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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2014 (03.01.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/002355 A1

(51) International Patent Classification:
H04W 4/00 (2009.01)

(21) International Application Number:
PCT/JP2013/002757

(22) International Filing Date:
23 April 2013 (23.04.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2012-147982 29 June 2012 (29.06.2012) JP
2012-209393 24 September 2012 (24.09.2012) 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). **PRASAD, Anand Raghawa**; c/o NEC Corporation, 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP).

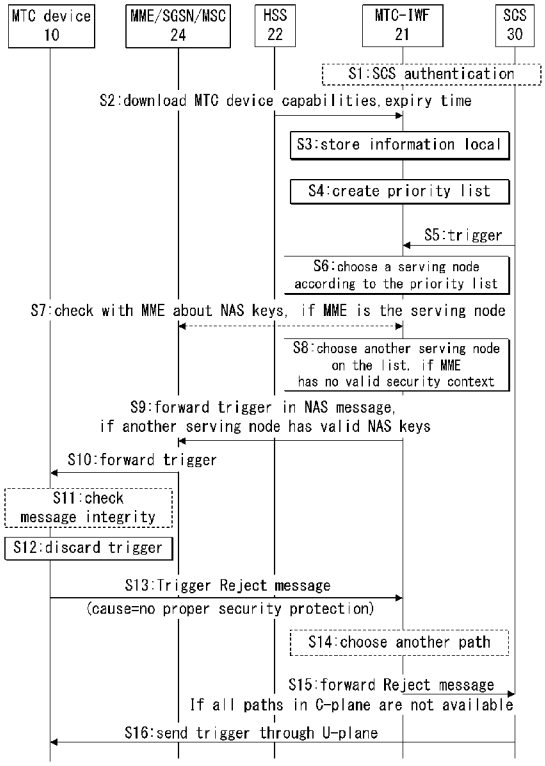
(74) Agent: **IEIRI, Takeshi**; HIBIKI IP Law Firm, Asahi Bldg. 10th Floor, 3-33-8, Tsuruya-cho, Kanagawa-ku, Yokohama-shi, Kanagawa, 2210835 (JP).

(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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, 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,

[Continued on next page]

(54) Title: OPTIMIZATION OF MTC DEVICE TRIGGER DELIVERY



(57) Abstract: A network node (21), which is placed within a core network, stores a list of network elements (24) capable of forwarding a trigger message to a MTC device (10). The network node (21) receives the trigger message from a transmission source (30, 40) placed outside the core network, and then selects, based on the list, one of the network elements to forward the trigger message to the MTC device (10). The MTC device (10) validates the received trigger message, and then transmits, when the trigger message is not validated, to the network node (21) a reject message indicating that the trigger message is not accepted by the MTC device (10). Upon receiving the reject message, the network node (21) forwards the trigger message through a different one of the network elements, or forwards the reject message to transmission source (30, 40) to send the trigger message through user plane.

WO 2014/002355 A1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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))*

Description

Title of Invention: OPTIMIZATION OF MTC DEVICE TRIGGER DELIVERY

Technical Field

[0001] The present invention relates to new functions for UE (User Equipment)/MTC (Machine-Type-Communication) device and MTC-IWF (MTC-Interworking Function), in order to provide an efficient mechanism for MTC device trigger delivery.

Background Art

[0002] MTC device triggering is a feature defined by the 3GPP's (Third Generation Partnership Project's) LTE-A (Long Term Evolution-Advanced) (see e.g. NPL 1). The MTC device triggering is sent from SCS (Services Capability Server) or SME (Short Message Entities) to network and terminated at MTC device. MTC device triggering message can be sent in NAS (Non-Access-Stratum) messages, SMS (Short Message Service), or user plane message.

[0003] MTC device trigger may not reach MTC device due to security protection check failure at UE. For example, it is described in NPL 2 that some NAS messages (e.g. Identity Request, Authentication Request, Detach Accept, etc.) with no protection can be processed by UE. If a fake MTC device trigger is embedded in such NAS messages, it can cause MTC device battery consumption, and potential mis-behaviour/mis-configuration of the MTC device.

[0004] When the secure exchange of NAS messages has not been established, UE discards the NAS messages which do not pass the integrity check (see e.g. NPL 3). When MTC device trigger is carried in such NAS messages and discarded, SCS will not have knowledge about it and may send the same trigger again. This will cause 1) overloading the network, 2) MTC device battery consumption. Another example is when trigger sent over user plane. The current 3GPP security mechanism requires con-fidential protection on user plane. Similarly problem should be considered that when the user plane message carrying trigger is not properly protected.

[0005] There is also considered an issue for SMS based trigger. In LTE where CSFB (CS (Circuit Switched) Fall Back) is in use, and SMS trigger is sent from SCS, without knowledge about if MTC device is IMS (IP (Internet Protocol) Multimedia Subsystem) support, MTC-IWF may forward the message to MME (Mobility Management Entity, assuming it is the serving node), then MME will decide what is the correct route. For example, if the UE is not IMS supported, MME will forward the SMS trigger to MSC (Mobile Switching Centre).

Citation List

Non Patent Literature

[0006] NPL 1: 3GPP TS 23.682, "Architecture Enhancements to facilitate communications with packet data networks and applications (Release 11)", v11.1.0, 2012-06

NPL 2: 3GPP TS 24.301, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 11)", v11.2.1, 2012-03

NPL 3: 3GPP TR 33.868, "Security aspects of Machine-Type Communications; (Release 11)", v0.8.0

Summary of Invention

Technical Problem

[0007] Assume that the trigger source (e.g. SCS or SME) is outside of 3GPP network domain. MTC device triggering can be sent in NAS message, user plane message or SMS message. Now, based on the background art given above, the issues to be solved include:

1. Solution for receiving not properly protected message (e.g. NAS message) carrying trigger(s);

2. Reducing network load and MTC device battery consumption; and

3. Decision making on MTC device trigger delivery route by MTC-IWF.

[0008] Currently when MTC device receives a trigger without NAS protection or user plane message, it only discards the message.

[0009] There is no requirement for MTC-IWF storing MTC device capabilities, MTC device serving node information, and trigger message.

[0010] MTC-IWF only forwards the trigger to the serving node but there is no mechanism for an optimization of path selection.

[0011] As mentioned above, currently if MTC device does not support IMS, for a network which supports CSFB, MME can forward the SMS trigger to MSC. However, the inventors of this application have found that if MTC-IWF has knowledge in the early stage, a shorter route can be taken that MTC-IWF directly forwards the SMS trigger directly to MSC.

[0012] Accordingly, an exemplary object of the present invention is to provide solutions to the above described issues such that MTC device trigger can be delivered efficiently.

Solution to Problem

[0013] In order to achieve the above-mentioned object, one exemplary aspect of this invention first considers MTC device triggering carried in unprotected NAS or user plane message. When such messages carry MTC device trigger, MTC device can discard the trigger and send a Trigger Reject message to MTC-IWF or GGSN (Gateway GPRS (General Packet Radio Service) Support Node)/P-GW (PDN (Packet data network) Gateway). MTC-IWF or GGSN/P-GW will hold this trigger message

and forward it via a different path like SGSN (Serving GPRS Support Node) in case of NAS message or S-GW (Serving Gateway) in case of user plane message. In case of NAS message, MTC-IWF can alternatively check the security status with MME and SGSN beforehand, and wrap the trigger in NAS message only when MME has valid NAS security context. The route in which the MTC device trigger is delivered, can be decided by a priority list of MTC device trigger delivery. The priority can be decided by UE capabilities and serving node information. The list can be either created in HSS (Home Subscriber Server) or MTC-IWF.

[0014] When the SMS trigger is in use and MTC device does not support IMS, without knowledge about MTC device capability, MTC-IWF may still forward the SMS trigger message to MME, if it was indicated that the MME is the current serving node by HSS. When MME finds out MTC device does not support IMS, it will forward the trigger to MSC to make it reach MTC device. This will delay the trigger delivery. While MTC-IWF can access HSS for some of MTC device information, it is proposed that MTC-IWF also requests MTC device capabilities of IMS support or not. When the MTC-IWF receives a SMS trigger, it will check its local stored MTC device capability, if the MTC device does not support IMS, it can directly forward the trigger to MSC.

Advantageous Effects of Invention

[0015] According to the present invention, it is possible to solve one or more of the above-described issues. For example, it is possible to achieve at least a part or one of the following effects 1 to 3.

[0016] 1. The network node (MTC-IWF or GGSN/P-GW) which forwards trigger or trigger source can have knowledge of the trigger discarding. It can find another path to deliver the trigger such that 1) the trigger can reach MTC device, 2) the trigger will not be re-sent on the same path thus unnecessary network traffic can be reduced and MTC device battery consumption will not be wasted.

2. MTC-IWF can decide a right path for MTC device trigger delivery in an early stage so that the trigger delivery time can be shorten and network traffic will not be wasted.

3. A priority list of MTC device trigger delivery path provides a route selection optimization such that MTC-IWF will be able to choose a proper route in an early stage and will not send the trigger through a failed path.

Brief Description of Drawings

[0017] [fig.1]Fig. 1 is a block diagram showing an example of system architecture according to an exemplary embodiment of the present invention.

[fig.2]Fig. 2 is a sequence diagram showing an example of message sequence (trigger carried in NAS message) in a system according to the exemplary embodiment of the

present invention.

[fig.3]Fig. 3 is a block diagram showing a configuration example of a network node placed within a core network in the system according to the exemplary embodiment of the present invention.

[fig.4]Fig. 4 is a block diagram showing a configuration example of a MTC device in the system according to the exemplary embodiment of the present invention.

[fig.5]Fig. 5 is a block diagram showing a configuration example of a network node placed outside the core network in the system according to the exemplary embodiment of the present invention.

Description of Embodiments

[0018] Hereinafter, an exemplary embodiment of the present invention will be described with reference to Figs. 1 to 5.

[0019] As mentioned above, when the trigger message is send over NAS, it is described in NPL 3 that trigger without NAS security protection should be discarded by MTC device. The trigger source or network node such as MTC-IWF will not know about the discard and repeatedly send the same trigger again, which may be discarded by the MTC device again. This can cause a few problems: 1) the trigger will not reach MTC device; 2) MTC device (power sensitive) will consume and waste battery; 3) network traffic waste.

[0020] In order to address these problems, as shown in Fig. 1, a system according to this exemplary embodiment includes a core network (3GPP network), one or more MTC devices 10 which connect to the core network through a RAN (Radio Access Network), and an SCS 30 and an SME 40, each of which is placed outside the core network and serves as a transmission source of a trigger message.

[0021] Among them, each MTC device 10 is a UE for MTC communication with the core network via the Um/Uu/LTE-Uu interface. The UE can host one or multiple MTC Applications. The corresponding MTC Applications in the external network are hosted on one or multiple ASs (Application Servers).

[0022] Further, the SCS 30 and the SME 40 connect to the core network to communicate with the MTC device 10.

[0023] Furthermore, the core network includes an MTC-IWF 21, an HSS 22, and GGSN/P-GW 23 in the HPLMN (Home Public Land Mobile Network), and includes MME/SGSN/MSC 24 and an S-GW 25 in the VPLMN (Visited PLMN). In the core network, each of the MTC-IWF 21 and the GGSN/P-GW 23 serves as a network node which receives a trigger message from its transmission source, each of the MME/SGSN/MSC 24 and the S-GW 25 serves as a network element which forwards the trigger message to the MTC device 10, and the HSS 22 (or e.g. HLR (Home Location Register)) serves

as a server which provides various information to the network node. Typically, in a case of NAS message, the MTC-IWF 21 receives a trigger message from the SCS 30 via Tsp interface, and then forwards the trigger message to the MME via T5b interface. On the other hand, in a case of SMS message, the MTC-IWF 21 receives a trigger message from the SME 40 via T4 and Tsms interfaces (i.e. through SMS-SC/GMSC/IWMSC) or from the SCS 30 via Tsp interface, and then forwards the trigger message to the MME/SGSN/MSC 24 via T5b/T5a/T5c interface. Thus, the trigger message can be routed by the MME/SGSN/MSC 24 to the MTC device 10. The HSS 22 stores MTC device capabilities and serving node information which will be described later, and notifies them to the MTC-IWF 21 via S6m interface. The GGSN/P-GW 23 receives a trigger message from the SCS 30 or directly from the AS via Gi/SGi interface, and then forwards the trigger message to the SGSN or the S-GW 25 through user plane, so that the trigger message can be also routed to the MTC device 10.

[0024] Next, operation examples of this exemplary embodiment will be described in detail with reference to Fig. 2.

[0025] In this exemplary embodiment, assume that the trigger source (i.e. SCS 30 or SME 40) is properly authenticated to the network (Step S1). Mutual authentication between the MTC device 10 and the network is also performed.

[0026] (1) Optimization of MTC device trigger delivery

1) MTC-IWF 21 downloads UE capabilities from HSS 22 via interface S6m (Step S2). This can be a new message or the same message that MTC-IWF 21 retrieves UE's serving node information from HSS 22. The UE capabilities can include, for example, information on which communication system (e.g. SAE (System Architecture Evolution)/LTE or 3G) the MTC device 10 supports. Preferably, as will be described in the following (2), the UE capabilities may include information as to whether or not the MTC device 10 supports IMS. On the other hand, the serving node information includes usage rates of the MME/SGSN/MSC 24. Additionally, routing information can be downloaded from the HSS 22 or the HLR. Data of routing information, serving node information can be pushed or downloaded from HSS/HLR and saved locally in SMSC/SMS-GMSC.

[0027] The downloading can happen when:

(A) MTC-IWF 21 receives the first trigger; or

(B) MTC device 10 is attached to the network and HSS 22 pushes the information to MTC-IWF 21.

[0028] 2) MTC-IWF 21 stores the UE capabilities and serving node information locally, for a given period (Step S3).

[0029] 3) HSS 22 or MTC-IWF 21 creates a priority list of MTC device trigger delivery

route, with an expiry timer (Step S4). The priority could be simply a random selection, or decided by operator policy of network usage, or based on the serving node information and UE capabilities. Taking as an example the case where the serving node information includes the usage rates, priority list includes records in which the MME/SGSN/MSC 24 are stored in association with their respective usage rates. Further, in the case where the list is created by the HSS 22, the MTC-IWF 21 downloads the list from the HSS 22. The downloading and/or creation are performed before the MTC-IWF 21 receives the trigger from the SCS 30. Note that the list should be removed if MTC-IWF 21 is informed the MTC device 10 is detached or when it is expired.

[0030] 4) MTC-IWF 21 receives the trigger from the SCS 30 (Step S5).

[0031] 5) MTC-IWF 21 performs authorization to SCS 30, to see whether it can send trigger message.

[0032] 6) MTC-IWF 21 checks security context at a given network element, e.g. MME (Steps S6 and S7), which can be done by:

(A) Pinging given network element for information or by analyzing the information received from the HSS; or

(B) Check with the information that provided by HSS 22 when MTC-IWF 21 downloaded the serving node information, or pushed from HSS 22 e.g. when UE changed its location.

[0033] 7) If MME responds that it has no valid security context for the UE, MTC-IWF 21 will send the trigger message to the next serving node in the priority list, e.g. SGSN (Steps S8 and S9). Then, SGSN forwards the trigger message to MTC device 10 (Step S10). MTC-IWF 21 should ensure that it does not choose the same route, by marking the failed path invalid. Thus, it is possible to prevent the trigger message from being redundantly re-forwarded through the failed path, so that the trigger message can more rapidly reach the MTC device 10. The route can be valid if MTC-IWF 21 receives information from HSS 22 or MME that security context is established.

[0034] Thus, in this exemplary embodiment, it is possible to ensure that the trigger message can securely reach the MTC device 10, by deciding the network element which should transfer the trigger message based on the list. In the case where the MTC-IWF 21 creates the list, it is possible to rapidly select the valid path. This is because that the MTC-IWF 21 operates as an entrance into the core network.

[0035] Further, in the case where the list includes records in which the MME/SGSN/MSC 24 are stored in association with their respective usage rates, the MTC-IWF 21 can select the MME/SGSN/MSC 24 in ascending order of usage rate. Therefore, it is possible to reduce congestion of the core network.

[0036] 8) UE (MTC device 10) checks validity of the message carrying the trigger (this follows the current 3GPP specification security requirements) (Step S11).

[0037] 9) If message is not validated correctly then MTC device 10 discards the trigger message (Step S12) and sends a Reject message to MTC-IWF 21 indicating the reject cause (e.g. no proper security protection) (Step S13), otherwise accepts the trigger.

[0038] 10) After received the Reject message, MTC-IWF 21 can do as follows:

(A) Choose the next path which is not marked as invalid from propriety list, and then forward the trigger through the chosen path (Step S14);

(B) When there is no any control plane path available, MTC-IWF 21 can forward the Reject message to SCS 30 such that SCS 30 can send the trigger through user plane (Steps S15 and S16);

(C) Request MME to initiate AKA (Authentication and Key Agreement) and SMC (Short Message Control) procedure to establish security context such that it can forward the trigger message.

[0039] Thus, in this exemplary embodiment, it is also possible to prevent the trigger message from being redundantly re-forwarded by use of the Reject message. Therefore, it is possible to reduce congestion of the core network and battery consumption of the MTC device 10. For example, it can be ensured that an emergent trigger message or the like reaches the MTC device 10.

[0040] Although the illustration is omitted, with respect to user plane, the GGSN/P-GW 23 performs similar processing with that of the MTC-IWF 21. Specifically, the GGSN/P-GW 23 receives from the MTC device 10 a Reject message with a cause indicating there was no proper user plane confidentiality protection, finds another path to deliver the trigger. For example, if a path via the SGSN is not protected, the GGSN/P-GW 23 chooses a protected path via the S-GW 25 to forward the trigger message.

[0041] (2) Consideration of SMS based trigger for non-IMS support MTC device

When the trigger message is sent as SMS, MTC devices which do not support IMS should also be considered. An SMS trigger message carried in NAS message to a MTC device which does not support IMS, CSFB may be initiated such that MME will forward the message to MSC. This will cause unnecessary traffic and delay the trigger delivery.

[0042] In order to avoid them, the operation of this exemplary embodiment is performed as follows.

[0043] 1) MTC-IWF 21 can download MTC device capability of support IMS from HSS 22 as described in (1). When an SMS trigger is to be forwarded, MTC-IWF 21 should check the local stored information to see whether MTC device 10 supports IMS or not.

[0044] 2) If the MTC device 10 does not support IMS, MTC-IWF 21 should forward the trigger directly to MSC, not MME.

[0045] In this way, the SMS trigger message is directly forwarded to the MMC not through the MME. Therefore, it is possible to avoid causing unnecessary traffic from the MME

to the MSC, and thus to prevent the SMS trigger message from being delayed due to the redundant routing through both of the MME and the MSC.

[0046] As shown in Fig. 3, the MTC-IWF 21 includes at least a part or all of a storage unit 211, a selection unit 212, a forwarding unit 213, a reception unit 214, a switching unit 215, a check unit 216, an exclusion unit 217, and a downloading unit 218. These units 211 to 218 are mutually connected with each other through a bus or the like. The storage unit 211 stores the priority list. The selection unit 212 selects one of the MME/SGSN/MSC 24 based on the priority list. The forwarding unit 213 forwards the trigger message to the MTC device 10 through the selected one of the MME/SGSN/MSC 24. The reception unit 214 receives the trigger message from the SCS 30 or the SME 40, and receives the Reject message from the MTC device 10 through the selected one of the MME/SGSN/MSC 24. The switching unit 215 causes the forwarding unit 213 to forward the trigger message through a different one of the MME/SGSN/MSC 24, when the Reject message is received by the reception unit 214. The check unit 216 checks whether or not the selected one of the MME/SGSN/MSC 24 can securely forward the trigger message to the MTC device 10. The exclusion unit 217 instructs the forwarding unit 213 to exclude the selected one of the MME/SGSN/MSC 24 upon the subsequent forwarding, when the check unit 216 determines that the selected one of the MME/SGSN/MSC 24 cannot securely forward the trigger message. The downloading unit 218 can download from the HSS 22 the priority list to be stored in the storage unit 211. Further, the downloading unit 218 downloads the MTC device capability from the HSS 22. When the MTC device capability indicates that the MTC device 10 does not support IMS, the forwarding unit 213 forwards the trigger message directly to the MSC.

[0047] These units 211 to 218 can be configured by, for example, transceivers which respectively conduct communication with the HSS 22, the MME/SGSN/MSC 24, the SCS 30 and the SME 40, and a controller which controls these transceivers to execute the processes shown at Steps S1 to S9 and S13 to S15 in Fig. 2 or processes equivalent thereto. The GGSN/P-GW 23 can be also configured as with the MTC-IWF 21, except conducting communication with the SGSN, the S-GW 25, the SCS 30 and the AS through the user plane.

[0048] Further, as shown in Fig. 4, the MTC device 10 includes at least a reception unit 101, a validity unit 102, and a transmission unit 103. These units 101 to 103 are mutually connected with each other thorough a bus or the like. The reception unit 102 receives the trigger message from the core network. The validity unit 102 validates the trigger message. The transmission unit 103 transmits the Reject message to the core network, when the trigger message is not validated by the validity unit 102. These units 101 to 103 can be configured by, for example, a transceiver which wirelessly conducts com-

munication with the core network through the RAN, and a controller which controls this transceiver to execute the processes shown at Steps S10 to S13 and S16 in Fig. 2 or processes equivalent thereto.

[0049] Furthermore, as shown in Fig. 5, the SCS 30 includes at least a transmission unit 301, a reception unit 302, and a send unit 303. These units 301 to 303 are mutually connected with each other thorough a bus or the like. The transmission unit 301 transmits the trigger message to the core network through control plane (i.e. transmits the trigger message to the MTC-IWF 21 via Tsp interface). The reception unit 302 receives the Reject message from the MTC-IWF 21. The send unit 303 sends the trigger message through user plane (i.e. sends the trigger message to the GGSN/P-GW 23 via Gi/SGi interface), when the Reject message is received by the reception unit 302. These units 301 to 303 can be configured by, for example, transceivers which respectively conduct communication with the MTC-IWF 21 and the GGSN/P-GW 23, and a controller which controls these transceivers to execute the processes shown at Steps S1, S5, S15 and S16 in Fig. 2 or processes equivalent thereto. The SME 40 can be also configured as with the SCS 30, except transmitting the trigger message to the MSC-IWF 21 via the SMS-SC/GMSC/IWMSC.

[0050] Note that the present invention is not limited to the above-mentioned exemplary embodiment, 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.

[0051] For example, the MTC-IWF 21 or the GGSN/P-GW 23 may transfer the trigger message through a different network element, when a response to the trigger message is not received within a predetermined period of time. Specifically, the reception unit 214 receives the response from the MTC device 10. If the response is not received by the reception unit 214 within the period of time, the switching unit 215 causes the forwarding unit 213 to forward the trigger message through a network element different from the selected network element. Note that the period of time can be measured by use of a timer, a counter or the like. Thus, it can be also ensured that the trigger message reaches the MTC device 10. In this case, it may not be required for the MTC device 10 to sends the Reject message, so that modification to the MTC device 10 can be reduced compared with the above-mentioned exemplary embodiment.

[0052] The whole or part of the exemplary embodiment disclosed above can be described as, but not limited to, the following supplementary notes.

[0053] (Supplementary note 1)

MTC-IWF downloads (requesting or being pushed) MTC device capabilities from HSS via interface S6m including for example if MTC device supports IMS. This can be a new message or a new field in the message which MTC-IWF retrieves MTC device serving node information.

[0054] (Supplementary note 2)

MTC device trigger delivery route priority list. This list is created based on the operator policy of network usage and/or by UE capability. The list can be created in HSS then pushed to MTC-IWF, or created by MTC-IWF after it downloaded the necessary information from HSS. The list can be stored in MTC-IWF locally.

[0055] (Supplementary note 3)

If a MME is the serving node, MTC-IWF checks with MME to see if it has valid NAS security context. When MME does not have valid security context, MTC-IWF should forward the trigger to other entities like SGSN/MSC according to the delivery route priority.

[0056] (Supplementary note 4)

When MTC device receives a trigger embedded in an unprotected NAS or user plane message, it sends a Trigger Reject message with cause indication to network node: MTC-IWF or GGSN/P-GW.

[0057] (Supplementary note 5)

MTC-IWF, which receives a reject message with a cause indicating there was no proper NAS protection, finds another path to deliver the trigger. When all the control plane paths are not available, MTC-IWF can initiate AKA and SMC procedure. It also can forward the Reject message to SCS, such that SCS can send the trigger message via user plane.

[0058] (Supplementary note 6)

GGSN/P-GW which receives a reject message with a cause indicating there was no proper user plane confidentiality protection, finds another path to deliver the trigger.

[0059] 2. Discussion

There are two issues discussed in this document.

[0060] First, SA2 TS 23.682 considers roaming in the architecture. In this case, the visited network may not be trusted by the MTC device and the triggers forwarded from such network should not be trusted and taken as valid either.

[0061] Thus MTC device should:

- verify if the MTC-IWF it communicates with is authorized.
- be able to verify if the trigger is from a authorized MTC-IWF. If it is from an invalid MTC-IWF, MTC device should inform MME such that MME will suspend the communication with MTC-IWF and may have a further action.

[0062] Second, when the MTC device receives a trigger without NAS integrity protection, the MTC device (as described in TR 33.868) "could discard the trigger or alternatively look deeper into the trigger if end-to-end protection was applied".

[0063] A few things are concerned:

- The trigger cannot be received and MTC server or MTC user has no knowledge

about the discard.

- It wastes network traffic and MTC device's battery, that if MME sends a trigger which will not be received.

[0064] In order to solve the above described issue:

- MME should not send the trigger without protection in the first place
- If such trigger is received, MTC device should send Reject message to MME/ MTC-IWF/SCS with a cause of reject such that network can act accordingly:
- MME can Initiate AKA procedure to establish security context
- MTC-IWF can send the trigger from another path (i.e. via another network node), for example, SGSN. This can depend on operator policy and/or MTC device capabilities.

[0065] Based on the discussion above, we propose to have the following change to TR 33.868.

[0066] Solution 1: Triggering via NAS signalling

The main Device triggering mechanisms currently being considered in SA2 TR 23.888 [10] are triggering via NAS signalling (e.g. a new information element in an existing NAS message or a new NAS message) and triggering via SMS. The SMS trigger may possibly also be sent from the network to the MTC Device using NAS as a transport. In this case, current NAS security mechanisms can be used to solve the security issue. After NAS SMC, NAS security is activated. All NAS signaling messages should be integrity-protected according to TS 33.401 [13], and therefore current LTE security mechanisms ensure that the trigger indication is not tampered with. In this case the SMS trigger will also benefit from the integrity protection of NAS signalling in LTE.

[0067] Source verification needs to be considered which in this context is understood to mean that the MTC Device can verify that the source of the trigger is a valid MTC server. This could be achieved in the following way.

[0068] MTC Device trusts the 3GPP network sending the NAS integrity protected trigger. In this case the MTC Device could be configured with identities of trusted 3GPP networks. (Somewhat analogically as trusted non3GPP access networks can be configured in the UE in TS 33.402.) In this context trusted 3GPP network would mean networks which have a secured interface from the MTC server to the 3GPP network, and which are trusted to ensure that only trigger indications received from authorized MTC Servers will lead to triggering of MTC Devices "belonging" to that MTC server.

[0069] The network may not be trusted for example when MTC device is roaming in the visited network, or when there is a strict security requirement for MTC. The MTC device should verify if the trigger is forwarded from a valid MTC-IWF.

[0070] When the MTC Device then receives a NAS integrity protected trigger, it can, after

verifying NAS integrity protection, verify the 3GPP network in the sense as described above. If both can be verified, the trigger can be accepted.

[0071] MME should not send the trigger in a NAS message without integrity protection. If there is no NAS integrity protection of the trigger or if the 3GPP network is not trusted, the MTC Device could discard the trigger and send a Reject message to MME and MTC-IWF with a proper cause or alternatively look deeper into the trigger if end-to-end protection was applied.

[0072] When MME receives a reject response from MTC device with a cause indicating no integrity protection or integrity check failure, MME can

- Initiate 3GPP AKA procedure towards MTC device so that when there is security context shared between them MME can forward the trigger;
- Or forward the reject message to MTC-IWF, so that MTC-IWF can choose another route to send the trigger.

[0073] This application is based upon and claims the benefit of priority from Japanese patent application No. 2012-147982, filed on June 29, 2012, and Japanese patent application No. 2012-209393, filed on September 24, 2012, the disclosures of which are incorporated herein in their entirety by reference.

Reference Signs List

[0074] 10 MTC DEVICE
21 MTC-IWF
22 HSS
23 GGSN/P-GW
24 MME/SGSN/MSC
25 S-GW
30 SCS
40 SME
101, 214, 302 RECEPTION UNIT
102 VALIDITY UNIT
103, 301 TRANSMISSION UNIT
211 STORAGE UNIT
212 SELECTION UNIT
213 FORWARDING UNIT
215 SWITCHING UNIT
216 CHECK UNIT
217 EXCLUSION UNIT
218 DOWNLOADING UNIT
303 SEND UNIT

Claims

[Claim 1] A network node placed within a core network, comprising:
a storage means for storing a list of network elements capable of forwarding a trigger message to a MTC (Machine-Type-Communication) device attached to the core network, the trigger message being received from a transmission source placed outside the core network; and
a selection means for selecting, based on the list, one network element to forward the trigger message to the MTC device.

[Claim 2] The network node according to Claim 1,
wherein the storage means is configured to:
download information of the network elements from a server; and
create the list by use of the downloaded information,
wherein the downloading and the creation are performed prior to a reception of the trigger message.

[Claim 3] The network node according to Claim 1,
wherein the list is created by a server based on information of the network elements, and
wherein the storage means is configured to download the list from the server, and
wherein the downloading is performed prior to a reception of the trigger message.

[Claim 4] The network node according to any one of Claims 1 to 3,
wherein in the list, the network elements are stored in association with their respective usage rates, and
wherein the selection means is configured to select, as said one network element, the network elements in ascending order of usage rate.

[Claim 5] The network node according to any one of Claims 1 to 4, wherein the selection means is configured to check whether or not said one network element can securely forward the trigger message to the MTC device, by pinging said one network element or analyzing information on said one network element received from a server.

[Claim 6] The network node according to any one of Claims 1 to 5, wherein the network node comprises an MTC-IWF (MTC-Interworking Function), a GGSN (Gateway GPRS (General Packet Radio Service) Support Node), or a P-GW (PDN (Packet data network) Gateway).

[Claim 7] A MTC (Machine-Type-Communication) device attached to a core

network, and configured to receive a trigger message forwarded by the network node according to any one of Claims 1 to 6.

[Claim 8] A network node placed outside a core network, and configured to transmit a trigger message to the network node according to any one of Claims 1 to 6.

[Claim 9] The network node according to Claim 8, wherein the network node placed outside the core network comprises an SCS (Services Capability Server) or an SME (Short Message Entity).

[Claim 10] A method of controlling a network node that is placed within a core network and that forwards a trigger message to a MTC (Machine-Type-Communication) device attached to the core network, a transmission source of the trigger message being placed outside the core network, the method comprising:
storing a list of network elements capable of forwarding the trigger message to the MTC device; and
selecting, based on the list, one network element to forward the trigger message to the MTC device.

[Claim 11] A network node placed within a core network, comprising:
a forwarding means for forwarding a trigger message received from a transmission source placed outside the core network to a MTC (Machine-Type-Communication) device attached to the core network through one of network elements capable of forwarding the trigger message to the MTC device;
a reception means for receiving from the MTC device a reject message indicating that the trigger message is not accepted by the MTC device; and
a switching means for causing, when the reject message is received, the forwarding means to forward the trigger message through a different one of the network elements.

[Claim 12] The network node according to Claim 11, wherein the reject message further indicates a cause for which the trigger message is not accepted by the MTC device.

[Claim 13] The network node according to Claim 12, wherein the cause indicates that the trigger message does not have proper security protection.

[Claim 14] The network node according to any one of Claims 11 to 13,
wherein each of network elements forwards the trigger message through control plane, and
wherein the switching means is configured to forward, when no

network element can securely forward the trigger message, the reject message to the transmission source to send the trigger message through user plane.

[Claim 15] The network node according to any one of Claims 11 to 13, further comprising:
a request means for requesting, when no network element can securely forward the trigger message, any one of the network elements to establish a secure connection between said any one of the network elements and the MTC device.

[Claim 16] The network node according to any one of Claims 11 to 15, wherein the network node comprises an MTC-IWF (MTC-Interworking Function), a GGSN (Gateway GPRS (General Packet Radio Service) Support Node), or a P-GW (PDN (Packet data network) Gateway).

[Claim 17] A MTC (Machine-Type-Communication) device attached to a core network, comprising:
a reception means for receiving a trigger message from the core network;
a validity means for validating the trigger message; and
a transmission means for transmitting, when the trigger message is not validated, to the core network a reject message indicating that the trigger message is not accepted by the MTC device itself.

[Claim 18] The MTC device according to Claim 17, wherein the transmission means is configured to include, in the reject message, a cause for which the trigger message is not accepted by the MTC device itself.

[Claim 19] The MTC device according to Claim 18, wherein the cause indicates that the trigger message does not have proper security protection.

[Claim 20] A network node placed outside a core network, comprising:
a transmission means for transmitting, to the core network through control plane, a trigger message addressed to a MTC (Machine-Type-Communication) device;
a reception means for receiving from the core network a reject message indicating that the trigger message is not accepted by the MTC device; and
a send means for sending, when the reject message is received, the trigger message through user plane.

[Claim 21] The network node according to Claim 20, wherein the reject message further indicates a cause for which the trigger message is not accepted by the MTC device.

[Claim 22] The network node according to Claim 21, wherein the cause indicates that the trigger message does not have proper security protection.

[Claim 23] The network node according to any one of Claims 20 to 22, wherein the network node comprises an SCS (Services Capability Server).

[Claim 24] A method of controlling a network node placed within a core network, the method comprising:
forwarding a trigger message received from a transmission source placed outside the core network to a MTC (Machine-Type-Communication) device attached to the core network through one of network elements capable of forwarding the trigger message to the MTC device;
receiving from the MTC device a reject message indicating that the trigger message is not accepted by the MTC device; and
forwarding, when the reject message is received, the trigger message through a different one of the network elements.

[Claim 25] A method of controlling a MTC (Machine-Type-Communication) device attached to a core network, the method comprising:
receiving a trigger message from the core network;
validating the trigger message; and
transmitting, when the trigger message is not validated, to the core network a reject message indicating that the trigger message is not accepted by the MTC device itself.

[Claim 26] A method of controlling a network node placed outside a core network, the method comprising:
transmitting, to the core network through control plane, a trigger message addressed to a MTC (Machine-Type-Communication) device;
receiving from the core network a reject message indicating that the trigger message is not accepted by the MTC device; and
sending, when the reject message is received, the trigger message through user plane.

[Claim 27] A network node placed within a core network, comprising:
a forwarding means for forwarding a trigger message to a MTC (Machine-Type-Communication) device attached to the core network through one of network elements capable of forwarding the trigger message to the MTC device, the trigger message being received from a transmission source placed outside the core network;
a check means for checking whether or not said one network element can securely forward the trigger message to the MTC device; and

an exclusion means for instructing, when said one network element cannot securely forward the trigger message, the forward means to exclude said one network element upon the subsequent forwarding.

[Claim 28] The network node according to Claim 27, wherein the network node comprises an MTC-IWF (MTC-Interworking Function), a GGSN (Gateway GPRS (General Packet Radio Service) Support Node), or a P-GW (PDN (Packet data network) Gateway).

[Claim 29] A MTC (Machine-Type-Communication) device attached to a core network, and configured to receive a trigger message forwarded by the network node according to Claim 27 or 28.

[Claim 30] A network node placed outside a core network, and configured to transmit a trigger message to the network node according to Claim 27 or 28.

[Claim 31] The network node according to Claim 30, wherein the network node placed outside the core network comprises an SCS (Services Capability Server) or an SME (Short Message Entity).

[Claim 32] A method of controlling a network node placed within a core network, the method comprising:
forwarding a trigger message to a MTC (Machine-Type-Communication) device attached to the core network through one of network elements capable of forwarding the trigger message to the MTC device, the trigger message being received from a transmission source placed outside the core network;
checking whether or not said one network element can securely forward the trigger message to the MTC device; and
excluding, when said one network element cannot securely forward the trigger message, said one network element upon the subsequent forwarding.

[Claim 33] A network node placed within a core network, comprising:
a forwarding means for forwarding a trigger message to a MTC (Machine-Type-Communication) device attached to the core network through one of network elements capable of forwarding the trigger message to the MTC device, the trigger message being received from a transmission source placed outside the core network;
a reception means for receiving a response to the trigger message from the MTC device through said one of network elements; and
a switching means for causing, when the response is not received within a predetermined period of time, the forwarding means to

forward the trigger message through a different one of the network elements.

[Claim 34] The network node according to Claim 33, wherein the network node comprises an MTC-IWF (MTC-Interworking Function), a GGSN (Gateway GPRS (General Packet Radio Service) Support Node), or a P-GW (PDN (Packet data network) Gateway).

[Claim 35] A MTC (Machine-Type-Communication) device attached to a core network, and configured to receive a trigger message forwarded by the network node according to Claim 33 or 34.

[Claim 36] A network node placed outside a core network, and configured to transmit a trigger message to the network node according to Claim 33 or 34.

[Claim 37] The network node according to Claim 36, wherein the network node placed outside the core network comprises an SCS (Services Capability Server) or an SME (Short Message Entity).

[Claim 38] A method of controlling a network node placed within a core network, the method comprising:
forwarding a trigger message to a MTC (Machine-Type-Communication) device attached to the core network through one of network elements capable of forwarding the trigger message to the MTC device, the trigger message being received from a transmission source placed outside the core network;
receiving a response to the trigger message from the MTC device through said one of network elements; and
forwarding, when the response is not received within a predetermined period of time, the trigger message through a different one of the network elements.

[Claim 39] A network node placed within a core network that supports CSFB (CS (Circuit Switched) Fall Back), the network node comprising:
a downloading means for downloading, from a server, a capability of a MTC (Machine-Type-Communication) device attached to the core network, the capability indicating whether or not the MTC device supports IMS (IP (Internet Protocol) Multimedia Subsystem); and
a forwarding means for forwarding, when the MTC device does not support IMS, a trigger message addressed to the MTC device directly to a MSC (Mobile Switching Centre).

[Claim 40] The network node according to Claim 39, wherein the network node comprises an MTC-IWF (MTC-Interworking Function).

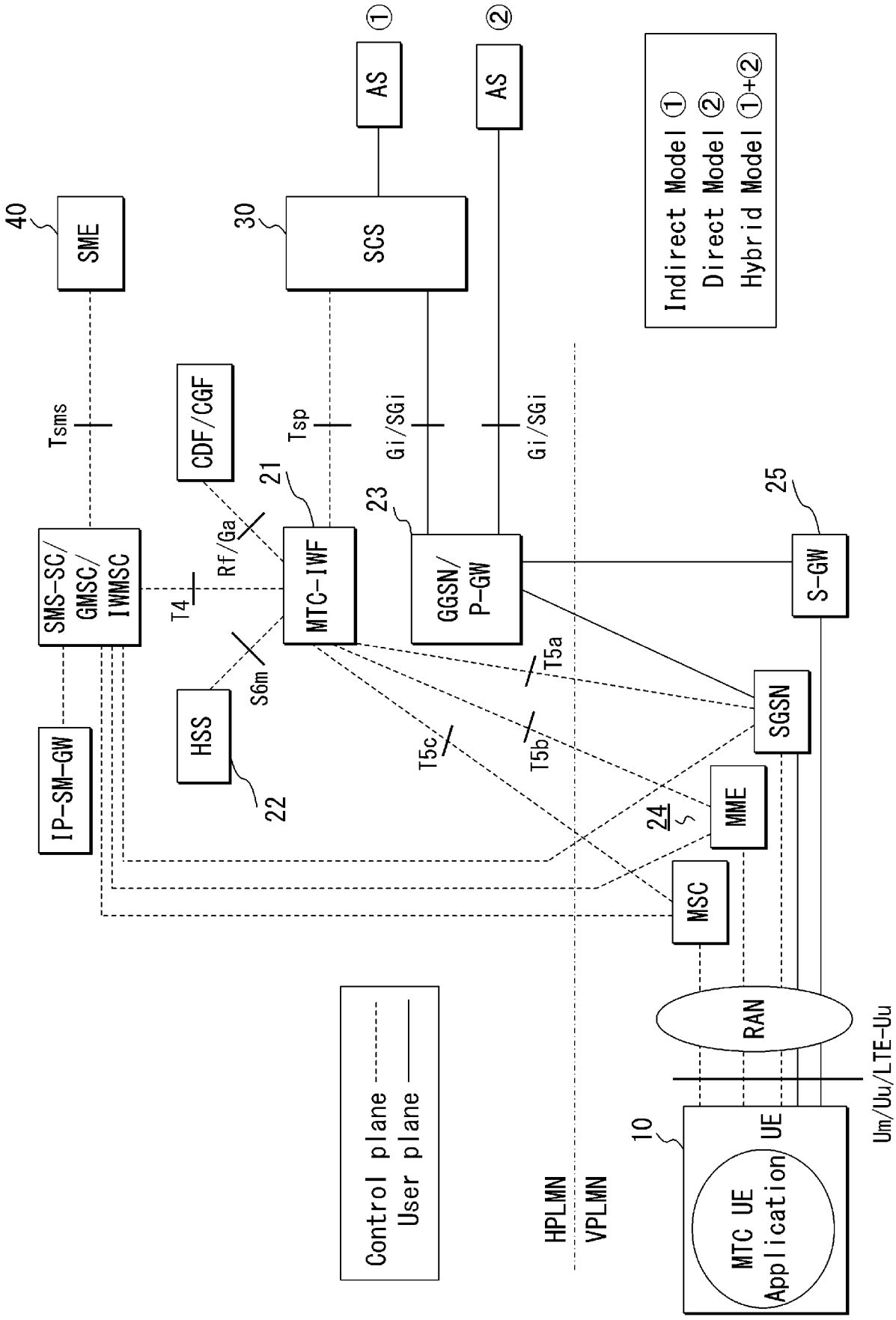
[Claim 41] A MTC (Machine-Type-Communication) device attached to a core network, and configured to receive a trigger message forwarded by the network node according to Claim 39 or 40.

[Claim 42] A network node placed outside a core network, and configured to transmit a trigger message to the network node according to Claim 39 or 40.

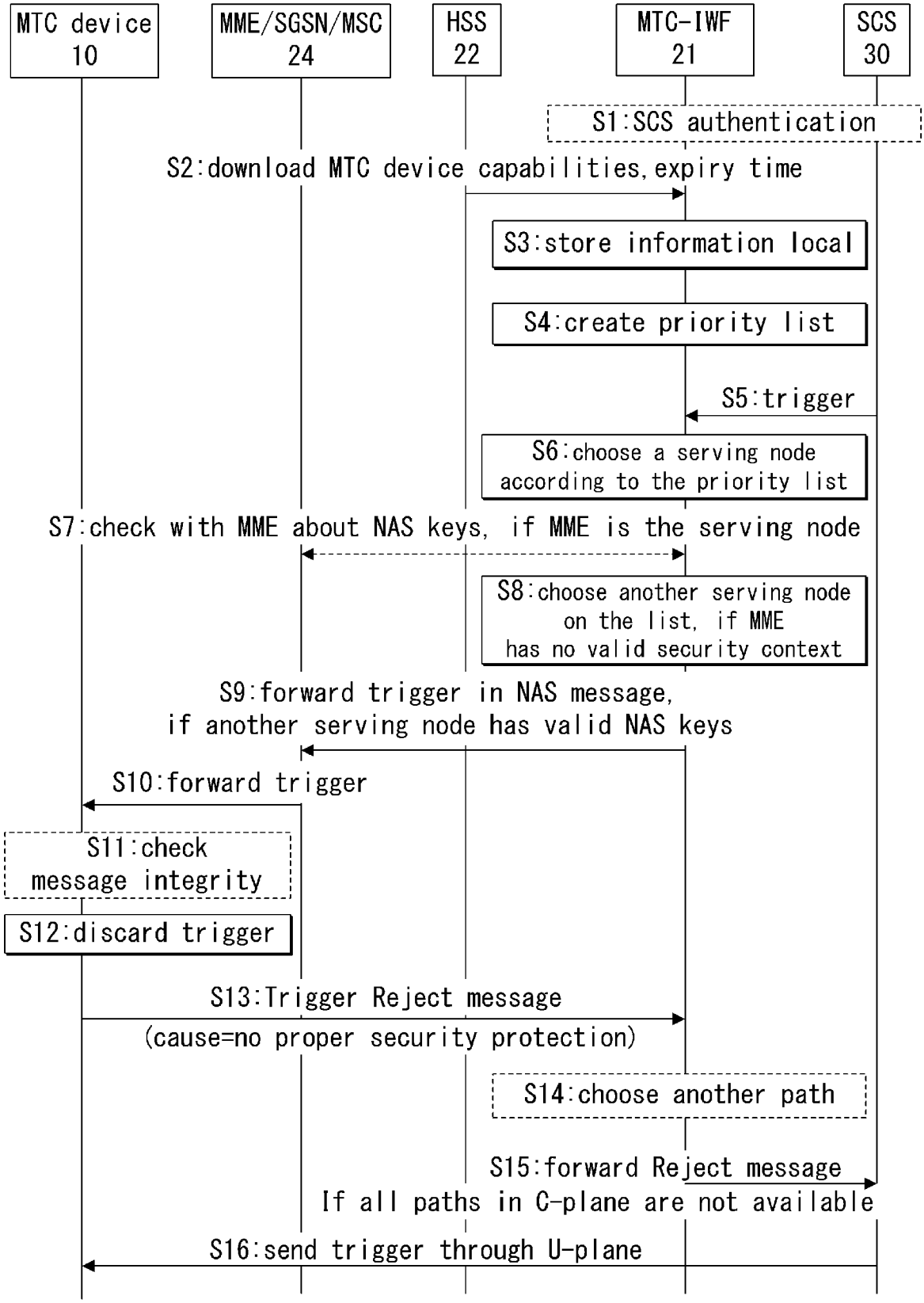
[Claim 43] The network node according to Claim 42, wherein the network node placed outside the core network comprises an SCS (Services Capability Server) or an SME (Short Message Entity).

[Claim 44] A method of controlling a network node placed within a core network that supports CSFB (CS (Circuit Switched) Fall Back), the method comprising:
downloading, from a server, a capability of a MTC (Machine-Type-Communication) device attached to the core network, the capability indicating whether or not the MTC device supports IMS (IP (Internet Protocol) Multimedia Subsystem); and
forwarding, when the MTC device does not support IMS, a trigger message addressed to the MTC device directly to a MSC (Mobile Switching Centre).

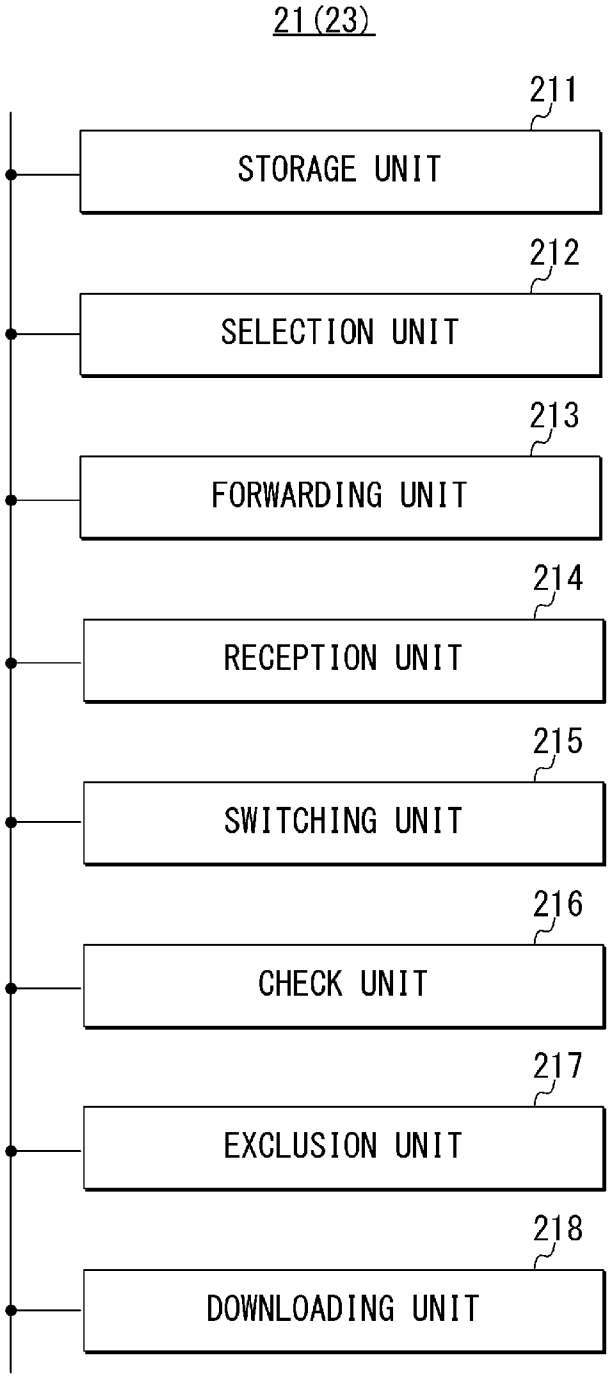
[Fig. 1]


AS
①
AS
②
Indirect Model ①
Direct Model ②
Hybrid Model ①+②
40
SME
30
SCS
Tsms
CDF/CGF
Tsp
Gi/SGi
Gi/SGi
21
23
25
SMS-SC/
GMSC/
IWMSC
Rf/Ga
MTC-IWF
GGSN/
P-GW
S-GW
T4
T5a
S6m
HSS
SGSN
T5c
T5b
IP-SM-GW
22
24
MME
MSC
RAN
Um/Uu/LTE-Uu
10
UE
MTC UE
Application
HPLMN
VPLMN
Control plane
User plane

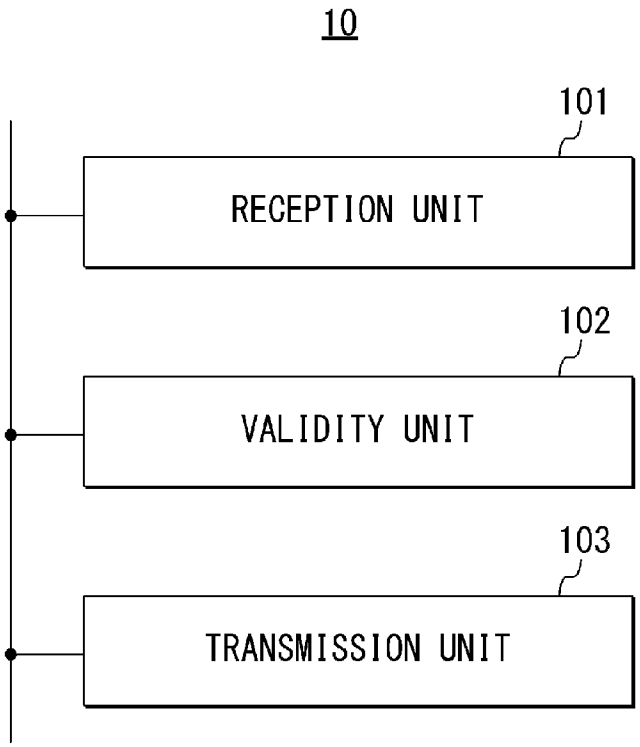
[Fig. 2]


MTC device 10
MME/SGSN/MSC 24
HSS 22
MTC-IWF 21
SCS 30
S1:SCS authentication
S2:download MTC device capabilities, expiry time
S3:store information local
S4:create priority list
S5:trigger
S6:choose a serving node according to the priority list
S7:check with MME about NAS keys, if MME is the serving node
S8:choose another serving node on the list, if MME has no valid security context
S9:forward trigger in NAS message, if another serving node has valid NAS keys
S10:forward trigger
S11:check message integrity
S12:discard trigger
S13:Trigger Reject message
(cause=no proper security protection)
S14:choose another path
S15:forward Reject message
If all paths in C-plane are not available
S16:send trigger through U-plane

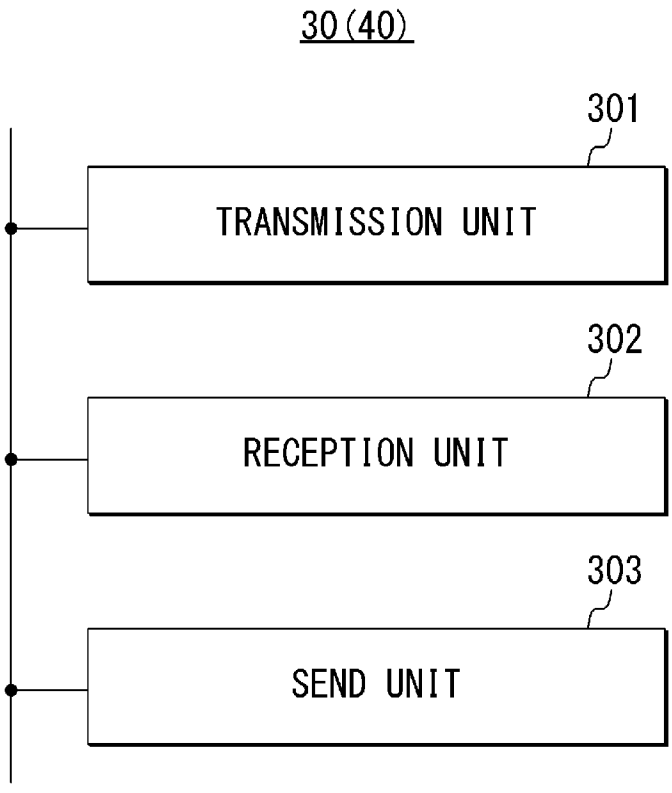
[Fig. 3]


21(23)
211
STORAGE UNIT
212
SELECTION UNIT
213
FORWARDING UNIT
214
RECEPTION UNIT
215
SWITCHING UNIT
216
CHECK UNIT
217
EXCLUSION UNIT
218
DOWNLOADING UNIT

[Fig. 4]


10
101
RECEPTION UNIT
102
VALIDITY UNIT
103
TRANSMISSION UNIT

[Fig. 5]


30(40)
301
TRANSMISSION UNIT
302
RECEPTION UNIT
303
SEND UNIT

INTERNATIONAL SEARCH REPORT

International application No
PCT/JP2013/002757

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W4/00
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, COMPENDEX, INSPEC, IBM-TDB, 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	SIERRA WIRELESS: "Solution for MTC Device Trigger indication from MTC Server", 3GPP DRAFT; S2-111038_00295_DEVICE_TRIGGER_SOLUTION, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. Salt Lake City; 20110221, 26 February 2011 (2011-02-26), XP050524100, the whole document ----- -/--	1-10

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 August 2013	24/10/2013

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

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements to facilitate communications with packet data networks and applications (Release 11)", 3GPP STANDARD; 3GPP TS 23.682, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. V11.1.0, 15 June 2012 (2012-06-15), pages 1-27, XP050580726, abstract section 4 section 5	1-10

X	WO 2012/046503 A1 (SONY CORP [JP]; KIMURA RYOTA [JP]) 12 April 2012 (2012-04-12) abstract -& US 2013/163520 A1 (KIMURA RYOTA [JP]) 27 June 2013 (2013-06-27) abstract paragraph [0001] - paragraph [0235] figures 1-24	1-10

X	"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. V1.6.1, 5 March 2012 (2012-03-05), pages 1-165, XP050555302, abstract section 4 section 5 section 6	1-10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/002757

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

see additional sheet(s)

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-10

A method, network node that is placed within a core network and a MTC device attached to the core network, a transmission source of the trigger message being placed outside the core network, the method comprising: storing a list of network elements capable of forwarding the trigger message to the MTC device; and selecting, based on the list, one network element to forward the trigger message to the MTC device.

---

2. claims: 11-19, 24, 25

A method, network node that is placed within a core network and a MTC device attached to the core network, a transmission source of the trigger message being placed outside the core network, the method comprising: receiving from the MTC device a reject message indicating that the trigger message is not accepted by the MTC device; and forwarding, when the reject message is received, the trigger message through a different one of the network elements.

---

3. claims: 20-23, 26

A method, network node that is placed outside a core network and a MTC device, transmitting to the core network through control plane a trigger message addressed to a MTC device, the method comprising: receiving from the core network a reject message indicating that the trigger message is not accepted by the MTC device; and sending, when the reject message is received, the trigger message through user plane.

---

4. claims: 27-32

A method, network node that is placed within a core network and a MTC device attached to the core network, a transmission source of the trigger message being placed outside the core network, the method comprising: checking whether or not said one network element can securely forward the trigger message to the MTC device; and excluding, when said one network element cannot securely forward the trigger message, said one network element upon the subsequent forwarding.

---

5. claims: 33-38

A method, network node that is placed within a core network

and a MTC device attached to the core network, a transmission source of the trigger message being placed outside the core network, the method comprising: receiving a response to the trigger message from the MTC device through said one of network elements; and forwarding, when the response is not received within a predetermined period of time, the trigger message through a different one of the network elements.

---

6. claims: 39-44

A method, network node placed within a core network that supports CSFB (CS (Circuit Switched) Fall Back) and MTC device attached to the core network comprising: downloading, from a server, a capability of a MTC (Machine-Type-Communication) device attached to the core network, the capability indicating whether or not the MTC device supports IMS (IP (Internet Protocol) Multimedia Subsystem); and forwarding, when the MTC device does not support IMS, a trigger message addressed to the MTC device directly to a MSC (Mobile Switching Centre).

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/JP2013/002757

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2012046503 A1	12-04-2012	AU 2011311009 A1	28-03-2013
		CA 2808204 A1	12-04-2012
		CN 103155649 A	12-06-2013
		EP 2627123 A1	14-08-2013
		JP 2012080413 A	19-04-2012
		US 2013163520 A1	27-06-2013
		WO 2012046503 A1	12-04-2012
US 2013163520 A1	27-06-2013	AU 2011311009 A1	28-03-2013
		CA 2808204 A1	12-04-2012
		CN 103155649 A	12-06-2013
		EP 2627123 A1	14-08-2013
		JP 2012080413 A	19-04-2012
		US 2013163520 A1	27-06-2013
		WO 2012046503 A1	12-04-2012