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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 January 2022 (13.01.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/008089 A1

(51) International Patent Classification:
H04W 4/80 (2018.01) *H04W 88/04* (2009.01)
H04W 28/16 (2009.01) *H04W 12/08* (2021.01)
H04W 40/02 (2009.01)

(21) International Application Number:
PCT/EP2020/073776

(22) International Filing Date:
25 August 2020 (25.08.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20382610.2 08 July 2020 (08.07.2020) EP

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; 164 83 Stockholm (SE).

(72) Inventors: **MUÑOZ DE LA TORRE ALONSO, Miguel Angel**; Padre Claret 6, 8C ESC D, ES-28002 Madrid (ES). **LOHMAR, Thorsten**; Tittardsfeld 29, 52072 AACHEN (DE).

(74) Agent: **ERICSSON**; Patent Development, Torshamnsgatan 21-23, 164 80 STOCKHOLM (SE).

(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, 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))*

(54) Title: USER EQUIPMENT TETHERING POLICY

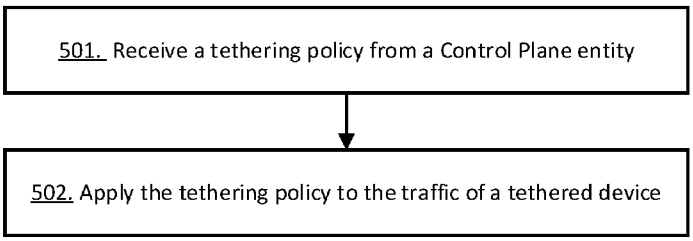

Figure 5

(57) Abstract: A method for enabling the detection of tethering traffic and the application of tethering policies to such traffic at a User Equipment (UE). The method comprises receiving subscription information at a policy control entity from a subscriber data repository entity, the subscription information including an indication of actions to apply to the traffic of tethered devices at the UE, transmitting from the policy control entity to the UE a tethering policy including the received actions to apply to the traffic of tethered devices, and applying at the UE the tethering policy to the traffic of a tethered device. The policy control entity may be a PCF. The subscriber data repository entity may be a UDR. The tethering policy may include an indication to block the tethering traffic, to mark the tethering traffic or to report information or events related to the tethering traffic and tethering devices.

WO 2022/008089 A1

USER EQUIPMENT TETHERING POLICY

TECHNICAL FIELD

The present invention generally relates to the provisioning of policy rules in mobile networks, and more specifically, the invention relates to the provisioning of policy rules to a User Equipment.

BACKGROUND

Tethering refers to the coupling of a tethering device, such as a computer, with a tethering-enabled device providing a so-called hotspot, such as a mobile phone, so that the tethering device is able to use the mobile connection and data plan service of the tethering-enabled device. The mobile phone is configured to behave as a modem, providing network connection to the tethering device. The coupling between the tethering device and the tethering-enabled device can be via a data cable, such as a USB cable or a proprietary cable, or be over wireless LAN (Wi-Fi), over Bluetooth or a proprietary communication protocol, to name a few.

The use of mobile phones as modems for other devices to access the Internet has caused a serious concern for telecom carriers (also referred to as wireless carriers, network operators or mobile network operators) who are not contracted or paid for use of their mobile networks to be accessed in such a way as to provide Internet services to laptops, computers, tablets or third party users.

Wireless carriers are working to identify tethering traffic and apply specific policies to it, for example blocking unauthorized or inappropriate tethering traffic, applying a specific Quality of Service or routing rules, charge it in a different way, etc. Nowadays this is possible using solutions implemented in the network gateways, for example

tethering traffic is identified by using fingerprinting techniques, trying to detect patterns that indicate that the source of the traffic is not the mobile device. Actions that are performed to the tethering traffic are for example counting the number of tethered devices, blocking the tethering traffic if the subscriber has not requested the service, blocking based on the number of tethering devices, application of a different tariff, change the Quality of Service, report the detection of tethering devices or tethering traffic.

The concept of Tethering can also be applied to other scenarios as well. For example, a 5G-RG (5G Residential Gateway) is a special UE device, which is offering connectivity for in-home devices, fixed and mobile. The devices connected to the 5G-RG are tethering devices, and in this case the network operator may want to offer specific services or apply specific policies to the devices connected to the 5G-RW.

A problematic aspect is that wireless carriers have failed to come up with adequate solutions to completely identify the tethering traffic. There is currently no solution that is able to completely detect and control tethering traffic, especially as the traffic encryption is growing and encrypted traffic cannot be inspected at the network side. Besides, some users hack their mobile devices to avoid tethering detection on the network side.

SUMMARY

An object of the invention is to enable the detection of tethering traffic and the application of tethering policies to such traffic.

A first aspect of the invention relates to a method performed by a User Equipment (UE) for enforcing tethering policies at said UE. The method includes receiving a tethering policy from a Control Plane (CP) entity of a mobile communication system, the tethering policy including actions to apply to the traffic of tethered devices, and

applying the tethering policy to the traffic of a tethered device. In an embodiment of the method, the tethering policy includes an indication to block the traffic of a tethered device. In an embodiment of the method, the tethering policy includes an indication to only allow traffic transmission of a maximum number of tethered devices connected simultaneously. In an embodiment of the method, the tethering policy includes an indication to mark the traffic of a tethered device with a specific value included in a protocol header, the value being the same for all tethered devices or different for each tethered device. In an embodiment of the method, the tethering policy includes an indication to report an event to the CP entity or another CP entity in response to the detection of traffic of a tethered device. In an embodiment of the method, the indication to report the event comprises an indication to report the number of tethered devices, the detection of a new tethered device, or the volume of the traffic of a tethered device. In an embodiment of the method, applying the tethering policy comprises transmitting a report to the CP entity or another CP entity including the number of tethered devices, the detection of a new tethered device, or the volume of the traffic of a tethered device. In an embodiment of the method, the tethering policy is received from an access and mobility management entity in a Protocol Data Unit session response message or in a UE Route Selection Policy, URSP. In an embodiment of the method, the tethering policy is received from a policy control entity in a UE Route Selection Policy (URSP).

A second aspect of the invention relates to a method performed by a policy control entity for providing a tethering policy to a User Equipment. The method includes receiving subscription information from a subscriber data repository entity of a mobile communication system, the subscription information including an indication of actions to apply to the traffic of tethered devices at the UE, and transmitting to the UE a tethering policy including the received actions to apply to the traffic of tethered devices. In an embodiment of the method, the tethering policy includes an indication to block the traffic of a tethered device. In an embodiment of the method, the tethering policy includes an indication to only allow traffic transmission of a

maximum number of tethered devices connected simultaneously. In an embodiment of the method, the tethering policy includes an indication to mark the traffic of a tethered device with a specific value included in a protocol header, the value being the same for all tethered devices or different for each tethered device. In an embodiment of the method, the tethering policy includes an indication to report an event to the CP entity or another CP entity in response to the detection of traffic of a tethered device. In an embodiment of the method, the indication to report the event comprises an indication to report the number of tethered devices, the detection of a new tethered device, or the volume of the traffic of a tethered device. In an embodiment of the method, the tethering policy is transmitted in a UE Route Selection Policy (URSP).

A third aspect of the invention relates to a method performed by an access and mobility management entity for providing a tethering policy to a User Equipment. The method includes receiving a tethering policy from a policy control entity of a mobile communication system, the tethering policy including an indication of actions to apply to the traffic of tethered devices at the UE and transmitting to the UE the tethering policy. In an embodiment of the method, the tethering policy includes an indication to block the traffic of a tethered device. In an embodiment of the method, the tethering policy includes an indication to only allow traffic transmission of a maximum number of tethered devices connected simultaneously. In an embodiment of the method, the tethering policy includes an indication to mark the traffic of a tethered device with a specific value included in a protocol header, the value being the same for all tethered devices or different for each tethered device. In an embodiment of the method, the tethering policy includes an indication to report an event to the CP entity or another CP entity in response to the detection of traffic of a tethered device. In an embodiment of the method, the indication to report the event comprises an indication to report the number of tethered devices, the detection of a new tethered device, or the volume of the traffic of a tethered device. In an

embodiment of the method, the tethering policy is transmitted in a Protocol Data Unit session response message or in a UE Route Selection Policy (URSP).

Other aspects of the invention relate to mobile network nodes, particularly a User Equipment and a control plane node, each configured to perform the respective methods as described herein. In some embodiments of these aspects, the control plane node may refer to an Access and Mobility Management Function (AMF) or a Policy Control Function (PCF). Other aspects of the invention relate to the corresponding computer programs or computer program products.

Advantageously, the solution disclosed herein enables the detection of tethering traffic at the UE in a simple an efficient way, which would be not possible to detect at the network side, for example when the traffic is encrypted.

Further advantageously, the solution disclosed herein enables the control of tethering traffic at the UE, and the application of tethering policies at the UE which would be not possible to apply at the network side.

Further advantageously, the solution disclosed herein enables the marking of tethering traffic at the UE and the application of tethering policies at the network side based on that marking.

Other objectives, features and advantages of the enclosed embodiments will be apparent from the following detailed disclosure, from the attached dependent claims as well as from the drawings.

Generally, all terms used in the claims are to be interpreted according to their ordinary meaning in the technical field, unless explicitly defined otherwise herein. All references to "a/an/the element, apparatus, component, means, module, step, etc." are to be interpreted openly as referring to at least one instance of the element, apparatus, component, means, module, step, etc., unless explicitly stated otherwise. The steps of any method disclosed herein do not have to be performed in the exact order disclosed, unless explicitly stated.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention may best be understood by referring to the following description and accompanying drawings that are used to illustrate particular embodiments of the invention. In the drawings:

Figure 1 is a networked system in accordance with particular embodiments of the solution described herein;

Figure 2 is a signaling diagram illustrating a procedure according to particular embodiments of the solution described herein;

Figure 3 is a signaling diagram illustrating a procedure according to particular embodiments of the solution described herein;

Figure 4 is a signaling diagram illustrating a procedure according to particular embodiments of the solution described herein;

Figure 5 is a flowchart illustrating a method performed by a UE according to particular embodiments of the solution described herein;

Figure 6 is a flowchart illustrating a method performed by a mobile network node according to particular embodiments of the solution described herein;

Figure 7 is a flowchart illustrating a method performed by a mobile network node according to particular embodiments of the solution described herein;

Figure 8 is a block diagram of a mobile network node configured in accordance with particular embodiments of the solution described herein.

Figure 9 is a block diagram of a UE configured in accordance with particular embodiments of the solution described herein.

DETAILED DESCRIPTION

The invention will now be described in detail hereinafter with reference to the accompanying drawings, in which examples of embodiments or implementations of the invention are shown. The invention may, however, be embodied or implemented in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of present invention to those skilled in the art. It should also be noted that these embodiments are not mutually exclusive. Components from one embodiment may be tacitly assumed to be present/used in another embodiment. These embodiments of the disclosed subject matter are presented as teaching examples and are not to be construed as limiting the scope of the disclosed subject matter. For example, certain details of the described embodiments may be modified, omitted, or expanded upon without departing from the scope of the described subject matter.

The example embodiments described herein arise in the context of a telecommunications network, including but not limited to a telecommunications network that conforms to and/or otherwise incorporates aspects of a fifth generation (5G) architecture. Figure 1 is an example networked system 100 in accordance with example embodiments of the present disclosure. Figure 1 specifically illustrates User Equipment (UE) 101, which may be in communication with a (Radio) Access Network (RAN) 102 and Access and Mobility Management Function (AMF) 106 and User Plane Function (UPF) 103. The AMF 106 may, in turn, be in communication with core network services including Session Management Function (SMF) 107 and Policy Control Function (PCF) 111. The core network services may also be in communication with an Application Server/ Application Function (AS/AF) 113. Other networked services also include Network Slice Selection Function (NSSF) 108, Authentication Server Function (AUSF) 105, User Data Management (UDM) 112, User Data Repository (UDR) 114, Network Exposure Function (NEF) 109, Network Repository

Function (NRF) 110 and Data Network (DN) 104. In some example implementations of embodiments of the present disclosure, an AMF 106, SMF 107, UPF 103, PCF 111, AUSF 105, NRF 110, UDM 112, UDR 114, NEF 109, AF 113, and NSSF 108 are each considered to be an NF. One or more additional instances of the network functions (NF) may be incorporated into the networked system.

3GPP TS 24.526 describes the UE policies for 5G system, which are delivered from the PCF to the UE. The UE policies include UE route selection policies (URSP) and Access network discovery and selection policies (ANDSP).

The network (PCF) installs URSP rules in the UE. A URSP rule includes a traffic descriptor and a list of route selection descriptors as specified in 3GPP TS 23.503. The traffic descriptor can include an application descriptor in the form of an application identifier or a traffic filter.

The solution described herein aims to enable the detection of tethering traffic and the application of tethering policies to such traffic.

To achieve such object, this disclosure provides a method performed by a UE 101, an access and mobility management entity, a session management entity, a policy control entity and a user data repository entity. In some embodiments, the access and mobility management entity is an AMF 106. In some embodiments, the session management entity is a SMF 107. In some embodiments, the policy control entity is a PCF 111. In some embodiments, the user data repository entity is a UDR 114.

The method comprises receiving subscription information at the policy control entity from the subscriber data repository entity, the subscription information including an indication of actions to apply to the traffic of tethered devices at the UE; transmitting from the policy control entity to the UE a tethering policy including the received actions to apply to the traffic of tethered devices; and applying at the UE the tethering policy to the traffic of a tethered device.

In some embodiments of the method, the tethering policy includes an indication to block the traffic of a tethered device. In some embodiments of the method, the

tethering policy includes an indication to only allow traffic transmission of a maximum number of tethered devices connected simultaneously. In some embodiments of the method, the tethering policy includes an indication to mark the traffic of a tethered device with a specific value included in a protocol header, the value being the same for all tethered devices or different for each tethered device. In some embodiments of the method, the tethering policy includes an indication to report an event to the CP entity or another CP entity in response to the detection of traffic of a tethered device. In some embodiments of the method, the indication to report the event comprises an indication to report the number of tethered devices, the detection of a new tethered device, or the volume of the traffic of a tethered device. In some embodiments of the method, applying the tethering policy comprises transmitting a report including the number of tethered devices, the detection of a new tethered device, or the volume of the traffic of a tethered device. In some embodiments of the method, the tethering policy is received at the UE from an access and mobility management entity in a Protocol Data Unit session response message or in a UE Route Selection Policy, URSP. In some embodiments of the method, the tethering policy is received at the UE from a policy control entity in a UE Route Selection Policy, URSP.

This disclosure also provides mobile network nodes, particularly a Control Plane entity 800 and a UE 900, each configured to perform the respective methods as described herein. This disclosure also provides the corresponding computer program comprising code, for example in the form of a computer program, that when run on processing circuitry of the mobile network nodes causes the mobile network nodes to perform the disclosed methods.

Advantageously, the solution disclosed herein enables the detection of tethering traffic at the UE in a simple an efficient way, which would be not possible to detect at the network side, for example when the traffic is encrypted.

Further advantageously, the solution disclosed herein enables the control of tethering traffic at the UE, and the application of tethering policies at the UE which would be not possible to apply at the network side.

Further advantageously, the solution disclosed herein enables the marking of tethering traffic at the UE and the application of tethering policies at the network side based on that marking.

Hereinafter, drawings showing examples of embodiments of the solution are described in detail.

Figure 2 is a signaling diagram illustrating a procedure for provisioning tethering policies to a UE at PDU session establishment. In this figure, the access and mobility management entity is an AMF 106, the session management entity is a SMF 107, the policy control entity is a PCF 111 and the user data repository entity is a UDR 114. Prior to the execution of this procedure, the UDR shall be provisioned with the corresponding subscription data indicating that the UE is subject to the appropriate tethering policies.

At step 211, the UE 101 triggers the PDU Session Establishment procedure, sending a PDU session establishment request to the SMF. This request is relayed by the AMF. As part of this procedure, the AMF 106 creates the policy association with the PCF 111.

At step 212, the SMF 107 creates the policy association with the PCF 111 and sends to the PCF a request to retrieve the policies for the user.

At step 213, the PCF sends to UDR a request for the corresponding subscription data.

At step 214, the PCF retrieves from UDR the subscriber policy profile including a tethering policy including actions to apply to the traffic of tethered devices.

At step 215, the PCF generates and transmits to the SMF the PCC rules including the tethering policy. The tethering policy may include:

- Precedence: Determines the precedence the policy is enforced with respect to other policies.
- Traffic Descriptor: Determines the traffic to which the policy applies to. For example it may be a match-all rule, which refers to all the traffic going through the hotspot, or in case there is a need to detect tethering on a per application basis, different sets of traffic filters (e.g. IP 3- or 5-tuples) can be included in the Traffic Descriptor.
- Tethering Descriptor: Determines the tethering enforcement actions. It may comprise:
    - Tethering enforcement actions: Determines the actions to apply when tethering is detected, e.g. to block tethering traffic after a maximum number of devices are connected simultaneously or to mark (with a token) the tethered traffic e.g. with an IP Options header or with a DSCP code or source port (different for each tethered device). The latter part will allow the network (e.g. in the UPF) to detect tethered traffic and to differentiate each of the tethered devices.
    - Tethering metrics for reporting: Determines the tethering metrics required to be reported, e.g. to report tethering events, report tethering volume vs UE´s volume, report the number of tethering devices, etc. Alternatively, a tethering action can be explicitly invoked though some UE internal APIs.
    - Destination URI: When present, it indicates the URI of the entity receiving the reports where the tethering metrics shall be forwarded to. It can be a NF IP address, or an IP of a Reporting Server. In case Destination URI is not included, it may indicate that the tethering metrics shall be forwarded to PCF (through AMF via Non-Access Stratum).

At step 216, the SMF sends a PDU session establishment response message to the UE including the tethering policy as described in the previous step. This message is relayed by the AMF.

At step 217, the UE receives and installs the tethering policy.

Figure 3 is a signaling diagram illustrating a procedure for provisioning tethering policies to a UE 101. In this figure, the access and mobility management entity is an AMF 106, the session management entity is a SMF 107, the policy control entity is a PCF 111 and the user data repository entity is a UDR 114. Prior to the execution of this procedure, the UDR shall be provisioned with the corresponding subscription data indicating that the UE is subject to the appropriate tethering policies.

At step 311, the PDU session establishment procedure takes place. In this step the PCF retrieves the tethering policies from UDR, e.g. as in step 213 and 214 in Figure 2.

At step 312, the PCF sends to the UE a UE policy including the tethering policy. In some embodiments, this step is based on an extension of the UE policies (generated by PCF and sent towards UE through AMF, as shown in steps 313 and 314), which allows the network operator to trigger tethering policies for the user´s traffic. The tethering policy may include:

- Precedence: Determines the precedence the policy is enforced with respect to other policies.
- Traffic Descriptor: Determines the traffic to which the policy applies to. For example it may be a match-all rule, which refers to all the traffic going through the hotspot, or in case there is a need to detect tethering on a per application basis, different sets of traffic filters (e.g. IP 3- or 5-tuples) can be included in the Traffic Descriptor.
- Tethering Descriptor: Determines the tethering enforcement actions. It may comprise:
    - Tethering enforcement actions: Determines the actions to apply when tethering is detected, e.g. to block tethering traffic after a maximum

number of devices are connected simultaneously or to mark (with a token) the tethered traffic e.g. with an IP Options header or with a DSCP code or source port (different for each tethered device). The latter part will allow the network (e.g. in the UPF) to detect tethered traffic and to differentiate each of the tethered devices.

- Tethering metrics for reporting: Determines the tethering metrics required to be reported, e.g. to report tethering events, report tethering volume vs UE´s volume, report the number of tethering devices, etc. Alternatively, a tethering action can be explicitly invoked though some UE internal APIs.
- Destination URI: When present, it indicates the URI of the entity receiving the reports where the tethering metrics shall be forwarded to. It can be a NF IP address, or an IP of a Reporting Server. In case Destination URI is not included, it may indicate that the tethering metrics shall be forwarded to PCF (through AMF via Non-Access Stratum).

Steps 313 and 314 show the case in which the AMF relies the UE policy sent from the PCF to the UE.

At step 315, the UE receives and installs the tethering policy.

Figure 4 is a signaling diagram illustrating the enforcement of the tethering policies at the UE 101 when a tethering device 401 connects to the hotspot of the UE or sends tethering traffic to the UE. Prior to the execution of this procedure, the procedure described in Figure 2 or Figure 3 shall have taken place and the UE shall have the tethering policies installed.

At step 411, the tethering device 401 connects to the hotspot of the UE.

At step 412, the UE detects the tethering device and applies the corresponding tethering policy. For example, the UE may configure to drop the traffic from the tethering device 401 if the maximum number of tethering devices has been reached,

or it may not allow the tethering device to connect, or it may configure the reporting actions to perform for the tethering device 401.

At step 413, if the tethering device 401 successfully connected to the hotspot of the UE, the tethering device 401 sends traffic to the UE.

At step 414, the UE detects the tethering traffic of the tethering device 401 and applies the corresponding tethering policy. For example, the UE may drop the traffic from the tethering device 401 if the maximum number of tethering devices has been reached, it may route the traffic according to the tethering policy, it may perform the reporting actions included in the tethering policy, or it may perform the traffic marking actions included in the tethering policy.

In some embodiments, in case the UE applies a marking policy, the UE may mark the traffic (e.g. in IP Options header) with the following information:

- An indication (e.g. token) of tethering traffic, which allows the network (e.g. UPF) to detect that the traffic is tethering traffic.
- An indication of the particular tethering device, or tethering device identifier. This allows the network (e.g. UPF) to differentiate between tethering devices and to apply differentiated policies on a per tethering device basis.
- Packet Flow Descriptor (PFD), PFD set or Application identifier. This indicates the matched traffic filter or application, and allows UPF to identify the particular application that is transmitting the tethering traffic.

Figure 5 is a flowchart illustrating a method performed by a UE for enforcing tethering policies at said UE.

At step 501, the UE receives a tethering policy from a Control Plane entity. In some embodiments, the Control Plane entity is a PCF. In some embodiments, the Control Plane entity is an AMF. The tethering policy is as defined in step 215.

At step 502, the UE applies the tethering policy to the traffic of a tethered device. For example, the UE may drop the traffic from the tethering device if the maximum

number of tethering devices has been reached, it may route the traffic according to the tethering policy, it may perform the reporting actions included in the tethering policy, or it may perform the traffic marking actions included in the tethering policy.

Figure 6 is a flowchart illustrating a method performed by a policy control entity for providing a tethering policy to a User Equipment. In some embodiments, the policy control entity is a PCF.

At step 601, the policy control entity receives subscription information from a subscriber data repository entity including an indication of actions to apply to the traffic of tethered devices at a UE.

At step 602, the policy control entity transmits to the UE a tethering policy including the received actions to apply to the traffic of tethered devices.

Figure 7 is a flowchart illustrating a method performed by an access and mobility management entity for providing a tethering policy to a User Equipment. In some embodiments, the access and mobility management entity is an AMF.

At step 701, the access and mobility management entity receives a tethering policy from a policy control entity including an indication of actions to apply to the traffic of tethered devices at a UE.

At step 702, the access and mobility management entity transmits to the UE the tethering policy.

Figure 8 is a block diagram illustrating elements of a mobile network node 800 of a mobile communications network. In some embodiments, the mobile network node 800 is an AMF. In some embodiments, the mobile network node 800 is a SMF. As shown, the mobile network node may include network interface circuitry 801 (also referred to as a network interface) configured to provide communications with other nodes of the core network and/or the network. The mobile network node may also include a processing circuitry 802 (also referred to as a processor) coupled to the network interface circuitry, and memory circuitry 803 (also referred to as memory)

coupled to the processing circuitry. The memory circuitry 803 may include computer readable program code that when executed by the processing circuitry 802 causes the processing circuitry to perform operations according to embodiments disclosed herein. According to other embodiments, processing circuitry 802 may be defined to include memory so that a separate memory circuitry is not required. As discussed herein, operations of the mobile network node may be performed by processing circuitry 802 and/or network interface circuitry 801. For example, processing circuitry 802 may control network interface circuitry 801 to transmit communications through network interface circuitry 801 to one or more other network nodes and/or to receive communications through network interface circuitry from one or more other network nodes. Moreover, modules may be stored in memory 803, and these modules may provide instructions so that when instructions of a module are executed by processing circuitry 802, processing circuitry 802 performs respective operations (e.g., operations discussed below with respect to Example Embodiments relating to core network nodes).

Figure 9 is a block diagram illustrating elements of a User Equipment (UE) 900 (also referred to as a communication device, a mobile terminal, a mobile communication terminal, a wireless device, a wireless communication device, a wireless terminal, mobile device, a wireless communication terminal, a user equipment node/terminal/device, etc.) configured to provide wireless communication according to embodiments of the disclosure. As shown, communication device UE may include an antenna 907, and transceiver circuitry 901 (also referred to as a transceiver) including a transmitter and a receiver configured to provide uplink and downlink radio communications with a base station(s) (also referred to as a RAN node) of a radio access network. The UE may also include processing circuitry 903 (also referred to as a processor) coupled to the transceiver circuitry, and memory circuitry 905 (also referred to as memory, e.g. corresponding to device readable medium) coupled to the processing circuitry. The memory circuitry 905 may include computer readable program code, such as application client 909, that when executed by the processing

circuitry 903 causes the processing circuitry to perform operations according to embodiments disclosed herein. According to other embodiments, processing circuitry 903 may be defined to include memory so that separate memory circuitry is not required. The UE 900 may also include an interface (such as a user interface) coupled with processing circuitry 903, and/or the UE may be incorporated in a vehicle. As discussed herein, operations of the UE may be performed by processing circuitry 903 and/or transceiver circuitry 901. For example, processing circuitry 903 may control transceiver circuitry 901 to transmit communications through transceiver circuitry 901 over a radio interface to a radio access network node (also referred to as a base station) and/or to receive communications through transceiver circuitry 901 from a RAN node over a radio interface. Moreover, modules may be stored in memory circuitry 905, and these modules may provide instructions so that when instructions of a module are executed by processing circuitry 903, processing circuitry 903 performs respective operations (e.g., the operations disclosed herein with respect to the example embodiments relating to the UE).

CLAIMS

1. A method performed by a User Equipment, UE (101), for enforcing tethering policies at said UE, the method comprising:

   receiving (216, 312, 314) a tethering policy from a Control Plane, CP, entity of a mobile communication system, the tethering policy including actions to apply to the traffic of tethered devices; and

   applying (412, 414) the tethering policy to the traffic of a tethered device.

2. The method of claim 1, wherein the tethering policy includes an indication to block the traffic of a tethered device.

3. The method of claim 1, wherein the tethering policy includes an indication to only allow traffic transmission of a maximum number of tethered devices connected simultaneously.

4. The method of claim 1, wherein the tethering policy includes an indication to mark the traffic of a tethered device with a specific value included in a protocol header, the value being the same for all tethered devices or different for each tethered device.

5. The method of claim 1, wherein the tethering policy includes an indication to report an event to the CP entity or another CP entity in response to the detection of traffic of a tethered device.

6. The method of claim 5, wherein the indication to report the event comprises an indication to report the number of tethered devices, the detection of a new tethered device, or the volume of the traffic of a tethered device.

7. The method of any one of claims 5 to 6, wherein applying the tethering policy comprises transmitting a report to the CP entity or another CP entity including

the number of tethered devices, the detection of a new tethered device, or the volume of the traffic of a tethered device.

8. The method of any one of claims 1 to 7, wherein the tethering policy is received from an access and mobility management entity in a Protocol Data Unit session response message or in a UE Route Selection Policy, URSP.

9. The method of any one of claims 1 to 7, wherein the tethering policy is received from a policy control entity in a UE Route Selection Policy, URSP.

10. A method performed by a policy control entity (111) for providing a tethering policy to a User Equipment, UE (101), the method comprising:

receiving (214, 311) subscription information from a subscriber data repository entity of a mobile communication system, the subscription information including an indication of actions to apply to the traffic of tethered devices at the UE; and

transmitting (215, 312, 313) to the UE or to a session management entity (107) handling the data session of the UE, a tethering policy including the received actions to apply to the traffic of tethered devices.

11. The method of claim 10, wherein the tethering policy includes an indication to block the traffic of a tethered device.

12. The method of claim 10, wherein the tethering policy includes an indication to only allow traffic transmission of a maximum number of tethered devices connected simultaneously.

13. The method of claim 10, wherein the tethering policy includes an indication to mark the traffic of a tethered device with a specific value included in a protocol header, the value being the same for all tethered devices or different for each tethered device.

14. The method of claim 10, wherein the tethering policy includes an indication to report an event to the CP entity or another CP entity in response to the detection of traffic of a tethered device.

15. The method of claim 14, wherein the indication to report the event comprises an indication to report the number of tethered devices, the detection of a new tethered device, or the volume of the traffic of a tethered device.

16. The method of any one of claims from 10 to 15, wherein the tethering policy is transmitted in a UE Route Selection Policy, URSP.

17. A method performed by an access and mobility management entity (106) for providing a tethering policy to a User Equipment, UE (101), the method comprising:

Receiving (313) a tethering policy from a policy control entity of a mobile communication system, the tethering policy including an indication of actions to apply to the traffic of tethered devices at the UE; and

Transmitting (314) to the UE the tethering policy.

18. The method of claim 17, wherein the tethering policy includes an indication to block the traffic of a tethered device.

19. The method of claim 17, wherein the tethering policy includes an indication to only allow traffic transmission of a maximum number of tethered devices connected simultaneously.

20. The method of claim 17, wherein the tethering policy includes an indication to mark the traffic of a tethered device with a specific value included in a protocol header, the value being the same for all tethered devices or different for each tethered device.

21. The method of claim 17, wherein the tethering policy includes an indication to report an event to the CP entity or another CP entity in response to the detection of traffic of a tethered device.

22. The method of claim 21, wherein the indication to report the event comprises an indication to report the number of tethered devices, the detection of a new tethered device, or the volume of the traffic of a tethered device.

23. The method of any one of claims 17 to 22, wherein the tethering policy is transmitted in a Protocol Data Unit session response message or in a UE Route Selection Policy, URSP.

24. A computer program comprising program code portions for performing the method of any one of claims 1 to 16 when the computer program is executed on one or more computing devices.

25. The computer program of claim 24, stored on a computer readable recording medium.

26. A User Equipment, UE (900), for enforcing tethering policies at said UE adapted to perform the method of any one of claims 1 to 9.

27. The UE of claim 26, comprising at least one processor and at least one memory, the at least one memory containing instructions executable by the at least one processor such that the UE is operable to perform the method of any one of claims 1 to 9.

28. A computing unit (800) configured to execute a control plane node of a mobile communication system for providing a tethering policy to a User Equipment, UE, adapted to perform any one of claims from 10 to 16 and from 17 to 23.

29. The computing unit of claim 28, comprising at least one processor and at least one memory, the at least one memory containing instructions executable by the at least one processor such that the control plane node is operable to perform the method of any one of claims from 10 to 16 and from 17 to 23.

30. A system comprising a UE according to any one of claims 26 and 27, a computing unit according to any one of claims 28 and 29, and a further computing unit according to any one of claims 28 and 29.

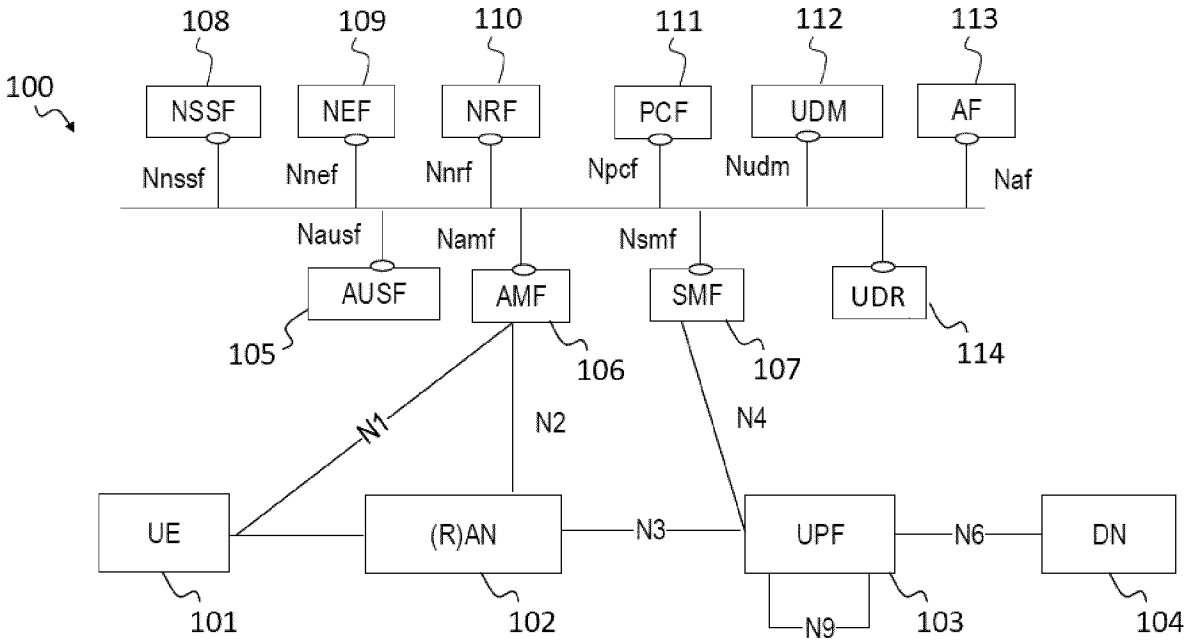

Figure 1

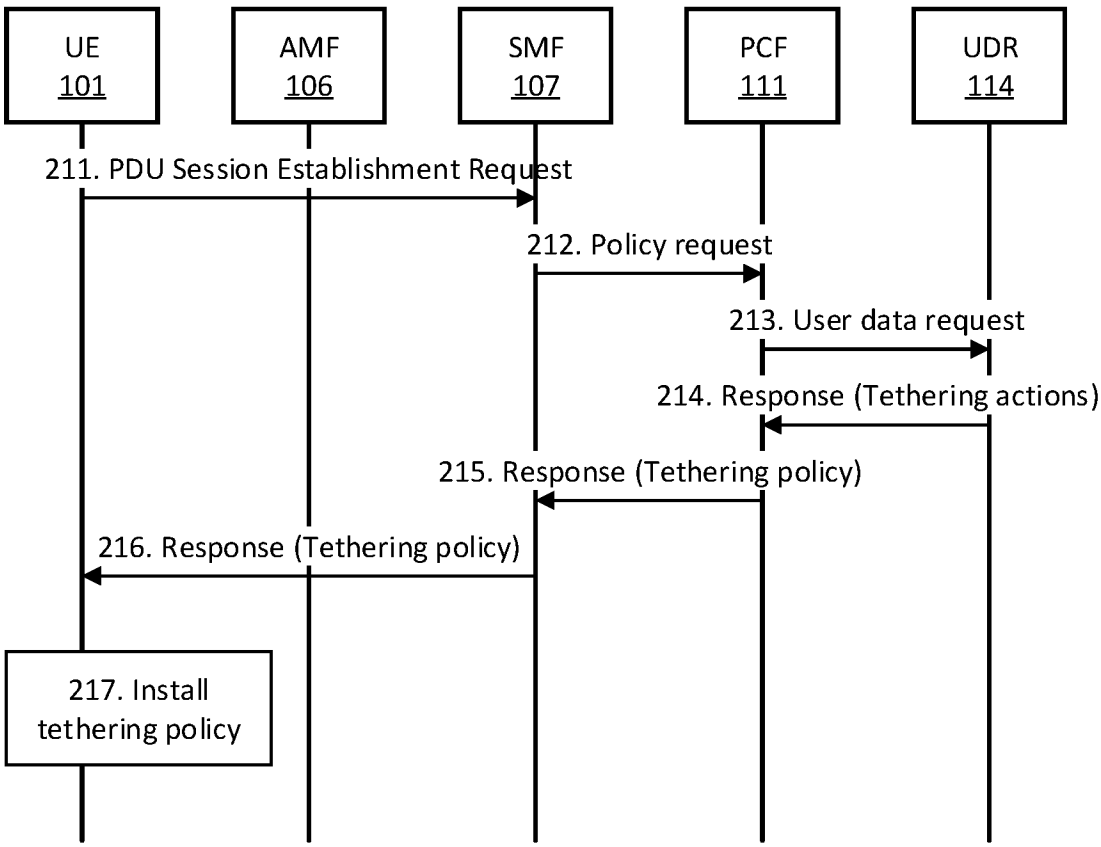

Figure 2

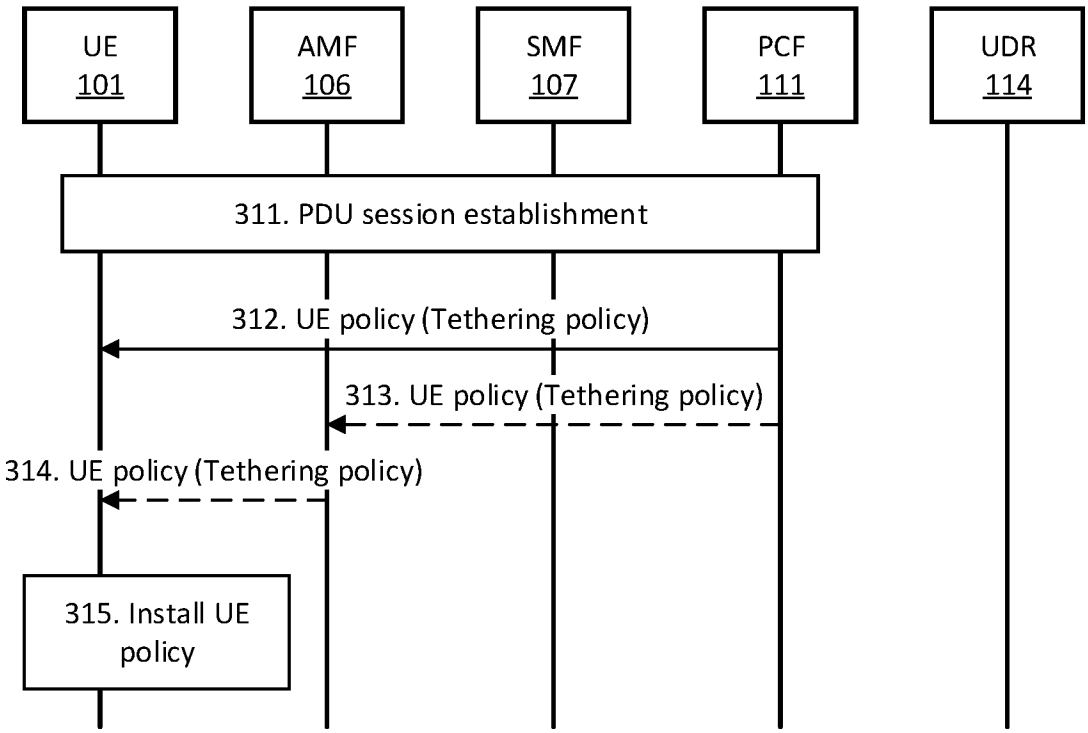

Figure 3

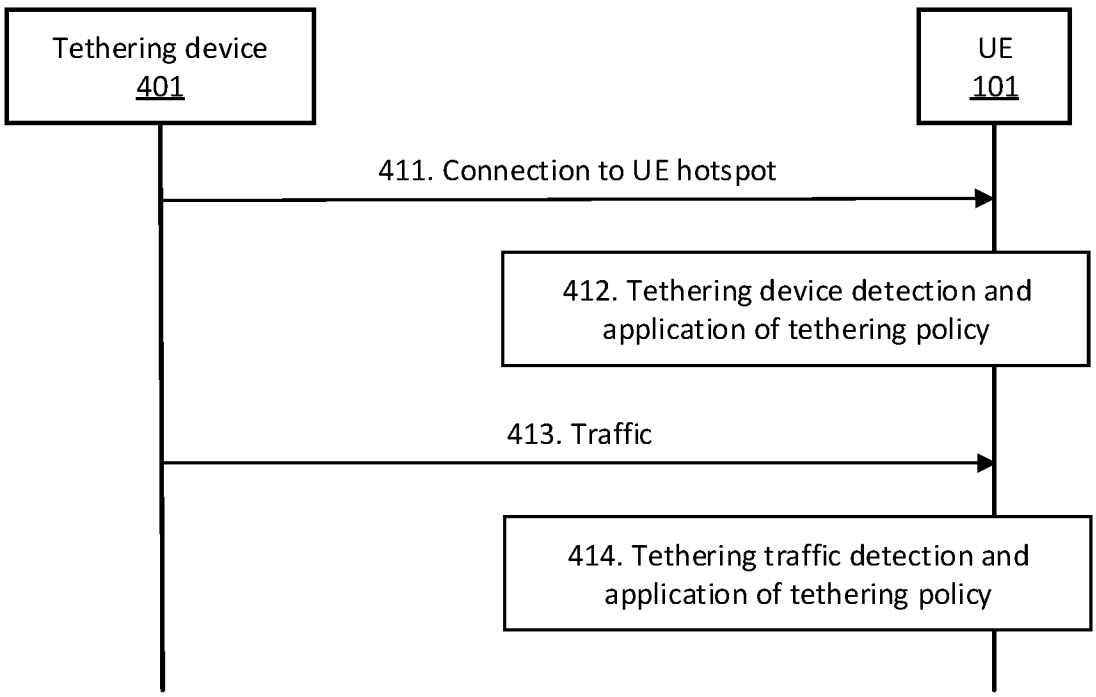

Figure 4

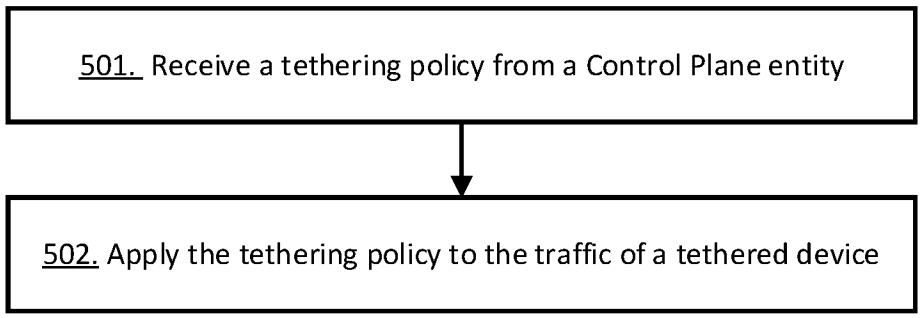

Figure 5

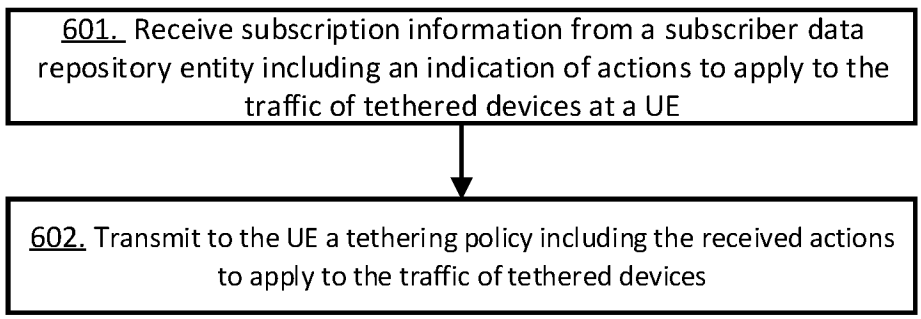

Figure 6

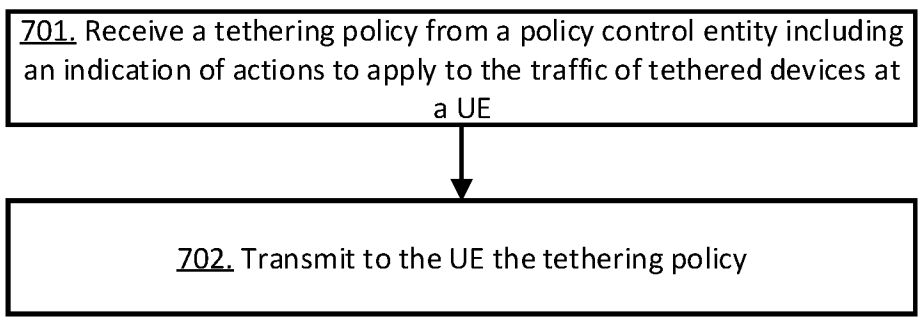

Figure 7

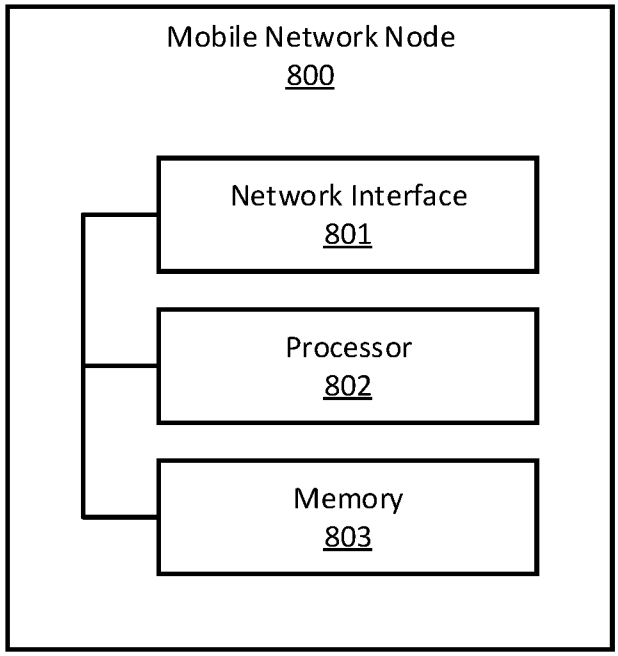

Figure 8

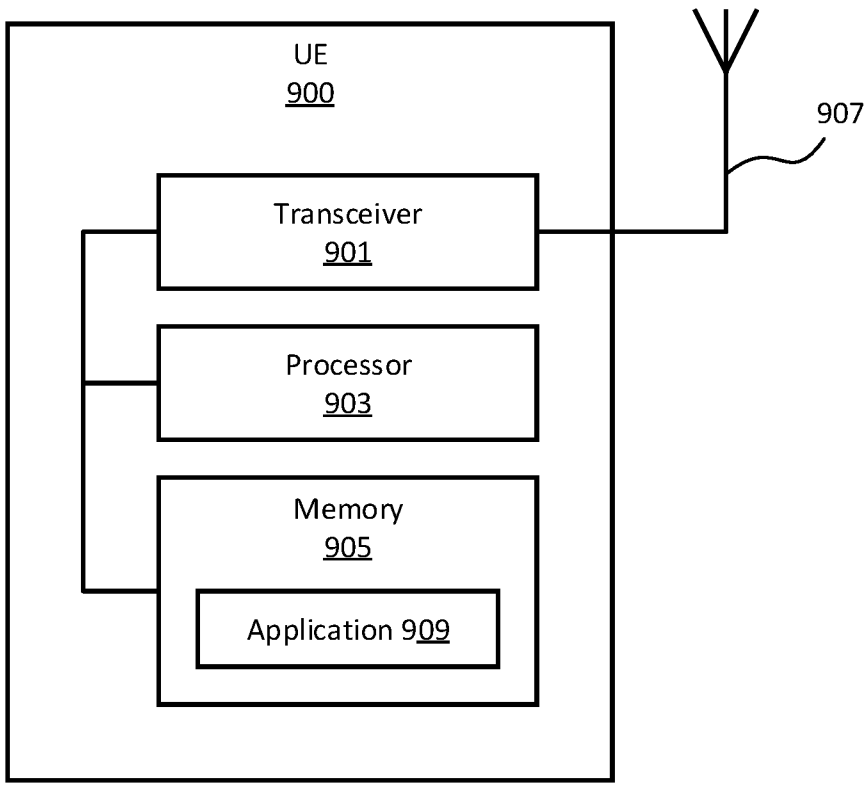

Figure 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/073776

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W4/80 H04W28/16 H04W40/02
ADD. H04W88/04 H04W12/08

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2019/223557 A1 (HUAWEI TECH CO LTD [CN]) 28 November 2019 (2019-11-28) abstract; figures 1A, 6-13	1-30
A	US 2012/240197 A1 (TRAN DZUNG [US] ET AL) 20 September 2012 (2012-09-20) paragraphs [0010] - [0035]	1-30
A	US 2020/008101 A1 (KOTECHA LALIT R [US] ET AL) 2 January 2020 (2020-01-02) paragraphs [0016] - [0017] paragraphs [0034] - [0050]	1-30
A	WO 2020/072652 A1 (INTEL CORP [US]) 9 April 2020 (2020-04-09) paragraph [0030] paragraphs [0066] - [0107]	1-30

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 February 2021	03/03/2021

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Ruiz Sanchez, J

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2020/073776

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2019/238252 A1 (ERICSSON TELEFON AB L M [SE]) 19 December 2019 (2019-12-19) page 9, line 29 - page 15, line 17; figures 2,4 -----	1-30

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2020/073776

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2019223557 A1	28-11-2019	NONE	
US 2012240197 A1	20-09-2012	EP 2687035 A1	22-01-2014
		US 2012240197 A1	20-09-2012
		WO 2012129113 A1	27-09-2012
US 2020008101 A1	02-01-2020	US 10412633 B1	10-09-2019
		US 2020008101 A1	02-01-2020
WO 2020072652 A1	09-04-2020	NONE	
WO 2019238252 A1	19-12-2019	CN 112219380 A	12-01-2021
		WO 2019238252 A1	19-12-2019