



- (51) International Patent Classification:
H04W 4/08 (2009.01) *G06N 20/00* (2019.01)

(21) International Application Number:
PCT/US2024/041425

(22) International Filing Date:
08 August 2024 (08.08.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/518,652 10 August 2023 (10.08.2023) US

(71) Applicant: **CONVIDA WIRELESS, LLC** [US/US]; 200 Bellevue Parkway, Suite 300, Wilmington, Delaware 19809 (US).

(72) Inventors: **LIU, Lu**; 200 Bellevue Parkway, Suite 300, Wilmington, Delaware 19809 (US). **SEED, Dale**; 200 Bellevue Parkway, Suite 300, Wilmington, Delaware 19809 (US). **LY, Quang**; 200 Bellevue Parkway, Suite 300, Wilmington, Delaware 19809 (US). **MLADIN, Catalina**; 200 Bellevue Parkway, Suite 300, Wilmington, Delaware 19809 (US).

(74) Agent: **LEICHT, Paul**; Baker & Hostetler LLP, 1735 Market Street, Suite 3300, Philadelphia, 19103 (US).

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

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, CV,

(54) Title: MECHANISMS FOR SERVICE LAYER SUPPORT OF FEDERATED LEARNING GROUPS

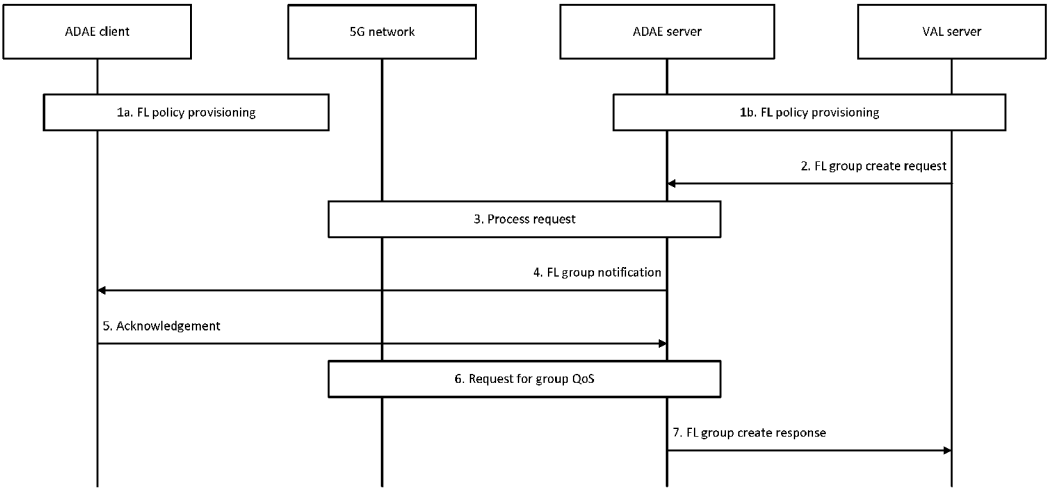


FIG. 10

(57) Abstract: Methods and systems for service layer support of federated learning groups are described herein. In one aspect, a method performed by an application enabler server, may include: receiving a first request for forming a federated learning (FL) group; sending one or more requests, to a core network, corresponding to assistance for FL operations; receiving a response to the one or more requests from the core network; and sending a response to the first request comprising one of a FL group identifier, a list of FL clients associated with the FL group, a validity time or schedule for the FL group, or a combination thereof.

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

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

MECHANISMS FOR SERVICE LAYER SUPPORT OF FEDERATED LEARNING GROUPS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims benefit of U.S. Provisional Application No. 63/518,652 titled “Mechanisms for Service Layer Support of Federated Learning Groups” filed August 10, 2023, the content of which are hereby incorporated by reference in their entirety for any and all purposes.

BACKGROUND

Application Layer Architecture

[0002] Applications are becoming increasingly more complex and various mechanisms have been designed to assist with quicker development of the applications. One such mechanism is the introduction of different functional layers within (or adjacent to) the application layer to separate functions that may be accessed via application programming interfaces or APIs. FIG. 1 shows an example of a generalized application layer architecture that separates application development into three distinct layers: application-specific, vertical application enabler, and service layers. At the bottom of the application stack is the service layer, which provides common services to all applications. The services may include location management, group management, configuration management, and security aspects for application development. Above the service layer is the vertical application enabler layer, which is a layer that manages services for a specific vertical application such as autonomous vehicles, drones, IoT, gaming, etc. At the top of the application stack is the application-specific layer which serves specific applications within a vertical application. This layer contains custom or business logic for a particular application and may be provided by various service providers in a vertical application domain. One goal of this three-layered approach is to abstract common services for all applications to the vertical application enabler and service layers to simplify application development for faster deployments of the applications.

[0003] The architecture shown in FIG. 1 is based on a client-server communication model. One or more client applications on devices may communicate with one or more server applications on application servers. Note that server applications may reside in one or more application servers. The client application and server application of each layer communicate with each other between the devices and application servers. The application-specific client

and server may communicate with client and server applications at any of the lower layers, respectively. For example, an application-specific client may communicate with the client application at either the vertical application enabler or service layers. A network between the client and server applications provides the medium for communication. The network may be a cellular network such as a mobile operator network or the network may be a broadband service provider network providing access to the internet for client and server applications.

[0004] It is worth noting that the architecture shown in FIG. 1 may also apply to publish-subscribe and subscription-notification communication models. It is also worth noting that for decentralized deployments in which devices communicate directly with other devices, server functionality may reside on a device rather than on the application servers. For this case, devices may communicate with one another such that one device may function as a client and another device may function as a server.

Application Data Analytics Enablement Service (ADAES) Architecture

[0005] 3GPP has defined an application data analytics enablement service (ADAES) available for applications to access application related analytics. The ADAES architecture is shown in FIG. 2. As shown in the figure, an ADAE client communicates with an ADAE server using the ADAE-UU interface over a 3GPP network. The ADAE client resides on a user equipment (UE) and the ADAE server may reside on an application server (AS) or application function (AF). The figure also shows that the ADAE client and server are part of the Service Enabler Architecture Layer (SEAL), which may be similar to the Service Layer shown in FIG. 1.

[0006] The ADAE layer supports generating application layer analytics to VAL servers and VAL clients. The generated analytics may comprise statistics or predictions associated with an analytics ID. Various analytics IDs are currently supported: application performance, slice-specific and UE-to-UE application performance, location accuracy, service APIs, slice usage patterns, and edge load analytics. Data collection is also managed by the ADAE layer to enable the derivation of the corresponding analytics. Finally, the ADAE server has access to core network services through the N33, N6, and ADAE-OAM interfaces as shown in FIG. 2.

Edge Enabler Layer (EEL)

[0007] Edge computing architecture allows communication and computing services to reside closer to end devices to reduce end-to-end latency and to off-load a network. Thus, an edge enabler layer may be incorporated as part of the service layer described in FIG. 1. FIG. 3 shows an example of a layered application deployment architecture that incorporates functionality from an edge enabler layer, a SEAL layer, an application enabler layer, and an application specific layer. With respects to FIG. 1, the edge enabler layer and the SEAL layer may be considered collectively as a service layer offering horizontal services to all applications.

[0008] Within the edge enabler layer (EEL), edge enabler servers (EESs) and edge enabler clients (EECs) provide services for user equipment (UEs) within an edge data network (EDN). Some of the edge services consist of: service provisioning, registration, discovery, capability exposure, security, and service continuity. Application clients (ACs) on UEs access the edge services through EECs while edge application servers (EASs) access edge services through EESs. Edge configuration servers (ECSs) provide provisioning services to enable EECs to connect with EESs.

Service Enabler Architecture Layer (SEAL)

[0009] As previously described, a service layer may provide common services to all applications regardless of the vertical application. In 3GPP, the Service Enabler Architecture Layer for Verticals (SEAL) provides such horizontal functionality to all applications. Some of the common services offered by SEAL are location management, group management, configuration management, identity management, key management, and network resource management. These services may be available to all applications as the services are agnostic to vertical industries. Each of the services offered may be associated with a corresponding management server, e.g. a group management server offering group services and a location management server offering location services.

[0010] As shown in FIG. 3, a SEAL client residing on a UE may communicate with a SEAL server on an edge data network. However, a SEAL server may also operate as an application server in a data network in the cloud independent of an edge data network. There are many other deployment scenarios within SEAL and FIG. 4 shows an example of support for location-based group creation procedure in SEAL where both a group management server and a location management server are utilized. The procedure provides the ability for a group

management client or VAL server to request the creation of a group (of UEs) based on a particular location that is provided in the request. The request is sent to a group management server, which then requests from a location management server a list of UEs that is in the indicated location. The group management server creates a group from the list of UEs that is returned from the location management server and returns a response to the group management client or VAL server.

Federated Learning

[0011] Federated Learning (FL) is an approach to machine learning (ML) that enables the creation of models trained on data that is distributed across multiple clients or locations, without the need to aggregate and store data in one central location. An FL server manages multiple FL clients during training and/or inferencing and data is kept private and stored locally at the individual FL clients. ML model(s) and the associated parameters are exchanged between the FL server and FL clients during training. The FL server aggregates the model parameters (e.g., weights) at each round of federated training and the FL training iterates for many rounds. This method has become increasingly popular in recent years as more and more organizations seek to harness the power of large datasets without compromising the privacy of individual users and/or data sources. FL also has the added benefits of reduced data movement and improved scalability.

[0012] There have been interests to incorporate federated learning within 3GPP cellular systems to take advantage of the abundance of user equipment (UEs) available and the associated data the UEs may provide for FL operations (e.g. training and/or inferencing). The federated learning requirements of frequent communications (e.g. between FL servers and FL clients), data privacy, and availability of FL clients align with the strengths of cellular systems of providing ubiquitous access to a large number of subscribers that can operate as FL clients.

[0013] Work has already started to provide support in the 3GPP core network for member selection and network performance exposure to assist with FL operations. However, support at the application enablement layer for creating FL groups and managing the FL groups during FL operations are not yet available. Furthermore, application enablers for FL operations such as FL client registration, discovery, and selection do not currently exist in the

existing 3GPP defined application enabler layers. Therefore, application users who want to deploy FL operations on 5G systems are not able to.

SUMMARY

[0014] Some support of federated learning operations has already been defined within the 3GPP 5G cellular core network where new analytics and network exposure were added to assist with creating and managing federated learning groups. However, complimentary federated learning support is lacking at the 3GPP defined application enabler layers to take advantage of these new core network functionalities. Such support is important for enabling federated learning processes and procedures for use by applications from different application service providers/verticals. This disclosure proposes both enhancements to existing procedures and introduction of new procedures for complete federated learning integration within 5G cellular systems.

[0015] According to the present disclosure, methods and systems for supporting federated learning integration at application enabler layers within 5G cellular systems are described herein. In one aspect, a method for an application enabler server to create FL group may include: receiving a first request for forming a federated learning group; where the request includes one or more of: FL server identifier, FL policy, FL client lists (e.g. UE Identifiers), FL client capabilities, minimum number FL clients, FL QoS requirements, location of interest, enable network analytics indicator, number training rounds, FL training schedule, time window recommendation, and policy expiration. In some cases, a FL policy comprises one or more of: client/server identifier, FL policy identifier, application identifier, ML models/algorithms, ML application types, FL capabilities, FL client requirements, dataset requirements, available datasets, dataset capabilities, dataset identifiers, ML application types, dataset description, dataset size, dataset age, target feature, feature list, feature identifier, feature name, data format, dataset metadata, and related features.

[0016] The method may also include sending one or more requests to a cellular 5G core network for assistance with federated learning operations. In some cases, the method may include sending a second request for UE member selection assistance from the 5G network that may include one or more UE member filtering criteria such as QoS requirements, access type, FL operation transfer time, UE location and mobility information. In some cases, the

method may include sending a third request for AF session with QoS that may include QoS requirements for FL operations and a list of UEs to serve as FL clients.

[0017] The method may also include receiving a response from the cellular 5G core network to the one or more requests. In some cases, the response may include a response to the second request with a list of candidate UEs matching the UE member filtering criteria. In some cases, the response may include a response to the third request with one or more of: expected UE moving trajectory, stationary indication, communication duration time, periodic time, scheduled communication time, battery indication, traffic profile, scheduled communication type, and expected time and day of week in trajectory.

[0018] In some cases, the method may include sending a response to the first request, the response may include one or more of: a FL group identifier, a list of FL clients associated with the FL group, and a validity time and/or schedule for the FL group.

[0019] In another aspect, a method for an application enabler server to perform FL group management may include: receiving a first request for forming a federated learning group; the request includes one or more of: FL server identifier, FL policy, FL client lists (e.g. UE Identifiers), FL client capabilities, minimum number FL clients, FL QoS requirements, location of interest, enable network analytics indicator, number training rounds, FL training schedule, time window recommendation, and policy expiration. In some cases, a FL policy comprises one or more of: client/server identifier, FL policy identifier, application identifier, ML models/algorithms, ML application types, FL capabilities, FL client requirements, dataset requirements, available datasets, dataset capabilities, dataset identifiers, ML application types, dataset description, dataset size, dataset age, target feature, feature list, feature identifier, feature name, data format, dataset metadata, and related features.

[0020] In some cases, the method may include sending a response to the first request, the response may include one or more of: a FL group identifier, a list of FL clients associated with the FL group, and a validity time and/or schedule for the FL group.

[0021] In some cases, the method may include sending one or more subscription requests to be notified of changes in location and/or QoS flows of FL clients.

[0022] In some cases, the method may include sending one or more subscription requests to receive analytics on FL clients from an analytics function in the network, including from an application analytics server.

[0023] In some cases, the method may include receiving notification of changes to location, QoS flows, and/or analytics outputs for one or more FL clients.

[0024] In some cases, the method may include updating members of the FL group according to the notification received for the subscriptions.

[0025] In another aspect, a method for an application enabler server to support FL registration may include: receiving a request for registering FL capabilities, the request includes one or more of: FL indication support, client/server identifier, FL policy identifier, application identifier, ML models/algorithms, ML application types, FL capabilities, FL client requirements, dataset requirements, available datasets, dataset capabilities, dataset identifiers, ML application types, dataset description, dataset size, dataset age, target feature, feature list, feature identifier, feature name, data format, dataset metadata, and related features.

[0026] In some cases, the method may include processing the request to authenticate and authorize the requestor; assign an identifier for the FL policy; create a context for the FL policy identifier, and associate and store the FL information within the context in a RESTful resource.

[0027] In some cases, the method may include sending a response to the request, the response includes a status to the registration request and an FL policy identifier.

[0028] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter. Furthermore, the claimed subject matter is not limited to features that solve any or all disadvantages noted in any part of this disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] FIG. 1 depicts an application layer architecture model.

[0030] FIG. 2 depicts an application data analytics enablement service (ADAES) architecture model.

[0031] FIG. 3 depicts a layered application architecture with edge computing.

- [0032] FIG. 4 depicts support of location-based group creation in service enabler architecture layer (SEAL).
- [0033] FIG. 5 depicts an example of federated learning (FL) client and FL server deployments.
- [0034] FIG. 6 depicts a federated learning application enabler layer architecture.
- [0035] FIG. 7 depicts EDGEAPP registration enhancements.
- [0036] FIG. 8 depicts an ADAE registration procedure.
- [0037] FIG. 9 depicts a FL client discovery and selection procedure.
- [0038] FIG. 10 depicts a single request FL group creation procedure.
- [0039] FIG. 11 depicts SEAL-based FL group creation.
- [0040] FIG. 12 depicts a dynamic FL group management procedure.
- [0041] FIG. 13 depicts an analytics-driven FL group management procedure.
- [0042] FIG. 14 depicts a graphical user interface (GUI) for managing FL groups.
- [0043] FIG. 15A depicts an example communications system in which the methods and apparatuses described and claimed herein may be an aspect of;
- [0044] FIG. 15B depicts a block diagram of an example apparatus or device configured for wireless communications;
- [0045] FIG. 15C depicts a system diagram of an example radio access network (RAN) and core network;
- [0046] FIG. 15D depicts a system diagram of another example RAN and core network;
- [0047] FIG. 15E depicts a system diagram of another example RAN and core network;
- [0048] FIG. 15F depicts a block diagram of an example computing system; and
- [0049] FIG. 15G depicts a block diagram of another example communications system.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0050] Prior to enabling federated learning support at application enabler layers, it is important that FL servers and FL clients register their capabilities to an enabler server such as an Edge Enabler Server (EES). The EES may be an ideal server to incorporate federated learning support as the server interfaces to both Edge Application Servers (EASs) and Edge Enabler Clients (EECs). Using FIG. 3 as a reference, the EASs and EECs (e.g. running on UEs) may function as FL servers and FL clients, respectively. Thus, the EES can manage

federated learning operations by incorporating FL registration, FL client discovery, and FL client selection as additional edge services in support of federated learning. Alternatively, the EES may incorporate FL server capabilities natively and provide FL services to the EECs. FIG. 5 shows example embodiments of FL clients and FL servers within the edge computing deployment scenario shown in FIG. 3.

[0051] Similarly, an ADAE server may also be utilized to support federated learning integration. The ADAE architecture supports data collection and application related analytics for VAL servers and VAL clients. In addition, ADAE servers have access to core network services that may be utilized to assist with FL client selection. As a result, ADAE servers and ADAE clients may also be ideal candidates for supporting federated learning. Within the ADAE architecture as shown in FIG. 2, ADAE clients may support FL client functionalities and VAL servers and/or ADAE servers may support FL server functionalities.

[0052] It may also be such that an application enablement layer is defined to support federated learning. An example of such an architecture is shown in FIG. 6. An FL client may reside within a UE and has an FL-C interface with VAL clients on the UE. Similarly, an FL server may reside in a cloud or edge network with an FL-S interface to VAL servers and may also have an FL-NW interface with a 3GPP network. The FL client communicates with the FL server using the FL-UU interface over the 3GPP network.

[0053] Hereinafter, solutions will be developed either by enhancing existing procedures or introducing new procedures in support of federated learning integration in application enabler layers. Note that while the following solutions may focus on edge enabler and application data analytics enabler layers, other application enabler layers, such as SEAL, and/or SEAL Data Delivery (SEALDD), may also be enhanced to support federated learning.

Registration Enhancements for Federated Learning

[0054] The edge enabler layer is an ideal layer where federated learning may be incorporated. As shown by FIG. 3, EECs, EESs, and ECSs all coordinate to provide edge computing services to UEs and EASs. An application client (AC) and/or EEC on a UE may provide FL client functionality while an EAS may provide services associated with an FL server. The edge enabler layer may provide communication services for model and model parameter exchanges between FL servers and FL clients and may also support FL client discovery, selection, and management. Existing procedures in the EEL may be enhanced to

integrate federated learning and FIG. 7 shows an example call flow of such enhancements. The enhancements may comprise the sharing of information about federated learning among the various entities within the edge enabler layer. An example of federated learning information is shown in Table 1.

Table 1 – FL Information for Registration Procedures

Information Element	Description
Client/server identifier	An identifier for an FL client or FL server. The identifier may be a user identifier, FL client/server identifier, UE identifier, VAL server identifier, etc.
FL configuration identifier	An identifier for an FL configuration associated with an FL client/server.
FL role	Specifies the FL role that the request applies to: FL server, FL client
Application identifier	An identifier for the ML(FL) application, which may serve as indications that FL operations are requested.
ML models/algorithms	Information describing ML models/algorithms the FL client/server supports such as neural networks, decision trees and random forests, gradient boost, etc.
ML application types	The types of ML applications the client/server supports. The type may be general, such as supervised, unsupervised, reinforcement learning, etc. or it may be more specific, such as finance, retail, manufacturing, meteorology, warehouse, etc. Other specific types may include identification of targeted features. Both general and specific types may be combined to provide as much information as possible about the extension of support for federated learning.
FL capabilities	Information about the capabilities of the FL client/server; may consist of client/server specific capabilities. Specific capabilities may be computing and storage capabilities, available ML functional packages, support of certain ML application types and/or aggregation strategies, data preparation capabilities, etc.
FL client requirements	Requirements for FL clients, such as the number of required clients for creating FL groups, client capabilities, client schedule availability, client location, etc.
FL security information	Information (e.g. capabilities, pre-provisioned keys, policies) necessary for meeting security requirements. This information may also provide client-specific security-related constraints.
FL user information	Information about the user for which the FL capabilities and resources can be deployed. This element may provide user identification, policies, or user constraint information in a secure manner.
FL historical information	This element may be used to provide information about historical FL tasks associated with the FL client/server, e.g. FL groups it belongs to, associated repositories with historical FL information, etc.
FL client consent	Information provided by FL clients to consent to participate in FL operations, which may include being part of FL client discovery, selection, group formation, etc. The information may also include a schedule of FL client availability (e.g. at night only), available KPIs

	(e.g. percentage of processor, memory, storage), suitable ML applications or types, etc. for FL operations.
Dataset requirements	A list of requirements for datasets that may be used in FL operations for a particular ML model/algorithm.
Available datasets	The number of available datasets for use in FL operations
Dataset capabilities	The capabilities of the client/server to obtain and process data, such as data collection, data preparation, data transformation, data engineering, etc.
Dataset identifiers	An identifier for a particular dataset
>ML application types	The ML application types the associated dataset can be used for FL operation with an ML model/algorithm (see ML application types above)
>Description	A description for the dataset
>Dataset size	The number of data instances in the dataset (e.g. rows of a tabular dataset)
>Dataset age	The time period from which data in the dataset was collected
>Target feature	The name of the target feature of the dataset
>Feature list	A list of features found in the dataset
>>Feature identifier	An identifier for a particular feature
>>Feature name	A name for a particular feature
>>Data format	The format of the data associated with the feature
>>Metadata	Metadata information about the feature
>>Related features	A list of features that may have relationship with the current feature; the list may be used as part of feature engineering to create new features.

[0055] An FL client may provide information about federated learning operations as part of registration procedures within the edge enabler layer (e.g. via AC registration or EEC registration). An FL client may share with an EES information about datasets that the FL client may have available for FL operations, such as the number of datasets available for training and/or inferencing, the ML application types the datasets apply to, a description of the dataset, the dataset size and age, a target feature name or identifier, a list of features found in the dataset, and other information about each feature (e.g. data format, metadata, related features, etc.). In addition, dataset processing capabilities may be provided by FL clients to allow for feature engineering of the dataset for cases where additional features may be created to meet dataset requirements.

[0056] Similarly, an FL server may also provide information about federated learning operations as part of EAS registration. An FL server may provide requirements of federated learning training and/or inferencing to an EES to assist with the creation and management of FL client groups. The FL server may specify an ML model/algorithm for use in FL

training/inferencing, ML application types, FL capabilities, FL client requirements, dataset requirements, and desired dataset capabilities.

[0057] The information shown in Table 1 may be grouped together as a federated learning policy and assigned a policy identifier. The identifier may be included as part of an AC profile and shared within the edge enabler layer as shown in the example of FIG. 7. The FL policy identifier may be referenced between FL clients (e.g. AC or EEC) and FL servers (e.g. EAS) during configuration and operations in support of federated learning.

[0058] Step 1: An FL policy may be provisioned to an AC, EEC, and/or EAS as part of FL integration. The FL policy may comprise information about FL client/server as shown in Table 1. Additionally and/or alternatively, an indicator may be provisioned to notify the AC, EEC, and EAS of federated learning capabilities. The provisioning of FL information may be done at the AC/EEC as shown in step 1a or at the EAS as shown in step 1b.

[0059] Step 2: If an FL policy was provisioned to the AC, the AC may share the information with an EEC (e.g. perform an AC registration request) on a UE with federated learning support. The FL policy may be sent as part of an AC profile or an indicator may be included to specify federated learning capabilities. Additionally and/or alternatively, the AC may request FL services in the List of requested EEC services or List of EAS characteristics information elements that may be included in the request message.

[0060] Step 3: The EEC may perform a request validation of the AC, e.g. checks the security credentials to authenticate and authorize the AC. The EEC may assign an identifier for the FL policy to associate with the FL information provided in the request, create a context for the FL policy identifier, and associate and store the FL information with the context in a RESTful resource maintained by the EEC.

[0061] Step 4: The EEC may return a response to the AC with a status to the request and the assigned FL policy identifier. Additionally and/or alternatively, the EEC may return an indicator that federated learning services are allowed in the List of allowed EEC services information element.

[0062] Step 5: The EEC may perform an EEC registration with an EES, the registration may include the FL policy and/or indicator of federated learning capability. The request may also include the EAS selection request indicator information element to request assistance from the EES for EAS selection, e.g. to enable FL client discovery and selection by an EAS

as part of FL services. Alternatively, a new information element such as Allowed FL client discovery and selection may be included in the request. The new information element may be used by the EES as part of user consent whereby the EEC (and therefore the FL client) is signaling the intention to participate in federated learning operations.

[0063] Step 6: The EES may perform a request validation of the EEC, e.g. checks the security credentials to authenticate and authorize the EEC. The EES may further process the request and determine whether the services requested by the EEC (e.g. as specified in the AC profile and/or federated learning related information elements) can be provided. If the EEC had specified requirements for FL services, the EES may add the Application client (AC)/EEC identifier to an FL client pool with the associated FL information (e.g. as shown in Table 1). The FL client pool may be used in FL client discovery and selection for forming FL groups. The EES may also assign an FL policy identifier to the EEC where information of FL service operations may be associated with. Note that the FL policy identifiers maintained by the EEC and EES may be the same or different from each other.

[0064] Step 7: The EES may further process the request if an EEC context ID and Source EES endpoint IEs were included in the registration request.

[0065] Step 8: The EES may return a response to the EEC, the response may include a status for the registration request and whether FL services are enabled for the EEC via an indicator. Additionally and/or alternatively, a FL service indication may be included as part of AC profile. The FL service indicator may specify whether the requestor can operate as an FL client or server and that the requestor can participate in FL operations. If FL services are enabled, an FL configuration identifier may also be returned in the response or the presence of the FL configuration identifier may signal FL operations are allowed. The FL configuration identifier may be used by AC/EEC to make updates to the information found in Table 1.

[0066] Step 9: An EAS interested in serving as an FL server (e.g. by offering FL services) may indicate such capability in an EAS registration request to the EES. The EAS may have been provisioned and/or configured with FL information as shown in step 1b. The EAS profile may be enhanced to include an FL policy that contains federated learning related information as shown in Table 1. Additionally and/or alternatively, an FL capability indicator may be added to the EAS policy. The FL capability indicator may specify whether the

requestor operates as an FL server or FL client and that the requestor is giving consent for participation in FL operations, e.g. to discover and select clients for FL operations. An FL policy may have been pre-provisioned to each entity and the FL capability indicator may be used to trigger FL services and operations.

[0067] Step 10: The EES may perform an authorization check to verify whether the EAS is able to register to the EES. Upon authorization, the EES may assign an identifier for the FL policy, create an internal context for the EAS profile, and store the information locally in a RESTful resource maintained by the EES.

[0068] Step 11: The EES may return the FL policy identifier and a status in a response message to the EAS.

[0069] For some deployments, it may be such that an EES may also be provisioned with FL policies to simplify communications overhead with FL operations or the EES may receive FL policies from an Edge Configuration Server (ECS) during EES registration. In such deployments, the AC, EEC, and EAS registration procedures may be simplified such that only an FL indicator may be provided to indicate user consent for participation in FL operations.

[0070] The procedures described in FIG. 7 are enhancements to existing edge registration procedures for ACs, EECs, and EASs to communicate support of federated learning. For FL integration with other application enabler layers, new procedures may be proposed to enable the support of federated learning in those enabler layers. As an example, a new registration procedure may be added to the ADAE architecture for ADAE clients and VAL servers/clients to communicate their FL capabilities to an ADAE server. FIG. 8 proposes an example ADAE registration procedure where ADAE clients and VAL servers may register their FL capabilities to an ADAE server similar to the edge enabler procedures. Note that the registration procedure could occur in any order, e.g. a VAL server may register before an ADAE client.

[0071] Step 1: An FL policy may be provisioned to an ADAE client and/or a VAL server/client as part of FL integration. The FL policy may comprise of information about FL client/server as shown in Table 1. Additionally and/or alternatively, an indicator may be provisioned to notify the ADAE client or VAL server/client of federated learning capabilities. The provisioning of FL information may be done at the ADAE client as shown in step 1a or

at the VAL server as shown in step 1b. Note that while not shown in the figure, an FL policy may also be provisioned to a VAL client, which may then communicate the support of federated learning to the ADAE client.

[0072] Step 2: The ADAE client may send a new registration request to the ADAE server, the registration request may include a client identifier, security credentials, and information about the FL policy. Additionally and/or alternatively, the request may include an indicator of the ADAE client's support for federated learning. The indicator may signal user consent for discovering and selecting the ADAE client for participation in federated learning operations. An example of FL registration request parameters is shown in Table 2.

Table 2 – ADAE Registration Request Parameters for FL

Information Element	Description
Client/server identifier	ADAE client or VAL server/client identifier
Security credentials	Credentials for the ADAE server to authenticate and authorize the ADAE client and VAL server/client.
FL indication support	Indication of support for federated learning, which may indicate consent to enable the discovery and selection of the client (e.g. VAL client or ADAE client) for participation in federated learning operations. For VAL servers, the indication may show a VAL server can serve as a FL server and is requesting authorization for FL client discovery and selection, e.g. to form FL client groups in support of FL operations.
FL policy	FL policy provisioned to the ADAE client or VAL server/client. See Table 1 for federated learning information found in an FL policy.

[0073] Step 3: The ADAE server may process the request, including checking the security credentials to authenticate and authorize the ADAE client. The ADAE server may assign an identifier for the FL policy to associate with the ADAE client, create a context for the FL policy identifier, and associate and store the FL information with the context in a RESTful resource maintained by the ADAE server.

[0074] Step 4: The ADAE server may return a response to the ADAE client with a status to the request and the assigned FL policy identifier. Additionally and/or alternatively, the ADAE server may return an indicator that federated learning services are allowed for the ADAE client.

[0075] Step 5: A VAL server interested in offering FL services may indicate such capability in a registration request to the ADAE server, the request may include the VAL

server identifier, security credentials, and information from the FL policy. The VAL server may have been provisioned and/or configured with FL information in step 1b. Additionally and/or alternatively, an FL capability indicator may be included in the request.

[0076] Step 6: The ADAE server may process the request, including checking the security credentials to authenticate and authorize the VAL server. The ADAE server may assign an identifier for the FL policy to associate with the VAL server, create a context for the FL policy identifier, and associate and store the FL information with the context in a RESTful resource maintained by the ADAE server.

[0077] Step 7: The ADAE server may return a response to the VAL server with a status to the request and the assigned FL policy identifier. Additionally and/or alternatively, the ADAE server may return an indicator that federated learning services are allowed for the VAL server.

[0078] Note that while FIG. 7 describes a registration procedure for the ADAES architecture, it may readily be applied to other application enabler layers such as Service Enabler Architecture Layer (SEAL). The basics of the registration procedure, e.g. providing the FL policy or information from the FL policy, may be shared with a SEAL server to indicate the requestor's FL capabilities.

[0079] The registration procedures in FIG. 7 and FIG. 8 share a common element in that an FL policy is communicated to an EES/ADAE server for indicating support of federated learning. The information in the FL policy may be used to not only indicate FL capabilities but also assist in FL client discovery and selection, FL group creation, and FL group management. These procedures will be described in more detail hereinafter.

Client Discovery and Selection

[0080] After an application enabler server (e.g. an EES or ADAE server) is informed of FL clients and their capabilities, the application enabler server may support FL client discovery and selection procedures to form FL groups. FIG. 9 shows an example procedure in which an EAS may request FL client discovery from an EES and use the discovery results to select FL clients for inclusion in an FL group that may be used for federated training and/or inferencing. Once again, enhancements are proposed to existing procedures in edge enabler layers.

[0081] Step 1: An EAS may send an AC information subscription request to an EES to discover all ACs (and hence FL clients) that support federated learning. The EAS may include in the request within the Filters information element, information from a FL policy (e.g. as shown in Table 1) to be matched and other filter parameters such as a geographic service area, UE locations and identifiers (if known), operational schedule, etc. To minimize the size of AC profiles sent in the response to the request, the EAS may include a discovery level information element that further filters information returned to the EAS. For example, the discovery level may indicate all information in an AC profile including all information in FL policy or the discovery level may only request information from the FL policy. Other embodiments for more finer granular levels may be envisaged to filter information included in a response.

[0082] Step 2: The EES may check the security credentials of the EAS to verify the EAS is authorized to perform the operation. The authorization check may include the verification that the EAS is authorized to perform FL operations within the edge data network (EDN). If authorized, the EES may match the FL information provided by the EAS with information of FL clients in the client pool that the EES may manage to fulfill the FL client discovery request.

[0083] Step 3: The EES may return a status to the request and AC information associated with FL clients that fulfills the FL client discovery request to the EAS. The AC information returned may include information from FL policies from Table 1 such as client identifiers, application identifiers, ML models/algorithms, ML application types, FL capabilities, available datasets, dataset capabilities and information. If discovery level filters were provided in the request, the EES may further filter the results and only return information specified by the discovery level filters.

[0084] Step 4: If the EAS does not have UE identifiers for any FL clients received in the response from the EES in step 3, the EAS may perform a UE identifier request to obtain the UE identifiers. The EAS may then use the UE identifiers to make further API requests to EESs and the 5G network. Note that the EAS may also make a UE identifier request independent of the information returned in step 3, e.g. if the EAS is provisioned with information about the FL clients and/or AC profiles. Additionally and/or alternatively, the

EAS may also provide discovery criteria as described in step 1 to the EES, which the EES may use to perform FL client discovery.

[0085] Step 5: The EES may use the information provided in the UE identifier request to find the requested UE identifiers. The EES may communicate with the 5G network, e.g. via a Network Exposure Function (NEF), to obtain the UE identifiers. The EES may then filter the results to obtain a list of only UEs which may operate as FL clients.

[0086] Step 6: The EES may return a status to the UE identifier request and include a list of UE IDs to the EAS. The EAS may use the UE identifiers in future edge API calls for federated learning operations.

[0087] Step 7: The EAS may also be interested in locating UEs within a certain service area to fulfill FL training requirements and make a UE location request to the EES. The request may include a UE identifier and location granularity of the service area the EAS is interested in. The EAS may make multiple UE location requests for all UEs the EAS may be interested in for FL operations. Similar to step 4, the EAS may also include discovery criteria in the request as described in step 1 to the EES.

[0088] Step 8: The EES may check with the 5G network to find the location of the UE or use valid locally cached location of the UE to respond to the UE location request. The EES may then filter the results to obtain a list of only UEs which may operate as FL clients.

[0089] Step 9: The EES may return the list of UEs in a response to the EAS.

[0090] Step 10: An EAS which is offering FL services may send an FL group creation request to the EES to request to form an FL group for federated learning operations. The request may include information as shown in Table 3.

Table 3 – FL group creation request parameters

Information Element	Description
FL server identifier	An identifier for the FL server. The identifier may be an EAS ID or a VAL server ID which is offering FL services.
FL group identifier	An identifier for the FL group that may be used to manage the FL group, e.g. to add/remove FL clients to/from the group.
FL policy	FL policy to use for a particular FL operation, e.g. creating FL group for FL training and/or inferencing. See Table 1 for federated learning information found in an FL policy.
FL client lists	A list of FL clients for inclusion in the FL group.
> UE Identifiers	A UE ID may be associated with each FL client to enable network monitoring of the UEs to assist with FL operations. Other identifiers may also be used, such as GPSI, user identifiers, etc.

FL client capabilities	Requirements of FL client capabilities to perform FL operation, which may include but not limited to processing capabilities, memory and storage capabilities, schedule availability, ML model capabilities, data processing capabilities, client mobility, access type, etc.
Minimum number FL clients	Specifies the minimum number of FL clients required for the group
FL QoS requirements	QoS requirements may be made for all UEs in the FL group in order to have consistent performance while performing FL operation.
Location of interest	Specifies a location for which FL operations are performed and FL clients must be present and available to collect data from.
Enable network analytics	An indicator to request for network analytics predictions to assist with FL operations. Network analytics may include but not limited to end-to-end data volume transfer time, DN performance, Network performance, UE mobility, and WLAN performance analytics. The prediction outputs may be used to manage the FL groups.
Number training rounds	Specifies the number of FL training rounds.
FL operational schedule	Specifies whether the FL operations should be scheduled or performed on demand. For scheduled FL operations, time windows may be specified to indicate when FL operation may be active.
Time window recommendation	An indication to request a recommendation for time windows for which FL operations are made available. The time window may also be provided by the requestor to specify when FL operations may be requested.
Expiration	An expiration for the FL group.

[0091] Step 11: The EES may check the security credentials of the EAS for authentication and authorization purposes. Upon authorization, the EES may assign an identifier for the FL group, create a context to associate the information received in the request to the FL group, and store the information in a RESTful resource within the EES or externally in a data storage entity. The EES may perform FL member selection by examining the FL policy information in the AC profiles. The EES may also communicate with the 5G network to perform member selection based on the requirements provided by the EAS. The EES may call the Nnef_AFsessionWithQoS API with the QoS requirements for FL operations and provide a list of UEs to serve as FL clients. The 5G network may respond with the results for the request, which may include expected UE moving trajectory, stationary indication, communication duration time, periodic time, scheduled communication time, battery indication, traffic profile, scheduled communication type, and expected time and day of week in trajectory. The EES may store the information received in the response from the 5G network in the RESTful resource. Additionally and/or alternatively, the EES may subscribe to

UE member selection assistance from the 5G network by providing UE member filtering criteria such as QoS requirements, access type, FL operation transfer time, UE location and mobility information. In response, the 5G network may send notification messages to the EES with a list of candidate UEs matching the UE member filtering criteria. Note the EES may communicate with the 5G network in a different order than what has been described, e.g. request for UE member selection assistance before calling the Nnef_AFsessionWithQoS API.

[0092] Step 12: The EES may send a notification to all the selected EECs (e.g. UEs) of their selection to be part of the FL group. The notification may include a subscription identifier, a FL policy identifier that may have previously been provisioned, the assigned FL group identifier, the group management operation performed (e.g. add, remove, etc.), and a schedule for when federated operation may be enabled. Note that the FL policy identifier may indicate what type of FL operations (e.g. training, inferencing, etc.) is required for the FL group.

[0093] Step 13: The EEC may return an acknowledgement to the EES and in the acknowledgement, the EEC may specify whether the client is able to perform the federated operation and at the desired schedule.

[0094] Step 14: The EES may return an FL group creation response with the status to the request, the FL group identifier, and a list of FL clients associated with the FL group. The response may also include the validity time and/or schedule for FL operations. Other information such as those found in the FL policy associated with each FL client may also be returned in the response. To preserve the privacy of the FL clients, the list of FL client identifiers may be anonymized.

[0095] The prior procedures require more interactions between FL clients (e.g. EEC, ADAE clients) and FL servers (e.g. EASs, VAL servers) with application enabler servers (e.g. EES, ADAE server) that assist with federated learning integration. For certain deployments where provisioning may be utilized to hasten federated learning adoption, a simpler procedure may be proposed to allow EASs and VAL servers the ability to request the creation of FL groups in one request. This new procedure may combine FL client discovery, selection, and FL group creation into a single request. An example of such a procedure is shown in FIG. 10. Note in the example that FL policy or information required for federated learning integration may be pre-provisioned to the respective entities such as ADAE

clients, ADAE servers, and VAL servers. This procedure may be applied to ADAES and/or SEAL architectures to simplify federated learning integration in application enabler layers since those architectures do not have defined registration procedures.

[0096] Step 1: FL policies may be pre-provisioned to ADAE clients, ADAE servers, and VAL servers as part of federated learning integration. The information provisioned may be those shown in Table 1 for the respective entities. Note that while not shown in the figure, an FL policy may also be provisioned to a VAL client, which may then communicate the support of federated learning to the ADAE client.

[0097] Step 2: An FL user via a VAL server may decide to create a FL group to train an ML application in a federated manner. The VAL server may send an FL group create request to an ADAE server, which may be responsible for managing the FL group during training and/or inferencing. The request may include information such as those shown in Table 3 to assist the ADAE server with discovering and selecting appropriate FL clients to participate in the federated operation. The request may contain explicit indicators for FL client discovery and selection for which the selected FL clients may then be grouped together into a FL group for further FL operations. Alternatively, the request may implicitly infer FL client discovery and selection with FL group creation.

[0098] Step 3: The ADAE server may process the request by first authenticating the VAL server and then checking authorization of the VAL server to make the request. Once authorized, the ADAE server may first query the FL client pool to search for FL clients that can fulfill the FL training requirements sent by the VAL server. The ADAE server may then choose from the discovered FL clients, e.g. to fulfill the minimum number of FL clients, to be part of the FL group. The ADAE server may then create the FL group and assign an identifier for the FL group. In addition, the ADAE server may also create a context to associate the information received in the request to the FL group and store the information in a RESTful resource within the ADAE server or externally in a data storage entity. Furthermore, the ADAE server may also communicate with the 5G network to perform member selection based on the requirements provided by the VAL server. The ADAE server may call the Nnef_AFsessionWithQoS API with the QoS requirements for FL operation and a list of UEs to serve as FL clients. The ADAE server may store the response from the 5G network in the RESTful resource. Additionally and/or alternatively, the ADAE server may subscribe to UE

member selection assistance from the 5G network by providing UE member filtering criteria such as QoS requirements, access type, FL operation transfer time, UE location and mobility information. In response, the 5G network may send notification messages to the ADAE server with a list of candidate UEs matching the UE member filtering criteria. Note the ADAE server may communicate with the 5G network in a different order than what has been described, e.g. request for UE member selection assistance before calling the Nnef_AFsessionWithQoS API.

[0099] Step 4: The ADAE server may send a notification to all the selected ADAE clients (e.g. UEs) of their selection to be part of the FL group. The notification may include a subscription identifier, a FL policy identifier that may have previously been provisioned, the assigned FL group identifier, the group management operation performed (e.g. add, remove, etc.), and a schedule for when federated operation may be enabled. Note that the FL policy identifier may indicate what type of FL operations (e.g. training, inferencing, etc.) is required for the FL group.

[00100] Step 5: The ADAE client may return an acknowledgement to the ADAE server and in the acknowledgement, the ADAE client may specify whether the client is able to perform the federated operation and at the desired schedule.

[00101] Step 6: The ADAE server may make a request to the 5G network to provide required QoS for FL clients in the FL group. The ADAE server may execute the Nnef_AFsessionWithQoS API if it was not already called in step 3 with a list of UE addresses and QoS information for the UEs in the FL group. The 5G network may return a result for each UE identified in the UE list found in the request.

[00102] Step 7: The ADAE server may return a response to the VAL server with the status of the FL group create request, the FL group identifier, a list of FL client identifiers that have been selected for the group, and validity and/or schedule for FL operations. Other information such as those found in the FL policy associated with each FL client may also be returned in the response. To preserve the privacy of the FL clients, the list of FL client identifiers may be anonymized.

[00103] The procedure of FIG. 10 shows enhancements to ADAE service in support of federated learning. Other embodiments may also be realized to add support of federated learning. For example, the aforementioned SEAL location-based group create procedure

shown in FIG. 4 may also be enhanced for federated learning. FIG. 11 shows an example of enhancing the SEAL group and location management servers to support federated learning. A location management client, which is part of the SEAL layer and may be considered a SEAL client, may indicate support for federated learning as part of the location service registration procedure. Then the location-based group create procedure in the group management server may be enhanced with an FL capable filter criteria to not only search for UEs in a particular location but also for UEs that are FL capable. Note within the SEAL architecture, a location management client and a group management client may also be considered as SEAL clients and this extends to other management clients within the SEAL architecture.

[00104] Step 1: A location management client, e.g. residing on a UE that supports FL client functionality, may perform a location service registration with a location management server. The location management client and server may be part of a SEAL layer, the client residing on a UE and the server residing in a network. The location service registration request may include additional information about FL capabilities the FL client supports, e.g. such as those shown in Table 1. As an alternative, the location management client may provide an indication of support for federated learning in the registration request. In addition, FL policies may be pre-provisioned to a VAL server and an ADAE server as part of federated learning integration. The information provisioned may be those shown in Table 1 for the respective entities.

[00105] Step 2: A VAL server may make a location-based group create request that may include a desired location and an indication that the UEs are FL capable. The request may include information such as those shown in Table 3 to assist the location management server with discovering and selecting appropriate FL clients to participate in the federated operation.

[00106] Step 3: The group management server may communicate with a location management server to obtain a list of UEs that are found in the desired location and that also have FL capabilities. The group management server may receive the list of UEs fulfilling the location with FL capabilities and store the list internally.

[00107] Step 4: The group management server may return a response to the location-based group create request with the status of the request, a group identifier, and the list of UEs that meets the location and FL capability criteria.

[00108] Step 5: The VAL server may utilize the list of UEs received from the group management server as input to an FL group create request sent to an ADAE server. The ADAE server may be able to assist the VAL server in managing the FL group due to UE mobility in and out of the desired location. For example, the ADAE server may be able to dynamically manage adding and removing UEs from the FL group. In addition, the ADAE server may also utilize analytics to predict when to add and remove FL capable UEs to/from the FL group.

[00109] Step 6: As part of processing the request, the ADAE server may notify ADAE clients (i.e. FL clients) of their selection to the FL group. The notification may include a subscription identifier, a FL policy identifier that may have previously been provisioned, an assigned FL group identifier, the group management operation performed (e.g. add, remove, etc.), and a schedule for when federated operations may be enabled. Note that the FL policy identifier may indicate what type of FL operations (e.g. training, inferencing, etc.) is required for the FL group.

[00110] Step 7: The ADAE server may return a response to the VAL server with the status of the FL group create request, the FL group identifier, the list of FL client identifiers that have been notified and accepted for inclusion in the FL group, and validity and/or schedule for FL operations. Other information such as those found in the FL policy associated with each FL client may also be returned in the response. To preserve the privacy of the FL clients, the list of FL client identifiers may be anonymized.

[00111] The procedure of FIG. 11 proposes to enhance both the location and group management procedures by adding FL capable indicators to the corresponding requests. The enhancement may be limited to only the group management server or the enhanced functionality may instead be added to the ADAE service with the ADAE server using the existing interface to the group management server as part of FL group creation request. The ADAE server may use the location-based group create procedure to first find all UEs in a particular location and then create an FL group based on notification responses received from ADAE clients (e.g. FL clients) that consent to inclusion in the FL group.

[00112] Note that the procedures shown in FIG. 10 and FIG. 11 show the combination of FL client discovery, selection, and FL group creation in the ADAES architecture. It should be

clear to one skilled in the art that the procedure may also apply to edge enabler layers, service enabler architecture layers (SEAL), and other application enabler layers.

FL Group Management

[00113] One main benefit of integrating federated learning capabilities with an application enabler server such as an EES or ADAE server is the application enabler server is able to dynamically manage FL groups due to changes in FL client availability, e.g. as a result of UE mobility. The application enabler server may have access to cellular network APIs that may be able to determine UEs in a certain area of interest. Furthermore, network analytics may be available to predict UE mobility into a certain area of interest to enable more proactive FL group management.

[00114] FIG. 12 shows an example procedure of dynamic FL group management where UE2 (i.e. EEC2) may leave an area of interest and UE1 (i.e. EEC1) may move into the area of interest. An EES managing an FL group may dynamically modify the group by removing EEC2 and adding EEC1. The EAS, serving as the FL server, may be offloaded from making such decisions to minimize signaling overhead for such management tasks that an application enabler server may readily perform.

[00115] Step 1: EEC1, EEC2, and EAS may have registered their FL support and capabilities to the EES and an FL group may have been created as previously described. Initially, EEC2 is a member of the FL group with other EECs that are not shown but EEC1 is not as it is not located in the area of interest for which FL operations may be requested. EAS provides FL server functionality and have requested to create the FL group and EES have created context information for the FL group. EEC1, EEC2, EES, and EAS all have FL policy information that may have been provisioned for a desired FL application.

[00116] Step 2: The EES may create subscriptions for location and monitoring of UEs with the 5G network to assist with managing the operations of the FL group. The subscriptions may be to monitor the QoS of the individual EEC during FL operations and also to obtain UE location for an area of interest.

[00117] Step 3: EEC2 leaves the area of interest and EEC1 moves into the area of interest.

[00118] Step 4: The 5G network may be tracking the UE mobility of both EEC1 and EEC2 and may inform the EES that EEC2 has left the area of interest while EEC1 is in the area of interest. The 5G network may send notification(s) to the EES of the UE location that was

detected by the network. Additionally and/or alternatively, the EES may receive registration update request from the EEC or receive an ACR detection/request as an indicator of location change of a UE. The EES may also receive UE location information from a location management server or receive application analytics data from an ADAE server. Note the additional and/or alternative update requests are not shown in the figure.

[00119] Step 5: The EES may detect that EEC2 is part of the FL group that EAS had created and may remove EEC2 from the FL group. In addition, EES may notice that EEC1 has entered the area of interest (e.g. via receiving a registration request regarding EEC1 or receiving EEC1's context) and may check the FL policy of EEC1 to evaluate whether EEC1 can be added to the FL group. Upon checking, the EES may determine that EEC1 could serve as an FL client for the FL group and may send a request message to EEC1 to obtain consent for adding it to the FL group. The request may include the FL group identifier, information from the FL policy such as ML application, dataset requirements, FL operation schedule, request user consent for participating in FL operations, and other information from the context of an FL group.

[00120] Step 6: If EEC1 is able to meet the FL operation schedule and wishes to participate in FL operations, EEC1 may send a response to the request indicating consent to be added to the FL group.

[00121] Step 7: The EES may perform an FL group modification to add EEC1 as a new member of the group. EES may update the context information associated with the FL group.

[00122] Step 8: EES may send EAS a notification of the modification to the FL group, the notification may include the FL group identifier, the FL group management operation (e.g. add or remove), the UE identifier associated with EEC1 that was added/removed and the corresponding policy showing the FL capabilities and dataset information provided by EEC1 for FL operations.

[00123] An application enabler server may also utilize analytics to assist with FL group management. The analytics may be performed by an analytics function within the 5G network or by the ADAE server in the ADAES architecture. Within the 5G network, analytics including but not limited to UE mobility, network and data network performance, location accuracy, end-to-end data volume transfer time, relative proximity, and (UE) movement behavior may be subscribed to by an ADAE server or an analytics function in the

5G network to assist with creating and managing FL groups. The resulting analytics output, either statistics or predictions, may be used to proactively manage adding and removing FL group members. Within an ADAE server, analytics including but not limited to edge network loading, service experience, network slice usage pattern, location accuracy, and network slice-specific application performance may be used with dynamically managing FL groups. FIG. 13 shows an example procedure of an ADAE server using either network and/or application-level analytics to assist with FL group management. Note other analytics that may assist with FL group management can be used in addition to the ones mentioned above.

[00124] Step 1: ADAE client and VAL server may have registered their FL support and capabilities to the ADAE server and an FL group may have been created as previously described. The VAL server may provide FL server functionality and may have requested to create an FL group and the ADAE server have created context information for the FL group. ADAE client, ADAE server, and VAL server all have FL policy information that may have been provisioned for a desired FL application.

[00125] Step 2: The ADAE server may configure application specific analytics for the FL group such as edge load analytics to determine whether FL operations are suitable to a particular edge data network. The ADAE server may also create subscriptions to receive analytics outputs from the 5G network to assist with managing the operations of the FL group. The subscriptions may be for example to obtain UE mobility, user data congestion, QoS sustainability, network function load, and network performance analytics for an area of interest. The analytics outputs may provide insights of network performance for which FL operations can complete successfully.

[00126] Step 3: An ADAE client on a UE who is not originally part of the FL group is moving towards the area of interest for which the FL group was created. The analytics component of the 5G network may be collecting data and performing analytics on UE mobility towards the area of interest.

[00127] Step 4: The generated analytics may be predicting that the ADAE client is moving towards the area of interest and may send notification(s) to the ADAE server the prediction results as well as an estimated time of arrival. Other analytics outputs may also provide statistics and/or predictions of network performance and congestion the FL server may use to make decisions on FL operations. Application specific analytics may also be generated, e.g.

by the ADAE server itself or by another ADAE server, and used to manage members of the FL group.

[00128] Step 5: The ADAE server may add the ADAE client to the FL client pool that the ADAE server manages and may send a FL group management request to the ADAE client. The request may include the FL group identifier and information from the context of the FL group such as ML application, dataset requirements, FL operational schedule, request user consent for participating in FL operations, etc.

[00129] Step 6: If the ADAE client is able to meet the FL operational schedule and wishes to participate in FL operations, the ADAE client may send a response to the request indicating consent to be added to the FL group.

[00130] Step 7: The ADAE server may perform an FL group modification to add the ADAE client as a new member of the FL group. The ADAE server may update the context information associated with the FL group. Note that the FL group may have a requirement for minimum number of FL clients and should the group member fall under the minimum number, the ADAE server may proactively use analytics to add more members to the FL group such that the minimum number of members are met. In addition, the analytics may indicate a time window for which the prediction is valid and the ADAE server may use the information to proactively manage the FL group.

[00131] Step 8: The ADAE server may send the VAL server a notification of the modification to the FL group, the notification may include the FL group identifier, the FL group management operation (e.g. add or remove), the UE identifier associated with ADAE client that was added/removed and the corresponding policy showing the FL capabilities and dataset information provided by the ADAE client for FL operations.

[00132] It is worth noting that the FL group management procedures shown in FIG. 12 and FIG. 13 may also apply to other application enablement layers such as the service enabler architecture layers (SEAL). For cases in which analytics is utilized for FL group management, the application enabler layer server may subscribe to analytics from an ADAE server and/or an analytics function in the 5G network.

User Interface

[00133] The process of FL client discovery, selection, and FL group creation and management may be presented in a graphical user interface that is exposed to users of an FL server, e.g. via a VAL server or an EAS. An example of such a GUI is shown in FIG. 14.

[00134] Within the GUI, an FL client pool that an application enabler server may manage can be displayed to enable users to select which FL clients to add to an FL group. Correspondingly, the members of an FL group may also be displayed and grouped together as shown. Information about the FL group may be obtained by pressing the More Info button while pressing each client name may show FL client specific information. Then as the UEs that the FL clients are hosted moves from area to area, the FL client pool may shrink and/or expand to align with the UE mobility. Furthermore, if a UE moves out of the service area of the FL group, the application enabler server may automatically remove the FL client associated with the UE from the FL group and/or client pool.

Example Communications System

[00135] The 3rd Generation Partnership Project (3GPP) develops technical standards for cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities - including work on codecs, security, and quality of service. Recent radio access technology (RAT) standards include WCDMA (commonly referred as 3G), LTE (commonly referred as 4G), LTE-Advanced standards, and New Radio (NR), which is also referred to as “5G”. 3GPP NR standards development is expected to continue and include the definition of next generation radio access technology (new RAT), which is expected to include the provision of new flexible radio access below 7 GHz, and the provision of new ultra-mobile broadband radio access above 7 GHz. The flexible radio access is expected to consist of a new, non-backwards compatible radio access in new spectrum below 7 GHz, and it is expected to include different operating modes that may be multiplexed together in the same spectrum to address a broad set of 3GPP NR use cases with diverging requirements. The ultra-mobile broadband is expected to include cmWave and mmWave spectrum that will provide the opportunity for ultra-mobile broadband access for, e.g., indoor applications and hotspots. In particular, the ultra-mobile broadband is expected to share a common design framework with the flexible radio access below 7 GHz, with cmWave and mmWave specific design optimizations.

[00136] 3GPP has identified a variety of use cases that NR is expected to support, resulting in a wide variety of user experience requirements for data rate, latency, and mobility. The use cases include the following general categories: enhanced mobile broadband (eMBB) ultra-reliable low-latency Communication (URLLC), massive machine type communications (mMTC), network operation (e.g., network slicing, routing, migration and interworking, energy savings), and enhanced vehicle-to-everything (eV2X) communications, which may include any of Vehicle-to-Vehicle Communication (V2V), Vehicle-to-Infrastructure Communication (V2I), Vehicle-to-Network Communication (V2N), Vehicle-to-Pedestrian Communication (V2P), and vehicle communications with other entities. Specific service and applications in these categories include, e.g., monitoring and sensor networks, device remote controlling, bi-directional remote controlling, personal cloud computing, video streaming, wireless cloud-based office, first responder connectivity, automotive ecall, disaster alerts, real-time gaming, multi-person video calls, autonomous driving, augmented reality, tactile internet, virtual reality, home automation, robotics, and aerial drones to name a few. All of these use cases and others are contemplated herein.

[00137] FIG. 15A illustrates an example communications system 100 in which the methods and apparatuses described and claimed herein may be an aspect of. As shown, the example communications system 100 may include wireless transmit/receive units (WTRUs) 102a, 102b, 102c, 102d, 102e, 102f, and/or 102g (which generally or collectively may be referred to as WTRU 102), a radio access network (RAN) 103/104/105/103b/104b/108B, a core network 106/107/109, a public switched telephone network (PSTN) 108, the Internet 110, other networks 112, and V2X server (or ProSe function and server) 113, though it will be appreciated that the disclosed examples contemplate any number of WTRUs, base stations, networks, and/or network elements. Each of the WTRUs 102a, 102b, 102c, 102d, 102e, 102f, 102g may be any type of apparatus or device configured to operate and/or communicate in a wireless environment. Although each WTRU 102a, 102b, 102c, 102d, 102e, 102f, 102g is depicted in FIGS. 15A-5E as a hand-held wireless communications apparatus, it is understood that with the wide variety of use cases contemplated for 5G wireless communications, each WTRU may comprise or be embodied in any type of apparatus or device configured to transmit and/or receive wireless signals, including, by way of example only, user equipment (UE), a mobile station, a fixed or mobile subscriber unit, a pager, a

cellular telephone, a personal digital assistant (PDA), a smartphone, a laptop, a tablet, a netbook, a notebook computer, a personal computer, a wireless sensor, consumer electronics, a wearable device such as a smart watch or smart clothing, a medical or eHealth device, a robot, industrial equipment, a drone, a vehicle such as a car, truck, train, or airplane, and the like.

[00138] The communications system 100 may also include a base station 114a and a base station 114b. Base stations 114a may be any type of device configured to wirelessly interface with at least one of the WTRUs 102a, 102b, 102c to facilitate access to one or more communication networks, such as the core network 106/107/109, the Internet 110, and/or the other networks 112. Base stations 114b may be any type of device configured to wirelessly and/or wirelessly interface with at least one of the RRHs (Remote Radio Heads) 118a, 118b, TRPs (Transmission and Reception Points) 119a, 119b, and/or RSUs (Roadside Units) 120a and 120b to facilitate access to one or more communication networks, such as the core network 106/107/109, the Internet 110, the other networks 112, and/or V2X server (or ProSe function and server) 113. RRHs 118a, 118b may be any type of device configured to wirelessly interface with at least one of the WTRU 102c, to facilitate access to one or more communication networks, such as the core network 106/107/109, the Internet 110, and/or the other networks 112. TRPs 119a, 119b may be any type of device configured to wirelessly interface with at least one of the WTRU 102d, to facilitate access to one or more communication networks, such as the core network 106/107/109, the Internet 110, and/or the other networks 112. RSUs 120a and 120b may be any type of device configured to wirelessly interface with at least one of the WTRU 102e or 102f, to facilitate access to one or more communication networks, such as the core network 106/107/109, the Internet 110, the other networks 112, and/or V2X server (or ProSe function and server) 113. By way of example, the base stations 114a, 114b may be a base transceiver station (BTS), a Node-B, an eNode B, a Home Node B, a Home eNode B, a site controller, an access point (AP), a wireless router, and the like. While the base stations 114a, 114b are each depicted as a single element, it will be appreciated that the base stations 114a, 114b may include any number of interconnected base stations and/or network elements.

[00139] The base station 114a may be part of the RAN 103/104/105, which may also include other base stations and/or network elements (not shown), such as a base station

controller (BSC), a radio network controller (RNC), relay nodes, etc. The base station 114b may be part of the RAN 103b/104b/105b, which may also include other base stations and/or network elements (not shown), such as a base station controller (BSC), a radio network controller (RNC), relay nodes, etc. The base station 114a may be configured to transmit and/or receive wireless signals within a particular geographic region, which may be referred to as a cell (not shown). The base station 114b may be configured to transmit and/or receive wired and/or wireless signals within a particular geographic region, which may be referred to as a cell (not shown). The cell may further be divided into cell sectors. For example, the cell associated with the base station 114a may be divided into three sectors. Thus, the base station 114a may include three transceivers, e.g., one for each sector of the cell. In some cases, the base station 114a may employ multiple-input multiple output (MIMO) technology and, therefore, may utilize multiple transceivers for each sector of the cell.

[00140] The base stations 114a may communicate with one or more of the WTRUs 102a, 102b, 102c over an air interface 115/116/117, which may be any suitable wireless communication link (e.g., radio frequency (RF), microwave, infrared (IR), ultraviolet (UV), visible light, cmWave, mmWave, etc.). The air interface 115/116/117 may be established using any suitable radio access technology (RAT).

[00141] The base stations 114b may communicate with one or more of the RRHs 118a, 118b, TRPs 119a, 119b, and/or RSUs 120a and 120b, over a wired or air interface 115b/116b/117b, which may be any suitable wired (e.g., cable, optical fiber, etc.) or wireless communication link (e.g., radio frequency (RF), microwave, infrared (IR), ultraviolet (UV), visible light, cmWave, mmWave, etc.). The air interface 118B/116b/117b may be established using any suitable radio access technology (RAT).

[00142] The RRHs 118a, 118b, TRPs 119a, 119b and/or RSUs 120a, 120b, may communicate with one or more of the WTRUs 102c, 102d, 102e, 102f over an air interface 118C/116c/117c, which may be any suitable wireless communication link (e.g., radio frequency (RF), microwave, infrared (IR), ultraviolet (UV), visible light, cmWave, mmWave, etc.). The air interface 115c/116c/117c may be established using any suitable radio access technology (RAT).

[00143] The WTRUs 102a, 102b, 102c, 102d, 102e, 102f, and/or 102g may communicate with one another over an air interface 115d/116d/117d (not shown in the figures), which may

be any suitable wireless communication link (e.g., radio frequency (RF), microwave, infrared (IR), ultraviolet (UV), visible light, cmWave, mmWave, etc.). The air interface 118D/116d/117d may be established using any suitable radio access technology (RAT).

[00144] More specifically, as noted above, the communications system 100 may be a multiple access system and may employ one or more channel access schemes, such as CDMA, TDMA, FDMA, OFDMA, SC-FDMA, and the like. For example, the base station 114a in the RAN 103/104/105 and the WTRUs 102a, 102b, 102c, or RRHs 118a, 118b, TRPs 119a, 119b and RSUs 120a, 120b, in the RAN 103b/104b/105b and the WTRUs 102c, 102d, 102e, 102f, may implement a radio technology such as Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access (UTRA), which may establish the air interface 115/116/117 or 115c/116c/117c respectively using wideband CDMA (WCDMA). WCDMA may include communication protocols such as High-Speed Packet Access (HSPA) and/or Evolved HSPA (HSPA+). HSPA may include High-Speed Downlink Packet Access (HSDPA) and/or High-Speed Uplink Packet Access (HSUPA).

[00145] In some cases, the base station 114a and the WTRUs 102a, 102b, 102c, or RRHs 118a, 118b, TRPs 119a, 119b, and/or RSUs 120a, 120b, in the RAN 103b/104b/108B and the WTRUs 102c, 102d, may implement a radio technology such as Evolved UMTS Terrestrial Radio Access (E-UTRA), which may establish the air interface 115/116/117 or 118C/116c/117c respectively using Long Term Evolution (LTE) and/or LTE-Advanced (LTE-A). In the future, the air interface 115/116/117 may implement 3GPP NR technology. The LTE and LTE-A technology includes LTE D2D and V2X technologies and interface (such as Sidelink communications, etc.) The 3GPP NR technology includes NR V2X technologies and interface (such as Sidelink communications, etc.)

[00146] In some cases, the base station 114a in the RAN 103/104/105 and the WTRUs 102a, 102b, 102c, or RRHs 118a, 118b, TRPs 119a, 119b and/or RSUs 120a, 120b, in the RAN 103b/104b/105b and the WTRUs 102c, 102d, 102e, 102f may implement radio technologies such as IEEE 802.16 (e.g., Worldwide Interoperability for Microwave Access (WiMAX)), CDMA2000, CDMA2000 1X, CDMA2000 EV-DO, Interim Standard 2000 (IS-2000), Interim Standard 95 (IS-95), Interim Standard 856 (IS-856), Global System for Mobile communications (GSM), Enhanced Data rates for GSM Evolution (EDGE), GSM EDGE (GERAN), and the like.

[00147] The base station 114c in FIG. 15A may be a wireless router, Home Node B, Home eNode B, or access point, for example, and may utilize any suitable RAT for facilitating wireless connectivity in a localized area, such as a place of business, a home, a vehicle, a campus, and the like. In some cases, the base station 114c and the WTRUs 102e, may implement a radio technology such as IEEE 802.11 to establish a wireless local area network (WLAN). In some cases, the base station 114c and the WTRUs 102d, may implement a radio technology such as IEEE 802.15 to establish a wireless personal area network (WPAN). In some cases, the base station 114c and the WTRUs 102e, may utilize a cellular-based RAT (e.g., WCDMA, CDMA2000, GSM, LTE, LTE-A, etc.) to establish a picocell or femtocell. As shown in FIG. 15A, the base station 114b may have a direct connection to the Internet 110. Thus, the base station 114c may not be required to access the Internet 110 via the core network 106/107/109.

[00148] The RAN 103/104/105 and/or RAN 103b/104b/105b may be in communication with the core network 106/107/109, which may be any type of network configured to provide voice, data, applications, and/or voice over internet protocol (VoIP) services to one or more of the WTRUs 102a, 102b, 102c, 102d. For example, the core network 106/107/109 may provide call control, billing services, mobile location-based services, pre-paid calling, Internet connectivity, video distribution, etc., and/or perform high-level security functions, such as user authentication.

[00149] Although not shown in FIG. 15A, it will be appreciated that the RAN 103/104/105 and/or RAN 103b/104b/105b and/or the core network 106/107/109 may be in direct or indirect communication with other RANs that employ the same RAT as the RAN 103/104/105 and/or RAN 103b/104b/105b or a different RAT. For example, in addition to being connected to the RAN 103/104/105 and/or RAN 103b/104b/105b, which may be utilizing an E-UTRA radio technology, the core network 106/107/109 may also be in communication with another RAN (not shown) employing a GSM radio technology.

[00150] The core network 106/107/109 may also serve as a gateway for the WTRUs 102a, 102b, 102c, 102d, 102e to access the PSTN 108, the Internet 110, and/or other networks 112. The PSTN 108 may include circuit-switched telephone networks that provide plain old telephone service (POTS). The Internet 110 may include a global system of interconnected computer networks and devices that use common communication protocols, such as the

transmission control protocol (TCP), user datagram protocol (UDP) and the internet protocol (IP) in the TCP/IP internet protocol suite. The networks 112 may include wired or wireless communications networks owned and/or operated by other service providers. For example, the networks 112 may include another core network connected to one or more RANs, which may employ the same RAT as the RAN 103/104/105 and/or RAN 103b/104b/108B or a different RAT.

[00151] Some or all of the WTRUs 102a, 102b, 102c, 102d in the communications system 100 may include multi-mode capabilities, e.g., the WTRUs 102a, 102b, 102c, 102d, and 102e may include multiple transceivers for communicating with different wireless networks over different wireless links. For example, the WTRU 102e shown in FIG. 15A may be configured to communicate with the base station 114a, which may employ a cellular-based radio technology, and with the base station 114c, which may employ an IEEE 802 radio technology.

[00152] FIG. 15B is a block diagram of an example apparatus or device configured for wireless communications in accordance with the aspects illustrated herein, such as for example, a WTRU 102. As shown in FIG. 15B, the example WTRU 102 may include a processor 118, a transceiver 120, a transmit/receive element 122, a speaker/microphone 124, a keypad 113, a display/touchpad/indicators 128, non-removable memory 130, removable memory 132, a power source 134, a global positioning system (GPS) chipset 136, and other peripherals 138. It will be appreciated that the WTRU 102 may include any sub-combination of the foregoing elements while remaining consistent with an example. Also, in some cases the base stations 114a and 114b, and/or the nodes that base stations 114a and 114b may represent, such as but not limited to transceiver station (BTS), a Node-B, a site controller, an access point (AP), a home node-B, an evolved home node-B (eNodeB), a home evolved node-B (HeNB), a home evolved node-B gateway, and proxy nodes, among others, may include some or all of the elements depicted in FIG. 15B and described herein.

[00153] The processor 118 may be a general purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Array (FPGAs) circuits, any other type of integrated circuit (IC), a state machine, and the

like. The processor 118 may perform signal coding, data processing, power control, input/output processing, and/or any other functionality that enables the WTRU 102 to operate in a wireless environment. The processor 118 may be coupled to the transceiver 120, which may be coupled to the transmit/receive element 122. While FIG. 15B depicts the processor 118 and the transceiver 120 as separate components, it will be appreciated that the processor 118 and the transceiver 120 may be integrated together in an electronic package or chip.

[00154] The transmit/receive element 122 may be configured to transmit signals to, or receive signals from, a base station (e.g., the base station 114a) over the air interface 115/116/117. For example, in some cases, the transmit/receive element 122 may be an antenna configured to transmit and/or receive RF signals. In some cases, the transmit/receive element 122 may be an emitter/detector configured to transmit and/or receive IR, UV, or visible light signals, for example. In some cases, the transmit/receive element 122 may be configured to transmit and receive both RF and light signals. It will be appreciated that the transmit/receive element 122 may be configured to transmit and/or receive any combination of wireless signals.

[00155] In addition, although the transmit/receive element 122 is depicted in FIG. 15B as a single element, the WTRU 102 may include any number of transmit/receive elements 122. More specifically, the WTRU 102 may employ MIMO technology. Thus, in some cases, the WTRU 102 may include two or more transmit/receive elements 122 (e.g., multiple antennas) for transmitting and receiving wireless signals over the air interface 115/116/117.

[00156] The transceiver 120 may be configured to modulate the signals that are to be transmitted by the transmit/receive element 122 and to demodulate the signals that are received by the transmit/receive element 122. As noted above, the WTRU 102 may have multi-mode capabilities. Thus, the transceiver 120 may include multiple transceivers for enabling the WTRU 102 to communicate via multiple RATs, such as UTRA and IEEE 802.11, for example.

[00157] The processor 118 of the WTRU 102 may be coupled to, and may receive user input data from, the speaker/microphone 124, the keypad 126, and/or the display/touchpad/indicators 128 (e.g., a liquid crystal display (LCD) display unit or organic light-emitting diode (OLED) display unit). The processor 118 may also output user data to the speaker/microphone 124, the keypad 126, and/or the display/touchpad/indicators 128. In

addition, the processor 118 may access information from, and store data in, any type of suitable memory, such as the non-removable memory 130 and/or the removable memory 132. The non-removable memory 130 may include random-access memory (RAM), read-only memory (ROM), a hard disk, or any other type of memory storage device. The removable memory 132 may include a subscriber identity module (SIM) card, a memory stick, a secure digital (SD) memory card, and the like. In some cases, the processor 118 may access information from, and store data in, memory that is not physically located on the WTRU 102, such as on a server or a home computer (not shown).

[00158] The processor 118 may receive power from the power source 134, and may be configured to distribute and/or control the power to the other components in the WTRU 102. The power source 134 may be any suitable device for powering the WTRU 102. For example, the power source 134 may include one or more dry cell batteries, solar cells, fuel cells, and the like.

[00159] The processor 118 may also be coupled to the GPS chipset 136, which may be configured to provide location information (e.g., longitude and latitude) regarding the current location of the WTRU 102. In addition to, or in lieu of, the information from the GPS chipset 136, the WTRU 102 may receive location information over the air interface 115/116/117 from a base station (e.g., base stations 114a, 114b) and/or determine its location based on the timing of the signals being received from two or more nearby base stations. It will be appreciated that the WTRU 102 may acquire location information by way of any suitable location-determination method while remaining consistent with an aspect.

[00160] The processor 118 may further be coupled to other peripherals 138, which may include one or more software and/or hardware modules that provide additional features, functionality and/or wired or wireless connectivity. For example, the peripherals 138 may include various sensors such as an accelerometer, biometrics (e.g., finger print) sensors, an e-compass, a satellite transceiver, a digital camera (for photographs or video), a universal serial bus (USB) port or other interconnect interfaces, a vibration device, a television transceiver, a hands free headset, a Bluetooth® module, a frequency modulated (FM) radio unit, a digital music player, a media player, a video game player module, an Internet browser, and the like.

[00161] The WTRU 102 may be embodied in other apparatuses or devices, such as a sensor, consumer electronics, a wearable device such as a smart watch or smart clothing, a

medical or eHealth device, a robot, industrial equipment, a drone, a vehicle such as a car, truck, train, or airplane. The WTRU 102 may connect to other components, modules, or systems of such apparatuses or devices via one or more interconnect interfaces, such as an interconnect interface that may comprise one of the peripherals 138.

[00162] FIG. 15C is a system diagram of the RAN 103 and the core network 106. As noted above, the RAN 103 may employ a UTRA radio technology to communicate with the WTRUs 102a, 102b, and 102c over the air interface 115. The RAN 103 may also be in communication with the core network 106. As shown in FIG. 15C, the RAN 103 may include Node-Bs 140a, 140b, 140c, which may each include one or more transceivers for communicating with the WTRUs 102a, 102b, 102c over the air interface 115. The Node-Bs 140a, 140b, 140c may each be associated with a particular cell (not shown) within the RAN 103. The RAN 103 may also include RNCs 142a, 142b. It will be appreciated that the RAN 103 may include any number of Node-Bs and RNCs while remaining consistent with an aspect of the disclosure.

[00163] As shown in FIG. 15C, the Node-Bs 140a, 140b may be in communication with the RNC 142a. Additionally, the Node-B 140c may be in communication with the RNC 142b. The Node-Bs 140a, 140b, 140c may communicate with the respective RNCs 142a, 142b via an Iub interface. The RNCs 142a, 142b may be in communication with one another via an Iur interface. Each of the RNCs 142a, 142b may be configured to control the respective Node-Bs 140a, 140b, 140c to which it is connected. In addition, each of the RNCs 142a, 142b may be configured to carry out or support other functionality, such as outer loop power control, load control, admission control, packet scheduling, handover control, macro-diversity, security functions, data encryption, and the like.

[00164] The core network 106 shown in FIG. 15C may include a media gateway (MGW) 144, a mobile switching center (MSC) 146, a serving GPRS support node (SGSN) 148, and/or a gateway GPRS support node (GGSN) 150. While each of the foregoing elements are depicted as part of the core network 106, it will be appreciated that any one of these elements may be owned and/or operated by an entity other than the core network operator.

[00165] The RNC 142a in the RAN 103 may be connected to the MSC 146 in the core network 106 via an IuCS interface. The MSC 146 may be connected to the MGW 144. The MSC 146 and the MGW 144 may provide the WTRUs 102a, 102b, 102c with access to

circuit-switched networks, such as the PSTN 108, to facilitate communications between the WTRUs 102a, 102b, 102c and traditional land-line communications devices.

[00166] The RNC 142a in the RAN 103 may also be connected to the SGSN 148 in the core network 106 via an IuPS interface. The SGSN 148 may be connected to the GGSN 150. The SGSN 148 and the GGSN 150 may provide the WTRUs 102a, 102b, 102c with access to packet-switched networks, such as the Internet 110, to facilitate communications between and the WTRUs 102a, 102b, 102c and IP-enabled devices.

[00167] As noted above, the core network 106 may also be connected to the networks 112, which may include other wired or wireless networks that are owned and/or operated by other service providers.

[00168] FIG. 15D is a system diagram of the RAN 104 and the core network 107. As noted above, the RAN 104 may employ an E-UTRA radio technology to communicate with the WTRUs 102a, 102b, and 102c over the air interface 116. The RAN 104 may also be in communication with the core network 107.

[00169] The RAN 104 may include eNode-Bs 160a, 160b, 160c, though it will be appreciated that the RAN 104 may include any number of eNode-Bs while remaining consistent with an aspect of the disclosure. The eNode-Bs 160a, 160b, 160c may each include one or more transceivers for communicating with the WTRUs 102a, 102b, 102c over the air interface 116. In some cases, the eNode-Bs 160a, 160b, 160c may implement MIMO technology. Thus, the eNode-B 160a, for example, may use multiple antennas to transmit wireless signals to, and receive wireless signals from, the WTRU 102a.

[00170] Each of the eNode-Bs 160a, 160b, and 160c may be associated with a particular cell (not shown) and may be configured to handle radio resource management decisions, handover decisions, scheduling of users in the uplink and/or downlink, and the like. As shown in FIG. 15D, the eNode-Bs 160a, 160b, 160c may communicate with one another over an X2 interface.

[00171] The core network 107 shown in FIG. 15D may include a mobility management gateway (MME) 162, a serving gateway 164, and a packet data network (PDN) gateway 166. While each of the foregoing elements are depicted as part of the core network 107, it will be appreciated that any one of these elements may be owned and/or operated by an entity other than the core network operator.

[00172] The MME 162 may be connected to each of the eNode-Bs 160a, 160b, and 160c in the RAN 104 via an S1 interface and may serve as a control node. For example, the MME 162 may be responsible for authenticating users of the WTRUs 102a, 102b, 102c, bearer activation/deactivation, selecting a particular serving gateway during an initial attach of the WTRUs 102a, 102b, 102c, and the like. The MME 162 may also provide a control plane function for switching between the RAN 104 and other RANs (not shown) that employ other radio technologies, such as GSM or WCDMA.

[00173] The serving gateway 164 may be connected to each of the eNode-Bs 160a, 160b, and 160c in the RAN 104 via the S1 interface. The serving gateway 164 may generally route and forward user data packets to/from the WTRUs 102a, 102b, 102c. The serving gateway 164 may also perform other functions, such as anchoring user planes during inter-eNode B handovers, triggering paging when downlink data is available for the WTRUs 102a, 102b, 102c, managing and storing contexts of the WTRUs 102a, 102b, 102c, and the like.

[00174] The serving gateway 164 may also be connected to the PDN gateway 166, which may provide the WTRUs 102a, 102b, 102c with access to packet-switched networks, such as the Internet 110, to facilitate communications between the WTRUs 102a, 102b, 102c and IP-enabled devices.

[00175] The core network 107 may facilitate communications with other networks. For example, the core network 107 may provide the WTRUs 102a, 102b, 102c with access to circuit-switched networks, such as the PSTN 108, to facilitate communications between the WTRUs 102a, 102b, 102c and traditional land-line communications devices. For example, the core network 107 may include, or may communicate with, an IP gateway (e.g., an IP multimedia subsystem (IMS) server) that serves as an interface between the core network 107 and the PSTN 108. In addition, the core network 107 may provide the WTRUs 102a, 102b, 102c with access to the networks 112, which may include other wired or wireless networks that are owned and/or operated by other service providers.

[00176] FIG. 15E is a system diagram of the RAN 105 and the core network 109. The RAN 105 may be an access service network (ASN) that employs IEEE 802.16 radio technology to communicate with the WTRUs 102a, 102b, and 102c over the air interface 117. As will be further discussed below, the communication links between the different functional entities of

the WTRUs 102a, 102b, 102c, the RAN 105, and the core network 109 may be defined as reference points.

[00177] As shown in FIG. 15E, the RAN 105 may include base stations 180a, 180b, 180c, and an ASN gateway 182, though it will be appreciated that the RAN 105 may include any number of base stations and ASN gateways while remaining consistent with an aspect of the disclosure. The base stations 180a, 180b, 180c may each be associated with a particular cell in the RAN 105 and may include one or more transceivers for communicating with the WTRUs 102a, 102b, 102c over the air interface 117. In some cases, the base stations 180a, 180b, 180c may implement MIMO technology. Thus, the base station 180a, for example, may use multiple antennas to transmit wireless signals to, and receive wireless signals from, the WTRU 102a. The base stations 180a, 180b, 180c may also provide mobility management functions, such as handoff triggering, tunnel establishment, radio resource management, traffic classification, quality of service (QoS) policy enforcement, and the like. The ASN gateway 182 may serve as a traffic aggregation point and may be responsible for paging, caching of subscriber profiles, routing to the core network 109, and the like.

[00178] The air interface 117 between the WTRUs 102a, 102b, 102c and the RAN 105 may be defined as an R1 reference point that implements the IEEE 802.16 specification. In addition, each of the WTRUs 102a, 102b, and 102c may establish a logical interface (not shown) with the core network 109. The logical interface between the WTRUs 102a, 102b, 102c and the core network 109 may be defined as an R2 reference point, which may be used for authentication, authorization, IP host configuration management, and/or mobility management.

[00179] The communication link between each of the base stations 180a, 180b, and 180c may be defined as an R8 reference point that includes protocols for facilitating WTRU handovers and the transfer of data between base stations. The communication link between the base stations 180a, 180b, 180c and the ASN gateway 182 may be defined as an R6 reference point. The R6 reference point may include protocols for facilitating mobility management based on mobility events associated with each of the WTRUs 102a, 102b, 102c.

[00180] As shown in FIG. 15E, the RAN 105 may be connected to the core network 109. The communication link between the RAN 105 and the core network 109 may be defined as an R3 reference point that includes protocols for facilitating data transfer and mobility

management capabilities, for example. The core network 109 may include a mobile IP home agent (MIP-HA) 184, an authentication, authorization, accounting (AAA) server 186, and a gateway 188. While each of the foregoing elements are depicted as part of the core network 109, it will be appreciated that any one of these elements may be owned and/or operated by an entity other than the core network operator.

[00181] The MIP-HA may be responsible for IP address management, and may enable the WTRUs 102a, 102b, and 102c to roam between different ASNs and/or different core networks. The MIP-HA 184 may provide the WTRUs 102a, 102b, 102c with access to packet-switched networks, such as the Internet 110, to facilitate communications between the WTRUs 102a, 102b, 102c and IP-enabled devices. The AAA server 186 may be responsible for user authentication and for supporting user services. The gateway 188 may facilitate interworking with other networks. For example, the gateway 188 may provide the WTRUs 102a, 102b, 102c with access to circuit-switched networks, such as the PSTN 108, to facilitate communications between the WTRUs 102a, 102b, 102c and traditional land-line communications devices. In addition, the gateway 188 may provide the WTRUs 102a, 102b, 102c with access to the networks 112, which may include other wired or wireless networks that are owned and/or operated by other service providers.

[00182] Although not shown in FIG. 15E, it will be appreciated that the RAN 105 may be connected to other ASNs and the core network 109 may be connected to other core networks. The communication link between the RAN 105 the other ASNs may be defined as an R4 reference point, which may include protocols for coordinating the mobility of the WTRUs 102a, 102b, 102c between the RAN 105 and the other ASNs. The communication link between the core network 109 and the other core networks may be defined as an R5 reference, which may include protocols for facilitating interworking between home core networks and visited core networks.

[00183] The core network entities described herein and illustrated in FIGS. 15A, 15C, 15D, and 15E are identified by the names given to those entities in certain existing 3GPP specifications, but it is understood that in the future those entities and functionalities may be identified by other names and certain entities or functions may be combined in future specifications published by 3GPP, including future 3GPP NR specifications. Thus, the particular network entities and functionalities described and illustrated in FIGS. 15A, 15B,

15C, 15D, and 15E are provided by way of example only, and it is understood that the subject matter disclosed and claimed herein may be embodied or implemented in any similar communication system, whether presently defined or defined in the future.

[00184] FIG. 15F is a block diagram of an exemplary computing system 90 in which one or more apparatuses of the communications networks illustrated in FIGS. 15A, 15C, 15D and 15E may be embodied, such as certain nodes or functional entities in the RAN 103/104/105, Core Network 106/107/109, PSTN 108, Internet 110, or Other Networks 112. Computing system 90 may comprise a computer or server and may be controlled primarily by computer readable instructions, which may be in the form of software, wherever, or by whatever means such software is stored or accessed. Such computer readable instructions may be executed within a processor 91, to cause computing system 90 to do work. The processor 91 may be a general purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Array (FPGAs) circuits, any other type of integrated circuit (IC), a state machine, and the like. The processor 91 may perform signal coding, data processing, power control, input/output processing, and/or any other functionality that enables the computing system 90 to operate in a communications network. Coprocessor 81 is an optional processor, distinct from main processor 91, that may perform additional functions or assist processor 91. Processor 91 and/or coprocessor 81 may receive, generate, and process data related to the methods and apparatuses disclosed herein.

[00185] In operation, processor 91 fetches, decodes, and executes instructions, and transfers information to and from other resources via the computing system's main data-transfer path, system bus 80. Such a system bus connects the components in computing system 90 and defines the medium for data exchange. System bus 80 typically includes data lines for sending data, address lines for sending addresses, and control lines for sending interrupts and for operating the system bus. An example of such a system bus 80 is the PCI (Peripheral Component Interconnect) bus.

[00186] Memories coupled to system bus 80 include random access memory (RAM) 82 and read only memory (ROM) 93. Such memories include circuitry that allows information to be stored and retrieved. ROMs 93 generally contain stored data that may not easily be

modified. Data stored in RAM 82 may be read or changed by processor 91 or other hardware devices. Access to RAM 82 and/or ROM 93 may be controlled by memory controller 92. Memory controller 92 may provide an address translation function that translates virtual addresses into physical addresses as instructions are executed. Memory controller 92 may also provide a memory protection function that isolates processes within the system and isolates system processes from user processes. Thus, a program running in a first mode may access only memory mapped by its own process virtual address space; it may not access memory within another process's virtual address space unless memory sharing between the processes has been set up.

[00187] In addition, computing system 90 may contain peripherals controller 83 responsible for communicating instructions from processor 91 to peripherals, such as printer 94, keyboard 84, mouse 95, and disk drive 85.

[00188] Display 86, which is controlled by display controller 96, is used to display visual output generated by computing system 90. Such visual output may include text, graphics, animated graphics, and video. The visual output may be provided in the form of a graphical user interface (GUI). Display 86 may be implemented with a CRT-based video display, an LCD-based flat-panel display, gas plasma-based flat-panel display, or a touch-panel. Display controller 96 includes electronic components required to generate a video signal that is sent to display 86.

[00189] Further, computing system 90 may contain communication circuitry, such as for example a network adapter 97, that may be used to connect computing system 90 to an external communications network, such as the RAN 103/104/105, Core Network 106/107/109, PSTN 108, Internet 110, or Other Networks 112 of FIGS. 15A, 15B, 15C, 15D, and 15E, to enable the computing system 90 to communicate with other nodes or functional entities of those networks. The communication circuitry, alone or in combination with the processor 91, may be used to perform the transmitting and receiving steps of certain apparatuses, nodes, or functional entities described herein.

[00190] FIG. 15G illustrates an example communications system 111 in which the methods and apparatuses described and claimed herein may be an aspect of. As shown, the example communications system 111 may include wireless transmit/receive units (WTRUs) A, B, C, D, E, F, a base station, a V2X server, and a RSUs A and B, though it will be appreciated that

the disclosure contemplates any number of WTRUs, base stations, networks, and/or network elements. One or several or all WTRUs A, B, C, D, E may be out of range of the network (for example, in the figure out of the cell coverage boundary shown as the dash line). WTRUs A, B, C form a V2X group, among which WTRU A is the group lead and WTRUs B and C are group members. WTRUs A, B, C, D, E, F may communicate over Uu interface or Sidelink (PC5) interface.

[00191] It is understood that any or all of the apparatuses, systems, methods and processes described herein may be embodied in the form of computer executable instructions (e.g., program code) stored on a computer-readable storage medium which instructions, when executed by a processor, such as processors 118 or 91, cause the processor to perform and/or implement the systems, methods and processes described herein. Specifically, any of the steps, operations or functions described herein may be implemented in the form of such computer executable instructions, executing on the processor of an apparatus or computing system configured for wireless and/or wired network communications. Computer readable storage media include volatile and nonvolatile, removable and non-removable media implemented in any non-transitory (e.g., tangible or physical) method or technology for storage of information, but such computer readable storage media do not include signals. Computer readable storage media include, but are not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other tangible or physical medium which may be used to store the desired information and which may be accessed by a computing system.

Definitions

[00192] Provided below are definitions for abbreviations found within the body of the disclosure.

3GPP	3 rd Generation Partnership Project
AC	Application Client
ACR	Application Context Relocation
ADAE	Application Data Analytics Enablement
AF	Application Function
API	Application Programming Interface
AS	Application Server

EAS	Edge Application Server
ECS	Edge Configuration Server
EDN	Edge Data Network
EEC	Edge Enabler Client
EEL	Edge Enabler Layer
EES	Edge Enabler Server
GPSI	Generic Public Subscription Identifier
GUI	Graphical User Interface
IP	Internet Protocol
NEF	Network Exposure Function
SEAL	Service Enabler Architecture Layer
SEALDD	SEAL Data Delivery
SL	Service Layer
UE	User Equipment
URI	Uniform Resource Identifier
VAL	Vertical Application Layer

[00193] Provided below are definitions for terms found within the body of the disclosure.

FL user	A user apparatus (e.g., computer, smart phone, tablet) hosting compute, memory and network connectivity resources capable of hosting a user application (e.g., web browser, application client) which a user utilizes to perform FL centric operations with an FL server such as but not limited to discovery and selection of available FL clients to create FL groups. An FL user may interface with VAL servers to perform FL operations and could also be the owner of one or more FL clients.
FL server	A network apparatus (e.g., device, gateway or server) hosting compute, memory and network connectivity resources capable of hosting an FL service which performs FL management operations such as FL client registration, discovery and selection, and FL group management.
FL client	A network apparatus (e.g., device, gateway or server) hosting compute, memory and network connectivity resources capable of hosting an FL client (e.g., client application) which registers to an FL server and also hosts local data that may be used for training machine learning models in a federated manner. FL clients may reside and operate on UEs.

CLAIMS

What is claimed:

1. A method performed by an application enabler server, comprising:
receiving a request for forming a federated learning (FL) group;
assigning at least one UE to the FL group;
sending a request to a core network to obtain one or more UEs for the FL group
wherein the request may include filter criteria comprising QoS requirements, access type, FL operation transfer time, UE location and mobility information, or a combination thereof;
receiving a response from the core network with a list of one or more UEs; and
sending a response to the request for forming the FL group indicating a status corresponding to the FL group.
2. The method of claim 1, wherein the response to the request for forming the FL group comprises a status of the request for forming the FL group, a FL group identifier, one or more UE identifiers selected for the FL group, a schedule for FL operations, or a combination thereof.
3. The method of claim 1, wherein the request for forming the FL group comprises a FL server identifier, a FL group identifier, a FL policy, a FL client list, FL client capability requirements, a number of clients to be a part of the FL group, quality of service requirements, a geographical location, or a combination thereof.
4. The method of claim 1, sending a notification to the at least one UE indicating a selection of the at least one UE as part of the FL group; and
receiving a response from the at least one UE indicating the UE is able to participate in the FL operation.
5. The method of claim 1, wherein the assigning UEs to the FL group may result from discovering UEs from the list of UEs received from the core network.

6. The method of claim 1, further comprising:
discovering a plurality of UEs from a FL client pool, wherein the assigning the at least one UE to the FL group is based on the discovering.
7. The method of claim 1, further comprising:
assigning a FL group identifier to the FL group.
8. A method performed by an application enabler server, comprising:
sending a location-based group create request to a group management server;
receiving a response to the location-based group create request comprising at least a list of UEs satisfying a location criteria, a federated learning (FL) criteria, or both;
sending, based on the list of UEs, a FL group create request; and
receiving a response to the FL group create request comprising information corresponding to the FL group.
9. The method of claim 8, wherein the response to the location-based group create request further comprises a status of the request, a group identifier, or both.
10. The method of claim 8, wherein the information corresponding to the FL group comprises a status of the FL group create request, a FL group identifier, one or more FL client identifier, a schedule of FL operations, or a combination thereof.
11. The method of claim 8, wherein the location-based group create request comprises a FL server identifier, a FL group identifier, a FL policy, a FL client list, FL client capability requirements, a number of clients to be a part of the FL group, quality of service requirements for the FL group, a geographical location for the FL group, or a combination thereof.
12. The method of claim 8, wherein the application enabler server is pre-provisioned with one or more FL policies.

13. The method of claim 12, wherein the one or more FL policies comprise a server identifier, a FL configuration identifier, a FL role, an application identifier, a machine learning (ML) model or algorithm, a ML application type, one or more FL capabilities, FL security information, FL user information, FL historical information, or a combination thereof.
14. The method of claim 8, wherein the FL group create request is sent to an application data analytics enablement (ADAE) server.
15. An apparatus comprising:
one or more processors;
memory; and
a set of instructions stored in the memory that, when executed by the one or more processors, cause:
 receiving a request for forming a federated learning (FL) group;
 assigning at least one UE to the FL group;
 sending a notification to the at least one UE indicating a selection of the at least one UE as part of the FL group;
 sending a request to a core network for quality of service metrics for one or more UEs of the FL group;
 receiving the quality of service metrics for the one or more UEs; and
 sending a response to the request for forming the FL group indicating a status corresponding to the FL group.
16. The apparatus of claim 15, wherein the response to the request for forming the FL group comprises a status of the request for forming the FL group, a FL group identifier, one or more FL UE identifiers selected for the FL group, a schedule for FL operations, or a combination thereof.
17. The apparatus of claim 15, wherein the request for forming the FL group comprises a FL server identifier, a FL group identifier, a FL policy, a FL client list, FL client capability

requirements, a number of clients to be a part of the FL group, quality of service requirements for the FL group, a geographical location for the FL group, or a combination thereof.

18. The apparatus of claim 15, wherein the request for forming the FL group is received from a VAL server.

19. The apparatus of claim 18, wherein the set of instructions, when executed by the one or more processors, further cause:
 authenticating the VAL server.

20. The apparatus of claim 15, wherein the set of instructions, when executed by the one or more processors, further cause:
 discovering a plurality of UEs from a FL client pool, wherein the assigning the at least one UE to the FL group is based on the discovering.

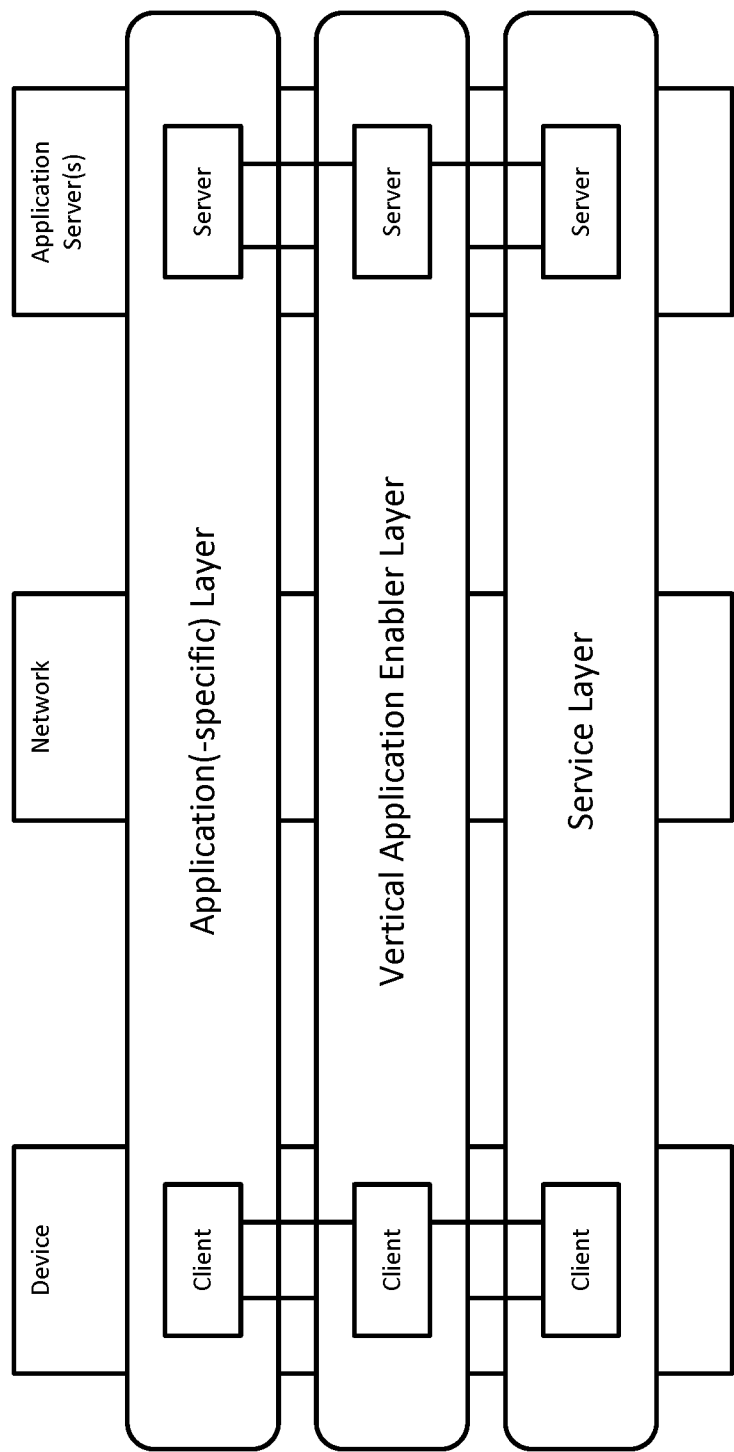


FIG. 1

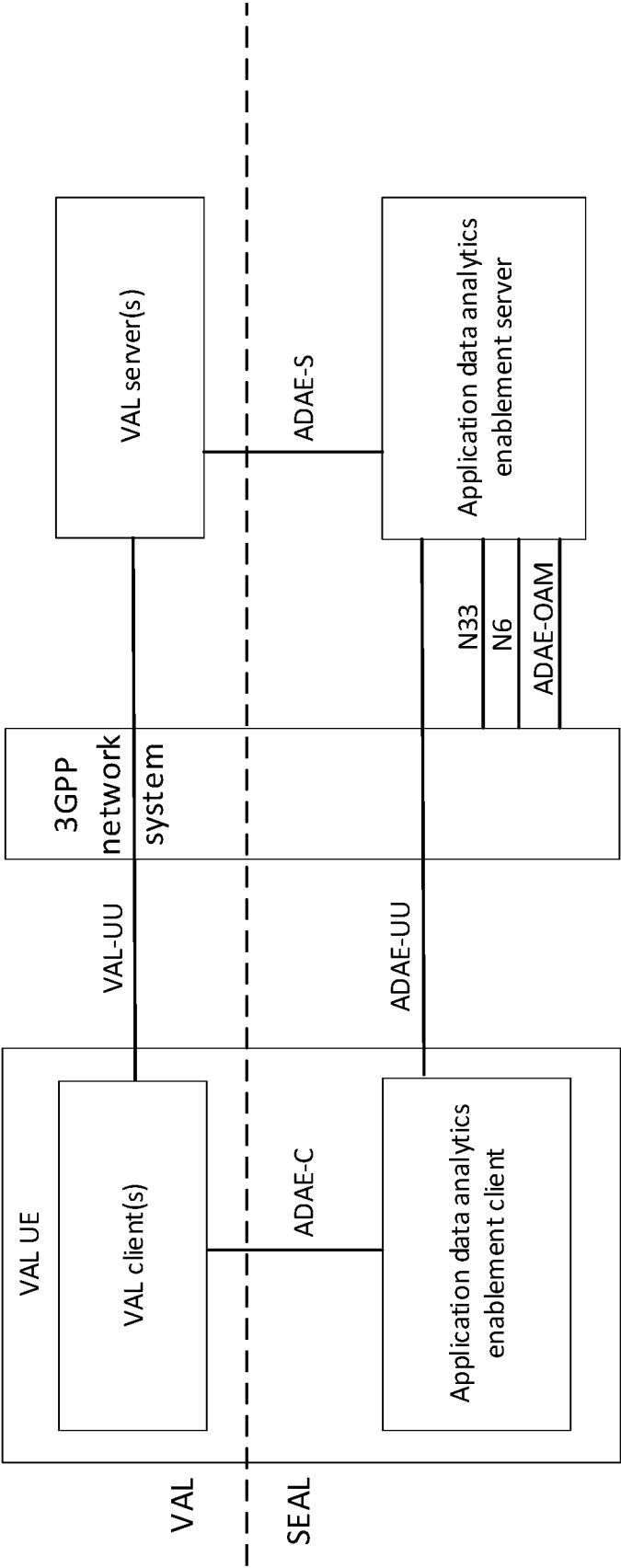


FIG. 2

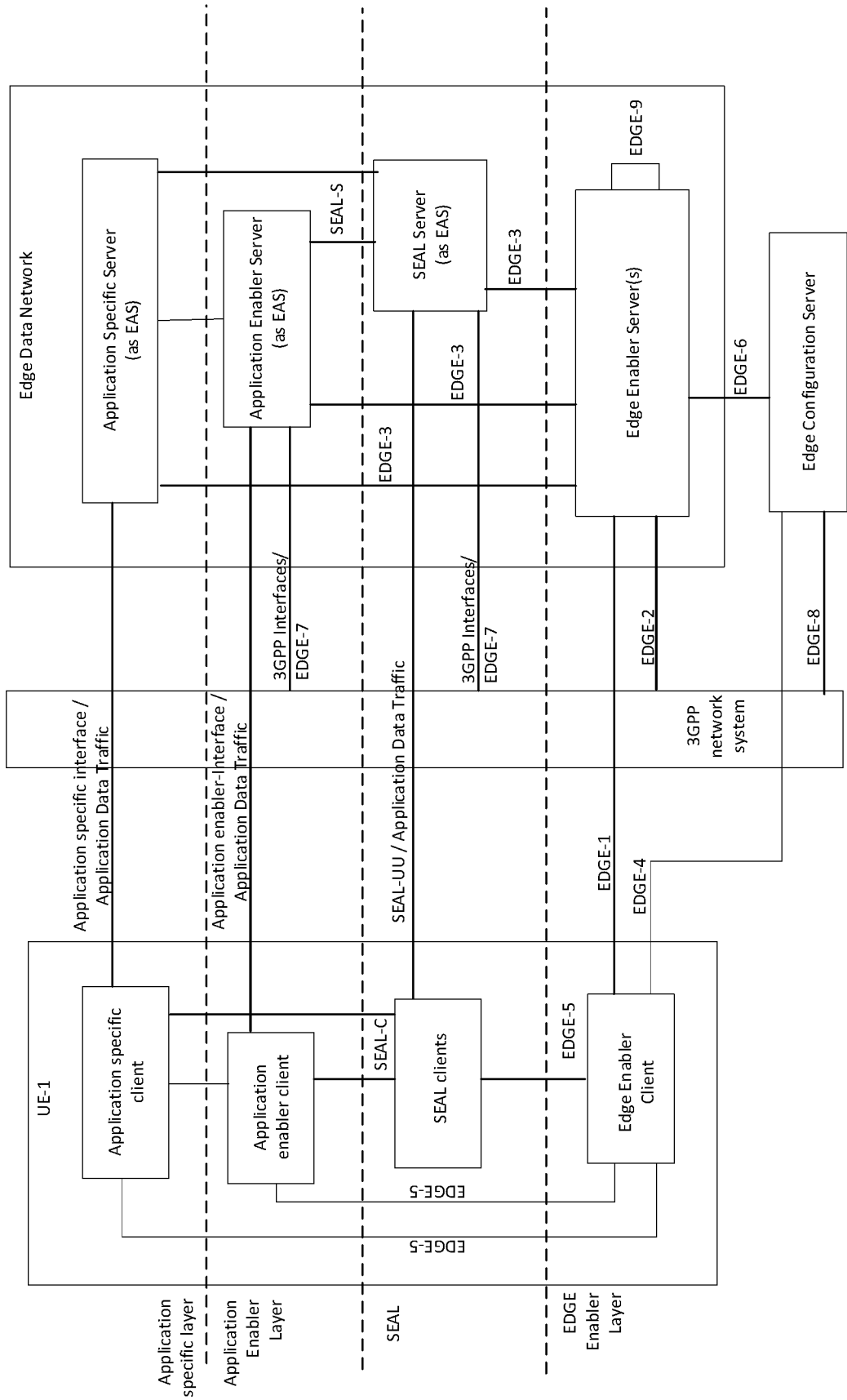


FIG. 3

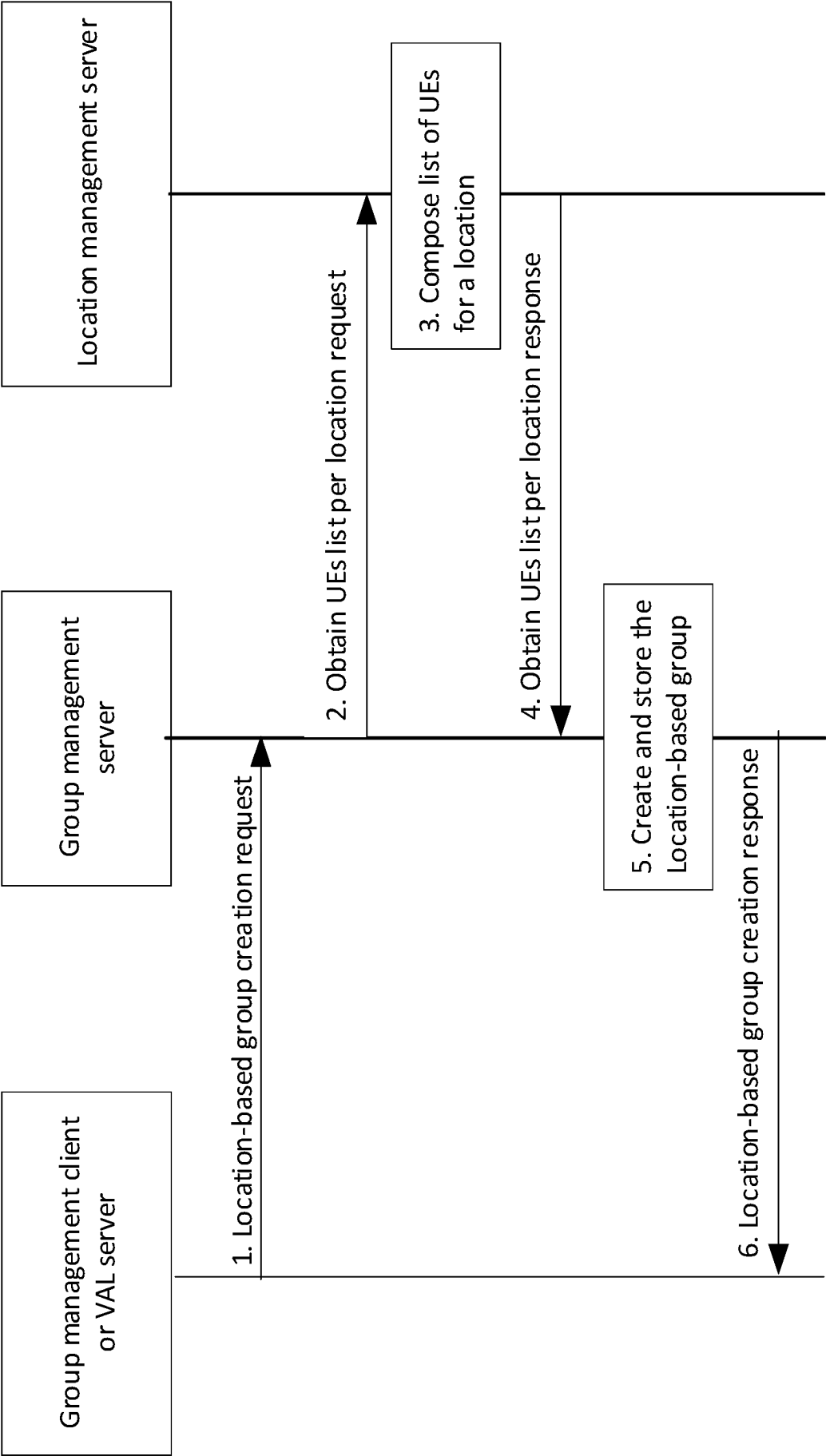


FIG. 4

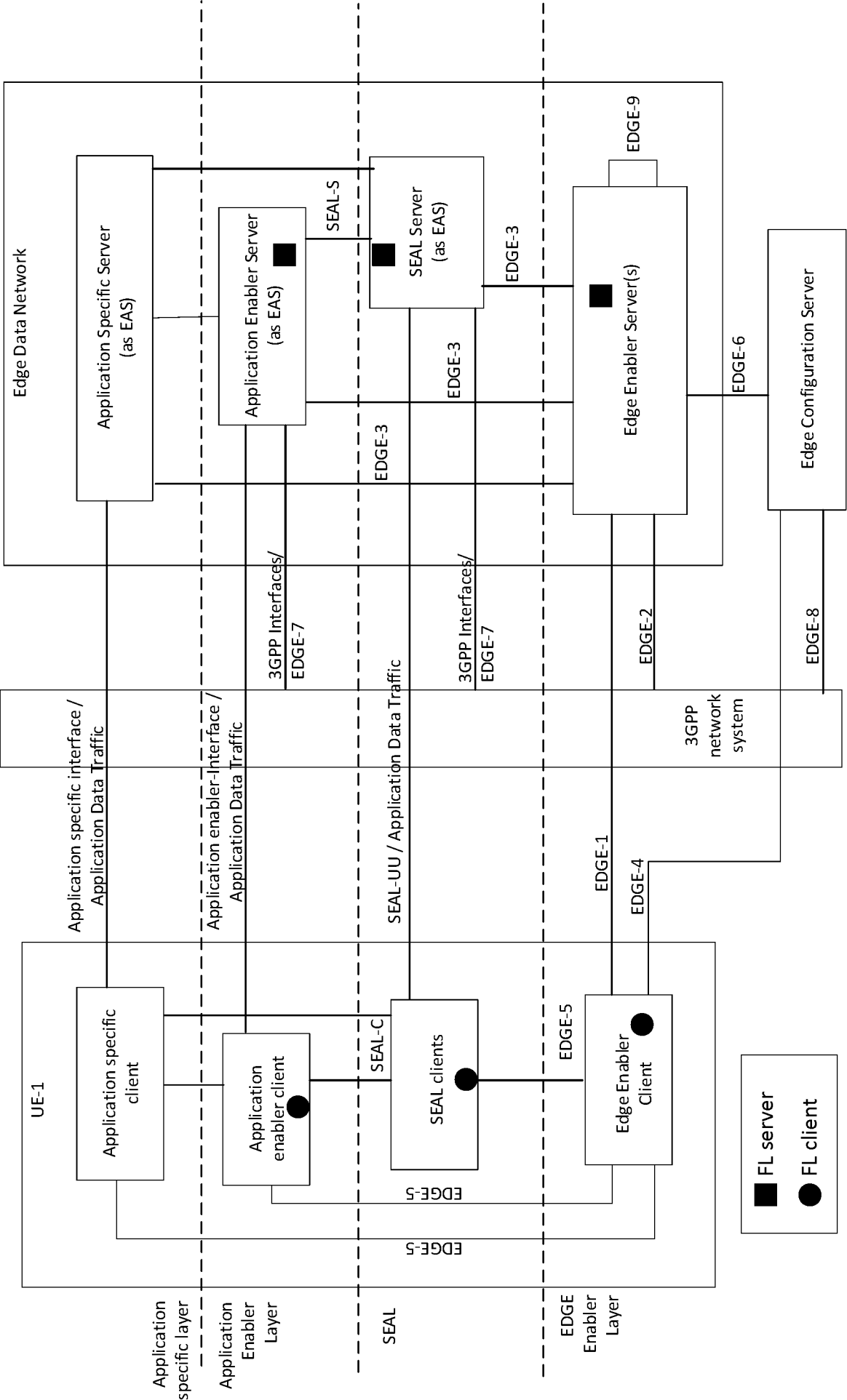


FIG. 5

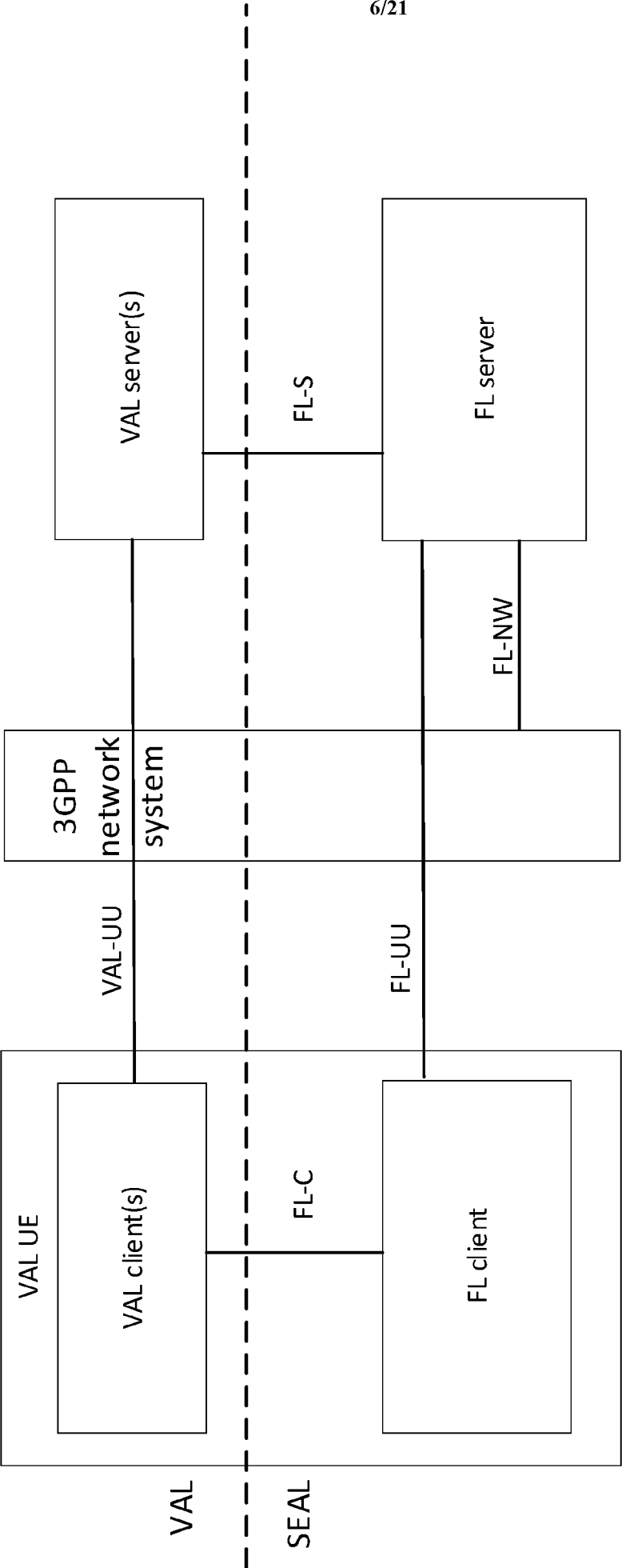


FIG. 6

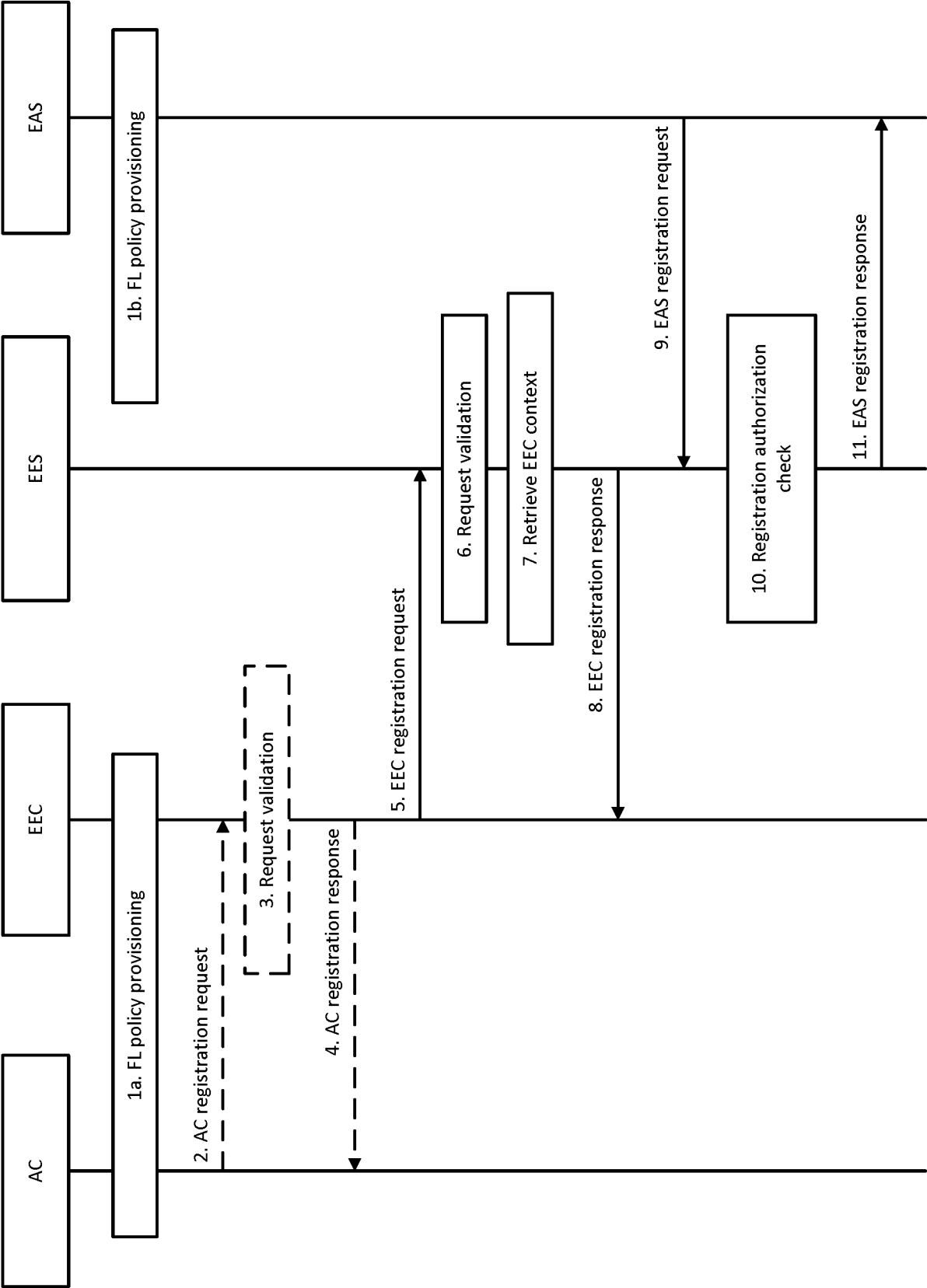


FIG. 7

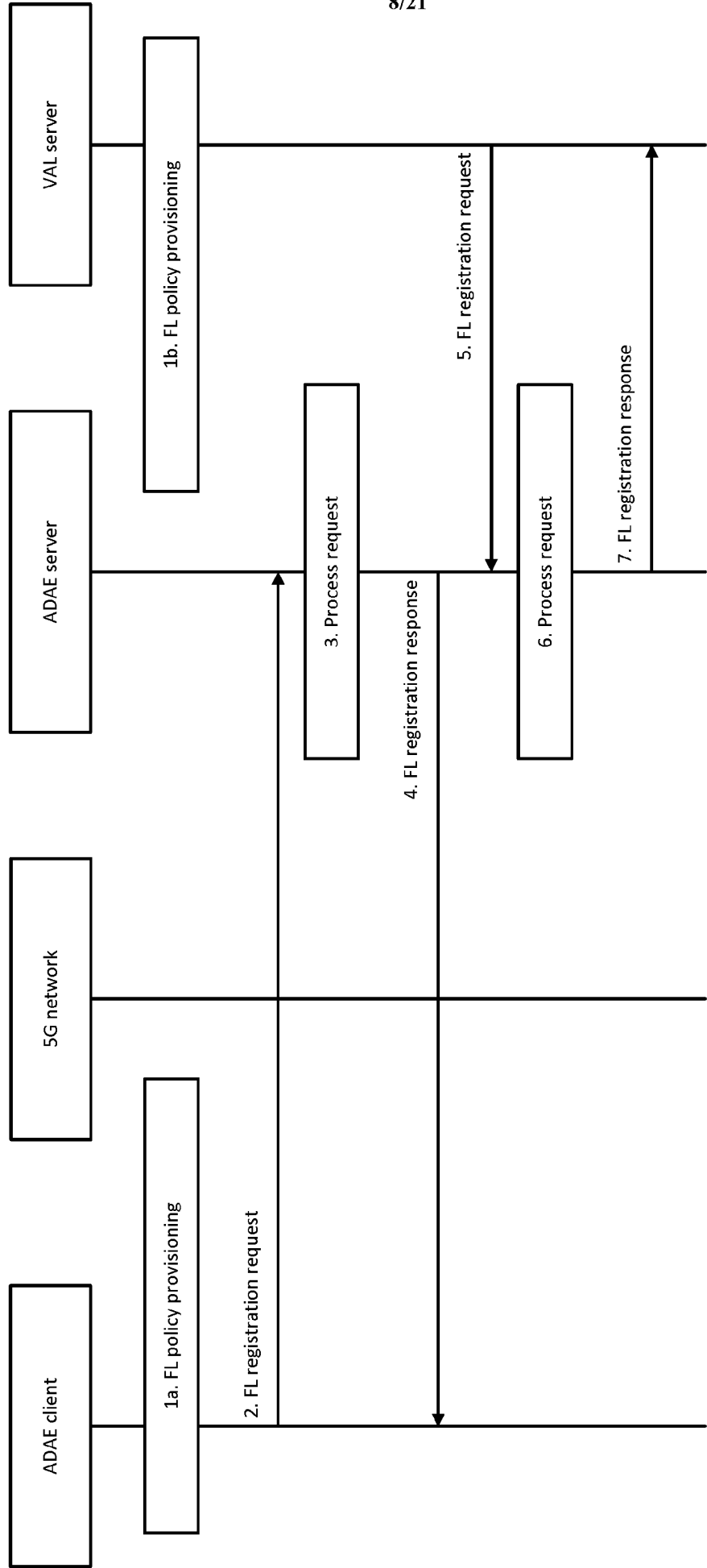


FIG. 8

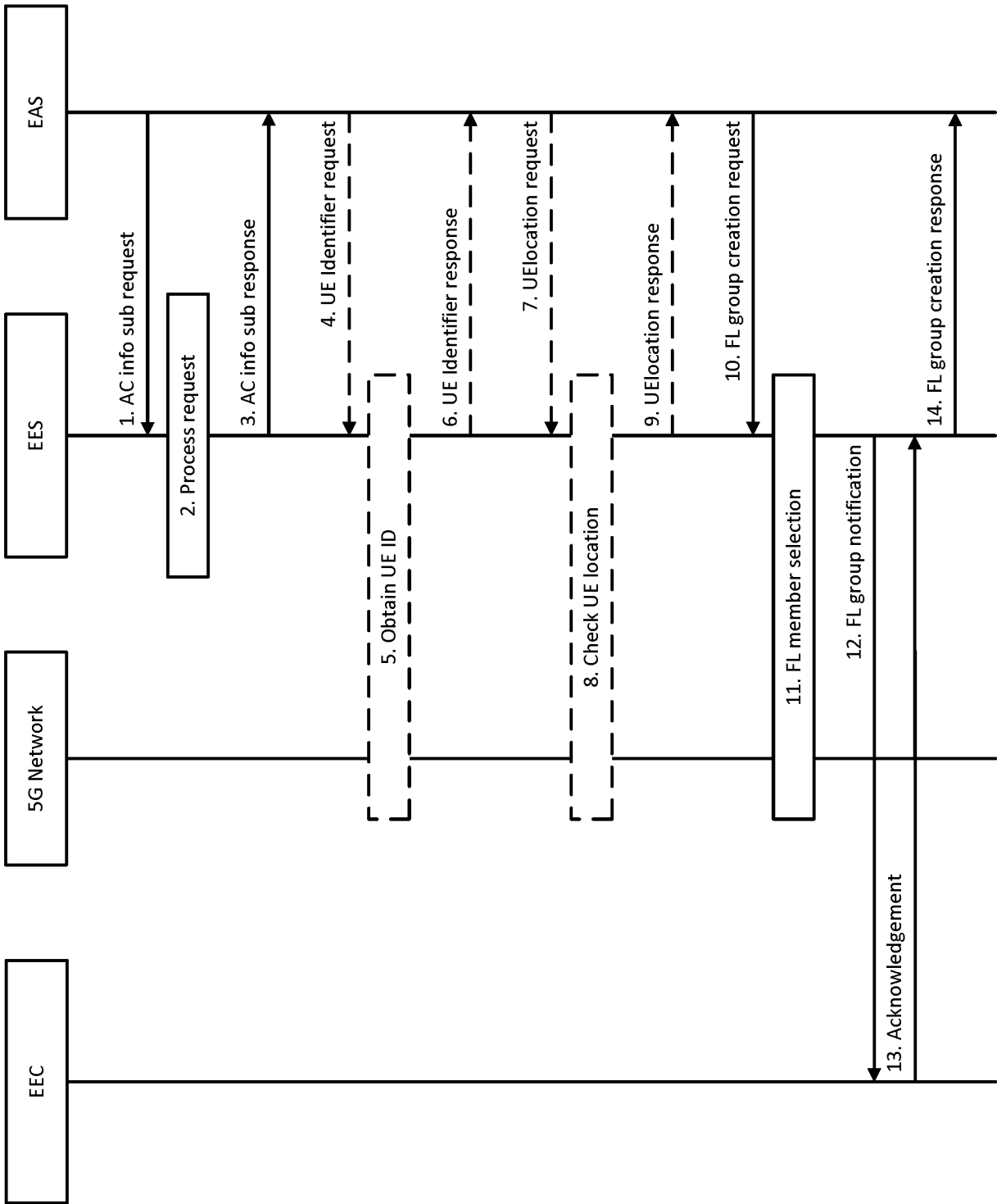


FIG. 9

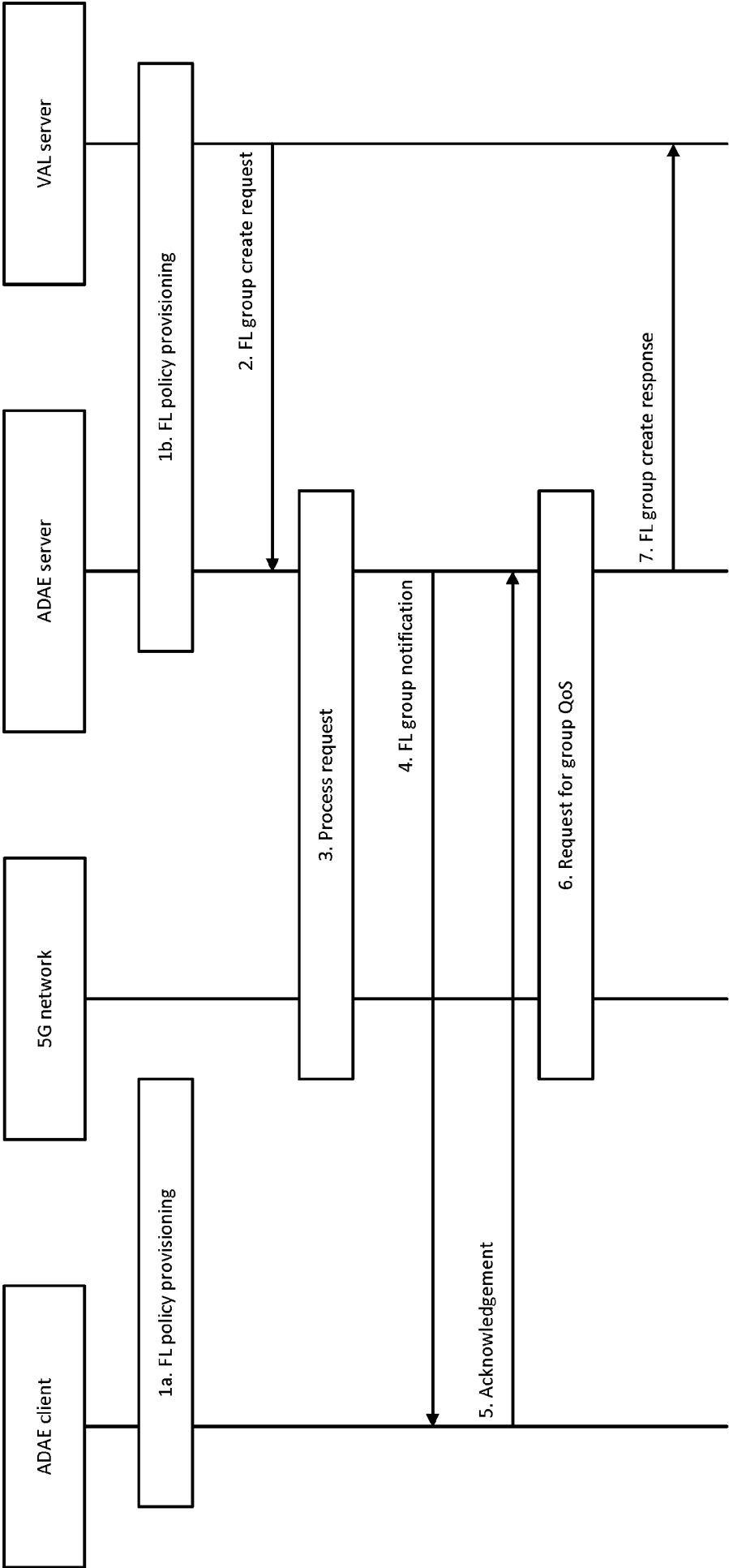


FIG. 10

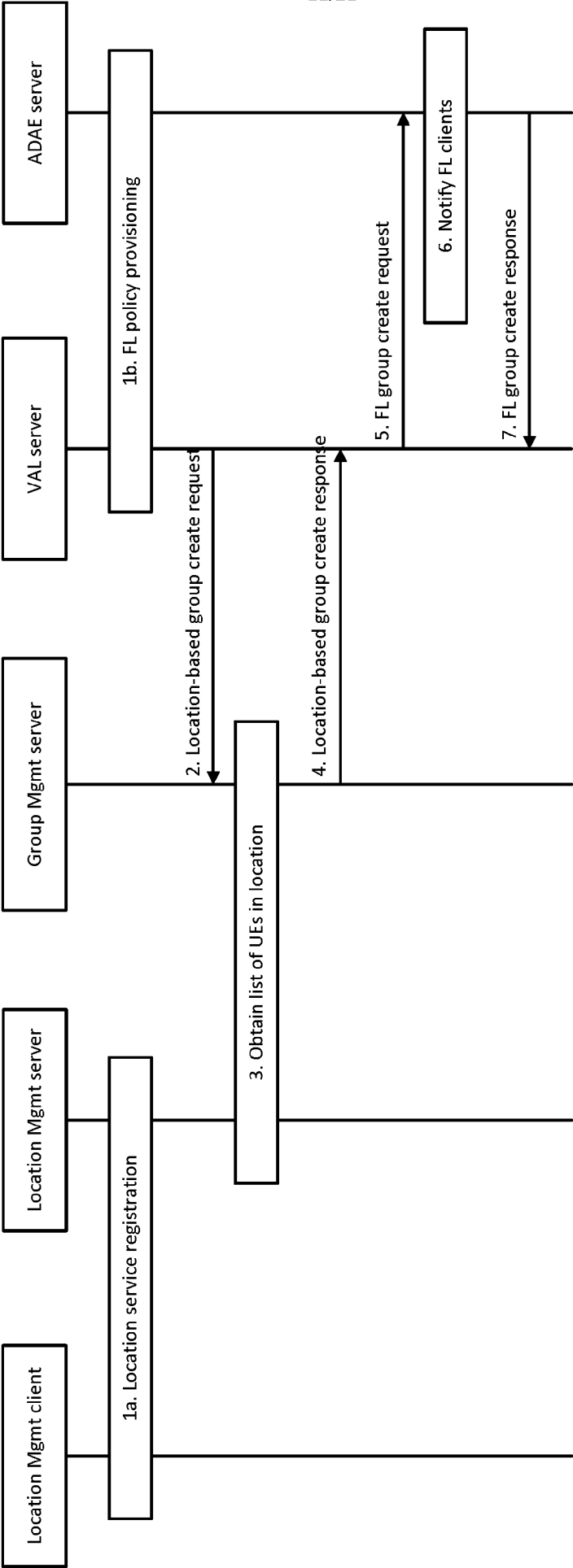


FIG. 11

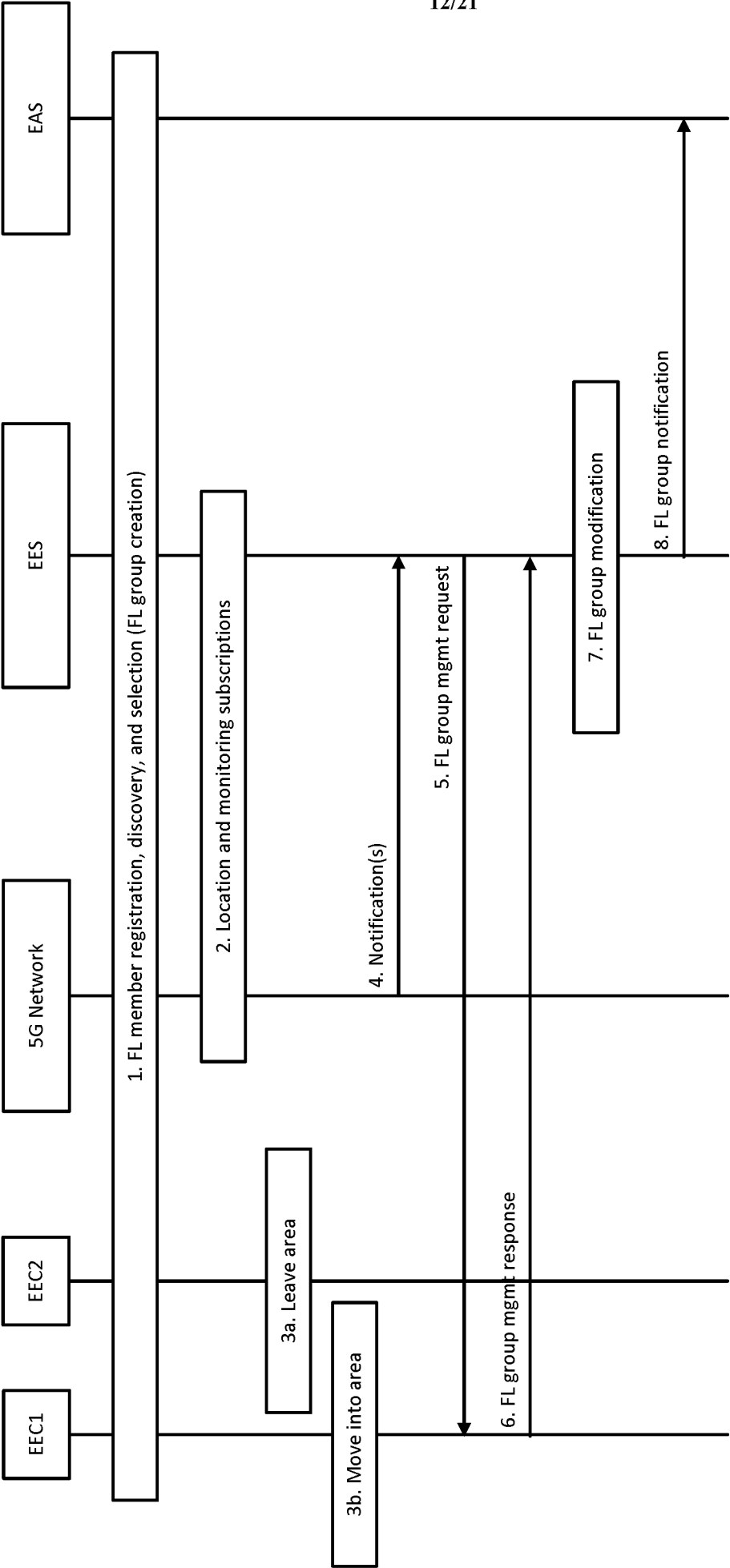


FIG. 12

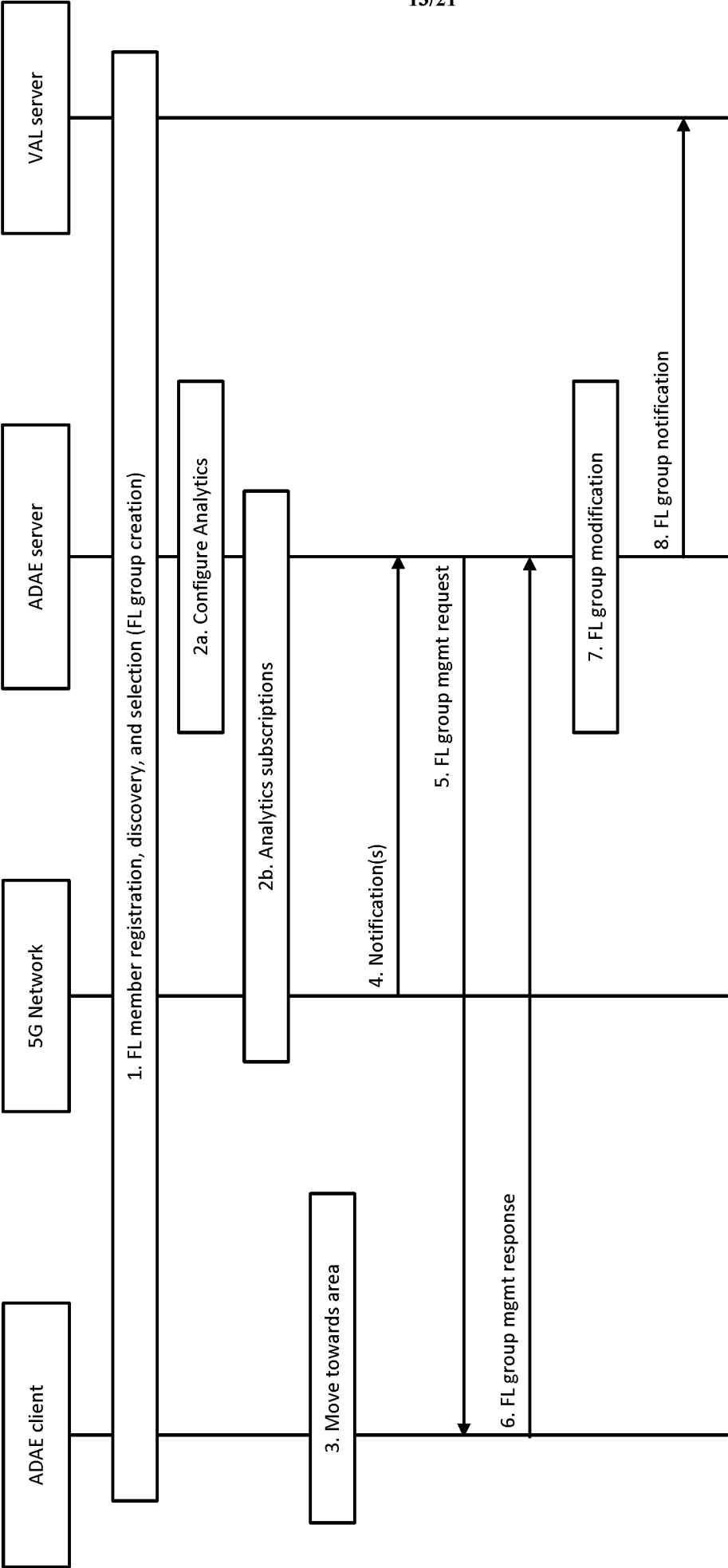


FIG. 13

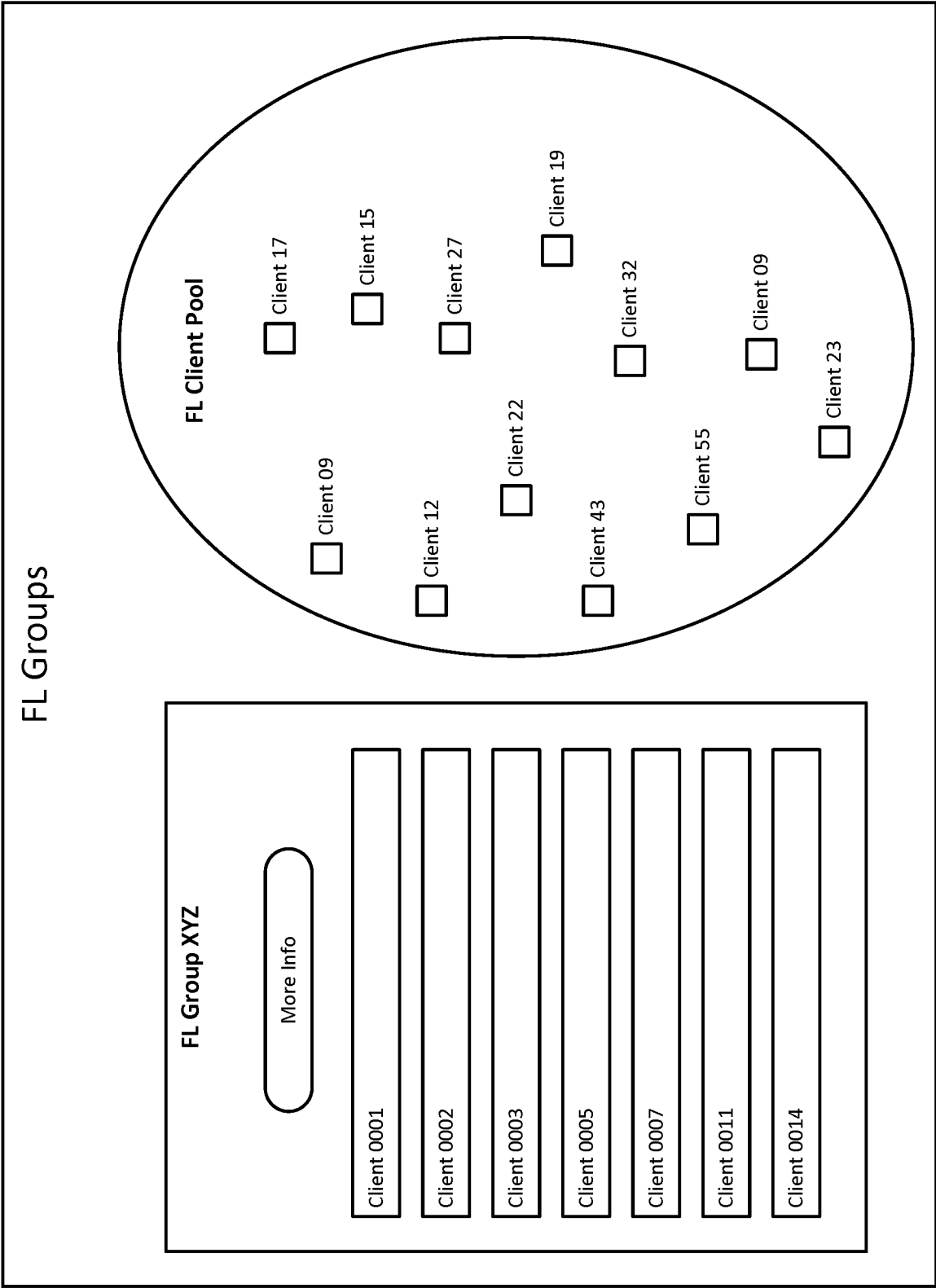


FIG. 14

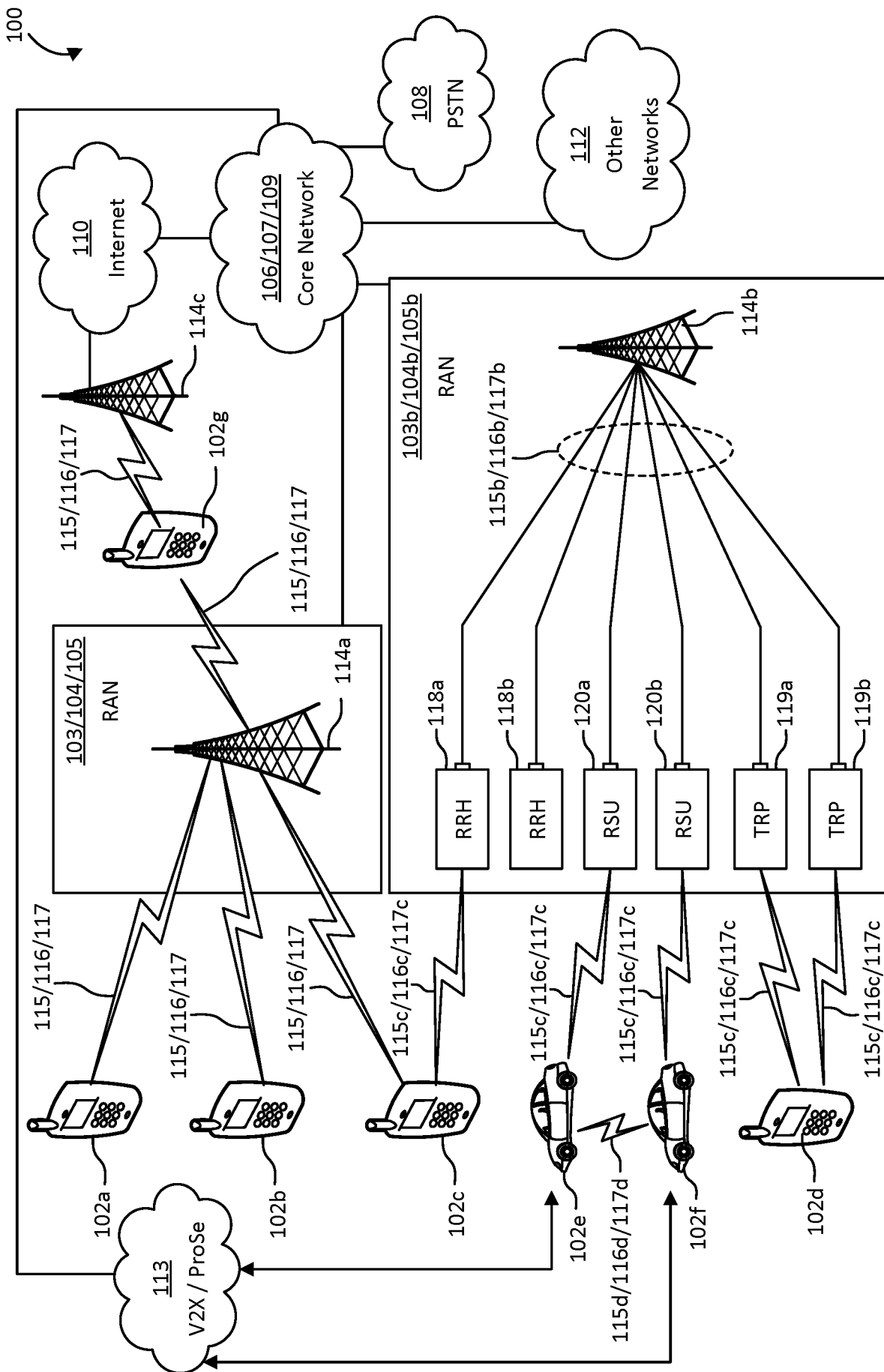


FIG. 15A

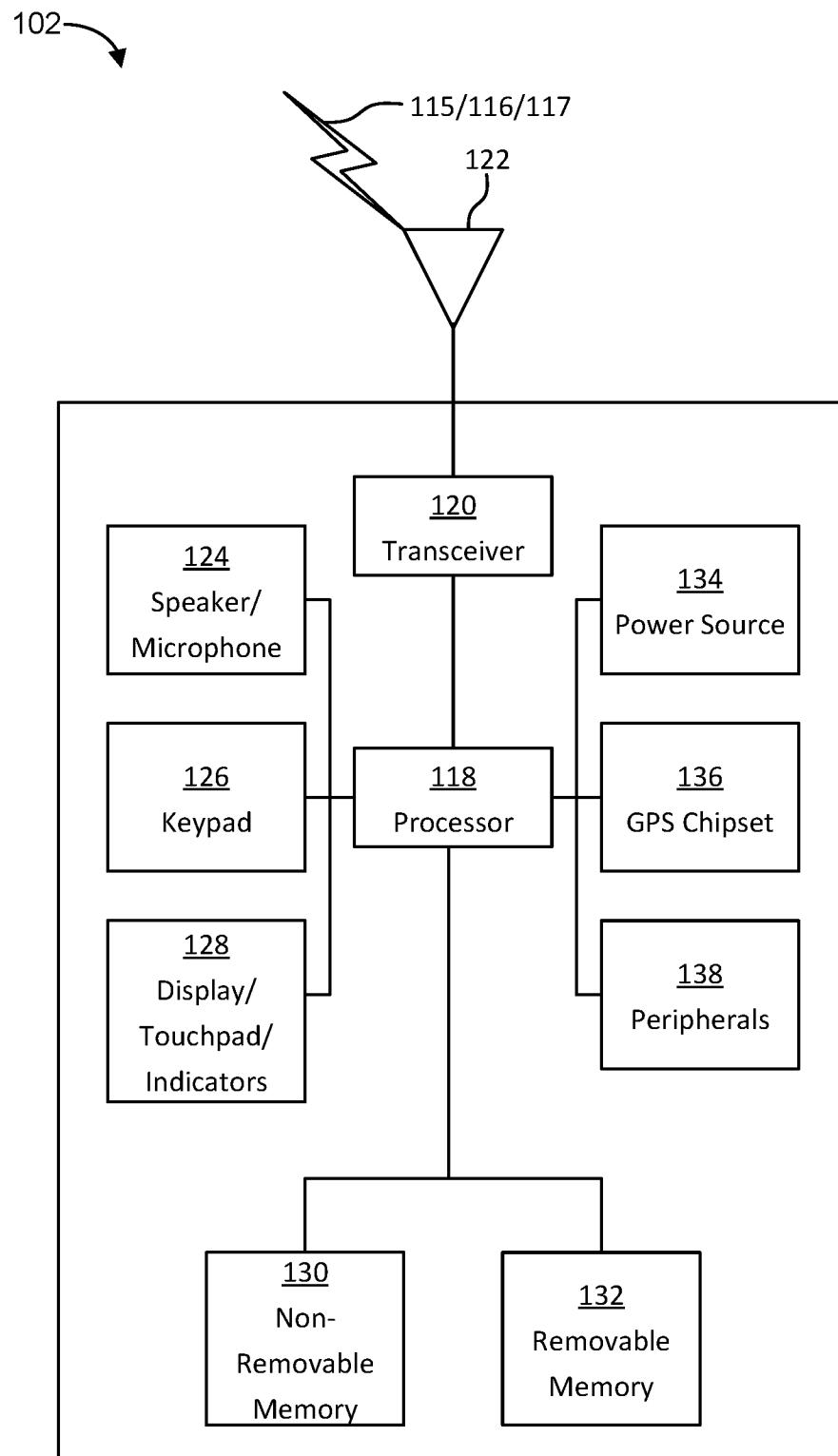


FIG. 15B

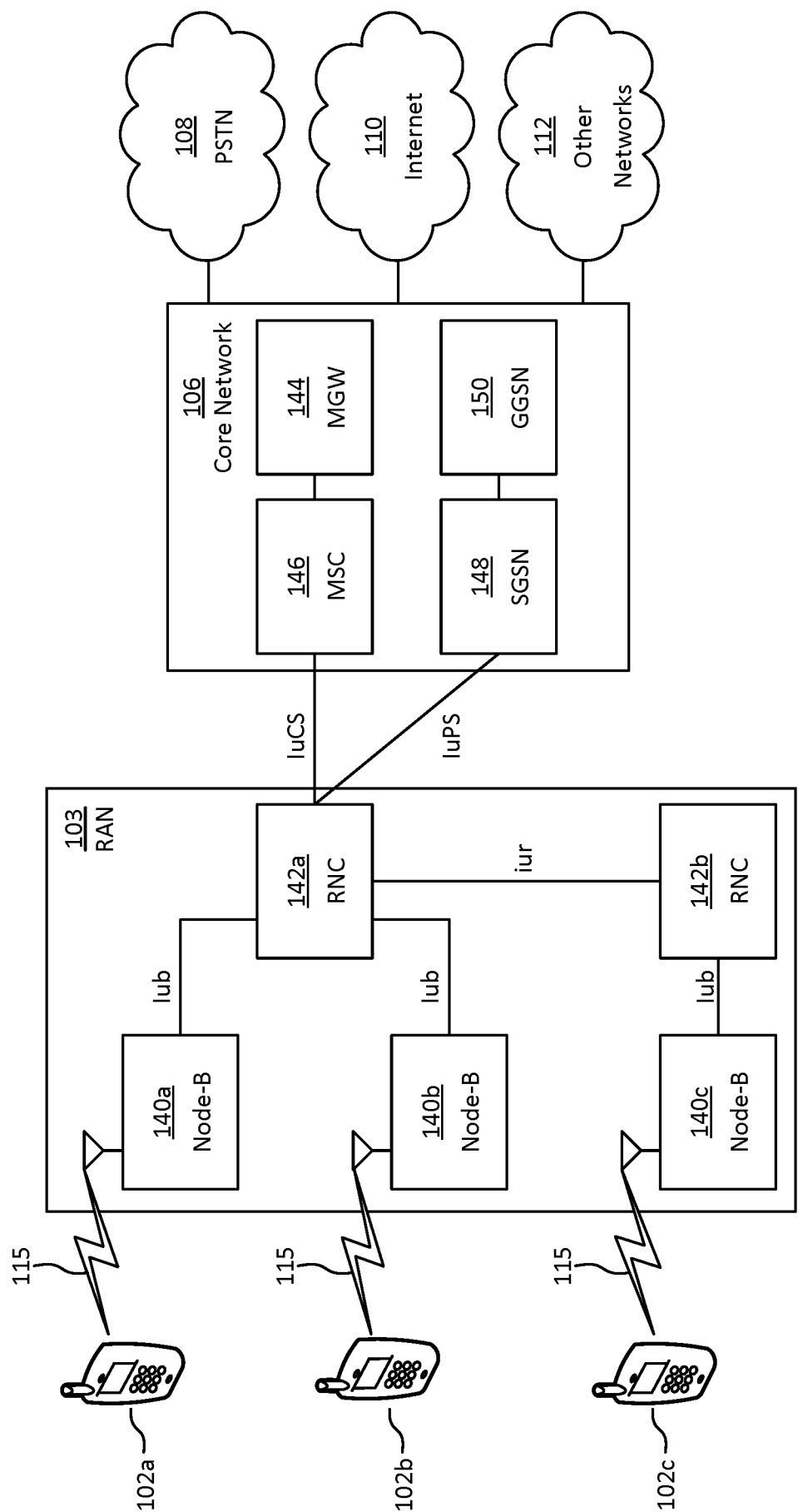


FIG. 15C

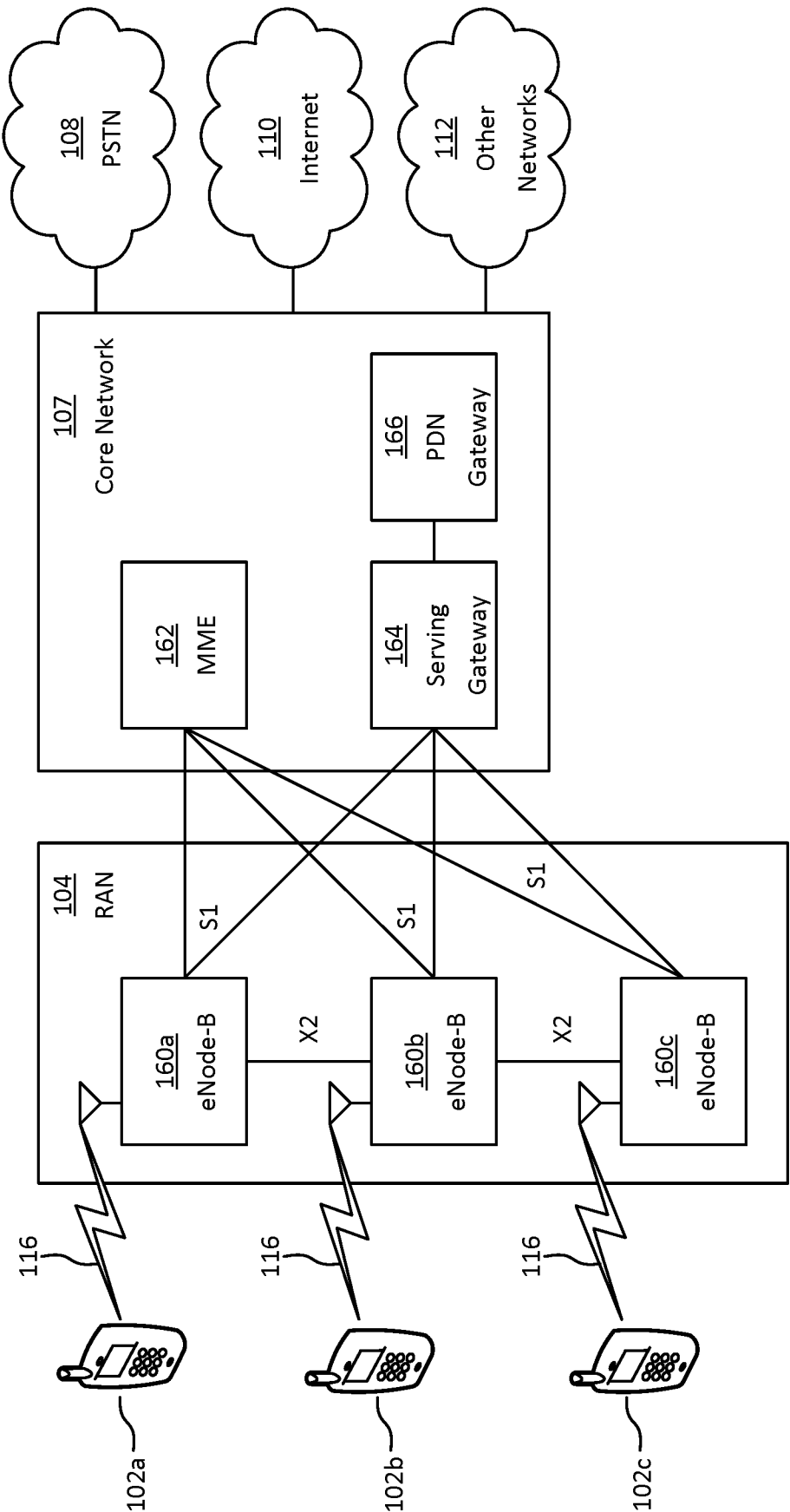


FIG. 15D

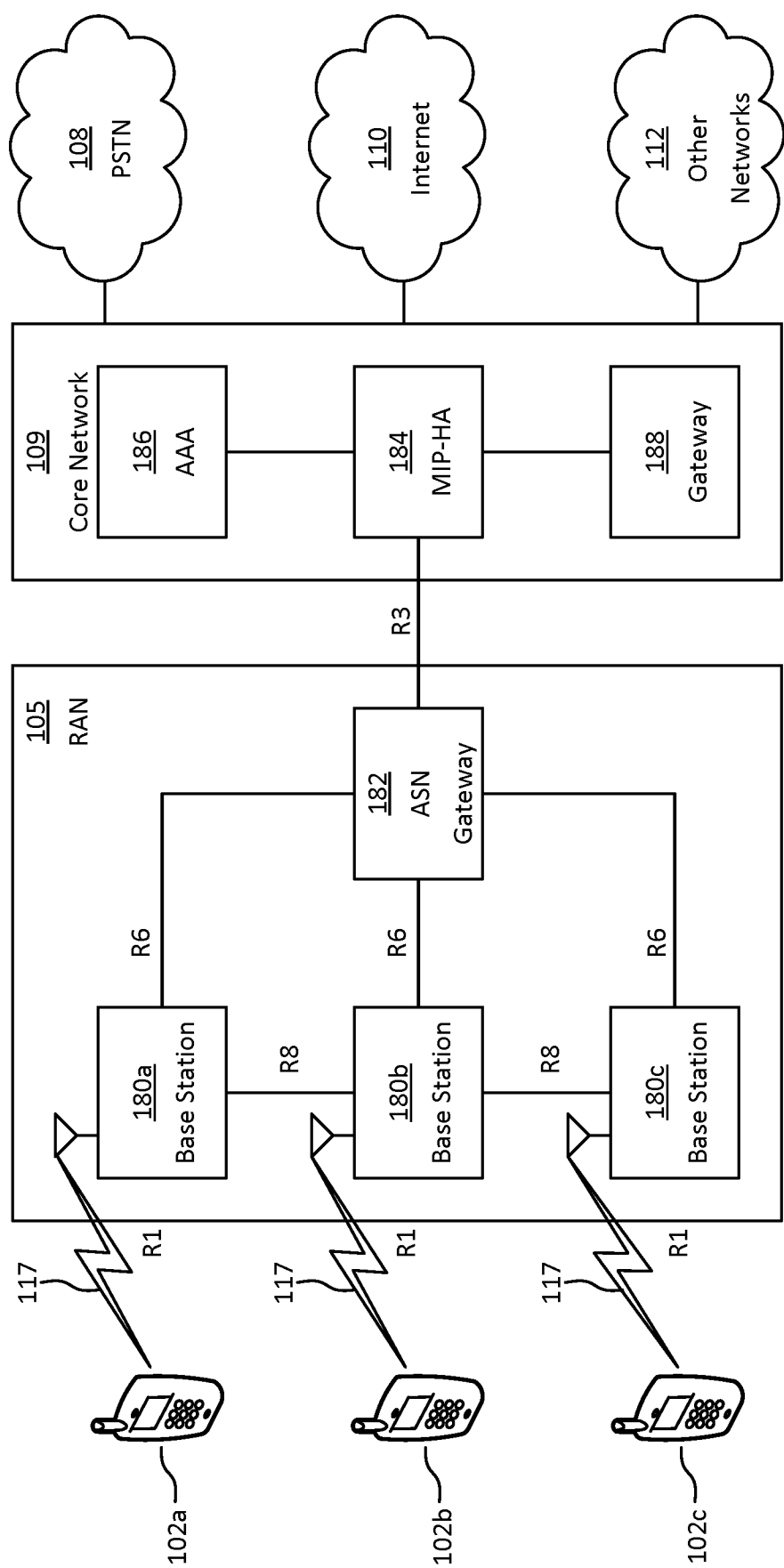


FIG. 15E

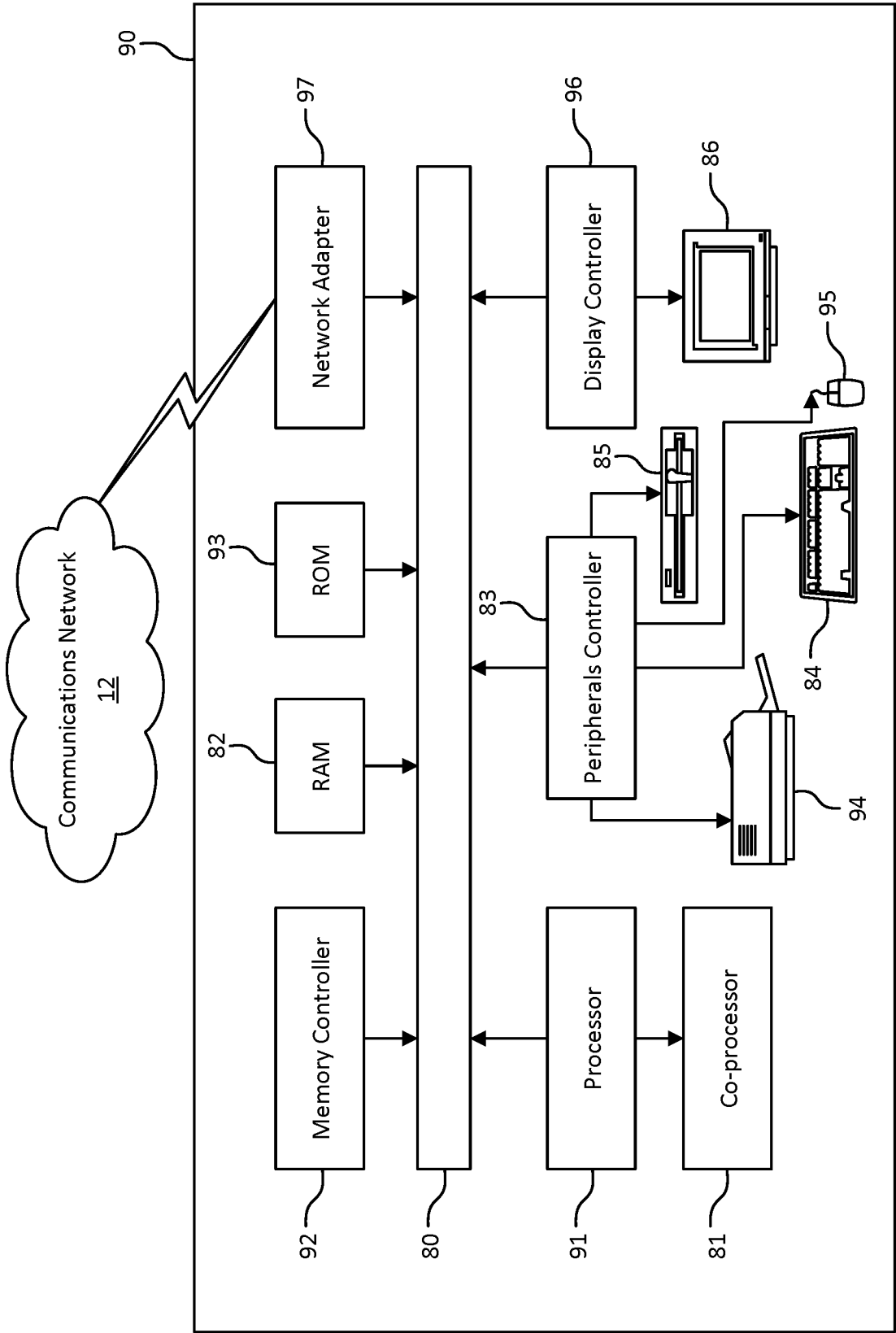


FIG. 15F

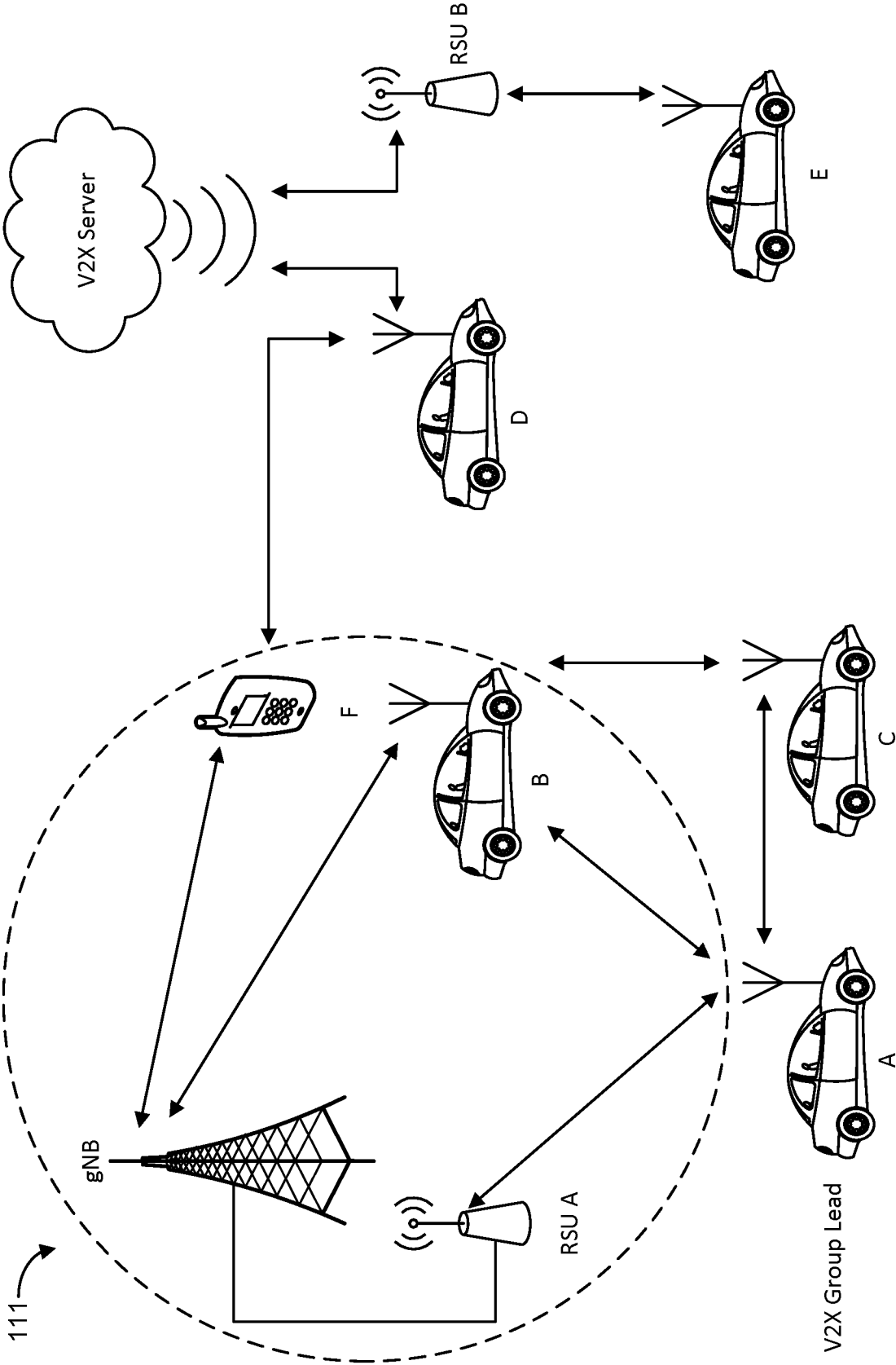


FIG. 15G

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2024/041425

A. CLASSIFICATION OF SUBJECT MATTER INV. H04W4/08 G06N20/00 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04W G06N H04L Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on 5G System Support for AI/ML-based Services (Release 18)", 3GPP STANDARD; TECHNICAL REPORT; 3GPP TR 23.700-80, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , no. V18.0.0 21 December 2022 (2022-12-21), pages 1-220, XP052234764, Retrieved from the Internet: URL:https://ftp.3gpp.org/Specs/archive/23_ series/23.700-80/23700-80-i00.zip 23700-80-i00.docx [retrieved on 2022-12-21] page 101 - page 103 - / - -	1 - 20
☒ 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 30 October 2024		Date of mailing of the international search report 12/11/2024
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Jurca, Alexandru

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2024/041425

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	page 110 - page 111 ----- "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study of Enablers for Network Automation for the 5G System (5GS); Phase 3 (Release 18)", 3GPP STANDARD; TECHNICAL REPORT; 3GPP TR 23.700-81, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , no. V18.0.0 21 December 2022 (2022-12-21), pages 1-278, XP052234765, Retrieved from the Internet: URL:https://ftp.3gpp.org/Specs/archive/23_ series/23.700-81/23700-81-i00.zip 23700-81-i00.docx [retrieved on 2022-12-21] section 6.50	1-20
A	----- "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on traffic characteristics and performance requirements for AI/ML model transfer in 5GS (Release 18)", 3GPP STANDARD; TECHNICAL REPORT; 3GPP TR 22.874, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , no. V18.1.0 24 September 2021 (2021-09-24), pages 1-111, XP052056706, Retrieved from the Internet: URL:https://ftp.3gpp.org/Specs/archive/22_ series/22.874/22874-i10.zip 22874-i10.doc [retrieved on 2021-09-24] section 7 ----- -/-	1-20

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2024/041425

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on application layer support for AI/ML services; (Release 19)", 3GPP STANDARD; TECHNICAL REPORT; 3GPP TR 23.700-82, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , no. V19.0.0 25 June 2024 (2024-06-25), pages 1-137, XP052624549, Retrieved from the Internet: URL:https://ftp.3gpp.org/Specs/archive/23_ series/23.700-82/23700-82-j00.zip 23700-82-j00.docx [retrieved on 2024-06-25] sections 8.6, 8.7, 8.10, 8.14, 8.27 -----	1 - 20