



(51) International Patent Classification:

H04L 29/06 (2006.01) H04W 12/12 (2021.01)

(21) International Application Number:

PCT/US2021/033030

(22) International Filing Date:

18 May 2021 (18.05.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

17/076,482 21 October 2020 (21.10.2020) US

(71) Applicant: **ORACLE INTERNATIONAL CORPORATION** [US/US]; 500 Oracle Parkway, Mail Stop 50P7, Redwood Shores, CA 94065 (US).

(72) Inventors: **IDDYA, Arjun**; 'Madhwa Manasa' H-No 2/69/J2, 76 Badagubettu, Near Indiranagar Church, Chitpady, Udupi 576101 (IN). **MAHALANK, Shashikiran, Bha-**

lachandra; Unit No. 003, V2 Vaibhav Apt., Kempamma Layout, 24th Cross, Hulimavu, Bangalore 560076 (IN).

(74) Agent: **HUNT, Gregory, A.**; Jenkins, Wilson, Taylor & Hunt, P.A., 3015 Carrington Mill Boulevard, Suite 550, Morrisville, NC 27560 (US).

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

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

(54) Title: METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR VALIDATING A SESSION MANAGEMENT FUNCTION (SMF) REGISTRATION REQUEST

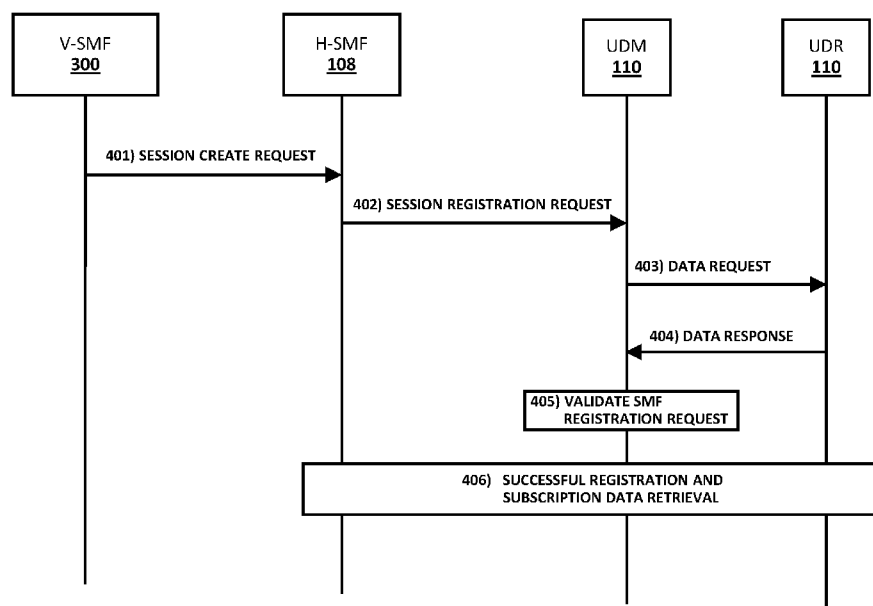


FIG. 4

(57) Abstract: Methods, systems, and computer readable media for validating a session management function (SMF) registration request are disclosed. One method occurs at a network node. The method comprises: receiving, from a first SMF in a home network, a registration request indicating a first network identifier identifying a visited network where a user device is roaming; determining whether the registration request is valid by comparing the first network identifier and a second network identifier associated with an access and mobility management function (AMF) serving the user device; and performing at least one action based on the determining.

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

Published:

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

METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR
VALIDATING A SESSION MANAGEMENT FUNCTION (SMF)
REGISTRATION REQUEST

5

PRIORITY CLAIM

This application claims the priority benefit of U.S. Patent Application Serial No. 17/076,482, filed October 21, 2020, the disclosure of which is incorporated herein by reference in its entirety.

10

TECHNICAL FIELD

The subject matter described herein relates to methods and systems for preventing fraud related to communications networks. More particularly, the subject matter described herein relates to methods, systems, and computer readable media for validating a session management function (SMF) registration request.

15

BACKGROUND

Communications networks can be targeted by malicious actors for a variety of reasons, e.g., financial gain, espionage, or political aims. For example, vulnerabilities associated with “next generation” and current networks (e.g., a third generation partnership project (3GPP) fifth generation (5G) core network) allow some entities to commit revenue fraud, perform unauthorized data interceptions or data taps, and/or steal personal subscriber information. When such issues occur, many times an innocent party may be held responsibility for rectifying and/or mitigating the damage. While network operators generally use security appliances, firewalls, and/or other devices to help prevent unauthorized access to their networks and customers, numerous issues can still exist within their networks due to the inherent security issues associated with protocols and/or procedures used in these networks.

20

25

30

SUMMARY

Methods, systems, and computer readable media for validating a session management function (SMF) registration request are disclosed. One method occurs at a network node. The method comprises: receiving, from a

first SMF in a home network, a registration request indicating a first network identifier identifying a visited network where a user device is roaming; determining whether the registration request is valid by comparing the first network identifier and a second network identifier associated with an access and mobility management function (AMF) serving the user device; and performing at least one action based on the determining.

One system includes a network node. The network node includes at least one processor and memory. The network node is configured for receiving, from a first SMF in a home network, a registration request indicating a first network identifier identifying a visited network where a user device is roaming; determining whether the registration request is valid by comparing the first network identifier and a second network identifier associated with an AMF serving the user device; and performing at least one action based on the determining.

The subject matter described herein can be implemented in software in combination with hardware and/or firmware. For example, the subject matter described herein can be implemented in software executed by a processor. In one example implementation, the subject matter described herein may be implemented using a computer readable medium having stored thereon computer executable instructions that when executed by the processor of a computer control the computer to perform steps. Example computer readable media suitable for implementing the subject matter described herein include non-transitory devices, such as disk memory devices, chip memory devices, programmable logic devices, and application specific integrated circuits. In addition, a computer readable medium that implements the subject matter described herein may be located on a single device or computing platform or may be distributed across multiple devices or computing platforms.

As used herein, the terms 'node' refers to a physical computing platform including one or more processors and memory.

As used herein, the terms 'function' or 'module' refer to software in combination with hardware and/or firmware for implementing features described herein.

BRIEF DESCRIPTION OF THE DRAWINGS

The subject matter described herein will now be explained with reference to the accompanying drawings of which:

Figure 1 is a diagram illustrating an example communications environment for validating a session management function (SMF) registration request;

Figure 2 is a diagram illustrating an example node for validating an SMF registration request;

Figure 3 is a diagram illustrating example messages associated with processing an SMF registration request;

Figure 4 is a diagram illustrating example messages associated with validating an SMF registration request; and

Figure 5 is a diagram illustrating an example process for validating an SMF registration request.

DETAILED DESCRIPTION

The subject matter described herein relates to methods, systems, and computer readable media for validating a session management function (SMF) registration request. Vulnerabilities exist in various communications networks, including mobile communications networks. For example, a malicious network node (e.g., a malicious AMF or SMF) may be programmed or otherwise configured to generate and send a fraudulent session create request (e.g., a Nsmf_PDU_Session_Create message) to a home network of one or more subscribers. In this example, the fraudulent message may be for creating a protocol data unit (PDU) session and may include a subscriber and/or user device identifier (e.g., a subscription permanent identifier (SUPI) or an international mobile subscriber identity (IMSI)) and location information (e.g., a public land mobile network (PLMN) identifier) indicating that the subscriber is roaming in its network. In response to receiving this message, an SMF in the home network may generate and send a registration request (e.g., a Nudm_UECM_Registration message) to a unified data management (UDM) for registering itself as handling the PDU session. Since UDMs do not validate SMF registration requests, a home network or a node therein may act on

fraudulent messages by completing the registration and providing the malicious network node with subscriber data (e.g., a subscriber profile) and/or other information which can be utilized to commit revenue fraud, perform data interception, steal subscriber profile details, and/or other malicious activities.

5 In accordance with some aspects of the subject matter described herein, techniques, methods, systems, or mechanisms are disclosed for validating an SMF registration request. For example, a network node (e.g., a UDM node) may use a registration validation algorithm for determining whether an SMF registration request is invalid, e.g., fraudulent, erroneous,
10 inappropriate, etc. In some embodiments, the registration validation algorithm may involve comparing a first network identifier (e.g., a PLMN identifier of a visited network) located in the registration request and a second network identifier (e.g., a PLMN identifier) associated with an access and mobility management function (AMF) serving the user device. In some embodiments,
15 if an SMF registration request is determined to be invalid or likely to be invalid (e.g., by determining that the first network identifier and the second network identifier do not match), the network node may perform one or more actions, such as discarding the message, averting a registration, notifying a network operator of potential malicious activities, or other mitigating actions.

20 Advantageously, by validating an SMF registration requests and performing one or more mitigating actions when an SMF registration request is determined to be invalid or likely to be invalid, malicious activities and their negative consequences (e.g., revenue fraud) can be avoided and/or prevented. It will be appreciated that various aspects of the subject matter
25 described herein may be implemented in a 5G system network architecture or a network architecture that includes both 5G and non-5G network elements.

Reference will now be made in detail to various embodiments of the subject matter described herein, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers
30 will be used throughout the drawings to refer to the same or like parts.

Figure 1 is a diagram illustrating an example communications environment **100** for validating an SMF registration request. Figure 1 includes a UE **102** (e.g., a mobile device, a computer, a tablet computing platform, or a

smartphone) capable of roaming or moving between different portions of a communications environment **100**. In some embodiments, communications environment **100** may include one or more nodes associated with a fifth generation (5G) network with one or more entities having at least some functionality defined in one or more third generation partnership project (3GPP) technical specifications (TS), e.g., 3GPP TS 23.502 V16.6.0 (2020-09), 3GPP TS 23.501 V16.6.0 (2020-09), or 3GPP TS 29.502 V16.5.0 (2020-09).

Communications environment **100** may include a home network (e.g., a home public land mobile network (HPLMN)) and a visited network (e.g., a visited public land mobile network (VPLMN)). The home network may be associated with UE **102** and may be the UE's default network, while the visited network may be a network that UE **102** may use, may attempt to use, or may appear to use while roaming outside the home network's coverage area. In some embodiments, the home network and the visited network may include nodes for communicating with an external network, such as Internet **116**.

In some embodiments, a home network and/or its related nodes may be configured to handle data services (e.g., Internet access or a PDU session), e.g., even when its subscribers are using a visited network for voice services. For example, a home network may handle data services for a roaming subscriber by routing a data flow service request through its network regardless of whether a visited network can provide the same services.

The visited network may include an access network **104**, an AMF **106**, a visited network SMF (V-SMF) **107**, and a visited network user data plane function (V-UPF) **112**. Access network **104** may represent a radio access network (e.g., a next-generation radio access network (NG-RAN)) and may include various nodes for communicating with UE **102** and elements within communications environment **100**. Example nodes in access network **104** may include a next generation node B (gNB), a next generation evolved node B (ng-eNB), or other transceiver node, which may perform radio access functions. Access network **104**, or nodes therein, may be used for communications between UE **102** and nodes in the visited network or communications environment **100**, e.g., AMF **106**. For example, a gNB or

other node (e.g., a gateway) may communicate UE-related messages (e.g., authentication or mobility related messages) to AMF **106** or other nodes.

AMF **106** represents a node or gateway for facilitating communications between access network **104** and other nodes (e.g., V-UPF **112**) or networks.

5 In some embodiments, AMF **106** may communicate user traffic to other nodes in communications environment **100**. In some embodiments, AMF **106** may also perform one or more mobility management functions, e.g., similar to those performed by a mobility management entity (MME) in 4G networks. In some embodiments, AMF **106** may forward session management
10 requirements and/or related messages to V-SMF **107**, e.g., via an N11 interface.

V-SMF **107** may represent any suitable entity or entities for performing one or more session management functions. For example, V-SMF **107** may interact with nodes in a decoupled data plane for creating, updating, and/or
15 removing PDU sessions and/or for managing session contexts with V-UPF **112**. In some embodiments, V-SMF **107** may communicate session related information to a home network SMF (H-SMF) **108** or other nodes in communications environment **100** for performing of facilitating various session management functions. For example, during a home-network routing scenario
20 and after receiving a Nsmf_PDUSession_CreateSMContext request from AMF **106**, V-SMF **107** may send a Nsmf_PDUSession_Create request to H-SMF **108** containing various information, e.g., a visited network PLMN identifier, a PDU session identifier, a UE identifier, and a V-SMF identifier. In this example, after storing an association between a PDU session identifier
25 and V-SMF **107**, H-SMF **108** may send a registration request (e.g., using a Nudm_UECM_Registration request) to UDM **110** for performing authentication and/or for registering itself as handling the PDU session.

V-UPF **112** may be any suitable entity for providing access to Internet **116** or other data networks, e.g., an Internet access point. In some
30 embodiments, if AMF **106** may route IP traffic and/or related messages destined for Internet **116** via V-UPF **112** in the visited network. In some embodiments, e.g., if the home network is to handle data services for a roaming subscriber, AMF **106** may route IP traffic and/or related messages

destined for Internet **116** via a home network user data plane function (H-UPF) **114** instead of via V-UPF **112**.

5 The home network may include various nodes, e.g., H-SMF **108**, a UDM **110**, H-UPF **114**, and a user data repository (UDR) **118**. In some embodiments, a home network may be configured as a subscriber's default roaming provider. In some embodiments, a home network may be configured to allow a subscriber to change his roaming provider, e.g., for a certain or specified period of time.

10 H-SMF **108** may represent any suitable entity or entities for performing one or more session management functions. For example, H-SMF **108** may interact with nodes in a decoupled data plane for creating, updating, and/or removing PDU sessions and/or for managing session contexts with V-UPF **112**. In some embodiments, H-SMF **108** may facilitate various session management functions associated with V-SMF **107**, e.g., when UE **102** is
15 roaming. For example, during a home-network routing scenario and after receiving a Nsmf_PDUSession_Create request from V-SMF **107**, H-SMF **108** may store an association between a PDU session identifier and V-SMF **107** and then send a registration request (e.g., using a Nudm_UECM_Registration request) to UDM **110** for performing authentication and/or for registering itself
20 as handling the PDU session.

H-UPF **114** may be any suitable entity for providing access to Internet **116** or other data networks, e.g., an Internet access point. In some embodiments, e.g., if the home network is handling data services for a roaming subscriber, AMF **106** may route IP traffic and/or related messages
25 destined for Internet **116** via H-UPF **114** in the home network.

UDM **110** may represent any suitable entity or entities for managing user data, e.g., for access authorization, user registration, and/or data network profiles. In some embodiments, UDM **110** may include a stateful implementation where subscriber data is stored locally or may be a stateless
30 or semi-stateless implementation where subscriber data is stored remotely, e.g., at UDR **118**. In some embodiments, UDM **110** or related entity (e.g., UDR **118**) may maintaining and/or providing one or more subscriber data management (SDM) or customer relationship management (CRM) functions.

UDM **110** or related entity (e.g., UDR **118**) may manage or provide subscriber-related information, such as user identification, control information for user authentication and authorization, UE location information, and user profile data. In some embodiments, UDM **110** may include or interact with an authentication server function (AUSF) that performs authentication services for UEs, such as UE **102**.

UDR **118** may represent any suitable entity or entities for storing data for access authorization, user registration, and/or data network profile information. For example, UDR **118** may maintain or store subscriber-related information, such as user identification, control information for user authentication and authorization, UE location information, and user profile data. In this example, UDR **118** may include or utilize a database containing details about a subscriber identity module (SIM) card associated with UE **102**, services available to UE **102**, and the current location (e.g., current serving node) of UE **102**.

In some embodiments, where UDM **110** or UDR **118** involves multiple nodes, each node may manage and/or maintain information for a portion of subscribers, e.g., hundreds of thousands to millions of subscribers and various nodes in communications environment **100** may be configured to identify and consult the appropriate node for information about a particular subscriber.

In some embodiments, UDM **110** may perform session and/or network registration procedures in response to receiving a registration request or other messages. For example, when UE **102** is roaming in a visited network, a registration request may be sent from H-SMF **108** in response to receiving a session create request from V-SMF **107**.

In some embodiments, UDM **110** may include functionality for performing a validation analysis on a registration message, e.g., sent by H-SMF **108**. For example, UDM **110** may be configured to analyze a header or payload portion of an SMF registration message and retrieve location information about a visited network (e.g., where UE **102** is roaming). In this example, UDM **110** may perform a validation analysis that includes executing one or more validation algorithms and/or rules for determining whether the

SMF registration message or related information is valid or appears to be valid.

In some embodiments, a network identifier or related information may include any information usable for identifying a location of UE **102** or an associated subscriber. For example, a network identifier or related information may include a PLMN identifier, a mobile country code (MCC) a mobile network code (MNC), a location area code (LAC), a network identifier, a cell global identifier (CGI), a base station identifier (BSID), an access node identifier, a cell identity (CI), a service area code (SAC), a routing area identity (RAI), a routing area code (RAC), a tracking area identity (TAI), a tracking area code (TAC), an eUTRAN CGI (EGCI), location coordinates (e.g., global positioning system (GPS) information), and/or relative location information.

In some embodiments, a validation analysis or related algorithm may determine whether an SMF registration request is valid (or appears valid) by comparing a network identifier or related information indicated by the registration request as being where UE **102** is located and another network identifier or related information indicated by another source (e.g., UDR **118**) as being where UE **102** is located. For example, determining that an SMF registration request is valid may involve confirming that the SMF registration request indicated the same visited network as a distinct or separate known reliable source (e.g., UDR **118**).

For example, a validation analysis may involve comparing a first PLMN identifier indicated by or contained in an SMF registration request and a second PLMN identifier obtained by querying or accessing UDR **118**. In this example, the second PLMN identifier may identify the network where AMF **106** is serving the same UE associated with the registration request, e.g., this information may be trusted and/or previously provided to UDR **118** by a trusted node or procedure. Continuing with this example, if the first network identifier and the second network identifier match (e.g., they identify the same network), then the validation analysis or related algorithm may determine that the SMF registration request is valid. However, if the first network identifier and the second network identifier do not match (e.g., they identify different

networks), then the validation analysis or related algorithm may determine that the SMF registration request is invalid.

In some embodiments, UDM **110** may be configured to perform one or more actions based on a validation analysis or a related determination. For example, in response to determining that an SMF registration request is valid, UDM **110** may initiate or perform registration based on the registration request. In another example, in response to determining that an SMF registration request is invalid, UDM **110** may screen, filter, or discard an SMF registration request or a related message, may avert a registration based on the registration request, may send a notification message to a management or security node indicating that the registration request is invalid, may send a notification message to a management or security node indicating that a related node is potentially malicious, or may copy or store a portion of the registration request.

It will be appreciated that Figure 1 is for illustrative purposes and that various nodes and/or modules, locations, and/or functionality described above in relation to Figure 1 may be changed, altered, added, or removed.

Figure 2 is a diagram illustrating an example node **200** for validating an SMF registration request. Node **200** may represent any suitable entity or entities for performing aspects of validating an SMF registration request. In some embodiments, node **200** may represent or include UDM **110**, UDR **118**, an AUSF, or another node or function.

Referring to Figure 2, node **200** may include one or more communications interface(s) **202** for communicating messages via communications environment **100**, e.g., a 5G core network. In some embodiments, communications interface(s) **202** may include a first communication interface for communicating with UDR **118** and a second communications interface for communicating with H-SMF **108**.

Node **200** may include a registration validation engine (RVE) **204**. RVE **204** may be any suitable entity (e.g., software executing on at least one processor) for performing one or more aspects of validating an SMF registration request. In some embodiments, RVE **204** may include functionality for identifying messages that contain subscriber location

information, such as mobility management messages from roaming subscribers. For example, RVE **204** may identify relevant messages by filtering message based on header data and/or payload data.

5 In some embodiments, RVE **204** may include functionality for performing a validation analysis on a registration message, e.g., sent by H-SMF **108**. For example, RVE **204** may be configured to analyze a header or payload portion of an SMF registration message and retrieve location information about a visited network (e.g., where UE **102** is roaming). In this example, RVE **204** may perform a validation analysis that includes executing
10 one or more validation algorithms and/or rules for determining whether the SMF registration message or related information is valid or appears to be valid.

In some embodiments, a network identifier or related information may include any information usable for identifying a location of UE **102** or an
15 associated subscriber. For example, a network identifier or related information may include a PLMN identifier, an MCC, an MNC, an LAC, a network identifier, a CGI, a BSID, an access node identifier, a CI, an SAC, an RAI, an RAC, a TAI, a TAC, an EGCI, location coordinates (e.g., GPS information), and/or relative location information.

20 In some embodiments, a validation analysis or related algorithm may determine whether an SMF registration request is valid (or appears valid) by comparing a network identifier or related information indicated by the registration request as being where UE **102** is located and another network identifier or related information indicated by another source (e.g., UDR **118**)
25 as being where UE **102** is located. For example, determining that an SMF registration request is valid may involve confirming that the SMF registration request indicated the same visited network as a distinct or separate known reliable source (e.g., UDR **118**).

For example, a validation analysis may involve comparing a first PLMN
30 identifier indicated by or contained in an SMF registration request and a second PLMN identifier obtained by querying or accessing UDR **118**. In this example, the second PLMN identifier may identify the network where AMF **106** is serving the same UE associated with the registration request.

Continuing with this example, if the first network identifier and the second network identifier match (e.g., they identify the same network), then the validation analysis or related algorithm may determine that the SMF registration request is valid. However, if the first network identifier and the second network identifier do not match (e.g., they identify different networks), then the validation analysis or related algorithm may determine that the SMF registration request is invalid.

In some embodiments, RVE **204** may be configured to perform one or more actions based on a validation analysis or a related determination. For example, in response to determining that an SMF registration request is valid, RVE **204** may perform or initiate registration based on the registration request. In another example, in response to determining that an SMF registration request is invalid, RVE **204** may screen, filter, or discard an SMF registration request or a related message, may avert a registration based on the registration request, may send a notification message to a management or security node indicating that the registration request is invalid, may send a notification message to a management or security node indicating that a related node is potentially malicious, or may copy or store a portion of the registration request.

Node **200** may access (e.g., read from and/or write information to) data storage **206**. Data storage **206** may be any suitable entity (e.g., a computer readable medium or memory) for storing various data. In some embodiments, data storage **206** may include registration related validation rules and/or policies. Data storage **206** may include information or logic for determining whether an SMF registration request is valid or invalid. Example information or logic usable in determining whether an SMF registration request is valid or invalid may include historical (e.g., prior) location information associated with a UE or a related node (e.g., AMF **106** or V-SMF **107**) and/or logic to access or query one or more relevant databases or nodes, e.g., UDR **118**, for obtaining various subscriber related information, e.g., an identifier for identifying the AMF currently serving a UE and/or an identifier for identifying a network associated with that AMF.

Data storage **206** may include UE related network information. For example, Data storage **206** may include mappings of PLMN identifiers, APNs, or other network identifiers and valid location information (e.g., MCC and/or MNCs). In some embodiments, a home network may store an approved
5 access list of valid network identifiers or related information that roaming subscribers can use to receive data services or other services. In this example, node **200** or another node may access UE related network information to determine whether a registration request is associated with an appropriate network identifier. If the location information is associated with an
10 appropriate network identifier in the approved access list, the registration request may be determined to be valid.

In some embodiments, a home network may store a blocked access list of invalid network identifiers or related information that roaming subscribers cannot use to receive data services or other services. In this example, node
15 **200** or another node may access UE related network information to determine whether a registration request is associated with an inappropriate network identifier. If the location information is associated with a network identifier in the blocked access list, the registration request may be determined to be invalid.

20 It will be appreciated that Figure 2 and its related description are for illustrative purposes and that node **200** may include additional and/or different modules, components, or functionality.

Figure 3 is a diagram illustrating example messages associated with processing an SMF registration request. In some embodiments, a session
25 create request may be provided or initiated by a V-SMF **300**, which may or may not be controlled by a malicious actor and/or used for malicious activities (e.g., revenue fraud and/or data interception). In some embodiments, V-SMF **300** may have or appear to have similar functionality as described above with regard to V-SMF **107**.

30 Referring to Figure 3, a portion of a PDU session creation procedure for a home routed roaming scenario is generally depicted. An example PDU session creation procedure for a home routed roaming scenario is defined in Section 4.3.2.2.2 of 3GPP TS 23.502 V16.6.0 (2020-09).

In step **301**, a potentially fraudulent session create request (e.g., a Nsmf_PDU_Session_Create message) may be sent from V-SMF **300** to H-SMF **108**. In some embodiments, the session create request may include a visited network PLMN identifier, a PDU session identifier, a UE identifier, and/or a V-SMF identifier.

In step **302**, a registration request (e.g., a Nudm_UECM_Registration request) may be sent from H-SMF **108** to UDM **110**. For example, after receiving a session create request from V-SMF **300**, H-SMF **108** may store an association between a PDU session identifier and V-SMF **300** and may then send a registration request (e.g., using a Nudm_UECM_Registration request) to UDM **110** for registering itself as handling the PDU session.

In step **303**, a successful registration and subscription data retrieval may occur. For example, a successful registration may occur when a success response to the registration request is received by H-SMF **108**. In this example, V-SMF **300** may be capable of obtaining subscription data from UDM **110** or UDR **118** via H-SMF **108**.

As shown, a potential security risk is evident in the message flow of Figure 3. For example, when H-SMF **108** registers itself with UDM **110** for a given PDU session identifier associated with roaming UE **102**, H-SMF **108** does not check with UDM **110** to confirm that the AMF that has triggered the registration request (e.g., by sending a Nsmf_PDUSession_CreateSMContext Request to V-SMF **300** which triggered V-SMF **300** to send a Nsmf_PDU_Session_Create message which in turn triggered H-SMF **108** to send the Nudm_UECM_Registration request) is registered for that UE with UDM. Further, UDM **110** allows successful SMF registration even if AMF **106** has not performed access registration using a UECM registration procedure. As such, since UDM **110** does not validate an SMF registration request, an attacker could send a fake Nsmf_PDUSession_Create Request to H-SMF **108**, thus registering themselves with UDM **110**.

It will be appreciated that Figure 3 is for illustrative purposes and that different and/or additional messages and/or actions may be used. It will also

be appreciated that various messages and/or actions described herein may occur in a different order or sequence.

Figure 4 is a diagram illustrating example messages associated with validating an SMF registration request. In some embodiments, a session create request may be provided or initiated by a V-SMF **300**, which may or may not be controlled by a malicious actor and/or used for malicious activities (e.g., revenue fraud and/or data interception). In some embodiments, V-SMF **300** may have or appear to have similar functionality as described above with regard to V-SMF **107**.

In some embodiment, UDM **110** may determine whether a received SMF registration request is valid and may perform various actions based on this determination. In some embodiments, UDM **110** may include RVE **204** and be configured to analyze SMF registration requests.

Referring to Figure 4, a portion of a PDU session creation procedure for a home routed roaming scenario with SMF registration request validation is generally depicted.

In step **401**, a potentially fraudulent session create request (e.g., a Nsmf_PDU_Session_Create message) may be sent from V-SMF **300** to H-SMF **108**. In some embodiments, the session create request may include a visited network PLMN identifier, a PDU session identifier, a UE identifier, and/or a V-SMF identifier.

In step **402**, a registration request (e.g., a Nudm_UECM_Registration request) may be sent from H-SMF **108** to UDM **110**. For example, after receiving a session create request from V-SMF **300**, H-SMF **108** may store an association between a PDU session identifier and V-SMF **300** and may then send a registration request (e.g., using a Nudm_UECM_Registration request) to UDM **110** for registering itself as handling the PDU session.

In some embodiments, e.g., after UDM **110** receives a registration request from H-SMF **108**, UDM **110** may validate a registration request by verifying that an AMF registered as serving a given UE has a same network identifier (e.g., PLMN identifier) as that of a requesting or trigger V-SMF **300**. In such embodiments, a network identifier associated with the AMF registered as serving a given UE may be received in Amf3GppAccessRegistration data

from UDR **118**, e.g., using a GET request. If the PLMN identifiers match, then UDM **110** may proceed with processing the registration request. However, if PLMN identifiers do not match, then UDM **110** may perform one or more mitigating actions may be performed, e.g., do not proceed with processing the registration request.

In step **403**, a data request may be sent from UDM **110** to UDR **118** for requesting a network identifier associated with an AMF serving a UE that corresponds to the registration request.

In step **404**, a data response may be sent from UDR **118** to UDM **110** for providing the requested network identifier associated with an AMF serving a UE that corresponds to the registration request.

In step **405**, UDM **110** may validate the registration request by verifying that the network identifier obtained from the UDR **118** matches the network identifier indicated by the registration request.

In step **406**, if a registration request is determined to be valid, a successful registration and subscription data retrieval may occur. For example, a successful registration may occur when a success response to the registration request is received by H-SMF **108**. In this example, V-SMF **300** may be capable of obtaining subscription data from UDM **110** or UDR **118** via H-SMF **108**.

It will be appreciated that Figure 4 is for illustrative purposes and that different and/or additional messages and/or actions may be used. It will also be appreciated that various messages and/or actions described herein may occur in a different order or sequence.

Figure 5 is a diagram illustrating an example process **500** for validating an SMF registration request. In some embodiments, example process **500** described herein, or portions thereof, may be performed at or performed by UDM **110**, node **200**, RVE **204**, and/or another module or node.

Referring to example process **500**, in step **502**, a registration request indicating a first network identifier identifying a visited network where a user device is roaming may be received from a first SMF in a home network.

In some embodiments, a registration request may include a Nudm_UECM_Registration request.

In step **504**, it may be determined whether the registration request is valid by comparing the first network identifier and a second network identifier associated with an AMF serving the user device.

In some embodiments, a second network identifier may be included in
5 Amf3GppAccessRegistration data obtained from UDR **110**.

In some embodiments, determining that a second SMF or a registration request is valid may include determining that a first network identifier and a second network identifier match.

In some embodiments, determining that a registration request is invalid
10 may include determining that a first network identifier and a second network identifier do not match.

In step **506**, at least one action may be performed based on the determining. For example, if location information is determined to be invalid, one or more mitigating actions may be performed, e.g., to prevent or minimize
15 malicious activities.

In some embodiments, performing at least one action based on a registration related validation determination may include in response to determining that a registration request is valid, performing a registration based on the registration request.

20 In some embodiments, performing at least one action based on a registration related validation determination may include in response to determining that a registration request is invalid, discarding the registration request, averting a registration based on the registration request, sending a notification message to a management or security node indicating that the
25 registration request is invalid, sending a notification message to a management or security node indicating that a related node is potentially malicious, or copying or storing a portion of the registration request.

In some embodiments, a first network identifier or a second network identifier may include a PLMN identifier or a PLMN code.

30 In some embodiments, a network node may include wherein the network node includes a UDM node, an AUSF, or a UDR.

It will be appreciated that process **500** is for illustrative purposes and that different and/or additional actions may be used. It will also be appreciated

that various actions described herein may occur in a different order or sequence.

It will be appreciated that while some aspects of the subject matter described herein has been discussed with reference to 5G networks various other networks may utilize some aspects of the subject matter described herein. For example, any network that utilize registration requests and/or includes a UDM-like and/or UDR-like node may use features, mechanisms and techniques described herein to validate (e.g., screen or filter) registration requests.

It should be noted that UDM **110**, node **200**, RVE **204**, and/or functionality described herein may constitute a special purpose computing device. Further, UDM **110**, node **200**, RVE **204**, and/or functionality described herein can improve the technological field of network security and/or fraud prevention. For example, by validating an SMF registration request and performing one or more mitigating actions when an SMF registration request is determined to be invalid or likely to be invalid, malicious activities and their negative consequences (e.g., revenue fraud) can be mitigated and/or prevented.

The disclosure of each of the following references is incorporated herein by reference in its entirety to the extent not inconsistent herewith and to the extent that it supplements, explains, provides a background for, or teaches methods, techniques, and/or systems employed herein.

References:

1. 3GPP TS 23.501; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2 (Release 16) V16.6.0 (2020-09)
2. 3GPP TS 23.502; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS); Stage 2 (Release 16) (2020-03) V16.6.0 (2020-09)

3. 3GPP TS 29.502, Technical Specification Group Core Network and Terminals; 5G System, Session Management Services, Stage 3, (Release 16) V16.5.0 (2020-09)

5 It will be understood that various details of the subject matter described herein may be changed without departing from the scope of the subject matter described herein. Furthermore, the foregoing description is for the purpose of illustration only, and not for the purpose of limitation.

CLAIMS

What is claimed is:

1. A method for validating a session management function (SMF) registration request, the method comprising:
5 at a network node:
receiving, from a first session management function (SMF) in a home network, a registration request indicating a first network identifier identifying a visited network where a user device is roaming;
determining whether the registration request is valid by
10 comparing the first network identifier and a second network identifier associated with an access and mobility management function (AMF) serving the user device; and
performing at least one action based on the determining.
2. The method of claim 1 wherein the second network identifier is
15 included in Amf3GppAccessRegistration data obtained from a user data repository (UDR).
3. The method of claim 1 or claim 2, wherein determining that the registration request is valid includes determining that the first network identifier and the second network identifier match.
- 20 4. The method of any preceding claim, where determining that the registration request is invalid includes determining that the first network identifier and the second network identifier do not match.
5. The method of any preceding claim, wherein performing the at least one action includes in response to determining that the registration
25 request is valid, performing a registration based on the registration request.
6. The method of any preceding claim, wherein performing the at least one action includes in response to determining that the registration request is invalid, discarding the registration request, averting a
30 registration based on the registration request, sending a notification message to a management or security node indicating that the registration request is invalid, sending a notification message to a management or security node indicating that a related node is

- potentially malicious, or copying or storing a portion of the registration request.
7. The method of any preceding claim, wherein the first network identifier or the second network identifier includes a public land mobile network (PLMN) identifier or a PLMN code.
8. The method of any preceding claim, wherein the registration request includes a Nudm_UECM_Registration request.
9. The method of any preceding claim, wherein the network node includes a unified data management (UDM) node, an authentication server function (AUSF), or a user data repository (UDR).
10. A system for validating a session management function (SMF) registration request, the system comprising:
a network node comprising:
at least one processor; and
a memory,
wherein the network node is configured for:
receiving, from a first session management function (SMF) in a home network, a registration request indicating a first network identifier identifying a visited network where a user device is roaming;
determining whether the registration request is valid by comparing a first network identifier and a second network identifier associated with an access and mobility management function (AMF) serving the user device; and
performing at least one action based on the determining.
11. The system of claim 10 wherein the second network identifier is included in Amf3GppAccessRegistration data obtained from a user data repository (UDR).
12. The system of claim 10 or claim 11, wherein the network node is configured for determining that the registration request is valid by determining that the first network identifier and the second network identifier match.
13. The system of any of claims 10 to 12, wherein the network node is configured for determining that the registration request is invalid by

determining that the first network identifier and the second network identifier do not match.

14. The system of any of claims 10 to 13, wherein the network node is configured for:

5 in response to determining that the registration request is valid, performing a registration based on the registration request.

15. The system of any of claims 10 to 14, wherein the network node is configured for:

10 in response to determining that the registration request is invalid, discarding the registration request, averting a registration based on the registration request, sending a notification message to a management or security node indicating that the registration request is invalid, sending a notification message to a management or security node indicating that a related node is potentially malicious, or copying
15 or storing a portion of the registration request.

16. The system of any of claims 10 to 15, wherein the first network identifier or the second network identifier includes a public land mobile network (PLMN) identifier or a PLMN code.

17. The system of any of claims 10 to 16, wherein the registration request
20 includes a Nudm_UECM_Registration request.

18. The system of any of claims 10 to 17, wherein the network node includes a unified data management (UDM) node, an authentication server function (AUSF), or a user data repository (UDR).

19. A non-transitory computer readable medium comprising computer
25 executable instructions embodied in the non-transitory computer readable medium that when executed by at least one processor of at least one computer cause the at least one computer to perform steps comprising:

at a network node:

- 30 receiving, from a first session management function (SMF) in a home network, a registration request indicating a first network identifier identifying a visited network where a user device is roaming;

determining whether the registration request is valid by comparing the first network identifier and a second network identifier associated with an access and mobility management function (AMF) serving the user device; and

5 performing at least one action based on the determining.

20. The non-transitory computer readable medium of claim 19 wherein the second network identifier is included in Amf3GppAccessRegistration data obtained from a user data repository (UDR).

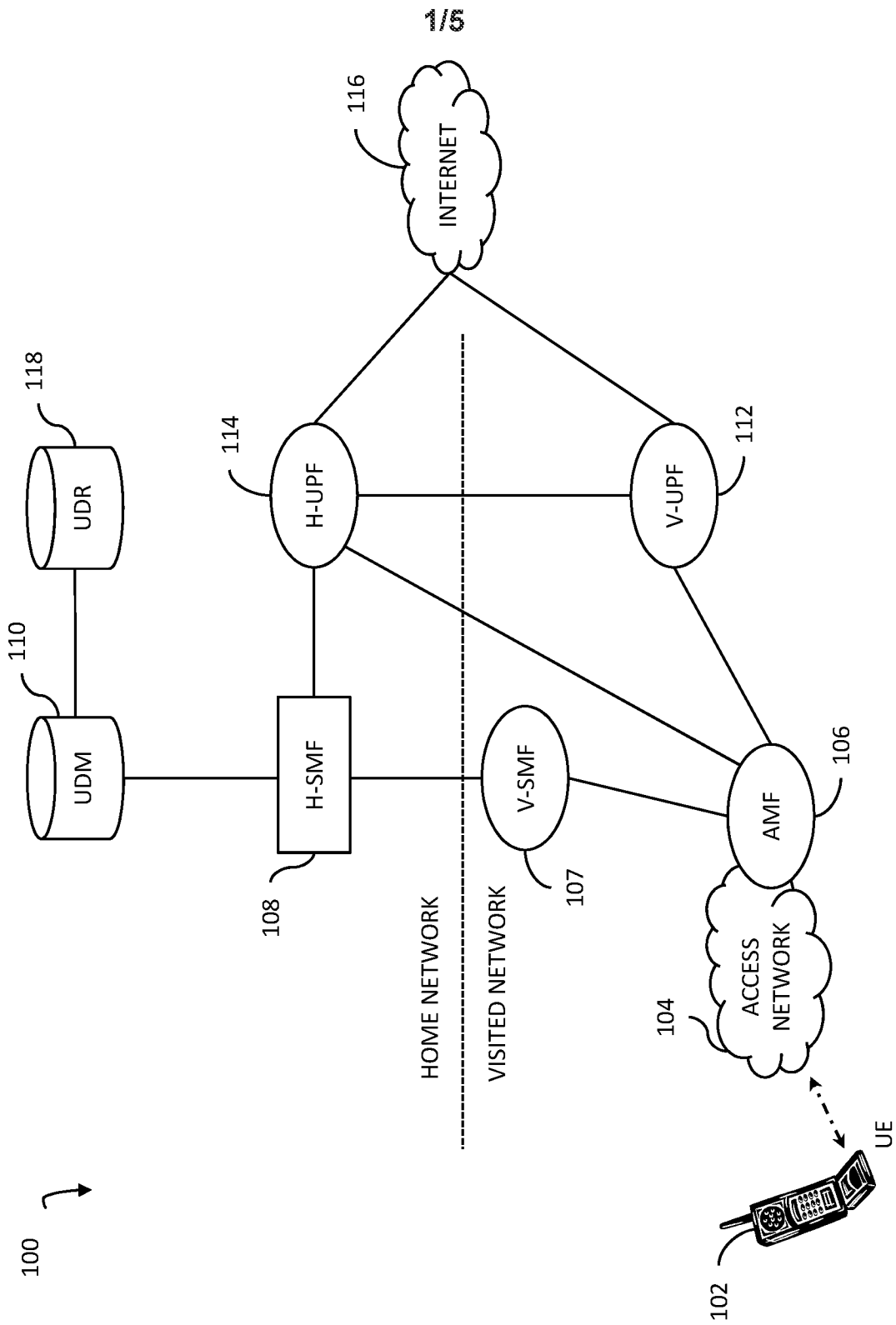


FIG. 1

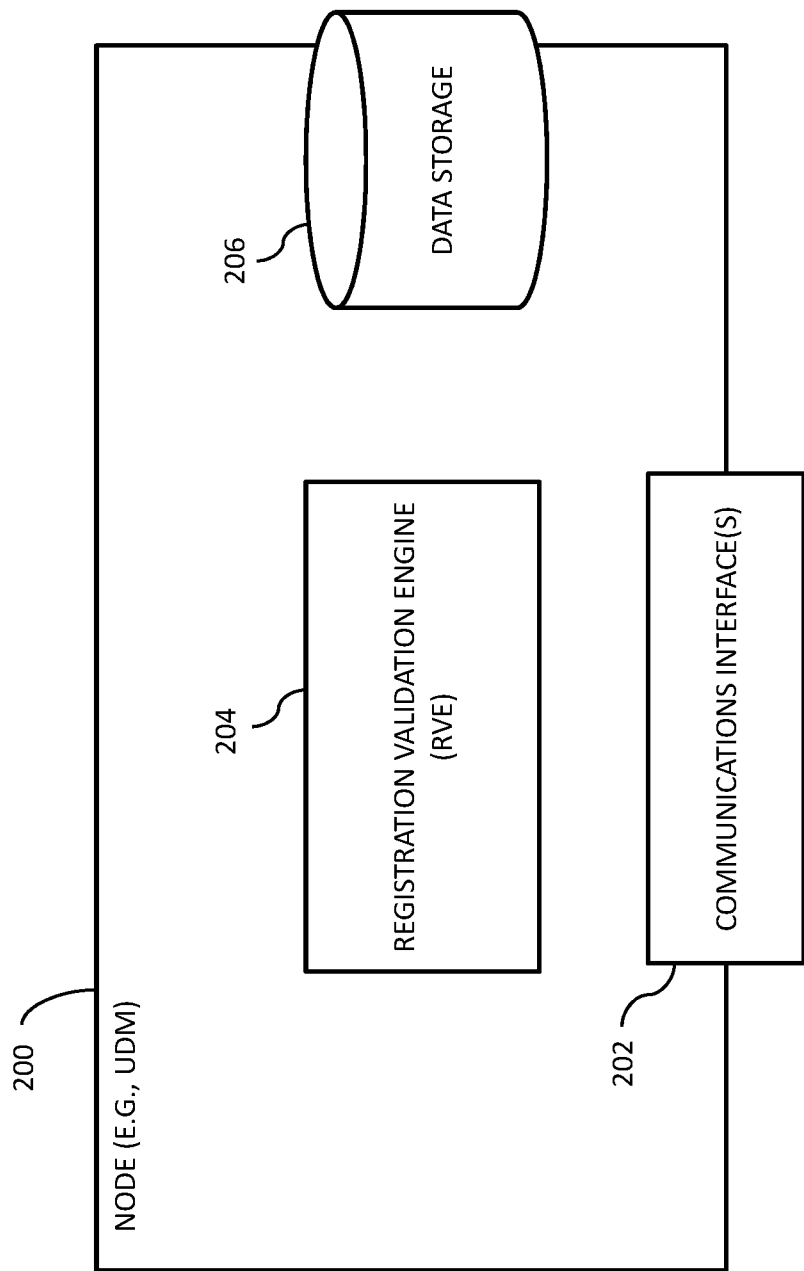


FIG. 2

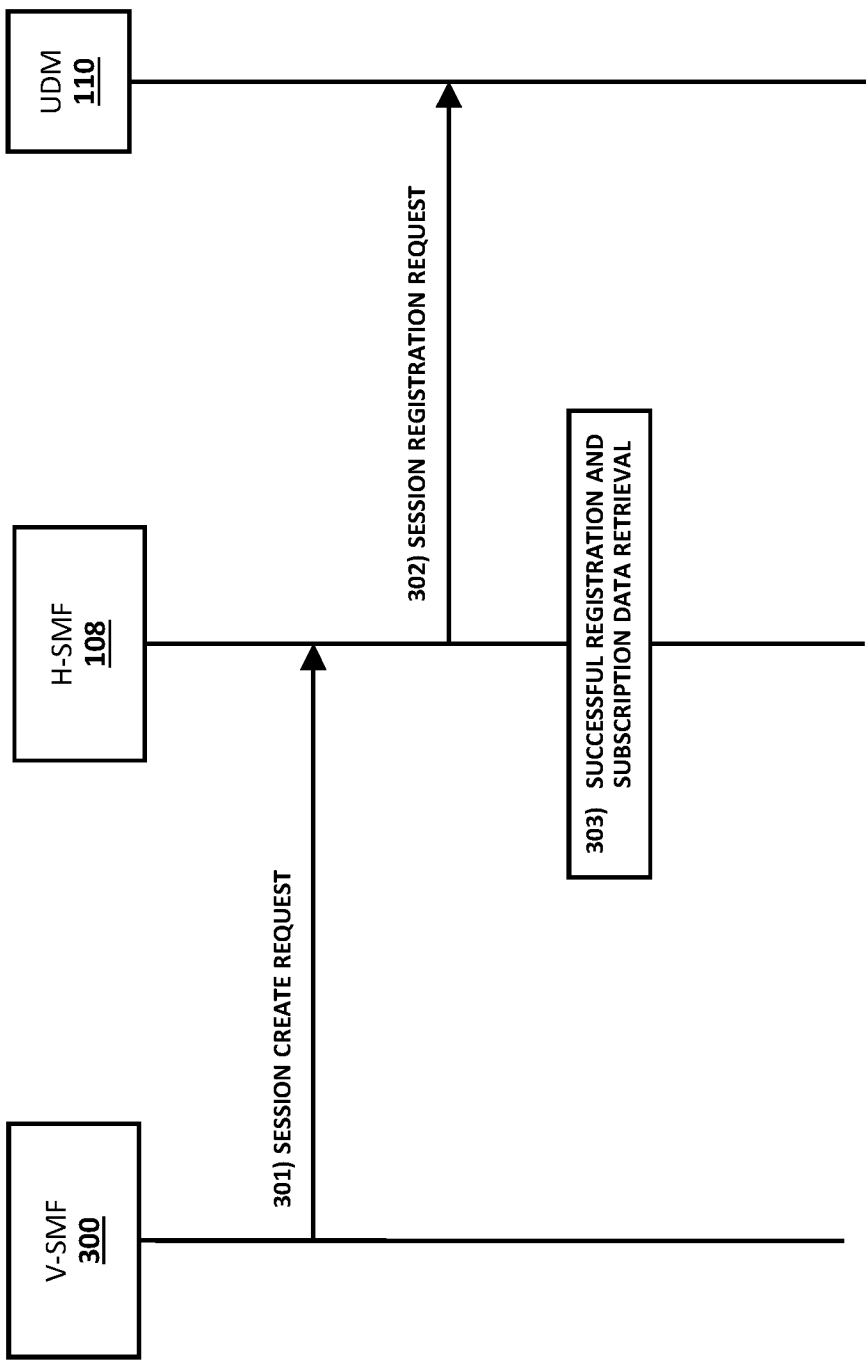


FIG. 3

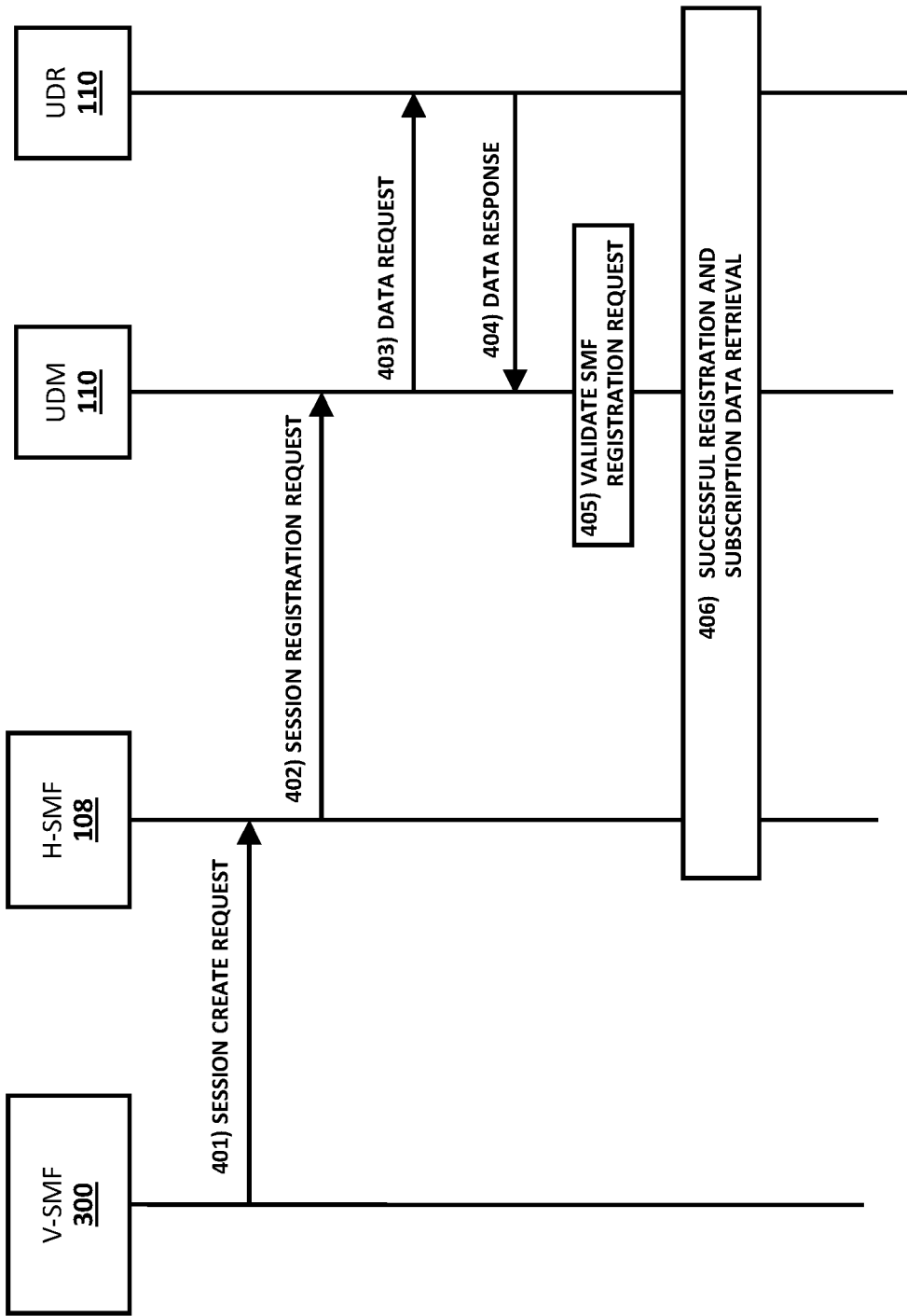


FIG. 4

5/5

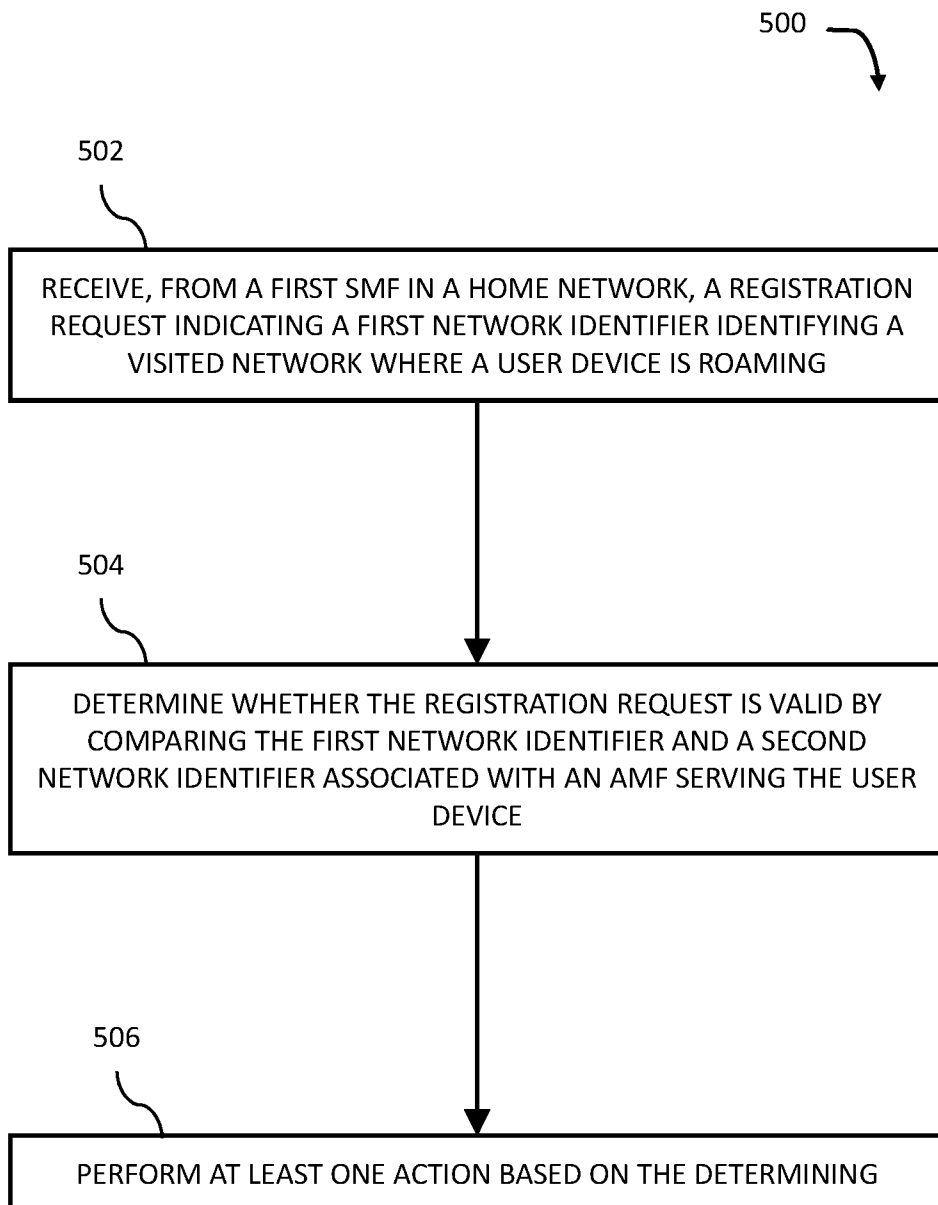


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2021/033030

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06 H04W12/12
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)

H04L H04W

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

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

EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2020/164763 A1 (TELEFONAKTIEBOLAGET LM ERICSSON [SE]) 20 August 2020 (2020-08-20) page 3 - page 7 page 30 - page 38 -----	1-20
X	WO 2018/202284 A1 (ERICSSON TELEFON AB L M [SE]) 8 November 2018 (2018-11-08) page 4 - page 6 page 11 - page 20 -----	1-20
A	US 2018/310162 A1 (KIM HYUNSOOK [KR] ET AL) 25 October 2018 (2018-10-25) paragraph [0080] - paragraph [0110] paragraph [0157] - paragraph [0197] -----	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

11 August 2021

Date of mailing of the international search report

20/08/2021

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

Kraska, Nora

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2021/033030

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2020164763 A1	20-08-2020	NONE	
WO 2018202284 A1	08-11-2018	NONE	
US 2018310162 A1	25-10-2018	US 2018310162 A1	25-10-2018
		WO 2017082532 A1	18-05-2017