



(51) International Patent Classification:

H04W 12/06 (2009.01) H04L 9/08 (2006.01)

H04W 12/08 (2009.01) H04L 29/06 (2006.01)

H04W 88/06 (2009.01) G06F 21/62 (2013.01)

(21) International Application Number:

PCT/FI2020/050201

(22) International Filing Date:

27 March 2020 (27.03.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

201941014730 11 April 2019 (11.04.2019) IN

(71) Applicant: NOKIA TECHNOLOGIES OY [FI/FI];

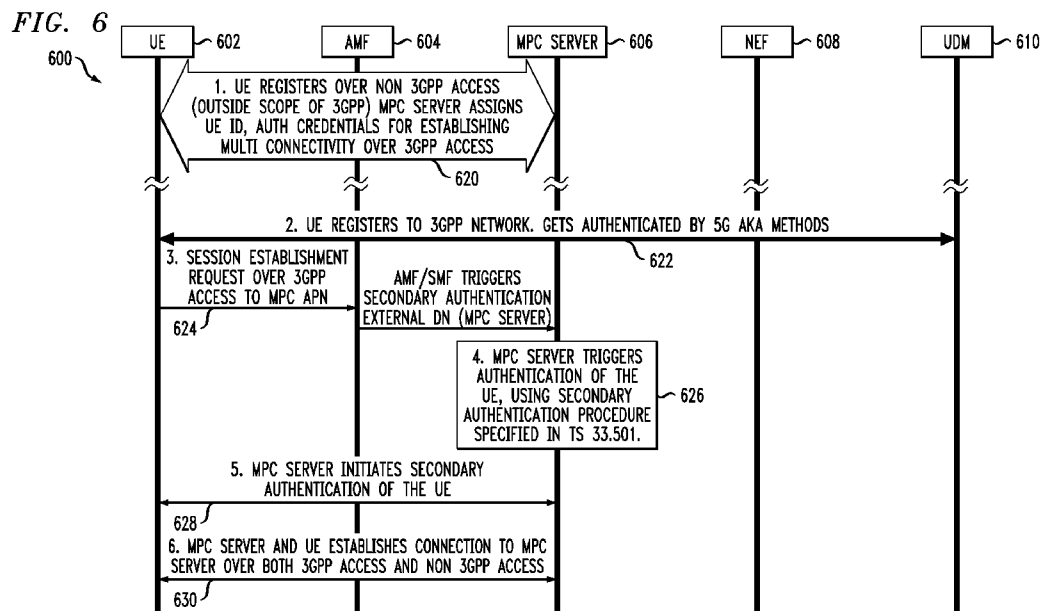
Karakaari 7, 02610 Espoo (FI).

(72) Inventors: **KANUGOVI, Satish**; 163/x, 4th Main Road, Katriguppa East, BSK 3rd Stage, 4th Phase, Begaluru 560085 (IN). **THEIMER, Thomas**; Forstenrieder Weg 1 g, 82065 Baierbrunn (DE). **VAN DE VELDE, Thierry**; Kon. Kasteeldreef 81, 1860 Meise (BE). **NAIR, Suresh**; 33 Deerfield Road, Whippany, New Jersey 07981 (US).

(74) Agent: **NOKIA TECHNOLOGIES OY** et al.; Ari Aarnio, IPR Department, Karakaari 7, 02610 Espoo (FI).

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

(54) Title: ESTABLISHING SECURE COMMUNICATION PATHS TO MULTIPATH CONNECTION SERVER WITH INITIAL CONNECTION OVER PRIVATE NETWORK



(57) Abstract: With regard to given user equipment, a method comprises establishing a multipath connectivity security context when registering with a first communication network, wherein the multipath connectivity security context relates to a multipath connection server. The multipath connectivity security context is then utilized to establish a first connection with the multipath connection server through the first communication network and a second connection with the multipath connection server through a second communication network. The first communication network comprises a wireless private network (e.g., a non 3GPP network) and the second communication network comprises a wireless public network (e.g., a 3GPP network).

SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

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

Published:

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

**ESTABLISHING SECURE COMMUNICATION PATHS TO MULTIPATH
CONNECTION SERVER WITH INITIAL CONNECTION OVER PRIVATE
NETWORK**

Field

The field relates generally to communication systems, and more particularly, but not exclusively, to security management within such systems.

Background

10 This section introduces aspects that may be helpful to facilitate a better understanding of the inventions. Accordingly, the statements of this section are to be read in this light and are not to be understood as admissions about what is in the prior art or what is not in the prior art.

15 Fourth generation (4G) wireless mobile telecommunications technology, also known as Long Term Evolution (LTE) technology, was designed to provide high capacity mobile multimedia with high data rates particularly for human interaction. Next generation or fifth generation (5G) technology is intended to be used not only for human interaction, but also for machine type communications in so-called Internet of Things (IoT) networks.

20 While 5G networks are intended to enable massive IoT services (e.g., very large numbers of limited capacity devices) and mission-critical IoT services (e.g., requiring high reliability), improvements over legacy mobile communication services are supported in the form of enhanced mobile broadband (eMBB) services providing improved wireless Internet access for mobile devices.

25 In an example communication system, user equipment (5G UE in a 5G network or, more broadly, a UE) such as a mobile terminal (subscriber) communicates over an air interface with a base station or access point referred to as a gNB in a 5G network. The access point (e.g., gNB) is illustratively part of an access network of the communication system. For example, in a 5G network, the access network is referred to as a 5G System and is described in 5G Technical Specification (TS) 23.501, V15.4.0, entitled "Technical
30 Specification Group Services and System Aspects; System Architecture for the 5G System," the disclosure of which is incorporated by reference herein in its entirety. In general, the access point (e.g., gNB) provides access for the UE to a core network (CN), which then

provides access for the UE to other UEs and/or a data network such as a packet data network (e.g., Internet).

TS 23.501 goes on to define a 5G Service-Based Architecture (SBA) which models services as network functions (NFs) that communicate with each other using representational state transfer application programming interfaces (Restful APIs).

Furthermore, 5G Technical Specification (TS) 33.501, V15.3.1, entitled “Technical Specification Group Services and System Aspects; Security Architecture and Procedures for the 5G System,” the disclosure of which is incorporated by reference herein in its entirety, further describes security management details associated with a 5G network.

Still further, a multiple access management service (MAMS) is proposed for 5G networks. In such a service, it is intended that a UE be able to access a multipath connection server via multiple independent communications networks. However, security management in the context of such multipath connectivity presents several challenges.

Summary

Illustrative embodiments provide improved techniques for security management in communication systems particularly with respect to multipath connectivity.

For example, in one illustrative embodiment in accordance with given user equipment, a method comprises establishing a multipath connectivity security context when registering with a first communication network, wherein the multipath connectivity security context relates to a multipath connection server. The multipath connectivity security context is then utilized to establish a first connection with the multipath connection server through the first communication network and a second connection with the multipath connection server through a second communication network. The first communication network comprises a wireless private network (e.g., a non 3GPP network) and the second communication network comprises a wireless public network (e.g., a 3GPP network).

In a further embodiment in accordance with a multipath connection server, a method comprises authenticating given user equipment, registering through a first communication network, using at least part of a multipath connectivity security context established with the given user equipment. The multipath connection server then authenticates the given user equipment through a second communication network, and receives a session establishment request from the given user equipment through the second communication network. The

multipath connection server then re-authenticates the given user equipment using at least part of the security context, and establishes a first connection with the given user equipment through the first communication network and a second connection with the given user equipment through the second communication network. The first communication network comprises a wireless private network and the second communication network comprises a wireless public network. Further, in one or more illustrative embodiments, the multipath connection server is able to establish more connections to user equipment over available communication networks as needed.

Further illustrative embodiments are provided in the form of a non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor causes the processor to perform the above steps. Still further illustrative embodiments comprise apparatus with a processor and a memory configured to perform the above steps.

These and other features and advantages of embodiments described herein will become more apparent from the accompanying drawings and the following detailed description.

Brief Description of the Drawings

FIG. 1 illustrates a communication system with which one or more illustrative embodiments are implemented.

FIG. 2 illustrates processing architectures for security management participants, according to an illustrative embodiment.

FIG. 3 illustrates multipath connectivity scenarios, according to an illustrative embodiment.

FIG. 4 illustrates a first connection with a multipath connection server over a wireless private network, according to an illustrative embodiment.

FIG. 5 illustrates a second connection with a multipath connection server over a wireless public network, according to an illustrative embodiment.

FIG. 6 illustrates a security management methodology for multiple connections with a multipath connection server, according to an illustrative embodiment.

Detailed Description

Embodiments will be illustrated herein in conjunction with example communication systems and associated techniques for providing security management (e.g., cryptographic key management) in communication systems. It should be understood, however, that the scope of the claims is not limited to particular types of communication systems and/or processes disclosed. Embodiments can be implemented in a wide variety of other types of communication systems, using alternative processes and operations. For example, although illustrated in the context of wireless cellular systems utilizing 3GPP system elements such as a 3GPP next generation system (5G), the disclosed embodiments can be adapted in a straightforward manner to a variety of other types of communication systems.

In accordance with illustrative embodiments implemented in a 5G communication system environment, one or more 3GPP technical specifications (TS) and technical reports (TR) provide further explanation of user equipment and network elements/functions and/or operations that interact with one or more illustrative embodiments, e.g., the above-referenced 3GPP TS 23.501 and 3GPP TS 33.501. Other 3GPP TS/TR documents provide other conventional details that one of ordinary skill in the art will realize. However, while illustrative embodiments are well-suited for implementation associated with the above-mentioned 5G-related 3GPP standards, alternative embodiments are not necessarily intended to be limited to any particular standards.

Furthermore, illustrative embodiments may be explained herein in the context of the Open Systems Interconnection model (OSI model) which is a model that conceptually characterizes communication functions of a communication system such as, for example, a 5G network. The OSI model is typically conceptualized as a hierarchical stack with a given layer serving the layer above and being served by the layer below. Typically, the OSI model comprises seven layers with the top layer of the stack being the application layer (layer 7) followed by the presentation layer (layer 6), the session layer (layer 5), the transport layer (layer 4), the network layer (layer 3), the data link layer (layer 2), and the physical layer (layer 1). One of ordinary skill in the art will appreciate the functions and interworkings of the various layers and, thus, further details of each layer are not described herein. However, it is to be appreciated that while illustrative embodiments are well-suited for implementations that utilize an OSI model, alternative embodiments are not necessarily limited to any particular communication function model.

Illustrative embodiments are related to security management associated with the Service-Based Architecture (SBA) for 5G networks. Prior to describing such illustrative embodiments, a general description of main components of a 5G network will be described below in the context of FIGS. 1 and 2.

FIG. 1 shows a communication system 100 within which illustrative embodiments are implemented. It is to be understood that the elements shown in communication system 100 are intended to represent main functions provided within the system, e.g., UE access functions, mobility management functions, authentication functions, serving gateway functions, etc. As such, the blocks shown in FIG. 1 reference specific elements in 5G networks that provide these main functions. However, other network elements may be used in other embodiments to implement some or all of the main functions represented. Also, it is to be understood that not all functions of a 5G network are depicted in FIG. 1. Rather, functions that facilitate an explanation of illustrative embodiments are represented. Subsequent figures may depict some additional elements/functions.

Accordingly, as shown, communication system 100 comprises user equipment (UE) 102 that communicates via an air interface 103 with an access point (gNB) 104. The UE 102 in some embodiments is a mobile station, and such a mobile station may comprise, by way of example, a mobile telephone, a computer, or any other type of communication device. The term “user equipment” as used herein is therefore intended to be construed broadly, so as to encompass a variety of different types of mobile stations, subscriber stations or, more generally, communication devices, including examples such as a combination of a data card inserted in a laptop or other equipment such as a smart phone or other cellular device. In one or more illustrative embodiments, user equipment refers to an IoT device. Such communication devices are also intended to encompass devices commonly referred to as access terminals.

In one embodiment, UE 102 is comprised of a Universal Integrated Circuit Card (UICC) part and a Mobile Equipment (ME) part. The UICC is the user-dependent part of the UE and contains at least one Universal Subscriber Identity Module (USIM) and appropriate application software. The USIM securely stores the permanent subscription identifier and its related key, which are used to identify and authenticate subscribers to access networks. The ME is the user-independent part of the UE and contains terminal equipment (TE) functions and various mobile termination (MT) functions.

Note that, in one example, the permanent subscription identifier is an International Mobile Subscriber Identity (IMSI) of a UE. In one embodiment, the IMSI is a fixed 15-digit length and consists of a 3-digit Mobile Country Code (MCC), a 3-digit Mobile Network Code (MNC), and a 9-digit Mobile Station Identification Number (MSIN). In a 5G communication system, an IMSI is referred to as a Subscription Permanent Identifier (SUPI). In the case of an IMSI as a SUPI, the MSIN provides the subscriber identity. Thus, only the MSIN portion of the IMSI typically needs to be encrypted. The MNC and MCC portions of the IMSI provide routing information, used by the serving network to route to the correct home network. When the MSIN of a SUPI is encrypted, it is referred to as a Subscription Concealed Identifier (SUCI).

The access point 104 is illustratively part of an access network of the communication system 100. Such an access network comprises, for example, a 5G System having a plurality of base stations and one or more associated radio network control functions. The base stations and radio network control functions in some embodiments are logically separate entities, but in some embodiments are implemented in the same physical network element, such as, for example, a base station router or cellular access point.

The access point 104 in this illustrative embodiment is operatively coupled to mobility management functions 106. In a 5G network, the mobility management function is implemented by an Access and Mobility Management Function (AMF). A Security Anchor Function (SEAF) in some embodiments is also implemented with the AMF connecting a UE with the mobility management function. A mobility management function, as used herein, is the element or function (i.e., entity) in the core network (CN) part of the communication system that manages or otherwise participates in, among other network operations, access and mobility (including authentication/authorization) operations with the UE (through the access point 104). The AMF is also referred to herein, more generally, as an access and mobility management entity.

The AMF 106 in this illustrative embodiment is operatively coupled to home subscriber functions 108, i.e., one or more functions that are resident in the home network of the subscriber. As shown, some of these functions include the Unified Data Management (UDM) function, as well as an Authentication Server Function (AUSF). The AUSF and UDM (separately or collectively) are also referred to herein, more generally, as an authentication entity. In addition, home subscriber functions include, but are not limited to,

Network Slice Selection Function (NSSF), Network Exposure Function (NEF), Network Repository Function (NRF), and Policy Control Function (PCF).

Some of these functions will be further described herein in the context of security management with an application function that, in some illustrative embodiments, runs on an application server associated with a third party. By “third party” here, it is meant to refer to a party other than the subscriber of the UE or the operator of the core network. For example, in one or more illustrative embodiments, the third party is an enterprise (e.g., corporation, business, group, individual, or the like). In some embodiments, the subscriber of the UE is an employee of the enterprise (or otherwise affiliated) who maintains a mobile subscription with the operator of the core network or another mobile network. Note that a UE is typically subscribed to what is referred to as a Home Public Land Mobile Network (HPLMN) in which some or all of the home subscriber functions 108 reside. If the UE is roaming (not in the HPLMN), it is typically connected with a Visited Public Land Mobile Network (VPLMN) also referred to as a serving network. Some or all of the mobility management functions 106 may reside in the VPLMN, in which case, functions in the VPLMN communicate with functions in the HPLMN as needed. However, in a non-roaming scenario, mobility management functions 106 and home subscriber functions 108 can reside in the same communication network.

Note that the application function is a multipath connection server in illustrative embodiments. In some embodiments, the multipath connection server is associated with a third party, such as an enterprise as illustratively mentioned above.

The access point 104 is also operatively coupled to a serving gateway function, i.e., Session Management Function (SMF) 110, which is operatively coupled to a User Plane Function (UPF) 112. UPF 112 is operatively coupled to a Packet Data Network, e.g., Internet 114. As is known in 5G and other communication networks, the user plane (UP) or data plane carries network user traffic while the control plane (CP) carries signaling traffic. SMF 110 supports functionalities relating to UP subscriber sessions, e.g., establishment, modification and release of PDU sessions. UPF 112 supports functionalities to facilitate UP operations, e.g., packet routing and forwarding, interconnection to the data network (e.g., 114 in FIG. 1), policy enforcement, and data buffering.

It is to be appreciated that FIG. 1 is a simplified illustration in that not all communication links and connections between network functions (NFs) and other system

elements are illustrated in FIG. 1. One ordinarily skilled in the art given the various 3GPP TSs/TRs will appreciate the various links and connections not expressly shown or that may otherwise be generalized in FIG. 1.

Further typical operations and functions of certain network elements are not described herein in detail when they are not the focus of illustrative embodiments but can be found in appropriate 3GPP 5G documentation. It is to be appreciated that the particular arrangement of system elements in FIG. 1 is an example only, and other types and arrangements of additional or alternative elements can be used to implement a communication system in other embodiments. For example, in other embodiments, the system 100 comprises other elements/functions not expressly shown herein. Also, although only single elements/functions are shown in the FIG. 1 embodiment, this is for simplicity and clarity of illustration only. A given alternative embodiment may include larger numbers of such system elements, as well as additional or alternative elements of a type commonly associated with conventional system implementations.

It is also to be noted that while FIG. 1 illustrates system elements as singular functional blocks, the various subnetworks that make up the 5G network are partitioned into so-called network slices. Network slices (network partitions) comprise a series of network function (NF) sets (i.e., function chains) for each corresponding service type using network function virtualization (NFV) on a common physical infrastructure. The network slices are instantiated as needed for a given service, e.g., eMBB service, massive IoT service, and mission-critical IoT service. A network slice or function is thus instantiated when an instance of that network slice or function is created. In some embodiments, this involves installing or otherwise running the network slice or function on one or more host devices of the underlying physical infrastructure. UE 102 is configured to access one or more of these services via gNB 104. NFs can also access services of other NFs.

Illustrative embodiments provide a security management methodology for multipath connectivity where a multipath connectivity security context is established for a given UE and used when connecting with a multipath connection server. The term “security context” is understood to refer to any information relating to the establishment and maintenance of security of communications between two or more participants. By way of example only, a security context can comprise one or more identities and/or one or more keys or key

materials (e.g., generated, derived, or otherwise obtained). Note that when the term “key” is used alone, it is understood to refer to a cryptographic key.

FIG. 2 is a block diagram of processing architectures 200 of participants in a security management methodology for multipath connectivity in an illustrative embodiment. As will be further explained below, more than two participants are involved in security management according to illustrative embodiments, e.g., UE, AMF, NEF, UDM, SMF, non 3GPP elements. As such, FIG. 2 illustrates processing architectures associated with any two of the participants that directly or indirectly communicate. Therefore, in illustrative embodiments, each participant in a security management methodology is understood to be configured with the processing architecture shown in FIG. 2.

As shown, a first security management participant 202 comprises a processor 212 coupled to a memory 216 and interface circuitry 210. The processor 212 of the first security management participant 202 includes a security management processing module 214 that may be implemented at least in part in the form of software executed by the processor. The processing module 214 performs security management described in conjunction with subsequent figures and otherwise herein. The memory 216 of the first security management participant 202 includes a security management storage module 218 that stores data generated or otherwise used during security management operations.

As further shown, a second security management participant 204 comprises a processor 222 coupled to a memory 226 and interface circuitry 220. The processor 222 of the second security management participant 204 includes a security management processing module 224 that may be implemented at least in part in the form of software executed by the processor 222. The processing module 224 performs security management described in conjunction with subsequent figures and otherwise herein. The memory 226 of the second security management participant 204 includes a security management storage module 228 that stores data generated or otherwise used during security management operations.

The processors 212 and 222 of the respective security management participants 202 and 204 may comprise, for example, microprocessors, application-specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), digital signal processors (DSPs) or other types of processing devices or integrated circuits, as well as portions or combinations of such elements. Such integrated circuit devices, as well as portions or combinations thereof, are examples of “circuitry” as that term is used herein. A wide variety

of other arrangements of hardware and associated software or firmware may be used in implementing the illustrative embodiments.

The memories 216 and 226 of the respective security management participants 202 and 204 may be used to store one or more software programs that are executed by the
5 respective processors 212 and 222 to implement at least a portion of the functionality described herein. For example, security management operations and other functionality as described in conjunction with subsequent figures and otherwise herein may be implemented in a straightforward manner using software code executed by processors 212 and 222.

A given one of the memories 216 or 226 may therefore be viewed as an example of
10 what is more generally referred to herein as a computer program product or still more generally as a processor-readable storage medium that has executable program code embodied therein. Other examples of processor-readable storage media may include disks or other types of magnetic or optical media, in any combination. Illustrative embodiments can include articles of manufacture comprising such computer program products or other
15 processor-readable storage media.

The memory 216 or 226 may more particularly comprise, for example, an electronic random-access memory (RAM) such as static RAM (SRAM), dynamic RAM (DRAM) or other types of volatile or non-volatile electronic memory. The latter may include, for example, non-volatile memories such as flash memory, magnetic RAM (MRAM), phase-
20 change RAM (PC-RAM) or ferroelectric RAM (FRAM). The term “memory” as used herein is intended to be broadly construed, and may additionally or alternatively encompass, for example, a read-only memory (ROM), a disk-based memory, or other type of storage device, as well as portions or combinations of such devices.

The interface circuitries 210 and 220 of the respective security management
25 participants 202 and 204 illustratively comprise transceivers or other communication hardware or firmware that allows the associated system elements to communicate with one another in the manner described herein.

It is apparent from FIG. 2 that first security management participant 202 is configured for communication with the second security management participant 204 and vice-versa via
30 their respective interface circuitries 210 and 220. This communication involves the first security management participant 202 sending data to the second security management participant 204, and the second security management participant 204 sending data to the first

security management participant 202. However, in alternative embodiments, other network elements or other components may be operatively coupled between, as well as to, the security management participants 202 and 204. The term “data” as used herein is intended to be construed broadly, so as to encompass any type of information that may be sent between security management participants including, but not limited to, messages, tokens, identifiers, keys, indicators, user data, control data, etc.

It is to be appreciated that the particular arrangement of components shown in FIG. 2 is an example only, and numerous alternative configurations are used in other embodiments. For example, any given network element/function can be configured to incorporate additional or alternative components and to support other communication protocols.

Given the above illustrative architectures, illustrative embodiments of security management methodologies for multipath connectivity functionalities will be further described below. Prior to such descriptions, some main considerations that at least partially motivated development of illustrative embodiments will be described in the context of a 5G network (as an example of a 3GPP or wireless public network) and a wireless local area network or WLAN (as an example of a non 3GPP or wireless private network).

FIG. 3 illustrates a multipath connectivity scenario 300, according to an illustrative embodiment. As mentioned above, multipath connectivity functionality (e.g., MAMS) is intended to provide multipath connections consistent with a 5G network environment. More particularly, as shown in FIG. 3, UE 302 is connected to a multipath connection server 304 over a private network 306 (e.g., non 3GPP access such as a wireless local area network (WLAN) or wireless fidelity (Wi-Fi) network) and over a public network 308 (e.g. 3GPP access such as a 5G core network). Multipath connection server 304 functions as a multipath connectivity proxy (e.g., a network function in the context of a 5G network), which can be accessed over multiple independent networks (e.g., two networks in the FIG. 3 embodiments but which can be more than two independent networks in other embodiments).

However, secure establishment of multipath connections to a multipath connectivity proxy (e.g., multipath connection server 304) across independent networks (e.g., private network 306 and public network 308) presents challenges.

Multipath protocol procedures, e.g., MPTCP, may require the client to establish a multipath session when the initial access network connection is established, i.e. even when

the device starts with a single access network connection. For example, assume an IoT scenario that involves IoT devices in a factory setting, e.g., robotic devices operating on a factory floor that are also configured as UEs. When a robotic device connects via a WLAN, it has to setup the first leg of a multipath connection with the multipath connectivity function in the network. Later, when the robotic device connects via 5G, it establishes the second multipath leg to the same multipath connectivity function. Since, the robotic devices perform critical functions in the factory, often in cooperation with other robotic devices and other types of devices in the factory network, it is important to ensure a secured connection. Irrespective of the varied level of security offered by the underlying access network connections, it is realized herein that unauthorized users should not be able to establish new multipath sessions or break into existing multipath sessions.

Furthermore, it is realized herein that the network should control which devices are authorized to establish the initial multipath session and also ensure that the second leg establishment, from an independent network, is indeed from the originator of the first leg. In other words, it is further realized herein that a device should assert its identity of the multipath session. In illustrative embodiments, this is ensured by exchanging a commonly derived key (part of a security context) between the UE (e.g., robotic or other IoT device) and the multipath connectivity function during establishment of initial and subsequent legs, which cannot be carried across multipath sessions.

To address the above and other challenges, illustrative embodiments provide the following features.

Multipath connection server 304 is assumed to function as an external data network (DN) server to the public network 308 (3GPP network/5G core), when UE 302 is connected over the private network 306 (non 3GPP network/WLAN).

UE 302 first connects to multipath connection server 304 over the private network 306 (non 3GPP access or private access). In various embodiments, multiple authentication methods are contemplated for this access as well as how multipath connection server 304 authenticates UE 302. One or more of these authentication methods, in some embodiments, may be outside the scope of 3GPP.

Once UE 302 is connected over the private network 306 to multipath connection server 304, UE 302 obtains a unique identity, security key and credentials (security context) to be used for the subsequent connection over the public network 308 (3GPP access).

When UE 302 meets conditions for establishment of connection over 3GPP access, UE 302 makes connection to 3GPP network (public network 308). UE 302 is authenticated as any regular 3GPP UE, e.g., using one of the 5G AKA procedures, e.g., either 3GPP EAP AKA' (RFC 5448) procedure or 5G AKA procedure (RFC 5247).

5 Once UE 302 is authenticated in the 5G 3GPP network, UE 302 requests a connection to the multipath connection server APN (access point name). The APN for multipath connection server 304 is configured to trigger secondary authentication of UE 302 as specified in TS 33.501. Multipath connection server 304 performs secondary authentication of UE 302 using the identity and credentials previously exchanged over the non 3GPP access
10 (private network 306). Multipath connection server 304 identifies the already established multipath security context of UE 304 using the credentials.

Illustrative embodiments assume that UE 302 first makes the connection to multipath connection server 304 over a non 3GPP access, i.e., over private network 306.

Note that the concurrently filed patent application identified by attorney docket
15 number 316557-IN-NP and entitled "Establishing Secure Communication Paths to Multipath Connection Server with Initial Connection Over Public Network," the disclosure of which is incorporated by reference herein in its entirety, describes multipath connectivity for the scenarios when UE 302 first makes the connection to multipath connection server 304 over a 3GPP access, i.e., over public network 308.

20 Therefore, using both methods, UE 302 can start the connection over a 3GPP network or over a non 3GPP network and move around freely without losing the connection with multipath connection server 304.

These and other multipath connection features of illustrative embodiments will be described below in the context of FIGS. 4-6.

25 More particularly, FIG. 4 illustrates an embodiment for establishing the first or initial connection with a multipath connection (MPC) server over a private network, and FIG. 5 illustrates an embodiment for establishing the second or subsequent connection with the MPC server over a public network. FIG. 6 illustrates an exemplary message flow for a security management methodology to establish such connections.

30 As shown in multipath connectivity scenario 400 in FIG. 4, UE 402 accesses Wifi network 410 (private network) to establish a first connection with multiple connection server 420. Note that, in illustrative embodiments, multipath connection server 420 is configured

as an external DN 430, when first accessed over Wifi network 410, so as to facilitate a subsequent 3GPP access connection.

Multipath connectivity scenario 500 in FIG. 5 illustrates a second connection with multipath connection server 420 (configured as external DN 430) over a wireless public network, i.e., 5G core network 510. More particularly, FIG. 5 illustrates a 5G Core 510 with SEAF 512, UDM 514, NEF 516, and AUSF 518. NEF 516 is operatively coupled to UDM 514 and multipath connection server 420, while UE 402 is operatively coupled to multipath connection server 420 and AUSF 518.

In one embodiment, NEF 516 interfaces with UDM 514 in 5G Core 510 to obtain the required inputs (such as one or more AVs) for generating a UE-specific multipath connection (MPC) key (a key specific to UE 402 for multipath connection server 420). In another embodiment, UDM 514 generates an enterprise key based on UE subscription data, which is then used by NEF 516 to generate an MPC-specific cryptographic key using an MPC identifier as one of the inputs. Furthermore, NEF 516 provides a Service-Based Interface (SBI)-based northbound interface to multipath connection server 420. Further details and/or other methods of verification and authentication are described below.

FIG. 6 illustrates a security management methodology for multiple connections with a multipath connection server, according to an illustrative embodiment. More particularly, FIG. 6 depicts an end-to-end message flow 600 between UE 602, AMF 604, multipath connection (MPC) server 606, NEF 608, and UDM 610. Message flow 600 depicts steps for establishing connection to the MPC server starting the connection over private non 3GPP access and then establishing the second connection over 3GPP access.

Step 1 (620). UE 602 registers over non 3GPP access, gets authenticated, and establishes a UE security context with MPC server 606, as shown.

Step 2. (622). UE 602 moves around and when conditions are met, registers over 3GPP access. UE 602 gets authenticated in 3GPP access by 5G AKA procedures.

Step 3 (624). Once 5G authentication is completed and a connection is established, UE 602 requests AMF (SMF) 604 connection to MPC server 606. MPC server 606 is configured as an external DN where secondary authentication is needed.

Step 4 (626). The MPC server 606 may initiate secondary authentication using Extensible Authentication Protocol (EAP) methods as specified in TS 33.501.

Step 5 (628). The secondary authentication verifies the UE's identity (ID) assigned over the first non 3GPP connection, and security credentials assigned over the first connection (i.e., in step 620).

5 Step 6 (630). At the end of successful authentication, both UE 602 and MPC server 606 establish connection over the non 3GPP access network, as well as the 3GPP network.

The particular processing operations and other system functionality described in conjunction with the message flow diagram of FIG. 6 are presented by way of illustrative example only, and should not be construed as limiting the scope of the disclosure in any way. Alternative embodiments can use other types of processing operations and messaging
10 protocols. For example, the ordering of the steps may be varied in other embodiments, or certain steps may be performed at least in part concurrently with one another rather than serially. Also, one or more of the steps may be repeated periodically, or multiple instances of the methods can be performed in parallel with one another.

It should therefore again be emphasized that the various embodiments described
15 herein are presented by way of illustrative example only and should not be construed as limiting the scope of the claims. For example, alternative embodiments can utilize different communication system configurations, user equipment configurations, base station configurations, authentication and key agreement protocols, key pair provisioning and usage processes, messaging protocols and message formats than those described above in the
20 context of the illustrative embodiments. These and numerous other alternative embodiments within the scope of the appended claims will be readily apparent to those skilled in the art.

I/We Claim:

1. An apparatus comprising:
at least one processor;
5 at least one memory including computer program code;
the at least one memory and the computer program code being configured to, with
the at least one processor, cause the apparatus at least to:

establish a multipath connectivity security context when registering with a first
communication network, wherein the multipath connectivity security context relates to a
10 multipath connection server; and

utilize the multipath connectivity security context to establish a first connection with
the multipath connection server through the first communication network and a second
connection with the multipath connection server through a second communication network;
wherein the first communication network comprises a wireless private network and
15 the second communication network comprises a wireless public network.

2. The apparatus of claim 1, wherein establishing the multipath connectivity security
context further comprises causing the apparatus to obtain a unique identity for the apparatus,
a cryptographic key, and credentials when registering with the first communication network.

20

3. The apparatus of claim 2, wherein the at least one memory and the computer
program code are further configured to, with the at least one processor, cause the apparatus
to authenticate with the second communication network.

25 4. The apparatus of claim 3, wherein utilizing the multipath connectivity security
context further comprises causing the apparatus to send a session establishment request to
the multipath connection server through the second communication network.

5. The apparatus of claim 4, wherein utilizing the multipath connectivity security
30 context further comprises causing the apparatus to re-authenticate with the multipath
connection server in a secondary authentication process using the unique identity for the
apparatus and credentials obtained when registering with the first communication network.

6. The apparatus of claim 4, wherein the session establishment request sent to the multipath connection server through the second communication network is sent to an access point name corresponding to the multipath connection server.

5

7. The apparatus of claim 1, wherein the first communication network is a non 3GPP network, and the second communication network is a 3GPP network.

8. A method comprising:

10

in accordance with given user equipment;

establishing a multipath connectivity security context when registering with a first communication network, wherein the multipath connectivity security context relates to a multipath connection server; and

utilizing the multipath connectivity security context to establish a first connection with the multipath connection server through the first communication network and a second connection with the multipath connection server through a second communication network;

wherein the first communication network comprises a wireless private network and the second communication network comprises a wireless public network;

wherein the given user equipment comprises a processor and memory configured to execute the above steps.

9. The method of claim 8, wherein establishing the multipath connectivity security context further comprises the given user equipment obtaining a unique identity for the apparatus, a cryptographic key, and credentials when registering with the first communication network.

10. The method of claim 9, further comprising the given user equipment authenticating with the second communication network.

11. The method of claim 10, wherein utilizing the multipath connectivity security context further comprises the given user equipment sending a session establishment request to the multipath connection server through the second communication network.

12. The method of claim 11, wherein utilizing the multipath connectivity security context further comprises the given user equipment re-authenticating with the multipath connection server in a secondary authentication process using the unique identity for the apparatus and credentials obtained when registering with the first communication network.

13. The method of claim 11, wherein the session establishment request sent to the multipath connection server through the second communication network is sent to an access point name corresponding to the multipath connection server.

14. An article of manufacture comprising a non-transitory computer-readable storage medium having embodied therein executable program code that when executed by the processor associated with the given user equipment causes the given user equipment to perform the steps of claim 8.

15. An apparatus comprising:
at least one processor;
at least one memory including computer program code;
the at least one memory and the computer program code being configured to, with the at least one processor, cause the apparatus at least to:
authenticate given user equipment, registering through a first communication network, using at least part of a multipath connectivity security context established with the given user equipment;
authenticate the given user equipment through a second communication network;
receive a session establishment request from the given user equipment through the second communication network;
re-authenticate the given user equipment using at least part of the security context;
and
establish a first connection with the given user equipment through the first communication network and a second connection with the given user equipment through the second communication network;

wherein the first communication network comprises a wireless private network and the second communication network comprises a wireless public network.

16. The apparatus of claim 15, wherein the first communication network is a non
5 3GPP network, and the second communication network is a 3GPP network.

17. The apparatus of claim 15, wherein the apparatus is configured as a data network external to the second communication network.

10 18. The apparatus of claim 15, wherein the apparatus is part of a multiple access management service.

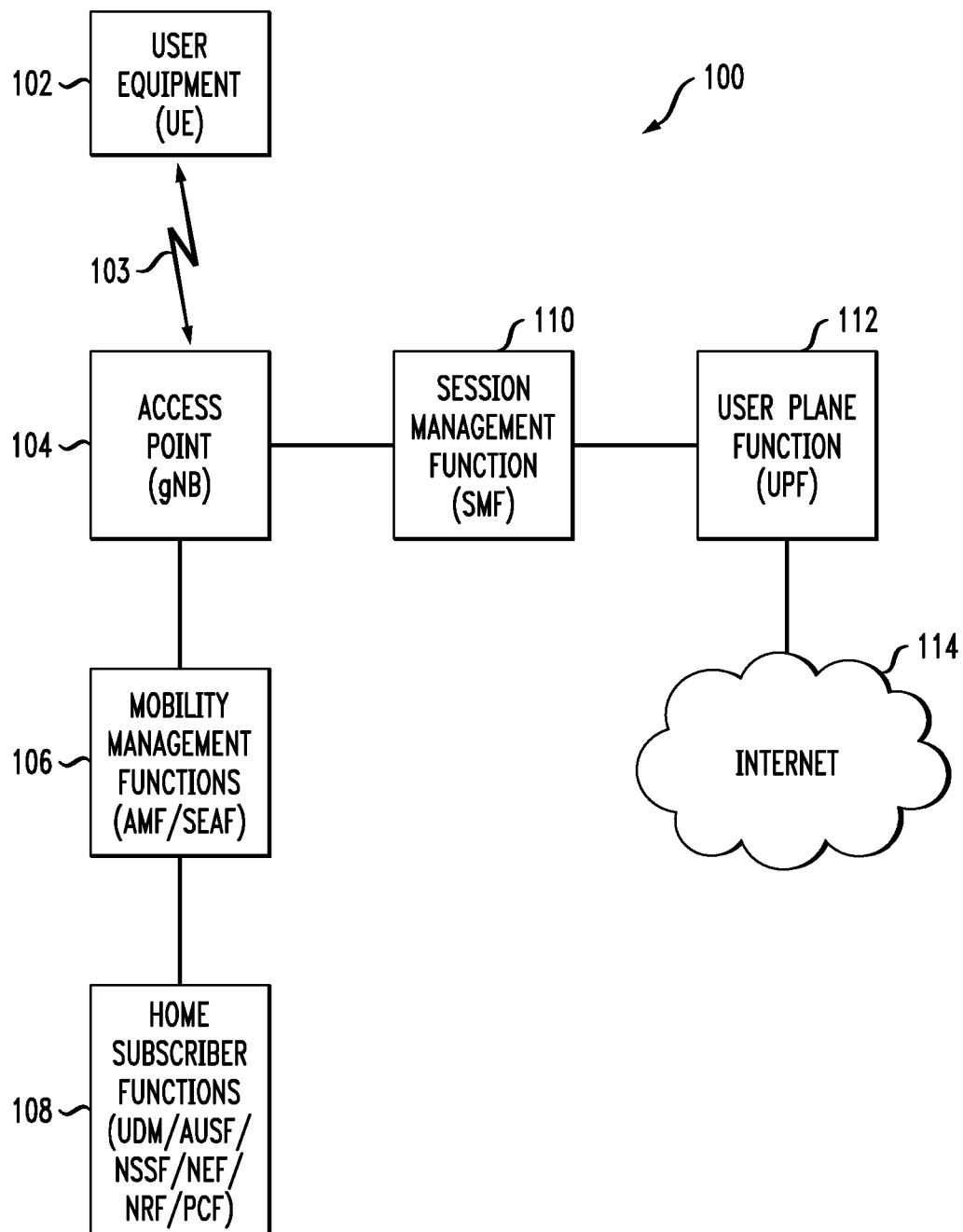
19. A method comprising:
in accordance with a multipath connection server;
15 authenticating given user equipment, registering through a first communication network, using at least part of a multipath connectivity security context established with the given user equipment;
authenticating the given user equipment through a second communication network;
receiving a session establishment request from the given user equipment through the
20 second communication network;
re-authenticating the given user equipment using at least part of the security context;
and
establishing a first connection with the given user equipment through the first communication network and a second connection with the given user equipment through the
25 second communication network;
wherein the first communication network comprises a wireless private network and the second communication network comprises a wireless public network;
wherein the multipath connection server is implemented by a processor and memory configured to execute the above steps.

30 20. An article of manufacture comprising a non-transitory computer-readable storage medium having embodied therein executable program code that when executed by

the processor associated with the multipath connection server causes the multipath connection server to perform the steps of claim 19.

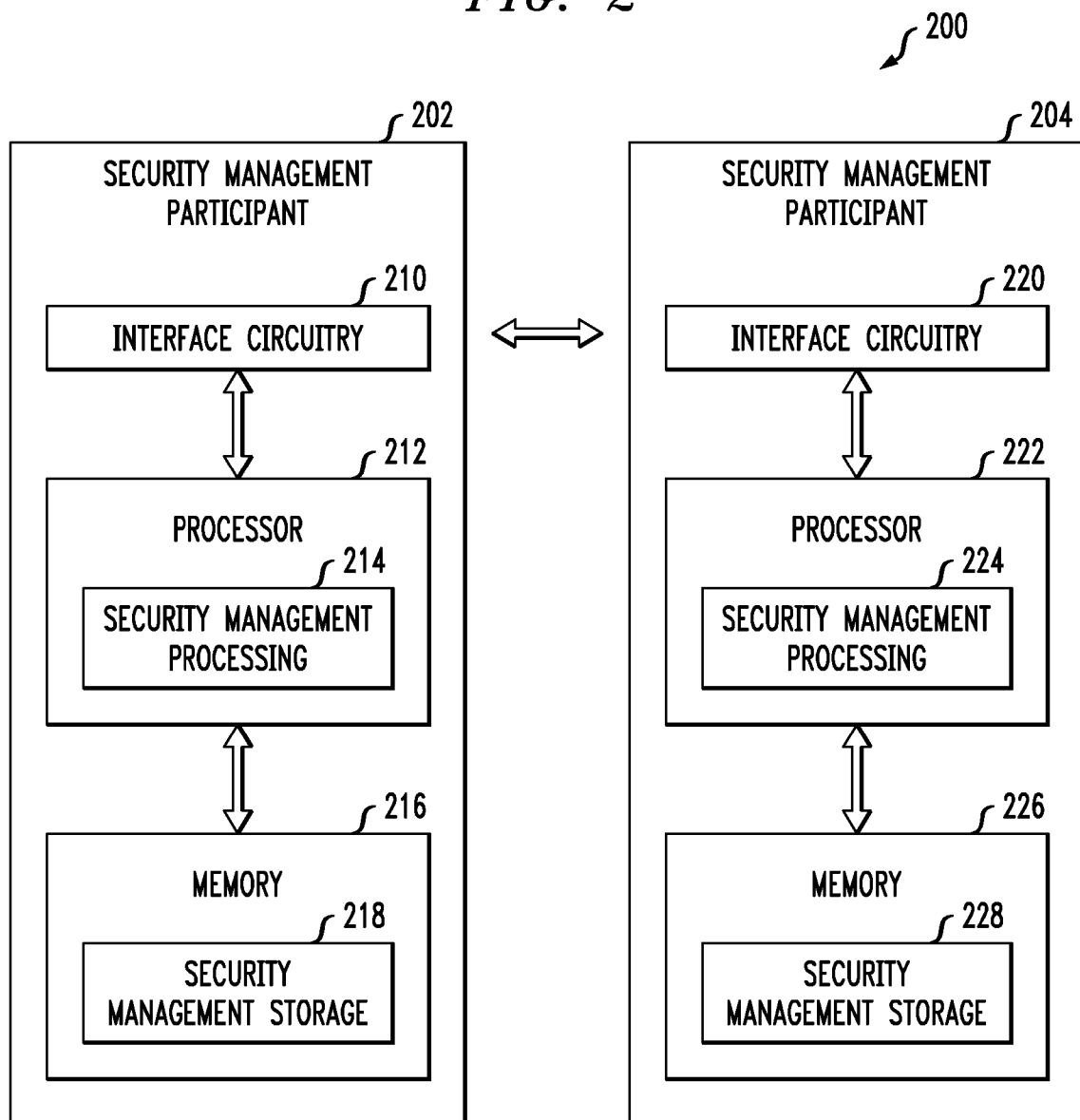
1/5

FIG. 1

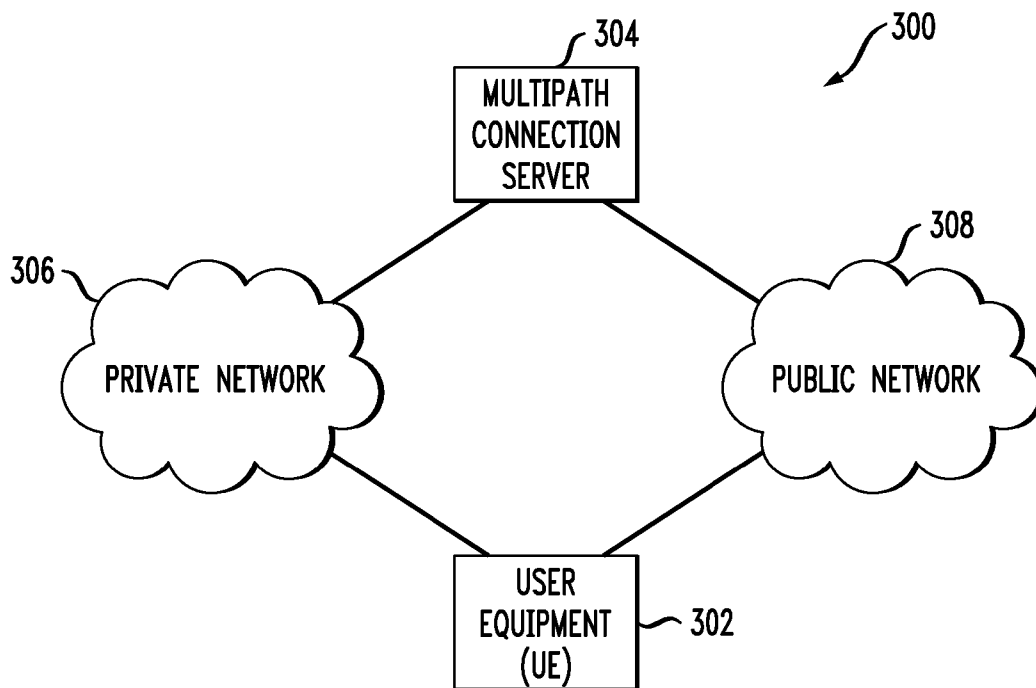
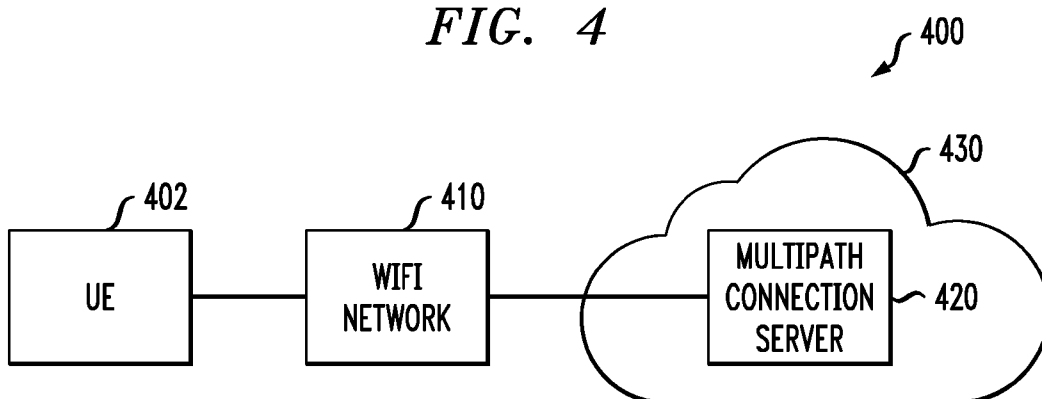


2/5

FIG. 2

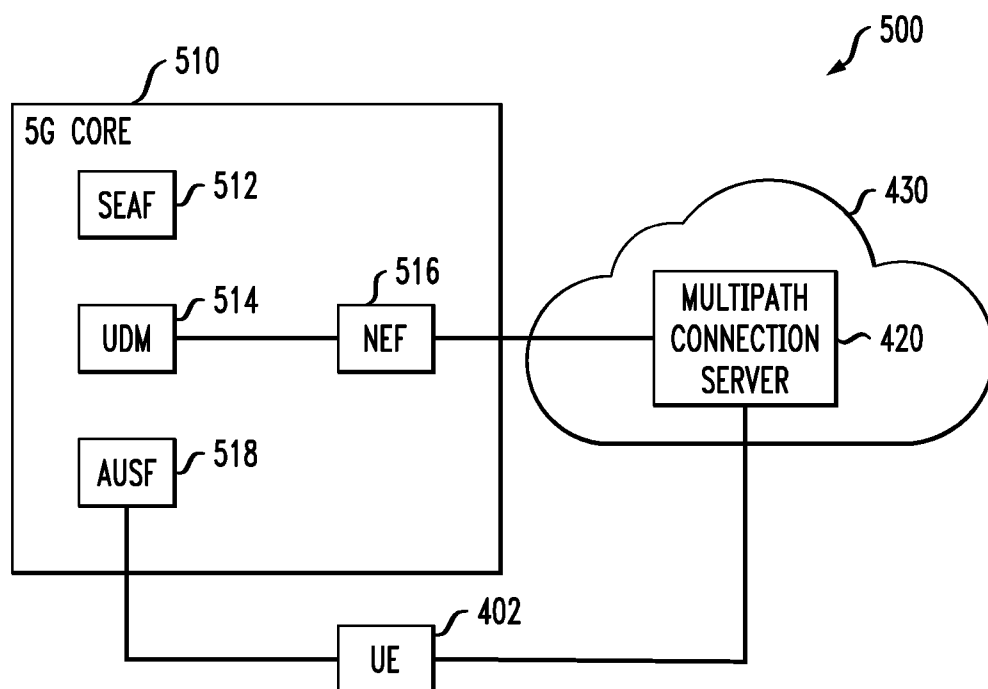


3/5

FIG. 3*FIG. 4*

4/5

FIG. 5



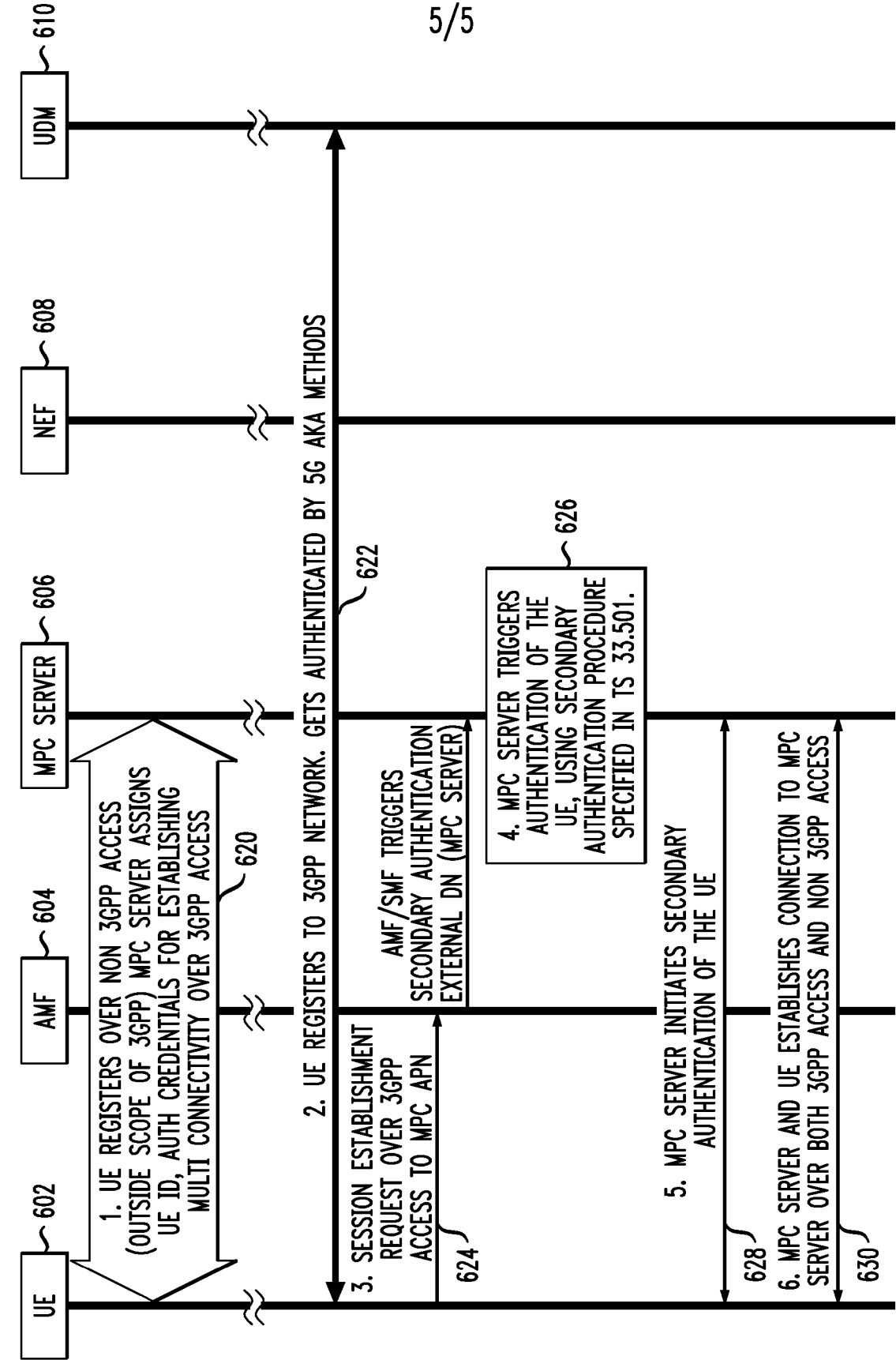


FIG. 6
600

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2020/050201

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04W, H04L, G06F, G16Y

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
FI, SE, NO, DK

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

EPODOC, EPO-Internal full-text databases, Full-text translation databases from Asian languages, WPIAP, XP3GPP, XPAIP, XPCPVO, XPESP, XPETSI, XPI3E, XPIEE, XPIETF, XPIOP, XPIPCOM, XPJPEG, XPMISC, XPOAC, XPRD, XPSRNG, XPTK, COMPDX, INSPEC, TDB, NPL, PRH-Internal, Internet, ACM, Springer

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2018206081 A1 (MOTOROLA MOBILITY LLC [US]) 15 November 2018 (15.11.2018) the whole document, in particular Figs. 2-5B; paragraphs [0002], [0046], [0066], [0082]-[0093]	1-20
A	US 2017223531 A1 (MESTANOV FILIP [SE] et al.) 03 August 2017 (03.08.2017) The whole document.	1-20
A	3GPP TS 23.502 V16.0.2 (2019-04). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Procedures for the 5G System; Stage 2 (Release 16). [online], 2019-04-01, [retrieved on 2020-06-30]. Retrieved from < https://www.3gpp.org/ftp/Specs/archive/23_series/23.502/23502-g02.zip >, the whole document, in particular Fig. 4.3.3.3-1; Section 4.3.2.3	1-20

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

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"D" document cited by the applicant in the international application	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"E" earlier application or patent but published on or after the international filing date	"&" document member of the same patent family
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 09 July 2020 (09.07.2020)	Date of mailing of the international search report 10 July 2020 (10.07.2020)
Name and mailing address of the ISA/FI Finnish Patent and Registration Office FI-00091 PRH, FINLAND Facsimile No. +358 29 509 5328	Authorized officer Yrjö Raivio Telephone No. +358 29 509 5000

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2020/050201

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
D, A	3GPP TS 33.501 V15.4.0 (2019-03). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 15). [online], 2019-03-28, [retrieved on 2020-06-30]. Retrieved from < https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-f40.zip >, the whole document, in particular Section 11	1-20
A	KANUGOVI, S. et al. Internet-Draft. Multiple Access Management Services, draft-kanugovi-intarea-mams-framework-03. IETF, [online], 2019-02-28, [retrieved on 2020-07-02]. Retrieved from < https://tools.ietf.org/pdf/draft-kanugovi-intarea-mams-framework-03.pdf >, the whole document, in particular Section 4.6	18

CLASSIFICATION OF SUBJECT MATTER

IPC

H04W 12/06 (2009.01)**H04W 12/08** (2009.01)**H04W 88/06** (2009.01)**H04L 9/08** (2006.01)**H04L 29/06** (2006.01)**G06F 21/62** (2013.01)

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2020/050201

WO 2018206081 A1	15/11/2018	CN 110603891 A	20/12/2019
		EP 3622731 A1	18/03/2020
		KR 20190139925 A	18/12/2019
		US 2019335330 A1	31/10/2019

US 2017223531 A1	03/08/2017	EP 3175639 A1	07/06/2017
		WO 2016015749 A1	04/02/2016
