



(43) International Publication Date
3 December 2015 (03.12.2015)

(10) International Publication Number
WO 2015/182111 A1

- (51) **International Patent Classification:**
H04W 48/18 (2009.01) *H04W 60/00* (2009.01)
- (21) **International Application Number:**
PCT/JP2015/002635
- (22) **International Filing Date:**
26 May 2015 (26.05.2015)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
2014-112269 30 May 2014 (30.05.2014) JP
- (71) **Applicant:** NEC CORPORATION [JP/JP]; 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP).
- (72) **Inventors:** ZHANG, Xiaowei; c/o NEC Corporation, 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP). TAMURA, Toshiyuki; c/o NEC Corporation, 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP). PRASAD, Anand Raghawa; c/o NEC Corporation, 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP).
- (74) **Agent:** IEIRI, Takeshi; HIBIKI IP Law Firm, Asahi Bldg. 5th Floor, 3-33-8, Tsuruya-cho, Kanagawa-ku, Yokohama-shi, Kanagawa, 2210835 (JP).
- (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) **Title:** APPARATUS, SYSTEM AND METHOD FOR DEDICATED CORE NETWORK

(57) **Abstract:** In order for more effectively supporting a Dedicated Core Network, there is provided a network system including a first node (30) that establishes secure connection with a UE (10) initially attempting to attach to a network, through a radio base station (20), and a second node (40) to which the UE (10) is redirected from the first node (30) through the radio base station (20). Upon the redirection, the first node (30) sends information on the first node (30) itself to the second node (40) through the radio base station (20). The second node (40) uses the information to retrieve security context necessary for establishing the connection with the UE (10) from the first node (30).



WO 2015/182111 A1

Description

Title of Invention: APPARATUS, SYSTEM AND METHOD FOR DEDICATED CORE NETWORK

Technical Field

[0001] The present invention relates to an apparatus, a system and a method for a Dedicated Core Network, and particularly to a technique to ensure that a UE (User Equipment) is served by the appropriate core network.

Background Art

[0002] Recently, enhancement to support the Dedicated Core Network has been studied by 3GPP (3rd Generation Partnership Project).

[0003] The Dedicated Core Network intends that for example, a specific type of subscriber (i.e., a specific type of UE) is redirected to an MME (Mobility Management Entity)/SGSN (Serving GPRS (General Packet Radio Service) Support Node) dedicated to serve that UE. The Dedicated Core Network is also sometimes referred to as "Specific Core Network" or "Overlay Core Network".

[0004] NPL 1 discloses the most prompting message flow to realize the Dedicated Core Network. In this message flow, when a UE sends an Attach Request message to new MME through an eNB (evolved Node B) (i.e., in a case of IMSI (International Mobile Subscriber Identity) attach), the one MME obtains information to use another specific MME from an HSS (Home Subscriber Server). Then, the one MME instructs the eNB to redirect the Attach Request message to the specific MME. Upon the redirection, the eNB performs the Attach procedure again to the specific MME.

[0005] NPL 2 also discloses a message flow similar to that disclosed in NPL 1.

Citation List

Non Patent Literature

[0006] NPL 1: TSG SA WG2 #99 S2-133304, "Addition of Subscription Information for Selecting a Specific Network", 2013-09, pp. 4

NPL 2: SA WG2 #100 S2-133910, "23.401 CR2606R3: Addition of Subscription Information for Selecting a Specific Network", 2013-11, pp. 7 and 9

NPL 3: TSG SA WG2 #100 S2-133909, "Discussion on Core Network Type Selection based on the Subscription Information", 2013-11

Summary of Invention

Technical Problem

[0007] However, the inventors of this application have found that there is a problem that the message flow disclosed in NPLs 1 and 2 decreases the efficiency upon supporting

the Dedicated Core Network.

[0008] Specifically, upon the re-performance of Attach procedure, the specific MME redundantly performs AKA (Authentication and Key Agreement) procedure and NAS (Non-Access Stratum) SMC (Security Mode Command) procedure that have been already performed by the different MME to which the UE attempted to attach. Therefore, there are caused signaling overload to devices/nodes involved in the redundant AKA/NAS SMC procedures and all interface therebetween, as well as overload to the specific MME.

[0009] Moreover, NPLs 2 and 3 each discloses another message flow for GUTI (Globally Unique Temporary Identity) attach, in which the specific MME contacts an MME referenced by the GUTI to retrieve security context.

[0010] However, even in this message flow, there are also caused the above-mentioned signaling overload and overload to the specific MME. This is because the GUTI merely indicates the old MME which may has removed the security context after the expiration of timer, after all the specific MME redundantly performs the AKA/NAS SMC procedures.

[0011] Note that details of these problems will be discussed more fully in the following description.

[0012] Accordingly, an exemplary object of the present invention is to provide a solution for more effectively supporting a Dedicated Core Network.

Solution to Problem

[0013] In order to achieve the above-mentioned object, a network system according to first exemplary aspect of the present invention includes: a first node that establishes secure connection with a UE (User Equipment) initially attempting to attach to a network, through a radio base station; and a second node to which the UE is redirected from the first node through the radio base station. Upon the redirection, the first node sends information on the first node itself to the second node through the radio base station. The second node uses the information to retrieve security context necessary for establishing the connection with the UE from the first node.

[0014] Further, according to second exemplary aspect of the present invention, there is provided a method of control for a network system including a first node that establishes secure connection with a UE initially attempting to attach to a network, through a radio base station, and a second node to which the UE is redirected from the first node through the radio base station. This method includes: sending, upon the redirection, information on the first node from the first node to the second node through the radio base station; and using, by the second node, the information to retrieve security context necessary for establishing the connection with the UE from

the first node.

[0015] Further, a network system according to third exemplary aspect of the present invention includes: a first node that receives an attach request from a UE initially attempting to attach to a network, through a radio base station; and a second node to which the attach request is redirected from the first node through the radio base station. Upon the reception of the attach request, the first node skips establishment of secure connection with the UE through the radio base station. Upon the redirection, the first node sends, to the second node through the radio base station, subscription information indicating that the UE is one to be redirected to the second node. In response to receiving the subscription information, the second node establishes the secure connection with the UE.

[0016] Further, according to fourth exemplary aspect of the present invention, there is provided a method of control for a network system including a first node that receives an attach request from a UE initially attempting to attach to a network, through a radio base station, and a second node to which the attach request is redirected from the first node through the radio base station. This method includes: skipping, by the first node upon the reception of the attach request, establishment of secure connection with the UE through the radio base station; sending, upon the redirection, from the first node to the second node through the radio base station, subscription information indicating that the UE is one to be redirected to the second node; and establishing, by the second node in response to receiving the subscription information, the secure connection with the UE.

[0017] Further, a network system according to fifth exemplary aspect of the present invention includes: a first node that established secure connection with a UE through a radio base station when the UE attached to a network previously, and that assigned a temporary identity to the UE; a second node that receives an attach request including the temporary identity from the UE through the radio base station; and a third node to which the attach request is redirected from the second node through the radio base station. The second node retrieves security context necessary for establishing the connection with the UE from the first node, and upon the redirection, sends information on the second node itself to the third node through the radio base station. The third node uses the information to retrieve the security context from the second node.

[0018] Further, according to sixth exemplary aspect of the present invention, there is provided a method of control for a network system including a first node that established secure connection with a UE through a radio base station when the UE attached to a network previously and that assigned a temporary identity to the UE, a second node that receives an attach request including the temporary identity from the

UE through the radio base station, and a third node to which the attach request is redirected from the second node through the radio base station. This method includes: retrieving, by the second node, security context necessary for establishing the connection with the UE from the first node; sending, upon the redirection, information on the second node from the second node to the third node through the radio base station; and using, by the third node, the information to retrieve the security context from the second node.

[0019] Further, a network system according to seventh exemplary aspect of the present invention includes: a first node that established secure connection with a UE through a radio base station when the UE attached to a network previously, and that assigned a temporary identity to the UE; a second node that receives an attach request including the temporary identity from the UE through the radio base station; and a third node to which the attach request is redirected from the second node through the radio base station. The second node retrieves security context necessary for establishing the connection with the UE from the first node, and upon the redirection, sends the security context to the third node through the radio base station.

[0020] Further, according to eighth exemplary aspect of the present invention, there is provided a method of control for a network system including a first node that established secure connection with a UE through a radio base station when the UE attached to a network previously and that assigned a temporary identity to the UE, a second node that receives an attach request including the temporary identity from the UE through the radio base station, and a third node to which the attach request is redirected from the second node through the radio base station. This method includes: retrieving, by the second node, security context necessary for establishing the connection with the UE from the first node; and sending, upon the redirection, the security context from the second node to the third node through the radio base station.

[0021] Further, a network system according to ninth exemplary aspect of the present invention includes: a first node that established secure connection with a UE through a radio base station when the UE attached to a network previously, and that assigned a temporary identity to the UE; a second node that receives an attach request including the temporary identity from the UE through the radio base station; and a third node to which the attach request is redirected from the second node through the radio base station. The first node maintains security context necessary for establishing the secure connection with the UE till an identification request is received from the third node. Upon the redirection, the third node sends the identification request to the first node to retrieve the security context from the first node.

[0022] Further, according to tenth exemplary aspect of the present invention, there is provided a method of control for a network system including a first node that es-

established secure connection with a UE through a radio base station when the UE attached to a network previously and that assigned a temporary identity to the UE, a second node that receives an attach request including the temporary identity from the UE through the radio base station, and a third node to which the attach request is redirected from the second node through the radio base station. This method includes: maintaining, by the first node, security context necessary for establishing the secure connection with the UE till an identification request is received from the third node; and sending, by the third node upon the redirection, the identification request to the first node to retrieve the security context from the first node.

[0023] Further, a core network system according to eleventh exemplary aspect of the present invention includes: a plurality of core network nodes; and a server. In this system, a UE sends a message to a first core network node through a radio base station. The UE is redirected from the first core network node to a second core network node based on subscription information of the UE provided by the server. The first core network node sends a first message including information on the redirection to the radio base station. The radio base station sends a second message including the information to the second core network node.

[0024] Further, according to twelfth exemplary aspect of the present invention, there is provided a method for a core network system including a plurality of core network nodes and a server. This method includes: a step that a UE (User Equipment) sends a message to a first core network node through a radio base station; a step that the UE is redirected from the first core network node to a second core network node based on subscription information of the UE provided by the server; a step that the first core network node sends a first message including information on the redirection to the radio base station; and a step that the radio base station sends a second message including the information to the second core network node.

[0025] Further, a UE according to thirteenth exemplary aspect of the present invention includes: means for sending a message to a first core network node through a radio base station. The UE is redirected from the first core network node received the message to a second core network node based on subscription information of the UE provided by a server. In the redirection, the first core network node sends a first message including information on the redirection to the radio base station, and the radio base station sends a second message including the information to the second core network node.

[0026] Furthermore, according to fourteenth exemplary aspect of the present invention, there is provided a method for a UE. This method includes: a step that the UE sends a message to a first core network node through a radio base station; and a step that the UE is redirected from the first core network node received the message to a second

core network node based on subscription information of the UE provided by a server. In the redirection, the first core network node sends a first message including information on the redirection to the radio base station, and the radio base station sends a second message including the information to the second core network node.

Advantageous Effects of Invention

[0027] According to the present invention, it is possible to solve at least one of the above-mentioned problems, and thus to provide a solution for more effectively supporting a Dedicated Core Network.

Brief Description of Drawings

[0028] [fig.1]Fig. 1 is a block diagram showing a configuration example of a network system according to a first exemplary embodiment of the present invention.

[fig.2]Fig. 2 is a sequence diagram showing a first example of operations in the network system according to the first exemplary embodiment.

[fig.3]Fig. 3 is a sequence diagram showing a second example of operations in the network system according to the first exemplary embodiment.

[fig.4]Fig. 4 is a sequence diagram showing a first example of operations in a network system according to a second exemplary embodiment of the present invention.

[fig.5]Fig. 5 is a sequence diagram showing a second example of operations in the network system according to the second exemplary embodiment.

[fig.6]Fig. 6 is a sequence diagram showing a third example of operations in the network system according to the second exemplary embodiment.

[fig.7]Fig. 7 is a sequence diagram for explaining problems in typical IMSI attach procedure.

[fig.8]Fig. 8 is a sequence diagram for explaining problems in typical GUTI attach procedure.

Description of Embodiments

[0029] Hereinafter, several exemplary embodiments according to the present invention will be described with reference to the accompanying drawings.

[0030] <First Exemplary Embodiment>

As shown in Fig. 1, a network system according to this exemplary embodiment includes MMEs 30 and 40 by way of example only. Among them, the MME 30 is the one to which a UE 10 initially attaches through an eNB 20 serving as a radio base station, and thus sometimes referred to as "New MME" in the following description. On the other hand, the MME 40 is the one dedicated to serve the UE 10 according to subscription and to which the UE 10 is redirected from the MME 30, and thus referred to as "Dedicated MME" or "DMME". Note that the MME 40 can also be referred to as "Specific MME", in conformity with the Dedicated Core Network being sometimes

referred to as "Specific Core Network". If necessary, each of the MMEs 30 and 40 can obtain, from an HSS 50, subscription information on the UE 10, information necessary for authenticating the UE 10, and the like. The New MME 30 is also connected to an S-GW (Serving Gateway) and/or a P-GW (PDN (Public Data Network) Gateway). Similarly, the Dedicated MME 40 is also connected to a Dedicated S-GW and/or a Dedicated P-GW.

[0031] In general, this exemplary embodiment deals with IMSI attach in E-UTRAN (Evolved Universal Terrestrial Radio Access Network), particularly with a case where the New MME 30 redirects an Attach Request message received from the eNB 20 to the DMME 40, according to the subscription information on the UE 10 obtained from the HSS 50.

[0032] Next, prior to describing operation examples of this exemplary embodiment, there are firstly defined problems in typical IMSI attach procedure as disclosed by NPLs 1 and 2 with reference to Fig. 7. Then, there will be described solutions for addressing these problems as the operation examples. The solutions include Option 1 shown in Fig. 2 and Option 2 shown in Fig. 3.

[0033] Problem Defined:

As shown in Fig. 7, in the typical IMSI attach procedure, a UE 110 sends an Attach Request message including its IMSI to an eNB 120 (step S101), and the eNB 120 forwards the Attach Request message to an New MME 130 (step S102).

[0034] Upon receiving the Attach Request message, the New MME 130 sends an Authentication data request message to an HSS 150, and as a response thereto, receives an Authentication data response message including AVs (Authentication Vectors) (step S103). Then, the New MME 130 corporates with the UE 110 to perform AKA procedure and NAS SMC procedure (step S104). As a result, The UE 10 and the New MME 130 each can share K_{asme} (Key for access security management entity) and NAS keys, so that secure connection is established between them (step S105).

[0035] After that, the New MME 130 sends an Update Location Request message to the HSS 150, and as a response thereto, receives an Update Location Response message (step S106). The Update Location Response message includes the IMSI and the subscription information/data. Moreover, the subscription information includes information on a Dedicated MME 140 (hereinafter, such information will be sometimes referred to as "DMME information").

[0036] Then, the New MME 130 selects the Dedicated MME 140 to which the UE 110 should be redirected based on the DMME information (step S107), and sends a Redirect message to the eNB 120 (step S108). Upon receiving the Redirect message, the eNB 120 forwards the Attach Request message to the Dedicated MME 140 (step S109).

[0037] However, at this time, the following problems arise:

(a) Since the Attach Request message is not protected, the Dedicated MME 140 starts AKA procedure to the UE 10;

(b) due to (a), the Dedicated MME 140 sends/receives Authentication data request/response messages and Update Location Request/Response messages to/from the HSS 150, and also cooperates with the UE 110 to perform AKA procedure and NAS SMC procedure; and

(c) due to (a) and (b), there are caused signaling overload to the HSS 150, the Dedicated MME 140, the eNB 120, the UE 110 and all interfaces therebetween, as well as overload to the Dedicated MME 140 for key computation.

[0038] Solutions:

(Option 1)

Fig. 2 shows a sequence diagram for this option. Processes at steps S1 to S7 are performed in a similar manner to those at the above-mentioned steps S101 to S107 shown in Fig. 7.

[0039] Meanwhile, upon the redirection, the New MME 30 sends to the eNB 20 a Redirect message including information on the New MME 30 itself (herein after, such information will be sometimes referred to as "MME information") (step S8). For example, the MME information includes an ID (identification, identity), an FQDN (Fully Qualified Domain Name) or an IP (Internet Protocol) address assigned to the New MME 30. Then, the eNB 20 forwards to the Dedicated MME 40 the MME information with being included in an Attach Request message (step S9).

[0040] The Dedicated MME 40 uses the received MME information to retrieve, from the New MME 30, security context concerning secure connection which has been established between the UE 10 and the New MME 30. Specifically, the Dedicated MME 40 sends an Identification Request message to the New MME 30 (step S10), and as a response thereto, receives an Identification Response message including UE context (step S11). The UE context includes the AVs and all security context. Then, the Dedicated MME 40 extracts the K_{asme} and the NAS keys from the retrieved UE context (step S12).

[0041] After that, a message 5b and the subsequent message sequences as disclosed in 3GPP TS 23.401, section 5.3.2.1 follows.

[0042] According to this option, the Dedicated MME 40 is indicated about the MME information such that the Dedicated MME 40 can retrieve necessary security context from the New MME 30. Therefore, unlike the typical IMSI attach procedure, the Dedicated MME 40 needs not to perform AKA procedure and NAS SMC procedure. Thus, compared with the typical IMSI attach procedure, it is possible to drastically reduce signaling overload, as well as overload to the Dedicated MME for key com-

putation. Moreover, since the existing message sequences can be reused (the Identification Request/Response messages are also the existing ones as will be described later), it is possible to minimize the impact on the mobile communication system.

[0043] Further, at the above-mentioned step S11, the New MME 30 may include, in the Identification Response message, an Authentication Indication which indicates that the UE 10 has been authenticated as the one to be redirected to the Dedicated MME 40. In this case, the Dedicated MME 40 needs not to contact the HSS 50 for the purpose of authenticating the UE 10, so that it is possible to further reduce signaling overload.

[0044] (Option 2)

Fig. 3 shows a sequence diagram for this option. Processes at steps S21 and S22 are performed in a similar manner to those at the above-mentioned steps S1 and S2 shown in Fig. 2.

[0045] Meanwhile, upon receiving the Attach Request message, the New MME 30 firstly retrieves from the HSS 50 the subscription information including the DMME information (step S23a).

[0046] As described above, the DMME information indicates that the UE 10 should be redirected to the Dedicated MME 40. Therefore, the New MME 30 skips establishment of secure connection with the UE 10. Specifically, the New MME 30 does not perform the AKA procedure, the NAS SMC procedure, the computation of NAS keys, and the like.

[0047] Then, the New MME 30 selects the Dedicated MME 40 based on the DMME information (step S24), and sends to the eNB 20 a Redirect message including the subscription information (which also includes the DMME information) (step S25). Then, the eNB 20 forwards to the Dedicated MME 40 the subscription information with being included in an Attach Request message (step S26).

[0048] In response to receiving the subscription information (i.e., DMME information), the Dedicated MME 40 establishes secure connection with the UE 10 through the eNB 20, as a substitute for the New MME 30. Specifically, Dedicated MME 40 sends an Authentication data request message to the HSS 50, and as a response thereto, receives an Authentication data response message including the AVs (step S27). Then, the Dedicated MME 40 cooperates with the UE 10 to perform AKA procedure and NAS SMC procedure (step S28). As a result, The UE 10 and the Dedicated MME 40 each can share K_{asme} and NAS keys, so that secure connection is established therebetween through the eNB 20 (step S29).

[0049] After that, a message 5b and the subsequent message sequences as disclosed in 3GPP TS 23.401, section 5.3.2.1 follows.

[0050] According to this option, as will be understood by comparing the sequence shown in Fig. 3 with that shown in Fig. 2, it is possible to reduce the amount of signaling

compared to the above-mentioned Option 1. Moreover, since the New MME 30 skips the establishment of secure connection, it is also possible to reduce overload to the New MME 30.

[0051] Further, as a substitute for the above-mentioned step S23a, the DMME information may be preconfigured in the New MME 30 (step S23b). In this case, the New MME 30 can also skip the retrieval of subscription information from the HSS 50 when it receives the initial Attach Request from the UE 10, so that it is possible to further reduce the amount of signaling.

[0052] Furthermore, at the above-mentioned step S23a, the New MME 30 may further retrieve the AVs from the HSS 50. The retrieved AVs can be transferred to the Dedicated MME 40 through the eNB 20 with the Redirect message shown at the above-mentioned step S25 and the Attach Request message shown at the above-mentioned step S26. In this case, the Dedicated MME 40 can skip the acquisition of AVs from the HSS 50 shown at the above-mentioned step S27, so that it is possible to further reduce the amount of signaling.

[0053] <Second Exemplary Embodiment>

As shown in Fig. 4, a network system according to this exemplary embodiment further includes an MME 60 in addition to the above-mentioned MMEs 30 and 40. The MME 60 is the one to which the UE 10 previously attached, and thus sometimes referred to as "Old MME" in the following description. If necessary, the Old MME 60 can also obtain, from the HSS 50, the subscription information, the DMME information, the AVs and the like. Note that there is a case where the UE 10 previously attached to an SGSN (i.e., "Old SGSN"). Even in this case, the following description about the Old MME can be similarly applied to that about the Old SGSN.

[0054] In general, this exemplary embodiment deals with GUTI attach in E-UTRAN, particularly with a case where the New MME 30 redirects an Attach Request message received from the eNB 20 to the DMME 40, according to the DMME information obtained from the Old MME 60.

[0055] Next, prior to describing operation examples of this exemplary embodiment, there are firstly defined problems in typical GUTI attach procedure as disclosed by NPLs 2 and 3 with reference to Fig. 8. Then, there will be described solutions for addressing these problems as the operation examples. The solutions include Option 1 shown in Fig. 4, Option 2 shown in Fig. 5, and Option 3 shown in Fig. 6.

[0056] Problem Defined:

As shown by dotted lines in Fig. 8, assume that the UE 110 previously attached to an Old MME 160, and the Old MME 160 assigned a GUTI to the UE 110, so that the UE has gotten the GUTI.

[0057] In the typical GUTI attach procedure, the UE 110 sends an Attach Request

message including the GUTI to the eNB 120 (step S201), and the eNB 120 forwards the Attach Request message to the New MME 130 (step S202).

[0058] Upon receiving the Attach Request message, the New MME 130 sends to the Old MME 160 an Identification Request message including the GUTI and the complete Attach Request message (step S203), and as a response thereto, receives an Identification Response message including the IMSI of the UE 110 and MM (Mobility Management) Context (step S204).

[0059] Then, the New MME 130 selects the Dedicated MME 140 (step S205), and sends a Redirect message to the eNB 120 (step S206). Upon receiving the Redirect message, the eNB 120 forwards the Attach Request message to the Dedicated MME 140 (step S207).

[0060] However, the Old MME 160 might remove UE context (i.e., security context) after a predetermined timer expired. Moreover, the GUTI merely indicates the Old MME 160. Therefore, the Dedicated MME 140 fails in retrieving the AVs and the security context from the Old MME 160, and thus starts AKA procedure.

[0061] Accordingly, as with the typical IMSI attach procedure, the following problems arise:

signaling overload to the HSS 150, the Dedicated MME 140, the eNB 120, the UE 110 and all interfaces therebetween; and

overload to the Dedicated MME 140 for key computation.

[0062] Solutions:

(Option 1)

Fig. 4 shows a sequence diagram for this option. Processes at steps S31 to S35 are performed in a similar manner to those at the above-mentioned steps S201 to S205 shown in Fig. 8.

[0063] Meanwhile, upon the redirection, the New MME 30 sends to the eNB 20 a Redirect message including information on the New MME 30 itself (i.e., MME information) (step S36). Then, the eNB 20 forwards to the Dedicated MME 40 the MME information with being included in an Attach Request message (step S37).

[0064] The Dedicated MME 40 uses the received MME information to retrieve, from the New MME 30, the security context which has been obtained at the above-mentioned step S34 by the New MME 30 from the Old MME 60. Specifically, the Dedicated MME 40 sends an Identification Request message to the New MME 30 (step S38), and as a response thereto, receives an Identification Response message including UE context (step S39). As described above, the UE context includes the AVs and all security context. Then, the Dedicated MME 40 extracts the K_{asme} and the NAS keys from the retrieved UE context (step S40).

[0065] After that, a message 5b and the subsequent message sequences as disclosed in

3GPP TS 23.401, section 5.3.2.1 follows.

[0066] According to this option, the Dedicated MME 40 is indicated about the MME information such that the Dedicated MME 40 can retrieve necessary security context from the New MME 30. Therefore, unlike the typical GUTI attach procedure, the Dedicated MME 40 needs not to contact the Old MME 60 for the purpose of retrieving the AVs and the security context from the Old MME 60, and thus needs not to start AKA procedure if it fails in retrieving the security context from the Old MME 60. Thus, compared with the typical GUTI attach procedure, it is possible to drastically reduce signaling overload, as well as overload to the Dedicated MME for key computation. Moreover, since the existing message sequences can be reused, it is possible to minimize the impact on the mobile communication system.

[0067] Further, at the above-mentioned step S39, the New MME 30 may include, in the Identification Response message, an Authentication Indication which indicates that the UE 10 has been authenticated as the one to be redirected to the Dedicated MME 40. In this case, the Dedicated MME 40 needs not to contact the HSS 50 for the purpose of authenticating the UE 10, so that it is possible to further reduce signaling overload.

[0068] (Option 2)

Fig. 5 shows a sequence diagram for this option. Processes at steps S41 to S45 are performed in a similar manner to those at the above-mentioned steps S31 to S35 shown in Fig. 4.

[0069] Meanwhile, upon the redirection, the New MME 30 sends to the eNB 20 a Redirect message including the UE context (step S46). Then, the eNB 20 forwards to the Dedicated MME 40 the UE context with being included in an Attach Request message (step S47). As described above, the UE context includes the AVs and all security context.

[0070] Then, the Dedicated MME 40 extracts the K_{asme} and the NAS keys from the received UE context (step S48).

[0071] After that, a message 5b and the subsequent message sequences as disclosed in 3GPP TS 23.401, section 5.3.2.1 follows.

[0072] According to this option, the Dedicated MME 40 needs not to contact any MME to retrieve the UE context. Therefore, it is possible to reduce the amount of signaling compared to the above-mentioned Option 1, and it is also possible to reduce to reduce overload to the Dedicated MME 40.

[0073] Further, this option may be optimized such that the Old MME 60 remembers that integrity check for the Attach Request message is done at the above-mentioned step S43. In this case, the Dedicated MME 40 needs not to do the integrity check again at the above-mentioned step S47, so that it is possible to further reduce the overload to the Dedicated MME 40.

[0074] (Option 3)

Fig. 6 shows a sequence diagram for this option. Processes at steps S51 to S55 are performed in a similar manner to those at the above-mentioned steps S31 to S35 shown in Fig. 4.

[0075] Meanwhile, in this option, since the Old MME 60 served as the DMME for subscriber, the Old MME 60 maintains the security context for a while without removing it just till a second Identification Request message is received from a dedicated MME.

[0076] Upon the redirection, the New MME 30 sends a Redirect message to the eNB 20 (step S56). Then, the eNB 20 forwards the Attach Request message to the Dedicated MME 40 (step S57).

[0077] Upon receiving the Attach Request message, the Dedicated MME 40 sends to the Old MME 60 an Identification Request message including the GUTI and the complete Attach Request message (step S58).

[0078] Now, since the second Identification Request message is received, the Old MME 60 sends back to the Dedicated MME 40 an Identification Response message including the maintained MM Context (security context) (step S59).

[0079] Then, the Dedicated MME 40 extracts the K_{asme} and the NAS keys from the received MM context (step S60).

[0080] After that, a message 5b and the subsequent message sequences as disclosed in 3GPP TS 23.401, section 5.3.2.1 follows.

[0081] According to this option, like the typical GUTI attach procedure, the Dedicated MME 40 can retrieve necessary security context from the Old MME 60 by only using the GUTI, and thus needs not to start AKA procedure. Therefore, it is possible to drastically reduce signaling overload, as well as overload to the Dedicated MME for key computation. Moreover, since the Dedicated MME only has to contact the MME indicated by the GUTI, in other words, since the Dedicated MME only performs the existing message sequences, it is possible to minimize the impact on the Dedicated MME.

[0082] Further, it is preferable that the New MME 30 informs, through the Redirect message and the Attach Request message shown at the above-mentioned steps S56 and S57, the Dedicated MME 40 that no AV is consumed, and the Old MME 60 informs only valid AVs to the Dedicated MME 40 in the second Identification Response message shown at the above-mentioned step S59. This ensures that the Dedicated MME 40 can use the received AVs for conducting communication with the UE 10. Note that as a substitute for the valid AVs or in addition thereto, the Old MME 60 may inform other additional information to the Dedicated MME 40.

[0083] Furthermore, this option may be optimized such that the Old MME 60 remembers

that integrity check for the Attach Request message is done at the above-mentioned step S53. In this case, the Dedicated MME 40 needs not to do the integrity check again at the above-mentioned step S57, and the Old MME 60 also needs not do the integrity check again at the above-mentioned step S58, so that it is possible to reduce the overload to the Dedicated MME 40 and the Old MME 60.

[0084] Note that although the exemplary embodiments have been described hereinbefore by taking as an example E-UTRAN, the present invention can also be applied to IMSI attach and P-TMSI (Packet-TMSI (Temporary Mobile Subscriber Identity)) attach in UTRAN. The mechanism is basically the same as for attach in E-UTRAN, except that e.g., the message is changed to carry Dedicated MME/SGSN information.

[0085] If the exemplary embodiments are referred to the UTRAN and GERAN (GSM (Global System for Mobile communications) EDGE (Enhanced Data GSM Environment) RAN), then the following replacements need to be made:

replacing MME with SGSN;

replacing DMME with DSGSN;

replacing eNB with BTS (Base Transceiver Station)/BSC (Base Station Controller);

replacing HSS with HLR (Home Location Register)/HSS; and

replacing GUTI with P-TMSI.

[0086] Further, although the illustration is omitted, the New MME 30, the Dedicated MME 40 and the Old MME 60 each can be configured by, for example, one or more transceivers which conduct communication with the UE 10 through the eNB 20, which conduct communication between the MMEs 30, 40 and 60 through or not through the eNB 20 and which conduct communication with the HSS 50, and a controller such as a CPU (Central Processing Unit) which controls these transceivers to execute the processes shown in the accompany sequence diagrams or processes equivalent thereto.

[0087] Note that the present invention is not limited to the above-mentioned exemplary embodiments, and it is obvious that various modifications can be made by those of ordinary skill in the art based on the recitation of the claims.

[0088] The whole or part of the exemplary embodiments disclosed above can be described as, but not limited to, the following supplementary notes.

[0089] (Supplementary note 1)

A network system comprising:

a first node that establishes secure connection with a UE (User Equipment) initially attempting to attach to a network, through a radio base station; and

a second node to which the UE is redirected from the first node through the radio base station,

wherein upon the redirection, the first node sends information on the first node

itself to the second node through the radio base station, and

wherein the second node uses the information to retrieve security context necessary for establishing the connection with the UE from the first node.

[0090] (Supplementary note 2)

A method of control for a network system including a first node that establishes secure connection with a UE initially attempting to attach to a network, through a radio base station, and a second node to which the UE is redirected from the first node through the radio base station, the method comprising:

sending, upon the redirection, information on the first node from the first node to the second node through the radio base station; and

using, by the second node, the information to retrieve security context necessary for establishing the connection with the UE from the first node.

[0091] (Supplementary note 3)

A network system comprising:

a first node that receives an attach request from a UE initially attempting to attach to a network, through a radio base station; and

a second node to which the attach request is redirected from the first node through the radio base station,

wherein upon the reception of the attach request, the first node skips establishment of secure connection with the UE through the radio base station,

wherein upon the redirection, the first node sends, to the second node through the radio base station, subscription information indicating that the UE is one to be redirected to the second node, and

wherein in response to receiving the subscription information, the second node establishes the secure connection with the UE.

[0092] (Supplementary note 4)

A method of control for a network system including a first node that receives an attach request from a UE initially attempting to attach to a network, through a radio base station, and a second node to which the attach request is redirected from the first node through the radio base station, the method comprising:

skipping, by the first node upon the reception of the attach request, establishment of secure connection with the UE through the radio base station;

sending, upon the redirection, from the first node to the second node through the radio base station, subscription information indicating that the UE is one to be redirected to the second node; and

establishing, by the second node in response to receiving the subscription information, the secure connection with the UE.

[0093] (Supplementary note 5)

A network system comprising:

a first node that established secure connection with a UE through a radio base station when the UE attached to a network previously, and that assigned a temporary identity to the UE;

a second node that receives an attach request including the temporary identity from the UE through the radio base station; and

a third node to which the attach request is redirected from the second node through the radio base station,

wherein the second node retrieves security context necessary for establishing the connection with the UE from the first node, and upon the redirection, sends information on the second node itself to the third node through the radio base station, and

wherein the third node uses the information to retrieve the security context from the second node.

[0094] (Supplementary note 6)

A method of control for a network system including a first node that established secure connection with a UE through a radio base station when the UE attached to a network previously and that assigned a temporary identity to the UE, a second node that receives an attach request including the temporary identity from the UE through the radio base station, and a third node to which the attach request is redirected from the second node through the radio base station, the method comprising:

retrieving, by the second node, security context necessary for establishing the connection with the UE from the first node;

sending, upon the redirection, information on the second node from the second node to the third node through the radio base station; and

using, by the third node, the information to retrieve the security context from the second node.

[0095] (Supplementary note 7)

A network system comprising:

a first node that established secure connection with a UE through a radio base station when the UE attached to a network previously, and that assigned a temporary identity to the UE;

a second node that receives an attach request including the temporary identity from the UE through the radio base station; and

a third node to which the attach request is redirected from the second node through the radio base station,

wherein the second node retrieves security context necessary for establishing the connection with the UE from the first node, and upon the redirection, sends the security context to the third node through the radio base station.

[0096] (Supplementary note 8)

A method of control for a network system including a first node that established secure connection with a UE through a radio base station when the UE attached to a network previously and that assigned a temporary identity to the UE, a second node that receives an attach request including the temporary identity from the UE through the radio base station, and a third node to which the attach request is redirected from the second node through the radio base station, the method comprising:

retrieving, by the second node, security context necessary for establishing the connection with the UE from the first node; and

sending, upon the redirection, the security context from the second node to the third node through the radio base station.

[0097] (Supplementary note 9)

A network system comprising:

a first node that established secure connection with a UE through a radio base station when the UE attached to a network previously, and that assigned a temporary identity to the UE;

a second node that receives an attach request including the temporary identity from the UE through the radio base station; and

a third node to which the attach request is redirected from the second node through the radio base station,

wherein the first node maintains security context necessary for establishing the secure connection with the UE till an identification request is received from the third node, and

wherein upon the redirection, the third node sends the identification request to the first node to retrieve the security context from the first node.

[0098] (Supplementary note 10)

A method of control for a network system including a first node that established secure connection with a UE through a radio base station when the UE attached to a network previously and that assigned a temporary identity to the UE, a second node that receives an attach request including the temporary identity from the UE through the radio base station, and a third node to which the attach request is redirected from the second node through the radio base station, the method comprising:

maintaining, by the first node, security context necessary for establishing the secure connection with the UE till an identification request is received from the third node; and

sending, by the third node upon the redirection, the identification request to the first node to retrieve the security context from the first node.

[0099] This application is based upon and claims the benefit of priority from Japanese

patent application No. 2014-112269 filed on May 30, 2014, the disclosure of which is incorporated herein in its entirety by reference.

Reference Signs List

[0100] 10, 110 UE
 20, 120 eNB
 30, 40, 60, 130, 140, 160 MME
 50, 150 HSS

Claims

- [Claim 1] A core network system comprising:
a plurality of core network nodes; and
a server,
wherein a UE (User Equipment) sends a message to a first core network node through a radio base station,
wherein the UE is redirected from the first core network node to a second core network node based on subscription information of the UE provided by the server,
wherein the first core network node sends a first message including information on the redirection to the radio base station, and
wherein the radio base station sends a second message including the information to the second core network node.
- [Claim 2] The core network system according to Claim 1,
wherein the first core network node does not authenticate the UE before the redirection and the second core network node authenticates the UE after the redirection.
- [Claim 3] The core network system according to Claim 1,
wherein the first core network node sends the first message without authenticating the UE, and
wherein the second core network node authenticates the UE upon receiving the second message.
- [Claim 4] The core network system according to any one of Claims 1 to 3,
wherein the first and second core network nodes each comprise an MME (Mobility Management Entity).
- [Claim 5] The core network system according to any one of Claims 1 to 4,
wherein the server comprises an HSS (Home Subscriber Server).
- [Claim 6] The core network system according to any one of Claims 1 to 5,
wherein the first core network node selects the second core network node that serves the UE by using the subscription information.
- [Claim 7] The core network system according to any one of Claims 1 to 6,
wherein the second core network node extracts information for authenticating the UE from the second message.
- [Claim 8] A method for a core network system including a plurality of core network nodes and a server, the method comprising:
a step that a UE (User Equipment) sends a message to a first core network node through a radio base station;

a step that the UE is redirected from the first core network node to a second core network node based on subscription information of the UE provided by the server;

a step that the first core network node sends a first message including information on the redirection to the radio base station; and

a step that the radio base station sends a second message including the information to the second core network node.

[Claim 9] The method according to Claim 8,
wherein the first core network node does not authenticate the UE before the redirection and the second core network node authenticates the UE after the redirection.

[Claim 10] The method according to Claim 8,
wherein the first core network node sends the first message without authenticating the UE, and
wherein the second core network node authenticates the UE upon receiving the second message.

[Claim 11] The method according to any one of Claims 8 to 10,
wherein the first and second core network nodes each comprise an MME (Mobility Management Entity).

[Claim 12] The method according to any one of Claims 8 to 11,
wherein the server comprises an HSS (Home Subscriber Server).

[Claim 13] The method according to any one of Claims 8 to 12,
wherein the first core network node selects the second core network node that serves the UE by using the subscription information.

[Claim 14] The method according to any one of Claims 8 to 13,
wherein the second core network node extracts information for authenticating the UE from the second message.

[Claim 15] A UE (User Equipment) comprising:
means for sending a message to a first core network node through a radio base station,

wherein the UE is redirected from the first core network node received the message to a second core network node based on subscription information of the UE provided by a server, and

wherein in the redirection, the first core network node sends a first message including information on the redirection to the radio base station, and the radio base station sends a second message including the information to the second core network node.

[Claim 16] The UE according to Claim 15, wherein the UE is not authenticated

by the first core network node before the redirection, and the UE is authenticated by the second core network node after the redirection.

[Claim 17]

A method for a UE (User Equipment) comprising:

a step that the UE sends a message to a first core network node through a radio base station; and

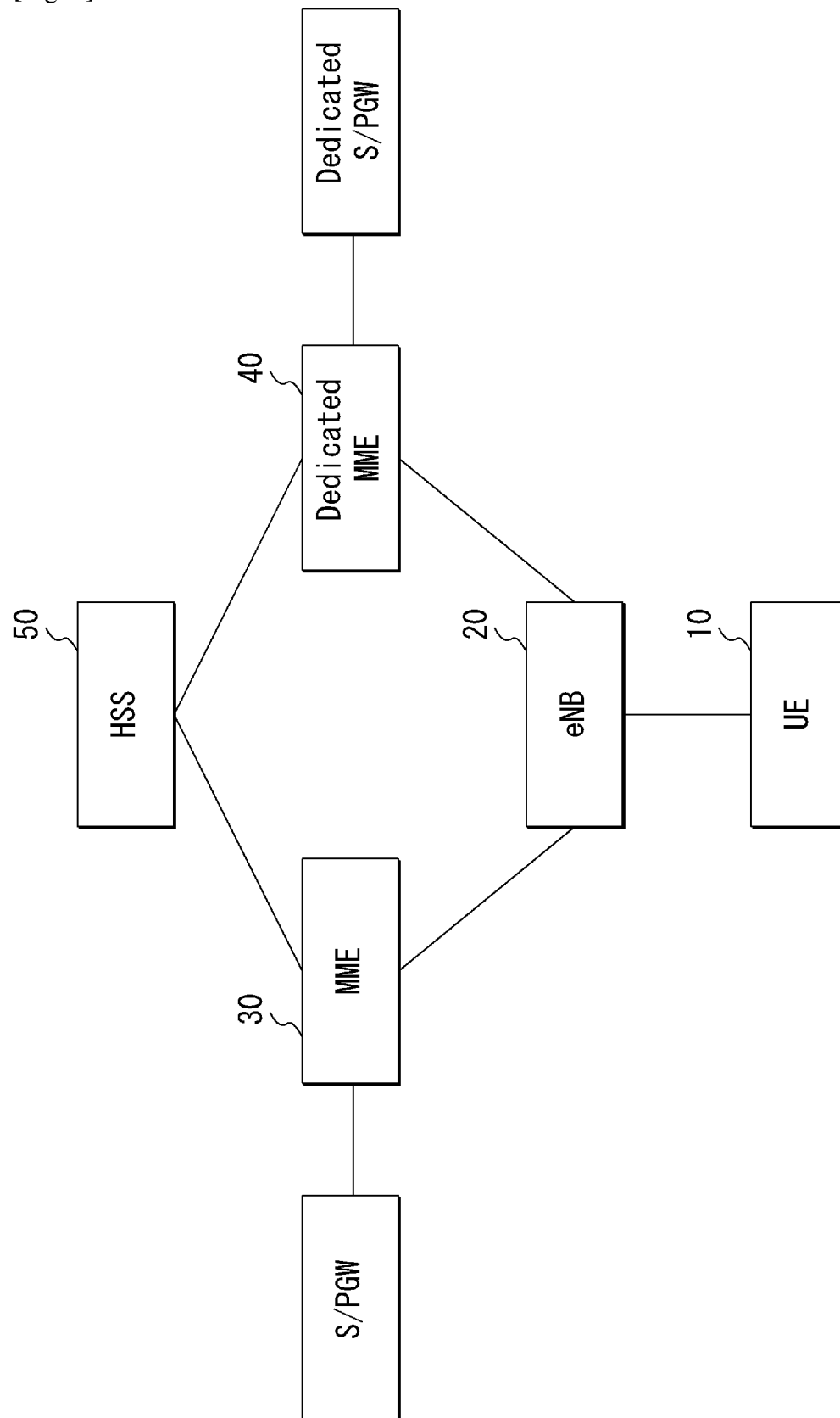
a step that the UE is redirected from the first core network node received the message to a second core network node based on subscription information of the UE provided by a server,

wherein in the redirection, the first core network node sends a first message including information on the redirection to the radio base station, and the radio base station sends a second message including the information to the second core network node.

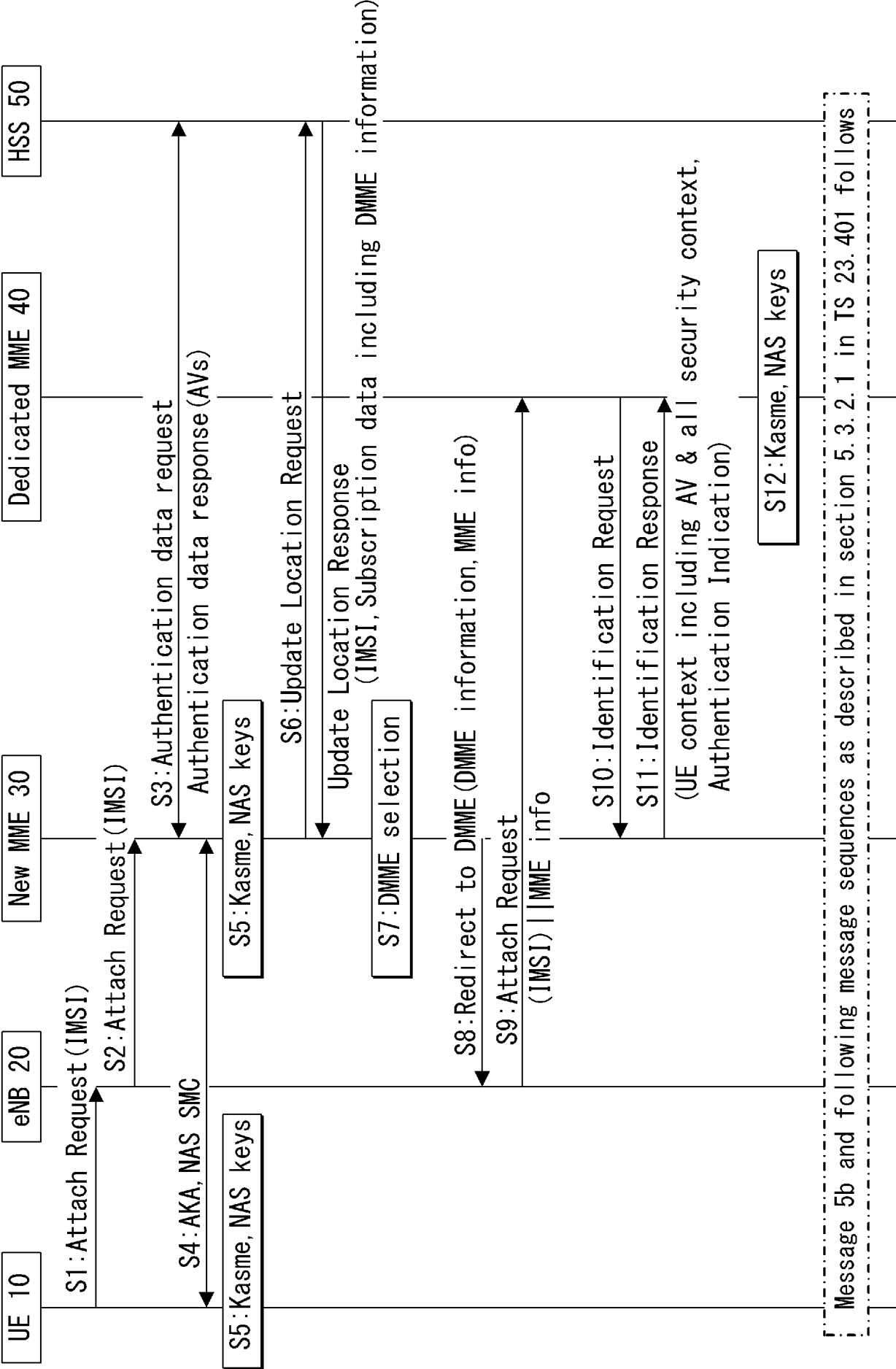
[Claim 18]

The method according to Claim 17, wherein the UE is not authenticated by the first core network node before the redirection, and the UE is authenticated by the second core network node after the redirection.

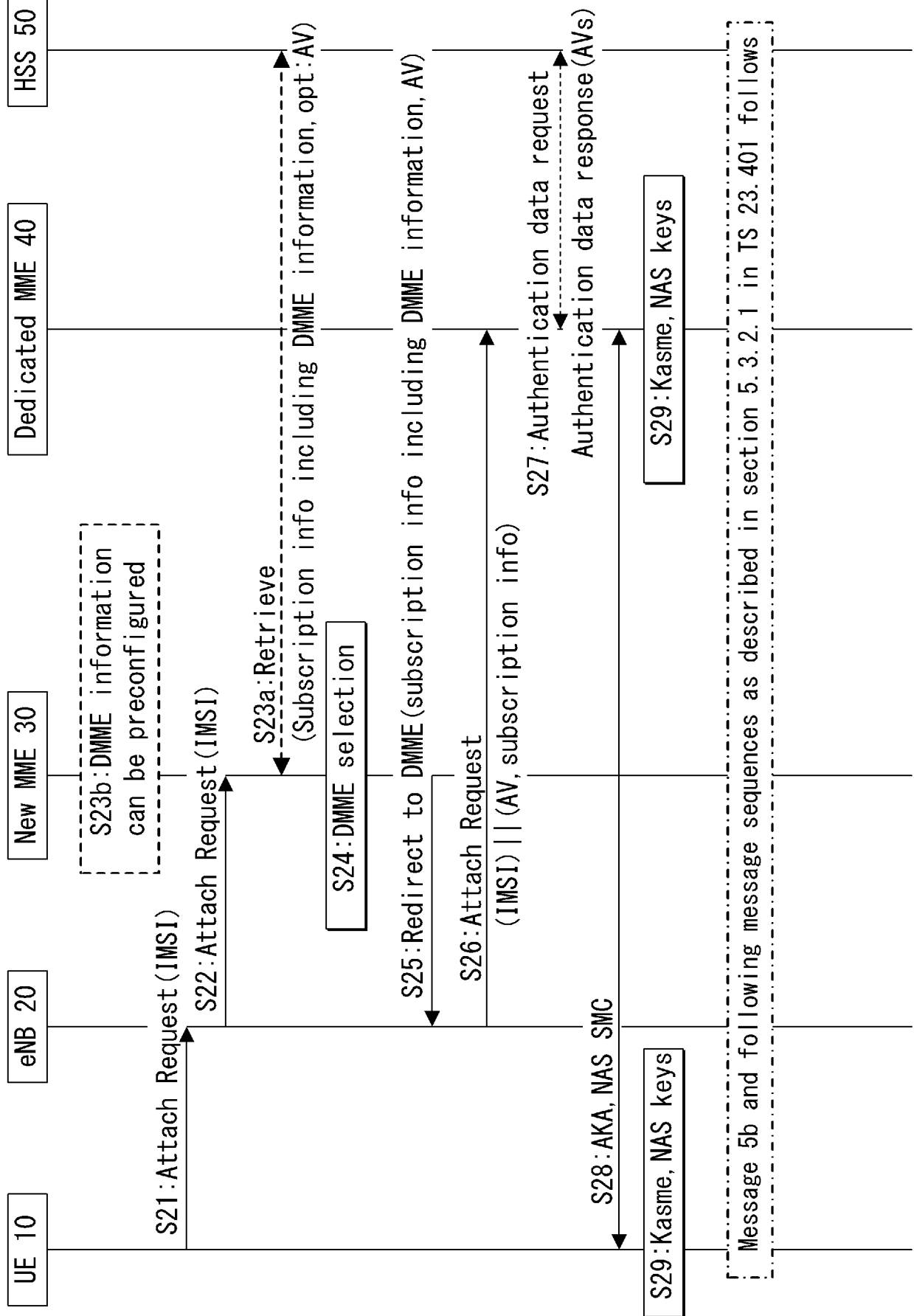
[Fig. 1]



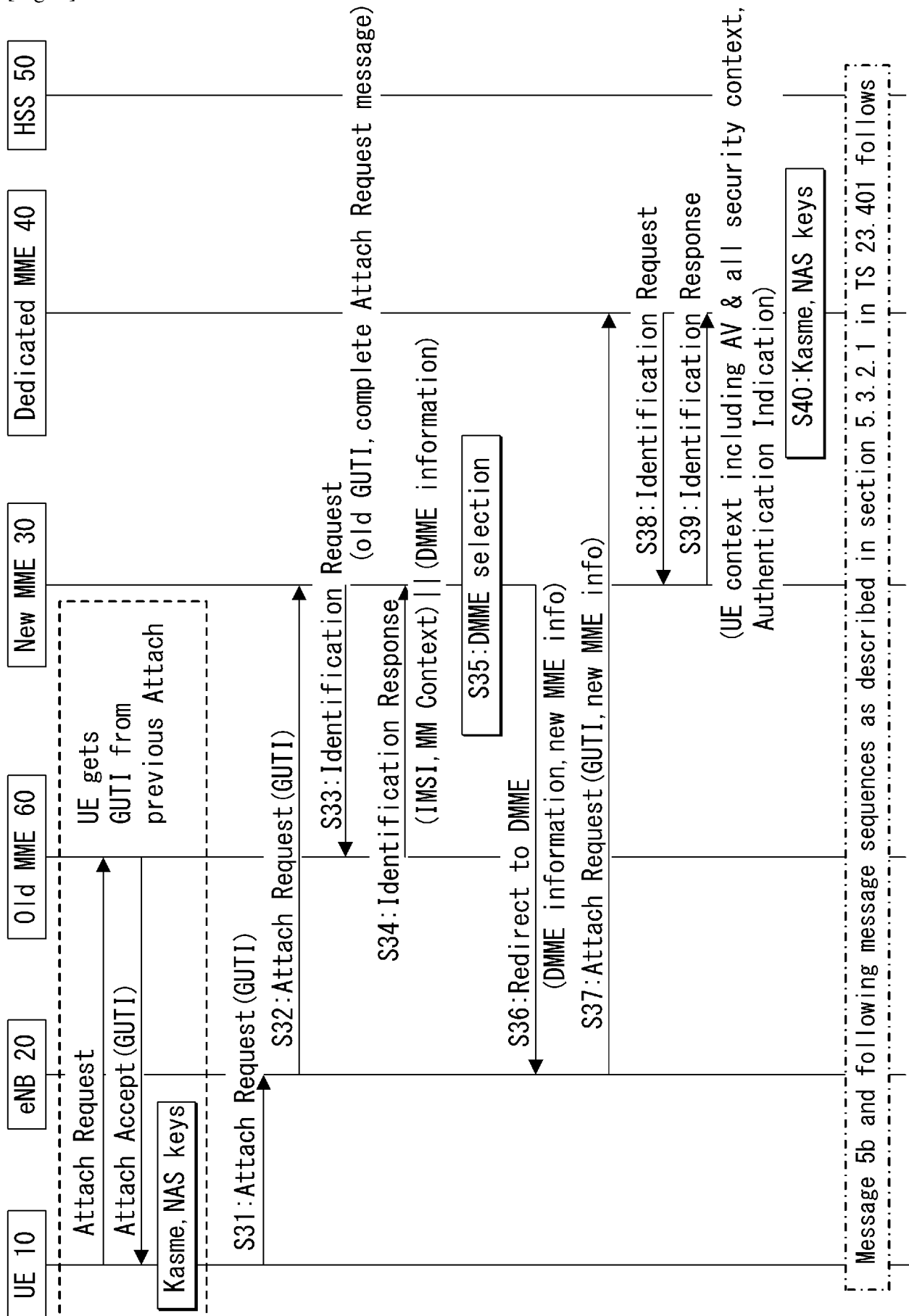
[Fig. 2]



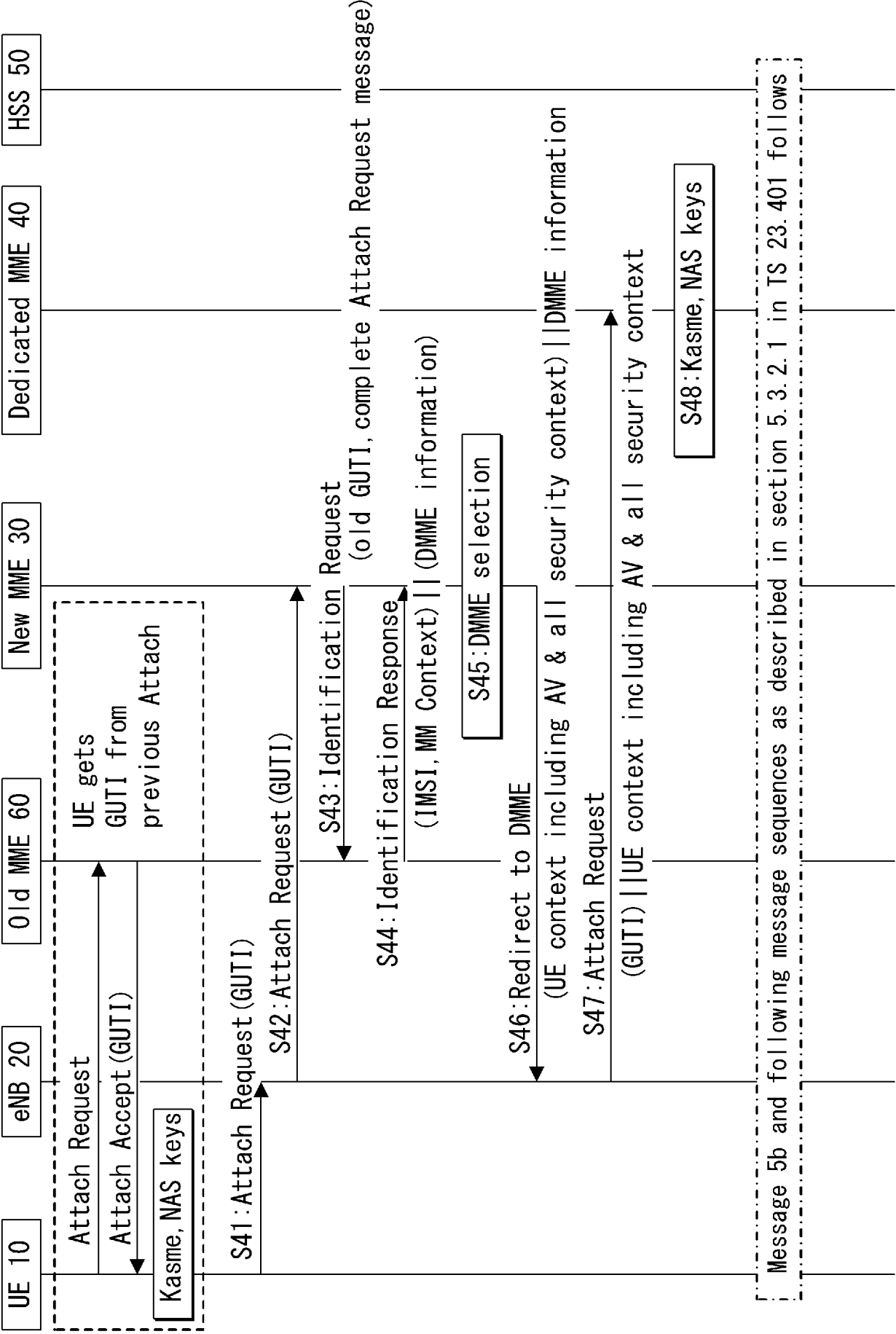
[Fig. 3]



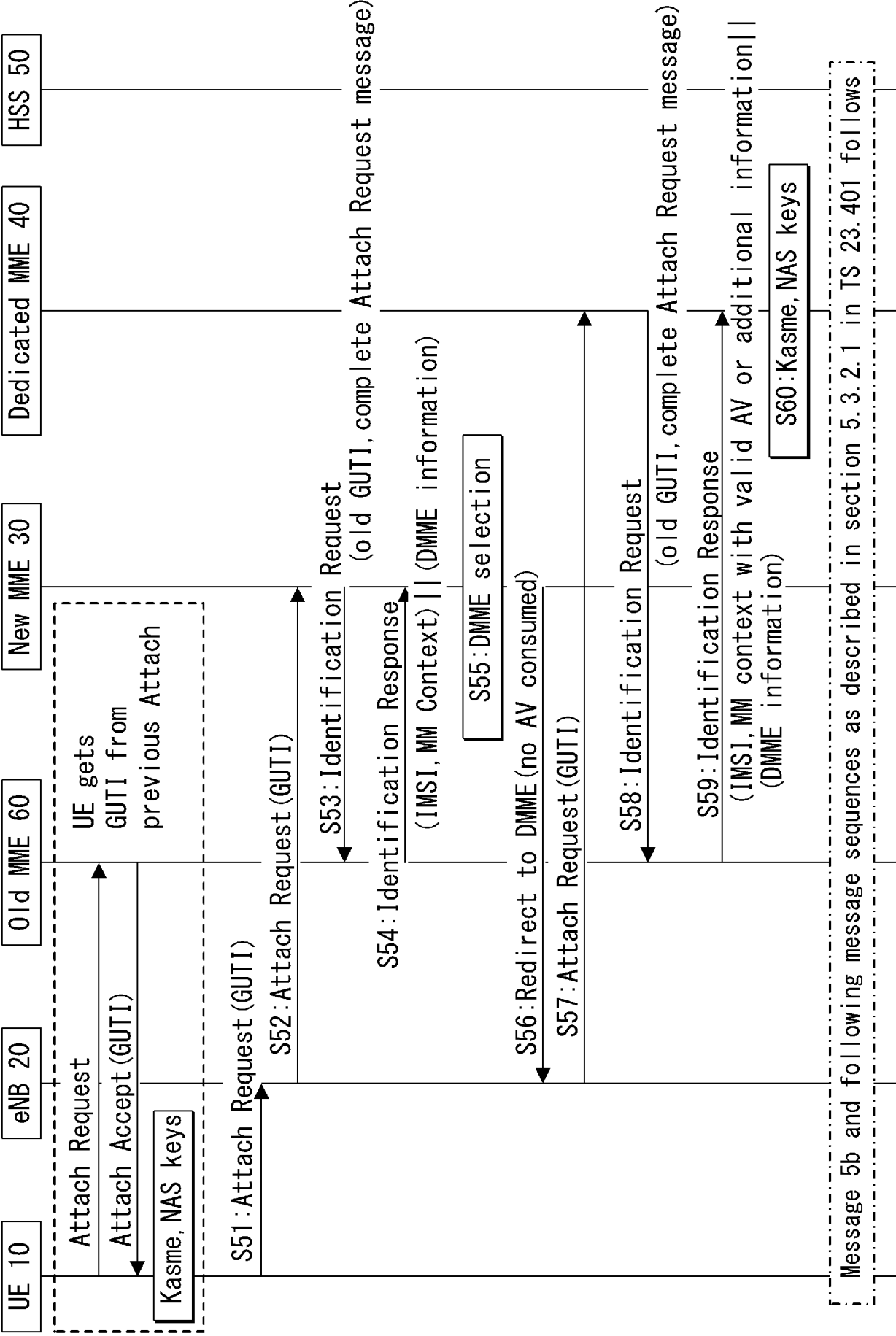
[Fig. 4]



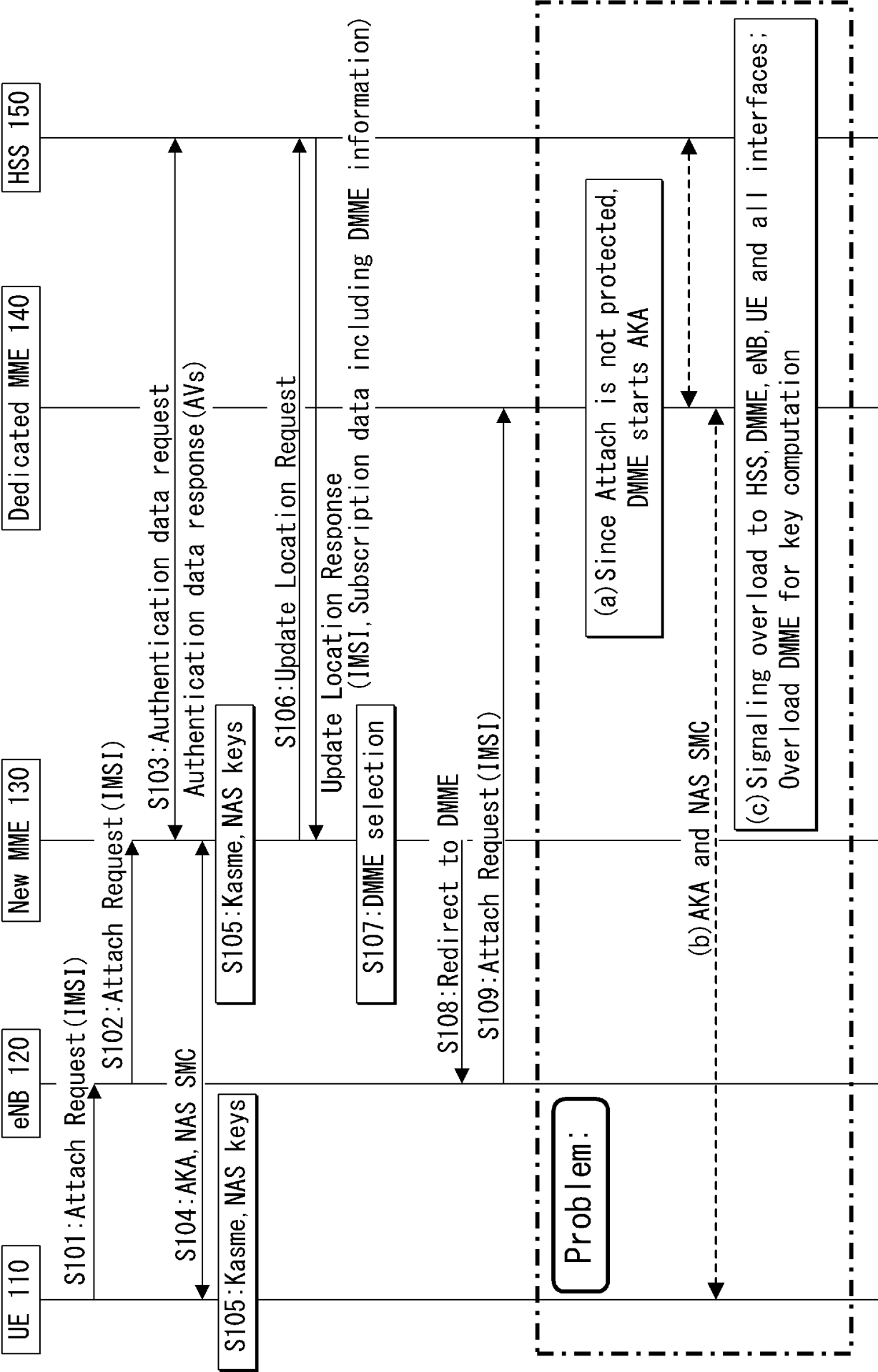
[Fig. 5]



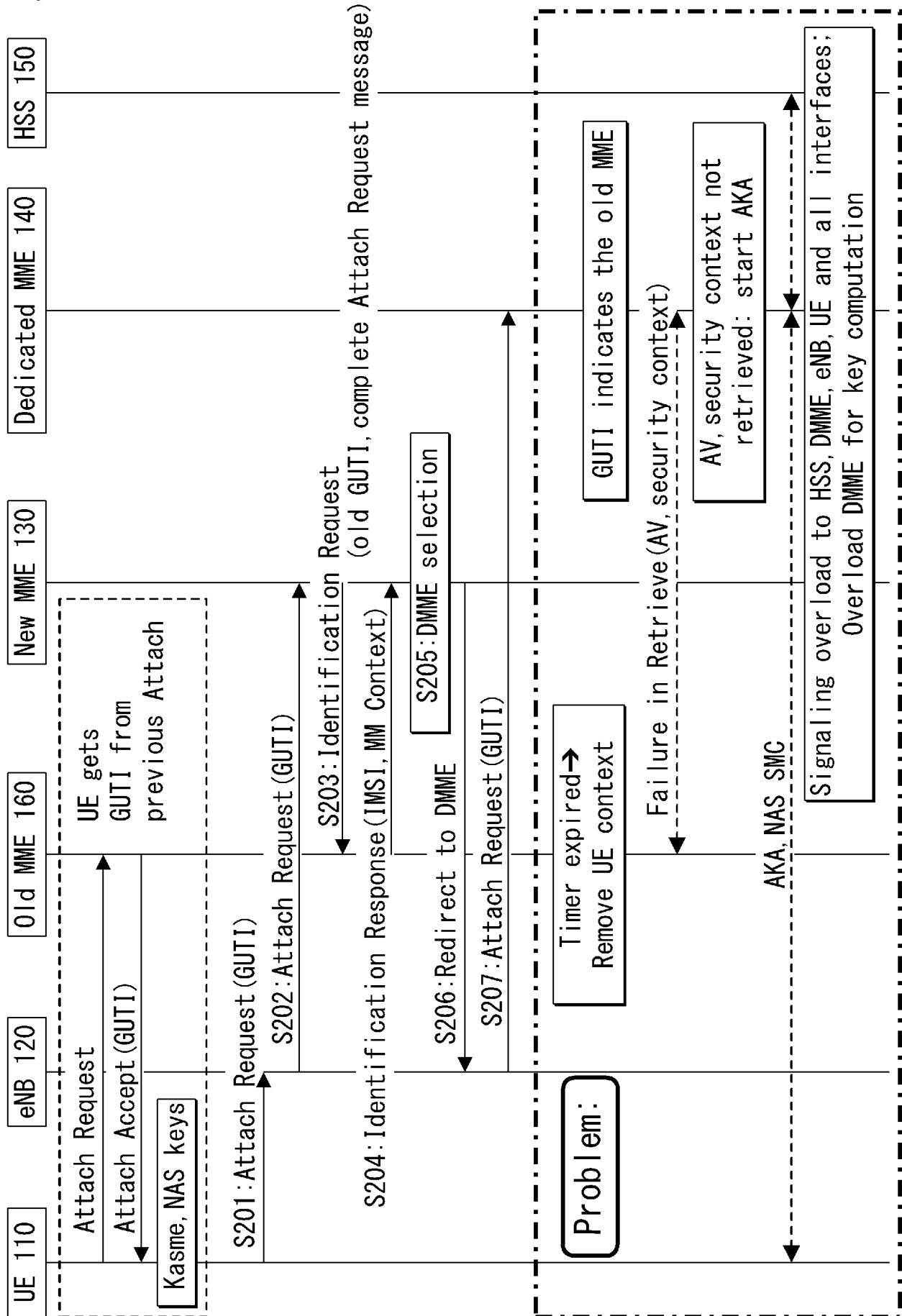
[Fig. 6]



[Fig. 7]



[Fig. 8]



INTERNATIONAL SEARCH REPORT

International application No

PCT/JP2015/002635

A. CLASSIFICATION OF SUBJECT MATTER
 INV. H04W48/18 H04W60/00
 ADD.

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

B. FIELDS SEARCHED

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

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 2013/047822 A1 (NEC CORP [JP]; ZEMBUTSU HAJIME [JP]; TAMURA TOSHIYUKI [JP]; IWAI TAKAN) 4 April 2013 (2013-04-04)	1,8,15, 17
Y	the whole document	2-7, 9-14,16, 18
	& EP 2 763 496 A1 (NEC CORP [JP]) 6 August 2014 (2014-08-06) abstract paragraph [0016] - paragraph [0019] paragraph [0025] paragraph [0049] - paragraph [0057] figures 1,3 ----- -/--	



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

15 September 2015

Date of mailing of the international search report

22/09/2015

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

del Sorbo, Filomena

INTERNATIONAL SEARCH REPORT

International application No

PCT/JP2015/002635

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2011/230188 A1 (GEMSKI SVEN [SE]) 22 September 2011 (2011-09-22) abstract figures 2-3 paragraph [0010] - paragraph [0013] paragraph [0027] - paragraph [0031] claims 9-12 claims 15-16 -----	2-7, 9-14, 16, 18
A	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System Improvements for Machine-Type Communications; (Release 11)", 3GPP STANDARD; 3GPP TR 23.888, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. V1.4.0, 5 August 2011 (2011-08-05), pages 1-139, XP050553713, page 1 - page 10 page 58 - page 70 -----	1-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/JP2015/002635

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2013047822 A1	04-04-2013	CN 103858517 A	11-06-2014
		EP 2763496 A1	06-08-2014
		JP 5500320 B2	21-05-2014
		JP 2014132785 A	17-07-2014
		JP WO2013047822 A1	30-03-2015
		US 2014211728 A1	31-07-2014
		WO 2013047822 A1	04-04-2013

US 2011230188 A1	22-09-2011	EP 2548396 A1	23-01-2013
		US 2011230188 A1	22-09-2011
		WO 2011115543 A1	22-09-2011
