



(51) International Patent Classification:

H04W 12/04 (2009.01) *H04B* 7/26 (2006.01)
H04W 12/06 (2009.01) *H04W* 4/08 (2009.01)

(21) International Application Number:

PCT/KR2011/004021

(22) International Filing Date:

1 June 2011 (01.06.2011)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

1508/CHE/2010 1 June 2010 (01.06.2010) IN

(71) Applicant (for all designated States except US): **SAM-SUNG ELECTRONICS CO., LTD.** [KR/KR]; 416, Maetan-dong, Yeongtong-gu, Suwon-si, Gyeonggi-do 442-742 (KR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **RAJADURAI, Rajavelsamy** [IN/IN]; Bagmane Lakeview, Block 'B', No. 66/1, Bagmane Tech Park, C V Raman Nagar, Byrasandra, Bangalore 560093 (IN). **LIM, Han-Na** [KR/KR]; #202, 612-135, Banpo 4-dong, Seocho-gu, Seoul 137-807 (KR).

(74) Agent: **LEE, Keon-Joo**; Mihwa Bldg. 110-2, Myongryun-dong 4-ga, Chongro-gu, Seoul 110-524 (KR).

(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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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.

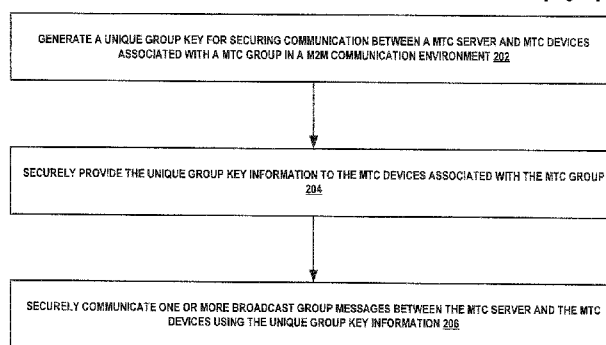
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, 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, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report (Rule 48.2(g))

(54) Title: METHOD AND SYSTEM OF SECURING GROUP COMMUNICATION IN A MACHINE-TO-MACHINE COMMUNICATION ENVIRONMENT

[Fig. 2]



299

(57) Abstract: The present invention provides a method and system for securing group communication in a machine-to-machine communication environment. In one embodiment, a non-access stratum attach request message is received from a MTC device associated with a MTC group. The MTC device is then authenticated based on subscription data associated with the MTC device. Accordingly, a unique group key is generated for securing group communication with the MTC device associated with a MTC group in a M2M communication environment. The unique group key information is then securely provided to the MTC device and to an associated enhanced node B. The unique group key information may include a unique group key, an index value associated with the unique group key, selected security algorithm, and key validity period. Based on the unique group key information, broadcast group messages are securely communicated between a MTC server or a network entity and the MTC device.

Description

Title of Invention: METHOD AND SYSTEM OF SECURING GROUP COMMUNICATION IN A MACHINE-TO-MACHINE COMMUNICATION ENVIRONMENT

Technical Field

- [1] The present invention relates to the field of machine to machine (M2M) communication, and more particularly relates to group communication in a M2M environment.

Background Art

- [2] Machine-to-Machine (M2M) communication (also referred to as "machine-type communications" or "MTC") is a form of data communication between devices that do not necessarily need human interaction (commonly known as MTC devices). For example, in an M2M communication, a MTC device (such as a sensor or meter) may capture an event data which is then relayed through an operator network to an application residing in a MTC server for analysis and necessary action. Typically, the MTC device and the MTC server communicate with each other using an operator network based on network technologies such as Third Generation Partnership Project (3GPP) technologies such as Global System for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS), Long Term Evolution (LTE), and so on.
- [3] M2M communication may be used in a variety of areas such as smart metering systems (e.g., in applications related to power, gas, water, heating, grid control, and industrial metering), surveillance systems, order management, gaming machines, and health care communication. Additionally, M2M communication based on machine type communication (MTC) technology may be used in areas such as customer service.
- [4] Recent advancement in M2M communication has enabled grouping of MTC devices together such that the operator of MTC devices can easily manage MTC devices belonging to the same group. For example, a MTC server can be linked to production plants (employing MTC devices) together to monitor and maximize production. The MTC devices belonging to the same group can be in a same location, have same MTC features and/or belong to the same MTC user. This provides flexibility to allocate a group and hence may provide easier mode to control/update/charge the MTC devices in a granularity of a group. Thus, redundant signalling may be significantly reduced to avoid congestion.
- [5] In a MTC group, it is desirable that the MTC devices are securely addressed for control, management, or charging facilities. However, currently, one or more group messages are broadcasted to the MTC devices in an insecure manner, which may

sometimes lead to spoofing of group messages.

Disclosure of Invention

Technical Problem

- [6] An aspect of the present invention is to provide a method and system for securing group communication in a machine-to-machine communication environment.

Solution to Problem

- [7] In accordance with one aspect of the present invention, there is provided a method for securing group communication in a machine-to-machine (M2M) communication environment, wherein the M2M communication environment comprises a plurality of machine type communication (MTC) groups, and wherein each of the plurality of MTC groups comprises a plurality of MTC devices, the method comprises generating a unique group key for securing communication with MTC devices associated with a MTC group in a M2M communication environment, securely providing the unique group key information to the MTC devices associated with the MTC group, and securely communicating one or more broadcast group messages with the MTC devices using the unique group key information.
- [8] In accordance with another aspect of the present invention, there is provided a machine-to-machine communication system. The machine-to-machine communication system comprises a plurality of machine type communication (MTC) devices, wherein the plurality of MTC devices are belong to one or more MTC groups, a MTC server communicatively coupled with the plurality of MTC devices, and a network entity for securing group communication between the MTC server and the plurality of MTC devices, wherein network entity comprises a group key module for generating a unique group key for securing communication with one or more of the plurality of MTC devices associated with at least one MTC group, securely providing the unique group key information to the one or more of the plurality of MTC devices associated with the at least one MTC group, and securely communicating one or more broadcast group messages with the one or more of plurality of MTC devices using the unique group key information.
- ### **Brief Description of Drawings**
- [9] The above and other aspects, features and advantages of certain exemplary embodiments of the present invention will be more apparent from the following description taken in conjunction with the accompanying drawings, in which:
- [10] Figure 1 is a block diagram illustrating a machine-to-machine (M2M) communication environment for securing group communication with machine type communication (MTC) devices belonging to a MTC group, according to one embodiment.
- [11] Figure 2 is a process flowchart illustrating an exemplary method of securing group

communication between a MTC server and the MTC devices belonging to the MTC group, according to one embodiment.

[12] Figure 3a and 3b are a flow diagram illustrating distributing a unique group key to MTC devices in a MTC group using a non-access stratum (NAS) security mode command (SMC) procedure in a long term evolution (LTE) network, according to one embodiment.

[13] Figure 4a and 4b are a flow diagram illustrating distributing a unique group key to MTC devices in a MTC group using a NAS SMC procedure, according to another embodiment.

[14] Figure 5a and 5b are a flow diagram illustrating distributing a unique group key to MTC devices in a MTC group using a protocol configuration options (PCO), according to another embodiment.

[15] The drawings described herein are for illustration purposes only and are not intended to limit the scope of the present disclosure in any way.

Mode for the Invention

[16] The present invention provides a method and system for securing communication in a machine-to-machine (M2M) communication environment. In the following detailed description of the embodiments of the invention, reference is made to the accompanying drawings that form a part hereof, and in which are shown by way of illustration specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that changes may be made without departing from the scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims.

[17] Figure 1 is a block diagram illustrating a M2M communication environment 100 for securing group communication with MTC devices belonging to a MTC group, according to one embodiment. In Figure 1, the M2M communication environment 100 includes an operator network 102, MTC groups 104A-N and a MTC server 106. The operator network 102 illustrated herein is a long term evolution network and hence includes a mobile management entity (MME) (e.g., a network entity) 104, a home subscriber server (HSS) 106, a serving gateway 108, a packet data network (PDN) gateway 110, one or more eNB terminals 112A-N. It can be understood that, the operator network 102 can be a Global System for Mobile Communications (GSM) network, a Universal Mobile Telecommunications System (UMTS) network, a Worldwide Interoperability for Microwave Access (WiMAX) network and the like.

[18] The MTC groups 104A-N are formed by grouping a plurality of MTC devices as-

sociated with the operator network 102. For example, the operator network 102 may form a MTC group 114A including MTC devices 116A-N and a MTC group 114B including MTC devices 118A-N based on user, location and features associated with the MTC devices 116A-N and 118A-N.

- [19] In some embodiments, the MTC server 120 communicates with the MTC devices 116A-N and 118A-N based on MTC group(s) to which it belongs. It can be noted that, one or more MTC devices may belong to more than one MTC group. In these embodiments, the operator network 102 enables the MTC server 120 or any other network entity to securely communicate with MTC devices belonging to the MTC groups 114A-N.
- [20] For the purpose of illustration, consider that the MTC server 120 has to send a group message to the MTC devices 116A-N belonging to the MTC group 114A via the operator network 102. In order to securely communicate the group message, a group key module 112 in the MME 104 identifies a MTC group associated with the MTC devices 116A-N. The group key module 112 may identifies the MTC group 114A by obtaining the information associated with the MTC group 114A from the HSS 106 or a source MME or Serving GPRS Support Node (SGSN). If the MTC group 114A is formed by the HSS 106, then the information associated with the MTC group 114A is obtained from the HSS 106. Accordingly, the group key module 112 generates a unique group key based on the information (e.g., group identifier) associated with the MTC group 114A. In one embodiment, the unique group key identifier may be provided with a validity period. The validity period indicates duration of time for which the unique group key is valid.
- [21] Then, the group key module 112 securely distributes the unique group key information to the MTC devices 116A-N associated with the MTC group 114A via an associated eNB (e.g., the eNB 112A). For example, the unique group key information includes unique group key, an index value associated with the unique group key, validity period associated with the unique group key, and selected security algorithm for group message protection. In some embodiments, the unique group key information is securely distributed to the MTC devices 116A-N using a non access stratum (NAS) security mode command (SMC) procedure, a new MTC group SMC procedure, or a protocol configuration options (PCO) as will be illustrated in Figures 3 through 5. Upon secured distribution, the group key module 112 also communicates the unique group key information associated with the MTC group 114A to the associated eNB 112A, whereby the eNB 112A stores the unique group key information in its memory for further use.
- [22] Accordingly, when a group message(s) is received from the MTC server 120, the eNB 114 encrypts the group message(s) using the unique group key information and

broadcast the encrypted group message(s) to the MTC devices 116A-N. Thus, the group message(s) are protected from spoofing. When each of the MTC devices 116A-N receives the encrypted group message(s), each of the MTC devices 116A-N decrypts the encrypted group message(s) using the unique group key information received from the operator network 102 for further processing. In this manner, data communication of group messages is performed in a secured manner using the unique group key information. It can be noted that, if the unique group key is carrying a validity period, the group key module 122 generates a new group key and an index associated with the new group key and distributes the same prior to expiry of the validity period as the manner explained above.

[23] Figure 2 is a process flowchart illustrating an exemplary method 200 of securing group communication between the MTC server 120 and the MTC devices 116A-N belonging to the MTC group 114A, according to one embodiment. At step 202, a unique group key is generated for securing communication between the MTC server 120 and the MTC devices 116A-N associated with the MTC group 114A in the M2M communication environment. In one exemplary implementation, the unique group key is generated based upon receipt of non-access stratum (NAS) attach request message from one of the MTC devices 116A-N (e.g., a first member of the MTC group 114A) and performing a network access authentication procedure.

[24] At step 204, the unique group key information is securely provided to the MTC devices 116A-N associated with the MTC group 114A. In one embodiment, the unique group key information is encrypted using a non-access stratum (NAS) security context established between said one of the MTC device 116A-N and the MME 104. At step 206, one or more broadcast group messages are securely communicated between the MTC server 120 and the MTC devices 116A-N using the unique group key information.

[25] Figure 3a and 3b are a flow diagram 300 illustrating distributing a unique group key to MTC devices in a MTC group using a non-access stratum (NAS) security mode command (SMC) procedure in a LTE network, according to one embodiment. At step 302, a MTC device 116A sends a NAS attach request message to an eNB 112A. For example, the NAS attach request message is sent at the end of a radio resource control (RRC) connection set procedure. At step 304, the eNB 112A forwards the NAS attach request message to the MME 104. At step 306, the MME 104 performs a network access authentication procedure with the MTC device 116A. During the authentication procedure, the MME 104 downloads subscription information from the HSS 106. For example, the subscription information includes a group identifier associated with a MTC group to which the MTC belongs to.

[26] At step 308, the MME 104 generates a unique group key per group (Gkey) and

assigns a group key index (Gki) to the unique group key (e.g., if the key is not generated previously for the MTC group). Alternatively, if the unique group key is already generated, the MME 104 retrieves the previously stored unique group key for the MTC device 116A. Also, at step 308, the MME 104 stores the group information for NAS level protection of group messages for the MTC group 114A. In one embodiment, the MME 104 may derive cryptographic keys from the unique group key for userplane, NAS and AS message protection. In another embodiment, the MME 104 may dynamically form a new group based on the subscriber information and MTC feature subscribed. For example, the MME creates the MTC group for MTC devices accessing the MTC server 120 from a particular location.

- [27] At step 310, the MME 104 performs a NAS SMC procedure with the MTC device 116A to activate integrity protection and NAS ciphering. At step 312, the MME 104 securely communicates the unique group key information (e.g., group identifier, Gkey, and Gki) in a group SMC message to the MTC device 116A. It can be noted that, the group SMC message including the unique group key information can also be sent during the NAS SMC procedure. In some embodiments, the unique group key information is protected by a NAS security context established between the MTC device 116A and the MME 104. In these embodiments, the unique group key information is encrypted by the NAS security context such that only the MTC device 116A can decrypt it. In one embodiment, the group SMC message also includes selected security algorithms (integrity protection and encryption algorithms) for group message protection. It is appreciated that, the MME 104 is also capable of initiating a group SMC procedure at any point of time to refresh or to assign a new group key (Gkey) and related information. It is understood that, the decision to refresh the unique group key based on validity period or based on number of messages protected or based on number of MTC devices attached or detached or wrap-around of a count value. Moreover, the unique group key is refreshed based on configuration option and operator policy.

- [28] At step 314, the MME 104 sends an update location request to the HSS 106. At step 316, the HSS 106 sends an update location acknowledgment including subscription information associated with the MTC device 116A to the MME 104. At step 318, the MME 104 sends a create session request to the serving gateway 108 for creating a default bearer. The create session request may include IMSI, E-RAB setup list (E-RAB ID), and Group ID. At step 320, the serving gateway 108 forwards the create session request to the PDN gateway 110. The forwarded create session request may include IMSI, E-RAB ID, Group ID, S5 downlink information and so on. The S5 downlink information includes internet protocol (IP) address of the serving gateway 108 and GTP-U TEID.

- [29] Accordingly, at step 322, the PDN gateway 110 sends a create session response (e.g., including Enhanced Radio Access Bearer Identity (E-RAB ID), common S5 uplink information, etc.) to the serving gateway 108 in response to the create session request. The serving gateway 108 then forwards the create session response (e.g., including E-RAB ID, common S1 uplink information, etc.) to the MME 104, at step 324. At step 326, the MME 104 sends a context setup message (including NAS attach accept, E-RAB setup list, unique group key information, S1 uplink information, etc.) to the eNB 112A. At step 328, the eNB 112A stores the unique group key information for group message protection.
- [30] At step 330, the eNB 112A performs a RRC connection reconfiguration procedure with the MTC device 116A. At step 332, the MTC device 116A sends a RRC connection reconfiguration complete message to the eNB 112A. Upon completion, the eNB 112A sends a context setup response including E-RAB setup list (e.g., E-RAB ID, S1 downlink information and so on) to the MME 104, at step 334. For example, the S1 downlink information includes Internet Protocol (IP) address of the eNB 112A and General Packet Radio Service (GPRS) Tunnelling Protocol Tunnel Endpoint Identifier (GTP-U TEID).
- [31] At step 336, the MME 104 sends an update session request (e.g., IMSI, E-RAB ID, S1 downlink information, etc.) to the serving gateway 108. Accordingly, at step 338, the serving gateway 108 sends an update session response to the MME 104 in response to the update session request. At step 340, uplink and downlink data transmission between the MTC server 120 and the MTC device 116A is performed in a secured manner using the unique group key information, as explained in Figure 1. It can be noted that, the MTC device 116A deletes the unique group key information when the MTC device detaches from the operator network 102.
- [32] Figure 4a and 4b are a flow diagram 400 illustrating distributing a unique group key to MTC devices in a MTC group using a NAS SMC procedure, according to another embodiment. At step 402, a MTC device 116A sends a NAS attach request message to an eNB 112A. For example, the NAS attach request message is sent at the end of a radio resource control (RRC) connection set procedure. At step 404, the eNB 112A forwards the NAS attach request message to the MME 104. At step 406, the MME 104 performs a network access authentication procedure with the MTC device 116A. During the authentication procedure, the MME 104 downloads subscription information from the HSS 106. For example, the subscription information includes a group identifier indicating a MTC group to which the MTC belongs to.
- [33] At step 408, the MME 104 performs a NAS SMC procedure with the MTC device 116A to activate integrity protection and NAS ciphering. At step 410, the MME 104 sends an update location request to the HSS 106. At step 412, the HSS 106 sends an

update location acknowledgment including subscription information associated with the MTC device 116A to the MME 104.

- [34] At step 414, the MME 104 generates a unique group key per group (Gkey) and assigns a group key index (Gki) (if not generated previously for the MTC group 114A). Also, at step 414, the MME 104 stores the group information for NAS level protection of group messages for the MTC group 114A. At step 416, the MME 104 securely communicates the unique group key information (e.g., group identifier, Gkey, and Gki) in a group SMC message to the MTC device 116A. In one embodiment, the unique group key information is protected using a NAS security context established between the MTC device 116A and the MME 104. At step 418, the MME 104 sends a create session request to the serving gateway 108 for creating a default bearer. The create session request may include IMSI, E-RAB setup list (E-RAB ID), and Group ID. At step 420, the serving gateway 108 forwards the create session request to the PDN gateway 110. The forwarded create session request may include IMSI, E-RAB ID, Group ID, S5 downlink information and so on. The S5 downlink information includes internet protocol (IP) address of the serving gateway 108 and GTP-U TEID.
- [35] Accordingly, at step 422, the PDN gateway 110 sends a create session response (e.g., including E-RAB ID, common S5 uplink information, etc.) to the serving gateway 108 in response to the create session request. The serving gateway 108 then forwards the create session response (e.g., including E-RAB ID, common S1 uplink information, etc.) to the MME 104, at step 424. At step 426, the MME 104 sends a context setup message (including NAS attach accept, E-RAB setup list, unique group key information, S1 uplink information, etc.) to the eNB 112A. At step 428, the eNB 112A stores the unique group key information for group message protection.
- [36] At step 430, the eNB 112A performs a RRC connection reconfiguration procedure with the MTC device 116A. At step 432, the MTC device 116A sends a RRC connection reconfiguration complete message to the eNB 112A. Upon completion, the eNB 112A sends a context setup response including E-RAB setup list (e.g., E-RAB ID, S1 downlink information and so on) to the MME 104, at step 434. For example, the S1 downlink information includes IP address of the eNB 112A and GTP-U TEID.
- [37] At step 436, the MME 104 sends an update session request (e.g., IMSI, E-RAB ID, S1 downlink information, etc.) to the serving gateway 108. Accordingly, at step 438, the serving gateway 108 sends an update session response to the MME 104 in response to the update session request. At step 440, communication of group messages between the MTC server 120 and the MTC device 116A is performed in a secured manner using the unique group key information, as explained in Figure 1.
- [38] Figure 5a and 5b is a flow diagram 500 illustrating distributing a unique group key to MTC devices in a MTC group using a PCO, according to another embodiment. At step

502, a MTC device 116A sends a NAS attach request message to an eNB 112A. For example, the NAS attach request message is sent at the end of a radio resource control (RRC) connection set procedure. At step 504, the eNB 112A forwards the NAS attach request message to the MME 104. At step 506, the MME 104 performs a network access authentication procedure with the MTC device 116A. During the authentication procedure, the MME 104 request authentication vectors for an Authentication and Key Agreement (AKA) procedure from the HSS 106. It can be noted that, the HSS 106 can send one or more authentication vectors to the MME104.

[39] At step 508, the MME 104 performs a NAS SMC procedure with the MTC device 116A to activate integrity protection and NAS ciphering. At step 510, the MME 104 sends an update location request to the HSS 106. At step 512, the HSS 106 sends an update location acknowledgment including subscription information associated with the MTC device 116A to the MME 104. In one embodiment, the HSS 106 indicates a group ID to which the MTC device 116 belongs to.

[40] At step 514, the MME 104 generates a unique group key per group (Gkey) and assigns a group key index (Gki) or retrieves the unique group key per group (Gkey) and assigns a group key index (Gki) if already generated and stored previously for the MTC group 114A. Also, at step 514, the MME 104 stores the newly generated group information for NAS level protection of group messages for the MTC group 114A. At step 516, the MME 104 sends a create session request to the serving gateway 108 for creating a default bearer. The create session request may include IMSI, E-RAB setup list (E-RAB ID), Group ID, Gkey, Gki, supported algorithms for group message protection or MTC device capabilities for group communication, and key for group message protection at the PDN gateway 110. At step 518, the serving gateway 108 forwards the create session request to the PDN gateway 110. The forwarded create session request may include IMSI, E-RAB ID, Group ID, S5 downlink information and so on. The S5 downlink information includes internet protocol (IP) address of the serving gateway 108 and GTP-U TEID. Upon receiving the create session request, the PDN gateway 110 checks whether a common S5 uplink bearer for the MTC group 114A is existing or not. If there is no common S5 uplink bearer for the MTC group 114A, then the PDN gateway 110 creates a S5 uplink bearer.

[41] At step 520, the PDN gateway 110 manages the MTC group 114A by assigning a particular group IP address for the MTC group 114A. Also, the PDN gateway 110 may protect the content received from the MTC subscriber at the IP layer or above the IP layer. The PDN gateway 110 also selects algorithms from the selected algorithms. At step 522, the PDN gateway 110 sends a create session response to the serving gateway 108 in response to the create session request. The create session response includes E-RAB ID, common S5 uplink information, and unique group key information in a PCO.

For group based MTC feature, the PCO contains IP address (multi-cast or unicast), group identifier, selected algorithms for group based protection, Gkey, and Gki. Upon receiving the create session response, the serving gateway 108 checks whether a common S1 uplink bearer for the MTC group 114A is existing or not. If there is no common S1 uplink bearer for the MTC group 114A, then the serving gateway 108 creates a S1 uplink bearer.

[42] The serving gateway 108 then forwards the create session response (e.g., including E-RAB ID, common S1 uplink bearer, PCO, etc.) to the MME 104, at step 524. The common S1 uplink bearer includes IP address of the serving gateway 108, and GTP-U TEID. At step 526, the MME 104 sends a context setup message (including NAS attach accept, E-RAB setup list, unique group key information, and S1 uplink information, etc.) to the eNB 112A. At step 528, the eNB 112A stores the unique group key information for group message protection. It can be noted that, the unique group key for group message protection is encrypted by the eNB 112A using an AS security context (AS ciphering).

[43] At step 530, the eNB 112A performs a RRC connection reconfiguration procedure with the MTC device 116A. At step 532, the MTC device 116A sends a RRC connection reconfiguration complete message to the eNB 112A. In one embodiment, the RRC connection reconfiguration complete message includes the PCO. Upon completion, the eNB 112A sends a context setup response including E-RAB setup list (e.g., E-RAB ID, S1 downlink information and so on) to the MME 104, at step 534. For example, the S1 downlink information includes IP address of the eNB 112A and GTP-U TEID.

[44] At step 536, the MME 104 sends an update session request (e.g., IMSI, E-RAB ID, S1 downlink information, etc.) to the serving gateway 108. Accordingly, at step 538, the serving gateway 108 sends an update session response to the MME 104 in response to the update session request. At step 540, communication of group messages between the MTC server 120 and the MTC device 116A is performed in a secured manner using the unique group key information, as explained in Figure 1.

[45] The present embodiments have been described with reference to specific example embodiments, it will be evident that various modifications and changes may be made to these embodiments without departing from the broader spirit and scope of the various embodiments. Furthermore, the various devices, modules, selectors, estimators, and the like described herein may be enabled and operated using hardware circuitry, for example, complementary metal oxide semiconductor based logic circuitry, firmware, software and/or any combination of hardware, firmware, and/or software embodied in a machine readable medium. For example, the various electrical structure and methods may be embodied using transistors, logic gates, and electrical circuits,

such as application specific integrated circuit.

Claims

- [Claim 1] A method of securing group communication in a machine-to-machine (M2M) communication environment, wherein the M2M communication environment comprises a plurality of machine type communication (MTC) groups, and wherein each of the plurality of MTC groups comprises a plurality of MTC devices, the method comprising: generating a unique group key for securing communication with MTC devices associated with a MTC group in a M2M communication environment;
- securely providing the unique group key information to the MTC devices associated with the MTC group; and
- securely communicating one or more broadcast group messages with the MTC devices using the unique group key information.
- [Claim 2] The method of claim 1, wherein the unique group key information comprises a unique group key per group, an index value associated with the unique group key, validity period associated with the unique group key, and selected security algorithm for group message protection.
- [Claim 3] The method of claim 1, generating the unique group key for securing communication with the MTC devices associated with the MTC group comprises:
- receiving a non access stratum (NAS) attach request from a MTC device;
- retrieving group identifier information associated with the MTC device, wherein the group identifier information includes at least one group identifier associated with at least one MTC group associated with the MTC device; and
- generating a unique group key and assigning a group key index to the unique group key for securing communication with the MTC device associated with the at least one MTC group.
- [Claim 4] The method of claim 1, wherein securely communicating the one or more broadcast group messages with the MTC devices using the unique group key information comprises:
- receiving one or more broadcast group messages intended for the MTC devices associated with the MTC group;
- encrypting the one or more broadcast group messages using the unique group key information; and

broadcasting the one or more encrypted broadcast group messages to the MTC devices associated with the MTC group.

[Claim 5] The method of claim 4, wherein securely communicating the one or more broadcast group messages with the MTC devices using the unique group key information further comprises:
receiving the one or more encrypted broadcast group messages from an operator network associated with the MTC group; and
decrypting, by each of the MTC devices, the one or more encrypted broadcast messages using the unique group key information.

[Claim 6] The method of claim 1, wherein securely providing the unique group key information to the MTC devices associated with the MTC group comprises:
securely distributing the unique group key information substantially simultaneously to the MTC devices associated with the MTC group using a non-access stratum (NAS) security mode command procedure.

[Claim 7] The method of claim 1, wherein securely providing the unique group key information to the MTC devices associated with the MTC group comprises:
securely distributing the unique group key information substantially simultaneously to the MTC devices associated with the MTC group using a MTC group security mode command procedure.

[Claim 8] The method of claim 1, wherein securely providing the unique group key information to the MTC devices associated with the MTC group comprises:
securely distributing the unique group key information substantially simultaneously to the MTC devices associated with the MTC group using Protocol Configuration Options (PCO).

[Claim 9] The method of claim 6 or 7, wherein in securely distributing the unique group key information substantially simultaneously to the MTC devices associated with the MTC group, the unique group key information is secured using a NAS security context.

[Claim 10] A machine-to-machine communication system comprising:
a plurality of machine type communication (MTC) devices, wherein the plurality of MTC devices are belong to one or more MTC groups;
a MTC server communicatively coupled with the plurality of MTC devices; and
a network entity for securing group communication between the MTC server and the plurality of MTC devices, wherein network entity

comprises a group key module for:

generating a unique group key for securing communication with one or more of the plurality of MTC devices associated with at least one MTC group;

securely providing the unique group key information to the one or more of the plurality of MTC devices associated with the at least one MTC group; and

securely communicating one or more broadcast group messages with the one or more of plurality of MTC devices using the unique group key information.

[Claim 11] The system of claim 10, wherein the unique group key information comprises a unique group key per group, an index value associated with the unique group key, validity period for the unique group key, and selected security algorithm for group message protection.

[Claim 12] The system of claim 10, wherein securely providing the unique group key information to the one or more of the plurality of MTC devices associated with the at least one MTC group comprises:
securely distributing the unique group key information substantially simultaneously to the plurality of MTC devices associated with the MTC group using a non access stratum (NAS) security mode command procedure.

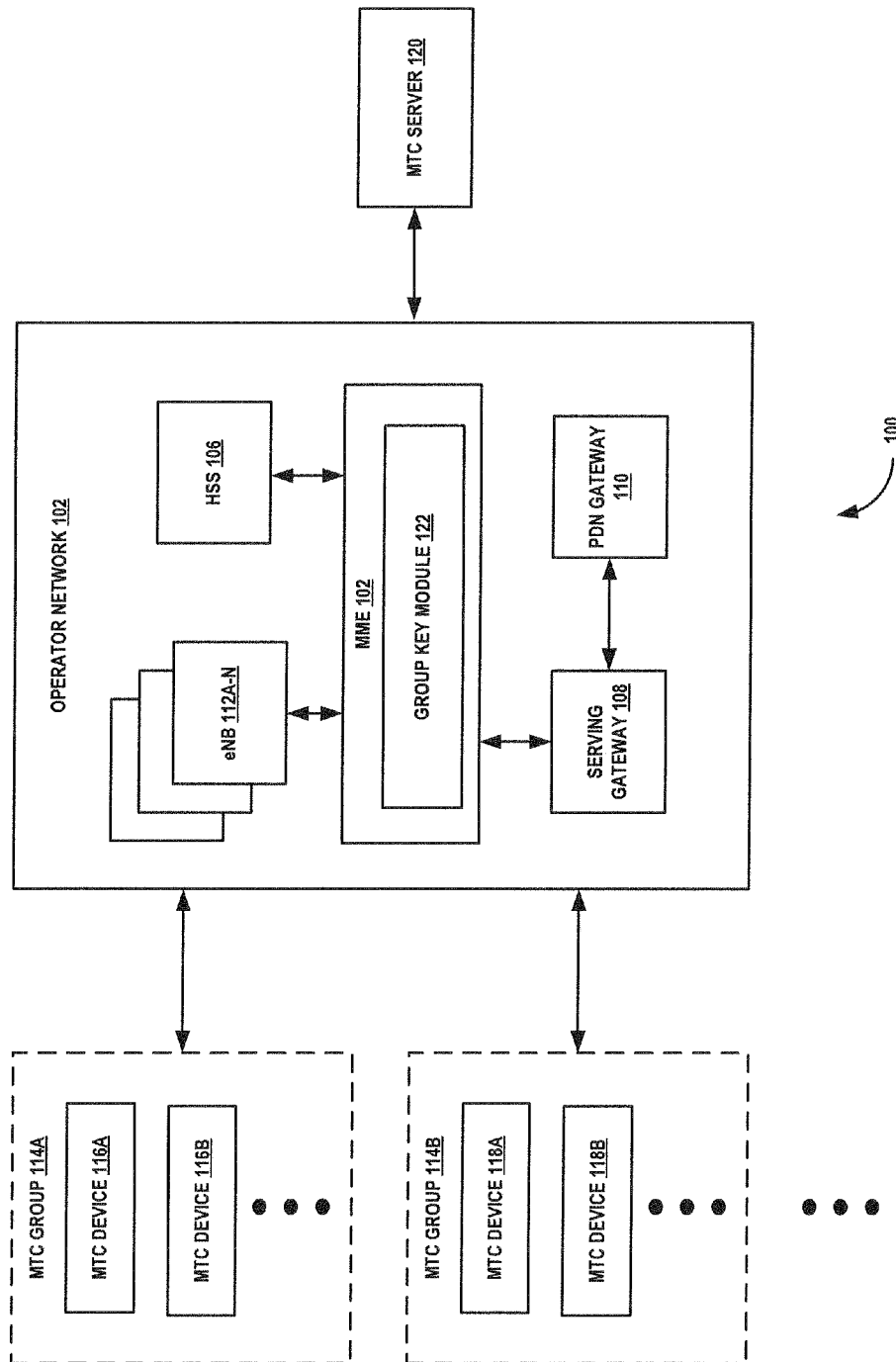
[Claim 13] The system of claim 10, wherein securely providing the unique group key information to the one or more of the plurality of MTC devices associated with the at least one MTC group comprises:
securely distributing the unique group key information substantially simultaneously to the one or more of the plurality of MTC devices associated with the at least one MTC group using a MTC group security mode command procedure.

[Claim 14] The system of claim 10, wherein securely providing the unique group key information to the one or more of plurality of MTC devices associated with the at least one MTC group comprises:
securely distributing the unique group key information substantially simultaneously to the one or more of plurality of MTC devices associated with the at least one MTC group using protocol configuration options.

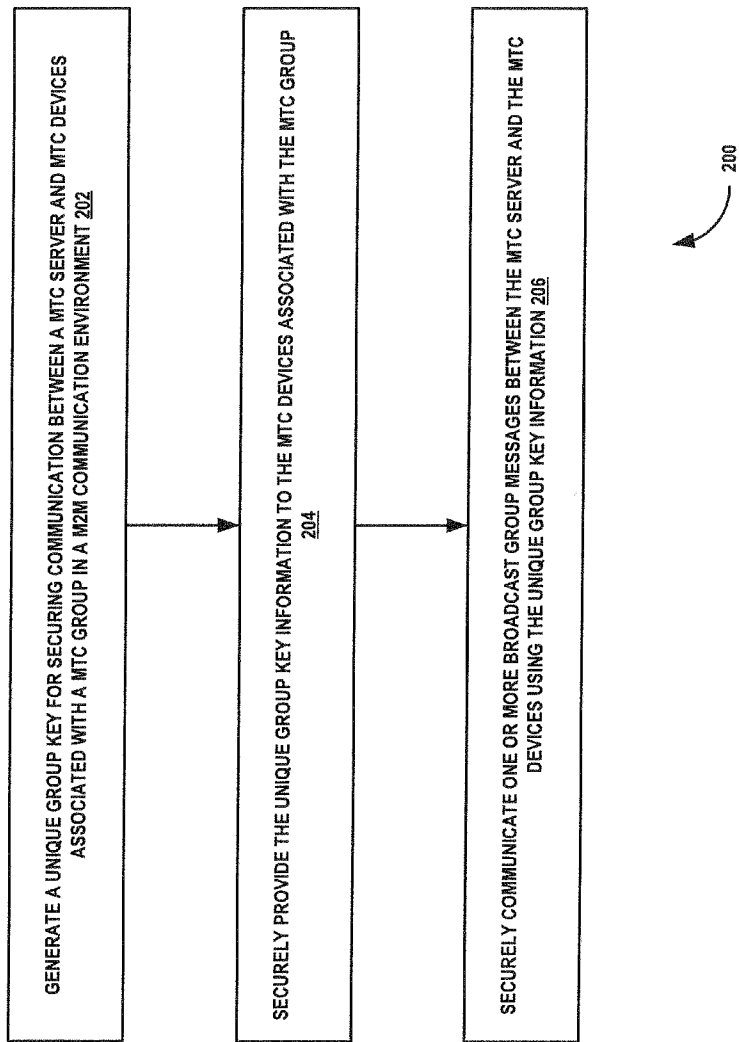
[Claim 15] The method of claim 12 or 13, wherein in securely distributing the unique group key information substantially simultaneously to the MTC devices associated with the MTC group, the unique group key information is secured using a non-access stratum (NAS) security

context.

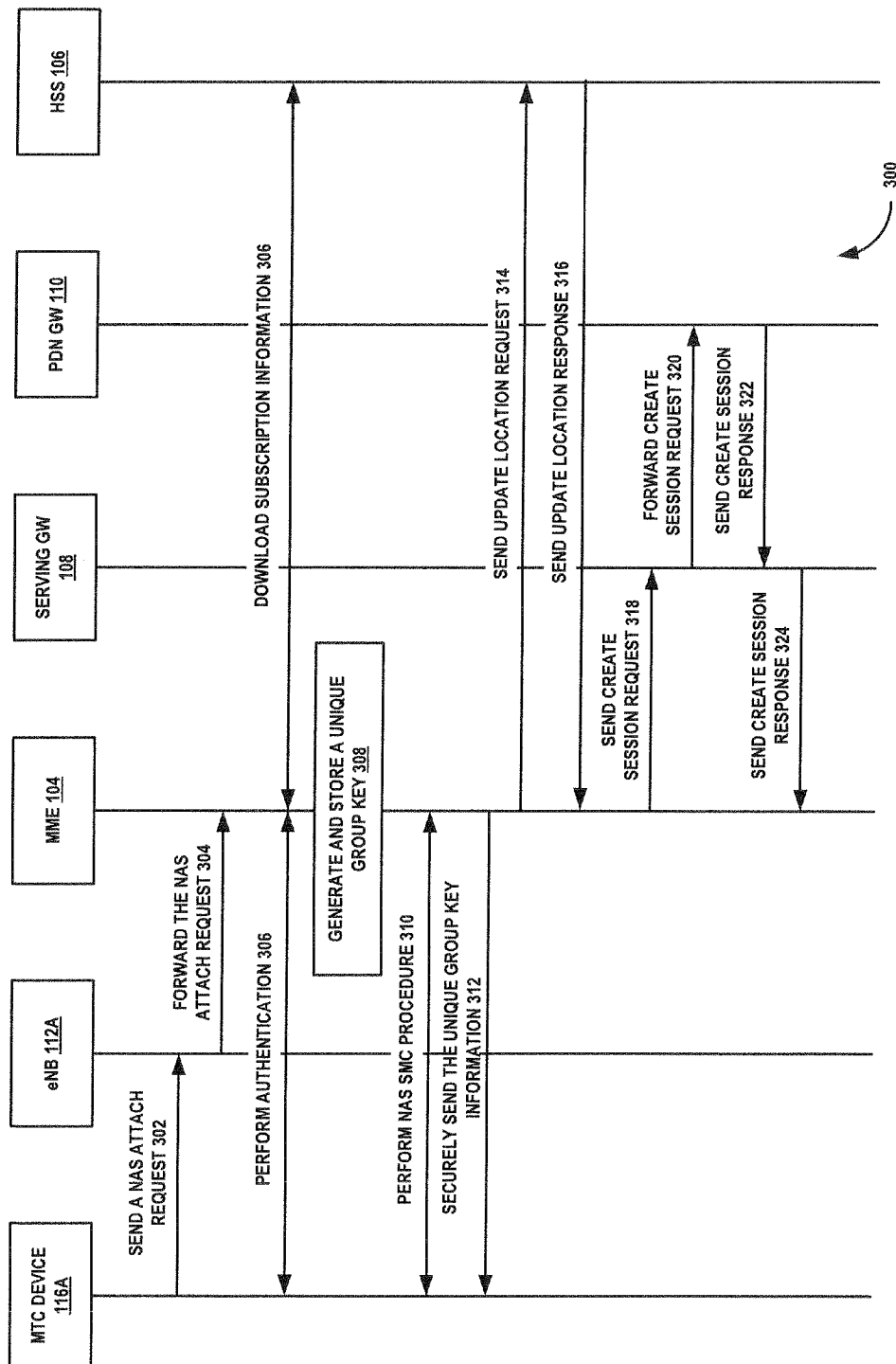
[Fig. 1]



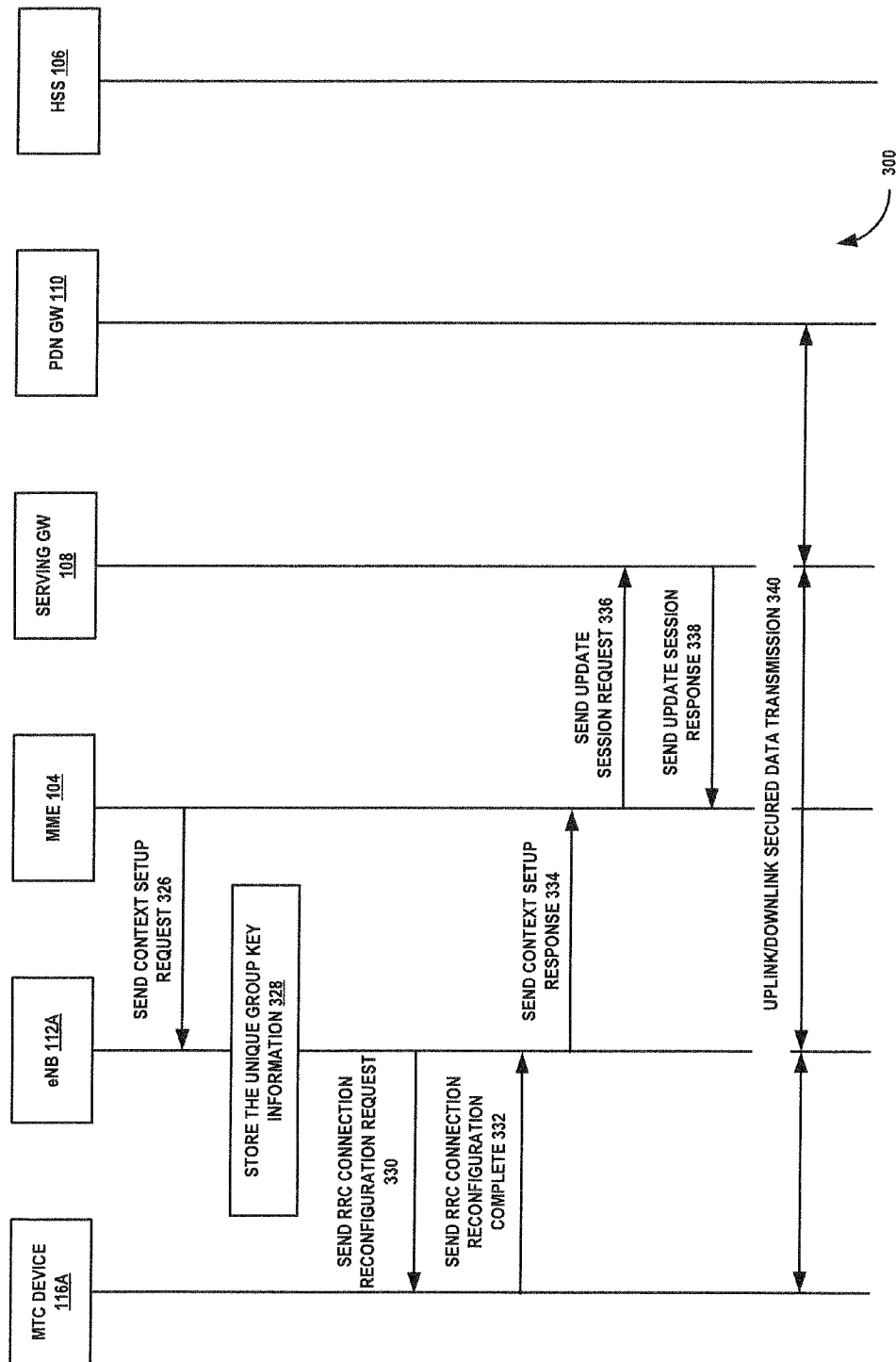
[Fig. 2]



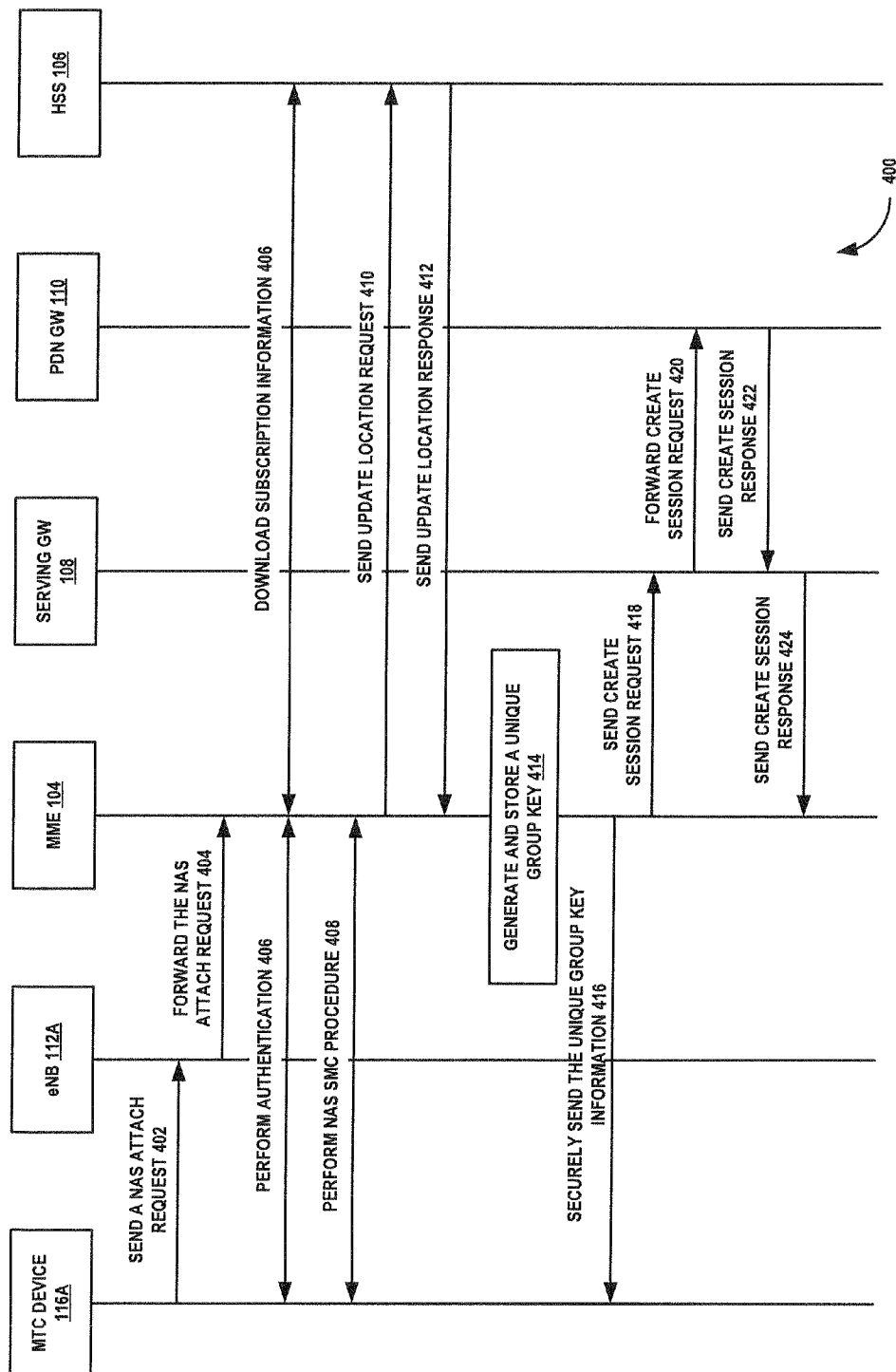
[Fig. 3a]



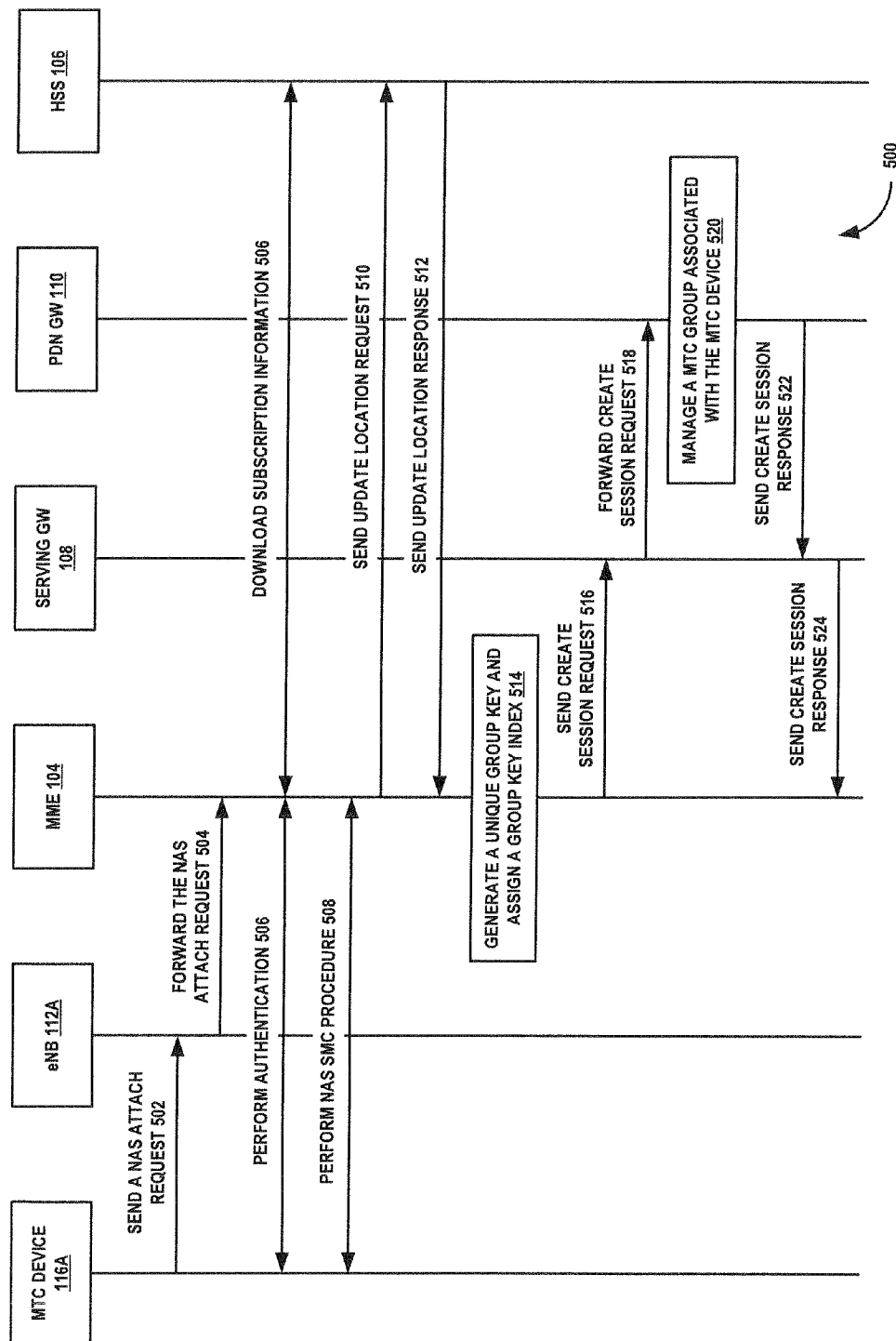
[Fig. 3b]



[Fig. 4a]



[Fig. 5a]



[Fig. 5b]

