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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
02 December 2021 (02.12.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/237391 A1

(51) International Patent Classification:
H04L 12/24 (2006.01) *H04L 12/813* (2013.01)

(21) International Application Number:
PCT/CN2020/091987

(22) International Filing Date:
25 May 2020 (25.05.2020)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **QUALCOMM INCORPORATED** [US/US]; Attn: International IP Administration, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(72) Inventors; and

(71) Applicants *(for US only)*: **ZHANG, Nan** [CN/CN]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US). **LI, Zhiguo** [CN/CN]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US). **HUI, ChaoFeng** [CN/CN]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(74) Agent: **NTD PATENT & TRADEMARK AGENCY LTD.**; 10th Floor, Tower C, Beijing Global Trade Center, 36 North Third Ring Road East, Dongcheng District, Beijing 100013 (CN).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, 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, 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).

Declarations under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

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

(54) **Title:** ENCRYPTING APPLICATION IDENTIFIERS

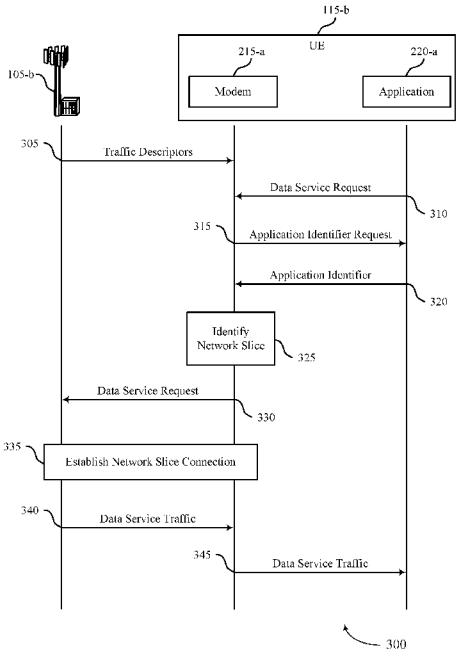

FIG. 3

(57) **Abstract:** Methods, systems, and devices for wireless communications are described. A user equipment (UE) may receive a traffic descriptor that includes an encrypted application identifier corresponding to an application. The UE may additionally receive an application identifier of the application and a decryption key for the application identifier. For example, an application requesting a data service may provide the identifier of the application and the decryption key for the application identifier to the UE. The UE may then transmit, to a base station, a data service request that requests data service for the application according to the received traffic descriptor. The UE may receive, from the base station, data service traffic for the data service that includes the encrypted application identifier. The UE may route the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application.

WO 2021/237391 A1

ENCRYPTING APPLICATION IDENTIFIERS

FIELD OF TECHNOLOGY

[0001] The following relates generally to wireless communications and more specifically to encrypting application identifiers.

BACKGROUND

[0002] Wireless communications systems are widely deployed to provide various types of communication content such as voice, video, packet data, messaging, broadcast, and so on. These systems may be capable of supporting communication with multiple users by sharing the available system resources (e.g., time, frequency, and power). Examples of such multiple-access systems include fourth generation (4G) systems such as Long Term Evolution (LTE) systems, LTE-Advanced (LTE-A) systems, or LTE-A Pro systems, and fifth generation (5G) systems which may be referred to as New Radio (NR) systems. These systems may employ technologies such as code division multiple access (CDMA), time division multiple access (TDMA), frequency division multiple access (FDMA), orthogonal frequency division multiple access (OFDMA), or discrete Fourier transform spread orthogonal frequency division multiplexing (DFT-S-OFDM). A wireless multiple-access communications system may include one or more base stations or one or more network access nodes, each simultaneously supporting communication for multiple communication devices, which may be otherwise known as user equipment (UE).

[0003] A wireless multiple-access communications system may include one or more base stations or one or more network access nodes, each simultaneously supporting communication for multiple communication devices, which may be otherwise known as user equipment (UE). In some wireless communications system, a UE may access a network slice for communicating with a base station. Improved techniques for managing communications between a base station and a UE via a network slice may be desirable.

SUMMARY

[0004] The described techniques relate to improved methods, systems, devices, and apparatuses that support encrypting application identifiers. Generally, the described techniques provide for a user equipment (UE) to receive a set of traffic descriptors each

including an encrypted application identifier corresponding to an application. Each traffic descriptor may additionally indicate, to the UE, a network slice (e.g., from a set of available network slices) that the UE is to use for establishing a data service for the associated application. When an application requests a data service, the UE may in turn request for the application to provide its application identifier and a decryption key for the application identifier. The UE may then identify the traffic descriptor associated with the application requesting the data service by decrypting the encrypted application identifier included in the traffic descriptor using the decryption key provided by the application to obtain the application identifier. Thus, the UE may transmit (e.g., to a base station) a data service request for the application according to the traffic descriptor associated with the application.

[0005] Once a data service for the application has been established (e.g., in response to the UE transmitting the data service request), the UE may receive data service traffic for the application. The data service traffic may include the encrypted application identifier of the application. The UE may decrypt the encrypted application identifier to obtain the application identifier of the application and route the data service traffic to the application based on decrypting the application identifier.

[0006] A method of wireless communication at a UE is described. The method may include receiving a traffic descriptor that includes an encrypted application identifier corresponding to an application, receiving an application identifier of the application and a decryption key for the application identifier, transmitting, to a base station, a data service request that requests data service for the application according to the received traffic descriptor, receiving, from the base station, data service traffic for the data service that includes the encrypted application identifier, and routing the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application.

[0007] An apparatus for wireless communication at a UE is described. The apparatus may include a processor, memory coupled with the processor, and instructions stored in the memory. The instructions may be executable by the processor to cause the apparatus to receive a traffic descriptor that includes an encrypted application identifier corresponding to an application, receive an application identifier of the application and a decryption key for the application identifier, transmit, to a base station, a data service request that requests data

service for the application according to the received traffic descriptor, receive, from the base station, data service traffic for the data service that includes the encrypted application identifier, and route the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application.

[0008] Another apparatus for wireless communication at a UE is described. The apparatus may include means for receiving a traffic descriptor that includes an encrypted application identifier corresponding to an application, receiving an application identifier of the application and a decryption key for the application identifier, transmitting, to a base station, a data service request that requests data service for the application according to the received traffic descriptor, receiving, from the base station, data service traffic for the data service that includes the encrypted application identifier, and routing the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application.

[0009] A non-transitory computer-readable medium storing code for wireless communication at a UE is described. The code may include instructions executable by a processor to receive a traffic descriptor that includes an encrypted application identifier corresponding to an application, receive an application identifier of the application and a decryption key for the application identifier, transmit, to a base station, a data service request that requests data service for the application according to the received traffic descriptor, receive, from the base station, data service traffic for the data service that includes the encrypted application identifier, and route the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application.

[0010] In some examples of the method, apparatuses, and non-transitory computer-readable medium described herein, transmitting the data service request may include operations, features, means, or instructions for transmitting the data service request according to the received traffic descriptor based on decrypting the application identifier within the received traffic descriptor using the decryption key.

[0011] In some cases of the method, apparatuses, and non-transitory computer-readable medium described herein, receiving the traffic descriptor may include operations, features,

means, or instructions for receiving a network slice selection policy indicating a first network slice from a set of available network slices associated with the application.

[0012] In some instances of the method, apparatuses, and non-transitory computer-readable medium described herein, receiving the application identifier may include operations, features, means, or instructions for receiving the application identifier that may be an operating system application identifier.

[0013] Some examples of the method, apparatuses, and non-transitory computer-readable medium described herein may further include operations, features, means, or instructions for establishing a connection with a trusted environment, and receiving the decryption key for the application identifier from the trusted environment.

[0014] In some cases of the method, apparatuses, and non-transitory computer-readable medium described herein, the trusted environment may be associated with a public land mobile network.

[0015] Some instances of the method, apparatuses, and non-transitory computer-readable medium described herein may further include operations, features, means, or instructions for receiving the traffic descriptor that includes the encrypted application identifier corresponding to the application from a public land mobile network.

[0016] Some examples of the method, apparatuses, and non-transitory computer-readable medium described herein may further include operations, features, means, or instructions for receiving, from the base station, a set of traffic descriptors that includes the received traffic descriptor.

[0017] In some cases of the method, apparatuses, and non-transitory computer-readable medium described herein, each of the set of traffic descriptors include an encrypted application identifier corresponding to a unique application.

[0018] Some instances of the method, apparatuses, and non-transitory computer-readable medium described herein may further include operations, features, means, or instructions for identifying a first network slice from a set of available network slices based on the received traffic descriptor, and transmitting a registration request requesting to register with the first network slice of the set of available network slices, where transmitting the data service request may be based on transmitting the registration request.

[0019] Some examples of the method, apparatuses, and non-transitory computer-readable medium described herein may further include operations, features, means, or instructions for receiving a first request for the data service from the application, and transmitting, to the application, a second request for the application identifier and the decryption key, where receiving the application identifier and the decryption key for the application identifier may be based on transmitting the second request.

[0020] Some cases of the method, apparatuses, and non-transitory computer-readable medium described herein may further include operations, features, means, or instructions for matching a decrypted application identifier to the application identifier of the application based on decrypting the encrypted application identifier, where routing the data service traffic to the application may be based on matching the decrypted application identifier to the application identifier.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] FIG. 1 illustrates an example of a system for wireless communications in accordance with aspects of the present disclosure.

[0022] FIG. 2 illustrates an example of a wireless communications system in accordance with aspects of the present disclosure.

[0023] FIG. 3 illustrates an example of a process flow in accordance with aspects of the present disclosure.

[0024] FIGs. 4 and 5 show block diagrams of devices in accordance with aspects of the present disclosure.

[0025] FIG. 6 shows a block diagram of a communications manager in accordance with aspects of the present disclosure.

[0026] FIG. 7 shows a diagram of a system including a device in accordance with aspects of the present disclosure.

[0027] FIGs. 8 through 10 show flowcharts illustrating methods in accordance with aspects of the present disclosure.

DETAILED DESCRIPTION

[0028] Some wireless communications system may support the use of network slices to support additional features and network function optimizations. A network slice may be a logical end-to-end network that can be dynamically created. For example, a user equipment (UE) may establish a protocol data unit (PDU) session for a logical data network, where the logical data network may be referred to as a network slice. In some cases, a UE may select a network slice based on an application or subscription service. For example, a UE may have an application that is an internet protocol (IP) multimedia systems (IMS) voice application, and the UE may select a network slice that is configured to support this mobile broadband application. A UE may, additionally or alternatively, have an application that is configured as an Internet of Everything (IoT) application; for example, the IoT application may configure the UE to operate as an IoT gateway device that compiles and transmits data to a remote server, periodically. As such, the UE may select a network slice that is configured to support massive IoT data traffic. By having different network slices serving different applications, subscriptions, etc., the UE may improve its resource utilization in a network, while also satisfying performance requirements of individual applications of the UE.

[0029] Each network slice may be characterized by a set of parameters which may be defined based on a generic network slice template (GST). For instance, the GST may indicate a quantity of protocol data unit (PDU) sessions per slice, the number of devices supported per slice, or a maximum uplink or downlink data rate per slice. A public land mobile network (PLMN) may provide a UE with a list of traffic descriptors associated with each application of the UE, where each traffic descriptor indicates a network slice (e.g., from a set of available network slices) for providing data service to the corresponding application. Each traffic descriptor may include an application identifier (e.g., an Operating System Application Identifier (OS APP ID) field) indicating a corresponding application. Thus, when an application requests a new data service, the UE may match the application identifier of the requesting application to the application identifier within a traffic descriptor. The UE may then transmit a data service request associated with the network slice indicated by the traffic descriptor.

[0030] The network slices may be served by different network functions (e.g., access and mobility management function (AMF), session management function (SMF), etc.). The

network may, in some cases, provide network slice selection assistance information (NSSAI) or a set of allowed NSSAIs (S-NSSAI) to the UE. The NSSAI may include information indicating allowed or supported network slices for the UE to use, among other information. A data network may be associated with an S-NSSAI. In some cases, a network operator may provide to a UE a network slice selection policy (NSSP). The NSSP may include one or more NSSP rules, each one associating an application with a certain S-NSSAI. In some cases, a default rule may match all applications to a S-NSSAI. In some cases, a UE application associated with an S-NSSAI may request data transmission.

[0031] In some cases, an application (e.g., a cheating application) may request a new data service using an application identifier other than its own application identifier. Here, the UE may match the application identifier (e.g., not associated with the requesting application) to the application identifier within a traffic descriptor that is not associated with the requesting application. Thus, the UE may establish a data service associated with a network slice that is not associated with the requesting application. Enabling an application to access a network slice not associated with that application may decrease a security of communications associated with the network slice.

[0032] To increase a security of communications associated with each network slice, each traffic descriptor may include an encrypted application identifier (e.g., instead of an unencrypted application identifier). When an application requests a data service, the UE may in turn request for the application to provide its application identifier and a decryption key for the application identifier. In some examples, an application vendor may apply for an application identifier (e.g., "OS App ID") from an operator and a secure decryption key at the same time. The UE may then identify the traffic descriptor associated with the application requesting the data service by decrypting the encrypted application identifier included in the traffic descriptor using the decryption key provided by the application to obtain the application identifier. Thus, the UE may transmit (e.g., to a base station) a data service request for the application according to the traffic descriptor associated with the application. Once a data service for the application has been established (e.g., in response to the UE transmitting the data service request), the UE may receive data service traffic for the application. The data service traffic may include the encrypted application identifier of the application. The UE may decrypt the encrypted application identifier to obtain the application

identifier of the application and route the data service traffic to the application based on decrypting the application identifier.

[0033] By encrypting the application identifiers included in each traffic descriptor, an application may not request a data service using an application identifier other than its own because the application may not have access to the decryption key. Thus, the UE may be unable to decrypt the application identifier included in the traffic descriptors. In some cases, this may increase a security associated with network slice instances.

[0034] Aspects of the disclosure are initially described in the context of wireless communications systems. Aspects of the disclosure are further illustrated by and described with reference to a process flow, apparatus diagrams, system diagrams, and flowcharts that relate to encrypting application identifiers.

[0035] **FIG. 1** illustrates an example of a wireless communications system 100 that supports encrypting application identifiers in accordance with aspects of the present disclosure. The wireless communications system 100 may include one or more base stations 105, one or more UEs 115, and a core network 130. In some examples, the wireless communications system 100 may be a Long Term Evolution (LTE) network, an LTE-Advanced (LTE-A) network, an LTE-A Pro network, or a New Radio (NR) network. In some examples, the wireless communications system 100 may support enhanced broadband communications, ultra-reliable (e.g., mission critical) communications, low latency communications, communications with low-cost and low-complexity devices, or any combination thereof.

[0036] The base stations 105 may be dispersed throughout a geographic area to form the wireless communications system 100 and may be devices in different forms or having different capabilities. The base stations 105 and the UEs 115 may wirelessly communicate via one or more communication links 125. Each base station 105 may provide a coverage area 110 over which the UEs 115 and the base station 105 may establish one or more communication links 125. The coverage area 110 may be an example of a geographic area over which a base station 105 and a UE 115 may support the communication of signals according to one or more radio access technologies.

[0037] The UEs 115 may be dispersed throughout a coverage area 110 of the wireless communications system 100, and each UE 115 may be stationary, or mobile, or both at

different times. The UEs 115 may be devices in different forms or having different capabilities. Some example UEs 115 are illustrated in FIG. 1. The UEs 115 described herein may be able to communicate with various types of devices, such as other UEs 115, the base stations 105, or network equipment (e.g., core network nodes, relay devices, integrated access and backhaul (IAB) nodes, or other network equipment), as shown in FIG. 1.

[0038] The base stations 105 may communicate with the core network 130, or with one another, or both. For example, the base stations 105 may interface with the core network 130 through one or more backhaul links 120 (e.g., via an S1, N2, N3, or other interface). The base stations 105 may communicate with one another over the backhaul links 120 (e.g., via an X2, Xn, or other interface) either directly (e.g., directly between base stations 105), or indirectly (e.g., via core network 130), or both. In some examples, the backhaul links 120 may be or include one or more wireless links.

[0039] One or more of the base stations 105 described herein may include or may be referred to by a person having ordinary skill in the art as a base transceiver station, a radio base station, an access point, a radio transceiver, a NodeB, an eNodeB (eNB), a next-generation NodeB or a giga-NodeB (either of which may be referred to as a gNB), a Home NodeB, a Home eNodeB, or other suitable terminology.

[0040] A UE 115 may include or may be referred to as a mobile device, a wireless device, a remote device, a handheld device, or a subscriber device, or some other suitable terminology, where the "device" may also be referred to as a unit, a station, a terminal, or a client, among other examples. A UE 115 may also include or may be referred to as a personal electronic device such as a cellular phone, a personal digital assistant (PDA), a tablet computer, a laptop computer, or a personal computer. In some examples, a UE 115 may include or be referred to as a wireless local loop (WLL) station, an Internet of Things (IoT) device, an Internet of Everything (IoE) device, or a machine type communications (MTC) device, among other examples, which may be implemented in various objects such as appliances, or vehicles, meters, among other examples.

[0041] The UEs 115 described herein may be able to communicate with various types of devices, such as other UEs 115 that may sometimes act as relays as well as the base stations 105 and the network equipment including macro eNBs or gNBs, small cell eNBs or gNBs, or relay base stations, among other examples, as shown in FIG. 1.

[0042] The UEs 115 and the base stations 105 may wirelessly communicate with one another via one or more communication links 125 over one or more carriers. The term "carrier" may refer to a set of radio frequency spectrum resources having a defined physical layer structure for supporting the communication links 125. For example, a carrier used for a communication link 125 may include a portion of a radio frequency spectrum band (e.g., a bandwidth part (BWP)) that is operated according to one or more physical layer channels for a given radio access technology (e.g., LTE, LTE-A, LTE-A Pro, NR). Each physical layer channel may carry acquisition signaling (e.g., synchronization signals, system information), control signaling that coordinates operation for the carrier, user data, or other signaling. The wireless communications system 100 may support communication with a UE 115 using carrier aggregation or multi-carrier operation. A UE 115 may be configured with multiple downlink component carriers and one or more uplink component carriers according to a carrier aggregation configuration. Carrier aggregation may be used with both frequency division duplexing (FDD) and time division duplexing (TDD) component carriers.

[0043] In some examples (e.g., in a carrier aggregation configuration), a carrier may also have acquisition signaling or control signaling that coordinates operations for other carriers. A carrier may be associated with a frequency channel (e.g., an evolved universal mobile telecommunication system terrestrial radio access (E-UTRA) absolute radio frequency channel number (EARFCN)) and may be positioned according to a channel raster for discovery by the UEs 115. A carrier may be operated in a standalone mode where initial acquisition and connection may be conducted by the UEs 115 via the carrier, or the carrier may be operated in a non-standalone mode where a connection is anchored using a different carrier (e.g., of the same or a different radio access technology).

[0044] The communication links 125 shown in the wireless communications system 100 may include uplink transmissions from a UE 115 to a base station 105, or downlink transmissions from a base station 105 to a UE 115. Carriers may carry downlink or uplink communications (e.g., in an FDD mode) or may be configured to carry downlink and uplink communications (e.g., in a TDD mode).

[0045] Signal waveforms transmitted over a carrier may be made up of multiple subcarriers (e.g., using multi-carrier modulation (MCM) techniques such as orthogonal frequency division multiplexing (OFDM) or discrete Fourier transform spread OFDM (DFT-

S-OFDM)). In a system employing MCM techniques, a resource element may consist of one symbol period (e.g., a duration of one modulation symbol) and one subcarrier, where the symbol period and subcarrier spacing are inversely related. The number of bits carried by each resource element may depend on the modulation scheme (e.g., the order of the modulation scheme, the coding rate of the modulation scheme, or both). Thus, the more resource elements that a UE 115 receives and the higher the order of the modulation scheme, the higher the data rate may be for the UE 115. A wireless communications resource may refer to a combination of a radio frequency spectrum resource, a time resource, and a spatial resource (e.g., spatial layers or beams), and the use of multiple spatial layers may further increase the data rate or data integrity for communications with a UE 115.

[0046] The time intervals for the base stations 105 or the UEs 115 may be expressed in multiples of a basic time unit which may, for example, refer to a sampling period of $T_s = 1/(\Delta f_{max} \cdot N_f)$ seconds, where Δf_{max} may represent the maximum supported subcarrier spacing, and N_f may represent the maximum supported discrete Fourier transform (DFT) size. Time intervals of a communications resource may be organized according to radio frames each having a specified duration (e.g., 10 milliseconds (ms)). Each radio frame may be identified by a system frame number (SFN) (e.g., ranging from 0 to 1023).

[0047] Each frame may include multiple consecutively numbered subframes or slots, and each subframe or slot may have the same duration. In some examples, a frame may be divided (e.g., in the time domain) into subframes, and each subframe may be further divided into a number of slots. Alternatively, each frame may include a variable number of slots, and the number of slots may depend on subcarrier spacing. Each slot may include a number of symbol periods (e.g., depending on the length of the cyclic prefix prepended to each symbol period). In some wireless communications systems 100, a slot may further be divided into multiple mini-slots containing one or more symbols. Excluding the cyclic prefix, each symbol period may contain one or more (e.g., N_f) sampling periods. The duration of a symbol period may depend on the subcarrier spacing or frequency band of operation.

[0048] A subframe, a slot, a mini-slot, or a symbol may be the smallest scheduling unit (e.g., in the time domain) of the wireless communications system 100 and may be referred to as a transmission time interval (TTI). In some examples, the TTI duration (e.g., the number of symbol periods in a TTI) may be variable. Additionally or alternatively, the smallest

scheduling unit of the wireless communications system 100 may be dynamically selected (e.g., in bursts of shortened TTIs (sTTIs)).

[0049] Physical channels may be multiplexed on a carrier according to various techniques. A physical control channel and a physical data channel may be multiplexed on a downlink carrier, for example, using one or more of time division multiplexing (TDM) techniques, frequency division multiplexing (FDM) techniques, or hybrid TDM-FDM techniques. A control region (e.g., a control resource set (CORESET)) for a physical control channel may be defined by a number of symbol periods and may extend across the system bandwidth or a subset of the system bandwidth of the carrier. One or more control regions (e.g., CORESETs) may be configured for a set of the UEs 115. For example, one or more of the UEs 115 may monitor or search control regions for control information according to one or more search space sets, and each search space set may include one or multiple control channel candidates in one or more aggregation levels arranged in a cascaded manner. An aggregation level for a control channel candidate may refer to a number of control channel resources (e.g., control channel elements (CCEs)) associated with encoded information for a control information format having a given payload size. Search space sets may include common search space sets configured for sending control information to multiple UEs 115 and UE-specific search space sets for sending control information to a specific UE 115.

[0050] In some examples, a base station 105 may be movable and therefore provide communication coverage for a moving geographic coverage area 110. In some examples, different geographic coverage areas 110 associated with different technologies may overlap, but the different geographic coverage areas 110 may be supported by the same base station 105. In other examples, the overlapping geographic coverage areas 110 associated with different technologies may be supported by different base stations 105. The wireless communications system 100 may include, for example, a heterogeneous network in which different types of the base stations 105 provide coverage for various geographic coverage areas 110 using the same or different radio access technologies.

[0051] The wireless communications system 100 may be configured to support ultra-reliable communications or low-latency communications, or various combinations thereof. For example, the wireless communications system 100 may be configured to support ultra-reliable low-latency communications (URLLC) or mission critical communications. The UEs

115 may be designed to support ultra-reliable, low-latency, or critical functions (e.g., mission critical functions). Ultra-reliable communications may include private communication or group communication and may be supported by one or more mission critical services such as mission critical push-to-talk (MCPTT), mission critical video (MCVideo), or mission critical data (MCData). Support for mission critical functions may include prioritization of services, and mission critical services may be used for public safety or general commercial applications. The terms ultra-reliable, low-latency, mission critical, and ultra-reliable low-latency may be used interchangeably herein.

[0052] In some examples, a UE 115 may also be able to communicate directly with other UEs 115 over a device-to-device (D2D) communication link 135 (e.g., using a peer-to-peer (P2P) or D2D protocol). One or more UEs 115 utilizing D2D communications may be within the geographic coverage area 110 of a base station 105. Other UEs 115 in such a group may be outside the geographic coverage area 110 of a base station 105 or be otherwise unable to receive transmissions from a base station 105. In some examples, groups of the UEs 115 communicating via D2D communications may utilize a one-to-many (1:M) system in which each UE 115 transmits to every other UE 115 in the group. In some examples, a base station 105 facilitates the scheduling of resources for D2D communications. In other cases, D2D communications are carried out between the UEs 115 without the involvement of a base station 105.

[0053] The core network 130 may provide user authentication, access authorization, tracking, Internet Protocol (IP) connectivity, and other access, routing, or mobility functions. The core network 130 may be an evolved packet core (EPC) or 5G core (5GC), which may include at least one control plane entity that manages access and mobility (e.g., a mobility management entity (MME), an access and mobility management function (AMF)) and at least one user plane entity that routes packets or interconnects to external networks (e.g., a serving gateway (S-GW), a Packet Data Network (PDN) gateway (P-GW), or a user plane function (UPF)). The control plane entity may manage non-access stratum (NAS) functions such as mobility, authentication, and bearer management for the UEs 115 served by the base stations 105 associated with the core network 130. User IP packets may be transferred through the user plane entity, which may provide IP address allocation as well as other functions. The user plane entity may be connected to the network operators IP services 150.

The operators IP services 150 may include access to the Internet, Intranet(s), an IP Multimedia Subsystem (IMS), or a Packet-Switched Streaming Service.

[0054] Some of the network devices, such as a base station 105, may include subcomponents such as an access network entity 140, which may be an example of an access node controller (ANC). Each access network entity 140 may communicate with the UEs 115 through one or more other access network transmission entities 145, which may be referred to as radio heads, smart radio heads, or transmission/reception points (TRPs). Each access network transmission entity 145 may include one or more antenna panels. In some configurations, various functions of each access network entity 140 or base station 105 may be distributed across various network devices (e.g., radio heads and ANCs) or consolidated into a single network device (e.g., a base station 105).

[0055] The wireless communications system 100 may operate using one or more frequency bands, typically in the range of 300 megahertz (MHz) to 300 gigahertz (GHz). Generally, the region from 300 MHz to 3 GHz is known as the ultra-high frequency (UHF) region or decimeter band because the wavelengths range from approximately one decimeter to one meter in length. The UHF waves may be blocked or redirected by buildings and environmental features, but the waves may penetrate structures sufficiently for a macro cell to provide service to the UEs 115 located indoors. The transmission of UHF waves may be associated with smaller antennas and shorter ranges (e.g., less than 100 kilometers) compared to transmission using the smaller frequencies and longer waves of the high frequency (HF) or very high frequency (VHF) portion of the spectrum below 300 MHz.

[0056] The wireless communications system 100 may utilize both licensed and unlicensed radio frequency spectrum bands. For example, the wireless communications system 100 may employ License Assisted Access (LAA), LTE-Unlicensed (LTE-U) radio access technology, or NR technology in an unlicensed band such as the 5 GHz industrial, scientific, and medical (ISM) band. When operating in unlicensed radio frequency spectrum bands, devices such as the base stations 105 and the UEs 115 may employ carrier sensing for collision detection and avoidance. In some examples, operations in unlicensed bands may be based on a carrier aggregation configuration in conjunction with component carriers operating in a licensed band (e.g., LAA). Operations in unlicensed spectrum may include

downlink transmissions, uplink transmissions, P2P transmissions, or D2D transmissions, among other examples.

[0057] A base station 105 or a UE 115 may be equipped with multiple antennas, which may be used to employ techniques such as transmit diversity, receive diversity, multiple-input multiple-output (MIMO) communications, or beamforming. The antennas of a base station 105 or a UE 115 may be located within one or more antenna arrays or antenna panels, which may support MIMO operations or transmit or receive beamforming. For example, one or more base station antennas or antenna arrays may be co-located at an antenna assembly, such as an antenna tower. In some examples, antennas or antenna arrays associated with a base station 105 may be located in diverse geographic locations. A base station 105 may have an antenna array with a number of rows and columns of antenna ports that the base station 105 may use to support beamforming of communications with a UE 115. Likewise, a UE 115 may have one or more antenna arrays that may support various MIMO or beamforming operations. Additionally or alternatively, an antenna panel may support radio frequency beamforming for a signal transmitted via an antenna port.

[0058] Beamforming, which may also be referred to as spatial filtering, directional transmission, or directional reception, is a signal processing technique that may be used at a transmitting device or a receiving device (e.g., a base station 105, a UE 115) to shape or steer an antenna beam (e.g., a transmit beam, a receive beam) along a spatial path between the transmitting device and the receiving device. Beamforming may be achieved by combining the signals communicated via antenna elements of an antenna array such that some signals propagating at particular orientations with respect to an antenna array experience constructive interference while others experience destructive interference. The adjustment of signals communicated via the antenna elements may include a transmitting device or a receiving device applying amplitude offsets, phase offsets, or both to signals carried via the antenna elements associated with the device. The adjustments associated with each of the antenna elements may be defined by a beamforming weight set associated with a particular orientation (e.g., with respect to the antenna array of the transmitting device or receiving device, or with respect to some other orientation).

[0059] The wireless communications system 100 may be a packet-based network that operates according to a layered protocol stack. In the user plane, communications at the

bearer or Packet Data Convergence Protocol (PDCP) layer may be IP-based. A Radio Link Control (RLC) layer may perform packet segmentation and reassembly to communicate over logical channels. A Medium Access Control (MAC) layer may perform priority handling and multiplexing of logical channels into transport channels. The MAC layer may also use error detection techniques, error correction techniques, or both to support retransmissions at the MAC layer to improve link efficiency. In the control plane, the Radio Resource Control (RRC) protocol layer may provide establishment, configuration, and maintenance of an RRC connection between a UE 115 and a base station 105 or a core network 130 supporting radio bearers for user plane data. At the physical layer, transport channels may be mapped to physical channels.

[0060] Wireless communications system 100 may support the use of network slices to support additional features and network function optimizations. A network slice may be a logical end-to-end network that can be dynamically created. Each network slice may be characterized by a set of parameters which may be defined based on a GST. For instance, the GST may indicate a quantity of PDU sessions per slice, the number of devices supported per slice, or a maximum uplink or downlink data rate per slice. A PLMN may provide a UE 115 with a list of traffic descriptors associated with each application of the UE 115 (e.g., by a base station 105), where each traffic descriptor indicates a network slice (e.g., from a set of available network slices) for providing data service to the corresponding application. Each traffic descriptor may include an application identifier (e.g., an OS APP ID field) indicating a corresponding application. Thus, when an application requests a new data service, the UE 115 may match the application identifier of the requesting application to the application identifier within a traffic descriptor. The UE 115 may then transmit a data service request associated with the network slice indicated by the traffic descriptor.

[0061] Using network slices may enable multiplexing of virtualized and independent logical networks on a same physical network infrastructure. Each network slice may include an isolated end-to-end network tailored to meet different requirements (e.g., QoS, different application profiles, usage, etc.) requested by a particular application. For example, different applications of a UE 115 may include services with different service level requirements. As such, the network slices may enable a flexible and scalable configuration on top of a common network infrastructure to meet the differing service level requirements for the different applications. In some cases, the different network slices may be administered by separate

operators (e.g., mobile virtual network operators), where an infrastructure provider leases physical resources to these operators that share the underlying physical network of the infrastructure provider. The operators may then deploy multiple network slices customized to the different applications provided to users associated with the operators.

[0062] Additionally, network slicing may enable a mobile operator to create specific virtual networks that cater to particular clients and use cases. For example, certain applications (e.g., such as eMBB communications, machine-to-machine (M2M) communications in manufacturing or logistics, smart cars, etc.) may benefit from leveraging different aspects of wireless communications. A first application may use higher speeds, a second application may use low latency, a third application may use edge computing resources, etc. By creating separate slices that prioritize specific resources, a mobile operator may offer tailored solutions to particular industries. For example, different industries (e.g., marketing, augmented reality, mobile gaming, etc.) may use these network slices for meeting corresponding requirements for the industries. Additionally, network slicing may also enhance service continuity via improved roaming across networks by creating a virtual network running on a physical infrastructure that spans multiple local or national networks, by allowing a host network to create an optimized virtual network which replicates the one offered by a home network for a roaming device (e.g., a UE 115), etc.

[0063] The network slices may be served by different network functions (e.g., AMF, SMF, etc.). The network may, in some cases, provide NSSAI or an S-NSSAI to the UE 115. The NSSAI may include information indicating allowed or supported network slices for the UE 115 to use, among other information. A data network may be associated with an S-NSSAI. In some cases, a network operator may provide to a UE 115 an NSSP. The NSSP may include one or more NSSP rules, each one associating an application with a certain S-NSSAI. In some cases, a default rule may match all applications to a S-NSSAI. In some cases, a UE application associated with an S-NSSAI may request data transmission.

[0064] To increase a security of communications associated with each network slice, each traffic descriptor may include an encrypted application identifier (e.g., instead of an unencrypted application identifier). When an application requests a data service, the UE 115 may in turn request for the application to provide its application identifier and a decryption key for the application identifier. The UE 115 may then identify the traffic descriptor

associated with the application requesting the data service by decrypting the encrypted application identifier included in the traffic descriptor using the decryption key provided by the application to obtain the application identifier. Thus, the UE 115 may transmit (e.g., to a base station 105) a data service request for the application according to the traffic descriptor associated with the application. Once a data service for the application has been established (e.g., in response to the UE 115 transmitting the data service request), the UE 115 may receive data service traffic for the application. The data service traffic may include the encrypted application identifier of the application. The UE 115 may decrypt the encrypted application identifier to obtain the application identifier of the application and route the data service traffic to the application based on decrypting the application identifier.

[0065] By encrypting the application identifiers included in each traffic descriptor, an application may not request a data service using an application identifier other than its own because the application may not have access to the decryption key. Thus, the UE 115 may be unable to decrypt the application identifier included in the traffic descriptors. In some cases, this may increase a security associated with network slice instances.

[0066] **FIG. 2** illustrates an example of a wireless communications system 200 that supports encrypting application identifiers in accordance with aspects of the present disclosure. In some examples, the wireless communications system 200 may implement aspects of wireless communications system 100. For example, the base station 105-a and UE 115-a may be examples of base stations 105 and UEs 115, respectively, as described with reference to FIG. 1.

[0067] The UE 115-a may include a modem 215 and one or more applications, including application 220. In some cases, the modem 215 may enable the UE 115-a to communicate with the base station 105-a using one or more radio access technologies (RATs). For example, the modem 215 may enable the UE 115-a to communicate with the base station 105-a by downlink channel 205 and uplink channel 210. In some cases, the application 220 may store an application identifier identifying the application 220 and a decryption key associated with the application identifier. For example, the application 220 may be provided to the U 115-a by an application vendor, which may supply the application identifier and secure decryption key to the application 220.

[0068] The UE 115-a may receive traffic descriptors 225 for each application 220 at the UE 115-a. For example, the base station 105-a may transmit the traffic descriptors 225 to the U 115-a by the downlink channel 205. In some cases, a PLMN (e.g., associated with the base station 105-a) may provide the traffic descriptors 225 to the UE 115-a during a registration process or during an update process. The traffic descriptors 225 may be network slice selection policy (NSSP) traffic descriptors 225. That is, each traffic descriptor 225 may associate an application with one or more network slices (e.g., from a set of available network slices). Thus, the traffic descriptors 225 may enable the UE 115-a to identify one or more network slices (e.g., one or more network slice instances) associated with the application 220. Each traffic descriptor 225 may include an encrypted application identifier (e.g., an encrypted OSS APP ID field). That is, one of the traffic descriptors 225 may include an encrypted application identifier associated with the application 220.

[0069] The application 220 may communicate a request for a new data service to the modem 215 of the UE 115-a. In response, the modem 215 may request the application identifier associated with the application 220 and a decryption key for the application identifier. The application 220 may provide both the application identifier and the decryption key to the modem 215. In some cases, the modem 215 may establish a trusted environment (e.g., a secure trust zone environment) to receive the decryption key from the application 220 Thus, no other applications 220 of the UE 115-a may be aware of, or be able to access, the decryption key for the application 220. In some examples, the UE 115-a may establish a connection to a trusted environment (e.g., associated with the PLMN) by the application 220 may receive its decryption key. The modem 215 may then decrypt the encrypted application identifiers within the traffic descriptors 225 using the decryption key provided by the application 220. Thus, the modem 215 may obtain a set of decrypted application identifiers, each associated with one of the traffic descriptors 225. The modem 215 may then attempt to match one of the decrypted application identifiers associated with a traffic descriptor 225 to the application identifier supplied to the modem 215 by the application 220. The modem 215 may identify the traffic descriptor 225 associated with the application 220 based on identifying a decrypted application identifier that matches the application identifier supplied by the application 220. This traffic descriptor 225 may indicate a network slice (e.g., from a set of available network slices) associated with the application 220.

[0070] The UE 115-a may then transmit a data service request 230 to the base station 105-a (e.g., by the uplink channel 210) in accordance with the traffic descriptor 225 associated with the application 220. For example, the UE 115-a may transmit a registration request requesting to register with the network slice indicated by the traffic descriptor 225 associated with the application 220. In some cases, the data service request 230 may be a request to establish a PDU session for the network slice indicated by the traffic descriptor 225. Here, the base station 105-a may communicate a PDU session establishment accept message to the U 115-a. In either case, the UE 115-a may establish the data service in accordance with the traffic descriptor 225 associated with the application 220.

[0071] Based on establishing the data service for the application 220, the UE 115-a may receive data service traffic 235 for the data service. The data service traffic 235 may include the encrypted application identifier associated with the application 220. Thus, the UE 115-a may decrypt the encrypted application identifier using the decryption key received from the application 220 to obtain the application identifier indicating the application 220. For example, the modem 215 may decrypt the encrypted application identifier in the trusted environment to prevent other applications 220 at the UE 115-a from identifying the decrypted application identifier. The UE 115-a may match the decrypted application identifier to the application identifier associated with the application 220 and route the data service traffic 235 to the application 220 accordingly.

[0072] **FIG. 3** illustrates an example of a process flow 300 that supports encrypting application identifiers in accordance with aspects of the present disclosure. In some examples, the process flow 300 may implement aspects of wireless communications system 100. For example, the base station 105-b and UE 115-b may be examples of base stations 105 and UEs 115, respectively, as described with reference to FIGs. 1 and 2. For example, UE 115-b may include a modem 215-a and an application 220-a, which may be respective examples of modem 215 and application 220 as described with reference to FIG. 2.

[0073] At 305, the base station 105-b may transmit a set of traffic descriptors to the UE 115-b (e.g., the modem 215-a of the UE 115-b). Each of the traffic descriptors may include an encrypted application identifier corresponding to a unique application 220 at the UE 115-a. Additionally, the set of traffic descriptors may indicate a network slice selection policy. Here, the UE 115-b may receive the network slice selection policy indicating a network slice

from a set of available network slices associated with each application 220 of the UE 115-a. In some cases, the base station 105-b may be associated with a PLMN and may transmit the traffic descriptors 225 to the UE 115-b during a registration or updating of the UE 115-b. Additionally or alternatively, the UE 115-b may receive the traffic descriptors from a different network device associated with the PLMN.

[0074] At 310, the application 220-a may transmit a data service request to the modem 215-a. At 315, the modem 215-a may communicate a second request (e.g., an application identifier request) to the application 220-a in response to receiving the data service request. The second request may additionally request a decryption key associated with the application identifier. At 320, the application 220-a may provide the application identifier of the application 220-a and the decryption key for the application identifier to the modem 215-a.

[0075] At 325, modem 215-a may identify a network slice from a set of available network slices based on the traffic descriptor associated with the application 220-a. That is, the modem 215-a may establish a trusted environment (e.g., to ensure that other applications 220 at the UE 115-b may not identify the application identifier associated with the application 220-a) and decrypt each of the application. The modem 215-a may then decrypt each of the application identifiers included in the set of traffic descriptors and identify the traffic descriptor associated with the application 220-a based on obtaining a decrypted application identifier that matches the application identifier of the application 220-a.

[0076] At 330, the modem 215-a may transmit, to the base station 105-b, a data service request that requests data service for the application 220-a according to the traffic descriptor associated with the application 220-a. For example, the UE 115-b may transmit a registration request to register with the network slice (e.g., identified at 325).

[0077] At 335, the base station 105-b and the UE 115-b may establish the network slice connection for the data service for the application 220-a. For example, the UE 115-b may transmit a PDU establishment request message (e.g., to establish a PDU session associated with the identified network slice) to the base station 105-b and the base station 105-b may respond with as PDU establishment accept message.

[0078] At 340, the base station 105-b may transmit data service traffic to the UE 115-b. The data service traffic may include an encrypted application identifier (e.g., corresponding to the application 220-a).

[0079] At 345, the UE 115-b (e.g., the modem 215-a of the UE 115-b) may route the data service traffic to the application 220-a based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application. For example, the modem 215-a may establish a trusted environment to receive the decryption key from application 220-a, and decrypt the encrypted application identifier within the data service traffic using the received decryption key. The modem 215-a may additionally match the decrypted application identifier to the application identifier of the application 220-a. Thus, the UE 115-b may route the data service traffic to the application 220-a based on identifying a successful match. Beneficially, the techniques described herein may enhance security for an application and a network slicing instance to reduce the likelihood of a cheating application being able to connect to the network slicing instance to which the cheating application is not authorized to connect.

[0080] **FIG. 4** shows a block diagram 400 of a device 405 that supports encrypting application identifiers in accordance with aspects of the present disclosure. The device 405 may be an example of aspects of a UE 115 as described herein. The device 405 may include a receiver 410, a communications manager 415, and a transmitter 420. The device 405 may also include a processor. Each of these components may be in communication with one another (e.g., via one or more buses).

[0081] The receiver 410 may receive information such as packets, user data, or control information associated with various information channels (e.g., control channels, data channels, and information related to encrypting application identifiers, etc.). Information may be passed on to other components of the device 405. The receiver 410 may be an example of aspects of the transceiver 720 described with reference to FIG. 7. The receiver 410 may utilize a single antenna or a set of antennas.

[0082] The communications manager 415 may receive a traffic descriptor that includes an encrypted application identifier corresponding to an application, receive an application identifier of the application and a decryption key for the application identifier, transmit, to a base station, a data service request that requests data service for the application according to the received traffic descriptor, receive, from the base station, data service traffic for the data service that includes the encrypted application identifier, and route the data service traffic to the application based on decrypting the encrypted application identifier using the decryption

key to obtain the application identifier of the application. The communications manager 415 may be an example of aspects of the communications manager 710 described herein.

[0083] The communications manager 415, or its sub-components, may be implemented in hardware, code (e.g., software or firmware) executed by a processor, or any combination thereof. If implemented in code executed by a processor, the functions of the communications manager 415, or its sub-components may be executed by 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, or any combination thereof designed to perform the functions described in the present disclosure.

[0084] The communications manager 415, or its sub-components, may be physically located at various positions, including being distributed such that portions of functions are implemented at different physical locations by one or more physical components. In some examples, the communications manager 415, or its sub-components, may be a separate and distinct component in accordance with various aspects of the present disclosure. In some examples, the communications manager 415, or its sub-components, may be combined with one or more other hardware components, including but not limited to an input/output (I/O) component, a transceiver, a network server, another computing device, one or more other components described in the present disclosure, or a combination thereof in accordance with various aspects of the present disclosure.

[0085] The transmitter 420 may transmit signals generated by other components of the device 405. In some examples, the transmitter 420 may be collocated with a receiver 410 in a transceiver module. For example, the transmitter 420 may be an example of aspects of the transceiver 720 described with reference to FIG. 7. The transmitter 420 may utilize a single antenna or a set of antennas.

[0086] **FIG. 5** shows a block diagram 500 of a device 505 that supports encrypting application identifiers in accordance with aspects of the present disclosure. The device 505 may be an example of aspects of a device 405, or a UE 115 as described herein. The device 505 may include a receiver 510, a communications manager 515, and a transmitter 545. The device 505 may also include a processor. Each of these components may be in communication with one another (e.g., via one or more buses).

[0087] The receiver 510 may receive information such as packets, user data, or control information associated with various information channels (e.g., control channels, data channels, and information related to encrypting application identifiers, etc.). Information may be passed on to other components of the device 505. The receiver 510 may be an example of aspects of the transceiver 720 described with reference to FIG. 7. The receiver 510 may utilize a single antenna or a set of antennas.

[0088] The communications manager 515 may be an example of aspects of the communications manager 415 as described herein. The communications manager 515 may include a traffic descriptor receiver 520, an application identifier manager 525, a data service request manager 530, a data service traffic receiver 535, and a routing manager 540. The communications manager 515 may be an example of aspects of the communications manager 710 described herein.

[0089] The traffic descriptor receiver 520 may receive a traffic descriptor that includes an encrypted application identifier corresponding to an application.

[0090] The application identifier manager 525 may receive an application identifier of the application and a decryption key for the application identifier.

[0091] The data service request manager 530 may transmit, to a base station, a data service request that requests data service for the application according to the received traffic descriptor.

[0092] The data service traffic receiver 535 may receive, from the base station, data service traffic for the data service that includes the encrypted application identifier.

[0093] The routing manager 540 may route the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application.

[0094] The transmitter 545 may transmit signals generated by other components of the device 505. In some examples, the transmitter 545 may be collocated with a receiver 510 in a transceiver module. For example, the transmitter 545 may be an example of aspects of the transceiver 720 described with reference to FIG. 7. The transmitter 545 may utilize a single antenna or a set of antennas.

[0095] **FIG. 6** shows a block diagram 600 of a communications manager 605 that supports encrypting application identifiers in accordance with aspects of the present disclosure. The communications manager 605 may be an example of aspects of a communications manager 415, a communications manager 515, or a communications manager 710 described herein. The communications manager 605 may include a traffic descriptor receiver 610, an application identifier manager 615, a data service request manager 620, a data service traffic receiver 625, a routing manager 630, and a network slice manager 635. Each of these modules may communicate, directly or indirectly, with one another (e.g., via one or more buses).

[0096] The traffic descriptor receiver 610 may receive a traffic descriptor that includes an encrypted application identifier corresponding to an application. In some examples, the traffic descriptor receiver 610 may receive, from the base station, a set of traffic descriptors that includes the received traffic descriptor. Here, each of the set of traffic descriptors may include an encrypted application identifier corresponding to a unique application. In some cases, the traffic descriptor receiver 610 may receive the traffic descriptor that includes the encrypted application identifier corresponding to the application from a public land mobile network. In some examples, the traffic descriptor receiver 610 may receive a network slice selection policy indicating a first network slice from a set of available network slices associated with the application.

[0097] The application identifier manager 615 may receive an application identifier of the application and a decryption key for the application identifier. In some examples, the application identifier manager 615 may receive the application identifier that is an operating system application identifier. In some cases, the application identifier manager 615 may establish a connection with a trusted environment. Here, the application identifier manager 615 may receive the decryption key for the application identifier from the trusted environment. In some instances, the trusted environment is associated with a public land mobile network. In some examples, the application identifier manager 615 may transmit, to the application, a second request for the application identifier and the decryption key, where receiving the application identifier and the decryption key for the application identifier is based on transmitting the second request.

[0098] The data service request manager 620 may transmit, to a base station, a data service request that requests data service for the application according to the received traffic descriptor. In some examples, the data service request manager 620 may transmit the data service request according to the received traffic descriptor based on decrypting the application identifier within the received traffic descriptor using the decryption key. In some cases, the data service request manager 620 may receive a first request for the data service from the application.

[0099] The data service traffic receiver 625 may receive, from the base station, data service traffic for the data service that includes the encrypted application identifier.

[0100] The routing manager 630 may route the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application. In some examples, the routing manager 630 may match a decrypted application identifier to the application identifier of the application based on decrypting the encrypted application identifier, where routing the data service traffic to the application is based on matching the decrypted application identifier to the application identifier.

[0101] The network slice manager 635 may identify a first network slice from a set of available network slices based on the received traffic descriptor. In some examples, the network slice manager 635 may transmit a registration request requesting to register with the first network slice of the set of available network slices, where transmitting the data service request is based on transmitting the registration request.

[0102] **FIG. 7** shows a diagram of a system 700 including a device 705 that supports encrypting application identifiers in accordance with aspects of the present disclosure. The device 705 may be an example of or include the components of device 405, device 505, or a UE 115 as described herein. The device 705 may include components for bi-directional voice and data communications including components for transmitting and receiving communications, including a communications manager 710, an I/O controller 715, a transceiver 720, an antenna 725, memory 730, and a processor 740. These components may be in electronic communication via one or more buses (e.g., bus 745).

[0103] The communications manager 710 may receive a traffic descriptor that includes an encrypted application identifier corresponding to an application, receive an application

identifier of the application and a decryption key for the application identifier, transmit, to a base station, a data service request that requests data service for the application according to the received traffic descriptor, receive, from the base station, data service traffic for the data service that includes the encrypted application identifier, and route the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application.

[0104] The I/O controller 715 may manage input and output signals for the device 705. The I/O controller 715 may also manage peripherals not integrated into the device 705. In some cases, the I/O controller 715 may represent a physical connection or port to an external peripheral. In some cases, the I/O controller 715 may utilize an operating system such as iOS®, ANDROID®, MS-DOS®, MS-WINDOWS®, OS/2®, UNIX®, LINUX®, or another known operating system. In other cases, the I/O controller 715 may represent or interact with a modem, a keyboard, a mouse, a touchscreen, or a similar device. In some cases, the I/O controller 715 may be implemented as part of a processor. In some cases, a user may interact with the device 705 via the I/O controller 715 or via hardware components controlled by the I/O controller 715.

[0105] The transceiver 720 may communicate bi-directionally, via one or more antennas, wired, or wireless links as described above. For example, the transceiver 720 may represent a wireless transceiver and may communicate bi-directionally with another wireless transceiver. The transceiver 720 may also include a modem to modulate the packets and provide the modulated packets to the antennas for transmission, and to demodulate packets received from the antennas.

[0106] In some cases, the wireless device may include a single antenna 725. However, in some cases the device may have more than one antenna 725, which may be capable of concurrently transmitting or receiving multiple wireless transmissions.

[0107] The memory 730 may include random-access memory (RAM) and read-only memory (ROM). The memory 730 may store computer-readable, computer-executable code 735 including instructions that, when executed, cause the processor to perform various functions described herein. In some cases, the memory 730 may contain, among other things, a basic input/output system (BIOS) which may control basic hardware or software operation such as the interaction with peripheral components or devices.

[0108] The processor 740 may include an intelligent hardware device, (e.g., a general-purpose processor, a DSP, a CPU, a microcontroller, an ASIC, an FPGA, a programmable logic device, a discrete gate or transistor logic component, a discrete hardware component, or any combination thereof). In some cases, the processor 740 may be configured to operate a memory array using a memory controller. In other cases, a memory controller may be integrated into the processor 740. The processor 740 may be configured to execute computer-readable instructions stored in a memory (e.g., the memory 730) to cause the device 705 to perform various functions (e.g., functions or tasks supporting encrypting application identifiers).

[0109] The code 735 may include instructions to implement aspects of the present disclosure, including instructions to support wireless communications. The code 735 may be stored in a non-transitory computer-readable medium such as system memory or other type of memory. In some cases, the code 735 may not be directly executable by the processor 740 but may cause a computer (e.g., when compiled and executed) to perform functions described herein.

[0110] **FIG. 8** shows a flowchart illustrating a method 800 that supports encrypting application identifiers in accordance with aspects of the present disclosure. The operations of method 800 may be implemented by a UE 115 or its components as described herein. For example, the operations of method 800 may be performed by a communications manager as described with reference to FIGs. 4 through 7. In some examples, a UE may execute a set of instructions to control the functional elements of the UE to perform the functions described below. Additionally or alternatively, a UE may perform aspects of the functions described below using special-purpose hardware.

[0111] At 805, the UE may receive a traffic descriptor that includes an encrypted application identifier corresponding to an application. The operations of 805 may be performed according to the methods described herein. In some examples, aspects of the operations of 805 may be performed by a traffic descriptor receiver as described with reference to FIGs. 4 through 7.

[0112] At 810, the UE may receive an application identifier of the application and a decryption key for the application identifier. The operations of 810 may be performed according to the methods described herein. In some examples, aspects of the operations of

810 may be performed by an application identifier manager as described with reference to FIGs. 4 through 7.

[0113] At 815, the UE may transmit, to a base station, a data service request that requests data service for the application according to the received traffic descriptor. The operations of 815 may be performed according to the methods described herein. In some examples, aspects of the operations of 815 may be performed by a data service request manager as described with reference to FIGs. 4 through 7.

[0114] At 820, the UE may receive, from the base station, data service traffic for the data service that includes the encrypted application identifier. The operations of 820 may be performed according to the methods described herein. In some examples, aspects of the operations of 820 may be performed by a data service traffic receiver as described with reference to FIGs. 4 through 7.

[0115] At 825, the UE may route the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application. The operations of 825 may be performed according to the methods described herein. In some examples, aspects of the operations of 825 may be performed by a routing manager as described with reference to FIGs. 4 through 7.

[0116] **FIG. 9** shows a flowchart illustrating a method 900 that supports encrypting application identifiers in accordance with aspects of the present disclosure. The operations of method 900 may be implemented by a UE 115 or its components as described herein. For example, the operations of method 900 may be performed by a communications manager as described with reference to FIGs. 4 through 7. In some examples, a UE may execute a set of instructions to control the functional elements of the UE to perform the functions described below. Additionally or alternatively, a UE may perform aspects of the functions described below using special-purpose hardware.

[0117] At 905, the UE may receive a traffic descriptor that includes an encrypted application identifier corresponding to an application. The operations of 905 may be performed according to the methods described herein. In some examples, aspects of the operations of 905 may be performed by a traffic descriptor receiver as described with reference to FIGs. 4 through 7.

[0118] At 910, the UE may receive an application identifier of the application and a decryption key for the application identifier. The operations of 910 may be performed according to the methods described herein. In some examples, aspects of the operations of 910 may be performed by an application identifier manager as described with reference to FIGs. 4 through 7.

[0119] At 915, the UE may transmit, to a base station, a data service request according to the received traffic descriptor based on decrypting the application identifier within the received traffic descriptor using the decryption key, where the data service request requests data service for the application according to the received traffic descriptor. The operations of 915 may be performed according to the methods described herein. In some examples, aspects of the operations of 915 may be performed by a data service request manager as described with reference to FIGs. 4 through 7.

[0120] At 920, the UE may receive, from the base station, data service traffic for the data service that includes the encrypted application identifier. The operations of 920 may be performed according to the methods described herein. In some examples, aspects of the operations of 920 may be performed by a data service traffic receiver as described with reference to FIGs. 4 through 7.

[0121] At 925, the UE may route the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application. The operations of 925 may be performed according to the methods described herein. In some examples, aspects of the operations of 925 may be performed by a routing manager as described with reference to FIGs. 4 through 7.

[0122] **FIG. 10** shows a flowchart illustrating a method 1000 that supports encrypting application identifiers in accordance with aspects of the present disclosure. The operations of method 1000 may be implemented by a UE 115 or its components as described herein. For example, the operations of method 1000 may be performed by a communications manager as described with reference to FIGs. 4 through 7. In some examples, a UE may execute a set of instructions to control the functional elements of the UE to perform the functions described below. Additionally or alternatively, a UE may perform aspects of the functions described below using special-purpose hardware.

[0123] At 1005, the UE may receive a traffic descriptor that includes an encrypted application identifier corresponding to an application, where the traffic descriptor indicates a network slice selection policy indicating a first network slice from a set of available network slices associated with the application. The operations of 1005 may be performed according to the methods described herein. In some examples, aspects of the operations of 1005 may be performed by a traffic descriptor receiver as described with reference to FIGs. 4 through 7.

[0124] At 1010, the UE may receive an application identifier of the application and a decryption key for the application identifier. The operations of 1010 may be performed according to the methods described herein. In some examples, aspects of the operations of 1010 may be performed by an application identifier manager as described with reference to FIGs. 4 through 7.

[0125] At 1015, the UE may transmit, to a base station, a data service request that requests data service for the application according to the received traffic descriptor. The operations of 1015 may be performed according to the methods described herein. In some examples, aspects of the operations of 1015 may be performed by a data service request manager as described with reference to FIGs. 4 through 7.

[0126] At 1020, the UE may receive, from the base station, data service traffic for the data service that includes the encrypted application identifier. The operations of 1020 may be performed according to the methods described herein. In some examples, aspects of the operations of 1020 may be performed by a data service traffic receiver as described with reference to FIGs. 4 through 7.

[0127] At 1025, the UE may route the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application. The operations of 1025 may be performed according to the methods described herein. In some examples, aspects of the operations of 1025 may be performed by a routing manager as described with reference to FIGs. 4 through 7.

[0128] It should be noted that the methods described herein describe possible implementations, and that the operations and the steps may be rearranged or otherwise modified and that other implementations are possible. Further, aspects from two or more of the methods may be combined.

[0129] Although aspects of an LTE, LTE-A, LTE-A Pro, or NR system may be described for purposes of example, and LTE, LTE-A, LTE-A Pro, or NR terminology may be used in much of the description, the techniques described herein are applicable beyond LTE, LTE-A, LTE-A Pro, or NR networks. For example, the described techniques may be applicable to various other wireless communications systems such as Ultra Mobile Broadband (UMB), Institute of Electrical and Electronics Engineers (IEEE) 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20, Flash-OFDM, as well as other systems and radio technologies not explicitly mentioned herein.

[0130] Information and signals described herein may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[0131] The various illustrative blocks and components described in connection with the disclosure herein may be implemented or performed with a general-purpose processor, a DSP, an ASIC, a CPU, an FPGA or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general-purpose processor may be a microprocessor, but in the alternative, the processor may be any processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices (e.g., a combination of a DSP and a microprocessor, multiple microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration).

[0132] The functions described herein may be implemented in hardware, software executed by a processor, firmware, or any combination thereof. If implemented in software executed by a processor, the functions may be stored on or transmitted over as one or more instructions or code on a computer-readable medium. Other examples and implementations are within the scope of the disclosure and appended claims. For example, due to the nature of software, functions described herein may be implemented using software executed by a processor, hardware, firmware, hardwiring, or combinations of any of these. Features

implementing functions may also be physically located at various positions, including being distributed such that portions of functions are implemented at different physical locations.

[0133] Computer-readable media includes both non-transitory computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A non-transitory storage medium may be any available medium that may be accessed by a general-purpose or special purpose computer. By way of example, and not limitation, non-transitory computer-readable media may include RAM, ROM, electrically erasable programmable ROM (EEPROM), flash memory, compact disk (CD) ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other non-transitory medium that may be used to carry or store desired program code means in the form of instructions or data structures and that may be accessed by a general-purpose or special-purpose computer, or a general-purpose or special-purpose processor. Also, any connection is properly termed a computer-readable medium. For example, if the software is transmitted from a website, server, or other remote source using a coaxial cable, fiber optic cable, twisted pair, digital subscriber line (DSL), or wireless technologies such as infrared, radio, and microwave, then the coaxial cable, fiber optic cable, twisted pair, DSL, or wireless technologies such as infrared, radio, and microwave are included in the definition of computer-readable medium. Disk and disc, as used herein, include CD, laser disc, optical disc, digital versatile disc (DVD), floppy disk and Blu-ray disc where disks usually reproduce data magnetically, while discs reproduce data optically with lasers. Combinations of the above are also included within the scope of computer-readable media.

[0134] As used herein, including in the claims, "or" as used in a list of items (e.g., a list of items prefaced by a phrase such as "at least one of" or "one or more of") indicates an inclusive list such that, for example, a list of at least one of A, B, or C means A or B or C or AB or AC or BC or ABC (i.e., A and B and C). Also, as used herein, the phrase "based on" shall not be construed as a reference to a closed set of conditions. For example, an example step that is described as "based on condition A" may be based on both a condition A and a condition B without departing from the scope of the present disclosure. In other words, as used herein, the phrase "based on" shall be construed in the same manner as the phrase "based at least in part on."

[0135] In the appended figures, similar components or features may have the same reference label. Further, various components of the same type may be distinguished by following the reference label by a dash and a second label that distinguishes among the similar components. If just the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label, or other subsequent reference label.

[0136] The description set forth herein, in connection with the appended drawings, describes example configurations and does not represent all the examples that may be implemented or that are within the scope of the claims. The term "example" used herein means "serving as an example, instance, or illustration," and not "preferred" or "advantageous over other examples." The detailed description includes specific details for the purpose of providing an understanding of the described techniques. These techniques, however, may be practiced without these specific details. In some instances, known structures and devices are shown in block diagram form in order to avoid obscuring the concepts of the described examples.

[0137] The description herein is provided to enable a person having ordinary skill in the art to make or use the disclosure. Various modifications to the disclosure will be apparent to a person having ordinary skill in the art, and the generic principles defined herein may be applied to other variations without departing from the scope of the disclosure. Thus, the disclosure is not limited to the examples and designs described herein, but is to be accorded the broadest scope consistent with the principles and novel features disclosed herein.

CLAIMS

What is claimed is:

1. A method for wireless communication at a user equipment (UE), comprising:

receiving a traffic descriptor that comprises an encrypted application identifier corresponding to an application;

receiving an application identifier of the application and a decryption key for the application identifier;

transmitting, to a base station, a data service request that requests data service for the application according to the received traffic descriptor;

receiving, from the base station, data service traffic for the data service that comprises the encrypted application identifier; and

routing the data service traffic to the application based at least in part on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application.

2. The method of claim 1, wherein transmitting the data service request comprises:

transmitting the data service request according to the received traffic descriptor based at least in part on decrypting the application identifier within the received traffic descriptor using the decryption key.

3. The method of claim 1, wherein receiving the traffic descriptor comprises:

receiving a network slice selection policy indicating a first network slice from a plurality of available network slices associated with the application.

4. The method of claim 1, wherein receiving the application identifier comprises:

receiving the application identifier that is an operating system application identifier.

5. The method of claim 1, further comprising:

establishing a connection with a trusted environment; and

receiving the decryption key for the application identifier from the trusted environment.

6. The method of claim 5, wherein the trusted environment is associated with a public land mobile network.

7. The method of claim 1, further comprising:

receiving the traffic descriptor that comprises the encrypted application identifier corresponding to the application from a public land mobile network.

8. The method of claim 1, further comprising:

receiving, from the base station, a plurality of traffic descriptors that includes the received traffic descriptor.

9. The method of claim 8, wherein each of the plurality of traffic descriptors comprise an encrypted application identifier corresponding to a unique application.

10. The method of claim 1, further comprising:

identifying a first network slice from a plurality of available network slices based at least in part on the received traffic descriptor; and

transmitting a registration request requesting to register with the first network slice of the plurality of available network slices, wherein transmitting the data service request is based at least in part on transmitting the registration request.

11. The method of claim 1, further comprising:

receiving a first request for the data service from the application; and

transmitting, to the application, a second request for the application identifier and the decryption key, wherein receiving the application identifier and the decryption key for the application identifier is based at least in part on transmitting the second request.

12. The method of claim 1, further comprising:

matching a decrypted application identifier to the application identifier of the application based at least in part on decrypting the encrypted application identifier, wherein

routing the data service traffic to the application is based at least in part on matching the decrypted application identifier to the application identifier.

13. An apparatus for wireless communication at a user equipment (UE), comprising:

a processor,

memory coupled with the processor; and

instructions stored in the memory and executable by the processor to cause the apparatus to:

receive a traffic descriptor that comprises an encrypted application identifier corresponding to an application;

receive an application identifier of the application and a decryption key for the application identifier;

transmit, to a base station, a data service request that requests data service for the application according to the received traffic descriptor;

receive, from the base station, data service traffic for the data service that comprises the encrypted application identifier; and

route the data service traffic to the application based at least in part on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application.

14. The apparatus of claim 13, further comprising a transceiver, wherein the instructions to transmit the data service request are executable by the processor to cause the apparatus to:

transmit, via the transceiver, the data service request according to the received traffic descriptor based at least in part on decrypting the application identifier within the received traffic descriptor using the decryption key.

15. The apparatus of claim 13, wherein the instructions to receive the traffic descriptor are executable by the processor to cause the apparatus to:

receive a network slice selection policy indicating a first network slice from a plurality of available network slices associated with the application.

16. The apparatus of claim 13, wherein the instructions to receive the application identifier are executable by the processor to cause the apparatus to:

receive the application identifier that is an operating system application identifier.

17. The apparatus of claim 13, wherein the instructions are further executable by the processor to cause the apparatus to:

establish a connection with a trusted environment; and

receive the decryption key for the application identifier from the trusted environment.

18. The apparatus of claim 17, wherein the trusted environment is associated with a public land mobile network.

19. The apparatus of claim 13, wherein the instructions are further executable by the processor to cause the apparatus to:

receive the traffic descriptor that comprises the encrypted application identifier corresponding to the application from a public land mobile network.

20. The apparatus of claim 13, wherein the instructions are further executable by the processor to cause the apparatus to:

receive, from the base station, a plurality of traffic descriptors that includes the received traffic descriptor.

21. The apparatus of claim 20, wherein each of the plurality of traffic descriptors comprise an encrypted application identifier corresponding to a unique application.

22. The apparatus of claim 13, wherein the instructions are further executable by the processor to cause the apparatus to:

identify a first network slice from a plurality of available network slices based at least in part on the received traffic descriptor; and

transmit a registration request requesting to register with the first network slice of the plurality of available network slices, wherein transmitting the data service request is based at least in part on transmitting the registration request.

23. The apparatus of claim 13, wherein the instructions are further executable by the processor to cause the apparatus to:

receive a first request for the data service from the application; and

transmit, to the application, a second request for the application identifier and the decryption key, wherein receiving the application identifier and the decryption key for the application identifier is based at least in part on transmitting the second request.

24. The apparatus of claim 13, wherein the instructions are further executable by the processor to cause the apparatus to:

match a decrypted application identifier to the application identifier of the application based at least in part on decrypting the encrypted application identifier, wherein routing the data service traffic to the application is based at least in part on matching the decrypted application identifier to the application identifier.

25. An apparatus for wireless communication at a user equipment (UE), comprising:

means for receiving a traffic descriptor that comprises an encrypted application identifier corresponding to an application;

means for receiving an application identifier of the application and a decryption key for the application identifier;

means for transmitting, to a base station, a data service request that requests data service for the application according to the received traffic descriptor;

means for receiving, from the base station, data service traffic for the data service that comprises the encrypted application identifier; and

means for routing the data service traffic to the application based at least in part on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application.

26. The apparatus of claim 25, wherein the means for transmitting the data service request comprises:

means for transmitting the data service request according to the received traffic descriptor based at least in part on decrypting the application identifier within the received traffic descriptor using the decryption key.

27. The apparatus of claim 25, wherein the means for receiving the traffic descriptor comprises:

means for receiving a network slice selection policy indicating a first network slice from a plurality of available network slices associated with the application.

28. The apparatus of claim 25, wherein the means for receiving the application identifier comprises:

means for receiving the application identifier that is an operating system application identifier.

29. The apparatus of claim 25, further comprising:

means for establishing a connection with a trusted environment; and

means for receiving the decryption key for the application identifier from the trusted environment.

30. The apparatus of claim 29, wherein the trusted environment is associated with a public land mobile network.

31. The apparatus of claim 25, further comprising:

means for receiving the traffic descriptor that comprises the encrypted application identifier corresponding to the application from a public land mobile network.

32. The apparatus of claim 25, further comprising:

means for receiving, from the base station, a plurality of traffic descriptors that includes the received traffic descriptor.

33. The apparatus of claim 32, wherein each of the plurality of traffic descriptors comprise an encrypted application identifier corresponding to a unique application.

34. The apparatus of claim 25, further comprising:

means for identifying a first network slice from a plurality of available network slices based at least in part on the received traffic descriptor; and

means for transmitting a registration request requesting to register with the first network slice of the plurality of available network slices, wherein transmitting the data service request is based at least in part on transmitting the registration request.

35. The apparatus of claim 25, further comprising:

means for receiving a first request for the data service from the application; and

means for transmitting, to the application, a second request for the application identifier and the decryption key, wherein receiving the application identifier and the decryption key for the application identifier is based at least in part on transmitting the second request.

36. The apparatus of claim 25, further comprising:

means for matching a decrypted application identifier to the application identifier of the application based at least in part on decrypting the encrypted application identifier, wherein routing the data service traffic to the application is based at least in part on matching the decrypted application identifier to the application identifier.

37. A non-transitory computer-readable medium storing code for wireless communication at a user equipment (UE), the code comprising instructions executable by a processor to:

receive a traffic descriptor that comprises an encrypted application identifier corresponding to an application;

receive an application identifier of the application and a decryption key for the application identifier;

transmit, to a base station, a data service request that requests data service for the application according to the received traffic descriptor;

receive, from the base station, data service traffic for the data service that comprises the encrypted application identifier; and

route the data service traffic to the application based at least in part on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application.

38. The non-transitory computer-readable medium of claim 37, wherein the instructions to transmit the data service request are executable to:

transmit the data service request according to the received traffic descriptor based at least in part on decrypting the application identifier within the received traffic descriptor using the decryption key.

39. The non-transitory computer-readable medium of claim 37, wherein the instructions to receive the traffic descriptor are executable to:

receive a network slice selection policy indicating a first network slice from a plurality of available network slices associated with the application.

40. The non-transitory computer-readable medium of claim 37, wherein the instructions to receive the application identifier are executable to:

receive the application identifier that is an operating system application identifier.

41. The non-transitory computer-readable medium of claim 37, wherein the instructions are further executable to:

establish a connection with a trusted environment; and

receive the decryption key for the application identifier from the trusted environment.

42. The non-transitory computer-readable medium of claim 41, wherein the trusted environment is associated with a public land mobile network.

43. The non-transitory computer-readable medium of claim 37, wherein the instructions are further executable to:

receive the traffic descriptor that comprises the encrypted application identifier corresponding to the application from a public land mobile network.

44. The non-transitory computer-readable medium of claim 37, wherein the instructions are further executable to:

receive, from the base station, a plurality of traffic descriptors that includes the received traffic descriptor.

45. The non-transitory computer-readable medium of claim 44, wherein each of the plurality of traffic descriptors comprise an encrypted application identifier corresponding to a unique application.

46. The non-transitory computer-readable medium of claim 37, wherein the instructions are further executable to:

identify a first network slice from a plurality of available network slices based at least in part on the received traffic descriptor; and

transmit a registration request requesting to register with the first network slice of the plurality of available network slices, wherein transmitting the data service request is based at least in part on transmitting the registration request.

47. The non-transitory computer-readable medium of claim 37, wherein the instructions are further executable to:

receive a first request for the data service from the application; and

transmit, to the application, a second request for the application identifier and the decryption key, wherein receiving the application identifier and the decryption key for the application identifier is based at least in part on transmitting the second request.

48. The non-transitory computer-readable medium of claim 37, wherein the instructions are further executable to:

match a decrypted application identifier to the application identifier of the application based at least in part on decrypting the encrypted application identifier, wherein routing the data service traffic to the application is based at least in part on matching the decrypted application identifier to the application identifier.

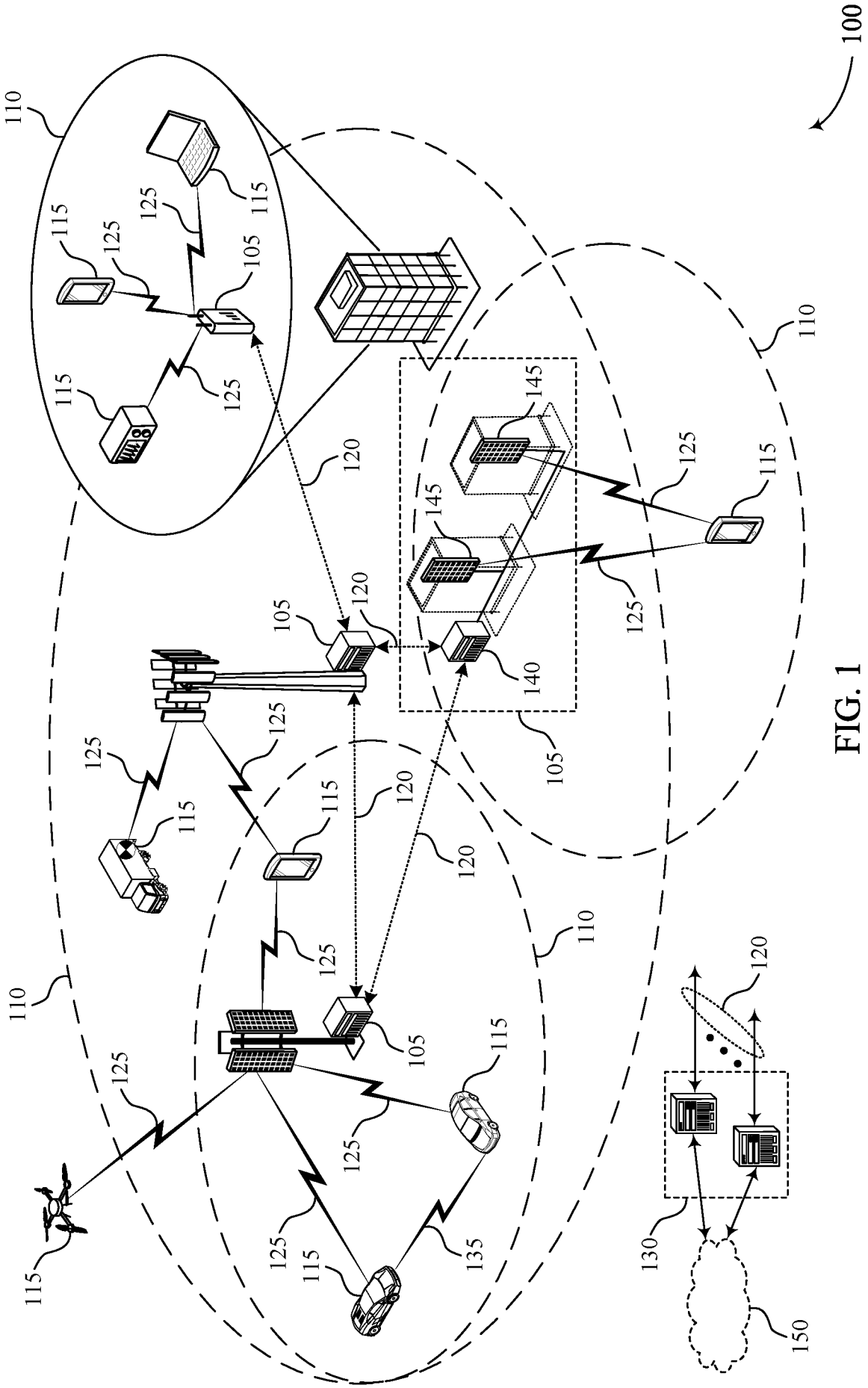

FIG. 1

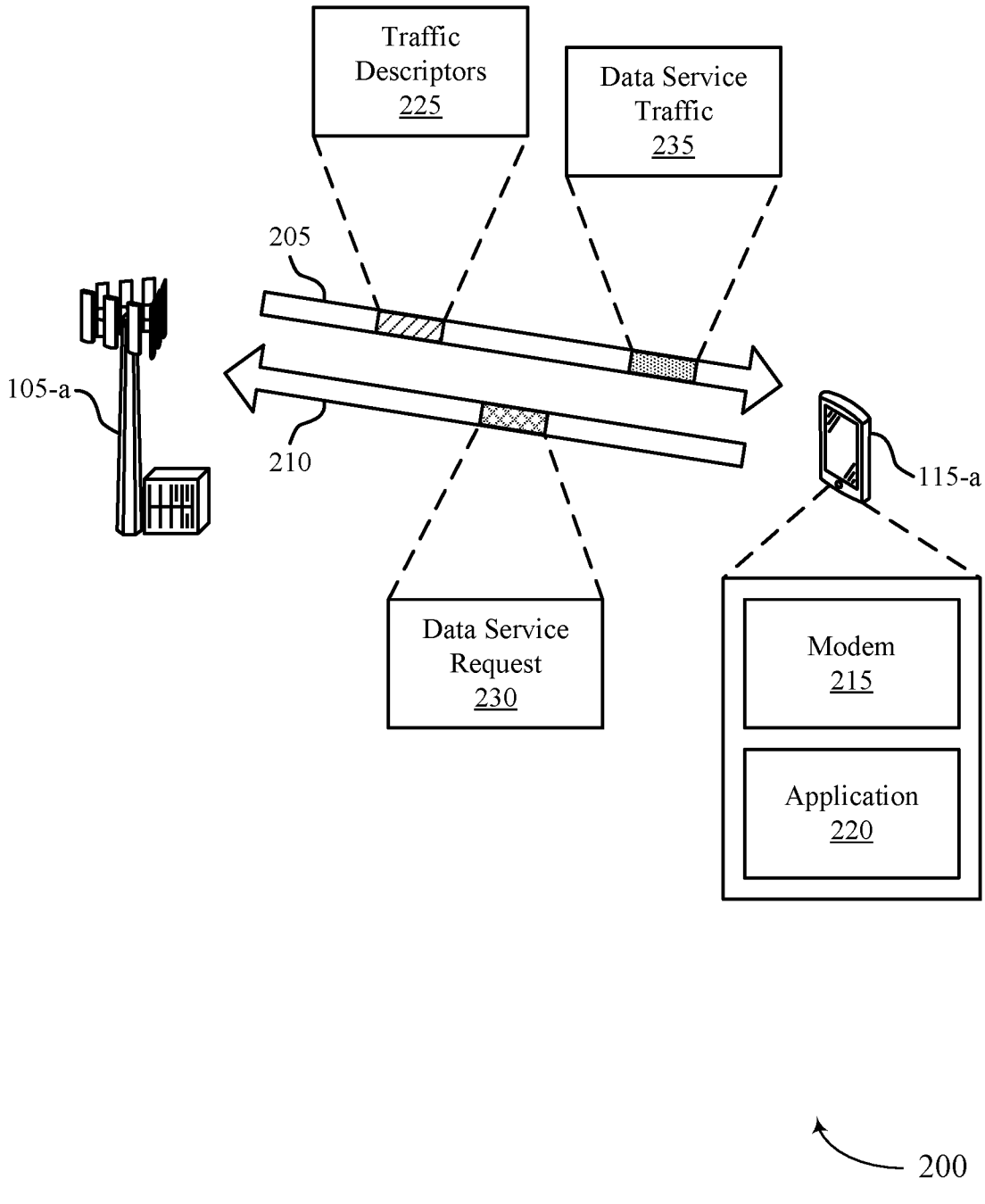
Traffic Descriptors 225
Data Service Traffic 235
205
105-a
210
115-a
Data Service Request 230
Modem 215
Application 220
200

FIG. 2

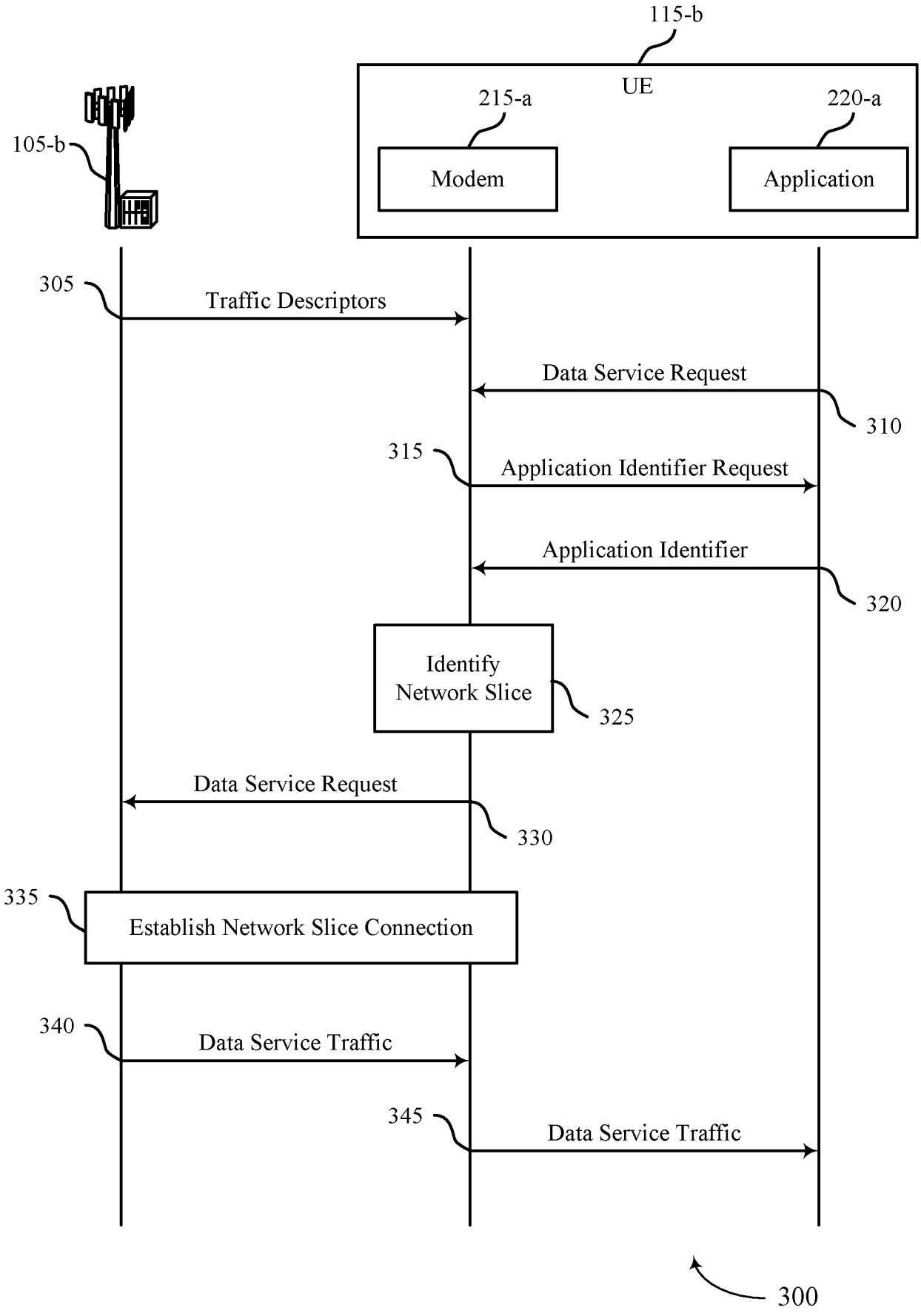
115-b
UE
215-a
220-a
105-b
Modem
Application
305
Traffic Descriptors
Data Service Request
310
315
Application Identifier Request
Application Identifier
320
Identify
Network Slice
325
Data Service Request
330
335
Establish Network Slice Connection
340
Data Service Traffic
345
Data Service Traffic
300

FIG. 3

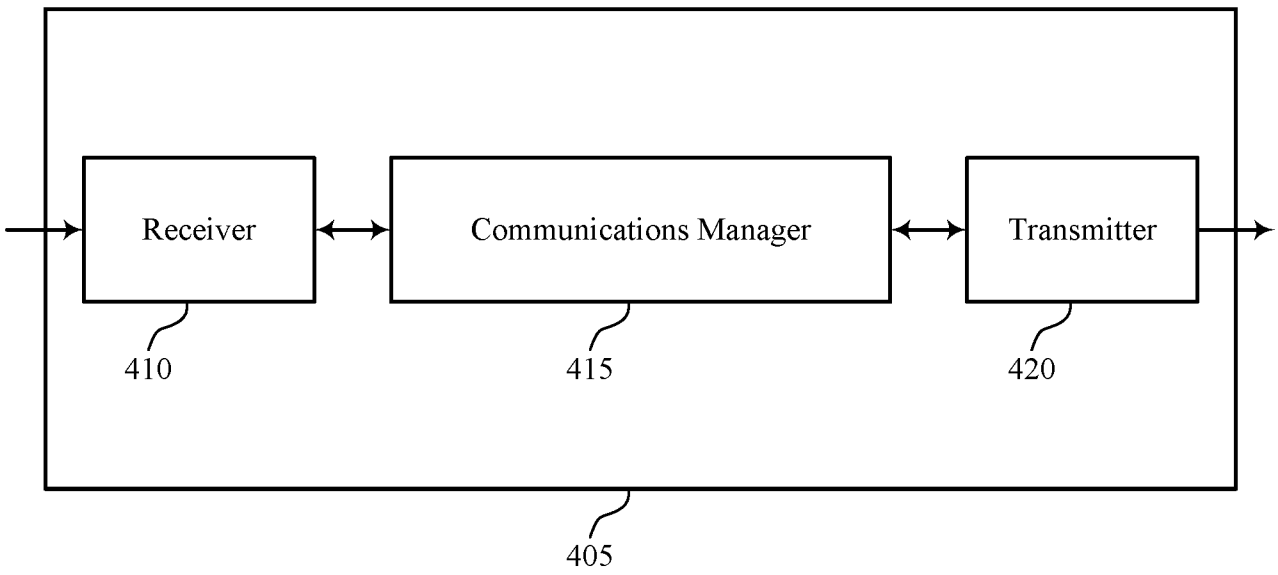
Receiver
Communications Manager
Transmitter
410
415
420
405
400

FIG. 4

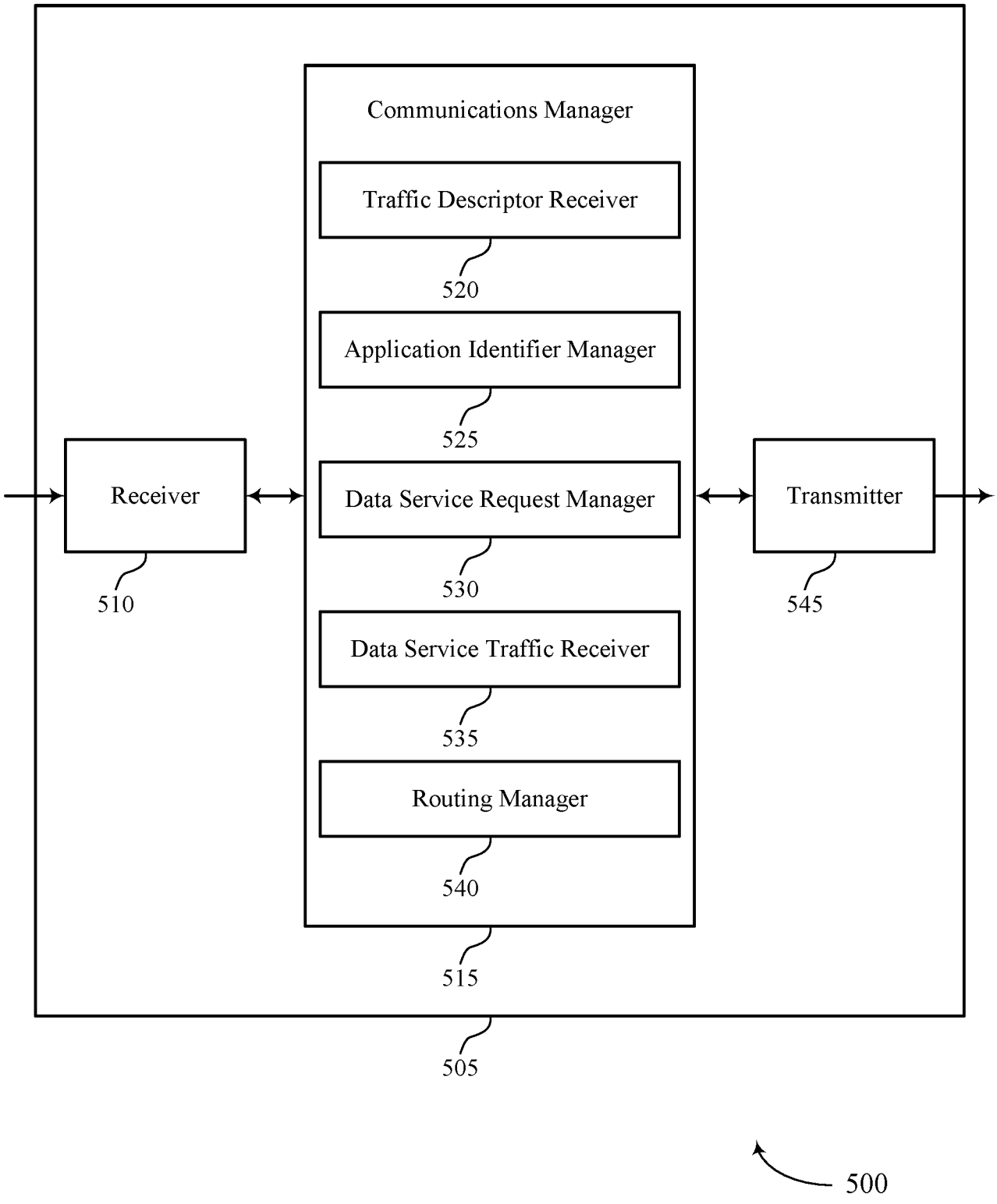
Communications Manager
Traffic Descriptor Receiver
520
Application Identifier Manager
525
Receiver
Data Service Request Manager
Transmitter
510
530
545
Data Service Traffic Receiver
535
Routing Manager
540
515
505
500

FIG. 5

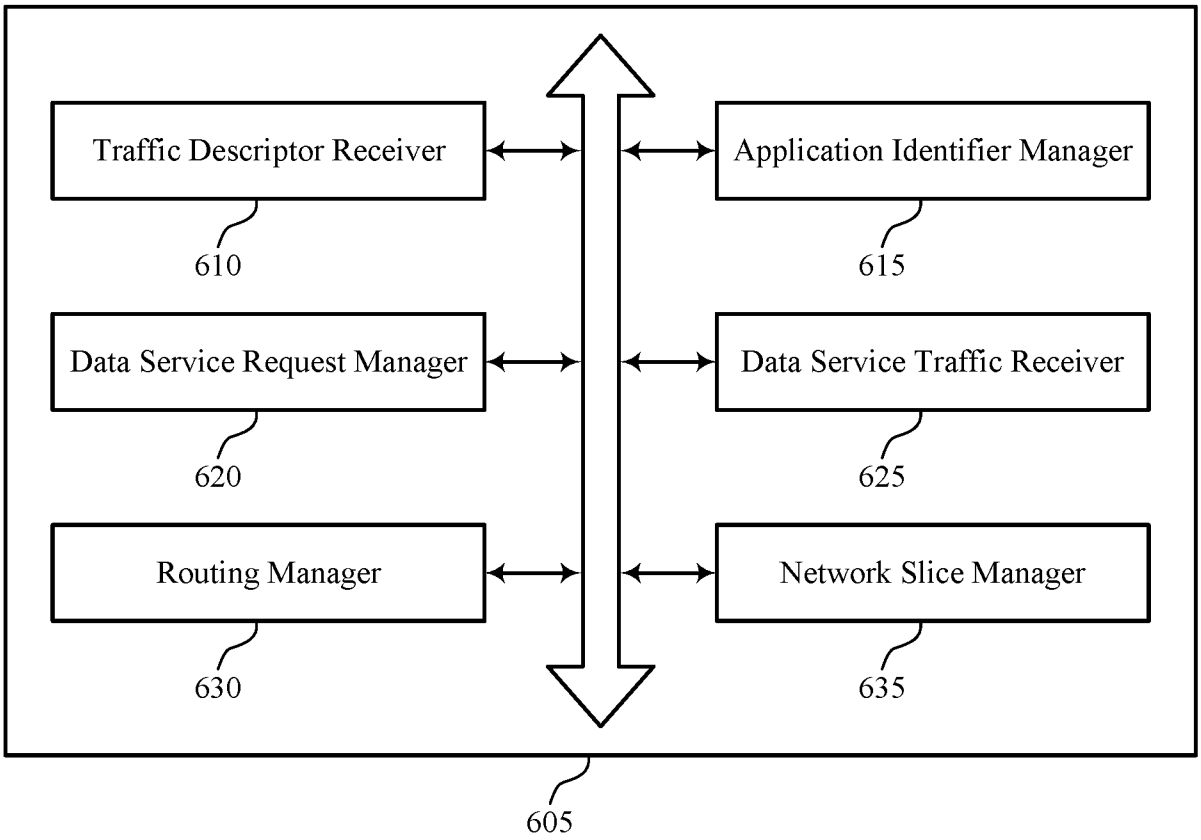
Traffic Descriptor Receiver
610
Application Identifier Manager
615
Data Service Request Manager
620
Data Service Traffic Receiver
625
Routing Manager
630
Network Slice Manager
635
605
600

FIG. 6

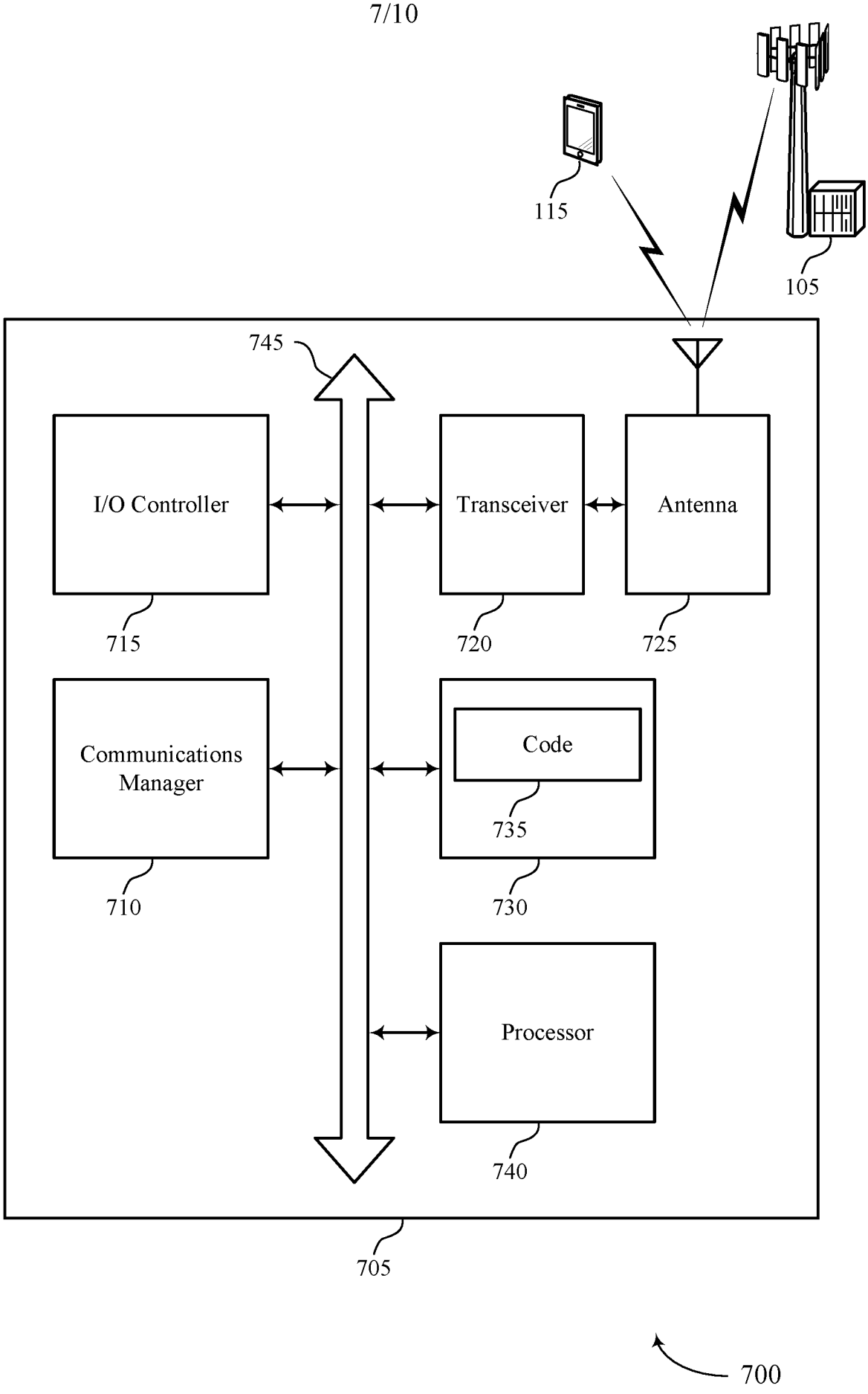
115
105
745
I/O Controller
Transceiver
Antenna
715
720
725
Communications Manager
Code
735
710
730
Processor
740
705
700

FIG. 7

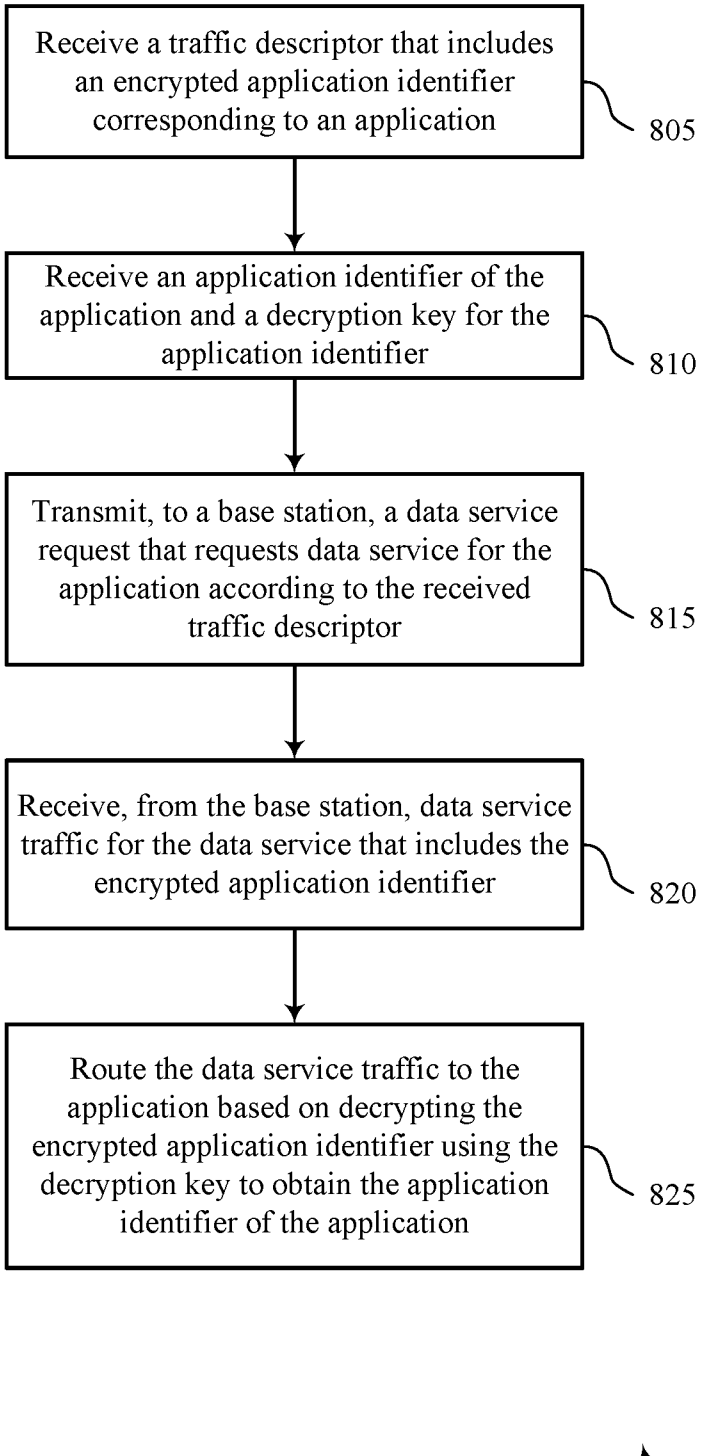
Receive a traffic descriptor that includes an encrypted application identifier corresponding to an application
805
Receive an application identifier of the application and a decryption key for the application identifier
810
Transmit, to a base station, a data service request that requests data service for the application according to the received traffic descriptor
815
Receive, from the base station, data service traffic for the data service that includes the encrypted application identifier
820
Route the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application
825
800

FIG. 8

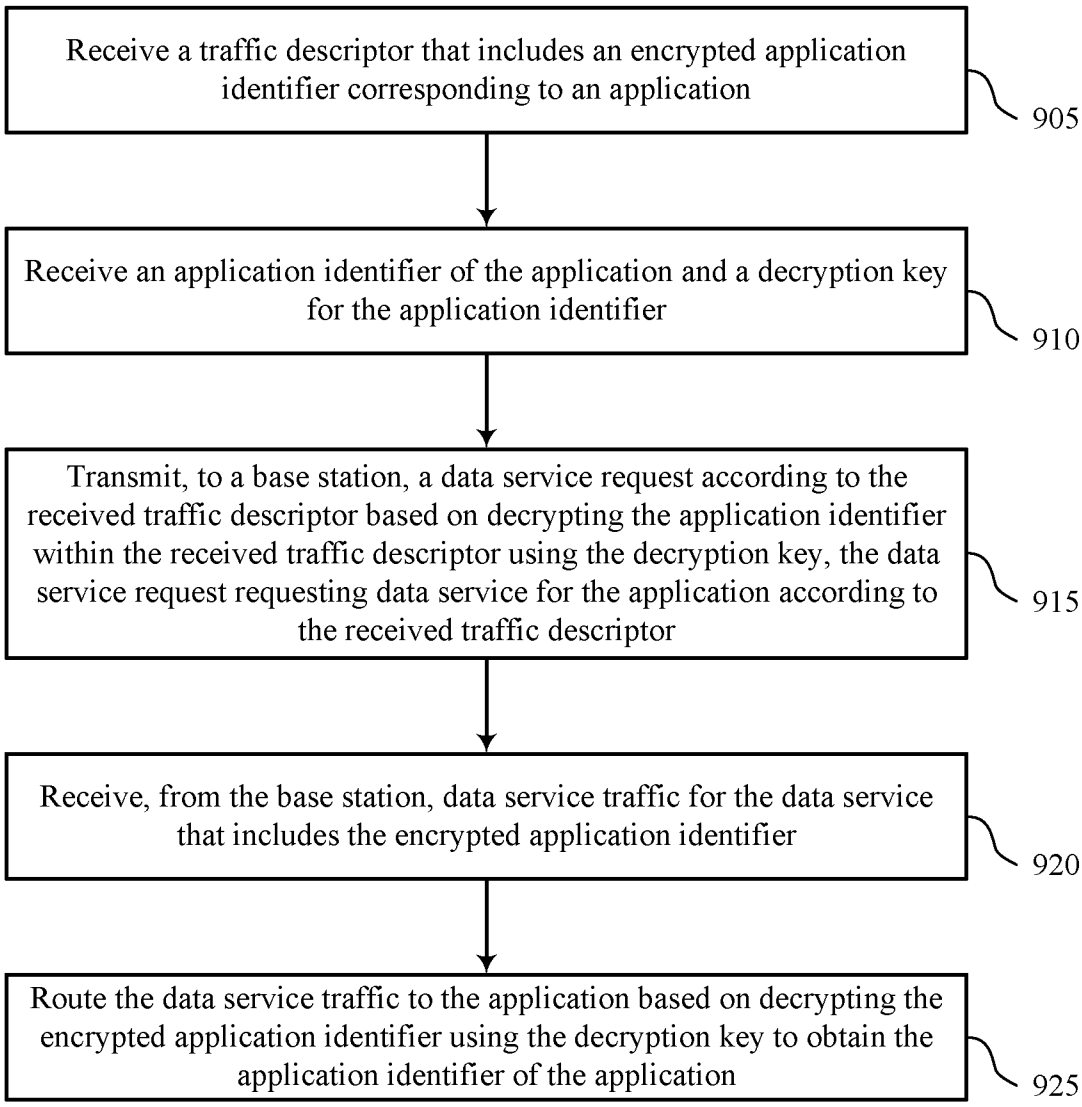
Receive a traffic descriptor that includes an encrypted application identifier corresponding to an application
905
Receive an application identifier of the application and a decryption key for the application identifier
910
Transmit, to a base station, a data service request according to the received traffic descriptor based on decrypting the application identifier within the received traffic descriptor using the decryption key, the data service request requesting data service for the application according to the received traffic descriptor
915
Receive, from the base station, data service traffic for the data service that includes the encrypted application identifier
920
Route the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application
925
900

FIG. 9

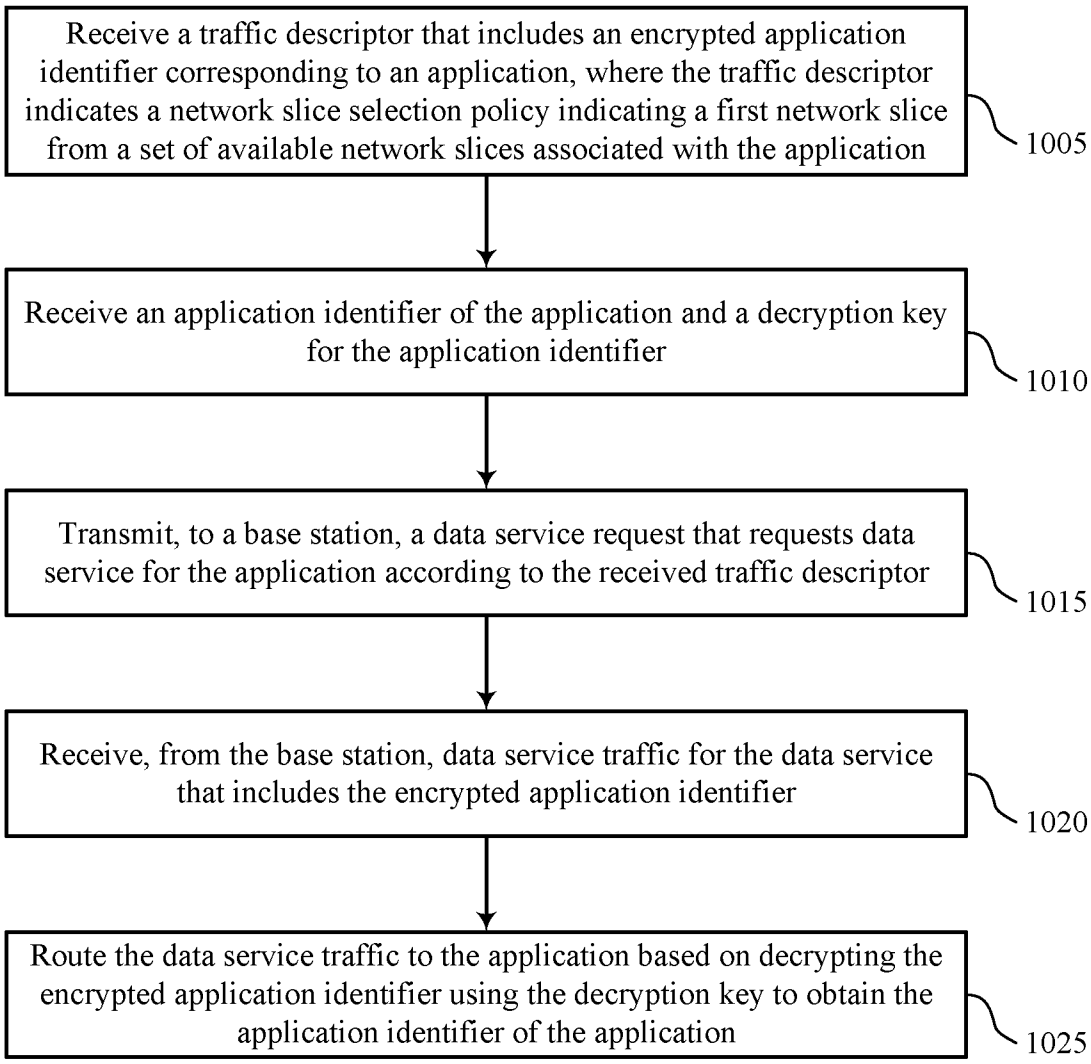
Receive a traffic descriptor that includes an encrypted application identifier corresponding to an application, where the traffic descriptor indicates a network slice selection policy indicating a first network slice from a set of available network slices associated with the application
1005
Receive an application identifier of the application and a decryption key for the application identifier
1010
Transmit, to a base station, a data service request that requests data service for the application according to the received traffic descriptor
1015
Receive, from the base station, data service traffic for the data service that includes the encrypted application identifier
1020
Route the data service traffic to the application based on decrypting the encrypted application identifier using the decryption key to obtain the application identifier of the application
1025
1000

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/091987

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24(2006.01)i; H04L 12/813(2013.01)i

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)

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)

CNPAT;CNKI;WPI;EPODOC;3GPP: user, UE, traffic, descriptor, encrypt, application, identifier, decryption, key, service, data, request, base station, BS, rout, network, slice, selection, policy, match

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2019386894 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 19 December 2019 (2019-12-19) abstract, claims 1-14	1-48
A	QUALCOMM INCORPORATED. "S2-185091: Clarifications and initial evaluation for Solution 7" *3GPP TSG-WG2 Meeting #127,* 01 June 2018 (2018-06-01), the whole document	1-48
A	US 2020146077 A1 (CONVIDA WIRELESS, LLC) 07 May 2020 (2020-05-07) the whole document	1-48
A	US 2015365227 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 17 December 2015 (2015-12-17) the whole document	1-48
A	WO 2019192672 A1 (LENOVO SINGAPORE PTE. LTD. et al.) 10 October 2019 (2019-10-10) the whole document	1-48

☐ 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	Date of mailing of the international search report
01 February 2021	**25 February 2021**
Name and mailing address of the ISA/CN **National Intellectual Property Administration, PRC** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer **YU, Xiaoxi** Telephone No. **86-(10)-53961578**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/091987

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2019386894 A1	19 December 2019	WO 2018157754 A1	07 September 2018
		JP 2020509666 A	26 March 2020
		KR 20190113985 A	08 October 2019
		CN 108512878 A	07 September 2018
		EP 3573311 A1	27 November 2019
		IN 201937035101 A	22 November 2019
US 2020146077 A1	07 May 2020	EP 3639612 A1	22 April 2020
		WO 2018232241 A1	20 December 2018
		CN 110771251 A	07 February 2020
US 2015365227 A1	17 December 2015	None	
WO 2019192672 A1	10 October 2019	None	