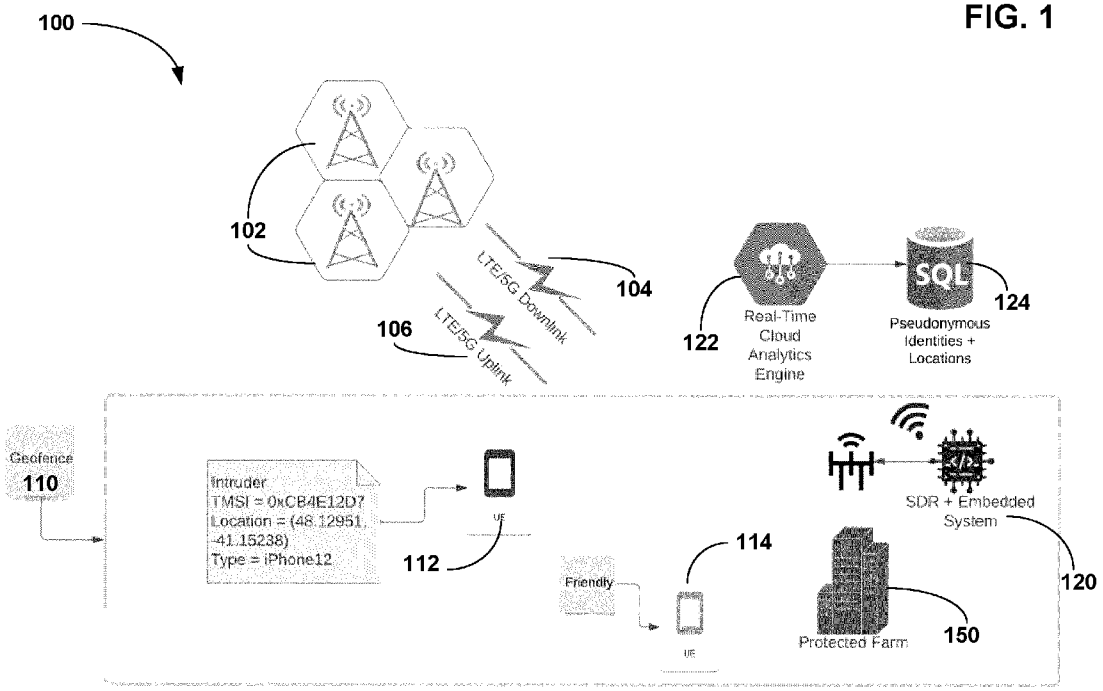
(72) Inventors: **SOULE ALAOFE, Idris**; 100 Stone Rd W, Suite 109, Guelph, Ontario N1G 5L3 (CA). **NELSON, Timothy**; 100 Stone Rd W, Suite 109, Guelph, Ontario N1G 5L3 (CA). **LIN, Xiaodong**; 100 Stone Rd W, Suite 109, Guelph, Ontario N1G 5L3 (CA). **WANG, Le**; 100 Stone Rd W, Suite 109, Guelph, Ontario N1G 5L3 (CA).

(74) Agent: **ALL OF THE AGENTS OF BENNETT JONES LLP, INCLUDING SALVATORE FEDERICO BARBIERI**; Suite 3400, One First Canadian Place, P.O. Box 130, Toronto, Ontario M5X 1A4 (CA).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) Title: SYSTEM AND METHOD OF DEVICE DETECTION

FIG. 1



(57) Abstract: A system and method of detecting mobile devices is provided. The method comprises a processor sending a soft page message via MSISDN to an MME, tracking at least one of a TMSI, S-TMSI, GUTI, or c-RNTI, and receiving a P-RNTI filtering message from an eNB. A system and method of classifying detected mobile devices is also provided. The method comprises listening on an uplink channel for a detected mobile device, receiving from the detected mobile device capabilities information regarding the detected mobile device, and obtaining a UE model of the detected mobile device where the UE model is determined based on the capabilities information.

WO 2023/201428 A1

[Continued on next page]

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, 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, ME, 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))*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*
— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

System and Method of Device Detection

FIELD

[0001] The present disclosure generally relates to detection, and in particular to a system and method of detecting mobile devices in a geo-fenced area.

INTRODUCTION

[0002] Livestock and poultry farms use biosecurity programs to detect and control authorized access to the property. Such biosecurity programs are intended to detect intruders and/or biohazards entering the property.

[0003] Some current methods that relate to detection of cellular presence analyze the presence of key cellular frequencies but cannot guarantee a particular perimeter to guard among other issues. For different reasons both video surveillance and movement detectors do not provide adequate protection from intrusion into private property. Often, new/emerging systems, such as biometric scanning/screening, can be prohibitively expensive for agricultural use.

SUMMARY

[0004] In accordance with an aspect, there is provided a system for detecting mobile devices is provided. The system comprises at least one processor and a memory storing instructions which when executed by the at least one processor cause the at least one processor to: send a soft page message via MSISDN to an MME, track at least one of a TMSI, S-TMSI, GUTI, or c-RNTI, and send a P-RNTI filtering message to an eNB.

[0005] In accordance with an aspect, there is provided a method of detecting mobile devices is provided. The method comprises a processor sending a soft page message via MSISDN to an MME, tracking at least one of a TMSI, S-TMSI, GUTI, or c-RNTI, and sending a P-RNTI filtering message to an eNB.

[0006] In accordance with another aspect, there is provided a system for classifying detected mobile devices is also provided. The system comprises at least one processor and a memory storing instructions which when executed by the at least one processor cause the at least one processor to: listen on an uplink channel for a detected mobile device, receive from the detected mobile device capabilities information regarding the detected mobile device, and obtain a UE

model of the detected mobile device where the UE model is determined based on the capabilities information.

[0007] In accordance with another aspect, there is provided a method of classifying detected mobile devices is also provided. The method comprises listening on an uplink channel for a detected mobile device, receiving from the detected mobile device capabilities information regarding the detected mobile device, and obtaining a UE model of the detected mobile device where the UE model is determined based on the capabilities information.

[0008] In various further aspects, the disclosure provides corresponding systems and devices, and logic structures such as machine-executable coded instruction sets for implementing such systems, devices, and methods.

[0009] In this respect, before explaining at least one embodiment in detail, it is to be understood that the embodiments are not limited in application to the details of construction and to the arrangements of the components set forth in the following description or illustrated in the drawings. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

[0010] Many further features and combinations thereof concerning embodiments described herein will appear to those skilled in the art following a reading of the instant disclosure.

DESCRIPTION OF THE FIGURES

[0011] Embodiments will be described, by way of example only, with reference to the attached figures, wherein in the figures:

[0012] **FIG. 1** illustrates, in a component diagram, an example of an environment for locating and detecting UEs on properties, in accordance with some embodiments;

[0013] **FIG. 2** illustrates, in a flowchart, an example of paging initiated by an MME or eNB on S1-MME or UU, in accordance with some embodiments;

[0014] **FIG. 3** illustrates, in a call flow diagram, an example of soft paging, in accordance with some embodiments;

[0015] **FIG. 4** illustrates an example of DRX modes in a network architecture, in accordance with some embodiments;

[0016] **FIG. 5** illustrates an example of DRX states in RRC connected/idle modes, in accordance with some embodiments;

[0017] **FIG. 6** illustrates, in a call flow diagram, an example of a method of determining a UE model, in accordance with some embodiments;

[0018] **FIG. 7** illustrates an example of a machine learning method of determining a UE model, in accordance with some embodiments;

[0019] **FIG. 8** illustrates an example of determining UE localization, in accordance with some embodiments; and

[0020] **FIG. 9** is a schematic diagram of a computing device such as a server or other computer.

[0021] It is understood that throughout the description and figures, like features are identified by like reference numerals.

DETAILED DESCRIPTION

[0022] Embodiments of methods, systems, and apparatus are described through reference to the drawings. Applicant notes that the described embodiments and examples are illustrative and non-limiting. Practical implementation of the features may incorporate a combination of some or all of the aspects, and features described herein should not be taken as indications of future or existing product plans.

[0023] In some embodiments, there is provided a biosecurity system and method to detect the presence of unauthorized people (e.g., trespassers) on properties (e.g., farms).

[0024] In some embodiments, a passive Radio Frequency (RF) system, for monitoring, detecting and locating Long-Term Evolution (LTE) / Fifth Generation (5G) devices in a geo-fenced area is provided. By principle, the system leverages flaws or “features” of the 3rd Generation Partnership Project (3GPP) protocols without compromising the integrity and encryption of messages exchanged between cellular devices and mobile base-station.

[0025] LTE systems operate through bi-directional communication of a base station or cell tower (e.g., eNodeB) and user equipment (UE) (e.g., a cellular device) over the air. A cell is a physical location containing one or more eNodeB’s in a tracking area. Once a UE synchronizes and attaches to an eNodeB with the strongest signal in the area, messages in the form of a Short Message Service (SMS) message or phone calls can be relayed to the UE. Each UE has a global unique identifier, termed an International Mobile Subscriber Identity (IMSI). The IMSI should be secured since it exposes the user to various attack vectors. As such, a temporary pseudonym, Temporary Mobile Subscriber Identity (TMSI) / Serving TMSI (S-TMSI) / Globally Unique Temporary UE Identity (GUTI) / cell Radio Network Temporary Identifier (c-RNTI), is used in the

exchange of messages between the eNodeB and UE (TMSI / S-TMSI for 3G or GUTI for LTE UEs or c-RNTI for 3G, LTE and 5G).

[0026] In some embodiments, a system is provided that operates by continuously monitoring the frequencies of eNodeB's in a cell, which serves the area under protection. Messages exchanged in the clear (unencrypted messages) are retrieved by the system, deconstructed and analyzed. The system monitors for GUTI/TMSI/S-TMSI/c-RNTI in network packets in order to understand: i) the amount of users camping on a cell tower, and ii) their time of entry and possible exit. The system is then effectively able to passively track TMSI's/S-TMSI's/GUTI's/c-RNTI's within a geofence, through proprietary temporal, spatial and context linking RF techniques. In the event of selective frequency jamming, the system is able to quickly mitigate. Furthermore, the system may be configures to whitelist cellular devices that are not seen as a threat, such as an owner on premise (e.g., Farm Health Guardian ™ users) and blacklist unknown or threating cellular devices.

[0027] The following technologies may be utilized as part of an overall system:

- Customized Software Defined Radios (SDR)
- mmWave (millimeterWave) sensors
- Field Programmable Gate Arrays (FPGAs)
- Embedded micro-controllers
- Spectrum analyzers

[0028] In some embodiments, there are different aspects to the methods of this system. For example:

- The possible linkability of IMSI's and GUTI/TMSI/S-TMSI/c-RNTI on properties
- Detection of whitelisted UEs presence based on a proprietary process
- RF baseband signature classification
- UE (mmWave) localization on FR1/2 for 5G-NR (New Radio)

[0029] **FIG. 1** illustrates, in a component diagram, an example of an environment **100** for locating and detecting UEs on properties **150**, in accordance with some embodiments. The environment **100** comprises one or more eNodeB (eNB) **102** in communication with a software defined radio (SDR) and embedded system **120** via LTE/5G downlink **104** and uplink **106** signals, a geofence **110** around a property **150** within which there may be intruder UEs **112** or friendly

UEs **114**, and the system **120**. The system **120** may be in communication with a real-time cloud analytics engine **122** which has access to a database (e.g., a SQL database) **124** storing pseudonymous identities and locations.

Detection of Whitelisted UEs presence based on MSISDN soft-paging

[0030] In some embodiments, the system **120** is configured to account for UEs **112**, **114** that are on the property, so as to not mistake them for intruders. The LTE paging protocol, application priority paging and smart paging may be used to ensure UEs registered or allowed are not to be flagged during scanning of LTE channels. Furthermore, a known identity of allowed UEs may be used to ensure the system **120** does not mistake an allowed device for an intruder. The Mobile Station Integrated Services Digital Network (MSISDN) may be used, which is the UEs phone number, easily known or obtained by the owners on property.

[0031] **FIG. 2** represents the canonical definition of a LTE network. **FIG. 2** illustrates, in a flowchart, an example of paging **200** initiated by a Mobility Management Entity (MME) **210** or eNB **102** on S1-MME or UU, in accordance with some embodiments. Specifically, the system **120** observes paging messages originating from the MME **210** for UEs **112**, **114** in the Tracking Area (e.g., approximate area defined by the geofence **110**). With the aid of smart paging, the system **120** is ensured to prevent signalling storms on the S1-MME link **208**. The determination of paging cycle and other SIB2 paging parameters are not required in some embodiments.

[0032] By retrieving a database of whitelisted UEs **114**, the system **120** can initiate what may be deemed as soft VoLTE calls or soft SMS. Soft paging is a presence test for each UE **112**, **114** under service by a cell, typically the last cell it camped on if in DRX (Discontinuous Reception) under the Radio Resource Control (RRC) IDLE state (see **FIGs. 4** and **5**).

[0033] In some embodiments, system **120** interacts only with eNodeB **102** and the UE **112**, **114**. All other systems are internal to the network (e.g., LTE network).

[0034] **FIG. 3** illustrates, in a call flow diagram, an example of soft paging **300**, in accordance with some embodiments. The system **120** sends a soft page message **302** via an MSISDN to an MME **210**. The MME **210** initiates a T3413 timer **304** and sends a Paging Control Channel (PCCH) – paging message **306** to an eNB **102**. The eNB **102** then sends an RRC paging message **308** to the known UE which does not trigger the UE **112**, **114**. I.e., trigger in the sense that the callee has no knowledge of the call being made to their UE via the display or notification method of said UE. Next, the system **120** initiates TMSI/S-TMSI/GUTI/c-RNTI tracking **310**. Next the system **120**

reads the PDSCH and performs P-RNTI filtering **312** that includes UE identities to the eNB **102**. The T3413 then expires **314**.

[0035] Once a paging message has propagated through the LTE architecture, system **120** reads the PDSCH and filters for paging message through the P-RNTI (Paging Radio Network Temporary Identifier). In each paging message, the system **120** checks for a reoccurring TMSI as it continues to soft page the MSISDN. Timer T3413 is an inactivity timer used by the MME in the event that there is no response to the paging message. When system **120** initiates the soft page it listens between the start and end of T3413 to ensure that the system **120** has the possibility to read paging messages (Note: read it too early and the system may have to wait a little while to see the message, read it too late and the message is gone).

[0036] The soft page is a term to denote the essence of system **120** calling (VoLTE) or texting (SMS) the known UE but "hanging" up: a) before the known UE can register the call, and b) within enough time to ensure the paging message is sent over the air.

[0037] **FIG. 4** represents an interaction diagram between the canonical definition of a LTE network of **FIG. 2** (including a server gateway (SGW), the MME **210**, the eNB **102** and a UE **112**, **114**. **FIG. 4** illustrates an example of DRX modes in a network architecture **400**, in accordance with some embodiments. When the UE is not listening to the DL transmission, most of its circuitry is turned off. The UE battery saving depends on the DRX parameter settings. DRX parameters in this mode are provided by the eNB **102** during the radio bearer setup.

[0038] **FIG. 4** shows the connection between the UE **112**, **114** and eNB **102** during the various states. Specifically, the soft paging mechanism is applicable when the UE **112**, **114** is in idle mode. There is no UE context as all connections have ceased because the UE is idle and is preserving battery life. Over the lifetime of monitoring the particular property, known UEs based on their MSISDN are going to be in the idle state allowing system **120** to successfully soft page the known UE.

[0039] **FIG. 5** represents transistions of DRX states in a UE. **FIG. 5** illustrates an example of DRX states in RRC connected/idle modes **500**, in accordance with some embodiments. In some embodiments, the soft-page embedded system **120** comprises UE hardware and eSIM enabling it to perform the functions of an off-the-shelf UE, with the addition of accessing advanced engineer mode specifics. The system **120** will soft page so as to not cause the known UE **112**, **114** to awake out of DRX or cause continuous alerts on the foreground of the UEs user interface. This mechanism is accomplished by starting and then stopping a UE terminated service before the

aforementioned alert is on the UE. However, it should be long enough to pass over the air interface to the EPC. The MME **210** will start T3413, paging service request is sent to the eNB **102**, the RRC paging message is not delivered to the UE. In doing so the UE does not respond after waking up out of DRX to check on the paging messages – i.e., there is no message in its slot. The system **120** may be configured to wait a given time window so as to ensure that the message is read. This process is repeated until the system **120** determines that there is a TMSI/S-TMSI/GUTI that is continuously seen in the paging messages. This TMSI/S-TMSI/GUTI can then be marked as safe within the system **120**. In the event that the TMSI/S-TMSI/GUTI is not seen, the system **120** may assume that either the UE is not in the TA, or that the UE is engaged in a call. Depending on the initial setup tests, whether or not certain services cause GUTI/TMSI/S-TMSI re-allocations are checked, the service based on the implementation of the area under protection is varied.

[0040] The following is an example of a paging record with a UE identity that is a type S-TMSI (other paging records could apply to TMSI/GUTI):

```
PCCH-Message : := SEQUENCE
  +-message : := CHOICE [c1]
    +-c1 : := CHOICE [paging]
      +-paging : := SEQUENCE [1000]
        +-pagingRecordList : := SEQUENCE OF SIZE(1..maxPageRec[16]) [1] OPTIONAL : Exist
        |+-PagingRecord : := SEQUENCE
        |  +-ue-Identity : := CHOICE [s-TMSI]
        |  | +-s-TMSI : := SEQUENCE
        |  |  +-mmec : := BIT STRING SIZE(8) [00000001]
        |  |  +-m-TMSI : := BIT STRING SIZE(32) [00000000000000000000000000000001]
        |  +-cn-Domain : := ENUMERATED [ps]
        +-systemInfoModification : := ENUMERATED OPTIONAL : Omit
        +-etws-Indication : := ENUMERATED OPTIONAL : Omit
        +-nonCriticalExtension : := SEQUENCE OPTIONAL : Omit
```

UE Baseband Signature Classification

[0041] The system **120** may utilize machine learning techniques to predict the model of a UE, via: UE capabilities and other uplink data sent in unencrypted channels. It should be noted that the UE capabilities are specific to both the make and model of the UE. The baseband in each phone model will have slight variations due to manufacturer design and implementation undefined function can be observed and modelled through the uu interface. Through supervised learning, a model may be trained to learn distinguishing features of a set of distinct UE. Trained sets may be stored in a database and when the system is live, UE capability information is queried from the database, and a resulting UE model is yielded.

[0042] **FIG. 6** illustrates, in a call flow diagram, an example of a method of determining a UE model **600**, in accordance with some embodiments. The system **120** listens **302** on the uplink for a UE **112**, **114**. The MME **210** requests **304** UE capabilities from the eNB **102**. The eNB **102** sends a UE capability enquiry message **606** to the UE **112**, **114**. The UE **112**, **114** sends its UE capability information **608** to the eNB **102**. The eNB **102** stores and reports **610** the UE capabilities to the MME **210**. The system **120** then reads **612** the capabilities of the UE **112**, **114**. The system **120** then looks up and retrieves the UE model from the database **224** which in turn sends the UE model to the system **120**.

[0043] System **120** monitors the uplink channel by listening to a particular frequency derived from a downlink E-UTRA Absolute Radio Frequency Channel Number (EARFCN) of the eNB(s) **102** serving the area under protection. The term listening refers to parsing various LTE based messages between the UE **112**, **114** and eNB **102**. System **120** does not connect with the UE **112**, **114**, the unencrypted messages exchanged over the air are monitored. Step **612** is a representation of system **120** also reading the UE capabilities when they are requested from the eNB **102**. In some embodiments, the database **224** is trained for a large set of UEs currently used. Should a UE exhibit capabilities that are not detected in the trained model, it may detect something close or nothing at all. In this particular scenario, the model can later be trained (e.g., via online learning) with the new unseen capabilities configurations. The method shown in **FIG. 6** may be used to gather additional information about a potential intruder and help shape the “image” or “signature” of an intruder.

[0044] **FIG. 7** illustrates an example of a machine learning method of determining a UE model **700**, in accordance with some embodiments. A set of various popular UE models (consisting of phones and tablets), and various operating systems (iOS, Android based, Windows based, others) may be gathered. In order to facilitate retrieving the features of the UEs, they need to be determined by training the model(s). Through the use of a customized eNB in a testing facility the capabilities for each device model may be determined, which can be further tagged by baseband radio manufacturer and operating system. This is a supervised learning exercise where labels are given to each UE. The trained model roughly computes the probability of a given label given known capability information as an output which is anchored to a particular UE model.

[0045] Supervised Labels **702** are fed into a machine learning (ML) classification algorithm **704**. A UE capability vector **706** specific to a make and model for a UE is fed into a feature extraction module **708**. The feather extraction outputs a set of features (f0, f1, …fj) **710** unique to the UE which are then fed into the ML classification algorithm **704**. The supervised labels **702** and

set of features **710** are used by the ML classification algorithm **704** to generate a classifier model **712**. Prediction pipeline **714** provides statistical modelling data for each make and model of UEs for the classifier model **712** to use to determine the probability of what make and model is being detected. The classifier model **712** generates an instantiated UE model **716** representing the make and model of the UE that is being detected.

LTE and 5G-NR localization aid with CSI, Timing Advance and mmWave+LIDAR

[0046] In some embodiments, UE localization aid in 4G/LTE may be achieved through the use of a fused solution to compensate for clock inefficiencies/errors, missed resource elements due to hardware inefficiencies, and counter-attack techniques of intruders. Furthermore for Fifth Generation mobile network (5G), a bifurcated system is provided due to low frequency bands (FR1) and high frequency bands (FR2). FR1 localization will use many of the concepts from Forth Generation (4G) and OTDOA, while FR2 will use mmWave technologies along with light detection and ranging (LIDAR).

[0047] **FIG. 8** illustrates an example of determining UE localization **800**, in accordance with some embodiments. In areas where either 4G, 5G or both are present, a fused solution may take care of various UEs **112**, **114** that may be on the property operating on different frequencies of the spectrum. Channel State Information **804** derived from the downlink along with other parameters may be used to improve position estimates of the UE **112**, **114** on the property. As it relates to 5G, a modified OTDOA (Observed Time Difference of Arrival) **806** may be used that receives device and location data pertaining to low frequency bands of 5G-FR1 **808** and/or device and location data pertaining to 5G-FR2 mmWave **810**. Lidar and mmWave technologies **812** are similarly commissioned to improve position accuracy for 5G frequencies with FR2 (24.25-52.6 GHz). These location estimators may be fused together in a model **802** (via machine learning) to determine the UEs geolocation based on a pre-calculated cellular RF map.

[0048] **FIG. 9** is a schematic diagram of a computing device **1000** such as a server or other computer. As depicted, the computing device includes at least one processor **1002**, memory **1004**, at least one I/O interface **1006**, and at least one network interface **1008**.

[0049] Processor **1002** may be an Intel or AMD x86 or x64, PowerPC, ARM processor, or the like. Memory **1004** may include a suitable combination of computer memory that is located either internally or externally such as, for example, random-access memory (RAM), read-only memory (ROM), compact disc read-only memory (CDROM).

[0050] Each I/O interface **1006** enables computing device **1000** to interconnect with one or more input devices, such as a keyboard, mouse, camera, touch screen and a microphone, or with one or more output devices such as a display screen and a speaker.

[0051] Each network interface **1008** enables computing device **1000** to communicate with other components, to exchange data with other components, to access and connect to network resources, to serve applications, and perform other computing applications by connecting to a network (or multiple networks) capable of carrying data including the Internet, Ethernet, plain old telephone service (POTS) line, public switch telephone network (PSTN), integrated services digital network (ISDN), digital subscriber line (DSL), coaxial cable, fiber optics, satellite, mobile, wireless (e.g. Wi-Fi, WiMAX), SS7 signaling network, fixed line, local area network, wide area network, and others.

[0052] The foregoing discussion provides example embodiments of the inventive subject matter. Although each embodiment represents a single combination of inventive elements, the inventive subject matter is considered to include all possible combinations of the disclosed elements. Thus, if one embodiment comprises elements A, B, and C, and a second embodiment comprises elements B and D, then the inventive subject matter is also considered to include other remaining combinations of A, B, C, or D, even if not explicitly disclosed.

[0053] The embodiments of the devices, systems and methods described herein may be implemented in a combination of both hardware and software. These embodiments may be implemented on programmable computers, each computer including at least one processor, a data storage system (including volatile memory or non-volatile memory or other data storage elements or a combination thereof), and at least one communication interface.

[0054] Program code is applied to input data to perform the functions described herein and to generate output information. The output information is applied to one or more output devices. In some embodiments, the communication interface may be a network communication interface. In embodiments in which elements may be combined, the communication interface may be a software communication interface, such as those for inter-process communication. In still other embodiments, there may be a combination of communication interfaces implemented as hardware, software, and combination thereof.

[0055] Throughout the foregoing discussion, numerous references will be made regarding servers, services, interfaces, portals, platforms, or other systems formed from computing devices. It should be appreciated that the use of such terms is deemed to represent one or more computing

devices having at least one processor configured to execute software instructions stored on a computer readable tangible, non-transitory medium. For example, a server can include one or more computers operating as a web server, database server, or other type of computer server in a manner to fulfill described roles, responsibilities, or functions.

[0056] The technical solution of embodiments may be in the form of a software product. The software product may be stored in a non-volatile or non-transitory storage medium, which can be a compact disk read-only memory (CD-ROM), a USB flash disk, or a removable hard disk. The software product includes a number of instructions that enable a computer device (personal computer, server, or network device) to execute the methods provided by the embodiments.

[0057] The embodiments described herein are implemented by physical computer hardware, including computing devices, servers, receivers, transmitters, processors, memory, displays, and networks. The embodiments described herein provide useful physical machines and particularly configured computer hardware arrangements.

[0058] Although the embodiments have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein.

[0059] Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification.

[0060] As can be understood, the examples described above and illustrated are intended to be exemplary only.

WHAT IS CLAIMED IS:

1. A system for detecting mobile devices, the system comprising:

at least one processor; and

a memory storing instructions which when executed by the at least one processor configure the at least one processor to:

send, by a processor, a soft page message via a Mobile Station Integrated Services Digital Network (MSISDN) to a Mobility Management Entity (MME);

track, by the processor, at least one of:

a Temporary Mobile Subscriber Identity (TMSI);

a Serving TMSI (S-TMSI);

a Globally Unique Temporary UE Identity (GUTI); or

a cell Radio Network Temporary Identifier (c-RNTI); and

send, by the processor to an Evolved Node B (eNB), a Paging Radio Network Temporary Identifier (P-RNTI) filtering message.

2. The system as claimed in claim 1, wherein the at least one processor is configured to:

start, by the MME, a T3413 timer;

send, by the MME to the eNB, a Paging Control Channel (PCCH) paging message; and

send, by the eNB to a known mobile device, a Radio Resource Control paging message.

3. The system as claimed in claim 1, wherein to track the at least one of the TMSI, S-TMSI, GUTI, or c-RNTI comprises the at least one processor receiving device and location data from at least one of:

an Observed Time Difference of Arrival (OTDOA);

light detection and ranging (LIDAR); or

Channel State Information.

4. The system as claimed in claim 3, wherein device and location data received from the OTDOA include data pertaining to Fifth Generation low frequency bands (5G-FR1) and data pertaining to 5G high frequency bands (5G-FR2) mmWave.

5. A system for classifying detected mobile devices, the system comprising:

at least one processor; and

a memory storing instructions which when executed by the at least one processor configure the at least one processor to:

listen, by a processor, on an uplink channel for a detected mobile device;

receive, by the processor from the detected mobile device, capabilities information regarding the detected mobile device; and

obtain, by the processor from a database, a user equipment (UE) model of the detected mobile device, said UE model determined based on the capabilities information.

6. The system as claimed in claim 5, wherein the processor is configured to:

retrieve, by the processor from a database, the UE model based on the capabilities.

7. The system as claimed in claim 5, wherein the processor is configured to:

send, by an MME to an eNB, a request message for capabilities of the detected mobile device;

send, by the eNB to the detected mobile device, a capability enquiry request;

receive, by the eNB from the detected mobile device, the capabilities information; and

receive, by the MME from the eNB, the capabilities information.

8. The system as claimed in claim 5, wherein to receive includes the processor receiving device and location data from at least one of:

an OTDOA;

LIDAR; or

Channel State Information.

9. The system as claimed in claim 8, wherein device and location data received from the OTDOA include data pertaining to 5G-FR1 and data pertaining to 5G-FR2 mmWave.

10. A method of detecting mobile devices, the method comprising:

sending, by a processor, a soft page message via MSISDN to an MME;

tracking, by the processor, a TMSI/S-TMSI/GUTI/c-RNTI; and

sending, by the processor to an eNB, a P-RNTI filtering message.

11. The method as claimed in claim 10, comprising:

starting, by the MME, a T3413 timer;

sending, by the MME to the eNB, a PCCH – paging message; and

sending, by the eNB to a known mobile device, an RRC paging message.

12. The method of claim 10, wherein tracking includes receiving device and location data from at least one of:

an OTDOA;

LIDAR; or

Channel State Information.

13. The method of claim 12, wherein device and location data received from the OTDOA include data pertaining to 5G-FR1 and data pertaining to 5G-FR2 mmWave.

14. A method of classifying detected mobile devices, the method comprising:

listening, by a processor, on an uplink channel for a detected mobile device;

receiving, by the processor from the detected mobile device, capabilities information regarding the detected mobile device; and

obtaining, by the processor from a database, a UE model of the detected mobile device, said UE model determined based on the capabilities information.

15. The method as claimed in claim 14, comprising:

retrieving, by the processor from a database, the UE model based on the capabilities.

16. The method as claimed in claim 14, comprising:

sending, by an MME to an eNB, a request message for capabilities of the detected mobile device;

sending, by the eNB to the detected mobile device, a capability enquiry request;

receiving, by the eNB from the detected mobile device, the capabilities information; and

receiving, by the MME from the eNB, the capabilities information.

17. The method of claim 14, wherein receiving includes receiving device and location data from at least one of:

an OTDOA;

LIDAR; or

Channel State Information.

18. The method of claim 17, wherein device and location data received from the OTDOA include data pertaining to 5G-FR1 and data pertaining to 5G-FR2 mmWave.

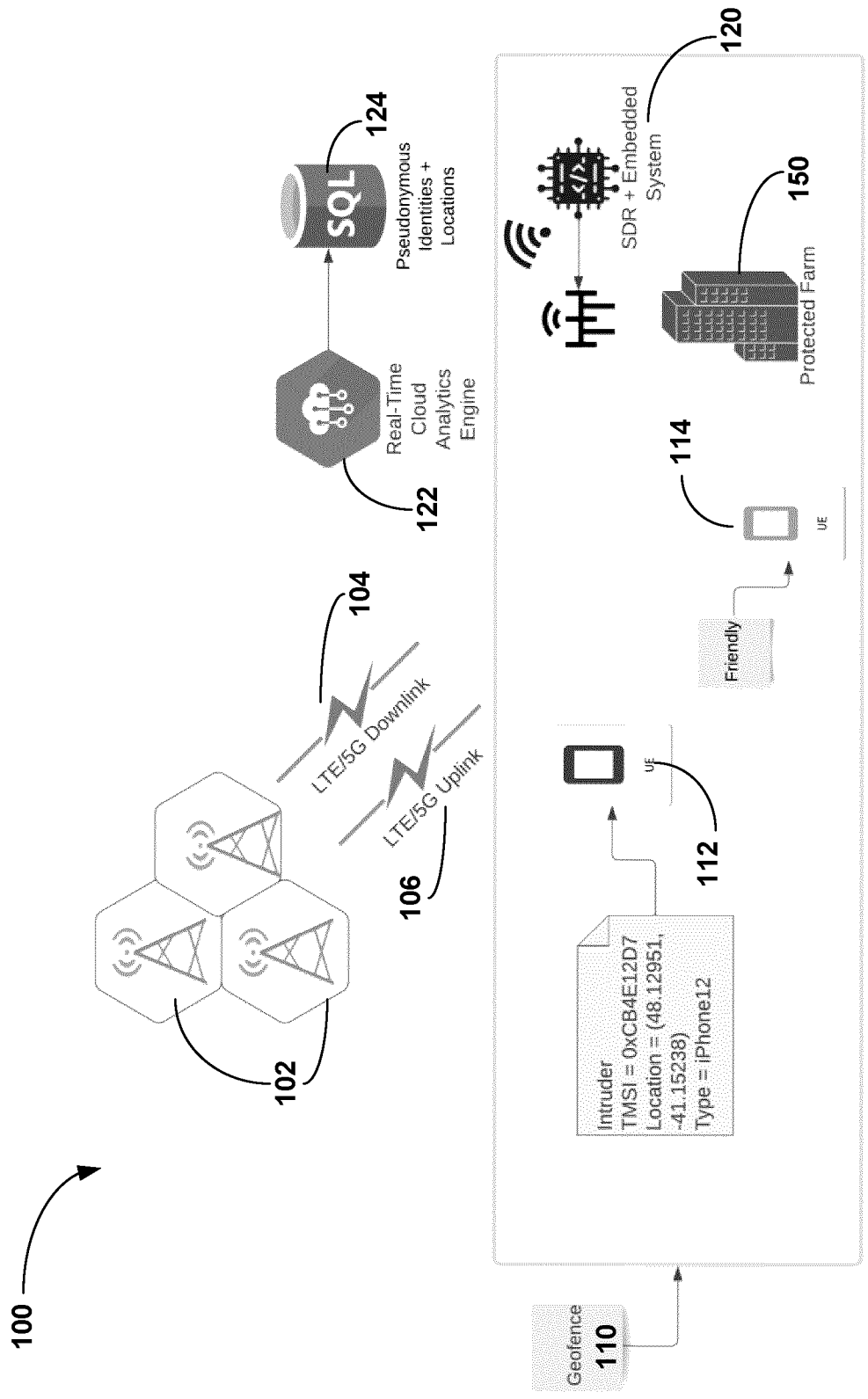

100
102
104
LTE/5G Downlink
106
LTE/5G Uplink
122
Real-Time Cloud Analytics Engine
124
SQL
Pseudonymous Identities + Locations
120
SDR + Embedded System
150
Protected Farm
114
UE
Friendly
112
UE
Intruder
TMSI = 0xCB4E12D7
Location = (48.12951, -41.15238)
Type = iPhone12
Geofence
110

FIG. 1

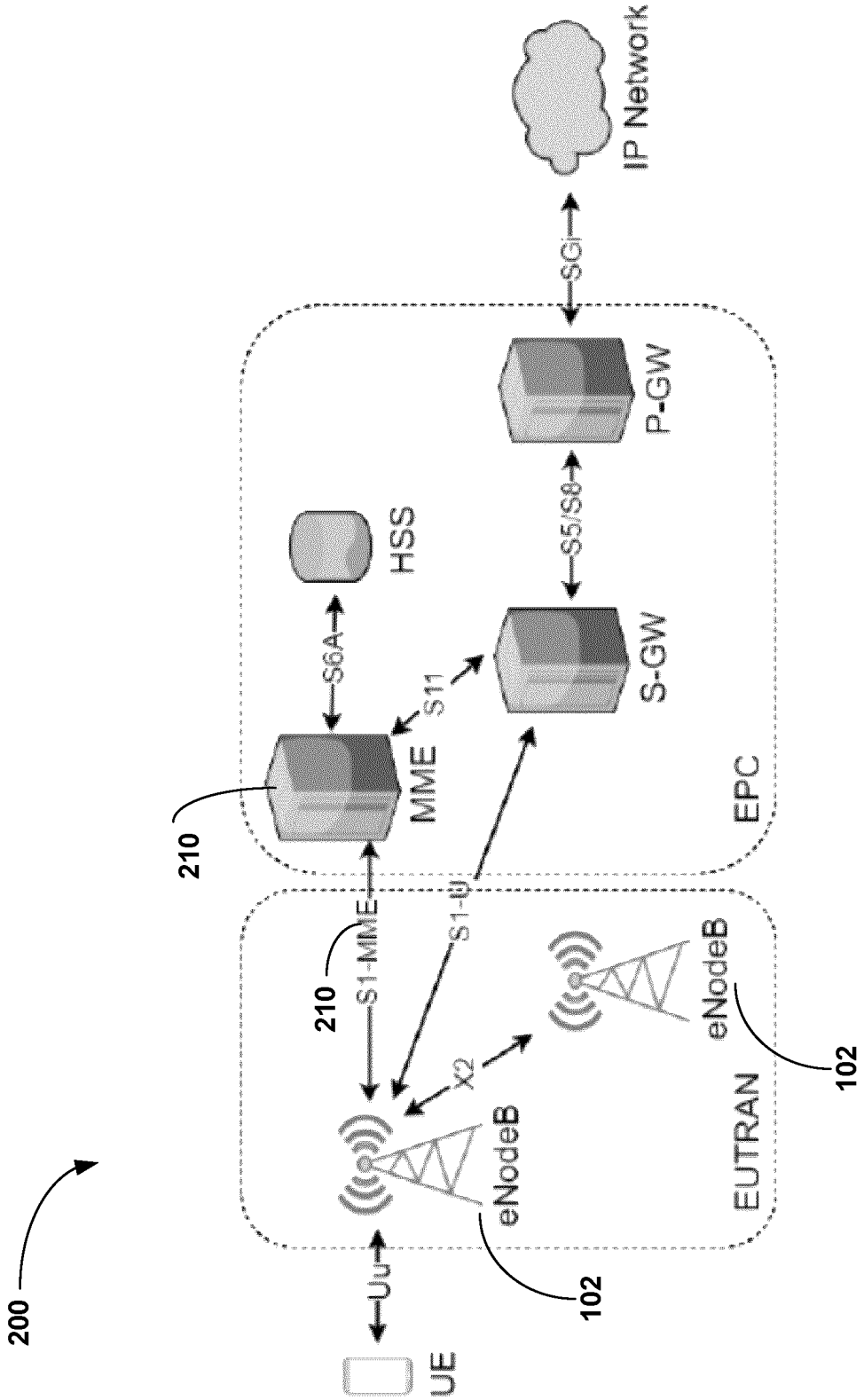

200
UE
Uu
eNodeB
102
EUTRAN
X2
eNodeB
102
S1-MME
210
S1-U
MME
210
S11
S-GW
S6A
HSS
S5/S8
P-GW
EPC
SGi
IP Network

FIG. 2

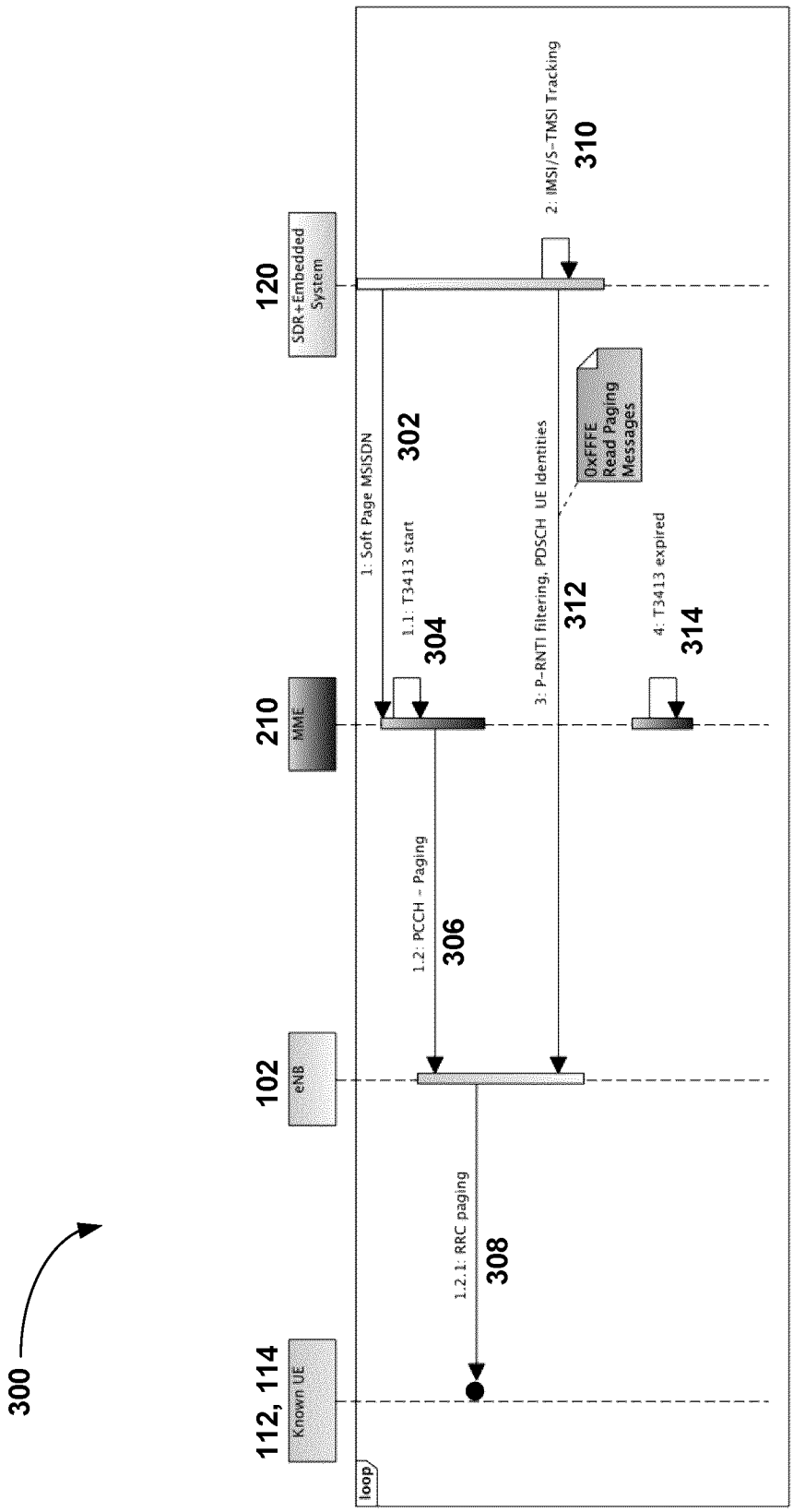

300
112, 114
Known UE
102
eNB
210
MME
120
SDR+Embedded System
loop
1: Soft Page MSISDN
302
1.1: T3413 start
304
1.2: PCCH - Paging
306
1.2.1: RRC paging
308
2: IMSI/S-TMSI Tracking
310
3: P-RNTI filtering, PDSCH UE Identities
312
0xFFFE Read Paging Messages
4: T3413 expired
314

FIG. 3

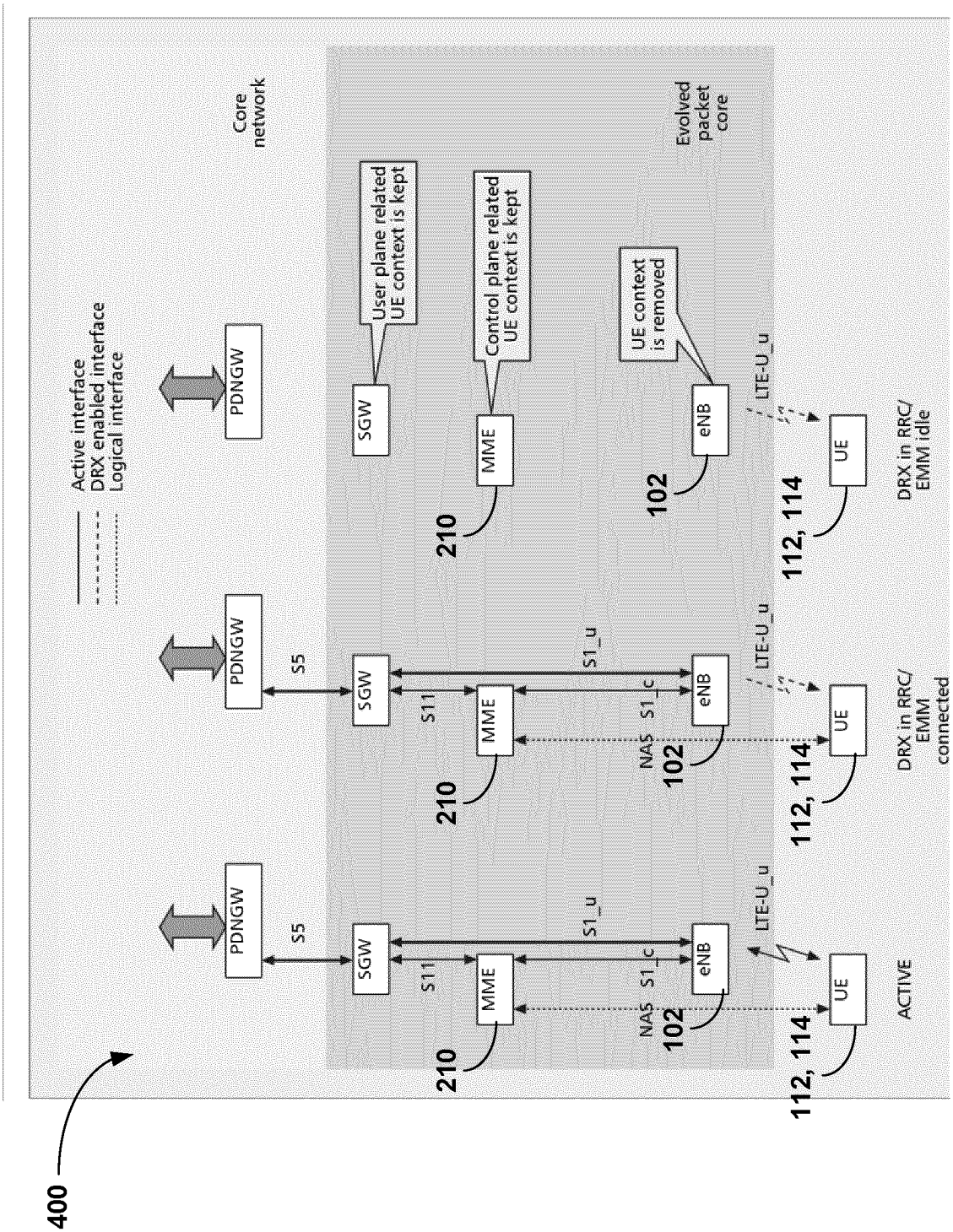

400
Active interface
DRX enabled interface
Logical interface
Core network
Evolved packet core
PDNGW
PDNGW
PDNGW
S5
S5
SGW
SGW
SGW
S11
S11
S11
MME
MME
MME
210
210
210
S1_u
S1_u
S1_u
S1_c
S1_c
S1_c
NAS
NAS
NAS
eNB
eNB
eNB
102
102
102
LTE-U_u
LTE-U_u
LTE-U_u
LTE-U_u
UE
UE
UE
UE
112, 114
112, 114
112, 114
User plane related UE context is kept
Control plane related UE context is kept
UE context is removed
ACTIVE
DRX in RRC/ EMM connected
DRX in RRC/ EMM idle

FIG. 4

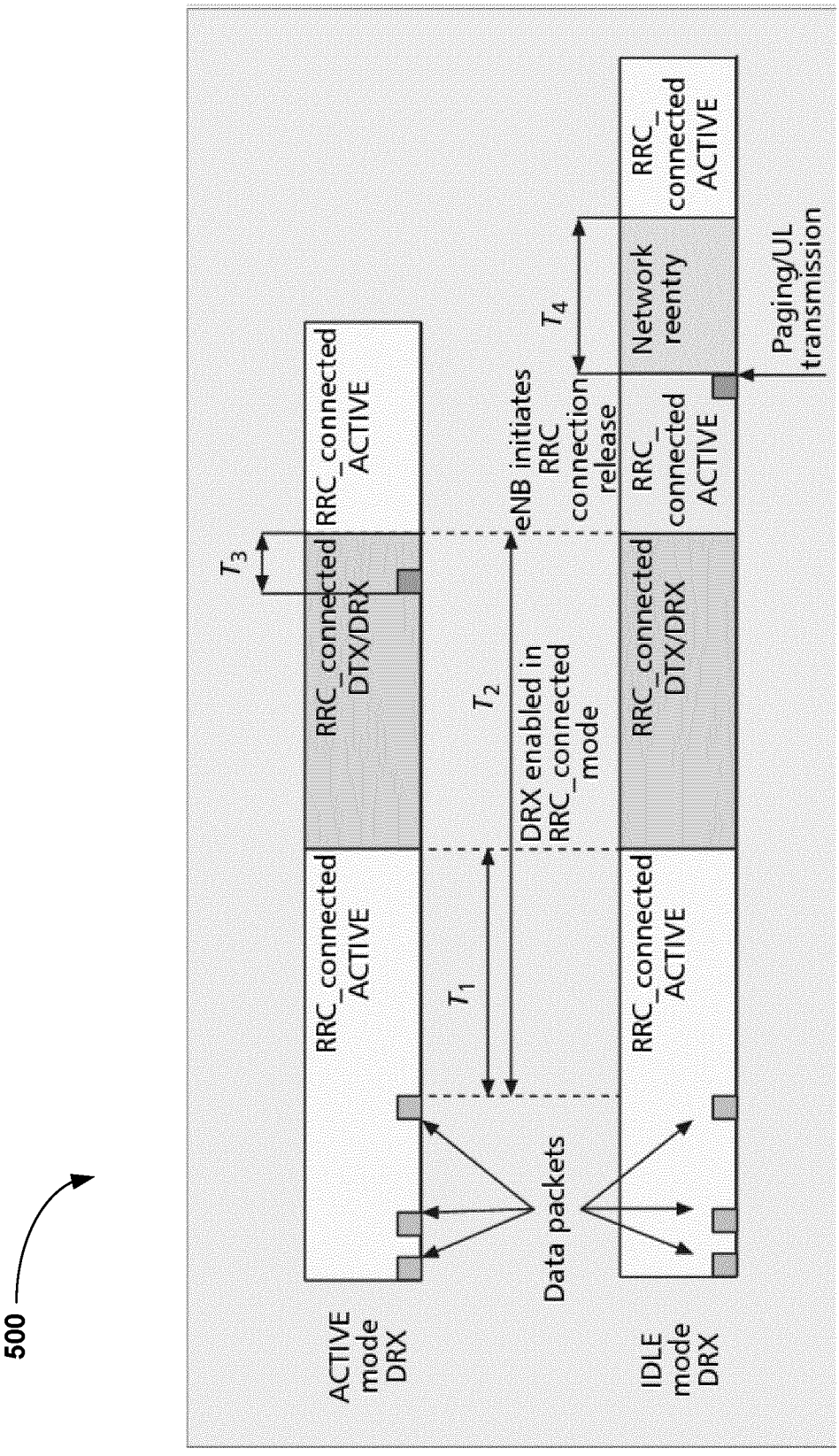

500
ACTIVE mode DRX
IDLE mode DRX
RRC_connected ACTIVE
RRC_connected DTX/DRX
RRC_connected ACTIVE
RRC_connected DTX/DRX
RRC_connected ACTIVE
RRC_connected ACTIVE
Network reentry
RRC_connected ACTIVE
Data packets
T_1
T_2
T_3
T_4
DRX enabled in RRC_connected mode
eNB initiates RRC connection release
Paging/UL transmission

FIG. 5

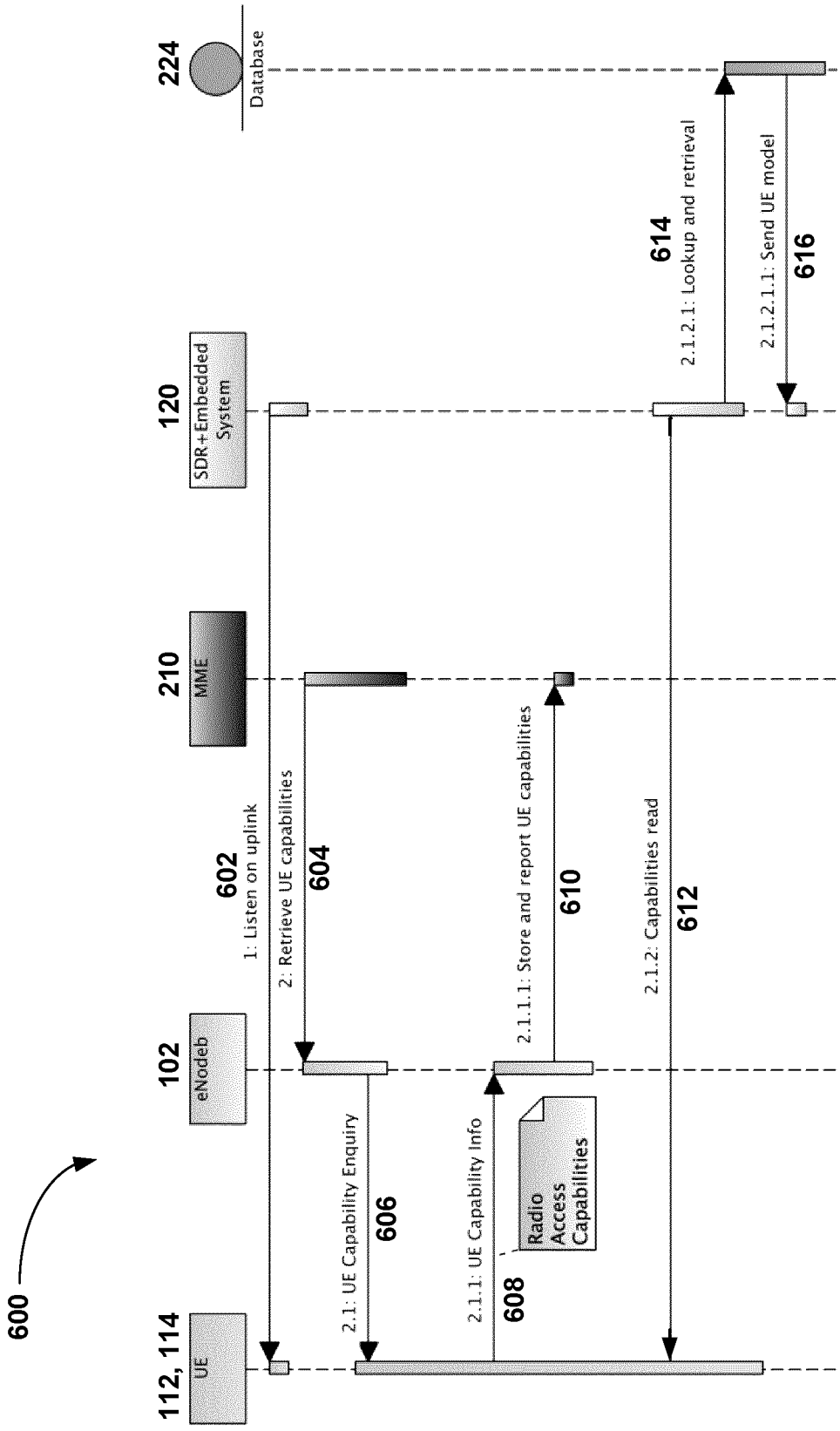

600
112, 114
UE
102
eNodeb
210
MME
120
SDR+Embedded System
224
Database
602
1: Listen on uplink
604
2: Retrieve UE capabilities
606
2.1: UE Capability Enquiry
608
2.1.1: UE Capability Info
Radio Access Capabilities
610
2.1.1.1: Store and report UE capabilities
612
2.1.2: Capabilities read
614
2.1.2.1.1: Lookup and retrieval
616
2.1.2.1.1: Send UE model

FIG. 6

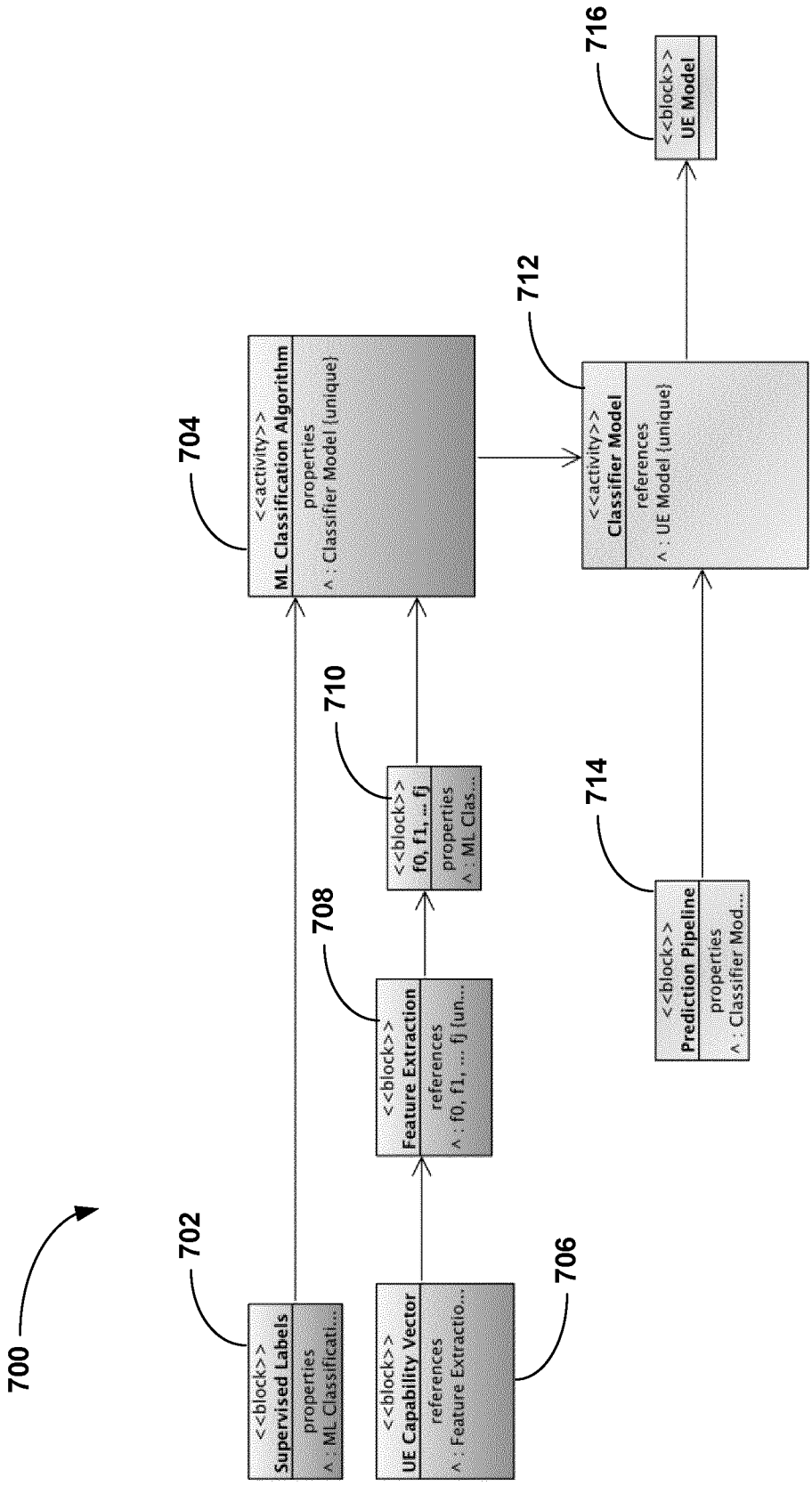

700
702
<<block>>
Supervised Labels
properties
^ : ML Classificati...
706
<<block>>
UE Capability Vector
references
^ : Feature Extractio...
708
<<block>>
Feature Extraction
references
^ : f0, f1, ... fj {un...
710
<<block>>
f0, f1, ... fj
properties
^ : ML Clas...
704
<<activity>>
ML Classification Algorithm
properties
^ : Classifier Model {unique}
712
<<activity>>
Classifier Model
references
^ : UE Model {unique}
714
<<block>>
Prediction Pipeline
properties
^ : Classifier Mod...
716
<<block>>
UE Model
710

FIG. 7

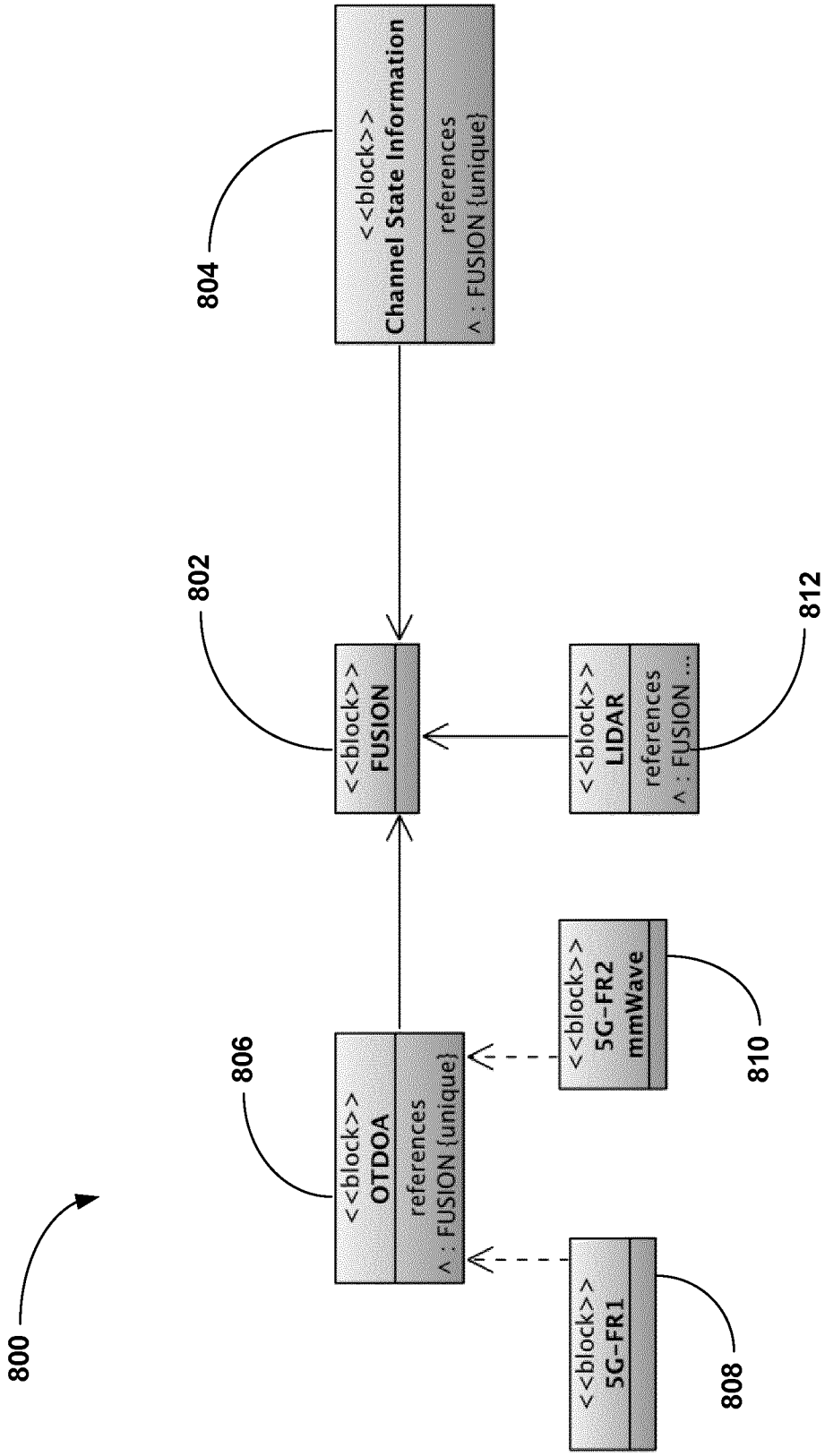

800
804
<<block>>
Channel State Information
references
^ : FUSION {unique}
802
<<block>>
FUSION
812
<<block>>
LIDAR
references
^ : FUSION ...
806
<<block>>
OTDOA
references
^ : FUSION {unique}
<<block>>
5G-FR2
mmWave
810
<<block>>
5G-FR1
808

FIG. 8

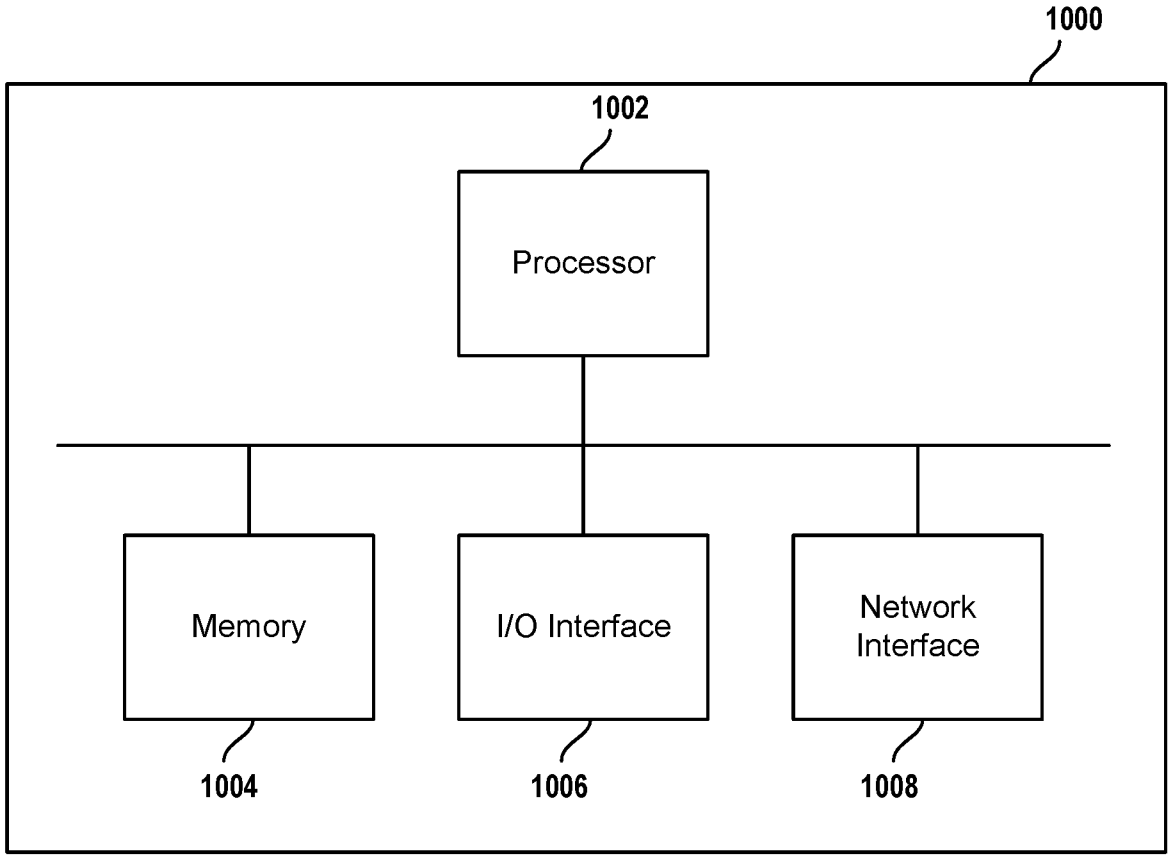

1000
1002
Processor
Memory
I/O Interface
Network Interface
1004
1006
1008

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2023/050528

A. CLASSIFICATION OF SUBJECT MATTER

IPC: ***H04W 8/00*** (2009.01) , ***G01S 1/20*** (2006.01) , ***H04W 64/00*** (2009.01)

CPC: **H04W 8/005** (2020.01) , G01S 1/20 (2020.01) , H04W 64/00 (2020.01)

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)
IPC: ***H04W 8/00*** (2009.01) , ***G01S 1/20*** (2006.01) , ***H04W 64/00*** (2009.01)

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Database: Questal Orbit
Keywords: mobile device, mobile model, UE model, capability, uplink, page, TMSI, GUTI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 11224004 B (Sotomayor et al.) 11 Jan 2022 (11-01-2022) See the whole document, especially Abstract; Figs. 2-6; Claim 1; Column 2, line 44-column 6, line 19	1-4, 10-13
X	US 20070155372 A (Huang) 05 July 2007 (05-07-2007) See the whole document, especially: Claim 1, Abstract; Figs. 1-2; Paragraphs 0012-0013; Paragraphs 0026-0034	5-9, 14-18

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"D"	document cited by the applicant in the international application	"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
"E"	earlier application or patent but published on or after the international filing date	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search 20 August 2023	Date of mailing of the international search report 05 September 2023 (05-09-2023)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 819-953-2476	Authorized officer Ning Huang (819) 639-5259

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2023/050528

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of the first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claim Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claim Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claim Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Claims 1-4 and 10-13 are directed to a method/system of detecting mobile devices.
Claims 5-9 and 14-18 are directed to a method/system of classifying detected mobile devices.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claim Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claim Nos.:

Remark on Protest

☒ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2023/050528

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US11224004B2	11 January 2022 (11-01-2022)	US2021084570A1	18 March 2021 (18-03-2021)
		US2020084701A1	12 March 2020 (12-03-2020)
		US10785708B2	22 September 2020 (22-09-2020)
		US2022132398A1	28 April 2022 (28-04-2022)
US2007155372A1	05 July 2007 (05-07-2007)	None	