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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
03 December 2020 (03.12.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/242564 A1

(51) International Patent Classification:
H04W 76/50 (2018.01) *H04W 88/16* (2009.01)
H04W 4/90 (2018.01)

(21) International Application Number:
PCT/US2020/024519

(22) International Filing Date:
24 March 2020 (24.03.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/422,908 24 May 2019 (24.05.2019) US

(71) Applicant: **ORACLE INTERNATIONAL CORPORATION** [US/US]; 500 Oracle Parkway, Mail Stop 5OP7, Redwood Shores, CA 94065 (US).

(72) Inventor: **JUNEJA, Rohit**; 218-2 Deerfield Drive, Nepean, ON K2G3R6 (CA).

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

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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.

WO 2020/242564 A1

(54) Title: METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR ENHANCED SIGNALING GATEWAY (SGW) STATUS DETECTION AND SELECTION FOR EMERGENCY CALLS

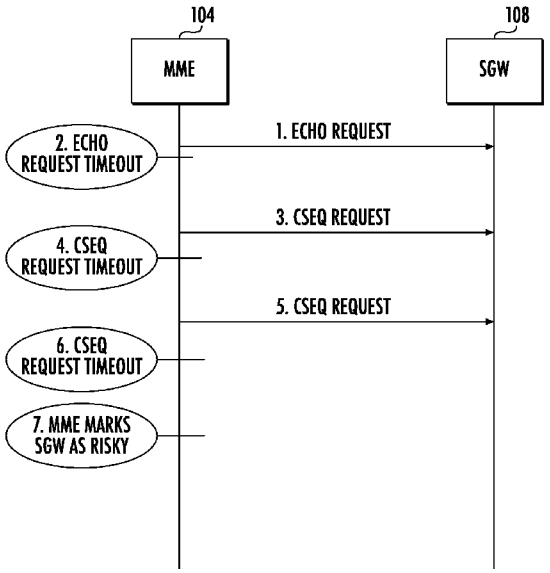

FIG. 3A

(57) Abstract: The subject matter described herein includes a method for enhanced signaling gateway status detection and selection for emergency calls. The method includes, in a mobility management entity (MME) including at least one processor, detecting that a signaling gateway is in a risky state using a combination of echo request and call setup signaling timeouts. The method further includes marking the signaling gateway as risky in a signaling gateway status database maintained by the MME. The method further includes performing signaling gateway selection for an emergency call in a manner that excludes signaling gateways marked as risky. The method further includes routing the emergency call to a signaling gateway selected by the signaling gateway selection

[Continued on next page]

(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))*

DESCRIPTION

METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR ENHANCED SIGNALING GATEWAY (SGW) STATUS DETECTION AND SELECTION FOR EMERGENCY CALLS

PRIORITY CLAIM

This application claims the priority benefit of U.S. Patent Application Serial No. 16/422,908, filed May 24, 2019, the disclosure of which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

The subject matter described herein relates to selecting or reselecting signaling gateways to handle emergency calls. More particularly, the subject matter described herein relates to methods, systems, and computer readable media for enhanced signaling gateway status detection and selection for emergency calls.

BACKGROUND

The signaling gateway is the node in the telecommunications network that communicates call setup signaling messages to a remote signaling gateway to set up voice calls between users. In some instances, the signaling gateway may go out of service, because of a hardware or software failure. In other instances, call setup may be delayed because there are multiple legs of the call between the end users. It may be desirable to avoid a failed or failing SGW for call setup procedures. In the event of multi-leg call setup traversal, it is desirable to wait for the SGW to respond to a call setup request. It may be difficult to distinguish between SGW failure and multi-leg traversal.

The mobility management entity (MME) is the node in the 3GPP mobile communications network that communicates with a signaling gateway to setup a call. While there are existing mechanisms for the MME to detect failure of a signaling gateway, the mechanisms can result in unacceptable delays in detecting the failure. In addition, as stated above, it is difficult to determine whether the signaling gateway has failed or whether

the delay in establishing the call is due to communications between multiple legs of the call.

For some types of calls, such as regular priority calls, the existing signaling gateway failure detection mechanisms are sufficient, as a delay in call setup is not critical for normal priority calls. However, for emergency calls, such as E911 calls, delayed call setup is unacceptable.

Accordingly, there exists a need for improved methods, systems, and computer readable media for signaling gateway status detection and selection for emergency calls.

SUMMARY

The subject matter described herein includes a method for enhanced signaling gateway status detection and selection for emergency calls. The method includes, in a mobility management entity (MME) including at least one processor, detecting that a signaling gateway is in a risky state using a combination of echo request and call setup signaling timeouts. The method further includes marking the signaling gateway as risky in a signaling gateway status database maintained by the MME. The method further includes performing signaling gateway selection for an emergency call in a manner that excludes signaling gateways marked as risky. The method further includes routing the emergency call to a signaling gateway selected by the signaling gateway selection.

According to one aspect of the subject matter described herein, detecting that the signaling gateway is in a risky state includes detecting that the signaling gateway is in a risky state in response to an echo request timeout from the MME to the signaling gateway and two create session request timeouts from the MME to the signaling gateway.

According to another aspect of the subject matter described herein, the echo request timeout occurs prior to the create session request timeouts.

According to yet another aspect of the subject matter described herein, the echo request timeout occurs after one of the create session request timeouts.

According to yet another aspect of the subject matter described herein, transmission of an echo request message for which the echo request timeout occurs is triggered by detection of a second of the two create session request timeouts.

According to yet another aspect of the subject matter described herein, the two create session request timeouts are for the same call.

According to yet another aspect of the subject matter described herein, the two create session request timeouts are for different calls.

According to yet another aspect of the subject matter described herein, performing the signaling gateway selection includes performing the signaling gateway selection in response to an initial attach message from an evolved Node B (eNode B).

According to yet another aspect of the subject matter described herein, performing the signaling gateway selection includes selecting a new signaling gateway for a call for which a signaling gateway assigned to the call is determined to be risky during setup of the call.

According to yet another aspect of the subject matter described herein, performing the signaling gateway selection includes selecting a new signaling gateway for a call for which a default bearer exists on an signaling gateway currently assigned to the call and that has been marked as risky.

According to yet another aspect of the subject matter described herein, a system for enhanced signaling gateway status detection and selection for emergency calls includes a mobility management entity (MME) including at least one processor. The system further includes a signaling gateway status database located in the MME and containing status information for signaling gateways accessible by the MME. The system further includes a signaling gateway status detector and emergency call router for detecting that a signaling gateway is in a risky state using a combination of echo request and call setup signaling timeouts, marking the signaling gateway as risky in a signaling gateway status database maintained by the MME, performing signaling gateway selection for an emergency call in a manner that excludes signaling gateways marked as

risky, and routing the emergency call to a signaling gateway selected by the signaling gateway selection.

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

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a network diagram illustrating an exemplary operating environment for enhanced signaling gateway failure detection and reselection for emergency calls;

Figure 2 is a block diagram of a mobility management entity for enhanced signaling gateway failure detection and reselection for emergency calls;

Figure 3A is a call flow diagram illustrating one combination of messages and timings that will result in a signaling gateway being marked as risky;

Figure 3B is a call flow diagram illustrating another combination of messages and timings that will result in a signaling gateway being marked as risky;

Figure 3C is a call flow diagram illustrating yet another combination of messages and timings that will result in a signaling gateway being marked as risky;

Figure 4A is a call flow diagram illustrating signaling gateway selection for an initial call setup when a signaling gateway has been marked as risky;

Figure 4B is a call flow diagram illustrating signaling gateway selection for an aborted call setup when a signaling gateway is marked as risky during the call setup; and

Figure 5 is a flow chart illustrating an exemplary process for enhanced signaling gateway status detection and selection for emergency calls.

DETAILED DESCRIPTION

The subject matter described herein includes methods, systems, and computer readable media for enhanced signaling gateway status detection and selection for emergency calls. As described above, it is desirable for emergency call establishment that a network node, such as an MME, be able to rapidly detect when a signaling gateway goes down and when reselection of a new signaling gateway is required. When a response from a signaling gateway is delayed for a call setup request, it is not possible for the MME to ascertain if the delay is caused by multi-leg traversal of the request or if the signaling gateway has failed or restarted. The subject matter described herein provides for rapid detection of signaling gateway status and reselection of a signaling gateway if it is determined that an existing signaling gateway has failed or is likely to be in a failure state.

Figure 1 illustrates an exemplary operating environment for the subject matter described herein. Referring to Figure 1, user equipment (UE) **100** may be a mobile device that attaches to an evolved node B (eNode B) **102** to communicate with the network. The eNode B **102** connects to an MME **104**, which performs mobility management functions and call setup functions. A home subscriber server (HSS) **106** stores mobile subscription and location information.

Signaling gateways **108** and **110** perform call setup operations to setup calls between users, such as UE **100** and a remote user. As such, each signaling gateway **108** and **110** may implement session initiation

protocol (SIP) or other call setup protocol to establish calls between end users. In the illustrated example, there are two signaling gateways **108** and **110**. MME **104** may select one of the two signaling gateways to establish a given call. Once a signaling gateway is selected for the call, provided that no failure occurs, the signaling gateway will remain in the call setup signaling path and maintain state information for the call. However, when one of signaling gateways **108** or **110** fails, MME **104** may detect the failure and attempt to reestablish the call with an alternate available signaling gateway. The subject matter described herein includes methodology for rapid identification of failure of a signaling gateway and reselection of a new signaling gateway to establish a given call.

Also illustrated in Figure 1 is a packet gateway (PGW) **112**, which provides packet-based data communications, including call setup signaling communications between network elements. An online charging system (OCS) **114** and an offline charging system (OFCS) **116** respectively perform online and offline charging functions for communications between users. A policy and charging rules function (PCRF) **118** implements network policies for communications between users. A subscription profile repository (SPR) **120** stores subscriber profile information. An application function (AF) **122** provides application services for UE devices. In one example, the UE devices may be Internet of Things (IoT) devices, such as sensors, and AF **122** may be a server that obtains data from the IoT devices.

One mechanism that can be used by MMEs to detect failure of a signaling gateway is the path management procedure described in 3GPP TS 29.060, V 15.4.0 (2019-03). According to the path management procedure described in TS 29.060, a gateway support node (GSN) or radio network controller (RNC) may send an echo request on a path to another GSN or RNC to find out if the peer GSN or RNC is alive. Echo request messages may be sent for each path associated with at least one of the active packet data protocol (PDP) context, multimedia broadcast/multicast (MBMS) UE context, or bearer context. When and how the echo request message is sent is implementation specific, but 3GPP TS 29.060 indicates that the echo

request should not be sent more often than every sixty seconds on each path (see section 7.2.1 of 3GPP TS 29.060).

When a sending node sends an echo request message on a path, the sending node starts a timer. If the timer times out before an echo response is received, a timeout occurs, and the path is considered to be down. Example values of the echo response time out can be from five to fifteen seconds and may be more, depending on the network configuration. The SGW must be prepared to receive an echo request at any time and reply with an echo response.

If the MME detects that the SGW or an S11 path has failed, the MME maintains UE context data for all UEs associated with the SGW and starts a restoration timer. An S11 path is a path between the MME and the SGW. The interface between the MME and the SGW is referred to as the S11 interface. The UE contexts are maintained on the MME for the duration of the restoration timer. Each S11 path has its own timer. A session hold time out configures a session hold timer for SGW restoration. The session hold timer must be an integer from 1 to 3600 seconds.

Another type of procedure implemented by MMEs to account for failing SGWs is requesting retransmission of a signaling message. According to 3GPP TS 29.060, a T3 response timer is started with signaling request message for which a response has been defined as sent. A signaling message request or response has probably been lost if a response is not received before the T3 response timer expires. The request is then retransmitted if the total number of request attempts is less than a number N3-request times. The timer is implemented in the control plane application as well as the user plane application for echo requests and echo responses. The wait time for a response (the T3 response timer value) and the number of retries (N3-request) is configurable by the network operator on a per procedure basis. The MME may implement a default timer of approximately five seconds for retry of a connectivity request. The MME may also have a maximum retry configuration of five times.

Once the T3 response timer expires, the message corresponding to the T3 response timer is retransmitted if the number of retry attempts is less

than N3-request times. The T3 response timer and N3-requests counter settings are implementation dependent. That is, the timers and counters are configurable per procedure. Multi-leg communications, such as create session requests and responses, require longer timer values and possibly a higher number of retransmission attempts as compared to a single leg communication. Thus, depending on the value of the counters and the number of retry attempts, call setup can be significantly delayed according to existing 3GPP echo request, response, and retransmission procedures.

Yet another document that further describes 3GPP functionality relating to SGW failure detection and recovery is 3GPP TS 29.274 V15.7.1 (2019-03). According to 3GPP 29.274, the echo request message contains a recovery information element. The recovery information element contains the value of the local restart counter. An optional private extension in the recovery information element can contain vendor or operator specific information.

Yet another 3GPP document that describes 3GPP functionality relating to recovery from SGW failure is 3GPP TS 23.401 V16.2.0 (2019-03). For example, section 4.3.8.2 of 3GPP TS 23.401 defines the signaling gateway selection function. The signaling gateway selection function selects an available signaling gateway to serve a UE. The selection is based on network topology such that the signaling gateway serves the UE's location. Considerations related to selection of a signaling gateway include the probability of changing signaling gateways and load balancing considerations. Signaling gateway selection is performed by the MME.

TS 23.401 also defines procedures for emergency services, such as emergency calls. However, there is no mention of procedures for signaling gateway selection or reselection for emergency calls.

Yet another specification that governs recovery procedures when an SGW goes down is ETSI TS 29.160 V15.2.0 (2018-07). ETSI TS 29.160 is the same specification as 3GPP TS 29.060. According to ETSI TS 29.160, the GSN that receives an echo request from a peer GSN shall compare the restart counter value received with the previous restart counter value stored for that peer GSN. If no previous value is stored, the restart counter value

received in the echo response is stored for the peer GSN. If the value of the restart counter previously stored for the peer is smaller than the restart counter value received in the echo response message, this indicates that the entity that sent the echo response has restarted. The received new restart counter value shall be stored by the receiving entity replacing the previously stored value for the peer.

Existing mechanisms for detecting SGW failure include the above-described echo request procedure and response timeouts. SGW failure with or without SGW restart consists of the MME maintaining UE context for a configurable period of time. When the MME detects path failure towards the SGW and the MME supports SGW restoration, then the MME relocates sessions from the failed SGW to another SGW. The MME sends an echo request message to an SGW and, if no response is received for three consecutive echo request messages, then the MME marks SGW as down and blacklisted.

Additionally, if three create session requests (CSReqs) for a call time out, then the SGW is marked down and blacklisted. General default value for each CSReq timeout is 60 seconds and can be more as well depending on the network.

The SGW will be marked as down if it is not possible for MME to restore the context within a time period defined by a configurable restoration timer. The SGW restoration timer is configurable by operators with values ranging from 1 to 3600 seconds. If the same SGW has recovered, then context data is not maintained on the MME/PGW. Thus, using either the echo request or the retransmission timeout procedure for detecting SGW failure, the detection can take 180 seconds or longer.

One instance in which delayed detection of SGW failure is undesirable is for emergency calls. An emergency call is made with an emergency registration. In one example, the MME has not marked an SGW as down but no response obtained from the SGW due to partial failure/transition to failure condition. An emergency call starts with the emergency registration by the UE during the initial attach procedure. The attach type in the registration message indicates emergency attach. The

MME selects the PGW based on the access point name (APN) provided in the initial attach message. The MME then selects the SGW based on the selected PGW and tracking area identifier (TAI) list. If the MME selects an SGW which is not marked as down/blacklisted but in partial failure condition, the MME would retry with three create session request and response timeouts, with each timeout at 60 seconds apart by default. Additionally, if three echo requests/responses fail, MME will mark the SGW as down. If there are pending call setup requests waiting for response, then those will be aborted as well. As indicated above, these existing mechanisms for handling SGW failure could lead to unacceptable delay in setting up emergency calls.

Another instance relating to emergency calls in which delayed detection of SGW failure causes further delay in emergency call establishment is when a default bearer is provided by a failed SGW. Like the previous examples, in this example, an emergency call is made with an emergency registration. The MME has not marked the SGW as down, but no response is obtained from the SGW due to partial failure/transition to failure condition. In this example, it is assumed that a default bearer already exists for the user with the failing SGW. The MME selects the same failing SGW while establishing the emergency call. If the MME selects a failing SGW, which is not marked as down/blacklisted but in partial failure condition, then the MME would retry with three create session request and response timeouts, with each timeout at 60 seconds apart by default. Additionally, if three echo request/response failures occur, the SGW is marked down, the transaction is aborted, and a new create session request is sent to an alternate SGW. Using this procedure, the delay in re-establishing the emergency call could be unacceptable.

In order to avoid the unacceptable delays in detecting SGW failure in establishing emergency calls, the subject matter described herein includes a two-part solution in which SGWs are identified as risky or in a partially failed state. A list of risky, healthy, and blacklisted or down SGWs are maintained by the MME. The MME uses the list of SGWs and their corresponding state to determine whether or how to allow emergency calls. Figure 2 is a block

diagram illustrating an MME **104** with enhanced SGW failure detection and emergency call routing. Referring to Figure 2, MME **104** includes at least one processor **200** and a memory **202**. MME **104** further includes an enhanced SGW status detector and emergency call router that rapidly detects SGW state, such as failed state, or partially failed state, stores SGW state in SGW status database **206** and uses the information in SGW status database **206** to establish and reestablish emergency calls. The operation of enhanced SGW status detector and emergency call router **204** will now be described in more detail.

In one example, enhanced SGW status detector and emergency call router **204** may utilize the following conditions to mark an SGW as risky in database **206**. The following conditions may be used to mark an SGW as risky:

1. At least one echo request timeout from MME **104** to the SGW; and
2. Two create session request timeouts for any calls from MME **104** to the SGW in question. The create session request timeouts may be from the same call or from different calls. Whether to mark the SGW as risky based on consecutive create session request timeouts from the same call or different calls may be a configurable parameter.

If the above listed conditions are met, enhanced SGW status detector and emergency call router **204** may mark the SGW as risky in SGW status database **206**. If two create session time outs occur between MME **104** and the SGW being tested and an echo request time out has not occurred, MME **104** may send an echo request message immediately, rather than waiting until the timeout period between echo requests expires. If the echo request times out, the SGW may be marked as risky. If the echo request does not time out, the SGW may be marked as up or available in the database **206**.

If a response from an SGW marked as risky is received, then the status of the SGW may be marked as available or up. The response can be a response to a create session request or a response to an echo request.

The echo request timeout is generally five seconds, and the create session request timeout is sixty seconds. Either of these values can be

increased depending on the network configuration. Thus, instead of waiting for three consecutive echo request timeouts, or three consecutive connection request timeouts, enhanced SGW status detector and emergency call router **204** marks an SGW as risky based on the above described combination of at least one echo request timeout and two create session request timeouts. Because echo request and create session request timeouts are used in combination to detect SGW status, the solution is more robust than methods that rely on these types of timeouts individually. In addition, because the number of timeouts required to mark an SGW are risky is reduced over the conventional case, SGW failure or riskiness can be detected more rapidly. Finally, because SGW status, including risky status, is stored in database **206** maintained by MME **104** and used by MME **104** in SGW selection, risky SGWs that would result in delayed emergency calls can be avoided.

In another example, risky SGW detection can be performed early if one echo request has already failed and two connection request timeouts occur across the MME to the SGW. In this case, the SGW is marked as risky and will be avoided for emergency calls.

Figures 3A and 3B are example call flows that illustrate two instances in which an SGW may be marked as risky. Referring to Figure 3A, in line 1 of the call flow, MME **104** sends an echo request message to SGW **108**. When MME **104** sends the echo request message, MME **104** starts an echo request timer, which may be set to a relatively short value, such as 5 seconds. If SGW **108** does not respond within the timeout period for the echo request, i.e., before the echo request timer expires, MME **104** may increment an echo request timeout counter, indicating that an echo request timeout has occurred. In line 2 of the call flow diagram, the echo request timer expires, and MME **108** increments the echo request timeout counter.

When MME **104** receives an initial attach message from an eNode B, MME **104** may select a signaling gateway using signaling gateway selection criteria, such as load balancing. MME **104** may exclude from the selection, any signaling gateways marked as risky. In this example, it is assumed that MME **104** selects signaling gateway **108**. Accordingly, in line 2 of the call

flow diagram, MME **104** sends a connection setup request to SGW **108**. In line 3 of the call flow, MME 104 sends a create session request to SGW **108**. The create session request message may be sent in response to an initial attach message received from an eNode B. When MME **104** sends the create session request message, MME **104** starts a timer for the create session request message. The time may be set to a longer value than the echo request timer, but the value may depend on whether the call has multiple legs. When MME **104** does not receive a response to the create session request within the timeout period for the request, MME **104** may increment a create session request counter. In the example illustrated in Figure 3A, it is assumed that a create session request timeout occurs in line 5. When the create session request timeout counter expires, MME **104** increments the create session request timeout counter. Thus, after line 2 in the call flow in Figure 3A, both the echo request timeout counter and the create session request timeout counter have a value of 1.

MME **104** may re-attempt transmission of the create session request a configurable number of times. Assuming that the configurable number of times has not been exceeded, in line 6 of the call flow diagram, MME **104** sends another create session request to SGW **108**. In this example, the create session request message is a retransmission of the create session request message in line 4, which is for the same call. When the create session request timer expires for the create session request message in line 6, MME **104** increments the create session request timeout counter. Because the echo request timeout counter is at least 1 and the create session request timeout counter is at least 2, in line 7, MME **104** marks SGW **108** as risky. Thus, one scenario in which MME **104** may mark an SGW as risky is when an echo request timeout followed by two create session request timeouts occurs.

Figure 3B illustrates another scenario in which MME **104** may mark an SGW as risky. In Figure 3B, in line 1 of the call flow diagram, MME **104** sends a create session request message to SGW **108**. The create session request may be in response to receiving a create session request from an eNode B. After sending the create session request message, SGW **108**

starts the create session request timer. If a response is not received before the timer expires, a timeout occurs. Accordingly, in line 2, the create session timer expires, and MME **104** increments the create session request timeout counter.

In line 2 of the call flow diagram, MME **104** sends a second create session request message to SGW **108**. The second create session request message may be for the same or for a different call than the create session request in line 1. When MME 104 transmits the create session request message in line 3, MME 104 starts the create session request timer. If a response is not received before the create session request timer expires, a timeout occurs. Accordingly, in line 4, a second create session request timeout occurs, and MME **104** increments the create session request timeout counter. Thus, after line 2, the create session request timeout counter has a value of 2.

In line 5 of the call flow diagram, rather than waiting for the next echo request retransmission period, the value of the create session request timeout counter reaching a value of two may trigger MME **104** to send an echo request message to SGW **108**. Immediately sending the echo request message when the create session request timeout counter reaches a value of two can facilitate rapid detection of an SGW with risky status. When MME **104** transmits the echo request message, MME 104 starts the echo request timer. If a response is not received before the timer expires, a timeout occurs. In line 6, the echo request timer expires, and MME 104 increments the echo request timeout counter. After line 6, the echo request timeout counter has a value of one, and the connection setup request timeout counter has a value of two. Accordingly, in line 7, MME **104** marks SGW **108** as risky.

It should be noted that the call setup request and echo request procedures operate independently from each other and thus the timeout period may be further shortened in the timeout period for the call setup requests and the echo requests run in parallel. This scenario is illustrated in Figure 3C. In Figure 3C, in line 1, MME **104** sends a create session request message to SGW **108**. Before the create session request timeout occurs,

MME **104** sends in line 2 an echo message to SGW **108**. The sending of the echo request message in line 2 may be triggered by the time period between successive echo request messages elapsing. In line 3, the echo request timer expires because MME **104** does not receive a response to the echo request message, and MME **104** increments the echo request timeout counter. In line 4 of the call flow diagram, the create session request timer expires, an MME **104** increments the create session request timeout counter.

In line 5, MME **104** sends a second create session request message to SGW **108**. In line 6, the create session request timer expires, and MME **104** increments the create session timeout counter. After line 6, the echo request timeout counter has a value of one and the create session request timeout counter has a value of two. Accordingly, in line 7, MME **104** marks SGW **108** as risky. Thus, Figure 3C illustrates the case where timeout periods for create session and echo request messages run in parallel.

As indicated above, once an SGW is marked as risky, emergency calls should not be routed to the risky SGW. In one example, when enhanced SGW status detector and emergency call router **204** receives a create session request for a call marked as an emergency call, enhanced SGW status detector and emergency call router **204** may traverse the list of SGWs in SGW status database **206**. If the status of a given SGW is marked as risky, it will be avoided for emergency call setup. If an SGW is not marked as risky or down, it may be selected for an emergency call, based on any other suitable criteria, including load balancing.

For an initial attachment for an emergency call, a UE identifies a call as an emergency call in the initial attach message. When such a message reaches MME **104**, it is determined whether plural SGWs are available for the call. If plural SGWs are available and some of the SGWs are marked as risky, the risky SGWs may be omitted from the SGW selection process. Enhanced SGW status detector and emergency call router **204** may select from SGWs that are not marked as risky or down. Enhanced SGW status detector and emergency call router **204** then routes the create session message to the selected SGW.

Figure 4A is a call flow diagram illustrating the bypassing of the risky signaling gateway for an initial attachment of an emergency call. Referring to Figure 4A, in line 1 of the call flow diagram, UE **100** sends an initial attach message to eNode B **102** for an emergency call. In line 2, eNode B **102** sends the initial attach message to MME **104**. In line 3, MME **104** performs signaling gateway selection by accessing database **206** and determining that SGW **108** is marked as risky. Accordingly, in line 4, MME **104** bypasses risky SGW **108** and sends a create session request message to SGW **110**, which is not marked as risky.

Another use case for the subject matter described herein occurs when an emergency call setup is in progress with an SGW and the SGW fails or is determined to be risky during the call setup. In this example, if an emergency call setup is in progress, enhanced SGW status detector and emergency call router **204** aborts call setup with the existing SGW, selects a new non-risky SGW, and initiates call setup with the newly selected SGW. Figure 4B illustrates this case.

Referring to Figure 4B, in line 1, UE **100** sends an initial attach message to eNode B **102** for an emergency call. In line 2, eNode B **102** sends the initial attach message to MME **104**. In line 3, MME **104** performs signaling gateway selection by accessing database **206** and selecting SGW **108**, which is not currently marked as risky. Accordingly, in line 4, MME **104** sends a create session request message to SGW **108**.

In line 5, the echo request request timer expires, resulting in an echo request timeout. In this example it is assumed that two CSeq request timeouts have occurred when the echo request timeout occurs. As a result, in line 5, MME **104** marks SGW **108** being marked as risky. In line 6, rather than waiting for the CSeq request timer to expire, MME **104** aborts the call setup with risky SGW **108**, selects a new non-risky SGW **110**, and, in line 7, sends a new create session request message to non-risky SGW **110**.

Yet another use case for the subject matter described herein is the routing of emergency calls when a default bearer exists. According to this procedure, when an emergency 911 call is made, and a default bearer already exists for the user with a signaling gateway SGW 1, and SGW 1 is

marked as risky, the following steps describe the processing of a new request:

1. A new create session request arrives at the MME.
2. The MME determines that SGW 1 is marked as risky in database **206** and thus does not select the default bearer provided by SGW 1 for the new session.
3. The MME selects another SGW, SGW 2, for the call where SGW 2 is not marked as risky.
4. Context data blocks at the PGW with respect to SGW 1 are deleted once the new create session request reaches the PGW.
5. The context data block on SGW 1 would timeout.
6. With additional configuration, once the temporary emergency call is completed, the context data on SGW 2 may be cleared because the context data was obtained from SGW 1.
7. The MME may be updated to select SGW 2 for all future calls while the configuration to pick SGW 2 remains.

The call flow for the default bearer case may be the same as that illustrated in Figure 4A or Figure 4B, depending on whether call setup is in progress or not at the time the SGW is marked as risky.

Figure 5 is a flow chart illustrating an exemplary process for enhanced SGW failure detection and emergency call routing. Referring to Figure 5, in step **500**, an SGW is determined to be in a risky state based on a combination of echo request and call setup signaling timeouts. For example, enhanced signaling gateway status detector and emergency call router **204** may determine that an SGW is in a risky state if one echo request timeout and two call setup signaling message timeouts occur for a given SGW. In one example, as illustrated in Figure 3A, enhanced signaling gateway status detector and emergency call router **204** may mark an SGW as risky in response to an echo request timeout followed by two create session setup request timeouts. In another example as illustrated in Figure 3B, enhanced signaling gateway status detector and emergency call router **204** may mark an SGW as risky when there is at least some overlap between create session setup and echo request timeout periods. In yet

another example as illustrated in Figure 3C, enhanced signaling gateway status detector and emergency call router **204** may send an echo request message triggered by a second create session request timeout and may mark an SGW as risky in response to timeout of the echo request timeout.

In step **502**, the SGW is marked as risky in an SGW status database maintained by the MME. For example, enhanced SGW status detector and emergency call router **204** may mark SGWs detected as being risky in database **206**.

In step **504**, signaling gateway selection is performed for the emergency call in a manner that bypasses signaling gateways marked as risky. For example, enhanced signaling gateway status detector and emergency call router **204** may select a non-risky signaling gateway for a call from among available non-risky signaling gateways in SGW status database **206**. The selection may be an initial signaling gateway selection for an emergency call for which no previous SGW has been selected, as illustrated in Figure 4A. In another example, the selection may be a selection of a new signaling gateway for a call setup in progress when the existing signaling gateway selected for the call is marked as risky during the call setup, as illustrated in Figure 4B.

In step **506**, the emergency call is routed to the SGW selected by the SGW selection process. Routing the call to the selected SGW may be effected by sending a create session setup request message to the selected SGW.

Exemplary advantages of the subject matter described herein include the following:

1. Because SGWs that are transitioning to a failure state can be detected early, a delay in establishment of emergency calls is reduced;
2. A network optimization can also be obtained as the number of calls routed to a failing SGW is reduced, which results in a reduced number of redirections and retry attempts.
3. The number of failure messages, network utilization, and time required for SGW transitions are reduced.

An advance or advantage relating to early detection of SGW failure during initial emergency call establishment over existing procedures is that under existing procedures, it takes three consecutive connection request timeouts to select another SGW. If the default value of the connection request timeouts is sixty seconds, it would take 180 seconds before blacklisting the SGW.

Similarly, if echo request is enabled, another echo request is sent after a default value of sixty seconds with a default value for a timeout of five seconds. Three failures would be required to mark the SGW as down. Thus, using existing echo request procedures, a minimum of 185 seconds would be required to detect the SGW failure.

With the enhanced SGW status detector and emergency call router **204**, instead of depending on three consecutive connection request time\outs or three consecutive echo request timeouts, a combination of these messages can be used to reduce call setup time. For example, enhanced SGW status detector and emergency call router **204** checks for an echo request failure towards an SGW in question across the node instead of a call. A counter of failed echo requests is incremented in response to an echo request timeout. If two call setup request time outs occur, an echo request is transmitted immediately instead of waiting sixty seconds since the last echo request initialization. This could result in sixty seconds or more of decreased call setup time. If a failure on an echo request and two call setup requests occur from the MME to the SGW, the SGW is marked as risky for emergency calls.

If an echo request has already failed and two more call setup failures occur, the SGW is marked as risky. If the call setup response is received, the counters are cleared, and the SGW is not marked as risky. Thus, the combination of detection using both types of messages results in rapid establishment of emergency calls.

The early SGW status detection procedures described herein can also facilitate reestablishment when a bearer is already set up, but radio frequency (RF) side channels have been cleaned up due to idle timeout, and a reattach is needed.

If an initial emergency attach is received, instead of picking a preselected signaling gateway or a new signaling gateway which could be in a risky state, MME **104** picks an SGW that is not marked as risky.

If an emergency call setup is in progress, instead of waiting for a complete failure detection timeout due to non-receipt of call setup signaling messages, MME **104** detects risky SGWs early, aborts call setup with risky SGWs, and starts a session with a non-risky SGW.

The disclosure of each of the following references is hereby incorporated by reference herein in its entirety.

REFERENCES

1. 3GPP TS 29.060, V 15.4.0 (2019-03); 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface (Release 15)
2. 3GPP TS 29.274 V15.7.1 (2019-03); 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3 (Release 15)
3. 3GPP TS 23.401 V16.2.0 (2019-03); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 16)
4. ETSI TS 29.160 V15.2.0 (2018-07) Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp interface (3GPP TS 29.060 version 15.2.0 Release 15)

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

5

CLAIMS

What is claimed is:

1. A method for enhanced signaling gateway status detection and selection for emergency calls, the method comprising:

in a mobility management entity (MME) including at least one processor:

detecting that a signaling gateway is in a risky state using a combination of echo request and call setup signaling timeouts;

marking the signaling gateway as risky in a signaling gateway status database maintained by the MME;

performing signaling gateway selection for an emergency call in a manner that excludes signaling gateways marked as risky; and

routing the emergency call to a signaling gateway selected by the signaling gateway selection.

2. The method of claim 1 wherein detecting that the signaling gateway is in a risky state includes detecting that the signaling gateway is in a risky state in response to an echo request timeout from the MME to the signaling gateway and two create session request timeouts from the MME to the signaling gateway.

3. The method of claim 2 wherein the echo request timeout occurs prior to the create session request timeouts.

4. The method of claim 2 wherein the echo request timeout occurs after one of the create session request timeouts.

5. The method of claim 2 wherein transmission of an echo request message for which the echo request timeout occurs is triggered by detection of a second of the two create session request timeouts.

6. The method of any one of claims 2 to 5 wherein the two create session request timeouts are for the same call.

7. The method of any one of claims 2 to 5 wherein the two create session request timeouts are for different calls.

8. The method of any preceding claim performing the signaling gateway selection includes performing the signaling gateway selection in

response to an initial attach message from an evolved Node B (eNode B).

9. The method of any preceding claim wherein performing the signaling gateway selection includes selecting a new signaling gateway for a call for which a signaling gateway assigned to the call is determined to be risky during setup of the call.

10. The method of any preceding claim wherein performing the signaling gateway selection includes selecting a new signaling gateway for a call for which a default bearer exists on an signaling gateway currently assigned to the call and that has been marked as risky.

11. A system for enhanced signaling gateway status detection and selection for emergency calls, the system comprising:

a mobility management entity (MME) including at least one processor;

a signaling gateway status database located in the MME and containing status information for signaling gateways accessible by the MME; and

a signaling gateway status detector and emergency call router for detecting that signaling a gateway is in a risky state using a combination of echo request and call setup signaling timeouts, marking the signaling gateway as risky in a signaling gateway status database maintained by the MME, performing signaling gateway selection for an emergency call in a manner that excludes signaling gateways marked as risky, and routing the emergency call to a signaling gateway selected by the signaling gateway selection.

12. The system of claim 11 wherein detecting that the signaling gateway is in a risky state includes detecting that the signaling gateway is in a risky state in response to an echo request timeout from the MME to the signaling gateway and two create session request timeouts from the MME to the signaling gateway.

13. The system of claim 12 wherein the echo request timeout occurs prior to the create session request timeouts.

14. The system of claim 12 wherein the echo request timeout occurs after one of the create session request timeouts.

15. The system of claim 12 wherein transmission of an echo request message for which the echo request timeout occurs is triggered by detection of a second of the two create session request timeouts.

16. The system of any one of claims 12 to 15 wherein the two create session request timeouts are for the same call.

17. The system of any one of claims 12 to 15 wherein the two create session request timeouts are for different calls.

18. The system of any one of claims 11 to 17 performing the signaling gateway selection includes performing the signaling gateway selection in response to an initial attach message from an evolved Node B (eNode B).

19. The system of any one of claims 11 to 18 wherein performing the signaling gateway selection includes selecting a new signaling gateway for a call for which a signaling gateway assigned to the call is determined to be risky during setup of the call.

20. A non-transitory computer readable medium having stored thereon executable instructions that when executed by the processor of a computer controls the computer to perform steps comprising:

in a mobility management entity (MME) including at least one processor:

detecting that a signaling gateway is in a risky state using a combination of echo request and call setup signaling timeouts;

marking the signaling gateway as risky in a signaling gateway status database maintained by the MME;

performing signaling gateway selection for an emergency call in a manner that excludes signaling gateways marked as risky; and

routing the emergency call to a signaling gateway selected by the signaling gateway selection.

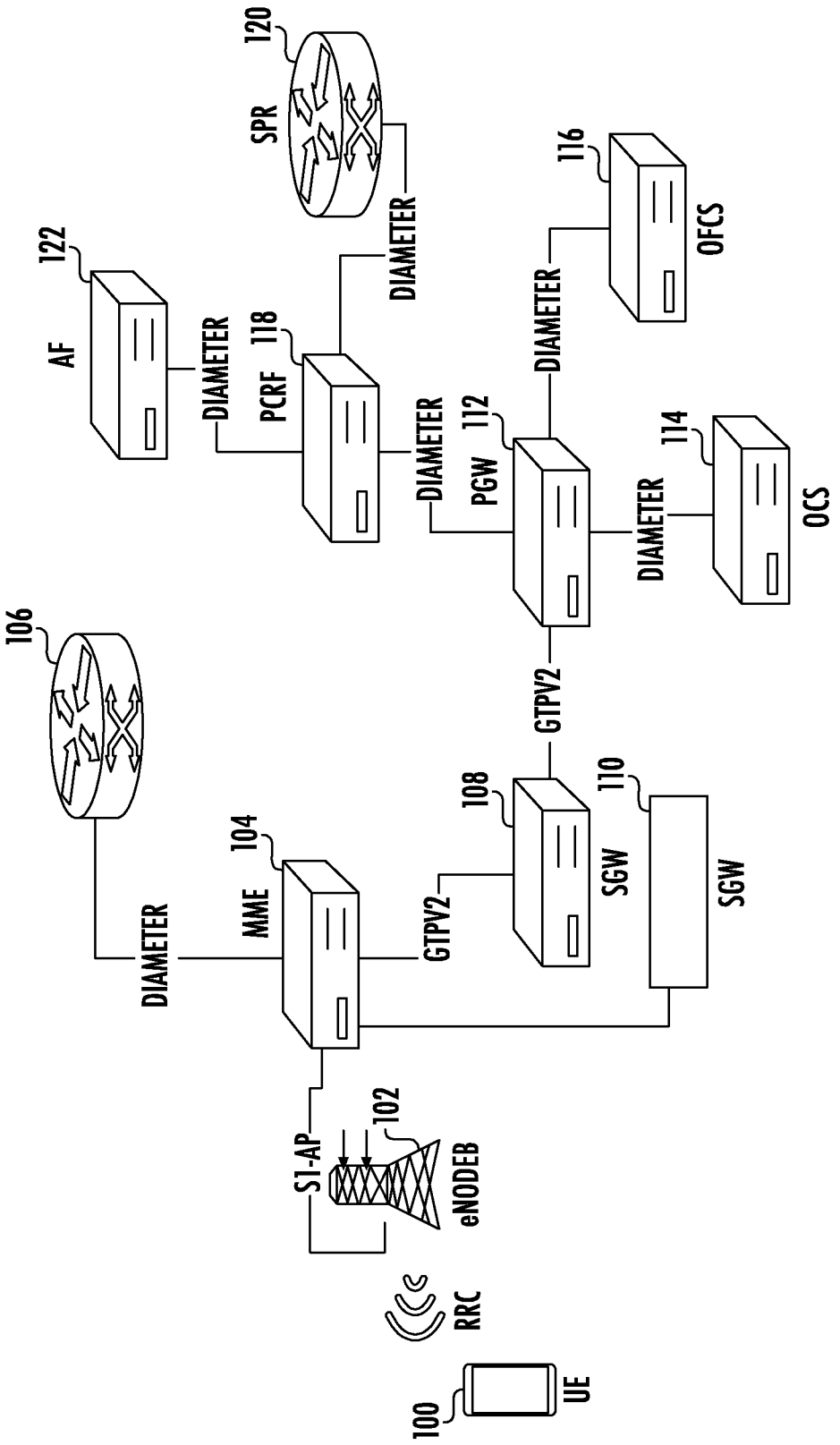
120
SPR
DIAMETER
116
OFCS
122
AF
DIAMETER
PCRF
118
DIAMETER
DIAMETER
112
PGW
114
DIAMETER
OCS
106
GTPV2
108
SGW
110
SGW
104
DIAMETER
MME
GTPV2
S1-AP
102
eNODEB
RRC
100
UE

FIG. 1

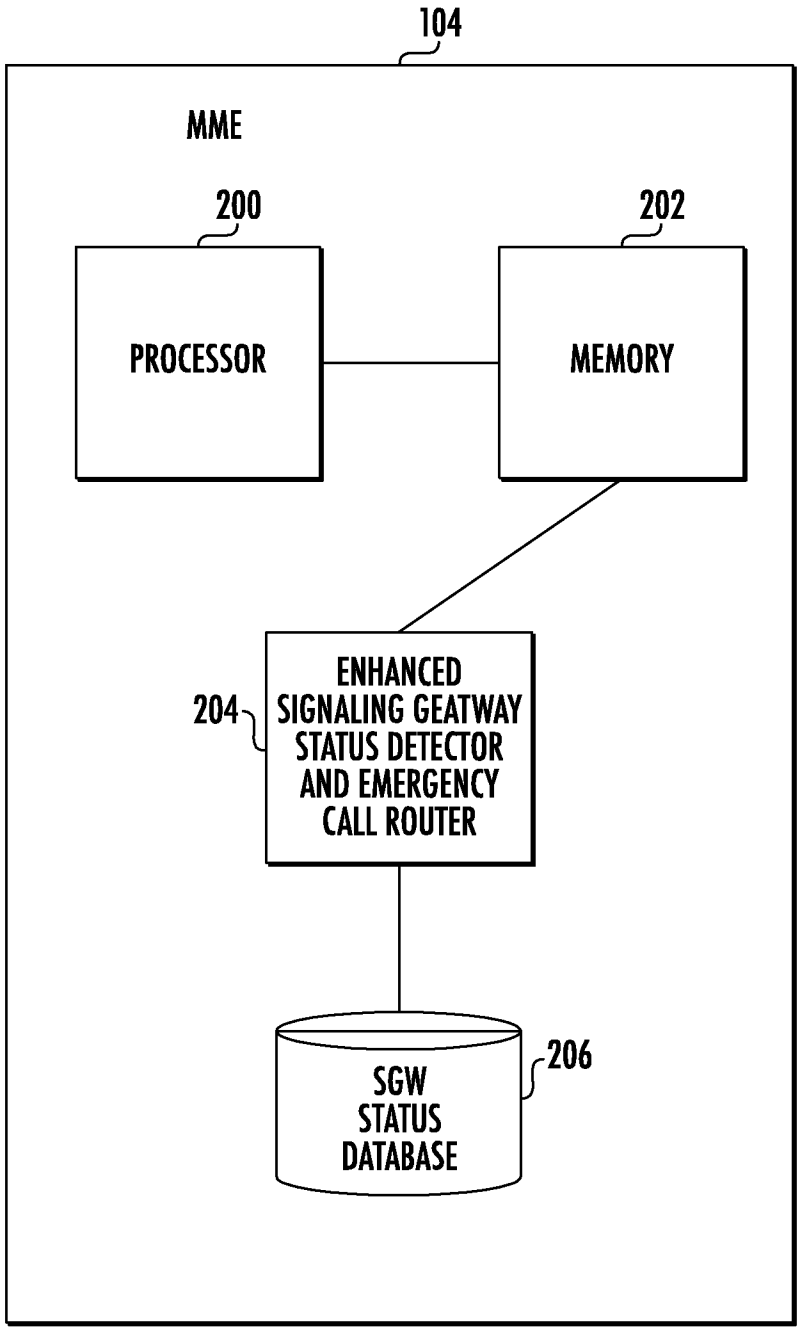
104
MME
200
PROCESSOR
202
MEMORY
204
ENHANCED SIGNALING GEATWAY STATUS DETECTOR AND EMERGENCY CALL ROUTER
206
SGW STATUS DATABASE

FIG. 2

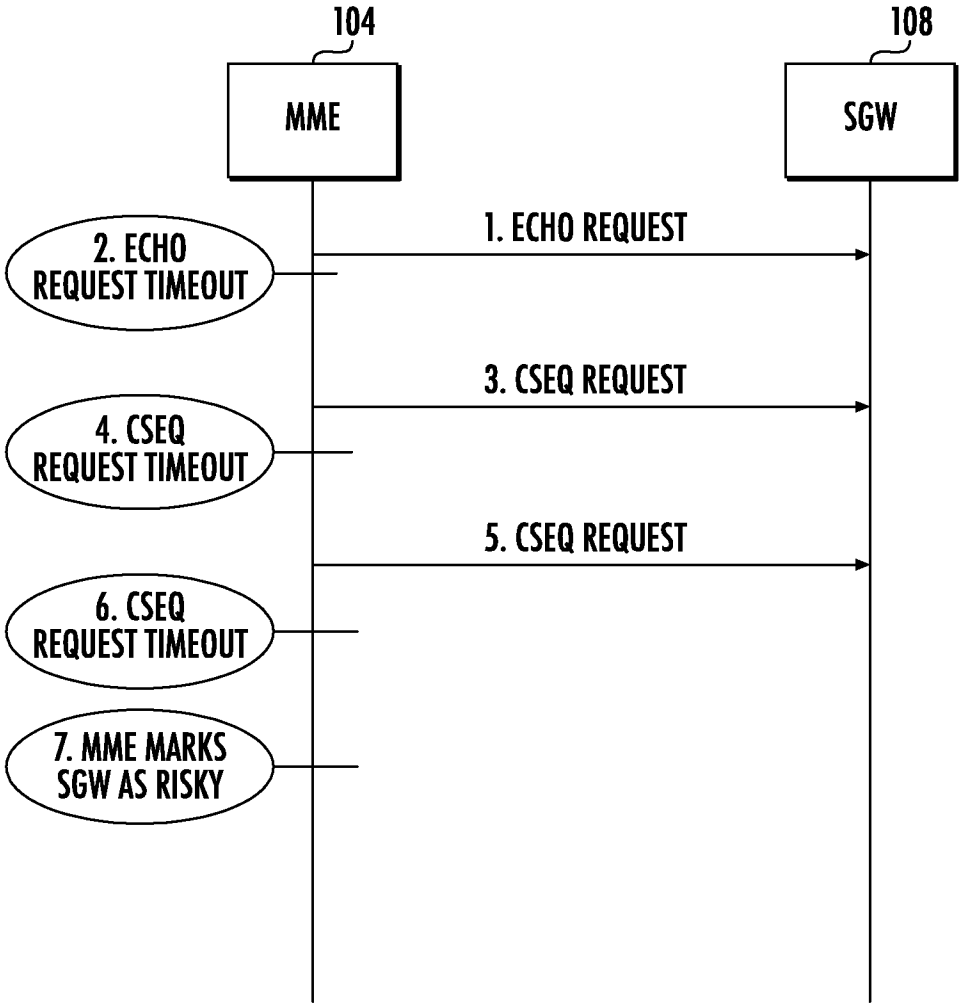
104
MME
108
SGW
1. ECHO REQUEST
2. ECHO REQUEST TIMEOUT
3. CSEQ REQUEST
4. CSEQ REQUEST TIMEOUT
5. CSEQ REQUEST
6. CSEQ REQUEST TIMEOUT
7. MME MARKS SGW AS RISKY

FIG. 3A

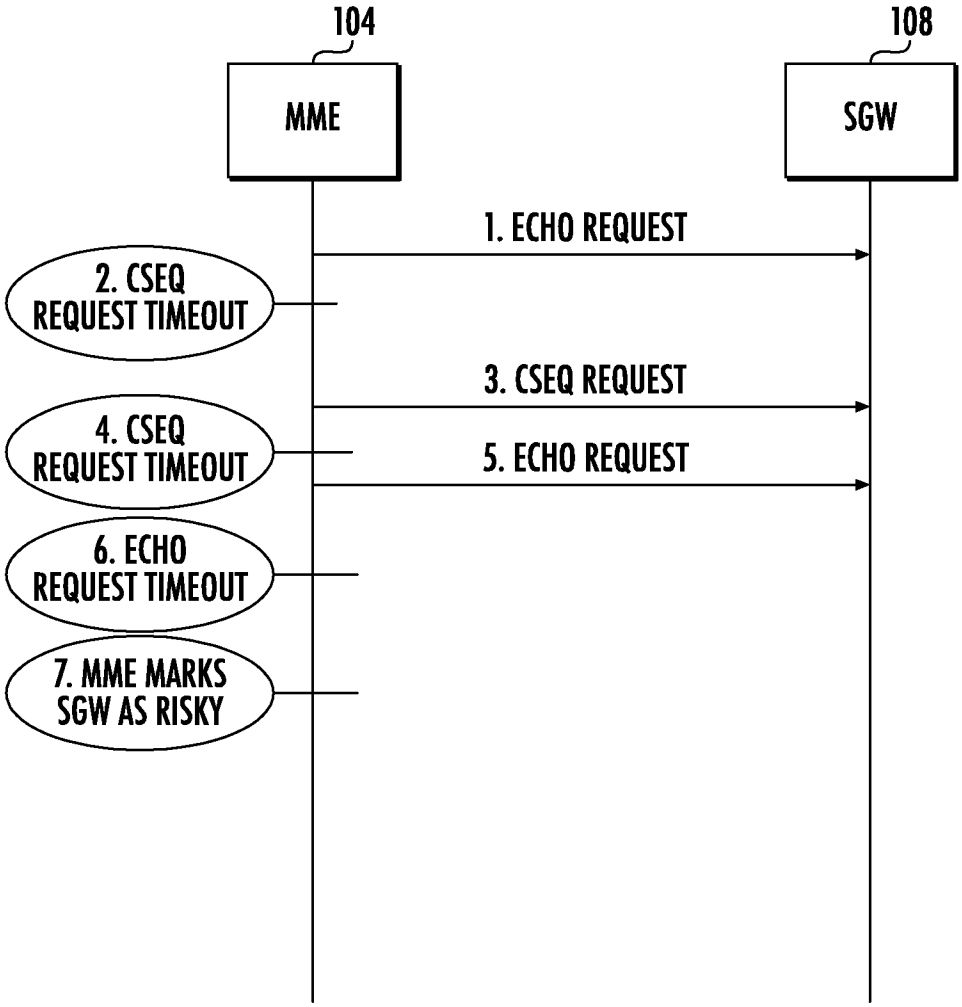
104
MME
108
SGW
1. ECHO REQUEST
2. CSEQ REQUEST TIMEOUT
3. CSEQ REQUEST
4. CSEQ REQUEST TIMEOUT
5. ECHO REQUEST
6. ECHO REQUEST TIMEOUT
7. MME MARKS SGW AS RISKY

FIG. 3B

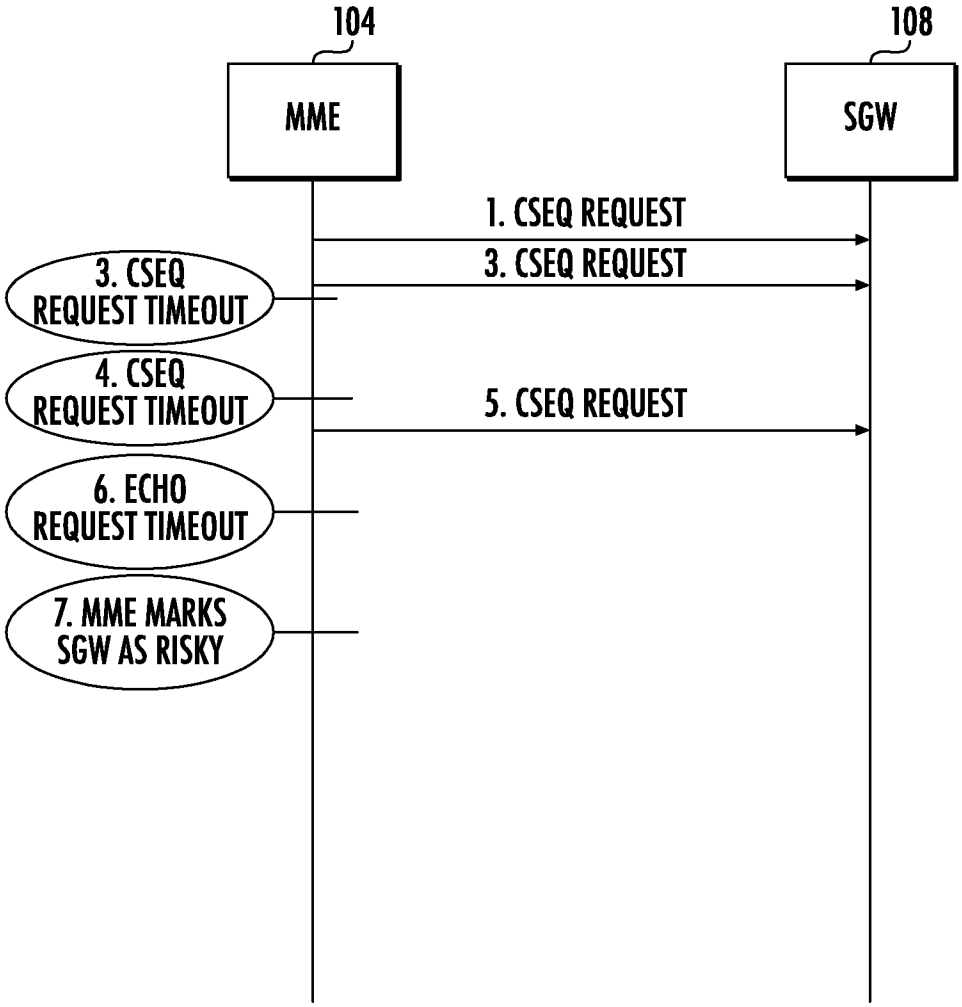
104
MME
108
SGW
1. CSEQ REQUEST
3. CSEQ REQUEST
3. CSEQ REQUEST TIMEOUT
4. CSEQ REQUEST TIMEOUT
5. CSEQ REQUEST
6. ECHO REQUEST TIMEOUT
7. MME MARKS SGW AS RISKY

FIG. 3C

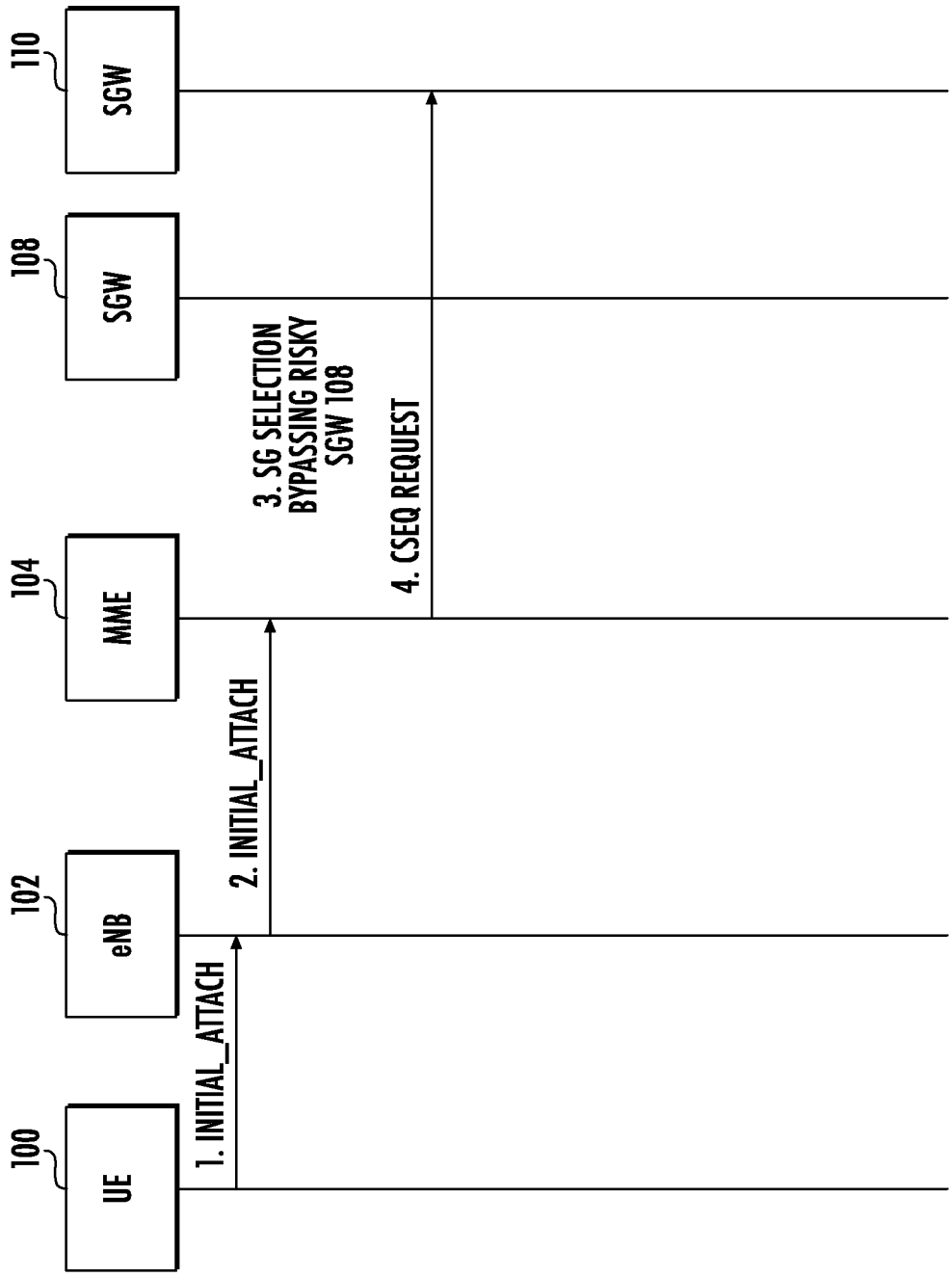
110
SGW
108
SGW
104
MME
102
eNB
100
UE
1. INITIAL_ATTACH
2. INITIAL_ATTACH
3. SG SELECTION BYPASSING RISKY SGW 108
4. CSEQ REQUEST

FIG. 4A

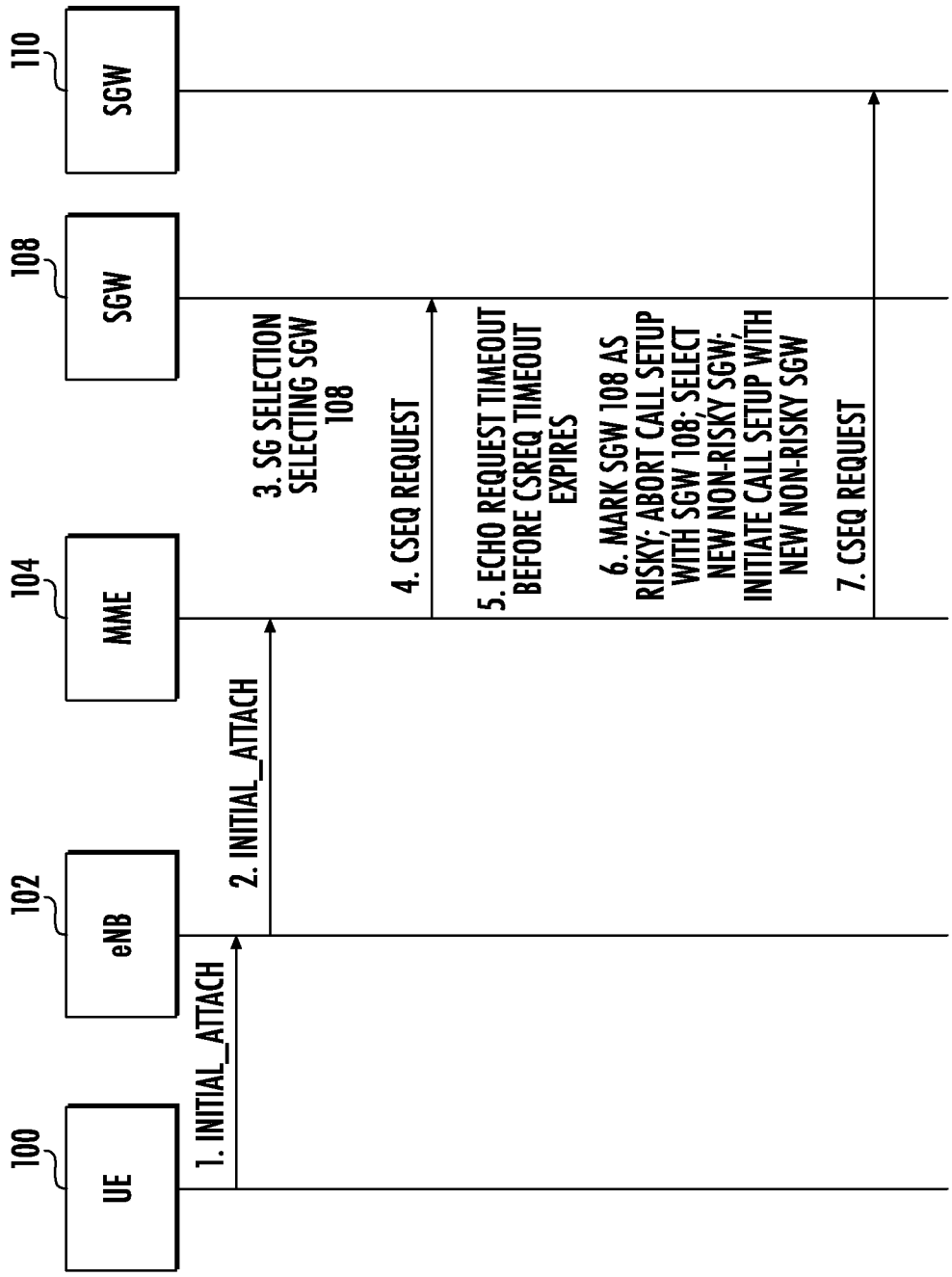
100
UE
102
eNB
104
MME
108
SGW
110
SGW
1. INITIAL_ATTACH
2. INITIAL_ATTACH
3. SG SELECTION SELECTING SGW 108
4. CSEQ REQUEST
5. ECHO REQUEST TIMEOUT BEFORE CSREQ TIMEOUT EXPIRES
6. MARK SGW 108 AS RISKY; ABORT CALL SETUP WITH SGW 108; SELECT NEW NON-RISKY SGW; INITIATE CALL SETUP WITH NEW NON-RISKY SGW
7. CSEQ REQUEST

FIG. 4B

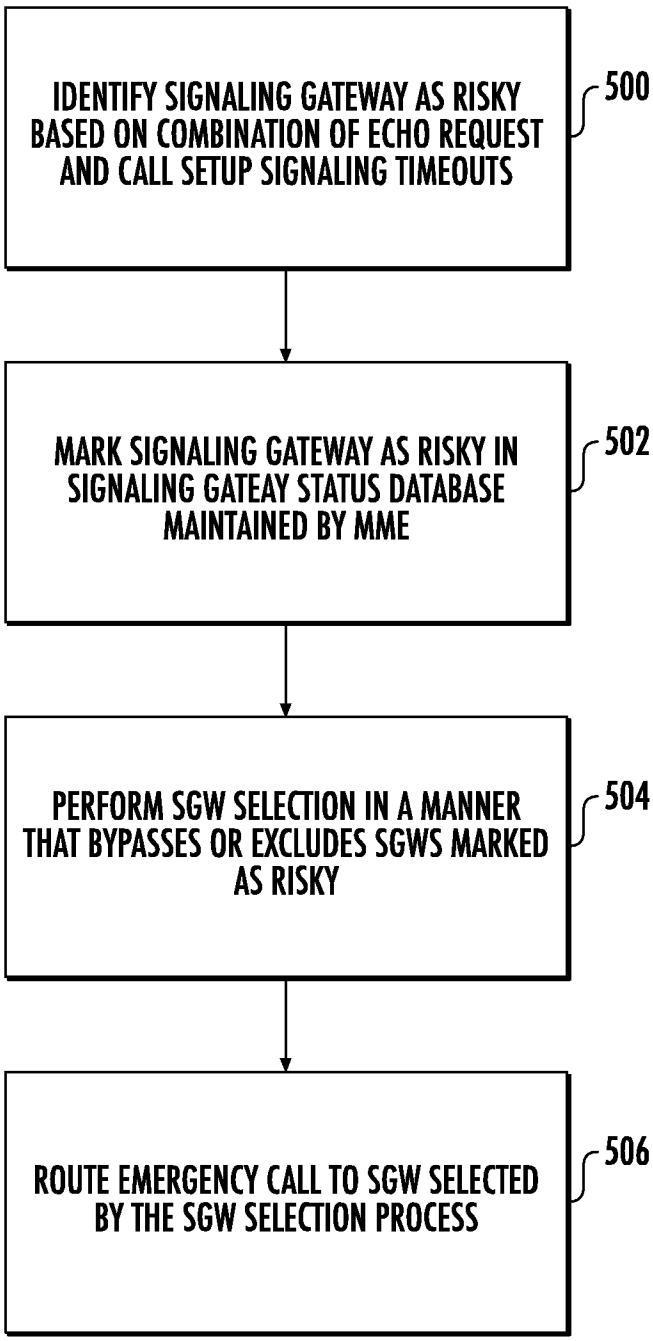
IDENTIFY SIGNALING GATEWAY AS RISKY BASED ON COMBINATION OF ECHO REQUEST AND CALL SETUP SIGNALING TIMEOUTS
500
MARK SIGNALING GATEWAY AS RISKY IN SIGNALING GATEAY STATUS DATABASE MAINTAINED BY MME
502
PERFORM SGW SELECTION IN A MANNER THAT BYPASSES OR EXCLUDES SGWS MARKED AS RISKY
504
ROUTE EMERGENCY CALL TO SGW SELECTED BY THE SGW SELECTION PROCESS
506

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2020/024519

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W76/50 H04W4/90 H04W88/16
ADD.

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

B. FIELDS SEARCHED

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

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 3 018 941 A1 (VODAFONE GMBH [DE]) 11 May 2016 (2016-05-11) abstract; figures 2-4 paragraphs [0016], [0032] - [0046] ----- -/--	1-20

[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
26 June 2020	11/09/2020

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	Binger, Bernard

1

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

International application No
PCT/US2020/024519

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (3GPP TS 29.060 version 15.2.0 Release 15)", ETSI TECHNICAL SPECIFICATION, EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI), 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS ; FRANCE , vol. 3GPP CT, no. V15.2.0 30 July 2018 (2018-07-30), pages 1-191, XP014329956, Retrieved from the Internet: URL:http://www.etsi.org/deliver/etsi_ts/129000_129099/129060/15.02.00_60/ts_129060v150200p.pdf [retrieved on 2018-07-30] paragraphs [07.2] - [7.2.4] -----	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2020/024519

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 3018941 A1	11-05-2016	EP 3018941 A1	11-05-2016
		US 2016135238 A1	12-05-2016